UNIVERSIDAD DE GRANADA

PROGRAMA DE DOCTORADO EN CRIMINOLOGÍA

TESIS DOCTORAL

ANÁLISIS CRIMINOLÓGICO DE LA DELINCUENCIA CON CRIPTOMONEDAS COMETIDA POR GRUPOS CRIMINALES Y SU APROXIMACIÓN DESDE LOS SISTEMAS INTELIGENTES

DOCTORANDA: PATRICIA SALDAÑA TABOADA

DIRECTORES: Prof. *Dr.* JAVIER VALLS PRIETO
Prof. *Dr.* JUAN GÓMEZ ROMERO

Granada, 2023

Editor: Universidad de Granada. Tesis Doctorales
Autor: Patricia Saldaña Taboada
ISBN: 978-84-1117-809-9
URI: https://hdl.handle.net/10481/81413

A mis padres y a mi hermana, por su cariño, su paciencia y su apoyo incondicional.

A Pablo, mi mayor tesoro.

Financiación

Esta tesis ha sido financiada por el Ministerio de Universidades a través de su programa de ayudas para la formación de profesorado universitario (FPU) con referencia FPU19/06616.

Al mismo tiempo, se han financiado dos estancias breves de investigación de tres meses de duración cada una. La primera de ellas, con destino en la Universidad de Mánchester, ha sido financiada a través del programa de Movilidad Internacional de Estudiantes de Doctorado de la Universidad de Granada en su convocatoria 2019/2020. La segunda, con destino en la Universidad de Montreal, fue financiada por el Ministerio de Universidades a través de su programa de ayudas para estancias breves y traslados temporales para beneficiarios de ayudas FPU en su convocatoria 2020/2021 con referencia EST21/00386.

Índice

Lista de abreviaturas

Acrónimo	Significado
AI	*Artificial Intelligence* (Inteligencia Artificial)
Art.	Artículo
ATM	*Automated Teller Machine* (Cajero automático)
BD	*Big Data*
BDE	Banco de España
BTC	Bitcoin
CaaS	*Crime-as-a-Service*
CEO	*Chief Executive Officer* (Director ejecutivo)
CNMV	Comisión Nacional del Mercado de Valores
CP	Código Penal
CPU	*Central Processing Unit* (Unidad Central de Procesamiento)
DoS	*Denial of Service* (Denegación de Servicio)
DeFi	*Decentralized Finance* (Finanzas descentralizadas)
DLT	*Distributed Ledger Tecnology* (Tecnología de Registro Distribuido)
DN	*Darknet*
DNM	*Darknet Market (*Mercado de la red oscura)
ECDSA	*Elliptic Curve Digital Signature Algorithm*
ETH	Ether
FCSE	Fuerzas y Cuerpos de Seguridad del Estado
FATF	*Financial Action Task Force* (Grupo de Acción Financiera Internacional)
GAFI	Grupo de Acción Financiera Internacional
GPU	*Graphics Processing Unit* (Unidad de Procesamiento Gráfico)
HSes	*Hidden Services* (Servicios ocultos)
IA	Inteligencia Artificial
I2P	*Invisible Internet Project* (I2P)
ICO	*Initial Coin Offering* (Oferta Inicial de Moneda)
IOCTA	*Internet Organised Crime Threat Assessment*
IVA	Impuesto sobre el Valor Añadido
KYC	*Know Your Customer* (Conoce a tu cliente)

LECrim	Ley de Enjuiciamiento Criminal
LDCA	*Live Distant Child Abuse* (Abuso sexual infantil *online*)
LO	Ley Orgánica
LTC	Litecoin
OCTA	*Organized Crime Threat Assessment*
OTP	*One-time password* (contraseña de un solo uso)
P2P	*Peer-to-Peer network* (Red de pares)
PC	*Personal Computer* (Ordenador personal)
PGP	*Pretty Good Privacy*
PoW	*Proof of Work* (Prueba de trabajo)
RPOW	*Reusable Proof Of Work* (Prueba de Trabajo Reutilizable)
SOCTA	*Serious and Organized Crime Threat Assessment*
TICs	Tecnologías de la Información y la Comunicación
TOR	*The Onion Router*
XMR	Monero
XRP	Ripple

Índice de tablas

Índice de figuras

Resumen

El origen de las criptomonedas tuvo lugar con la creación del Bitcoin por Satoshi Nakamoto. Su aparición se vio impulsada por la crisis económica del año 2008 que ocasionó un aumento de la desconfianza de la población hacia las entidades bancarias. Se consideraba que el comercio electrónico dependía excesivamente de las entidades bancarias, que actuaban como intermediarios capaces de revertir las transacciones realizadas. Por lo tanto, surgió un sistema de pago que, a través de su criptomoneda Bitcoin, permitía la realización de transacciones directamente entre personas sin intermediarios, de una forma segura debido a la protección mediante criptografía y que no disponía de ningún dato de carácter personal, dotándolo de anonimato. De esta forma, se daba respuesta a un amplio sector de la población que exigía un sistema de pago que garantizara la privacidad de su actividad financiera.

Sin embargo, al mismo tiempo las criptomonedas se han utilizado en el ámbito criminal. Las mismas características que garantizaban la privacidad del comercio electrónico con carácter legal, han favorecido el desarrollo de una gran variedad de actividades delictivas. Por ejemplo, el blanqueo de capitales, las estafas, los ataques *ransomware* y la criminalidad organizada. Esta tecnología ha permitido a los criminales la realización de transacciones anónimas, descentralizadas, internacionales, de bajo coste, sin intermediarios, rápidas y que permiten su conversión a otras monedas fiduciarias.

Todo ello, ha ocasionado la preocupación de las autoridades, que se enfrentan a una tecnología que favorece su utilización para el delito y que al mismo tiempo dificulta su detección y su persecución. Por ello, se han desarrollado una gran cantidad de investigaciones dirigidas al descubrimiento de los autores de las direcciones Bitcoin y al estudio de la *Blockchain* con el propósito de determinar patrones de actividades sospechosas de ser un delito con el objetivo de facilitar a las autoridades encargadas de la lucha contra la criminalidad la detección, persecución y prevención de este tipo de criminalidad, especialmente mediante el desarrollo de herramientas de análisis forense de la *Blockchain.*

No obstante, debido a la complejidad de este fenómeno criminal, se considera que es necesario ampliar su estudio y abordar otros aspectos del delito que vayan más allá de la detección, persecución y aprehensión de sus autores. Se requiere de una

aproximación criminológica que permita comprenderlo en su totalidad y elaborar políticas de prevención adecuadas en el futuro.

La hipótesis de partida es que una comprensión global del fenómeno criminal desde todos los elementos del delito permitiría determinar su importancia como herramienta para el delito y dirigir las actuaciones hacia los aspectos clave de estos delitos.

El objetivo general de este trabajo de investigación será estudiar el crimen con criptomonedas desde una perspectiva criminológica. Para ello, se han previsto varios objetivos específicos que se van a centrar en el estudio del autor, las víctimas, los tipos de delitos cometidos y las motivaciones criminales.

Para alcanzar los objetivos propuestos se ha llevado a cabo una metodología de carácter mixto que combina metodologías cuantitativas y cuantitativas a través del desarrollo de cinco experimentos. El primero de ellos se corresponde con la aplicación de sistemas inteligentes a casos de criminalidad en esta materia con el objetivo de obtener nuevo conocimiento que pudiera guiar esta investigación y las actuaciones policiales. Los cuatro experimentos restantes abordan cada uno de los aspectos del delito que se consideran relevantes para la comprensión del fenómeno que son: los autores, los tipos de delito, las víctimas y las motivaciones criminales.

Los resultados obtenidos muestran que: 1) los grupos criminales son el perfil de autor mayoritario; 2) Han surgido nuevos perfiles de autores individuales que son autodidactas; 3) predominan los delitos contra la propiedad; 4) la victimización depende de los patrones socioespaciales de autores y víctimas y por último y 5) la decisión de utilizar las criptomonedas puede verse influenciada por otros factores diferentes a sus características como los que permiten una mayor rentabilidad para el negocio criminal.

Finalmente, los resultados obtenidos podrían servir para orientar el desarrollo posterior de actuaciones de detección, persecución y lucha contra la criminalidad cometida con criptomonedas, así como para la elaboración de medidas de prevención del delito dirigidas las víctimas identificadas como potenciales y a los delitos más frecuentes.

Abstract

Cryptocurrencies originated with the creation of Bitcoin by Satoshi Nakamoto. Its emergence was prompted by the economic crisis of 2008, which led to an increase in public distrust of banking institutions. E-commerce was seen as overly dependent on banks, which acted as intermediaries capable of reversing the transactions made. Therefore, a payment system emerged which, using its cryptocurrency Bitcoin, allowed transactions to be carried out directly between people without intermediaries, in a secure way due to cryptographic protection and without any personal data, providing anonymity. In this way, a response was provided to a large sector of the population that demanded a payment system that guaranteed the privacy of their financial activity.

However, cryptocurrencies have also been used in the criminal realm. The same characteristics that ensured the privacy of legal e-commerce have favoured the development of a wide range of criminal activities. For example, money laundering, scams, *ransomware* attacks and organised crime. This technology has enabled criminals to conduct anonymous, decentralised, international, low-cost, unmediated, fast transactions that can be converted into other fiat currencies.

All of this has caused concern among the authorities, who are faced with a technology that favours its use for crime and makes it difficult to detect and prosecute. As a result, many investigations have been carried out to discover the authors of Bitcoin addresses and to study the Blockchain. The aim was to identify patterns of suspected criminal activity and to make it easier for law enforcement authorities to detect, prosecute and prevent this type of crime, especially through the development of Blockchain forensic analysis tools.

However, due to the complexity of this criminal phenomenon, it is considered necessary to broaden its study and address other aspects of crime that go beyond the detection, prosecution, and apprehension of its perpetrators. A criminological approach is required to understand it in its entirety and to develop appropriate prevention policies in the future.

The initial hypothesis is that a comprehensive understanding of the criminal phenomenon from all the elements of the crime would allow us to determine its importance as a tool for crime and to direct actions towards the key aspects of these crimes.

The main objective of this research will be to study cryptocurrency crime from a criminological perspective. To this end, several specific objectives have been set that will focus on the study of the offender, the victims, the types of crimes committed and the criminal motivations.

To achieve the proposed objectives, a mixed methodology combining quantitative and quantitative methodologies has been carried out through the development of five experiments. The first of them corresponds to the application of intelligent systems to cases of crime in this area with the aim of obtaining new knowledge that could guide this research and police actions. The remaining four experiments address each of the aspects of crime that are considered relevant to understanding the phenomenon: offenders, types of crime, victims, and criminal motivations.

The results obtained show that: 1) criminal groups are the majority perpetrator profile; 2) new profiles of individual offenders who are self-taught have emerged; 3) property crimes predominate; 4) victimis ation depends on the socio-spatial patterns of perpetrators and victims; 5) the decision to use cryptocurrencies can be influenced by factors other than their characteristics, such as those that allow for greater profitability for the criminal business.

Finally, the results obtained could be used to guide the subsequent development of actions to detect, prosecute and combat crime committed with cryptocurrencies, as well as for the development of crime prevention measures aimed at the victims identified as potential victims and the most frequent crimes.

Introducción

En las últimas décadas se ha podido observar un enorme avance tecnológico fruto de aumento en la utilización de las Tecnologías de la Información y la Comunicación (TICs) y un uso generalizado de Internet, lo que ha supuesto grandes beneficios para la sociedad (Fernández y Martínez, 2018). Se ha permitido una rápida comunicación y conexión entre personas situadas en cualquier parte del mundo y a cualquier momento, reduciendo los costes y aumentando su eficiencia. La tecnología ha avanzado para poder adaptarse a las necesidades de la sociedad, otorgándole multitud de beneficios.

Como parte de este avance tecnológico en el año 2009 surgió el Bitcoin marcando el inicio de las criptomonedas. Su creador, Satoshi Nakamoto, tenía como objetivo la creación de un sistema de pago descentralizado que dejara atrás la figura del intermediario habitualmente ocupada por entidades bancarias (Nakamoto, 2008). Según la explicación que él mismo ofrece en el documento en el que presenta esta tecnología, el comercio electrónico en aquel momento estaba fuertemente influenciado por intermediarios que tenían la posibilidad de intervenir en las transacciones realizadas y poder revertirlas lo que impedía la realización de transacciones irreversibles.

Aunque esta idea de sistema de pago se basaba en propuestas similares creadas con anterioridad, su aparición en el año 2009 estuvo motivada por la crisis financiera que tuvo lugar en el año 2008. A partir de este momento, la sociedad se hizo consciente de la relevancia que tenían las entidades bancarias en el comercio electrónico y aumentó la desconfianza hacia estos servicios (Ammous, 2018). Por lo tanto, el proyecto Bitcoin, se presenta como una alternativa al comercio electrónico habitual que estaba dominado por los bancos.

Si bien el sistema de pago Bitcoin fue pionero, su creador Satoshi Nakamoto, del cual se desconoce su identidad, utilizó en su desarrollo tecnologías que ya existían con anterioridad, como por ejemplo las redes *Peer-to-Peer* (P2P) o las pruebas de trabajo (Nakamoto, 2008). El éxito de esta propuesta en comparación con las anteriormente realizadas por otros autores como el "Bit Gold" (Szabo, 2005) se debe a que Nakamoto propuso por primera vez una solución a los problemas que surgían con la eliminación de los intermediarios en el comercio electrónico. Esta figura en los sistemas centralizados es la encargada de supervisar que una misma moneda no se pueda utilizar varias veces en diferentes transacciones, lo que conoce como el "doble pago" (Nakamoto, 2008). Por

lo tanto, aunque los intermediarios pueden suponer varios inconvenientes en el sistema de pago, su función permite garantizar la seguridad de dicho comercio ya que además de evitar el doble pago aseguran que no se produzcan ataques o modificaciones en el sistema y que las transacciones pudieran revertirse si las partes lo desean.

Por este motivo, considerando todos los inconvenientes anteriores, Nakamoto introdujo dos elementos claves en el sistema Bitcoin que motivaron su éxito frente a otras propuestas similares. Por un lado, creó la tecnología *Blockchain* que está formada por una cadena de bloques que contienen las transacciones realizadas con Bitcoin desde el origen del sistema pago (Antonopoulos, 2017). Estos registros tienen un carácter público lo que permite que cualquier persona interesada pueda consultar abiertamente cualquier evento de la red y así garantizar que no se producirá el doble pago. Por otro lado, Nakamoto estableció el sistema Bitcoin conforme a una red distribuida de nodos mineros, que serían los encargados de validar las transacciones realizadas, almacenarlas en los bloques y resolver complejas pruebas criptográficas para decidir el bloque que formaría parte de la *Blockchain* (Antonopoulos, 2017). Todo ello en su conjunto, aseguraba la supervisión y el control de toda la actividad realizada impidiendo que se pudieran realizar modificaciones o ataques u otras formas de alterar la seguridad del sistema y su pervivencia. Además, todo el proceso realizado desde que se inicia la transacción será irreversible, por lo que, a diferencia de lo que sucede en sistemas de pago centralizados, en el sistema Bitcoin las transacciones serán inmutables siendo imposible tomar una decisión en contra de lo establecido por la mayoría de los nodos de la red (Domingo, 2018).

Como resultado de todo lo anterior tuvo lugar la formación del sistema de pago Bitcoin, que junto con la tecnología *Blockchain* que lo sustenta, permite el comercio electrónico directamente entre las partes interesadas y sin intermediarios. Pero también hay que señalar que este sistema de pago también supuso la creación de la criptomoneda Bitcoin, que se presentaba como la primera moneda virtual protegida con criptografía que permitía el comercio electrónico por medio de transacciones anónimas y sin intermediarios (Ammous, 2018). Esto es, aunque el contenido de la *Blockchain* puede ser consultado de forma pública, no se muestra ningún tipo de dato personal de los usuarios que han participado en las transacciones. Los usuarios interesados en realizar una transacción con Bitcoin únicamente necesitaban una clave pública y una privada, la primera como dirección a la que enviar los fondos y la segunda como “contraseña” para acceder a la cartera y realizar las operaciones.

De esta forma, con la creación de este sistema de pago y su correspondiente criptomoneda, se daba respuesta a una parte de la sociedad que demandaba una forma de realizar pagos electrónicos en la que no intervinieran las entidades bancarias y que respetara la privacidad de su actividad financiera. Así, desde su creación la criptomoneda Bitcoin ha sido ampliamente utilizada por todas aquellas personas interesadas en proteger la privacidad de sus transacciones.

Aunque después de Bitcoin han surgido otras criptomonedas como Ethereum, Litecoin o Monero, en la actualidad Bitcoin sigue siendo la criptomoneda más popularmente conocida y la más utilizada (CoinMarketCap, 2023a). La tecnología que la sustenta la convierte en una forma de pago anónima, segura, inmutable y de bajo coste y mayor rapidez si se comparan con los sistemas de pago centralizados (Fernández, 2018). Además, su funcionamiento de forma digital permite el envío de dinero a cualquier parte del mundo, sin límites temporales o espaciales y sin necesidad de convertir la moneda al dinero fiduciario del país en cuestión (Boar, 2018).

Por lo tanto, el sistema de pago Bitcoin y su criptomoneda han supuesto grandes beneficios para la sociedad, que además han utilizado la tecnología *Blockchain* en otras áreas diferentes al comercio electrónico aprovechando la capacidad que ofrece de supervisar procesos de forma descentralizada. Por ejemplo, fue implementada en la cadena multinacional Carrefour para garantizar la transparencia y la trazabilidad de los alimentos (Carrefour, 2018) o en la universidad Carlos III de Madrid para la verificación de los títulos universitarios (Blázquez, 2019).

Sin embargo, de la misma forma que la aparición del sistema Bitcoin ha supuesto beneficios en multitud de ámbitos de la sociedad, también ha tenido consecuencias negativas, como que se está utilizando en el desarrollo de la actividad criminal. El primer uso conocido de la criptomoneda Bitcoin en el ámbito criminal tuvo lugar en el año 2012 en el criptomercado “Silk Road” en el que se utilizaba como forma de pago (Christin, 2013). Se trataba de un mercado ubicado en la *Darknet* en el que se podían encontrar productos y servicios ilegales muy diversos, pero que fundamentalmente estaba dedicado a la venta de drogas. La criptomoneda Bitcoin se ofrecía como forma de pago, por lo que las personas interesadas en la compra realizaban un depósito de la cantidad requerida en la cartera del mercado y este les enviaba dicha cantidad a los criminales una vez se hubiera comprobado que el pedido era correcto (Christin, 2013). Esta forma de adquirir productos ilegales como drogas suponía una innovación criminal, en este caso en el tráfico de drogas (Aldridge y Décary-Hétu,

2014). Permitía a los criminales la compraventa de drogas de una forma anónima gracias a la utilización de criptomonedas y de la ubicación del mercado en la *Darknet,* además de que facilitaba el alcance del negocio a clientes de cualquier parte del mundo sin la necesidad de encontrarse físicamente (Aldridge y Décary-Hétu, 2014).

De este modo, se pone de manifiesto la capacidad de los criminales de adaptarse a las nuevas herramientas que van surgiendo y mejorar la forma en la que cometen delitos, compiten con otros criminales y sobreviven. De la misma forma que otros avances tecnológicos han permitido el desarrollo de actividades delictivas como, por ejemplo, sucedió con el correo electrónico y el delito de *phishing*, las criptomonedas han favorecido el desarrollo de ciertos delitos (Kethineni y Cao, 2020).

Esto se debe a que la utilización de las criptomonedas permite a los criminales realizar transacciones de forma anónima, sin intermediarios, de forma irreversible, en cualquier parte del mundo, con bajos costes y con la posibilidad de cambiarlas a cualquier moneda fiduciaria. Es decir, las mismas características de la tecnología por la que fue creada con un propósito legal, están siendo aprovechadas por los criminales para el desarrollo de sus actividades delictivas. Por lo que desde su utilización como forma de pago en el criptomercado "Silk Road" en el 2012, las criptomonedas han sido utilizadas en una gran variedad de delitos.

Se ha visto su implicación tanto en la cibercriminalidad entendida desde una concepción amplia, que incluye aquellos delitos de un carácter más tradicional, como en delitos ciberdependientes (Higbee, 2018). La primera hace referencia a aquellos delitos que no requieren necesariamente de la utilización de tecnologías para su comisión efectiva, pero las incluyen para favorecer su desarrollo (Miró-Llinares, 2012), como por ejemplo el delito de estafa (Aránguez, 2020). Por otro lado, los delitos ciberdependientes son aquellos cuyo desarrollo no es posible sin la utilización de tecnologías (Europol, 2018)., como por ejemplo los ataques *ransomware* (Paquet-Clouston et al., 2019).

Tal ha sido la utilización de esta tecnología en el ámbito criminal, que algunos autores han comenzado a denominar a este tipo de criminalidad como "criptocrimen", considerándolo como un conjunto de actos socialmente peligrosos cometidos en relación con o con el uso de productos de registros distribuidos (Criptodivisas, tokens y otras formas de activos financieros digitales) (Ivantsov et al., 2019). Se trata de esta forma de una consideración amplia en la que se incluye todo delito que ha sido cometido utilizando criptomonedas y esta será la postura que se tomará en este trabajo.

Por lo tanto, las criptomonedas han intervenido en una gran cantidad de delitos desempeñando diversos roles. Además de su utilización como medio de pago, se ha utilizado como una herramienta para la ocultación del rastro del dinero ilegalmente obtenido y para lucrarse y obtener beneficios económicos.

En cuanto a su rol como forma de pago, además de su utilización en los criptomercados se han utilizado las criptomonedas en delitos como *phishing, blackmail* o extorsión y en delitos de *ransomware* (Ali et al., 2015). En estos delitos los criminales requieren del pago de una cantidad determinada para cesar su actividad delictiva, por lo que el éxito del delito dependerá de que la víctima acceda a realizar dicho pago. En la actualidad, es habitual que los criminales introduzcan en estos delitos el pago en criptomonedas, introduciendo en el mensaje enviado a la víctima la dirección de su cartera de Bitcoin (Vasek y Moore, 2015).

En su rol de ocultar el rastro del dinero ilegal, las criptomonedas se han utilizado para el delito de blanqueo de capitales (Fanusie y Robinson, 2018). Una vez han obtenido el dinero del delito, los criminales lo utilizan para comprar criptomonedas con el objetivo de dificultar el rastreo de su actividad (Choo, 2015). Esto es posible gracias a que según el funcionamiento de la *Blockchain,* no hay ningún dato personal registrado en las transacciones almacenadas, por lo que si mantienen las medidas de seguridad necesarias al comprar criptomonedas, no sería posible la identificación de los autores.

Finalmente, en relación con el propósito de lucrarse y obtener beneficios económicos, el elevado valor de una unidad de Bitcoin ha ocasionado que las criptomonedas se hayan convertido en objeto de delito (Ali et al. 2015). Una vez el delincuente es capaz de apropiarse o de robar las criptomonedas de un usuario, no será posible que este las recupere debido a la irreversibilidad de las transacciones.

Sin embargo, de entre todos los delitos en los que se ha observado la presencia de esta tecnología, son varios los autores que coinciden en que son los delitos contra la propiedad aquellos en los que se ha visto una mayor implicación de esta criptomoneda (Aránguez, 2020; Kethineni y Cao, 2020; Pérez, 2020; Saldaña-Taboada, 2022).

Por todo ello, este tipo de criminalidad se ha convertido en un tema de interés para las autoridades encargadas de la persecución del delito (Zetter, 2012). Las criptomonedas se han señalado como un facilitador de la criminalidad, especialmente para los grupos criminales, lo que ha quedado reflejado en los sucesivos informes elaborados por la agencia Europol (2014, 2017, 2018, 2019 y 2021). Se ha señalado su utilización en actividades delictivas vinculadas con la criminalidad organizada como el

blanqueo de capitales, la compraventa de drogas en mercados de la *Darknet,* cibercriminalidad y estafas entre otros (Europol, 2021). Por ello, se sitúa como un fenómeno criminal de interés en el que las mismas características que pudieran atraer a los criminales están dificultando la investigación y la persecución de los delitos (Europol, 2021). Aunque se puede consultar todo el registro de las transacciones de forma pública en la *Blockchain*, no se dispone de datos personales que puedan relacionarse con las direcciones de las carteras. Por este motivo, aunque las autoridades pudieran acceder a la *Blockchain* no podrían identificar a los autores de un delito.

Para conocer la actividad que ha llevado a cabo una persona en la *Blockchain* sería necesario, en primer lugar, obtener la información adicional necesaria que vincula a esa persona en concreto con una dirección Bitcoin. En segundo lugar, habría que obtener la actividad registrada en la *Blockchain* perteneciente a su historial de transacciones para poder determinar un patrón de su actividad. Solo con la unión de los dos requisitos anteriores se podría determinar si una persona sospechosa de haber cometido un delito con criptomonedas ha sido realmente responsable de este hecho.

Por este motivo, se están realizado una gran cantidad de investigaciones dirigidas a la obtención de la información adicional mencionada anteriormente y al estudio y análisis de los patrones de la actividad registrada en la *Blockchain* (Schickler, 2022). Así, por ejemplo, se han realizado investigaciones en las que se han empleado diversas técnicas con el objetivo de reducir el anonimato asociado a esta criptomoneda y demostrar que realmente se trata de un pseudoanonimato (Androulaki et al., 2013; Reid y Harrigan, 2013; Ron y Shamir, 2013 y Meiklejohn et al., 2013). Pero también se han realizado investigaciones con el objetivo de extraer patrones de las transacciones (Yan Wu et al., 2019); clasificar direcciones sospechosas de haber cometido un delito (Lee et al., 2020) o rastrear las transacciones maliciosas de Bitcoin y agruparlas (Zheng et al., 2018). En este sentido también han surgido muchas empresas, como la empresa Chainalysis (2022), que se han dedicado al estudio de la *Blockchain* con el objetivo de establecer patrones en las transacciones y obtener la información necesaria para que las autoridades puedan comenzar con la investigación de los delitos.

Sin embargo, se han observado pocas investigaciones en esta materia que aborden la criminalidad con criptomonedas desde una perspectiva criminológica, estudiando los autores implicados, las víctimas, los tipos de delitos cometidos o su prevención. Algunas de las investigaciones que se pueden señalar en este sentido son Kethineni y Cao (2020) que estudian la influencia de las criptomonedas en la actividad

criminal como facilitador de ciertos delitos, la situación de su regulación y lo desafíos actuales; Foley et al., (2019) que realizan una estimación sobre la cantidad de transacciones con Bitcoin que se pueden relacionar con actividades ilegales; Janze (2017) que estudia si las criptomonedas son una tecnología empleada principalmente por criminales o Buil-Gil y Saldaña-Taboada (2021) que estudiaron el comportamiento de los usuarios de estos delitos y hallaron que la mayoría de las actividades delictivas cometidas con criptomonedas se concentran en unos pocos usuarios.

Por lo tanto, se observa la necesidad de llevar a cabo un estudio integral de este fenómeno criminal desde una perspectiva criminológica que permita abordar aspectos que se consideran clave para su total comprensión como son los tipos de delitos más cometidos, la victimización por estos delitos, los aspectos de la tecnología que favorecen su utilización criminal y las motivaciones de los autores. De esta forma, se ampliaría el conocimiento existente en relación con su volumen, facilitadores del delito, motivaciones y características.

La hipótesis de partida es que una comprensión global del fenómeno criminal permitirá determinar su importancia como herramienta para el delito, esto es, si se trata de "dinero criminal" y dirigir las actuaciones de intervención y prevención hacia los aspectos clave.

El objetivo general de esta investigación consiste en estudiar el fenómeno de utilización de las criptomonedas en la comisión del delito desde una perspectiva criminológica. Para ello, se han propuesto a su vez unos objetivos específicos que se corresponden con cada uno de los aspectos que se deben abordar para la consecución del objetivo general. De esta forma, los objetivos específicos consistirán en el estudio de los autores, los tipos de delitos, la victimización, los roles de las criptomonedas en el delito y las motivaciones criminales.

Para conseguir los objetivos propuestos se plantea una metodología de carácter mixto que combina métodos cualitativos y cuantitativos para obtener una mejor comprensión de fenómenos complejos y multifacéticos como es este caso. Como parte de la metodología se desarrollan cinco experimentos cuyo contenido se describe a continuación.

El experimento primero consiste en una metodología de carácter cuantitativo basada en la utilización de los sistemas inteligentes en un conjunto de datos de delitos cometidos con criptomonedas por grupos criminales.

La utilización de la Inteligencia Artificial ha demostrado tener grandes beneficios en la detección de problemas y en la toma de decisiones en diversos ámbitos. Su éxito se debe a la capacidad aumentada de cómputo del *Big Data*, que al mismo tiempo se apoya en algoritmos de Inteligencia Artificial para estudiar el comportamiento de un fenómeno y estimar su futuro. Por ello, los algoritmos se están utilizando para estimar los riesgos delictivos en relación con el lugar o con las características de las personas para mejorar la toma de decisiones en cuanto a su prevención, investigación y persecución (Miró-Llinares, 2020). Y es que su aplicación se puede realizar a toda aquella área de actuación en la que se requiera la toma de decisiones por un humano (Valls-Prieto, 2021). Por ello, se planteó su utilización para abordar el fenómeno criminal que aquí se trata.

Por lo tanto, el objetivo general que se tenía inicialmente con este experimento era el de aplicar las técnicas de los sistemas inteligentes a este fenómeno criminal para descubrir nuevo conocimiento sobre los aspectos criminológicos del delito. Este conocimiento podría servir al mismo tiempo para la evaluación y la adaptación de las herramientas policiales basadas en técnicas de IA.

Sin embargo, dicho experimento no pudo llevarse a cabo de la forma propuesta debido a una serie de inconvenientes que se encontraron durante su desarrollo. Se propuso la utilización de herramientas de análisis de criptoactivos que permiten estudiar de forma interactiva los flujos monetarios. Sin embargo, no fue posible obtener los datos necesarios por parte de las autoridades y los proyectos de investigación relacionados, por lo que no se dispuso de una muestra suficiente y válida que permitiera obtener los resultados esperados. Al mismo tiempo se detectó la incapacidad de determinar lo que se considera como organización criminal únicamente por la observación de los datos. Se podía extraer información sobre sobre las transacciones realizadas, pero ningún contexto adicional de interés criminológico.

En el segundo experimento se realizó un análisis cualitativo del contenido de la jurisprudencia penal española en materia de delitos cometidos con criptomonedas, especialmente Bitcoin. Su elaboración permite obtener una visión completa del fenómeno criminal sobre el tipo de delitos, *modus operandi,* tipo de autores, tipo de víctimas y el rol de las criptomonedas en cada caso. Los datos del experimento fueron extraídos del estudio y el análisis de la jurisprudencia penal española elaborada por el Poder Judicial español. La búsqueda de las resoluciones judiciales se realizó a partir de la introducción de los términos “bitcoin”, “criptomoneda” y “Blockchain” en la base de

datos de carácter jurídico “Aranzadi” y se seleccionaron aquellos resultados en los que no solo aparecía el término buscado, sino que este elemento tenía una importancia real en el desarrollo del caso. A partir de los datos obtenidos se creó una base de datos con variables relativas al tipo de delito, tema, tipo de autor, tipo de víctima, *modus operandi,* país de desarrollo, rol de la criptomoneda y motivación para su utilización. Finalmente, se realizó un estudio descriptivo de las variables anteriores y se visualizaron los resultados utilizando el programa de análisis e inteligencia conocido como “Tableau”.

El tercer experimento consiste en un estudio espaciotemporal de la victimización de los delitos cometidos con criptomonedas. Su desarrollo permite explorar las variables tiempo y espacio en este tipo de criminalidad, hecho que no es fácil si se considera su dificultad de detección y la complejidad para obtener bases de datos oficiales. Para ello, se siguió una metodología de carácter cuantitativo a través de la que se obtuvieron patrones temporales y espaciales de la victimización. Los datos de la investigación fueron obtenidos del repositorio de la página web “Bitcoin Abuse” en el que las víctimas de este tipo de criminalidad registran el incidente. La descarga de los datos se realizó empleando una API disponible en la misma página web. A partir de estos se creó una base de datos que incluía las variables relativas al tipo de delito registrado, información sobre el lugar, la hora y el día en el que se realizó la denuncia y dirección Bitcoin. Finalmente, se realizó un análisis descriptivo de los datos empleando el programa de análisis e inteligencia conocido como “Tableau”.

El experimento cuatro consiste en un estudio de las motivaciones de los sujetos para utilizar las criptomonedas en sus actividades delictivas. Para ello, se desarrolló una metodología de carácter cualitativo consistente en un análisis del contenido de un foro de discusión de la *Darknet* conforme a un enfoque *Grounded Theory*. Su desarrollo permite obtener información sobre el fenómeno, sus motivaciones y el desarrollo del delito a partir del testimonio de los propios autores en una comunidad anónima en la que se estimula el intercambio de información sin temor a ser detectado. Los datos necesarios para la investigación fueron obtenidos a partir del estudio y el análisis de las discusiones contenidas en un foro de la *Darknet*. La recopilación de las discusiones se realizó de forma manual seleccionando aquellas que incluían el término “Bitcoin” y en las que la discusión trataba realmente sobre este elemento. Para realizar el análisis y la codificación de los temas presentes en las discusiones se empleó el programa de análisis de datos cualitativo conocido como “NVivo”. Del estudio y análisis de las discusiones obtenidas, en relación con el objetivo de las investigaciones, se identificaron varios

temas. Al mismo tiempo, se han podido encontrar otros temas y subtemas que no se habían previsto pero que resultan de interés para el desarrollo de la investigación.

El quinto experimento consiste en un estudio de la utilización de las criptomonedas como forma de pago en los mercados *online* de cannabis y productos derivados. Para ello, se seguirá una metodología cuantitativa consistente en el análisis de contenido de las conversaciones obtenidas. Su desarrollo permite conocer aquellas características de las criptomonedas que motivan a los criminales a utilizarlas en sus actividades delictivas. La investigación se centró en mercados *online* con sede en los territorios de Canadá debido a la situación especial que presentan en cuanto a la regulación de la compraventa de cannabis. La fuente de datos en este caso fue la web superficial en la que se ubicaban las tiendas *online* de cannabis. Se elaboró una base de datos con aquellas tiendas de cannabis y otros productos derivados que estaban ubicadas en los territorios de Canadá. Posteriormente, se accedió a cada uno de los mercados y se contactó con sus responsables para consultarles sobre la implementación de la criptomoneda Bitcoin como forma de pago. El contenido de estas conversaciones fue recopilado y posteriormente se realizó su análisis y codificación utilizando el programa de análisis de datos cualitativo conocido como "NVivo".

De esta forma, los resultados de los experimentos en su conjunto serán de utilidad para justificar y adaptar las medidas de prevención que consistan en la limitación o prohibición de la utilización de las criptomonedas. Las medidas adoptadas deberán adaptarse a los derechos y libertades de los usuarios interesados en utilizar esta tecnología de forma legal para respetar su privacidad. Al mismo tiempo, la comprensión global del fenómeno criminal permitirá la detección y persecución del delito de una forma más adecuada y precisa, especialmente en el desarrollo de herramientas y tecnología que sirvan de apoyo a las autoridades encargadas de la lucha contra este tipo de criminalidad.

Finalmente, en cuanto a la estructura del trabajo se pueden distinguir cuatro bloques además de la introducción. El primer bloque trata las criptomonedas y la Blockchain, haciendo hincapié en todo lo relativo a la criptomoneda Bitcoin. El segundo bloque se centrará en las criptomonedas en el ámbito criminal explicando el tipo de delitos en el que intervienen y el estado actual de la investigación en esta materia. El tercer bloque aborda las cuestiones metodológicas y analísticas sobre el estudio de la delincuencia cometida con criptomonedas. Finalmente, el último bloque se

realiza una discusión y se muestran las conclusiones generales de la investigación. De una forma más detallada, los bloques se organizan de la siguiente forma:

El primer bloque pretende mostrar una visión general de las características, el funcionamiento y los elementos que componen las criptomonedas y la *Blockchain*. El motivo es ofrecer al lector el conocimiento técnico necesario que le permita comprender la utilización posterior de las criptomonedas en el ámbito criminal. Con este fin se divide en cuatro capítulos. En el primero de ellos se realiza un repaso desde el origen del dinero fiduciario y el comercio electrónico hasta la creación de la criptomoneda Bitcoin. El segundo capítulo trata las características generales de las criptomonedas y de la *Blockchain* de Bitcoin. El tercer capítulo recoge todos los elementos que forman parte del sistema Bitcoin y que constituyen aquellos que permiten su funcionamiento. Por último, se realiza un repaso sobre algunas de las criptomonedas alternativas más relevantes en la actualidad y se realizan comparaciones con respecto a la criptomoneda Bitcoin.

El segundo bloque tiene como propósito ofrecer el panorama general de la utilización de las criptomonedas en el crimen y el estado actual de la investigación de este tipo de criminalidad. A su vez, este bloque queda dividido en tres capítulos. El capítulo cinco constituye una aproximación general al ámbito criminal de las criptomonedas, en la que se discute sobre las dificultades de estimación de esta criminalidad y se presentan aquellos aspectos de esta tecnología que podrían favorecer su utilización en el crimen. El capítulo seis realiza una descripción detallada de todos aquellos delitos en los que de una forma más frecuente se ha visto la utilización de las criptomonedas. Por último, en el capítulo siete se realiza un repaso del estado actual de la investigación de las criptomonedas en el crimen. Se pretende mostrar la investigación actual en esta materia e identificar los huecos existentes que podrían completarse con una aproximación criminológica al fenómeno. Por lo tanto, se hace hincapié en la necesidad de desarrollar más investigaciones de carácter criminológico en esta materia.

El tercer bloque recoge la metodología, los resultados, la discusión y las limitaciones de los cinco experimentos propuestos para alcanzar el objetivo de la investigación. En primer lugar, se presenta el diseño de la investigación de forma general para posteriormente presentar de forma diferenciada cada uno de los cinco experimentos propuestos.

Por último, en el cuarto bloque se recoge la discusión y las conclusiones de la investigación. Se divide en dos apartados, el primero pertenece a la discusión y el

segundo a las conclusiones generales del trabajo. Al final del apartado se incluyen las conclusiones redactadas en inglés.

BLOQUE I: CRIPTOMONEDAS Y BLOCKCHAIN. BITCOIN.

Capítulo 1. Del Dinero a las Criptomonedas: Los Orígenes del Bitcoin.

Los Orígenes y la Evolución del Dinero

El origen del dinero tal y como se conoce en la actualidad ha estado muy marcado por las necesidades que han surgido durante el desarrollo de las sociedades. En un principio, las sociedades eran autosuficientes, consumían todo lo que producían. No obstante, con la implementación de la división de trabajo comenzaron a surgir ciertas necesidades que no podían ser cubiertas únicamente con la producción individual, se debía recurrir a aquellas personas que producían u ofrecían los servicios deseados (Ammous, 2018).

Para poder adquirir estos productos y servicios se comenzó utilizando un sistema de trueque en el que las partes interesadas intercambiaban la producción excedente de sus trabajos. No obstante, este sistema contaba con algunos inconvenientes como que en ocasiones se necesitaban otros bienes que no se correspondían con el remanente de ninguna producción (Ammous, 2018). Para solventar esto, se continuó con el intercambio, pero esta vez estableciendo una serie de patrones de valor, es decir, se intercambiaban bienes que tuvieran un valor semejante a aquellos que se querían adquirir. Pero este sistema tampoco estuvo exento de problemas ya que establecer el valor equivalente para ciertos bienes era complejo, por ejemplo, determinar cuántas gallinas sería justo entregar a cambio de un cerdo (Ammous, 2018)..

De este modo, decidió crearse un objeto que tuviera valor y que se pudiera entregar a cambio de los bienes o servicios que se necesitaban. Así fue como surgieron las primeras formas de dinero y en especial lo que empezaría a crear el camino para las nuevas monedas. Solían ser materiales fácilmente divisibles, transportables y valiosos, así como semillas, sal u otros materiales de diferentes formas y tamaños según el lugar en el que eran utilizados. Para que un material pudiera ser considerado como moneda debía reunir tres funciones: 1) almacenar valor; 2) permitir su intercambio por otros bienes; y 3) servir como referencia de valor al determinar el precio de las cosas (Domingo, 2018). Así, para que una moneda pudiera cumplir estas tres funciones debía ser escasa, difícil de copiar, portable, perdurable, fácilmente divisible en unidades pequeñas y deseable por cualquier persona (Domingo, 2018).

De esta forma, no todo podía ser considerado como una moneda, para que las monedas de una sociedad pudieran entregarse a cambio de un bien o servicio, la sociedad

debía considerar que esa moneda tenía algún tipo de valor. Este valor podía estar determinado por la dificultad de obtención, producción o por la importancia del material del que estaban elaboradas. Así, por ejemplo, se han utilizado como monedas conchas marinas[1], pieles, dientes (América), cuentas elaboradas con cáscara de avestruz (Kenia), colgantes de dientes de animales (España), colgantes de dientes y conchas (Australia) o collares de conchas (Europa) (Szabo, 2002).

Similar a los anteriores, el sistema basado en las piedras "rai" no difería mucho de cómo funciona hoy en día la criptomoneda Bitcoin (Ammous, 2018). Este sistema adoptado en la isla de Yap consistía en unos discos de piedra caliza que cumplían la función de moneda. Dado que no se fabricaban en esta isla, sino en una isla cercana, los discos tenían que ser transportados y debido a su enorme tamaño, los propietarios de los discos no podían llevárselos, siendo público su intercambio y a su vez siendo difíciles de robar. Su valor estaba asegurado por su dificultad de transporte y producción y debido a la disponibilidad en varios tamaños también estaba asegurada la posibilidad de pago fraccionado (Ammous, 2018). Sin embargo, el valor que tenían las piedras de Yap se perdió cuando el capitán David O'Keefe, interesado en comprar los cocos de la isla, aumentó la producción de las piedras con un barco y explosivos para pagar a los habitantes de la isla, por lo que finalmente se prohibió su uso como moneda (Ammous, 2018).

De la misma forma que con las piedras "rai", la utilización de este tipo de materiales como dinero fue abandonándose progresivamente a medida que perdían aquello que los hacían valiosos. Bien podría ser porque se facilitaba su proceso de obtención, elaboración o transporte, porque perdían el valor como material que tenían para esa sociedad o bien por su poca durabilidad.

Con la aparición de los metales preciosos y la metalurgia se solucionaron los inconvenientes anteriores y se comenzó la acuñación de monedas de una forma similar a las monedas actuales. Las primeras monedas en el 600 a.C. estaban formadas por una aleación de oro y plata, eran fácilmente divisibles y su valor estaba determinado por su peso. Sin embargo, su transporte no era sencillo, ya que debido a su composición resultaba tedioso transportar grandes cantidades.

[1]En el siglo XVII, los indios americanos usaban como monedas un collar de abalorios elaborados con conchas que llamaban "wampum". Se convirtió en la moneda de curso legal en esa época en Nueva Inglaterra, pero dejó de ser así cuando descubrieron que otros materiales como el oro y la plata tenían mejores cualidades monetarias (Szabo, 2002).

De esta forma, a partir de esta nueva necesidad, alrededor del S. VIII d.C. surge en China el papel moneda, mucho más fácil de transportar que las piezas de oro anteriores. El valor de la moneda ya no dependía del soporte físico, sino que residía en el respaldo de sus emisores. El valor de cada uno de los billetes emitidos estaba sometido al patrón oro, es decir, a la cantidad de oro que disponían las entidades bancarias del país, lo que permitía a cada país tener su propia moneda (Domingo, 2018).

Con la Primera Guerra Mundial, se termina la emisión de la moneda según el patrón oro y surge el dinero fiduciario o *fiat* a partir de la necesidad de centralización del oro. Su valor ya no dependía de las reservas físicas de oro, sino del criterio de los gobiernos y la sociedad, es decir, de su emisor y el acuerdo común (Domingo, 2018).

El Origen del Comercio Electrónico y de las Criptomonedas

Con la globalización y el avance del comercio, surgió la necesidad de realizar transacciones entre personas que no se ubicaban en el mismo espacio físico y para las que por tanto no era posible el pago en efectivo. Así, surgieron los sistemas de pago con intermediación, conocidos así porque requerían de la introducción de un intermediario que se encargaba de la supervisión y validación de la transacción para evitar los problemas derivados de este sistema como el doble pago o el gasto (Ammous, 2018). Sin embargo, a pesar de las ventajas que pudiera suponer la introducción del sistema de comercio electrónico, muchas personas se mostraban disconformes con la pérdida total o parcial de aquellos derechos que podían disfrutar en el comercio realizado con el dinero en efectivo. Las transacciones realizadas con el dinero en efectivo carecen de control o supervisión de terceros, lo que permite respetar la identidad de cada una de las partes ya que no es necesario identificarse para que la transacción deseada pueda realizarse con éxito.

En comparación con esto, el comercio electrónico, con la supervisión y control de las entidades bancarias suponía la pérdida de la soberanía del dinero, desapareciendo propiedades deseables del dinero físico como su fungibilidad y liquidez (Ammous, 2018).

Con la crisis económica del año 2008 quedaron al descubierto las vulnerabilidades de las entidades bancarias, que perjudicaron la economía de muchas personas con los ajustes económicos realizados (Domingo, 2018). Esto ocasionó un aumento en la desconfianza de la población hacia estas entidades y un enorme descontento por el papel tan relevante que ocupaban como intermediarios en el comercio electrónico.

Esta situación supuso el detonante para que Satoshi Nakamoto, del que se desconoce su identidad real, creara el sistema de pago Bitcoin como una respuesta que pusiera solución

a la dependencia que el comercio electrónico tenía de las entidades bancarias. Este hecho supuso no solo el origen de la moneda Bitcoin, sino también supuso el origen de las criptomonedas.

Los Precursores al Proyecto de la Criptomoneda Bitcoin

Sin embargo, la idea de un sistema de pago con estas características que presentaba el Bitcoin no era nueva. Llevaba gestándose varios años atrás en el seno de una corriente de pensamiento conocida como *Cypherpunk* -unión de *cipher* y *cyberpunk*-, que se formalizó en el año 1992 con Eric Hughes, Timothy C. May y John Gilmore. Así, surgía un grupo integrado por firmes defensores de la privacidad en la era digital que compartían y exponían sus ideas en una lista de correo electrónico creada con este fin.

Sus ideas se recogieron por primera vez en el "Manifiesto Criptoanarquista"[2] elaborado por Timothy C. May en el que exponía que la mejora de velocidad en las redes de ordenadores y ordenadores personales permitiría la implementación y el desarrollo de una serie de tecnologías[3] que, aunque antes estaban limitadas, ahora podrían usarse para conseguir el anonimato de las comunicaciones (May, 1992). De esta forma y de acuerdo con el propósito de la anarquía criptográfica, se alteraría el control gubernamental y su capacidad para registrar y controlar las transacciones económicas, así como la posibilidad de mantener la información en secreto[4] (May, 1992). Más tarde, las ideas plasmadas por May en el primer manifiesto se ampliaron en el "Manifiesto *Cypherpunk*" elaborado por Eric Hughes, otro de los principales representantes de este movimiento. En dicha publicación exponían que la demanda de privacidad no significaba el derecho al sector absoluto de las comunicaciones, sino que suponía el derecho de todo individuo a decidir libremente a quién desea revelar su información personal (Hughes, 1993).

Este movimiento tuvo su origen en dos eventos destacables. Por un lado, en la decisión del gobierno de los Estados Unidos en el año 1970 de publicar abiertamente sobre criptografía, una práctica que anteriormente era considerada como secreta y reservada

[2]Traducción del inglés de "*The Crypto Anarchist Manifesto*" que surgió, tal y como expone Timothy May en su escrito, de las peticiones de personas afines a esta ideología tras escucharon su discurso años atrás en reuniones de esta temática.

[3]"*High-speed networks, ISDN, tamper-proof boxes, smart cards, satellites, Ku-band transmitters, multi-MIPS personal computers and encryption chips*" (May, 1992).

[4]"*These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation*" (May, 1992)

principalmente a agencias militares o espías[5]. Por otro lado, en la publicación en el año 1980 del trabajo del Dr. David Chaum en el que exponía su conocimiento sobre efectivo digital anónimo y los sistemas de reputación pseudoanónimos[6].

De esta forma, el objetivo de este grupo era conseguir que el funcionamiento de la sociedad en cuanto a sus aspectos tecnológicos estuviera orientado desde su diseño a preservar la privacidad de los usuarios. Así, eran partidarios de la utilización de tecnologías con las que cumplir este propósito como la criptografía, los sistemas de reenvío de correo anónimo, firmas digitales y dinero electrónico (Hughes, 1993).

De esta forma, las demandas de privacidad no quedaban únicamente limitadas al ámbito de las comunicaciones, sino que también se extendía a los sistemas de pago. Se defendía el derecho de los individuos a no revelar información que no fuera estrictamente necesaria en el desarrollo de una transacción, de forma que el sistema de pago pudiera asemejarse a los pagos realizados de forma física, en los que la transacción se realiza sin que sea necesario que vendedor y comprador revelen sus identidades (Hughes, 1993). Por lo tanto, se deja entrever cierta preocupación hacia la predilección de la sociedad por los sistemas de pago electrónicos como tarjetas de crédito y débito, aunque esto pudiera suponer la pérdida de su privacidad a través del registro de las transacciones realizadas y la elaboración de patrones de gasto de cada usuario (Finney, 1993a). Se apuesta por conseguir un sistema de pago similar al dinero en efectivo que se utiliza en el comercio físico, que permita mantener los mismos niveles de privacidad que en este.

No obstante, el sistema de pago Bitcoin no fue el único proyecto que surgió en ese sentido. Otros proyectos anteriores tenían como propósito conseguir que el comercio electrónico fuera lo más similar posible a los pagos en efectivo, lo que también supuso la creación de muchas tecnologías con este fin que posteriormente se utilizaron en Bitcoin.

Asimismo, en el año 1997 el Dr. Adam Back creó el proyecto “Hashcash”, una tecnología de Prueba de Trabajo o *Proof of Work* (PoW) que permitía evitar el correo basura o *spam* con un mecanismo de verificación que aseguraba que la persona interesada en enviar un mensaje estaba dispuesta a invertir la capacidad computacional necesaria. Para ello, se añadía un encabezado codificado al correo que funcionaba como un sello que aseguraba haber

[5]Las publicaciones que fueron pioneras en este sentido fueron los trabajos *Data Encryption Standard* y *New Directions in Cryptography* por el Dr.Whitfield Diffie y el Dr.Martin Hellman (Lopp, 2016).
[6]Para un mayor conocimiento sobre lo escrito por el Dr. David Chaum, se puede encontrar esta información en su publicación *Security without Identification: Transaction Systems to Make Big Brother Obsolete.* https://www.chaum.com/publications/Security_Wthout_Identification.html

pasado por la prueba de trabajo (Back, 1997), un mecanismo mucho más sencillo de utilizar que la propuesta "digicash" de Chaum (Back, 1997).

En 1998, Wei Dai propuso "b-money"[7], un protocolo con el que se pretendía conseguir que servicios como el dinero como medio de intercambio y el cumplimiento de los contratos, que tradicionalmente han sido proporcionados por el gobierno o instituciones relacionadas, ahora fueran proporcionados por entidades imposibles de rastrear (Dai, 1998).

Para ello, Wei describe dos protocolos, asumiendo en ambos la existencia de una red imposible de rastrear donde los remitentes y receptores son identificados por seudónimos digitales (claves públicas) y cada mensaje está firmado por su remitente y encriptado a su receptor (Dai, 1998). En el primer protocolo cada participante mantiene una base de datos (separada) del dinero que pertenece a cada pseudónimo. El segundo protocolo, es una variante del anterior en la que cada usuario guarda sus cuentas de dinero en un subconjunto de los participantes a los que llama servidores y propone un mecanismo para incentivarlos a ser honestos mediante el depósito de una cantidad de dinero en una cuenta especial utilizada para posibles multas o recompensas como prueba de mala conducta (Dai, 1998). Décadas más tarde Bitcoin utilizaría el segundo de estos protocolos.

En 2004, el ingeniero informático y miembro del grupo *Cypherpunks*, Hal Finney, en el año 1993 comenzó a hablar sobre las ventajas que tenía el efectivo digital para la privacidad (Finney, 1993a). Más tarde creó el primer sistema de efectivo digital en disponer de prueba de trabajo, las RPOW (Pruebas de trabajo reutilizables) y que estaba basado en el proyecto "Hashcash" de Adam Back (1997) (Satoshi Nakamoto Institute, 2021). En 1993 planteó un sistema en el que el efectivo digital sería otorgado por una entidad bancaria, que solo tendría conocimiento de una única retirada, pero no de la forma o la ubicación en la que se gastaba (Finney, 1993a). Ya entonces exponía que el principal inconveniente de este pago podría ser el problema del doble gasto, algo que se evitaría con la verificación en línea (Finney, 1993a). Unos meses más tarde, trató el tema del doble pago en su publicación *Detecting Double Spending,* tomando como referencia la propuesta de David Chaum y proponiendo una versión ligeramente simplificada (Finney, 1993b). El doble pago podría evitarse haciendo que cada efectivo tuviera un número de serie único, de forma que se podría comprobar con la entidad bancaria si ese efectivo había sido previamente utilizado (Finney,

[7]"*A community is defined by the cooperation of its participants, and efficient cooperation requires a medium of exchange (money) and a way to enforce contracts. Traditionally these services have been provided by the government or government sponsored institutions and only to legal entities. In this article I describe a protocol by which these services can be provided to and by untraceable entities*" (Dai, 1998).

1993b). Su sistema RPOW consistía en unos *tokens* criptográficos que sólo podían usarse una vez, sin embargo, la validación y protección continuaba a cargo de un servidor central (Lopp, 2016).

En el año 2005 el informático Nick Szabo, basándose en la propuesta de Hal Finney publicó el proyecto "Bit Gold", considerado hoy en día como el precursor de Bitcoin. No obstante, antes de la ideación de "Bit Gold", Szabo había realizado numerosas publicaciones sobre aspectos relacionados con esta materia (Szabo, 2021), siendo pionero en plantear las bases de los *Smart contracts* (Szabo, 1995, 1997) y de las criptomonedas, lo que ha quedado reflejado en sus reflexiones sobre el riesgo para la seguridad de los sistemas de los terceros de confianza (Szabo, 2001) o sobre el origen y evolución de la consideración del valor del dinero (Szabo, 2002). Así, su propuesta "Bit Gold" era finalmente el resultado de todas las ideas y su trabajo anterior sobre criptografía, descentralización, Prueba de Trabajo (PoW) y la desconfianza en terceras partes.

Szabo consideraba que el valor del dinero dependía demasiado de terceros, algo que no era lo ideal considerando los episodios inflacionarios de décadas anteriores (Szabo, 2005). Por ello, comparándolo con el valor que tenían los metales preciosos y objetos de colección con un elevado costo de producción, Szabo perseguía conseguir un efectivo digital que mantuviera la dificultad propia de extracción del oro sin depender de autoridades centrales y sin los inconvenientes que tenían anteriormente las otras formas de dinero[8] (Szabo, 2005).

De esta forma, "Bit Gold" se presentaba como una moneda virtual que conseguía la dificultad de extracción mediante la resolución de pruebas criptográficas que se solucionaban invirtiendo en potencia computacional. La secuencia de pasos de este sistema es descrita por el propio Szabo (Szabo, 2005), en la que pone como ejemplo a dos usuarios conocidos como Alice y Bob. Según explica Szabo en su trabajo (2005), para empezar en el sistema, se genera en el ordenador una cadena de *bits* llamada como "cadena desafío" o *Challenge string.* Alice en su ordenador genera la prueba de trabajo o *Proof of Work* de los *bits challenge* de la cadena anterior. Esta prueba de trabajo tiene una marca de tiempo y funciona de forma distribuida. Finalmente, Alice añade ambas cadenas con un sello de tiempo a un registro de título de la propiedad distribuido o *Distributed property title registry* para "Bit gold" que no depende de ningún servidor. El resultado de la prueba anterior se incluye en la prueba

[8]Aunque tenían un valor elevado debido a los elevados costos de su producción, estas formas de pago a su vez presentaban otros inconvenientes que impulsaron su sustitución por las formas de pago que se conocen posteriormente. Así, por ejemplo, era complejo el transporte de estos materiales, su producción y la determinación objetiva de su valor en su intercambio por otro producto o servicio.

siguiente, consiguiendo una vinculación en forma de cadena unidireccional que difícilmente permitía el cálculo "hacia atrás", lo que la dotaba de seguridad (Szabo, 2005). Bob podría confirmar que Alice es la verdadera propietaria de una cadena de "Bit Gold" comprobando la cadena de títulos infalsificable en el registro (Szabo, 2005).

Sin embargo, la propuesta de Szabo no contó con aceptación suficiente y finalmente no se implementó. Presentaba algunos inconvenientes que no se resolvieron como la reducción del valor ante el potencial de un exceso de suministro, de forma que una mayor producción saturaría el sistema (Szabo, 2005). No obstante, a pesar de ello, fue pionero en la utilización en un sistema de pago de una serie de tecnologías y herramientas que serían clave posteriormente en el desarrollo de Bitcoin. Tanto es así, que, aunque el propio Nick Szabo lo ha negado en varias ocasiones, muchas personas le siguen atribuyendo la autoría del sistema Bitcoin.

Los Inicios de la Criptomoneda Bitcoin. Hitos más Relevantes

En el año 2008, como resultado de todo el conocimiento generado por aquellas personas que constituyeron el movimiento *Cypherpunk*, Satoshi Nakamoto, del que se desconoce su identidad real[9], crea la criptomoneda Bitcoin. La primera aparición de la idea de creación del bitcoin fue a través de un correo electrónico en una lista de correos de criptografía, en el que un usuario conocido como Satoshi Nakamoto aseguraba haber desarrollado un sistema de dinero electrónico que funcionaba a través de una red *peer-to-peer* y que por tanto no requería de intermediarios. Más tarde publicaría el *White paper* del sistema de pago Bitcoin. En este describe la motivación para su creación, las características del sistema de pago y su funcionamiento, haciendo referencia además a trabajos anteriores de otros seguidores de esta filosofía.

Pero la fecha en la que aparece este trabajo no es algo causal. En el año 2008 tiene lugar una importante crisis económica que ocasiona un aumento de la desconfianza que la población tenía hacia las instituciones bancarias. Estas entidades ejercían un importante papel

[9] Según Kaminsky, el creador de Bitcoin se trataba de un programador con un profundo conocimiento del lenguaje de programación C++, economía, criptografía y redes *peer-to-peer.* Lo que le llevó a pensar que o bien se trataba de un equipo de personas o bien se trataba de un genio (Davis, 2011). No obstante, se cree que su creador tenía buenas razones para mantenerse en el anonimato, pues se conocen casos como el de Bernard von NotHaus, creador de unas monedas de oro y plata que denominó como *Liberty Dollars* en 1998, que fue acusado por el gobierno de Estados Unidos de "conspiración contra Estados Unidos", ya que, según el FBI, supone una violación de la ley federal crear monedas o sistemas monetarios para competir con monedas oficiales de los Estados Unidos (Davis, 2011). En cuanto a las monedas en línea, el gobierno de Estados Unidos también tuvo como objetivo la moneda digital "e-Gold" que permitía canjearse por oro y llevó a cabo el cierre de la empresa argumentando que se trataba de una moneda que permitiría el lavado de dinero y la pornografía ya que no era necesario presentar una identificación para operar con ella (Davis, 2011)

de terceras partes en el comercio electrónico por lo que de acuerdo con la preocupación ya manifestada desde el origen del movimiento *Cypherpunk*, inspirados en los sistemas de pago fiduciarios, se pretendía conseguir un sistema de pago que no dependiera de terceras partes, que fuera seguro y que respetara la identidad de los usuarios.

De esta forma, con el propósito de responder a todas estas demandas y como fruto del conocimiento anteriormente generado en esta materia, Satoshi Nakamoto lanza el sistema de pago Bitcoin en el año 2009. Las características propias de este sistema pretendían recuperar las características tan deseables del dinero en efectivo, de manera que el usuario podía disponer plenamente de su dinero para utilizarlo sin la intervención de terceros, lo que en palabras de Ammous (2018) suponía la devolución al usuario de la soberanía individual sobre su dinero, comparado con la consecución de una "libertad económica".

Aunque la creación de las criptomonedas era una absoluta novedad, su creador Satoshi Nakamoto había empleado para el desarrollo de la misma tecnología ya existente, aunque no tan conocidas en su momento, como las redes *peer-to-peer,* las funciones *hash*, firmas digitales, y prueba de trabajo. Cada una de ellas supondría la solución a los inconvenientes presentados por la introducción de la figura de un intermediario, además de otorgar estabilidad y seguridad al sistema.

La persona o personas que estaban detrás del nombre de Satoshi Nakamoto, desaparecieron de la esfera pública en el año 2010, dejado todo el sistema Bitcoin a disposición de los usuarios. Sólo se conoce una última aparición de Satoshi en el foro "BitcoinTalk", del que su fundador y un activo miembro, para comentar las correcciones realizadas a vulneraciones del sistema ante posibles ataques de denegación de servicio o ataques Dos (Satoshi, 2010).

Desde la creación de Bitcoin ha habido en su historia de vida una serie de hitos. El primero tuvo lugar el 3 de enero de 2009, momento en el que se minó el primer bloque de Bitcoin por una recompensa de 50 bitcoins y que pasó a conocerse como el "Bloque Génesis" o "Bloque 0" debido a la altura que ocupaba en la *Blockchain*[10] (Blockchain.com, 2021a). Unos días más tarde, el 12 de enero de 2009 tuvo lugar la primera transacción realizada con Bitcoin en la que Satoshi Nakamoto envió a Hal Finney, que estaba muy comprometido con la mejora del sistema, un total de 10 bitcoins (Finney, 2013) [11].

[10] La información relativa al primer bloque de la *Blockchain* de Bitcoin se puede consultar en https://www.blockchain.com/explorer/blocks/btc/0

[11]Hal Finney además de ser un desarrollador muy relevante e influyente en el movimiento *Cypherpunk* fue muy importante en los comienzos del sistema Bitcoin, ayudando a Nakamoto a solucionar diversos errores y

En el año 2010, tuvieron lugar varios eventos relevantes en la historia de Bitcoin. El primero de ellos tuvo lugar cuando se produjo un fallo seguridad en su *Blockchain* por el que se generaron por error 184 billones de bitcoins en una sola transacción. El 15 de agosto de ese mismo año el usuario Jeff Garzik advirtió este hecho en el popular foro "BitcoinTalk" señalando que el valor en uno de los bloques era extraño (Jgarzik, 2010)[12]. El error fue resuelto en menos de un día creando una bifurcación en la cadena que dejaba atrás el fallo en la cadena anterior, algo que de no haberse solucionado podría haber supuesto el fin del sistema Bitcoin.

En segundo lugar, otro momento significativo del 2010 fue la primera vez que el Bitcoin tuvo valor de mercado, es decir, la primera vez que estuvo disponible en una casa de cambio o *exchange* y por tanto podía obtenerse empleando dinero fiduciario. Se compraron 5050 bitcoins por el precio de 5,02 dólares a través de la ya extinta casa de cambio "*New Liberty Standard"* por un valor de 0,00094 dólares estadounidenses (Ammous, 2018). A partir de este momento, el valor de Bitcoin comenzó a experimentar sus características subidas y bajadas, siendo su inversión una actividad de riesgo.

En tercer lugar, el 22 de mayo fue relevante el hecho de que se pagaron 10.000 bitcoins por dos pizzas que en aquel momento tenían un valor de 25 dólares. Esa persona fue el desarrollador Laszlo Hanyecz que lanzó su propuesta el 18 de mayo de ese año a través del foro "BitcoinTalk*"* (Laszlo, 2010b) [13]. La propuesta fue aceptada cuatro días después[14], por lo que el 22 de mayo pasó a conocerse desde ese momento como el "Bitcoin Pizza Day*"*. Además de esto, el desarrollador Hanyecz también ha sido relevante en la historia de Bitcoin por su contribución al proceso de minado, siendo responsable de la adopción de minería con

haciendo varias pruebas con este. Durante el periodo de revisión del sistema estuvo en contacto con Nakamoto por correo electrónico tal y como cuenta él mismo en un mensaje en un foro el 19 de marzo de 2013, donde también cuenta que fue diagnosticado de la enfermedad ELA y que su calidad de vida y su actividad en programación se habían visto muy limitadas (Finney, 2013)

[12]El 15 de agosto de 2010 el usuario jgarzik comentaba en el foro: "*The value out in this block #74638 is quite strange*" (Jgarzik, 2010).

[13]En dicho mensaje en el foro, Laszlo exponía lo siguiente: "*I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy! I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire. If you're interested please let me know and we can work out a deal*"

[14]Cuatro días más tarde, el 22 de mayo, Laszlo vuelve a intervenir en el foro para exponer que había conseguido intercambiar 10.000 bitcoins por pizza, adjuntando fotos de ese momento y dando las gracias: "*I just want to report that I successfully traded 10,000 bitcoins for pizza. Pictures: http://heliacal.net/~solar/bitcoin/pizza/. Thanks jercos*!" (Laszlo, 2010c).

GPU (Unidad de Procesamiento Gráfico) en lugar de CPU (para obtener una mayor capacidad de procesamiento (Laszlo, 2010a).

Finalmente, en sus inicios Bitcoin estuvo implicado en dos importantes casos de delincuencia. El primero de ellos fue con la casa de cambio *Mt Gox Exchange* que fue lanzada el 18 de julio de 2010 y que ha sido una de las más populares en toda la trayectoria de vida de las criptomonedas llegando a alcanzar el 70% de todas las transacciones globales de Bitcoin. En el año 2011, *Mt Gox* sufrió un hackeo en el que desaparecieron alrededor de 850.000 bitcoins, lo que supuso un coste de unos 450 millones de dólares. El segundo evento tuvo lugar en el año 2011 en el que Bitcoin adquirió una elevada popularidad por el importante papel que tuvo en el criptomercado de drogas Silk Road en el que estaba disponible como forma de pago.

Aunque después de estos acontecimientos han tenido lugar otros momentos señalados en la historia de vida de Bitcoin hasta el día de hoy, se considera que los arriba presentados serían los sucesos más relevantes que tuvieron lugar en los primeros años de vida de la criptomoneda. Por tanto, se ofrece una visión suficiente sobre lo que supuso la creación de la criptomoneda Bitcoin, que previsiblemente podrá ayudar a comprender en detalle el funcionamiento de las tecnologías que permiten el éxito de esta moneda virtual.

Capítulo 2. Las Criptomonedas: Definiciones Y Características. La Bitcoin *Blockchain*.

Definiciones de Criptomoneda. Bitcoin.

Previamente a tratar las características de esta tecnología, será necesario aportar una definición de las criptomonedas que permita identificarlas y comprender aspectos más complejos de su funcionamiento. No obstante, esta no es una tarea sencilla, lo que ha ocasionado que existan una gran cantidad de definiciones válidas que han sido elaboradas desde ámbitos muy diversos.

El creador de la primera criptomoneda que existió -Satoshi Nakamoto- definió Bitcoin como un sistema de efectivo electrónico completamente *peer-to-peer* sin un tercero de confianza[15]. En este caso, la definición va mucho más allá de las criptomonedas y atiende al sistema Bitcoin[16] en su totalidad, no ofrece ninguna definición relacionada con su condición de moneda. Más adelante, en el *Whitepaper* de Bitcoin, se haría referencia al término "moneda electrónica", considerada como una cadena de firmas digitales (Nakamoto, 2008), pero no ofrece una definición clara con respecto al término criptomoneda.

De esta forma, una primera definición de este término pudiera venir derivada, de forma sencilla, de las dos partes que componen la palabra. El prefijo "cripto" procede del griego *criptos* u oculto. Por lo que hace alusión a la disciplina de la criptografía que permite hacer un mensaje inteligible empleando cifrado o codificación para que solo pueda ser leído por el destinatario señalado[17]. En segundo lugar, la palabra "moneda" se define como un "instrumento aceptado como unidad de cuenta, medida de valor y medio de pago" (RAE, 2020). Para criptomonedas como Bitcoin, la primera parte estaría garantizada, sin embargo, la consideración de moneda sigue siendo cuestionada por aquellos que han expuesto que, aunque permiten almacenar dinero, todavía no se ha solucionado el problema de la

[15]En el *email* original en una cadena de correos electrónicos sobre criptografía el 31 de octubre de 2008 a las 18:10h, el usuario Satoshi Nakamoto comenzaba diciendo: "*I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party*".

[16] Hay que señalar que a lo largo de esta investigación se utilizará el siguiente criterio para poder diferenciar el sistema de pago de la criptomoneda: cuando se escriba "Bitcoin" con "B" mayúscula se hará referencia al concepto de Bitcoin o a la totalidad del sistema de pago y cuando se escriba "bitcoin" con b minúscula se estará haciendo referencia a una unidad de la moneda cuyas abreviaturas son BTC o XBT (Bitcoin Project, 2020).

[17]La criptografía es la rama de las matemáticas que permite crear pruebas matemáticas que proporcionan altos niveles de seguridad. Para el caso del Bitcoin, esto impide que los monederos se puedan corromper y se pueda gastar el dinero de otras personas (Bitcoin Project, 2020). La primera parte hace referencia a que se trata de una moneda virtual protegida por criptografía, una técnica que permite hacer un mensaje ininteligible empleando el cifrado o codificación para que solo pueda ser leído por el destinatario señalado.

escalabilidad para soportar millones de transacciones, ni el problema de la volatilidad para poder ser utilizada como referencia de valor [18].

Los diccionarios podrían constituir también una fuente de la que obtener una definición sencilla del término. En el ámbito español, la Real Academia Española recoge el término criptomoneda en su Diccionario de la Lengua Española (DLE), definiéndola como "moneda virtual gestionada por una red de computadoras descentralizadas que cuenta con un sistema de encriptación para asegurar las transacciones entre usuarios" (RAE, 2023). Al mismo tiempo este término está recogido en otros diccionarios como el diccionario *Oxford Learner's*, que considera que una criptomoneda es un sistema de dinero electrónico que se utiliza para la compra y venta en línea sin la necesidad de un banco central[19] (Oxford University Press, 2020a). El diccionario Cambridge denomina criptomoneda a la moneda digital producida por una red pública, en lugar de por un gobierno, que utiliza criptografía para asegurar que los pagos se envían y reciben de forma segura[20] (Cambridge University Press, 2020). El *Oxford English Dictionary* define una criptomoneda como cualquiera de los diversos sistemas de pago digital que emplean técnicas criptográficas para controlar y verificar transacciones en una unidad de cuenta única independientemente de una autoridad central[21] (Oxford University Press, 2020b).

Aunque son muy variadas, estas definiciones permiten completar el concepto de criptomoneda, señalando aquellos elementos que es necesario que se conozcan para poder comprender su funcionamiento como "dinero electrónico", "utilización sin un banco central", "moneda digital", "criptografía" e "independiente de una autoridad central".

Por todo esto, ante la necesidad de una definición más completa del término, varias instituciones, tribunales y otros organismos que han trabajado en esta materia han elaborado y propuesto una definición de criptomoneda que les permitiera comenzar a trabajar en sus informes. Un ejemplo de ello es el Grupo de Acción Financiera Internacional- en adelante

[18]En el apartado referido a las características de las criptomonedas, en específico del Bitcoin se hablará con más detalle sobre las características de la escalabilidad y la volatilidad de la moneda y sus inconvenientes para la adopción de las criptomonedas como una moneda de uso habitual.

[19]Traducción al español de la definición original en inglés que aparece en el *Oxford Advanced Learner's Dictionary*: *any system of electronic money, used for buying and selling online and without the need for a central bank* (Oxford University Press, 2020a)

[20]Traducción al español de la definición original en inglés que aparece en el *Cambridge Dictionary*: *a digital currency produced by a public network, rather than any government, that uses cryptography to make sure payments are sent and received safely* (Cambridge University Press, 2020).

[21]Traducción al español de la definición original en inglés que aparece en el *Oxford English Dictionary*: *Any of various digital payment systems operating independently of a central authority and employing cryptographic techniques to control and verify transactions in a unique unit of account; (also) the units of account of such a system, considered collectively* (Oxford University Press, 2020b)

GAFI- o en inglés *Financial Action Task Force* (FATF)[22], que, en su informe del año 2014, previamente a la presentación de los riesgos asociados a las criptomonedas en materia de lavado de dinero y financiación del terrorismo, recoge una lista de términos clave de las monedas virtuales. El GAFI define una criptomoneda como "una moneda virtual descentralizada convertible, basada en las matemáticas que está protegida por criptografía, es decir, incorpora principios de la criptografía para implementar una economía de la información distribuida, descentralizada y segura" (2014, p. 5)[23].

Algunos autores expertos en la materia también han ofrecido su propia definición de criptomoneda. Un ejemplo de ello es Boar (2018) que la considera como "un activo creado fuera de las instancias del sistema financiero tradicional, basado en la confianza y la aceptación de sus usuarios a raíz de un sistema criptográfico que nos permite realizar transacciones dinerarias entre los miembros de la comunidad" (p.17). Schueffel et al. (2019) exponen que es una moneda digital en la que se utilizan técnicas de cifrado para controlar la generación de unidades monetarias y verificar la transferencia de fondos, operando independientemente de una sola unidad central[24] (p.11). Ron y Shamir (2013) consideran que Bitcoin es un sistema de dinero electrónico descentralizado que utiliza la red de pares para permitir los pagos entre las partes sin depender de la confianza mutua[25] (p. 8).

Desde el punto de vista legal, la utilización de nuevas tecnologías como las criptomonedas para cometer delitos ha requerido que los jueces se pronuncien al respecto. La primera definición relacionada con las criptomonedas en la jurisprudencia penal española aparece en la Sentencia del Tribunal Supremo (Sala de lo Penal, Sección 1.ª) número 326/2019, de 20 de junio ("STS 326/2019"). En esta se proporciona una definición de "Bitcoin" exponiendo que no es sino "un activo patrimonial inmaterial, en forma de unidad de cuenta definida mediante la tecnología informática y criptográfica denominada bitcoin,

[22]El GAFI o FATF es un organismo intergubernamental que tiene como objetivo prevenir el lavado de dinero, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva. Para ello desarrolla una serie de recomendaciones o estándares en esta materia, que abordan los nuevos riesgos que aparecen continuamente y orientan a los países -entre ellos España desde el año 1900- en cuanto a las reformas legislativas y regulatorias necesarias para afrontarlos (Financial Action Task Force, 2021).

[23]Traducción al español de la definición recogida en inglés en GAFI (2014): *Cryptocurrency refers to a math-based, decentralised convertible virtual currency that is protected by cryptography. —i.e., it incorporates principles of cryptography to implement a distributed, decentralised, secure information economy* (p.5).

[24]Traducción al español de la definición original en inglés que aparece en la enciclopedia de Schueffel et al. (2019): *A cryptocurrency is a digital currency in which encryption techniques are used to control the generation of units of currency and verify the transfer of funds, operating independently of one single central unit* (p.11).

[25] Traducción al español de la definición original en inglés que aparece en Ron y Shamir (2013): *Bitcoin is a decentralized electronic cash system using peer-to-peer networking to enable payments between parties without relying on mutual trust* (p.8).

cuyo valor es el que cada unidad de cuenta o su porción alcance por el concierto de la oferta y la demanda en la venta que de estas unidades se realiza a través de las plataformas de *trading* Bitcoin". Además, considera que el Bitcoin "no es algo susceptible de retorno, puesto que no se trata de un objeto material, ni tiene la consideración legal de dinero" (TS (Sala de lo Penal, Sección 1ª), sentencia núm. 326/2019 de 20 junio).

Por consiguiente, hablar de una definición de criptomoneda en realidad supone hablar de la definición del Bitcoin, la primera criptomoneda que supuso el origen de dicho término. Por lo tanto, siguiendo el mismo planteamiento que Nakamoto (2008), autores como Schueffel et al. (2019) también emplean el término Bitcoin para hacer referencia no solo a la criptomoneda basada en la *Blockchain*, sino también al sistema de pago digital creado por Satoshi Nakamoto.

Ahora bien, si se agrupan las definiciones mostradas hasta el momento, se puede ver que en su mayoría se hace referencia a que una criptomoneda es una moneda virtual, digital o incluso electrónica que está protegida mediante el uso de criptografía. La diferencia entre estos tres términos no es una cuestión baladí. De forma general, se hace referencia a las criptomonedas como monedas virtuales, aunque también en muchas ocasiones se han empleado términos como monedas digitales o dinero electrónico.

En el *Whitepaper* de Bitcoin, Satoshi Nakamoto únicamente habla de "moneda electrónica", denominando como tal a la cadena de firmas digitales (Nakamoto, 2008). El *e-money* o dinero electrónico es "una representación digital del dinero *fiat*[26] usada para transferir electrónicamente el valor de la moneda fiduciaria"[27] (Financial Action Task Force, 2014, p. 4). Por su parte, una moneda digital puede tratarse de una representación digital tanto de una moneda virtual (no *fiat*), como del dinero electrónico (*e-money*).

Algunos autores como Boar (2018) consideran que ambos términos, moneda digital y moneda virtual, pueden ser utilizados indistintamente para hacer referencia a las criptomonedas. En esta misma línea, Schueffel et al. (2019) también consideran que los términos *virtual currency, digital currency, electronic money* y *digital money* tienen el mismo significado incluyendo todos ellos dentro de la definición de *digital currency* o moneda digital que la definen como un tipo de moneda que no es física (es decir, no existen billetes ni

[26]El dinero *fiat* o dinero fiduciario, también conocido como "moneda real", "dinero real" o "moneda nacional" constituye la moneda o papel de un país que es designada como moneda de curso legal, circula, y es habitualmente usada y aceptada como medio de cambio en el país emisor (Financial Action Task Force, 2014, p. 4)

[27]Traducción al español de la definición en inglés recogida por el FATF (2014): *E-money is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency* (p.4).

monedas de la misma) y que sólo puede transmitirse por medios electrónicos, lo que suele permitir transacciones instantáneas y la transferencia de propiedad sin fronteras[28].

No obstante, hay autores que consideran que moneda digital y moneda virtual no son equivalentes. Así, Nieto (2018) establece diferencias entre ambos términos y hace distinciones entre los mismos. En primer lugar, considera que las monedas digitales son aquellas que se usan para pagar algún producto o servicio a través de un medio electrónico, son la representación digital del dinero físico -euros, libras, dólares- cuando no es posible su utilización en su forma física. Por ejemplo, cuando se paga por algún producto en comercios *online* en el que no se emplea dinero físico, sino que se utiliza la representación digital del dinero que se tiene depositado en la cuenta bancaria. En segundo lugar, considera una moneda virtual como aquella que solo existe en formato digital y que no tiene ningún equivalente en dinero físico. Se obtiene empleando dinero fiduciario, pero solo existiría y tendría valor en aquel entorno *online* que la acepte. Por ejemplo, son monedas virtuales aquellas que se utilizan en videojuegos *online* para adquirir nuevas funcionalidades o accesorios dentro del mismo.

En ese mismo sentido Kryskova Kuksa (2017) considera que una moneda virtual es una "representación digital de valor, no emitida por un Banco Central ni una autoridad. Funciona como un medio de intercambio; y/o una unidad de cuenta; y/o un depósito de valor. No se encuentra asociada a una moneda fiduciaria y no tiene estatus de moneda de curso legal, pero es aceptada por personas físicas o jurídicas como medio de pago y que puede transferirse, almacenarse o negociarse por medios electrónicos. Esta se diferencia de la moneda *fiat* (moneda real, dinero real o moneda nacional) que es la moneda de curso legal que posee un país" (Kryskova, 2017, p.315). Al mismo tiempo, diferencia por un lado la moneda virtual convertible o abierta, como aquella que puede transformar su valor en moneda real, por ejemplo, Bitcoin o los dólares "Linden" de la comunidad virtual *Second Life*. Por otro lado, expone que las monedas virtuales no convertibles o cerradas, son aquellas que tienen el objetivo de pertenecer a un dominio particular, como algunos videojuegos de rol en línea, que se rigen por las normas que impone el "propietario" y no pueden cambiarse por moneda fiduciaria.

[28]Traducción al español de la definición original en inglés que aparece en Schueffel et al. (2019): *A digital currency is a type of currency that is non-physical (i.e. no banknotes and coins exist thereof) and which can only be transmitted via electronic means, typically allowing for instantaneous transactions and borderless transfer of ownership* (p.14).

El GAFI en su informe del año 2014 considera una moneda virtual como "una representación digital de valor que puede ser comercializada digitalmente y que funciona como 1) medio de cambio; y/o 2) unidad de cuenta; y/o 3) almacén de valor, pero que no tiene estatus de moneda de curso legal en ninguna jurisdicción"[29] (Financial Action Task Force, 2014, p. 4)[30].

En España, las criptomonedas tienen una consideración de bien o activo, ya que se comercializa con ellas para obtener beneficios en su compraventa (González, 2021). Según esta concepción, las criptomonedas no serían consideradas monedas virtuales, ya que no se adaptan a la definición: "instrumento aceptado como unidad de cuenta, medida de valor y medio de pago", porque su objetivo es el almacenamiento de valor, no su utilización (González, 2021). Conforme a esta posición, el término criptomoneda no se ajustaría tampoco al concepto de moneda digital o al de activo, lo que supondrá una posterior preocupación en relación con la elaboración de su marco regulatorio.

La ausencia de un pronunciamiento del legislador sobre la naturaleza jurídica de las criptomonedas ha ocasionado que estas sean objeto de discusión[31]. Como expone (Pérez López, 2017), esta parece haberse orientado hacia una delimitación negativa de su definición, exponiendo no lo que se consideran, sino lo que no se consideran. De esta forma, las criptomonedas no se considerarían dinero electrónico en el sentido de la Ley 21/2011, de 26 de julio[32] por la que se transpone al ordenamiento jurídico español lo expuesto en la Directiva 2009/110/CE, de 16 de septiembre, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como la supervisión prudencial de dichas entidades[33]. Así, la Ley 21/2011, definía el "dinero electrónico"[34] de la misma forma que se hacía en la Directiva

[29]Traducción al español de la definición en inglés recogida por el FATF (2014): *Virtual currency is a digital representation5 of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment)6 in any jurisdiction* (p. 4).

[30] Desde la elaboración de esta definición hasta la actualidad, dos países han considerado las criptomonedas como moneda de curso legal, el Salvador y la República Centroafricana.

[31] En el informe del 2014 del BDE (Gorjón, 2014), parece evitarse continuamente el hecho de proporcionar una definición determinada de las criptomonedas, limitándose a hacer referencia a las mismas como "Las divisas o monedas virtuales constituyen un conjunto heterogéneo de instrumentos de pago innovadores que, por definición carecen de un soporte físico que los respalde"(Gorjón, 2014; Pérez López, 2017).

[32] Ley 21/2011, de 26 de julio, de dinero electrónico. https://www.boe.es/boe/dias/2011/07/27/pdfs/BOE-A-2011-12909.pdf

[33] DIRECTIVA 2009/110/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 16 de septiembre de 2009 sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE https://www.boe.es/doue/2009/267/L00007-00017.pdf

[34] Artículo 1.2 de la Ley 21/2011, de 26 de julio: "Se entiende por dinero electrónico todo valor monetario almacenado por medios electrónicos o magnéticos que represente un crédito sobre el emisor, que se emita al recibo de fondos con el propósito de efectuar operaciones de pago según se definen en el artículo 2.5 de la Ley

2009/110/CE[35]. No obstante, la ausencia de una definición exacta de criptomoneda en este texto es algo admisible si se repara en el hecho de que el texto fue promulgado en los comienzos del Bitcoin, por lo que no pretendía ni tampoco se podía tomar en consideración las criptomonedas para dar una definición (Pérez López, 2017).

El Parlamento Europeo y Consejo de la Unión Europea en el artículo 2 de la Directiva 2009/110/CE sobre el acceso a la actividad de las entidades de dinero electrónico, su ejercicio y la supervisión prudencial; definen el dinero electrónico como "todo valor monetario almacenado por medios electrónicos o magnéticos que representa un crédito sobre el emisor, se emite al recibo de fondos con el propósito de efectuar operaciones de pago, según se definen en el artículo 4, punto 5, de la Directiva 2007/64/CE, y que es aceptado por una persona física o jurídica distinta del emisor de dinero electrónico" (p. 11). En línea con esto, la Ley 21/2011, de 26 de julio, de dinero electrónico sostiene que dicha definición proporciona tres criterios a partir de los cuales determinar si un producto puede calificarse como dinero electrónico. Así, continúa diciendo que se excluye por tanto "[…] aquel valor monetario almacenado en instrumentos específicos, diseñados para atender a necesidades concretas y cuyo uso esté limitado, bien porque el titular sólo pueda utilizarlo en los establecimientos del propio emisor o en una red limitada de proveedores de bienes o servicios, bien porque pueda adquirirse con él únicamente una gama limitada de bienes o servicios" (p.84236)[36].

La Directiva 2018/843, incluye por primera vez una definición de moneda virtual en materia de la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo. Modificando lo expuesto en la directiva anterior en esta materia, añade a su artículo 3 la definición de "monedas virtuales" como: "representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto

16/2009, de 13 de noviembre, de servicios de pago, y que sea aceptado por una persona física o jurídica distinta del emisor de dinero electrónico" (p. 84238).

[35] Artículo 2.2 de la Directiva 2009/110/CE, de 16 de septiembre define «dinero electrónico» como: "todo valor monetario almacenado por medios electrónicos o magnéticos que representa un crédito sobre el emisor se emite al recibo de fondos con el propósito de efectuar operaciones de pago, según se definen en el artículo 4, punto 5, de la Directiva 2007/64/CE, y que es aceptado por una persona física o jurídica distinta del emisor de dinero electrónico" (L 267/11).

[36] Ley 21/2011, de 26 de julio, de dinero electrónico. https://www.boe.es/eli/es/l/2011/07/26/21
Aquí expone X. Pérez (2017), que las criptomonedas no se adaptarían a los dos primeros criterios de la definición mostrada, ya que no responden al esquema monetario clásico al no representar un título de valor respaldado por un emisor, y no son emitidas al recibo de "fondos", especialmente si entendemos que este término, en la línea marcada por nuestra interpretación de los considerados de la Directiva 2009/110/CE, podría hacer referencia a moneda de curso legal" (p.171).

jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos" (L156/54)[37].

Paradójicamente, en relación con lo anterior, el Bitcoin no se considera una moneda de curso legal en España, tal y como ha sido expuesto en reiteradas ocasiones. Hoy en día son pocos los defensores de las criptomonedas en el sentido de dinero propio o legal, de forma que incluso en muchos informes de autoridades o grupos de trabajo que utilizan el término "moneda" o *currency*, expresan la inexactitud de estos términos y niegan su condición de moneda (Pérez, 2017, p.142). Por otro lado, otros estudios se muestran más posibilistas y los califican como "dinero" o *money*, desde su función económica, pero precisan los matices y las diferencias con las monedas de curso legal (Pérez, 2017, p.143).

Por otro lado, se considera un método de pago legal y se ha de aplicar el Impuesto sobre el Valor Añadido, es decir, las transacciones están exentas de IVA para realizar pagos pero se debe declarar en la declaración de la renta porque se considera un bien, por lo que se tiene que incluir en el IRPF (González, 2021). Al mismo tiempo, desde el punto de vista del ordenamiento jurídico español, el Bitcoin es solo una mercancía, debiendo ser considerado desde el derecho civil español y atendiendo a los arts. 335, 337 y 345 CC, se trataría de un bien mueble, digital, no fungible y susceptible de propiedad privada (Aránguez, 2020).

En definitiva, por todo lo anterior, en este trabajo se considera que las criptomonedas se adaptarían mejor al término moneda virtual que moneda digital, ya que solo existen dentro de la red, es decir, no existen fuera del entorno *online*, pero a diferencia del resto de monedas virtuales estas no tienen un emisor concreto y están protegidas con criptografía. Al mismo tiempo, para el desarrollo de esta investigación se tendrán en cuenta aquellas definiciones de las criptomonedas que hacen referencia a aspectos técnicos de la moneda y su funcionamiento. No serán objeto de este trabajo las discusiones o reflexiones sobre si las criptomonedas tienen una consideración de dinero legal. Por tanto, se considerará para este estudio la definición oficial elaborada por Satoshi Nakamoto, considerando al resto como aportaciones complementarias con diversas características de las criptomonedas, algo que se tendrá en cuenta de una manera más detallada en apartados posteriores.

[37]Junto con este, también añade el punto 19 en el que define los "proveedores de servicios de custodia de monederos electrónicos" como: "una entidad que presta servicios de salvaguardia de claves criptográficas privadas en nombre de sus clientes, para la tenencia, el almacenamiento y la transferencia de monedas virtuales" (L 156/54).

Características Generales de las Criptomonedas y la *Blockchain* de Bitcoin

Las criptomonedas aparecieron en un momento de auge del dinero en efectivo, así como en una crisis financiera, lo que motivó que tuvieran mucho éxito ya que, tales circunstancias motivaban a que se apostara por un sistema que no estuviera controlado por los gobiernos ni bancos centrales (Antonopoulos, 2017). No obstante, el éxito de las criptomonedas, en especial del Bitcoin, se debe al mismo tiempo al desarrollo de la *Blockchain*, que constituye su principal tecnología. La *Blockchain* se desarrolló como la tecnología necesaria para que las criptomonedas pudieran funcionar de la forma que se plantearon. Así, aunque habitualmente se hable de criptomonedas y la extensión de su utilización, hay que señalar que su existencia tal y como se conocen actualmente no sería posible si al mismo tiempo no se hubiera desarrollado la *Blockchain.*

De esta forma, hablar de las características de las criptomonedas supondrá a su vez hablar de las características de la *Blockchain*. La mayoría de las características de las criptomonedas estarán determinadas por las características y el funcionamiento de la *Blockchain*, que es la tecnología que sustenta el sistema de pago.

Por este motivo, en el siguiente apartado se presentarán las características de las criptomonedas y de la *Blockchain.* El objetivo no será ofrecer un listado exhaustivo de todas las características de ambas de forma detallada, sino presentar de forma general aquellas que sean más significativas y que permitan al lector comprender el funcionamiento de este sistema de pago y disponer de la base de conocimiento en esta materia que le permita posteriormente abordar conceptos más complejos, así como casos de uso de esta tecnología.

Anonimato

El anonimato es una de las características más conocidas y destacadas al hablar de las criptomonedas. Consiste en la capacidad de utilizar las criptomonedas sin que se descubra la identidad de la persona que las ha utilizado.

No obstante, al contrario de lo que la mayoría de la sociedad cree, la utilización de bitcoins no ofrece un anonimato absoluto. Aunque las transacciones realizadas se pueden considerar anónimas porque no contienen datos o información que pueda ser relacionada directamente con la identidad de una persona, estas transacciones no son privadas. La transacción queda registrada de forma cronológica, irreversible y pública en la *Blockchain* y cualquier persona que acceda a esta puede conocer la cantidad de dinero transferida o el día y la hora de la transacción. De esta forma, aunque no se conozca la identidad el usuario, se podría estudiar su actividad con las criptomonedas y crear perfiles o patrones de actuación.

Surgen así las dudas en cuanto a la posibilidad de un anonimato total con Bitcoin, ya que, si se dispone de información adicional que pueda vincular una dirección con la identidad de una persona, se podría conocer toda su actividad en el sistema Bitcoin. El nivel de anonimato de las transacciones con criptomonedas como Bitcoin dependerá de que no se descubra la identidad que hay detrás de esta actividad.

En este sentido, se han observado diversas formas de revelar la identidad y terminar con el anonimato que se le atribuye a Bitcoin (Boar, 2018, p.94): 1) Compartir la identidad a través de una casa de cambio, que aunque no revelaría esta información a terceras partes, podría ser víctima de una brecha de seguridad y dejar al descubierto dicha información; 2) Utilizar de forma continuada y sin precauciones la misma dirección Bitcoin, lo que podría permitir el desarrollo de patrones de actividad y el estudio de perfiles; 3) Por medio del registro de la IP y la vinculación de esta con direcciones Bitcoin y el estudio de su actividad; 4) A través de la identificación de forma involuntaria por parte de las autoridades, que tienen la capacidad de rastrear movimientos de Bitcoin e identificar a los usuarios cuando esta actividad sea sospechosa.

Por todo ello, la comunidad de usuarios especializados en la utilización de las criptomonedas señala al Bitcoin como una criptomoneda pseudoanónima, en la que el anonimato dependerá de las precauciones que tome el usuario durante su utilización[38]. Por ejemplo, con la creación de varias direcciones Bitcoin para evitar el registro de los movimientos repetidos de una misma dirección (Fernández, 2018).

Este pseudoanonimato se ha dejado entrever como resultado de numerosas investigaciones en este ámbito que han analizado y representado el historial público de las transacciones de la *Blockchain* de Bitcoin obteniendo información sobre los patrones de los movimientos de bitcoins. Este es el caso, por ejemplo, del estudio de Reid y Harrigan (2013), que demostraron que mediante una representación adecuada de la red se pueden vincular direcciones públicas entre ellas y con información adicional exterior a la red. Esto posibilitaría la observación de la actividad de los usuarios en detalle en un análisis pasivo y la posible identificación de un usuario en específico en un análisis activo (Reid y Harrigan, 2013). Otro ejemplo sería la investigación de Ron y Shamir (2013), que analizaron el historial completo de todas las transacciones realizadas obteniendo información detallada sobre el comportamiento de los usuarios de la criptomoneda con respecto a cómo gastan y adquieren su dinero, el saldo de sus cuentas y cómo lo mueven para garantizar una mayor privacidad.

[38] Se desarrollará el debate sobre el supuesto anonimato de las criptomonedas en el bloque II.

Exponen que con información externa sobre la propiedad real de alguna de las direcciones se podría obtener la imagen completa de la actividad Bitcoin del individuo u organización (Ron y Shamir, 2013)[39].

A pesar de ello, muchos usuarios conscientes de esta peculiaridad de Bitcoin siguen una serie de métodos para intentar dificultar todo lo posible su identificación, como, por ejemplo: no usar siempre las mismas direcciones, usar direcciones diferentes para recibir el cambio de una transacción, *tumblers*, apostar por monedas de una mayor privacidad, usar a un tercero de confianza para enviar bitcoins y confundir el rastro, etc.

Por todo ello, muchos criminales han continuado utilizando Bitcoin para el desarrollo de sus actividades delictivas, ya que, aunque pueda no ser una característica determinante, el anonimato o pseudoanonimato de la moneda ha atraído a aquellos usuarios que son capaces de gestionar los riesgos de la moneda y desean ocultar su identidad criminal.

Volatilidad

Otra de las características más conocidas de la criptomoneda Bitcoin es su volatilidad que consiste en una variación intensa y frecuente en el precio de una unidad de la moneda.

El motivo por el que se produce esta inestabilidad en los precios de las criptomonedas es que el precio de una unidad no está establecido de forma oficial, sino que dependerá de los usuarios de la criptomoneda, de forma que una mayor demanda de esta supondrá un aumento de su valor.

De esta forma, las criptomonedas se han convertido en un activo de interés para actividades de inversión. Aunque puede conllevar un elevado riesgo debido a la alta volatilidad de su precio, también puede generar beneficios para aquellas personas que dispongan de los conocimientos necesarios para invertir de forma efectiva y segura. Este hecho no la convertiría en un activo menos recomendable, sino que exigiría considerar los riesgos de su utilización para aquellas personas interesadas en la inversión (Boar, 2013).

Un ejemplo de esta volatilidad se puede ver en los últimos registros del precio de la criptomoneda Bitcoin. Los valores han oscilado en el primer mes del año 2023 entre los 15.411,98 euros el primer día del mes hasta 21.116,35 euros el último día del mes[40]

[39] Utilizan como ejemplo para ilustrar sus afirmaciones el caso “WikiLeaks”. Debido a que se disponía de una dirección Bitcoin vinculada a este caso, los autores pudieron conocer al aplicar su metodología que disponían de 83 direcciones, que estuvieron implicados en 1088 transacciones y que habían acumulado 2605.25 bitcoins (Ron & Shamir, 2013).

[40] Datos recogidos de la plataforma CoinMarketCap para el mes de enero del año 2023 entre los días 01/01/2023 y 31/01/2023.

(CoinMarketCap, 2023b). En una misma semana, el precio ha osciló desde los 20.854,40 euros el lunes hasta los 21.878,92 euros un domingo, con picos mínimos de 20.546 euros y 21.986 euros[41] (CoinMarketCap, 2023b). Esto supondría una pérdida de una cantidad de dinero relevante para aquellas personas que no dispongan de la formación necesaria para gestionar las variaciones de miles de euros en periodos tan cortos de tiempo.

Por otro lado, también existiría la posibilidad de obtener precios fijos en la compra de criptomonedas a través de la gestión de una persona interesada en venderlas, que fijará un precio concreto como, por ejemplo, a través de la plataforma "LocalBitcoins". No obstante, esta opción no es la más reconocida ni mayormente utilizada.

Descentralización

La descentralización de los bitcoins fue la principal motivación que llevó a Satoshi Nakamoto a la creación del sistema Bitcoin. La figura del intermediario en el comercio electrónico aumentaba el riesgo de robo o fallo del sistema, además de la vigilancia o prohibiciones por parte del estado o instituciones para hacer frente a medidas relacionadas con la prevención del delito (p.ej. blanqueo de capitales), suponiendo un aumento del coste en términos de tiempo y dinero (Szabo, 2001).

El creador del Bitcoin era consciente de todo ello, por eso exponía que la confianza depositada en terceras partes para realizar una transacción lastraba el comercio *online* además de que no permitía que las transacciones fueran irreversibles (Nakamoto, 2008).

Como resultado de esta postura, el bitcoin es una moneda descentralizada, en otras palabras, no hay ninguna organización que respalde su valor y controle su emisión, de forma que cualquier persona puede instalarse el *software* correspondiente y ser parte de la red (Fernández, 2018). Esto es, no intervienen entidades centrales como bancos y gobiernos que emitan, distribuyan, regulen y controlen las transacciones y sustenten la economía. Esto ha sido posible gracias a la introducción de tecnologías como las redes P2P, que permiten al usuario del sistema Bitcoin realizar una transacción entre las partes interesadas de forma directa, sin la intervención de terceras partes (Nakamoto, 2008).

[41] Datos recogidos de la plataforma CoinMarketCap para la semana del mes de enero del año 2023 desde los días 23/01/2023 al 29/01/2023.

Inmutabilidad

La primera característica por excelencia de la *Blockchain* es su inmutabilidad, también conocida popularmente como la irreversibilidad de la cadena de bloques. Esto es, la cualidad de que no puede ser alterada o modificada[42].

Para conseguir esta cualidad, la cadena de bloques cuenta con varias tecnologías que lo permiten. Por un lado, es especialmente relevante el protocolo de consenso de Bitcoin. De esta forma, cualquier modificación que se desee introducir en el sistema, tendrá que aceptarse por la mayoría de los participantes, que mostrarán su consenso continuando con la minería a partir del último bloque minado en el que se habría introducido la modificación deseada. Los nodos mineros encargados de crear los bloques y formar la cadena, no aprobarían cualquier tipo de modificación realizada sobre la parte de la cadena ya establecida.

Por otro lado, son relevantes para este caso los elementos que se contienen en cada uno de los bloques. Como se decían anteriormente, los números *hashes* garantizan la integridad de la información de cada bloque, además de la unión cronológica y estable entre los bloques. Cualquier modificación en la información contenida en un bloque afectaría al número *hash* y por tanto alteraría la información contenida en el resto de los bloques posteriores. A medida que continúa formándose la cadena de bloques, aumenta la dificultad para realizar modificaciones. Una modificación que afecte a todos los bloques posteriores necesitaría de una elevada capacidad de cómputo para minar de nuevo los bloques siguientes. Este tipo de modificación tendría que ser aprobada por la mayoría de los nodos de la red en consenso, encargados de garantizar la estabilidad de la cadena. No es probable que se lleven a cabo modificaciones que afecten a la integridad de la cadena.

Este hecho dota al sistema de inmutabilidad, es decir no admite alteraciones, debido a que la distribución de la red de participantes, desconocidos entre sí y con una extensión global, hace imposible la manipulación de la red y la intervención en sus decisiones. Se puede afirmar que se trata de una moneda sólida, resistente a desórdenes y ataques.

Todo ello, supone una garantía de seguridad para el sistema de pago ante la imposibilidad de que los nodos verifiquen transacciones fraudulentas. Para que una transacción fraudulenta se pueda incorporar a la *Blockchain*, tiene que aceptarse por más de

[42] Pero esto no hace referencia al *software* Bitcoin, el cual es de código abierto y puede ser modificado por cualquier persona que lo desee, sino al funcionamiento del sistema Bitcoin.

la mitad de los nodos que forman parte del sistema[43]. No obstante, esta aceptación supondría afectar la integridad de la cadena de bloques, hecho del que no serían partidarios por dos motivos. El primero es que perderían la oportunidad de ganar una recompensa y la inversión realizada en la minería sería en vano. El segundo, es que la red perdería el valor que le aporta su integridad y robustez, ya que otros usuarios verían que es posible comprometer la cadena de bloques, las demandas de bitcoins se reducirían y con ello el precio de las monedas, dejando sin valor los fondos de los que pudieran disponer (Ammous, 2018).

Otro elemento que demuestra la inmutabilidad y seguridad del sistema de pago es el límite máximo de 21 millones de monedas. Esto convierte a esta criptomoneda en una de las mejores reservas de valor que existen ya que la oferta permanecerá inmutable, sin importar su demanda (no es posible la devaluación), a manipulaciones de otras autoridades o intentos de destrucción, obstaculización o confiscación por otros sujetos (Ammous, 2018, p. 263).

Irreversibilidad de las Operaciones

La irreversibilidad de las transacciones era una de las principales motivaciones de Satoshi Nakamoto para la creación del sistema Bitcoin. Según Nakamoto la confianza depositada en una tercera parte que actuaba como intermediario impedía que las transacciones realizadas en el comercio electrónico fueran irreversibles, ya que siempre existía la posibilidad de que esta parte interviniera revirtiendo la transacción (Nakamoto, 2008).

De esta forma, con la creación del sistema Bitcoin y la implementación de la denominada como "prueba de trabajo" o pruebas criptográficas resulta imposible revertir una transacción, ya que esto supondría deshacer toda la cadena de bloques de la *Blockchain* que habría sido minada hasta ese momento.

Las transacciones realizadas quedan registradas en la *Blockchain* de forma irreversible, sin que exista la posibilidad de cambiarlas. Esto dotaría a los individuos de la seguridad de que los bitcoins transferidos a sus carteras permanecerán en estas sin que la otra parte interviniente o terceras partes pueda revertir esta acción. No obstante, depende del usuario Bitcoin del que se trate, esta propiedad de irreversibilidad podría suponer un beneficio o un inconveniente[44]. Una vez verificada y confirmada una transacción, no podría

[43] Una red pública como Bitcoin tiene alrededor de 100.000 nodos, por lo que un ataque tendría que comprometer simultáneamente más de 50.000 nodos para alterar el consenso y realizar alteraciones fraudulentas sobre la cadena de bloques (García Meras, 2021).

[44] En este sentido, se ha reflexionado mucho acerca de la presencia de determinados delitos en la *Blockchain*, ya que esta información y sus vestigios no pueden ser eliminados. Esto sucede por ejemplo con la presencia de

ser revertida o modificada, lo que significaría la pérdida del dinero enviado en el caso del que se tratase de un error.

Este aspecto podría dotar de estabilidad, confianza y seguridad en los negocios que llevan a cabo, especialmente en los negocios criminales en los que es difícil establecer relaciones de confianza entre las partes.

Seguridad

En relación con la inmutabilidad de la cadena y la irreversibilidad de las operaciones, la *Blockchain* también es considerada como una tecnología muy segura, que ha captado la atención de aquellos negocios que requieren de este nivel de seguridad en sus actividades. Esto se debe a la combinación de diversos aspectos de la tecnología.

En primer lugar, la inmutabilidad de la información contenida en los bloques, lo que se consigue mediante las firmas digitales encadenadas y los números *hashes* de cada bloque.

En segundo lugar, el carácter distribuido de la red que permite a cada nodo disponer de una copia completa de la información de la cadena. En el caso de que pudiera suceder un incidente con alguno de los nodos, el resto de los participantes dispondría de una copia completa de la información. Si además se considera que los participantes son personas desconocidas distribuidas por diversas partes del mundo, esto hace que la cadena de bloques sea muy difícilmente manipulable.

Por último, el uso de la criptografía asimétrica para las firmas de las transacciones permite asegurar la identidad entre las partes de una forma segura e inequívoca sin la necesidad de que tengan que identificarse aportando sus datos personales.

Transparencia

La transparencia ha sido otra de las características relevantes de la cadena de bloques, de forma que se puede acceder de forma pública y libre a los registros realizados y almacenados desde que se creó la *Blockchain*. Además, se pueden obtener fácilmente copias de la información disponible, sin que esto pueda alterar o modificar los registros realizados.

material pornográfico infantil, un hecho que se ha investigado y detectado por las autoridades. Según T. García Meras (2021) en el Código penal se establece que este tipo de material debe borrarse del dispositivo o lugar en el que estuviere almacenado. Algunas investigaciones han determinado que alrededor del 99% de los más de 1600 archivos de la *Blockchain* en ese momento eran textos o imágenes, de las cuales, hay contenido como *links* a pornografía infantil que son distribuidos a todos los participantes del sistema (Matzutt et al., 2018). Este caso, la inmutabilidad de la cadena de bloques no permite que la información fuera eliminada, lo que supone un problema no solo para el buen desarrollo del a *Blockchain*, sino para las víctimas de este tipo de criminalidad (BBC, 2019).

Esta característica tiene una especial relevancia en la prevención del doble pago que Nakamoto preveía como posible riesgo en la eliminación de terceras partes del sistema de pago digital (Nakamoto, 2008). La posibilidad de acceder y conocer todos los registros realizados desde la fecha de creación de la cadena de bloques permite a cualquier usuario consultar y verificar la disponibilidad de saldos y que un saldo solo ha sido utilizado en una ocasión.

Al mismo tiempo, también se encuentra disponible el código de la *Blockchain* de forma abierta, para que cualquier persona que lo desee pueda estudiarlo, detectar posibles vulnerabilidades, proponer e incluso desarrollar modificaciones[45] que podrían dar lugar a nuevas creaciones independientes del sistema Bitcoin[46]. Se crea de esta forma una comunidad dedicada a la mejora y mantenimiento del sistema, lo que ha resultado ser de gran importancia considerando que se trata de un sistema que es posible gracias a la confianza depositada por los propios usuarios que conforman la red, siendo necesario que confíen en las técnicas criptográficas utilizadas y en el método de consenso que se utiliza para construir la cadena (Ponce de León, 2018, p. 37).

Envíos Globales y de Bajo Coste

Las criptomonedas suponen un modo rápido y barato de enviar fondos de forma global, 24 horas al día, siete días a la semana (Antonopoulos, 2017) con un coste muy bajo si se compara con otras monedas de carácter fiduciario como el euro o el dólar.

En relación con la posibilidad de envío de forma global, las criptomonedas solo existen en su forma digital lo que permite su utilización internacionalmente, sin límites territoriales y sin importar la moneda local que se utilice en el país en cuestión. Esto es posible gracias a la estructura del sistema Bitcoin en el que las transacciones se realizan a través de redes P2P en las que los nodos se sitúan al mismo nivel constituyendo un colectivo organizado de ordenadores interconectados que permiten el envío entre las partes de forma directa y sin intermediarios, sin importar su localización. Así, utilizando criptomonedas como los bitcoins, se puede enviar el dinero en forma de bitcoins y luego convertirlo a moneda *fíat*

[45] Esta propiedad permite el desarrollo de las conocidas como criptomonedas alternativas o *altcoins*, que se explicarán en apartados posteriores.

[46] En este sentido merece la pena señalar que esto no significa que existe la posibilidad de introducir modificaciones en el sistema de pago Bitcoin. El código de la cadena de bloques está disponible para poder modificarse y crear nuevas tecnologías que ya no formarían parte del sistema Bitcoin. Esto es, a partir del código fuente liberado por Satoshi Nakamoto, se pueden desarrollar otros proyectos similares, pero debido a las propias características del código del sistema Bitcoin no es posible introducir modificaciones al sistema ya establecido.

de nuevo (euros, dólares, pesos, etc.). No obstante, su utilización no requiere de realizar una conversión a dinero en efectivo, ni a la moneda que se utiliza localmente.

En cuanto a los bajos costes de las transacciones con criptomonedas, en primer lugar, habría que señalar que, en la actualidad, cualquier transacción de dinero fiduciario realizada mediante una entidad bancaria ordinaria traerá consigo una serie de costes asociados. Esto es incluso más notorio en el caso de que se trate de una transacción de grandes cantidades de dinero. Incluso puede suceder que las entidades bancarias se nieguen a realizar determinadas transacciones como aquellas que conllevan una cantidad muy pequeña de dinero.

Estos inconvenientes fueron algunos de los que Satoshi Nakamoto pretendía evitar con la creación del sistema Bitcoin (Nakamoto, 2008). Por ello, estableció que en las transacciones con bitcoins solo se pagaría un pequeño coste a los mineros o a los servicios de intercambio, con independencia del tamaño de la transacción de la que se trate.

Las tasas de las transacciones se muestran en una unidad de Bitcoin conocida como "Satoshi", que equivale a 0,00000001 BTC. Actualmente, la transacción más rápida y barata requiere del pago de 102 satoshis/*byte* (Coinbase, 2023)[47]. Esto es, para una transacción de un tamaño medio de 224 bytes, se requerirá del pago de 22,848 satoshis (Coinbase, 2023). Según la tasa de conversión actual, esta cifra equivaldría a 4,96 euros.

De esta forma, ha sido posible obtener una mayor eficiencia económica en comparación con los sistemas de pago centralizados. El coste para los usuarios individuales de este tipo de registros es mínimo en comparación con las tasas o costes de autoridades u otros agentes que actúan como terceros de confianza en los anteriores sistemas de pago. Esto puede verse reflejado también en los costes de las transacciones realizadas con la criptomoneda.

De acuerdo con la opinión de autores como Ammous (2018), la utilización de las criptomonedas no sustituirá por completo a la utilización del dinero fiduciario. No obstante, es necesario hacer referencia al bajo coste de los envíos de carácter internacional, porque se considera que puede ser un aspecto de interés en la valoración de esta tecnología como una herramienta para el delito.

Este aspecto puede ser de interés para criminales que operan con un carácter transaccional. En primer lugar, porque que no tendrían que convertir los beneficios de sus actividades delictivas a cada una de las monedas locales de los países en los que operan. Además de que se les permite la realización de transferencias de cualquier tipo entre

[47] Datos recogidos el 2 de febrero de 2023 de la página https://bitcoinfees.earn.com/

individuos de forma directa y sin la intervención de entidades bancarias o gobiernos. En segundo lugar, porque se les permite realizar transacciones con bitcoins de forma global de bajo coste y sin importar la cantidad de dinero que se desea transferir.

La *Blockchain* o Cadena de Bloques. Bitcoin *Blockchain.*

La creación de la criptomoneda Bitcoin tenía como objetivo conseguir un sistema de pago digital que permitiera mantener los beneficios que supone el pago con dinero en efectivo, como la independencia de terceros en confianza, la privacidad de las transacciones, la disponibilidad y el almacenamiento de forma independiente a autoridades políticas u otras instituciones.

No obstante, para la aparición de esta criptomoneda su creador, Satoshi Nakamoto, tuvo que desarrollar una tecnología que permitiera su adecuado funcionamiento al mismo tiempo que resolvía algunos de los problemas que podían surgir de la eliminación de intermediarios en un comercio electrónico.

De esta forma, desarrolló la tecnología *Blockchain*, que supuso desde su aparición una innovación tecnológica que ha adquirido una elevada importancia mucho más allá de la utilización de las criptomonedas. Por primera vez se disponía de una tecnología que permitía el desarrollo de procesos entre las partes interesadas sin la necesidad de intermediarios, lo que la ha posicionado como una tecnología disruptiva cuya creación se considera equiparable a la de Internet.

Por lo tanto, las características de las criptomonedas vienen determinadas por las características y el funcionamiento de la *Blockchain*. En este apartado se tratará la *Blockchain* del sistema de pago Bitcoin por haber sido la primera *Blockchain* que surgió y la que sigue teniendo una mayor importancia por la mayor utilización de su criptomoneda[48].

Definiciones de la Blockchain

De forma simplificada, la primera definición de la *Blockchain* viene dada de la traducción al español del propio término. Así, está formada por "*Block*" que significa "bloque" y *chain* que significa "cadena", de forma que se define como una cadena de bloques del sistema de pago Bitcoin.

[48] Hay otras redes *Blockchain* de uso general como: Ethereum (*smart contracts*), IOTA, NANO, Zcash, nem y EOS. Estas dos últimas primaron que las transacciones se puedan realizar de una forma más rápida para permitir que se puedan implementar esta tecnología en actividades que requieren esta confirmación de una forma más rápida. Hay redes específicas para las empresas como: Quorum, Hyperledger, TioTA, Alastria (Torrero, 2021).

Aunque se explicará su funcionamiento de manera detallada en apartados posteriores, de forma resumida con el propósito de que se comprendan mejor las definiciones de esta tecnología, se puede decir que cada uno de estos bloques contendrá las transacciones realizadas con la criptomoneda Bitcoin que han sido verificadas y almacenadas por los nodos mineros. La incorporación de cada bloque a la cadena final será realizada por aquel nodo ganador de una compleja prueba criptográfica llamada *proof-of-work* o prueba de trabajo. Cada uno de los bloques de la cadena estará unido al anterior y al posterior a través de un *hash*[49] desde el primer bloque de la *Blockchain* llamado "Bloque génesis" o "Bloque 0". Esto le otorga la propiedad de ser un registro inmutable y ordenado, que además puede ser consultado de manera pública como si se tratara de un listado de registros o un libro de contabilidad.

Este funcionamiento tan complejo ha ocasionado que presentar una única definición de *Blockchain* no sea una tarea sencilla. De forma general, se utilizan una gran variedad de términos para hacer referencia a la cadena de bloques denominándola un registro, una base de datos, un libro de contabilidad o un libro mayor.

Una definición clásica es la que considera una *Blockchain* como una cadena de bloques que contienen las transacciones realizadas y que se vinculan con el bloque anterior desde el primer bloque creado o bloque génesis[50] (Antonopoulos, 2017). Desde otra perspectiva general, también puede ser considerada como "un registro permanente, seguro y completamente descentralizado de transacciones, hechos o procesos ordenados cronológicamente" (Ponce de León, 2018, p. 36). Una postura más amplia es tomada por M. González-Meneses (2019) que, incluyendo todos los términos anteriores sugiere considerar la *Blockchain* desde diferentes planos: 1) como una base de datos de información que se va creando y registrando; 2) como un protocolo, programa o conjunto de reglas o instrucciones que rigen la información almacenada; 3) como una red de equipos o infraestructuras que mediante la aplicación de un protocolo va generando la infraestructura (p.51).

[49] En páginas posteriores se explicará con mayor detalle en qué consiste el término *hash,* así como otros elementos utilizados en esta breve explicación introductoria de la *Blockchain*.
[50]Definición original obtenida de Antonopoulos (2015): *A list of validated blocks, each linking to its predecessor all the way to the genesis block.*

Si se atiende a la tecnología que la conforma, la *Blockchain* se define como una tecnología de Registro Distribuido o *Distributed Ledger Tecnology* (DLT)[51,52]. Aunque las DLT ya existían como una tecnología independiente antes de la aparición de la *Blockchain*, el amplio desarrollo, popularidad y adopción en la sociedad de esta última ha ocasionado que se realice una equiparación entre DLT y *Blockchain*, en muchas ocasiones sin establecer ningún tipo de distinción. Esto se ha debido a que este término ha supuesto un amplio abanico que hace referencia a aquellos sistemas donde intervienen múltiples partes que operan en entornos sin un operador o autoridad central (Rauchs et al., 2018) [53].

Funcionamiento de la Blockchain

En la actualidad, el tamaño de la Blockchain es de 334.015k, el tamaño del bloque promedio es de 1323Mb y el tiempo medio de confirmación es de 12.5 minutos[54,55].

De acuerdo con su tecnología de registro distribuido (DLT) la *Blockchain* constituye una red de bloques de carácter descentralizado formada por todos los nodos de la red, que disponen de tantas copias de la cadena de bloques como participantes en la misma. Cualquier persona que lo desee, podría acceder a la *Blockchain* y consultar libremente cualquiera de las transacciones registradas, que quedan almacenadas cronológicamente, pudiendo obtener los datos relativos a su registro como la fecha y la hora, o bien con respecto a la cantidad de bitcoins enviados o recibidos, las direcciones de envío o destino o la altura del bloque en el que se encuentran. No obstante, no es posible obtener ningún dato relativo a la identidad

[51] Aunque este concepto se ha popularizado con la aparición de la *Blockchain* en el sistema Bitcoin, se trata de un concepto que emergió en el año 1982 con el estudio de los problemas de los generales Bizantinos, mucho antes de que se empezaran a ver las primeras ideas en relación con la creación de la *Blockchain* en el año 1992 (Rauchs et al., 2018). Las primeras pinceladas sobre una *Blockchain* se pueden ver en el trabajo de S. Haber y W. S. Stornetta (1991) sobre un método para certificar la creación o modificación de un documento en formato digital que consistía en un sellado de tiempo digital de los documentos; o en el trabajo de D. Bayer, S. Haber y W. S. Stornetta (1999) que revisa el trabajo anterior sobre el sellado de tiempo y las funciones hash para proponer modificaciones y otras mejoras tras la lógica de que para establecer que un documento fue creado antes de un momento dado, es necesario provocar un evento que se base en ese documento y pueda ser observado por otros. Ambos introdujeron las nociones de una cadena unida mediante criptografía que sella de forma segura y digital sus datos con un sello de tiempo y que se trata de un sistema distribuido usando funciones hash y árboles de Merkle (Rauchs et al., 2018, p. 13)

[52] En ocasiones algunos autores también utilizan el término "tecnología de contabilidad distribuida" o registro de transacciones". En este sentido, P. J. Ponce (2018) expone que no es correcto denominar a la *Blockchain* como un registro de cuentas, ya que lo que se almacena en los bloques son transacciones, no cuentas de usuario ni saldos de éstas.

[53] Dentro de esta concepción amplia de la DLT, autores como Rauchs et al. (2018) consideran que la *Blockchain* podría ser un subconjunto dentro de este entorno que dispone de una estructura especial que consiste en una cadena de bloques de datos unidos a través de *hashes.*

[54]Datos obtenidos para el 19 de marzo de 2021 de Blockchain.com (2021b).

[55]Tiempo medio para que una transacción con tarifas de minero se incluya en un bloque extraído y se agregue al libro mayor público (Blockchain.com, 2021b).

personal de ninguna de las partes involucradas en la transacción, lo que la dota de cierto anonimato.

Este carácter transparente de la *Blockchain* no surgió al azar, sino que fue ideado como una medida de seguridad para evitar el doble gasto. Esto es, en el proceso de creación de Bitcoin, Satoshi Nakamoto detectó que la eliminación de la figura del intermediario de confianza suponía la aparición de algunos riesgos, como en este caso el doble gasto[56]. Para poder evitar este problema, consideró que era necesario un sistema que permitiera a todos los usuarios de la red comprobar y verificar las transacciones realizadas y que una vez comprobadas, quedaran almacenadas de forma irreversible, dejando constancia de la fecha y hora en la que se registraron[57]. No obstante, en la actualidad esta tecnología ha servido para resolver numerosos tipos de problemas: desintermediación de procesos y modelos de negocio, trazabilidad y transparencia de procesos, visión única del dato sincronizada, consensuada e inalterable y por último, confiabilidad, finalización y no repudio de las transacciones (Lage, 2021).

En relación con lo anterior, la Tecnología de Registro Distribuido (DLT) es idónea en el sistema Bitcoin porque permite conseguir la supresión de la autoridad central. Aunque la utilización de esta tecnología se ha popularizado con la aparición de la *Blockchain,* debido a su carácter pionero y el papel que ha ocupado como tecnología disruptiva en la sociedad, lo cierto es que la tecnología que respalda tanto a la criptomoneda Bitcoin como a la Blockchain no es completamente nueva. Ambos productos están basados en conceptos y tecnologías que en su mayoría ya existían, la novedad en este caso fue la utilización de todas ellas de forma conjunta con el propósito de crear un sistema de pago digital que mantuviera los beneficios del pago en efectivo y solventara los posibles riesgos de eliminar las terceras partes en confianza.

De esta forma, el funcionamiento de la *Blockchain* estará determinado por la forma en la que opera la DLT, que se considera una tecnología de carácter distribuido debido a la estructura que la forma y a su funcionamiento.

---

[56] El control del doble gasto no es algo que haya aparecido con el surgimiento de la *Blockchain*. En los pagos digitales el saldo de las cuentas y los movimientos realizados son controlados por las entidades bancarias, de forma que supervisan que nadie pueda vulnerar el sistema y utilizar varias veces el mismo dinero. En la *Blockchain,* al suprimir la figura de la entidad bancaria, se requiere de un mecanismo que permita evitar este problema.

[57] Autores como Ammous (2018, p.233) han llegado a afirmar que la *Blockchain* como libro público sería la única serie objetiva de hechos del mundo, ya que a diferencia de lo que advierten muchos filósofos sobre que la veracidad de los hechos depende de la persona que lo afirma o lo oye, el registro de las transacciones Bitcoin no depende de la palabra de nadie, sino que se crea con electricidad y capacidad de procesamiento.

Como parte de esta estructura, en el desarrollo de la *Blockchain*, tienen un papel fundamental los nodos mineros, que son los encargados de crear los nuevos bloques que formarán parte de la cadena de bloques. Estos nodos están distribuidos formando una red sin ninguna autoridad central, por lo que la incorporación de uno de los bloques creados a la cadena de bloques tendrá que realizarse conforme a un algoritmo o protocolo de consenso distribuido[58] que consiste en el proceso de elaboración e incorporación de bloques a la *Blockchain*.

Este proceso comienza con el envío de una transacción realizada con Bitcoin a todos los nodos mineros que forman parte de la red y que son los encargados de verificarla comprobando que la persona que la ha ordenado dispone del saldo suficiente para llevarla a cabo. Una vez verificada, cada uno de los nodos almacena la transacción en su propio bloque, que una vez está completo y no admite más transacciones se "valida" o "sella", pasando a ser un potencial bloque para formar parte de la *Blockchain*.

De entre todos los potenciales bloques, se elegirá el bloque del nodo que haya superado con éxito una compleja prueba criptográfica conocida como "Prueba de trabajo" (*proof of work*) que consiste en la búsqueda de un valor que permita obtener un número determinado de ceros en el *hash* del bloque[59]. Esta actividad requerirá de una capacidad de computación exponencial al número de ceros requeridos y una vez se ha invertido la CPU, la PoW no podría ser modificada sin rehacerla, es decir, habría que volver a invertir la misma capacidad computacional, lo que incrementaría el costo a medida que se añaden nuevos bloques a la cadena (Nakamoto, 2008). El bloque que será seleccionado para formar parte de la cadena de bloques o *Blockchain* será el que corresponda al nodo ganador de la prueba de trabajo. Esta consiste en la resolución de un complejo problema matemático para el que se debe encontrar aquel hash que comience con un número determinado de ceros.

Una vez se determina el bloque seleccionado, este es comunicado al resto de nodos para que lo confirmen y verifiquen que efectivamente las transacciones y las firmas son válidas y que no ha tenido lugar un doble gasto.

---

[58] Hay varios tipos de algoritmo de consenso y este dependerá de la configuración de la red de nodos que da soporte al sistema, pudiendo ser una red pública o una red privada o autorizada (*permissioned*, en inglés). En la primera, cualquier persona que lo desee puede descargarse el *software* necesario y ejecutarlo en un ordenador conectado a internet generando un nuevo nodo en la red. Por otro lado, las redes privadas requieren del permiso del órgano que actúa como gestor de la red para poder participar de la misma y ejecutar un nodo (Ponce de León, 2018). En el sistema Bitcoin, con una *Blockchain* de carácter público, el protocolo de consenso permite verificar la información que se está enviando y compartiendo sin la necesidad de que exista la figura de un tercero que sea la encargada de esta tarea.

[59] Este concepto se explicará con detalle posteriormente en el apartado perteneciente a las tecnologías y elementos clave que conforman la *Blockchain*.

La aceptación del nuevo bloque por cada uno de los nodos se realiza desde el momento en el que continúan su actividad minera de un nuevo bloque incluyendo el hash del bloque anterior. Se podría hablar en este caso de un proceso democrático cuyo resultado ha sido fruto de la decisión de la mayoría, ya que la selección de cada uno de los bloques que forman parte de la *Blockchain* se ha realizado de forma conjunta y consensuada por la mayoría de los nodos que forman parte de la red. Así, la cadena principal de la *Blockchain* será aquella que presente una mayor longitud, y que por tanto ha recibido un mayor número de apoyos.

La novedad que presenta la *Blockchain* con respecto a sistemas de comprobación anteriores es que se trata de un sistema colaborativo, es decir, los nodos que forman parte de la red son los encargados de comprobar la veracidad de las transacciones que quedan registradas. Esto dota a la red de una elevada seguridad, ya que es muy improbable que tan elevado número de nodos, distribuidos por la red y desconocidos entre sí puedan coordinarse para manipular la red. Esto fue previsto en la creación de la *Blockchain* mediante la consideración durante su desarrollo de la formulación matemática del conocido problema de los generales bizantinos en adelante PBFT (*Practical Byzantine Fault Tolerance Algorithm*, en inglés) que ha supuesto la base tecnológica de la *Blockchain*. Habitualmente este problema se expone para evaluar las condiciones de fiabilidad o tolerancia a los fallos de un sistema de múltiples partes, resaltando la importancia del consenso y coordinación de cada una para conseguir el desarrollo efectivo de una actividad[60]. Se plasma con la fórmula $M=3t+1$, de forma que "M" es el número de agentes honestos que intervienen en el sistema y "t" el número de agentes traidores, corruptos o tramposos (González-Meneses, 2019). Así, el sistema se aseguraría de que los agentes honestos o fieles representan al menos 2/3 más que los agentes traidores. Esto queda reflejado en el desarrollo del protocolo de consenso de la *Blockchain*, donde se pone de manifiesto la importancia de la actuación coordinada y consensuada entre los nodos para verificar y validad las transacciones y para confirmar y aceptar un bloque de forma conjunta en la cadena de bloques. Al no existir un nodo central

[60]Para la explicación de este problema se pone como ejemplo el caso de un grupo de tropas bizantinas sitiando una ciudad. Cada una de las tropas está liderada por un teniente y estas a su vez tienen que seguir las órdenes del comandante de las tropas. El éxito de la actuación dependerá de que las tropas actúen de forma coordinada conforme a la decisión del comandante sobre si atacar la ciudad o retirarse. El problema reside en que las tropas que rodean la ciudad están separadas geográficamente, por lo que la comunicación entre los grupos y con el comandante tenía que realizarse a través de un mensajero. Para garantizar una actuación coordinada, el mensaje de actuación o de retirada debía mantenerse íntegro para cada una de las tropas, por lo que la presencia de un comandante o teniente traidor que modificaran el mensaje en algún punto podría suponer un fallo en la coordinación de las tropas y por tanto el fracaso del ejército.

que sea el encargado de coordinar esta actividad, el papel de los nodos mineros en este caso es fundamental para mantener la integridad y estabilidad de la *Blockchain*.

El funcionamiento en conjunto de todas las tecnologías mencionadas anteriormente dota a la *Blockchain* de una serie de características que le permiten desarrollar de forma eficaz el propósito por el que fue creada en el sistema Bitcoin. Por ello, será de utilidad dedicar un apartado a señalar y describir dichas tecnologías.

Tecnologías y Elementos Clave que Forman la Blockchain

Aunque la DLT se posiciona como la tecnología clave en el funcionamiento de la *Blockchain*, existen al mismo tiempo otras tecnologías y elementos que son clave en el desarrollo de su actividad.

Aunque algunos de los términos siguientes fueron mencionados anteriormente en la explicación general del su funcionamiento, en el siguiente apartado se desarrollarán detalladamente con el propósito de que se comprenda la relevancia que tienen dentro del sistema Bitcoin.

Estos son la tecnología de carácter distribuido, las redes *peer-to-peer,* la criptografía asimétrica o de clave pública, los algoritmos *hash* y la prueba de trabajo (*proof-of-work*). Además, también se considera de relevancia la explicación de la estructura y contenido de los bloques de la cadena para comprender de una forma completa y amplia el desarrollo de la *Blockchain*.

Tecnología de Carácter Distribuido o de Redes Distribuidas. Según la forma en la que se comunican los nodos que conforman la red de un sistema se pueden encontrar tres tipos de redes: redes centralizadas, redes descentralizadas y redes distribuidas. La elección de una forma de organización u otra puede parecer una cuestión baladí. Sin embargo, cada una de las diferentes formas que existen puede suponer diferentes riesgos para la comunicación que pretenden soportar, por lo que se deben considerar estos aspectos previamente.

Las redes centralizadas son aquellas en las que un nodo central es el encargado de la supervisión y gestión de la comunicación de la red. El riesgo que presentan este tipo de redes consiste en que el nodo central puede comprometer la información que se está compartiendo. En relación con las redes descentralizadas y las redes distribuidas, aunque en ocasiones ambas han sido equiparadas, mantienen algunas diferencias. Aunque en ambos tipos de red los nodos cuentan con la libertad de una red en la que no se dispone de un nodo central que controla en tráfico de la información, en las redes descentralizadas existe cierto control por

parte de grupos de nodos que centralizan parte de la comunicación. No obstante, en las redes distribuidas como la que podemos encontrar en la Bitcoin *Blockchain*, los nodos se comunican entre sí en todas direcciones con los nodos más cercanos, sin necesidad de un nodo central que gestione la actividad, lo que dificulta que alguno de ellos pueda centralizar la información. Así, si uno de los nodos de esta red queda comprometido, la comunicación podría mantenerse a través de los nodos cercanos, aunque esta tuviera que recorrer una mayor distancia (González, 2021), lo que se asegura a su vez con la disposición de cada uno de los nodos de una copia completa de toda la información, sin que esta pueda ser parcialmente modificada o perdida durante la comunicación.

Redes *Peer-To-Peer* (P2P). Las redes *peer-to-peer* (P2P por sus siglas en inglés), son un tipo de arquitectura para la comunicación entre aplicaciones que permite a los ordenadores o nodos integrados comunicarse y compartir información sin necesidad de un servidor central que la facilite (Panda Security, 2010). De esta forma, permiten a un individuo de la red contactar con otro individuo sin ningún tipo de intermediario o tercera parte (Bitcoin Project, 2020).

Los usuarios interesados en participar en estas redes solo necesitan descargar el *software* de la red en cuestión y su ordenador pasará a ser uno de los nodos que la conforman. Así, se permite una relación horizontal entre los nodos compartiendo recursos como el almacenamiento y la capacidad de procesamiento sin intermediarios, de ahí que se les considere *peers*, iguales o pares.

A diferencia del paradigma anterior de cliente-servidor, en este caso no hay un servidor central que gestione, controle, compruebe y almacene los recursos que se están intercambiando. Esto permite solucionar que un aumento de clientes pueda ocasionar que el servidor central no sea capaz de reaccionar y adaptarse para dar respuesta a todas las peticiones realizadas sin perder calidad (escalabilidad). Se constituye de esta forma, como un colectivo organizado de ordenadores interconectados en el que no hay un "cliente-servidor", sino que todos los nodos actúan como iguales y comparten recursos a cambio de recursos.

De esta forma, este tipo de redes se han utilizado para intercambiar archivos, *software* libre, para aplicaciones de *streaming* de vídeo, videollamadas, música o incluso la transferencia de criptomonedas mediante la red Bitcoin como se verá en este caso.

En sus orígenes, comenzaron a tener éxito a partir de que "Napster", considerada como la primera gran red P2P de intercambio de archivos, permitiera el intercambio de archivos de música en un formato ".mp3" (García, 2019). No era realmente una red P2P pura,

sino que tenía un servidor central que indexaba usuarios y archivos compartidos. Esto le permitió cerrar completamente tras una serie de demandas millonarias por parte de discográficas (Romero, 2015)[61]. Sin embargo, inspiró la creación de muchos otros programas similares que han tenido mucho éxito como Ares (Ares Galaxy), eDonkey (eMule) y BitTorrent, que han sido utilizados mundialmente.

Sin embargo, aunque las redes P2P no son ilegales en sí mismas ya que se crearon con la finalidad de compartir recursos entre usuarios, la posibilidad de intercambiar archivos sin servidores centrales ha dado paso a ciertos tipos de actividades delictivas. Como se ha visto anteriormente, se utilizaron para intercambiar material audiovisual con derechos de autor, cometiendo delitos contra la propiedad intelectual, pero también se ha visto su utilización para la distribución de material de pornografía infantil, utilizando programas como "eMule" o "BitTorrent" que emplean redes P2P[62]. La descarga de archivos empleando estos programas supone su almacenamiento en una carpeta que a su vez se comparte con el resto de los integrantes de la red.

No obstante, aunque haya sido utilizada con fines delictivos, los protocolos P2P tienen un carácter legal, permitiendo la creación de estructuras descentralizadas y no estructuradas, difícilmente censurables y de uso libre (bit2me Academy, 2020b).

Todo ello motivó a que se desarrollara el sistema Bitcoin teniendo como base este protocolo para comunicar a dos partes sin intermediarios. Esta red permite una serie de ventajas en el sistema Bitcoin como que es resistente a la censura, es resistente a la caída de un nodo, presenta soluciones a los problemas de escalabilidad, ofrecen un alto ancho de banda, aseguran la confianza de los usuarios y sirven para transmitir información de cualquier tipo (bit2me Academy, 2020b).

Su utilización en Bitcoin permite garantizar la descentralización del sistema, evitando el control de entidades centrales, permitiendo a los usuarios manejar valor sin intermediarios y solucionar problemas de sistemas de pago anteriores como el doble pago (bit2me Academy, 2020b). La red construida permite disponer de un registro inmodificable (bit2me Academy, 2020b).

---

[61] La legalidad de la creación de estas ya se determinó con la sentencia histórica del desarrollador Pablo Soto en la que la Audiencia Provincial de Madrid desestimaba el recurso de las discográficas Warner, Universal EMI, Sony BMG y la patronal musical española "Promusicae" que lo demandaban por 13 millones de euros por haber desarrollado un programa de intercambio de archivos P2P, acusado de infringir la propiedad intelectual y por competencia desleal (Romero, 2015).

[62] Según Policía Nacional ha aumentado en un 25% el número de conexiones detectadas en las se ha descargado este tipo de material a través de redes *peer-to-peer* (eMule, Gnutella y BitTorrent) pasando de 16911 casos entre 17-24 de marzo a 21094 casos entre el 24-31 de marzo (Europol, 2020, p.8).

Criptografía Asimétrica o de Clave Pública. En términos generales, la criptografía permite cifrar un mensaje a través de un algoritmo con clave de cifrado, para evitar que pueda ser leído por cualquier persona. Solo aquella persona que disponga de la clave de descifrado podrá acceder al contenido original del mensaje.

De esta forma, la criptografía consiste en una ciencia que permite asegurar la comunicación entre las partes evitando el acceso a personas externas. Tradicionalmente, la criptografía utilizada era la denominada criptografía simétrica o de clave única, en la que se utiliza la misma clave para cifrar una información y para descifrarla. Esto es, Alice desea comunicarle a Bob un mensaje de forma privada, por lo que cifrará el mensaje empleando una clave. Para poder conocer el contenido del mensaje, Bob tendrá que utilizar la misma clave que empleó Alice para descifrarlo, por lo que Alice debería compartir con Bob dicha clave.

De ese modo, aunque este tipo de criptografía es muy rápida, pone en peligro la confidencialidad de la información compartida. Al ser necesario compartir la clave entre las partes, la comunicación podría ser interceptada por personas externas que se hicieran con la clave para descifrar el mensaje y conocer el contenido (Conesa, 2019). Pero este no es el único inconveniente. Si más de una persona interviene en el envío del mensaje, no se podría conocer con exactitud la titularidad del autor del mensaje. Esto es, si además de Alice y Bob también comparten la clave Carol y Dave, cada uno de ellos podrá conocer el contenido del mensaje recibido por alguno de los cuatro participantes, pero no podrá conocer cuál de ellos lo ha enviado (González-Meneses, 2019).

Todos estos inconvenientes impulsaron la creación y utilización de otro tipo de criptografía conocida como criptografía asimétrica o de clave pública[63], que dispone de dos claves una de carácter público y otra de carácter privado. La clave pública consiste en una cadena alfanumérica que al ser de carácter público puede ser compartida con cualquier usuario al que se desee. Es comparable con el número de la cuenta bancaria, que puede conocerse por otras personas sin el riesgo de que esto pudiera suponer la apropiación de los fondos. La clave privada también consiste en una cadena alfanumérica, pero en este caso, si se aplica al sistema Bitcoin, sería aquella que da acceso a los fondos de la cartera de forma

[63] El proceso de desarrollo de la criptografía asimétrica hasta el nivel al que la conocemos hoy día no fue fácil. Comenzando por Whitfield Diffie y Martin Hellman con su trabajo "*Multiuser Cryptographic Techniques"*en el año 1976 en el que por primera vez exponían una visión de un posible sistema criptográfico de doble clave, pasando por Ralph Merkle con los conocidos como "Puzzles de Merkle" hasta el paso definitivo con Ronald Rivest y sus colaboradores Adi Shamir y Leonard Adleman en el año 1977 que plantearon este tipo de criptografía tal y como lo conocemos actualmente (González-Meneses, 2019)

que aquella persona que disponga de ella también podrá disponer de los bitcoins correspondientes.

La diferencia con la criptografía simétrica es que en este tipo de criptografía no se dispone de una única clave que se utilice para cifrar y descifrar el mensaje, sino que se dispone de dos claves, una que se utilizará para cifrar y la otra para descifrar. Ambas claves se relación inequívoca y matemáticamente[64], de forma que a partir de la clave privada pueden generarse claves públicas que estén vinculadas. Sin embargo, no sería posible realizar esta acción en sentido contrario, es decir, a partir de la clave pública no es posible obtener la clave privada correspondiente. El único método posible en la actualidad para ello sería "usando la fuerza bruta" o en otras palabras, con el método de prueba y error (Ponce de León, 2018), lo que resulta prácticamente imposible[65].

Según la forma en la que se utilicen las claves pública y privada se pueden señalar dos propósitos para la criptografía asimétrica. Por un lado, el de mantener la seguridad y confidencialidad de un mensaje a través de Internet. Para ello, de la forma habitualmente conocida, si Alice quiere enviarle un mensaje a Bob de forma confidencial, tomaría la clave pública de Bob para cifrar el mensaje, que no tiene por qué ser privada y solo Bob podría conocer el contenido del mensaje descifrándolo con su clave privada. Por otro lado, este tipo de criptografía también podría servir como una muestra de identidad, es decir, para demostrar que el contenido de un mensaje corresponde a una persona determinada. Para ello, la persona cifraría el mensaje empleando su clave privada, de forma que cualquier persona que desee conocer la identidad del mensaje podría emplear esa misma clave pública, que es conocida, para conocer el contenido del mensaje. Esta muestra de identidad viene dada por la relación inequívoca entre la clave pública y la clave privada, de forma que la persona que escribió el mensaje y lo cifró con su clave privada tiene que ser inevitablemente la que se relaciona con la clave pública asociada a esta[66].

---

[64] La utilización de esta técnica de firma digital en el contexto de la *Blockchain* tiene tres propiedades (Ponce de León, 2018, p. 45): 1)Confidencialidad, un usuario puede utilizar su clave pública para cifrar un mensaje que únicamente puede ser descifrado utilizando su clave privada o secreta que se corresponde inequívocamente con la anterior; 2)No repudio, no se puede revocar la autoría de un mensaje una vez ha sido firmado con la clave secreta; 3)La verificación de un mensaje firmado implica que el mensaje ha llegado íntegro al receptor quedando invalidado ante cualquier cambio en el mensaje o en la firma.

[65] La utilización de este tipo de criptografía de dos claves permite el desarrollo de lo que M. González-Meneses (2019) llama como comunicación segura en una situación de cero-conocimiento. Es decir, entre aquellas partes que se consideran desconocidas, con este método

[66] Ante esto, podría surgir la duda de si la clave pública que se relaciona con la clave privada que efectivamente pertenece a la persona que escribió y cifró el mensaje. Esto es, si Bob escribe un mensaje y lo cifra usando su clave privada, cuando Alice lo descifre usando la clave pública, cómo sabría que esta clave pública pertenece efectivamente a Bob.

Para asegurar que la clave empleada se corresponde con una identidad en particular, sería necesaria la intervención de una tercera parte que pudiera asegurar esta correspondencia. Este procedimiento se podría realizar de dos formas. La primera consiste en un sistema descentralizado *peer-to-peer* en el que la red confirma las claves de otros, constituyendo una red de reconocimiento. La segunda consiste en un sistema centralizado, conocido como *PKI* (*Public Key Infraestructure*) en inglés, en el que un sujeto de forma profesional es el encargado de certificar las claves públicas[67] (González-Meneses, 2019). Sin embargo, sin extenderse en profundidad en esta cuestión, lo interesante en este caso es el hecho de que, pese a la base matemática de la criptografía asimétrica, la correspondencia entre las claves y la identidad de una persona no podrá realizarse de forma matemática sino que se dependerá del testimonio o certificación de un tercero en confianza (González-Meneses, 2019).

La criptografía de clave asimétrica es relevante en este caso porque se utiliza en la Bitcoin *Blockchain* en la realización de transacciones por parte de los usuarios del sistema. Aunque es un sistema que ya existía con otro tipo de aplicaciones, en este caso la novedad es que permite la identificación de las partes que desean ejecutar la transacción de bitcoins sin la necesidad de proporcionar ningún tipo de documento personal, ni entrevistas o similares. La creación de estas claves también se realiza de forma privada o anónima, a través de un algoritmo que se conoce por las siglas ECDSA (*Elliptic Curve Digital Signature Algorithm*). El sistema Bitcoin no dispone de ningún registro en el que se relacione una clave pública con la identidad de una persona determinada ya que lo importante es que una persona reciba los bitcoins de una transacción y disponga de la clave privada necesaria para poder acceder a estos. Para conseguir una mayor protección para la identidad del usuario, también es posible (y recomendable) crear más de una clave pública a través de la clave privada de la que se dispone.

El aseguramiento de la clave privada es de especial relevancia, ya que es la que da acceso a los fondos Bitcoin de la cartera en cuestión. Esto convierte a los saldos con esta criptomoneda en incoercibles, inembargables e irreivindicables (González-Meneses, 2019, p. 97). Esto es, ninguna persona ni autoridad externa, podrían obtener por la fuerza los fondos

[67] En este caso el papel del sujeto es doble: como autoridad de registro y como autoridad de certificación. La primera consiste en que se identifica a la persona a través de una entrevista u otro tipo de comparecencia personal, cotejando su identidad con un documento oficial, de esta forma, si usa las dos claves como firma digital, vincula la persona a una clave pública. A través de su papel como autoridad de certificación, el sujeto manteniene un registro accesible *online* de los certificados vigentes para que cualquiera pueda comprobar la identidad de cualquier clave pública (González-Meneses, 2019).

de una cuenta Bitcoin si no se dispone de la clave privada que les da acceso. La descentralización de la red no facilita el acceso a los fondos, ya que la ausencia de una figura central que ejerza el control sobre el sistema impide que autoridades u otras partes que lo necesiten se puedan dirigir a esta para obtener las claves privadas de las cuentas que deseen. Tampoco tendría mucho éxito coaccionar al usuario de la cartera para que proporcionara esta clave, porque además podría alegar que la ha perdido o que no la recuerda. Así, a pesar de cualquier intervención que se desee, el único propietario de los fondos siempre será la persona que disponga de la clave privada, hasta que no establezca esta lo contrario[68]. El propietario de los fondos obtendría de esta forma una seguridad mucho mayor que con el depósito de estos en una cuenta bancaria, siempre que mantenga a salvo el anonimato de la clave privada que da acceso a estos.

Identidad Digital: Algoritmo o Función *Hash*. Con el desarrollo de la *Blockchain* se popularizan de nuevo los términos "identidad digital". La supresión de la figura del tercero en confianza supuso el desarrollo de nuevos métodos que permitieran realizar las funciones que anteriormente le correspondían a esta figura. De forma general, en sistemas de pago centralizados el intermediario supervisaba el correcto desarrollo de las transacciones y el pago efectivo de las partes. De entre todas las tareas que incluyen estas actividades, resulta de importancia asegurar la identidad de las partes implicadas en la transacción, así como la integridad de la información transmitida.

En el sistema de pago ideado por Satoshi Nakamoto, se consideraron varias tecnologías que en su conjunto permitían asumir las funciones que tradicionalmente eran asignadas a los terceros en confianza. Una de estas tecnologías que han adquirido un papel clave en el funcionamiento del sistema Bitcoin son las funciones o algoritmos *hash* y los *hashes* resultantes.

De esta forma, cuando utiliza el término *hash* se está haciendo referencia a dos conceptos. Por un lado, se utiliza el término *hash* para hablar de la función criptográfica que, aplicada sobre un archivo, entrada de texto u otro tipo de ítem de longitud variable da como

[68] En este punto se hace una aclaración con respecto a las casas de cambio o *exchanges* y es que el depósito de los fondos de criptomonedas en una de sus cuentas sí que permitiría el acceso a las autoridades en el caso de que fuera necesario. La creación de una cuenta en una casa de cambio supone la identificación del usuario y el depósito de sus fondos en sus servidores, por lo que su disponibilidad ya no dependería del conocimiento o no de la clave privada y sería posible realizar una intervención.

resultado una secuencia de longitud fija y de numeración hexadecimal[69]. Por otro lado, se utiliza la para hacer referencia al resultado de la aplicación de la función hash, es decir, a la secuencia alfanumérica de longitud fija. Un ejemplo de ello es el número *hash*: 0000b9ad057ed4e50cfd3426b687192d34dca1201e2117523630b5903a59ebd6[70].

La introducción de esta tecnología en la *Blockchain* ha permitido la consecución de varios objetivos en el correcto desarrollo del sistema Bitcoin. De forma general, estos están relacionados con la integridad de la información y la identidad de las partes.

En primer lugar, la utilización de algoritmos o funciones hash en la *Blockchain* permite asegurar la integridad de la información, es decir, que la información no ha sido modificada desde que fue generada por la persona que disponía de la clave privada. Esto es, una vez se crea la información que contiene el bloque, se aplicará la función *hash* que tendrá como resultado el *hash* correspondiente. Cualquier variación en la información contenida en ese bloque, aunque solo fuera en un *bit*, alteraría el hash generado, obteniendo un *hash* diferente[71]. Esto supone una prueba de integridad del archivo de forma que, una vez se ha creado el *hash* correspondiente para una información y se da a conocer públicamente, cualquier persona que desee comprobar la integridad de esa información podría volver a calcular su *hash*. Si ambos *hashes*, el proporcionado y el nuevamente creado coinciden, significa que la información no ha sido alterada ni modificada[72]. No obstante, esta correspondencia del *hash* con la información no supone la existencia de reversibilidad, es decir, los *hashes* no son reversibles, sino unidireccionales, aunque se pueda conocer de forma pública el *hash* creado a partir de un archivo o información, no es posible obtener el archivo original a partir del *hash* generado. Se habla en este caso de una huella determinista, única

[69] El sistema hexadecimal o numérico hexadecimal es aquel en el que se forma un número empleando 16 dígitos, los dígitos numéricos del 0 al 9 (0, 1, 2, 3, 4, 5, 6, 7, 8, 9) y las primeras seis letras del alfabeto latino (a, b, c, d, e, f).

[70] Este número *hash* se ha obtenido introduciendo el texto "Esta es una investigación sobre criptomonedas y crimen" en un bloque de una demo de la Blockchain. Obtenido de https://andersbrownworth.com/blockchain/block

[71] Es casi imposible que dos archivos diferentes arrojen un mismo *hash* ("colisión de *hashes*").

[72] Al contrario de lo que se puede pensar, el *hash* no sirve para asegurar la información ni el contenido del archivo, es decir, no evita su desaparición o eliminación, tampoco es una seña de identidad, no se puede saber quién lo elaboró en su momento. Únicamente permite garantizar la integridad de un archivo u otro tipo de información incluso sin la necesidad de revelar el contenido original del archivo. Por ejemplo, M. González-Meneses (2019) pone el ejemplo de las contraseñas empleadas por los usuarios de un banco determinado, para las que señala que el banco no almacena todas estas contraseñas, sino que le es suficiente con almacenar los *hashes* generados para estas contraseñas y comprobar su veracidad o correspondencia de la información con el *hash* cuando sea necesario.

para un mismo binario, siendo probabilísticamente imposible encontrar dos huellas iguales, ni recrear un binario a partir de la huella (García Meras, 2021).

En segundo lugar, el *hash* actúa como la huella digital de una información con la que se corresponde inequívocamente. De la misma forma que sucedía anteriormente con la huella digital en el Documento Nacional de Identidad o con los dígitos de control en la cuenta bancaria, en la *Blockchain* se utiliza una huella digital criptográfica que actúa como identificador único de un binario (cualquier tipo de archivo binario: foto, archivos, etc., susceptibles de tener una huella), que lo hacen único (García Meras, 2021). Una vez creado un bloque, se aplica la función *hash* a la información que este contiene, creando un *hash* por el que se puede identificar la información. Este *hash* será incluido en el siguiente bloque de la cadena, que una vez completo creará otro *hash* a partir de la nueva información. Así, en cada bloque está incluido el *hash* del bloque anterior, lo que se conoce como "huellas encadenadas". Esto consiste en que si, por ejemplo, tenemos tres datos, en primer lugar se calcula la huella digital del "dato 1" y la huella digital del "dato 2" se calculará a partir de la huella del "dato 1" y a su vez, la huella del "dato 3" se calculará a partir de la huella del "dato 2", que a su vez ha tenido en cuenta previamente la huella del "dato 1" (García Meras, 2021). Esto en la *Blockchain* significa que cada *hash* actúa como huella digital o identificador del bloque anterior al que se unirá un bloque posterior, de forma que cada bloque está conectado al bloque anterior, considerado como su *parent block* o bloque padre, cuyo *hash* se incluye en un campo en la cabecera del *hash* del bloque siguiente o bloque hijo, formando una cadena de *hashes* desde el primer bloque que se creó o "bloque génesis" (Antonopoulos, 2015).

De esta forma, coincidiendo con la integridad de la información que se comentaba anteriormente, este sistema permite a su vez garantizar la inmutabilidad de la Blockchain. Cualquier modificación en un bloque alterará el *hash* de este, lo que requerirá de un cambio en el *hash* "hijo" y así sucesivamente[73]. Si, por ejemplo, se modificara la información del bloque 2, se modificaría su *hash*, que está incluido en el bloque 3. Esta modificación en el bloque 3 supondría a su vez la alteración del *hash* que se había creado inicialmente para el bloque 3. De esta forma, las posibilidades de introducir modificaciones en uno de los bloques de la cadena se reducirían a medida que se siguen creando nuevas generaciones de este bloque, ya que realizar un cambio en este supondría realizar un nuevo cálculo en los bloques

[73] Volviendo al ejemplo de *hash* que se ha presentado al comienzo del apartado si, por ejemplo, se modifica el mensaje añadiendo un signo de exclamación, esto es "¡Esta es una investigación sobre criptomonedas y crimen!", el número hash cambiaría por completo, aunque solo se ha añadido un carácter nuevo, obteniendo 0000ffc848860ed1224f4e5c192a0e67bc5e77d0c2245d6470a47444fa06e600

posteriores, lo que supone en la actualidad un esfuerzo insostenible computacionalmente (Antonopoulos, 2015).

Por último, el número *hash*, en su función de identificador digital de los bloques, permitiría gestionar y referenciar el contenido de una forma más fácil y sencilla. Al crear un *hash*, se está creando un código alfanumérico con un número de caracteres fijo a partir de un archivo o información de tamaño variable. Esto permite identificar fácilmente ese contenido de una forma más sencilla que si se gestionara la información original. Esta tecnología, ha resultado ser de gran utilidad en la *Blockchain*, ya que no ha sido desarrollada para incluir una gran cantidad de información en las transacciones, sino que se trabaja con datos ubicados fuera de la cadena de bloques que se referencian a través del identificador digital (García Meras, 2021). De esta forma, se permitiría por un lado identificar cualquiera de los bloques que pertenecen a la cadena y por otro, enlazarlos de forma cronológica e inmutable, garantizando su trazabilidad a través de la cadena[74].

En definitiva, se pueden señalar según P. J. Ponce de León (2018, p. 42) cuatro propiedades de los números *hash*: 1) no es factible recuperar la información a partir de la cual se generó un *hash*; 2) si la información se modifica aunque sea mínimamente, este *hash* se cambiará y no es posible establecer ninguna relación entre ellos; 3) No hay una mayor probabilidad de obtener un *hash* en concreto, la probabilidad es la misma en todos los números *hash*; 4) Es poco costoso crear un *hash* a partir de una información determinada, al igual que la comprobación de su correspondencia.

Aunque se han hecho conocidos en el entorno de las criptomonedas, los algoritmos *hash* ya eran utilizados anteriormente, siendo los más conocidos el SHA-1 y el MD5[75]. La estructura resultante de estos números suele tener una longitud que es potencia de 2. En el caso del sistema Bitcoin, el algoritmo *hash* criptográfico utilizado es el SHA-256, que crea números *hash* de 256 bits[76], lo que quiere decir que existen 2^{256} posibles números *hash* de 256 *bits* (Ponce de León, 2018).

[74] Junto con los *hashes*, también otros elementos de la *Blockchain* permiten asegurar la transparencia de los registros, como son las marcas de tiempo.
[75] Debido a la diferencia de los *hashes* según se utiliza un algoritmo de *hashing* u otro, es necesario que el cotejo de *hashes* se realice aplicando el mismo algoritmo que se utilizó en un primer momento para crear el *hash* que se está cotejando.
[76] 1 *bit* corresponde a 0,125 *bytes*, de forma que, en este caso, 256 *bits* se corresponden con 32 *bytes*.

Prueba de Trabajo (*Proof-of-Work*). La eliminación de la figura del intermediario requería de una solución que pudiera "cubrir" las funciones realizadas por este. La verificación de las transacciones era una de sus tareas clave, vigilando que no aparecieran problemas como el doble pago, empleando dos veces una misma moneda en diferentes transacciones o la realización de transacciones fraudulentas. Para encargarse de estas funciones sin la necesidad de intermediarios, Satoshi Nakamoto implementó el sistema de prueba de trabajo (*proof of work)* (Nakamoto, 2008).

La Prueba de trabajo o *Proof of Work* (PoW) consiste en una prueba criptográfica cuya resolución permitirá determinar el bloque que se incorporará a la *Blockchain.* El bloque que será seleccionado para formar parte de la cadena de bloques será el que corresponda al nodo ganador de la prueba de trabajo[77,78].

Esta prueba consiste en la resolución de un complejo problema matemático para el que se debe encontrar aquel *hash* que comience con un número determinado de ceros. Para ello, los mineros añadirán números al encabezamiento del bloque, de forma que se modifique el *hash* del bloque hasta conseguir el número deseado. Si a partir de ese número no se obtuviera el resultado deseado se pasaría al siguiente hasta encontrar el número a partir del que se pueda obtener el hash deseado. Este método se conoce como por la "fuerza bruta" o "no determinista".

El número que se debe encontrar para la resolución de la prueba de trabajo se conoce como *nonce*[79] y podrá estar formado por una cifra, un dígito o varios dígitos.

La prueba de trabajo será diferente para cada nodo, ya que, dado que el contenido de cada bloque es diferente, el *nonce* que se necesita buscar tendrá que ser también diferente[80].

---

[77] Para tomar esta decisión, el algoritmo o protocolo tiene que cumplir una serie de condiciones como que más de la mitad de los nodos de la red tiene que ser honestos, tiene que ser un nodo honesto el que propone el bloque y la decisión tomada tiene que ser acatada por todos los nodos (Ponce de León, 2018).

[78] La prueba de trabajo es un método de selección del bloque ganador que no se puede monopolizar, ya que mide la potencia de cómputo de los nodos. Para medir esta potencia de cómputo se plantea un puzle criptográfico que consiste en la búsqueda de un *nonce* para que el hash de la cabecera del bloque sea un número que esté dentro de un rango objetivo muy pequeño empleando el método de prueba y error (Ponce de León, 2018). Esta prueba de trabajo tiene tres propiedades importantes: 1) computacionalmente es muy costosa; 2) adapta la dificultad en función del poder de cálculo total de la red y 3) es sencillo verificar que es correcta, calculando el hash del bloque propuesto y compararlo con el objetivo (Ponce de León, 2018, p. 54)

[79] Etimológicamente, la palabra "*nonce*" está formada por la combinación de la palabra "*number*" y "*once*", la abreviatura de "*number used once*" y es que este tipo de números en informática son números de un solo uso u ocasión que se generan para un uso en específico, normalmente el de autentificación (González-Meneses, 2019).

[80] Esta prueba reajusta su dificultad también para que cada bloque tarde alrededor de diez minutos en ser confirmado e incluido a la red. Incrementará el número de ceros que debe contener el *hash* del bloque, incrementando la dificultad de encontrar un *nonce* que encaje (González-Meneses, 2019). Si fuera muy complicada esta prueba se reajustaría en el sentido contrario para poder respetar el promedio de los diez minutos de confirmación.

En este sentido se añade un cierto elemento de aleatoriedad, ya que, si todos los nodos tuvieran que buscar el mismo *nonce*, tendría mayor ventaja aquel minero con una mayor capacidad computacional [81].

La prueba de trabajo no sirve únicamente para decidir qué nodo añade su bloque a la cadena de bloques, sino que a su vez es una herramienta que asegura la cadena de bloques. Esto es posible porque cuando un nodo resuelve una prueba de trabajo, este bloque es enviado al resto de nodos que forma parte de la red, que comprobarán que el bloque cumple con los requisitos para ser incorporado a la cadena de bloques (verificación de las transacciones, disponibilidad de saldo y resolución de la prueba de trabajo).

Estructura y Contenido de la Cadena De Bloques

Se pueden establecer varios tipos de *Blockchain* según diversos criterios. Por un lado, atendiendo a quién puede ver la información de la transacción, la *Blockchain* podría ser seudonimizada (toda la red puede ver el valor de la transacción) o anonimizada (la información solo puede ser conocida por los intervinientes) (Torrero, 2021). Por otro lado, según quién puede acceder a la *Blockchain*, esta podría ser *permissioned* (permiso de alguna entidad para poder entrar a la red) o *permissionless* (cualquiera puede acceder descargando el *software* o código) (Torrero, 2021). Siguiendo estas clasificaciones, por ejemplo, las redes de Bitcoin y Ethereum serían seudonimizadas y *permissionless* y la de Zcash sería anonimizada y *permissionless* (Torrero, 2021).

En relación con los bloques que forman la *Blockchain, c*ada uno de los nodos mineros que conforman la red Bitcoin dispone de un bloque potencial candidato a formar parte finalmente de la *Blockchain*. En estos bloques, los mineros almacenan cada transacción según el orden en el que la reciben hasta completarlo. La estructuración del contenido de la *Blockchain* en bloques facilita el almacenamiento y la gestión de las transacciones realizadas, lo que permite obtener el registro de transacciones con carácter cronológico y ordenado. No obstante, aunque las transacciones son el elemento más característico del contenido de los bloques, no son el único elemento que se puede encontrar dentro de estos. De forma general,

[81] Pudiera suceder que dos nodos resuelvan la prueba de trabajo de forma casi simultánea y que al mismo tiempo envíen su bloque al resto de nodos de la red. En este caso, cada nodo confirmará el bloque que haya recibido y seguirá su actividad de minado empleando el *hash* de este bloque. Esto provocaría la aparición de una ramificación de la cadena de bloques, es decir, continuaría la cadena principal anterior y al mismo tiempo una pequeña cadena de forma paralela, lo que se conoce como *fork*, horquilla o bifurcación. La forma en la que se soluciona esta anomalía es, una vez se detecta la bifurcación por parte de los mineros, estos deciden continuar su actividad por la cadena más larga, que ha tenido un mayor número de apoyos y consenso durante más tiempo (González-Meneses, 2019).

la estructura de un bloque está compuesta por dos elementos principales. Por un lado, por las transacciones mencionadas anteriormente, agrupadas en una larga lista y que suponen la mayor parte del tamaño del bloque. Por otro lado, por una cabecera o encabezado de bloque que contiene elementos como una referencia al *hash* del bloque anterior, una marca de tiempo[82], un número aleatorio denominado "*nonce*"[83] y la raíz del "árbol de Merkle"[84]. Además, aunque de menor relevancia que los anteriores, también se puede encontrar otra información sobre el bloque como el número de confirmaciones, la altura de bloque, el minador, complejidad o dificultad de bloque[85], información de la versión, *bits*, peso, tamaño y la recompensa de bloque[86].

Aunque de forma general se puede decir que todos los bloques están formados por estos elementos, no es posible encontrar dos bloques con el mismo contenido. Todas las transacciones realizadas con Bitcoin se envían a todos los nodos de la red, no obstante, el orden en el que los nodos las reciben es diferente, lo que ocasiona que, aunque se almacenan casi de forma simultánea, el orden de registro por cada nodo es distinto. Además, habría que

[82] La marca de tiempo (*timestamp*, en inglés), indica el momento exacto en el que el bloque fue minado y validado. Supone una garantía más para evitar el doble pago, ya que a efectos de decidir qué transacción es válida, Nakamoto (2008) considera que es aquella que se ha realizado en primer lugar. El sello de tiempo determina por lo tanto qué transacción se realizó antes y por lo tanto aquella que es válida. Debido a que la red de nodos está descentralizada, la forma en la que se determina este momento es empleando la mediana de las marcas de tiempo de todos los nodos. Todos los nodos toman como referencia la misma franja horaria, la UTC-0 (hora local de Londres). Una vez se almacena este dato, cada nodo calcula el tiempo de desplazamiento entre la franja horaria UTC y la hora local. Este dato es utilizado en el proceso de minería, permite ajustar la dificultad de la minería estudiando cuánto tiempo ha sido necesario para extraer los bloques de un periodo y ajustando el parámetro de dificultad de la minería (bit2Me Academy, 2019). Este funcionamiento podría sugerir el riesgo de manipulación de este parámetro y modificación de la dificultad de minería, facilitando la creación de bloques (Ataque de Deformación del Tiempo o *Time Warp Attack*). No obstante, Satoshi Nakamoto tuvo este riesgo en cuenta y para ello estableció que solo fueran considerados aquellos bloques que están dentro del rango de tiempo del reloj interno de los bloques, solo se consideran las últimas transacciones (bit2Me Academy, 2019). Tomando un bloque como ejemplo, el sello de tiempo en el Bloque génesis es 2009-01-03 19:15 (Blockchain.com, 2021a).

[83] Contador utilizado por el algoritmo de prueba de trabajo (Antonopoulos, 2015). Como se ha mencionado en el apartado anterior, se trata de un número que se inserta en la cabecera de cada bloque con la finalidad de hacer que el *hash* de ese bloque cumpla ciertas propiedades (Ponce de León, 2018).

[84] En Bitcoin, un "Árbol Merkle" o "Árbol *hash* binario" es una estructura de datos que se utiliza para resumir todas las transacciones de un bloque, produciendo una huella digital general de todo el conjunto de transacciones (Antonopoulos, 2015). Esto permite identificar el conjunto de transacciones y verificar si una transacción se encuentra o no en un bloque sin necesidad de transmitir o almacenar el resto de la *Blockchain*. Este número se crea obteniendo el doble hash SHA-256 de cada una de las transacciones y se van agrupando de dos en dos para calcular el *hash* resultado de cada par, así hasta obtener un único *hash* que se sitúa en la raíz del árbol (Ponce de León, 2018). De esta forma, si se intenta modificar alguna de las transacciones se modificará este *hash*, alterando el bloque completo.

[85] La dificultad del bloque viene determinada por el número de ceros al comienzo del *hash* del bloque. Si la capacidad de cómputo ha sido elevada, la cantidad de ceros en este número también lo será (Torrero, 2021).

[86] Existen varios sitios web donde puede consultarse la información relativa a cualquier bloque de la *Blockchain*. A lo largo del desarrollo de este trabajo y para conocimiento del lector se ha utilizado el explorador de la página "Blockchain.com" https://www.blockchain.com/es?utm_campaign=expnav_logo.

considerar que, además de la transacción de emisión de criptomonedas hacia un usuario, también tiene lugar al mismo tiempo otra transacción en beneficio del nodo minero por el servicio realizado[87]. En cada bloque esta transacción será diferente, ya que cambiará la dirección Bitcoin del nodo ganador en cada uno de los minados.

De esta forma, el tamaño del bloque completo dependería del tamaño de cada uno de los elementos anteriores que lo conforman, aunque la larga lista de transacciones supone la mayor parte de su tamaño. El tamaño del encabezado del bloque es de 80 *bytes*, y la transacción promedia es de al menos 250 *bytes*, por lo que, si un bloque contiene de media más de 500 transacciones, el bloque completo con todas sus transacciones sería 1000 veces más grande que el encabezado del bloque (Antonopoulos, 2015).

Todos estos elementos no solo tienen su relevancia dentro del bloque del que forman parte, sino que a su vez influyen también en la formación de la estructura de cadena de la *Blockchain*. Como se mencionaba anteriormente, cada bloque incluye el número *hash* del bloque anterior y el *hash* del bloque en cuestión será a su vez incluido en el encabezado del bloque posterior. Esto permite el encadenamiento de los bloques, lo que supone a su vez un elemento clave para la identificación. El número *hash* permite a su vez situar el bloque en un lugar de la cadena de bloques que será inamovible, ya que no es posible realizar modificaciones en el *hash* sin afectar al resto de la cadena.

No obstante, el número *hash* no es el único indicador de la situación de un bloque dentro de la cadena. Si se accede a la información de un bloque se puede ver el identificador de bloque, también conocido como "altura de bloque" [88], que indica la posición que ocupa un bloque con respecto al resto de bloques de la cadena (Antonopoulos, 2015). Si se considera la *Blockchain* como una estructura lineal situada en vertical, el primer bloque creado o bloque génesis estaría situado en la base de la cadena, con un identificador de bloque o altura de

[87]Esta transacción es realizada para cubrir los costes de minería y puede suponer a su vez un incentivo a los mineros para reducir el tiempo de espera para la verificación de esta. Es decir, en el momento en el que los mineros eligen las transacciones que verifican y almacenan en su bloque, pueden priorizar aquellas transacciones para las que se ofrece un incentivo mayor, por lo que serían incluidas más rápidamente en el bloque y por lo tanto el tiempo de espera sería menor.

[88]No obstante, con respecto a esto, Antonopoulos (2015) expone que a diferencia del *hash*¸ la altura de bloque no es un identificadora único, esto es, mientras que el *hash* de un bloque siempre identifica un solo bloque de forma única, la altura de bloque puede identificar a más de un bloque que están compitiendo en ese momento por una sola posición en la cadena de bloques.

número 0[89]. A partir de este, el identificador iría adquiriendo un valor mayor conforme se fueran añadiendo bloques sobre bloque 0.

Aplicaciones y Tecnologías Basadas en la Blockchain

Aunque la tecnología de la *Blockchain* ha alcanzado una gran popularidad desde su creación para el sistema Bitcoin, sus bondades no han quedado únicamente reservadas para el ámbito de las criptomonedas.

El uso de la tecnología *Blockchain* se ha considerado de gran utilidad en el desarrollo de procesos, por su funcionamiento de bloques encadenados, cuando es necesario desarrollar una acción tras otra. Aunque, existen otras soluciones más rápidas, baratas y sencillas con las que se podrían resolver esos mismos problemas como las firmas electrónicas, por ejemplo (García Meras, 2021). No obstante, si bien es cierto que puede ser considerada como una solución ineficiente y lenta en muchos casos, sobre todo comparada con las soluciones centralizadas, la eliminación de terceras partes o intermediarios en el desarrollo de un proceso supuso una revolución que ha superado a sus inconvenientes en la decisión de implementarla (Ammous, 2018).

De esta forma, la cadena de bloques se ha posicionado en las últimas décadas como una innovación atractiva para el desarrollo de aquellos procedimientos que requerían de registros irreversibles e inmutables, por lo que se ha previsto su utilización en muchos ámbitos diferentes.

[89]El bloque de altura 0 o bloque génesis es el primer bloque de la *Blockchain* y fue minado el 3 de enero de 2009. Su *hash* es 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f y en la actualidad tiene 677.029 confirmaciones en la Bitcoin *Blockchain* https://www.blockchain.com/btc/block/0

Aplicaciones y Casos de Uso. Podrían establecerse dos divisiones para las aplicaciones de la tecnología *Blockchain*. Por un lado, aquellos ámbitos de negocio en los que se ha implementado esta tecnología debido a la importancia que ha adquirido su protocolo de consenso. Este es el caso de la industria alimentaria, en la que se persigue conseguir la máxima transparencia posible en la cadena de producción para mantener la confianza de los consumidores en la seguridad alimentaria de sus productos. Por ejemplo, en la cadena multinacional "Carrefour"[90], que colaboraron con la empresa "IBM" para desarrollar una tecnología *Blockchain* que consiguiera una mayor transparencia en el proceso que va desde la producción de los alimentos hasta su consumo (IBM, 2021c).

Al mismo tiempo, empresas de relevancia como el banco "Santander", la marca de electrodomésticos "Bosch", la cadena de automóviles "Ford" o la empresa de tecnología "IBM", conscientes de la disrupción tecnológica que ha supuesto la aparición y utilización de la *Blockchain* en multitud de ámbitos la han considerado y la están utilizando para innovar en muchos de sus procesos.

El Banco "Santander", apuesta por esta tecnología por tratarse de una alternativa de pago global, transparente, de bajo coste y más segura frente a fraudes y manipulaciones gracias al uso de la encriptación y codificación (Banco Santander, 2019). Para la realización de las transferencias internacionales ha desarrollado el servicio "One Pay FX" basado en la tecnología de la *Blockchain* y que permite el envío el envío de dinero a otros bancos Santander de forma rápida y con bajos costes (Banco Santander, 2021). Pero no únicamente la utiliza para la realización de las transacciones, sino que también la ha implementado en otros servicios como el almacenamiento y transferencia de documentos e información. Cabe señalar el bono bancario de 20 millones de dólares que ha desarrollado en la *Blockchain* pública de Ethereum, que se mantendrá en esta tecnología hasta su vencimiento[91] y que les ha permitido *tokenizarlo* y registrarlo de forma permisionada en la *Blockchain* (Banco Santander, 2019).

[90] Tras la pérdida de confianza del consumidor a partir de una serie de escándalos sanitarios, Carrefour decidió implantar la tecnología *Blockchain* inicialmente empleada en la red Bitcoin. Adoptaron la tecnología "Ethereum", que era la tecnología más estable en aquel momento y de esta forma, el "*Blockchain* alimentario" se hace transparente la trazabilidad de los alimentos. Esto se consigue registrando los datos de cada alimento -en un principio aves- desde su incubación hasta su distribución, siendo todos estos datos accesibles y públicos de la misma forma que para las transacciones con bitcoins (Carrefour, 2018).

[91] Los bonos bancarios son un tipo de contrato de préstamo habitualmente solicitado por empresas o gobiernos u otras entidades que se emiten a los inversores con el propósito de recaudar fondos para poder financiarse. Son emitidos por un tiempo específico y una vez finalizado el inversor recibirá la cantidad prestada más una serie de intereses conocidos como cupones de bono. Este tipo de préstamo en este caso adquiere el nombre de "deuda pública" en el caso de los gobiernos y "deuda corporativa" en el caso de las empresas.

La empresa IBM también ha apostado por la tecnología *Blockchain* desarrollando servicios que permiten a otras empresas y entidades implementar esta tecnología en sus actividades profesionales. Permiten unirse a una de sus redes existentes, crear sus propias soluciones según las necesidades que presenten, unirse a la propia empresa para crear una solución que se adecue a sus necesidades de forma conjunta, o bien recibir asesoramiento de otros expertos en esta tecnología. Los aspectos de la *Blockchain* que han sido valorados por las empresas para su implementación son aquellos que también le daban valor en el sistema de pago Bitcoin: validar las transacciones y compartir los registros entre todos los participantes de forma transparente y pública, pero con imposibilidad de realizar modificaciones una vez confirmados, lo que le dota de una elevada seguridad (IBM, 2021c). De esta forma, desde esta empresa se ha aplicado esta tecnología en la gestión de los contenedores de transporte en los barcos con *Tradelens* (IBM MediaCenter, 2021b) conectando a los consumidores con los productores de café con *Farmer Connect* e *IBM Trust* (IBM MediaCenter, 2021a) [92], en la gestión y distribución de entradas digitales a través de *True Tickets* [93] (Zarracina, 2020) y en las cadenas de suministro de los automóviles con *XCEED*[94] (Stelzer, 2021).

Pero las aplicaciones de esta tecnología no solo han tenido lugar a nivel de grandes multinacionales, también se ha visto su utilización en el entorno privado, como, por ejemplo, en la formalización de un matrimonio, estableciendo determinadas condiciones entre las partes si el matrimonio llegara a extinguirse[95]. También se ha considerado su implementación en la cadena de custodia de evidencias compartiendo datos entre cuerpos policiales y

[92] Esta tecnología ofrece una garantía de trazabilidad de su procedencia y prueba de sostenibilidad si se diera el caso. Permiten conocer más acerca de las granjas de producción de café e incluso contribuir con una aportación económica (IBM MediaCenter, 2021a)

[93] De esta forma, el Centro "Adrienne Arsht" para las Artes escénicas, pionero en la utilización de la tecnología *Blockchain*, consciente de la situación COVID, quiere garantizar la emisión segura de entradas sin contacto, habilitada por la IBM *Blockchain Platform.* Además, también garantiza la seguridad de la compra mediante cifrado, la gestión de derechos a través de contratos inteligentes y la protección contra el fraude y reventa garantizando la trazabilidad, autenticidad y el precio de las entradas vendidas (Zarracina, 2020).

[94] Consiste en un proyecto de *Blockchain* en la industria del automóvil que permite certificar el cumplimiento de los criterios de calidad de los componentes de un vehículo asegurando la trazabilidad en el ecosistema completo de desarrollo del automóvil, todo ello basado en la tecnología *Blockchain* de IBM. Asegura que durante este proceso, proveedores y fabricantes de automóviles compartan la información de cumplimiento de cada etapa del proceso a través de una red confiable, de forma automática y precisa sin dedicar tiempo adicional ocupándose de la documentación necesaria en cada caso (Stelzer, 2021).

[95] El matrimonio se celebró entre dos empleados de la casa de cambio "Coinbase", Rebecca Rose y Peter Kacherginsky, que en este caso emplearon la *Blockchain* de Ethereum para formalizar su enlace. Para ello, crearon un contrato inteligente en Ethereum al que dieron el nombre de "Tabaat" (anillo en hebreo) que costó alrededor de 500 dólares. A partir de este se emitió un par de anillos *tokenizados* por el contrato que fueron enviados en forma de transacción a cada uno de los prometidos y que consistían en una pequeña animación de dos círculos que se fusionaban (Quarmby, 2021).

registrando sus actuaciones (García Meras, 2021). De este modo, se evitaría el riesgo de alteración o desaparición de evidencias durante el proceso, o en el caso de que esto sucediera, podría consultarse el momento exacto del proceso en el que la desaparición o la alteración de la evidencia pudieron llegar a suceder, facilitando su investigación. También, Universidades como la Carlos III de Madrid (UC3M) y la escuela de negocios ISDI están utilizando esta tecnología para la verificación de los títulos universitarios (Blázquez, 2019), de forma que los estudiantes puedan obtener su título oficial rápidamente reduciendo los trámites y siendo casi imposible la falsificación y manipulación de estos.

Tecnologías Basadas en la *Blockchain.* La aparición de la *Blockchain* supuso una nueva forma de concebir el valor en el entorno digital. Con esta nueva concepción de la confianza entre las partes sin intermediarios y el valor del proceso, surgieron nuevas tecnologías inspiradas en ese nuevo pensamiento. Fuera del ámbito de las criptomonedas, surgen tecnologías que permiten que cualquier asunto de valor pueda rastrearse y comercializarse a través de una *Blockchain*.

De esta forma, vuelve a tomar relevancia el término *token*. Anteriormente, un *token* suponía una representación de valor, bien de un objeto físico o de un servicio. Este era el caso del dinero empleado en eventos sociales como conciertos, en los que, en lugar de emplear dinero fiduciario como euros o dólares, se compran los denominados *tokens*, que sería el dinero utilizado dentro del recinto del concierto. En este caso, una unidad de *token* se corresponde con una unidad de la moneda local, de forma que no es necesario emplear este dinero en efectivo y se utilizarán estas fichas en su lugar.

Con la aparición de la tecnología *Blockchain* el término *token* ha vuelto a adquirir relevancia como una forma de representar valor mediante la *tokenización* o representación de un activo mediante un *token* o ficha digital a través del sistema *Blockchain*[96]. Los *tokens* consisten por tanto en un bien digital protegido por criptografía que tiene relación con un bien físico o digital (Ponce de León, 2018, p. 38).

Debido la incorporación de la tecnología *Blockchain*, los *tokens* comparten muchas de las características que podemos encontrar en una criptomoneda como Bitcoin. Esto permite a

[96] M. Gonzáles-Meneses (2019) expone que en materia de *tokenización*, nos encontramos con una gran inseguridad terminológica. Esto es, la palabra "*token*" tiene su origen en el inglés y significa ficha, vale, prueba, símbolo. Hablar de "*token* digital" se consideraría más preciso pero, aun así, este autor considera, que dado que se trata de una palabra en inglés y otra en castellano, lo lógico sería emplear ambas palabras en el mismo idioma. Así, propone la utilización del término "*cripto-token*" o "*crypto-token*", siendo la versión literal en español "cripto-ficha".

su vez evitar algunos de los problemas que pudieran surgir con los *tokens* tradicionalmente empleados utilizando técnicas que evitan la generación o multiplicación discrecional, así como la posibilidad de doble gasto. Todo ello sin necesidad de una autoridad, banquero o tercero de confianza que controle esta emisión a través de una contabilidad centralizada (González-Meneses, 2019, p. 141)

A partir de esta concepción del valor en el entorno digital con los *tokens*, aparecen los contratos digitales conocidos como "contratos inteligentes" o *Smart Contracts*. Consisten en una serie de reglas transaccionales que tienen su fundamento en la posibilidad que ofrece la tecnología *Blockchain* de programar la circulación de activos *tokenizados*.

Esta idea empezó a circular en los años noventa entre los círculos criptoanarquistas, en los que Nick Szabo, autor de "Bit Gold", creó dicho término. Sin embargo, no ha sido hasta el desarrollo de la plataforma Ethereum en la actualidad cuando ha sido posible el desarrollo de la idea. Por este motivo, se tratarán con un mayor detalle en el apartado relativo a la criptomoneda Ether.

Su desarrollo comienza con varias partes que desean establecer un acuerdo con una serie de condiciones de cumplimiento. Para evitar la necesidad de una tercera parte encargada de la supervisión y velando por el cumplimiento de las condiciones, la tecnología *Blockchain* permite trasladar las condiciones acordadas por las partes a un código. Durante la ejecución del contrato inteligente, si se comprueba que se cumplen las condiciones establecidas, se libera el pago acordado sin que ninguna de las partes tenga que intervenir. Si bien es cierto que no se requiere de terceras partes que aseguren el desarrollo del contrato, sí que existe la figura del "oráculo", que aporta información externa de utilidad en la comprobación de las condiciones establecidas en el contrato[97].

Teniendo en cuenta lo anterior, la creación de un contrato inteligente es posible gracias a dos procesos, la *tokenización* y la virtualización (Torrero, 2021). El primero consiste en asociar un activo con un código, es decir, se asocia un *token* al objeto. La virtualización consiste en la representación en *software* de objetos reales para que puedan ser operados de forma automática. Al *token* se le asocia un *smart contract*, que tiene ciertas operaciones que

[97]En relación con el papel que juega la figura del "oráculo" en la cadena de bloques, J.A Torrero (2021) señala que sería un punto importante para atacar en el caso de que se quiera afectar a la cadena de bloques de algún modo, de forma que es muy importante que esta información que procede de terceros y que será determinante para liberar los fondos, esté asegurada y certificada. Si se introdujera información falsa a la cadena a través de esta figura, los *smart contracts* empezarían desarrollar acciones no previstas desde los acuerdos establecidos en el contrato inicial.

se pueden realizar sobre el objeto virtual y sobre el objeto físico (p.ej. Comprar o vender una casa o abrir y cerrar una casa).

En este sentido, Torrero (2021) utiliza un ejemplo muy ilustrativo para comprender los conceptos anteriores. Así, plantea la situación en la que un granjero quiere asegurar su cosecha frente al riesgo de incendio. Un miembro de una agencia de seguros y el granjero establecen un acuerdo o contrato con unas condiciones determinadas, que se codificará en *Smart contract.* La aseguradora aporta fondos en caso de que suceda la situación establecida en el contrato. Para comprobar que la cosecha está siendo expuesta a altas temperaturas será necesaria la figura del "Oráculo", que registrará esta situación. En el caso de que la cosecha esté expuesta de manera continua a altas temperaturas, de acuerdo con lo establecido en el contrato, se liberarán los fondos aportados por la agencia de seguros que serán recibidos por el granjero.

A partir de este concepto han aparecido otros términos como las aplicaciones descentralizadas o distribuidas (DApps) o las DAOs o *Distributed Autonomous Organization,* que permite la organización de una empresa. No obstante, dichos términos serán ampliados en el apartado posterior dedicado a la criptomoneda Ether.

Capítulo 3. El Ecosistema de la Criptomoneda Bitcoin

El ecosistema de la criptomoneda Bitcoin está formado por todos aquellos elementos que se relacionan entre sí y que pertenecen al sistema Bitcoin. Estos son los usuarios, las transacciones, las carteras o billeteras y las casas de cambio o *exchanges.*

El objetivo de este apartado será mostrar el funcionamiento y características de los elementos que pertenecen a este ecosistema de forma que, se pueda crear una imagen general del sistema Bitcoin y entender mejor su funcionamiento.

Los Usuarios de Bitcoin o Nodos. Los Nodos Mineros.

Se denomina "nodo" a todo aquel usuario que desee formar parte de la red Bitcoin y que decida unirse a esta a través de la descarga e instalación del *software* "Bitcoin Core". Una vez los nodos están conectados, conforman la red de Bitcoin que le otorga su carácter descentralizado, de forma que todos los nodos operan de la misma forma sin niveles ni jerarquías (bit2me Academy, 2020a).

Una vez conectados, puede haber varios tipos de nodos según las distintas funciones de las que se hagan cargo y el papel que desempeñen. De esta forma, se pueden encontrar: nodos completos (*full node*), supernodos, nodos de minería y nodos ligeros (*light node*). De acuerdo con el objetivo de este trabajo, aunque serán mencionados todos los nodos, se tratarán de una forma más detallada los nodos mineros.

Nodos Completos (Full Node) y Nodos Ligeros (Light Node)

Los nodos completos son los encargados de las tareas de gestión y almacenamiento de la cadena de bloques. Por el contrario, los nodos ligeros son los que se encargan únicamente de verificar la validez de las transacciones, emiten transacciones y consultan el estado de la cadena de bloques realizando consultas a los nodos completos, no se encargan de almacenar la cadena de bloques ni crear nuevos bloques (Ponce de León, 2018).

En el caso de las criptodivisas, los usuarios interactuarán con la red a través del monedero o *wallet*, que es un nodo (completo o ligero) que además de lo anterior permite definir y gestionar direcciones de usuario y operar con la criptomoneda (Ponce de León, 2018).

Nodos Mineros

Si los nodos completos se encargan de la creación de bloques se conocerán como nodos mineros o simplemente "mineros" (*miners*, en inglés), que serán los que desarrollan la actividad de minería.

Los mineros son las personas encargadas de procesar la transacción realizada y verificarla para que pueda almacenarse en la cadena de bloques o *Blockchain*. De esta forma, mediante esta red de nodos Nakamoto instauró un método para que las transacciones fueran comprobadas y se aseguraran de forma democrática, evitando el doble pago o la ausencia de transacción sin tener que confiar o depender de entidades bancarias que se encarguen de esta tarea (Nakamoto, 2008).

Se denomina minería al proceso de creación de criptomonedas que tuvo su origen con Bitcoin y que se ha ido adaptando al resto de criptomonedas que han aparecido posteriormente. En este proceso, los mineros son los nodos encargados de la verificación y confirmación de las transacciones que se almacenan en los bloques de la Blockchain. De forma general, este consiste en que el nodo minero recoge cada una de las transacciones de bitcoins que se emiten, las valida mediante la verificación de la autenticidad de las firmas electrónicas y la comprobación de la disponibilidad de saldo del firmante y las almacena en un bloque (González-Meneses, 2019).

De forma detallada, este proceso se puede describir de la siguiente forma. En primer lugar, un usuario de la red Bitcoin emite una orden de transacción, que será recibida por todos los nodos mineros de la red. La información recibida que les permitirá verificar la transacción incluye la cantidad de monedas que se desean enviar, la firma digital del usuario que desea enviarlas, así como una o varias transacciones realizadas por este usuario en el pasado para demostrar que cuenta con fondos para realizar la nueva transacción. Una vez los nodos verifican la transacción, cada uno de ellos la almacena en un bloque, que será un posible candidato para formar parte de la *Blockchain*. La forma en la que se decide el bloque que formará parte de la cadena, será a través de la resolución de complejos problemas criptográficos en los que todos los mineros competirán por encontrar la solución. Esto es lo que se conoce como *Proof-of-Work* (PoW) o Prueba de trabajo que supondrá para cada nodo una elevada capacidad de procesamiento y de electricidad hasta encontrar la clave. El bloque del nodo que primero resuelva esta prueba será el que se una al resto de bloques en la *Blockchain*. La cadena de nodos más larga de la *Blockchain* será la que tenga un mayor esfuerzo de procesamiento invertido y, por tanto, la que represente a la mayoría de los nodos,

que aceptaron esta cadena a través de la PoW de forma que "una-CPU-un-voto" (Nakamoto, 2008).

En definitiva, el proceso de minado requiere de tres elementos: un *software* básico de minado (por ejemplo, "CGminer", "BFGminer" o "GUIMiner"), *hardware* especializado para minar (por ejemplo, "AntMiner", "Avalon" o "ASICMiner") un *mining pool* y una cartera Bitcoin. Se considera como *mining pool* a un grupo de participantes Bitcoin que trabajan juntos para resolver el problema de computación (Kethineni, Cao and Dodge, 2018, p.141-142).

Por todo ello, se denomina a los nodos que realizan este proceso como "mineros", ya que de la misma forma que en la actividad de extracción de minerales en las minas, en este sistema los mineros invierten sus recursos trabajando en las pruebas criptográficas propuestas para obtener bienes de valor.

No obstante, la elevada inversión que hacen los nodos durante este proceso no puede provocar su abandono, ya que esto supondría el fin de la red. Por ello, el creador de este proceso, Satoshi Nakamoto, estableció que, por la realización de este trabajo, el nodo minero que resolviera la PoW recibiría una recompensa en criptomonedas, lo que supone un incentivo para continuar con el desarrollo de la actividad. Pero no es esta la única cantidad de monedas que recibiría el nodo, ya que los usuarios que realizan una transacción pueden reducir el tiempo de confirmación a través del pago de una tarifa, de forma que los nodos priorizan aquellas transacciones que han pagado la tarifa más alta. Así, según Ammous (2018) está por un lado el "subsidio de bloque" que constituye la recompensa en bitcoins que recibe el nodo que ha conseguido resolver la PoW y por otro, la "recompensa por bloque" que es la suma de la cantidad obtenida en el subsidio de bloque junto los costes o "comisiones" de transacción que pagan los usuarios.

Sin embargo, la posibilidad de obtención de una recompensa no puede suponer en ningún caso la aceleración del proceso de minado por parte de los mineros para aumentar las posibilidades de obtener un beneficio económico. Si esto sucediera, aumentaría de forma incontrolada la cantidad de criptomonedas existentes y perderían su valor, es decir, supondría la devaluación de la criptomoneda y los nodos mineros ya no tendrían incentivos para continuar con la actividad minera y sustentar la red. Para evitar este riesgo, Satoshi Nakamoto, programó el sistema Bitcoin de forma que, la creación de un nuevo bloque se realizará cada diez minutos y la recompensa se ajustaría progresivamente.

De esta forma, las recompensas obtenidas con el minado o "subsidio de bloque" ajustan su valor a través de un proceso que se denomina *halving* y que supone una reducción

progresiva a la mitad cada 210.000 bloques resueltos hasta alcanzar el límite impuesto de 21 millones de bitcoins que se estima que será en el año 2140. Este proceso es inalterable y se realizará en conjunto con un "ajuste de dificultad" que permite ajustar el nivel de dificultad del minado calibrando y controlando que no se exceda o alcance el objetivo según la actividad de los mineros. Por lo tanto, se controla que, ante un aumento del valor del Bitcoin, no se aumente la capacidad de procesamiento de los mineros para crear monedas y alterar el proceso.

Por todo ello, el Bitcoin es un dinero sólido, ya que el aumento de su valor no supondrá un aumento de su oferta (Ammous, 2018). Si el proceso anterior no hubiera sido estandarizado puede que los mineros hubieran reducido su implicación en esta actividad a medida que un aumento de usuarios o transacciones en la red hubiera disminuido su rentabilidad en relación con la capacidad de procesamiento invertida o la electricidad consumida. Un aumento fácilmente de la cantidad de criptomonedas producida hubiera disminuido el valor de estas.

En relación con la recompensa recibida por los mineros, en el momento de creación de Bitcoin los mineros obtenían 50BTC por cada bloque resuelto[98]. El primer *halving* de Bitcoin tuvo lugar el 28 de noviembre de 2012 en el que se redujo la recompensa del bloque a 25BTC. Después de este han sucedido otros *halving*, así, en el año 2016 la recompensa se redujo a 12,5BTC por bloque y a partir del 11 de mayo del año 2020 la recompensa pasó a ser de 6,25BTC (Cointelegraph, 2023). Este proceso continuará conforme aumente la demanda de bitcoins aproximándose de forma asintótica al límite de 21 millones de monedas hasta el año 2140 en que se prevé que cese la producción de bitcoins.

Si se considera el precio de la unidad de Bitcoin, la minería de bitcoins se ha convertido en una actividad muy atractiva para aquellas personas motivadas por la búsqueda del beneficio económico[99]. Sin embargo, el minado de criptomonedas ha alcanzado una popularidad tan elevada que hoy en día requiere de recursos y equipos informáticos muy sofisticados, siendo una actividad mayormente dominada por grupos especializados en el minado de monedas conocidos como *mining pools* que, han apartado a los particulares con equipos personales de cualquier posibilidad de obtener beneficios con la minería de

[98] En la creación del bloque génesis de Bitcoin el 3 de enero de 2009 la recompensa por bloque minado era de 50BTC.

[99] El precio de la unidad de Bitcoin es de 21.342,24 euros a fecha de 30 de enero de 2023. Si la recompensa por bloque para el minero ganador es de 6,25BTC, la ganancia que obtendría por bloque sería de alrededor de 133.389 euros, además de las tarifas que pueden haber pagado los usuarios para acelerar las confirmaciones del bloque.

criptomonedas. Se requiere una elevada cantidad de electricidad y procesamiento[100], lo que supone una inversión económica que no en todos los casos podría verse recompensada debido al valor cambiante del Bitcoin y a la posibilidad de que no haya recompensa debido a la elevada competencia que existe en este ámbito. En este sentido, se ha señalado que, si se desea obtener beneficios con la utilización de criptomonedas, sería mucho más rentable la inversión en criptomonedas y el estudio de sus valores (Boar, 2018).

Transacciones con Bitcoin

Las transacciones en el sistema Bitcoin consisten en un intercambio de valor entre dos usuarios del sistema a través del envío de bitcoins de una parte a otra.

Estas transacciones pueden realizarse cualquier día, sin importar la hora y teniendo un carácter de disponibilidad inmediata del dinero una vez se ha validado y confirmado la transacción por los mineros. Habitualmente, el usuario deberá esperar alrededor de diez minutos para que se confirme la transacción. Sin embargo, se podrá acelerar este proceso mediante el pago de una pequeña comisión que dependerá de la actividad de la red en ese momento y la rapidez con la que el usuario desee que sea validada y confirmada su transacción.

Además, pueden realizarse con carácter nacional o internacional, lo que supondría una gran ventaja para todas aquellas personas que estén ubicadas en países con una infraestructura bancaria y financiera poco extendida o para aquellas personas que quieran mantener la privacidad de sus transacciones (Boar, 2018).

Debido a que no existen intermediarios, las transacciones realizadas son inmutables, es decir, una vez se han realizado y se han confirmado quedan registradas en la *Blockchain* y no podrán deshacerse, lo que dota a la transacción de una mayor seguridad. Si una persona ha recibido por error una cantidad de dinero que quiere enviar de vuelta, tendrá que realizar otra transacción diferente por la misma cantidad recibida. Esto ha planteado problemas con los monederos *online* y las plataformas de compraventa de bitcoins, ya que los usuarios pierden su dinero bien porque no han asegurado las claves de sus carteras o bien porque ha habido

[100] Sobre el desperdicio de electricidad y la capacidad de procesamiento que podría suponer esta actividad, el autor (Ammous, 2018) sostiene que hablar de desperdicio es algo que se debe a la naturaleza subjetiva del valor, ya que valoración de si se trata o no de un desperdicio es algo que incumbe a los propios usuarios del sistema Bitcoin. Esto es, para aquellos que crean firmemente en la minería y en la *Proof-of-work* como la única forma de mantener la seguridad y robustez del sistema Bitcoin, esta inversión será algo necesario para mantener el sistema de pago que desean continuar utilizando.

una brecha de seguridad que las ha filtrado. En ambas, la transacción realizada desde la otra parte en su beneficio sería irreversible.

Al mismo tiempo, una vez se realiza una transacción, los bitcoins conforman una unidad, bloque o trozo, de forma que han de ser transferidos de una vez. Esto es explicado por Ron y Shamir (2013) que exponen que si, por ejemplo, se dispone de tres trozos o *chunks* de 10 BTC cada uno y se quieren gastar 12,5 BTC, se tendría que enviar un *chunk* de 10 BTC más otro de 2,5 BTC y recibir 7,5 BTC de cambio. El cambio, formado por los bitcoins restantes, debería ser enviado a una nueva dirección que pertenezca al mismo usuario, pero cuyas claves pública y privada serán diferentes. Esta transacción de salida se conoce como salida de transacción sin gasto o UTXO en la jerga técnica (*Unspent Transaction Output*).

De forma detallada, al realizar una transacción se constituye un mensaje compuesto de entradas (*inputs*) y salidas (*outputs*). En las entradas, la persona "A" que quiere enviar dinero a la persona "B", demuestra que dispone de los fondos suficientes mostrando las transacciones que ha realizado anteriormente, que se pueden comprobar abiertamente accediendo a la *Blockchain*[101]. En el *input* se incluye 1) el *hash* de la transferencia previa; 2) la firma electrónica con la clave privada del transferente (encriptar el *hash* del mensaje de transferencia con la clave privada); 3) la clave pública del transferente (González-Meneses, 2019, p. 102). En las salidas, se indica a quién se quiere enviar el dinero y qué cantidad. Como *output* se generará un mensaje con: 1) la cantidad de bitcoins que se transfieren y 2) la dirección de Bitcoin del beneficiario (*hash* de la clave pública[102]) (González-Meneses, 2019, p. 102). Además, habría un tercer apartado formado por la comisión que se destina a los mineros por realizar la transacción. La cantidad de esta comisión determinará la velocidad a la que se confirma la transacción, teniendo prioridad aquellas transacciones que hayan pagado comisiones más elevadas para su confirmación. Por último, el emisor del mensaje

[101] Este hecho constituye otra diferencia del sistema Bitcoin con respecto a las cuentas bancarias. Mientras que una cuenta bancaria permite mostrar una suma del saldo disponible sin importar las transferencias realizadas, en el sistema Bitcoin para dar cuenta del dinero que se dispone hay que hacer referencia a las transacciones en específico recibidas donde está reflejado que se dispone de este dinero.

[102] Normalmente se denomina dirección Bitcoin a la clave pública de un usuario que le permite recibir fondos. No obstante, autores como M. González-Meneses (2019) consideran que la clave pública de Bitcoin es en realidad el *hash* de la clave pública. Las razones que ofrece para ello son, por un lado, en relación con la seguridad de la clave ya que, ofreciendo el *hash* de la clave pública, en lugar de esta directamente, se hace más difícil computacionalmente llegar a desvelar la clave privada del usuario. Por otro lado, también expone que el hash de la clave pública es mucho menos pesado que esta, lo que permite un ahorro de "bits" en la cadena de bloques.

firma con su clave secreta[103]. Cualquiera que conozca la clave pública del emisor podría verificar que el mensaje fue emitido por esa persona.

Cartera, Monedero o *Wallet* Bitcoin

Obtener una cartera o monedero de criptomonedas supone el primer paso para introducirse en el sistema Bitcoin. Consiste en un *software* o *hardware* que permite el almacenamiento de las claves públicas y privadas generadas automáticamente y empleadas para gestionar y acceder a las criptomonedas de las que se dispone.

De esta forma, al contrario de lo que se suele pensar, las criptomonedas no quedan almacenadas en las carteras, sino que, como se ha tratado en apartados anteriores, se encuentran distribuidas entre los diferentes nodos que forman parte de la cadena de bloques o *Blockchain.* Este hecho determina que la seguridad de la cartera quedará determinada por las precauciones que se guarden con respecto a la clave privada, de forma que aquella persona que disponga de esta tendrá acceso a la cantidad de criptomonedas con la que se corresponde.

En este sentido, existen tres requisitos que deberían cumplirse idealmente en la custodia de las claves secretas (Ponce de León, 2018, p. 46): disponibilidad, para acceder a ella en cualquier momento; seguridad, que solo esté a disposición de su propietario y comodidad, el sistema de custodia no debe ser excesivamente complejo.

Las carteras juegan un papel importante en el ecosistema Bitcoin ya que permiten operar con criptomonedas en un sistema totalmente descentralizado, sin entidades u organismos que pudieran controlar esto de otra forma (bit2me Academy, 2018). Pero no solo eso, ya que también permiten la creación de direcciones Bitcoin de carácter público que se asocian a la clave privada y que permiten realizar las transacciones.

Pero, aunque la cartera no suponga realmente el almacenamiento de las criptomonedas, hay que tener en cuenta que no todas las carteras son aptas para la gestión de todas las criptomonedas que existen, no siendo posible enviar criptomonedas entre carteras que no comparten el mismo tipo. A su vez, existen diferentes tipos de carteras siendo importante conocer las ventajas e inconvenientes de cada una de las existentes en el mercado

[103] Esta firma generará una firma digital que solo será válida para identificar ese mensaje. La verificación de la firma generada únicamente será válida si la clave pública se corresponde con la clave secreta que generó la firma. Aunque la clave pública se distribuye libremente, no es posible realizar modificaciones en la firma creada sin conocer la clave secreta, que únicamente dispone y conoce el emisor. De esta forma, esto serviría para evitar los llamados "ataques de intermediario" (*man-in-the-middle attack*), en los que el mensaje es interceptado por un tercero que lo manipula antes de que llegue al receptor (Ponce de León, 2018).

antes de decidir qué tipo se escoge para gestionar las criptomonedas de las que se dispone escogiendo aquellas que se adecue más a las necesidades que se tengan.

La diferenciación más conocida en este ámbito se establece según si estas carteras operan o no en línea, esto es *cold wallets* o *hot wallets.* Las primeras, tipo *hardware* o de papel, operan fuera de línea por lo que ofrecen un mayor nivel de seguridad para el almacenamiento de fondos, con un riesgo menor de posibles ataques cibernéticos. Por el contrario, las *hot wallets*, como las carteras de escritorio o *software* y las *online* requieren de una conexión a Internet y operan directamente desde un sitio web por lo que están conectadas siempre a Internet y a la *Blockchain* y presentan un mayor riesgo para la seguridad de los fondos (bit2me Academy, 2018).

Debido a su facilidad de uso, se considera que las *hot wallets* almacenarían bitcoins que se asemejan a la cantidad de dinero en efectivo que se suele utilizar diariamente en pequeñas transacciones, mientras que las *cold wallets* serían comparables con el almacenamiento de fondos de inversión o caja fuerte, para guardar importantes cantidades de dinero que tendrían que estar seguras ante posibles ataques (Boar, 2018).

Dentro de estos dos grupos se pueden encontrar a su vez varios tipos de carteras. Dentro de las *cold wallets* son conocidas las *hardware wallets* y las *paper wallets.* Las *hardware wallets* son dispositivos HSM (Módulos *Hardware* de Seguridad) externos similares a una memoria USB o disco duro diseñados para almacenar las claves privadas. Son una de las opciones más seguras que existen, ya que permanecen fuera de cualquier dispositivo, desconectados de Internet y se conectan vía USB para realizar una transacción, que es cuando el *software* correspondiente leería la clave privada. Además, disponen de una semilla que permite restaurar las claves y recuperar los fondos, iniciando un proceso de "autodestrucción" en el caso de que se intente manipular físicamente el dispositivo para acceder a la clave privada (bit2me Academy, 2016). El proceso de validación de la operación tiene lugar dentro de este dispositivo y no en el ordenador por lo que las claves privadas no salen en ningún momento del dispositivo (bit2me Academy, 2016). Sin embargo, autores como (Boar, 2018) ha señalado que esta opción como cualquier otra tiene también sus desventajas, como es su precio, que supondría una inversión de entre 20 a 120 euros, además del riesgo de pérdida o sustracción al tratarse de un dispositivo físico. En el mercado de las *hardware wallets* son conocidas "Trezor" y "Ledger".

Por otro lado, las *paper wallets* constituyen otro tipo de *cold wallet*, más conocidas y fáciles de crear, ya que consiste en una pieza de papel impreso que contiene las claves pública y privada. Debido a su formato, almacena las claves en un entorno *offline* y sólo requiere de

conexión a Internet en el momento de mover los fondos que contiene, lo que le dota de una elevada seguridad ante ataques informáticos. No obstante, esto no significa que no presente ningún tipo de riesgo. El formato en el que se presentan ocasiona que puedan extraviarse fácilmente, perdiendo el acceso a los fondos. Además, aunque las claves puedan ser almacenadas de forma segura una vez está impresa, habría que evitar que terceros puedan conocer las claves durante el desarrollo de la cartera. Para ello, se recomendaría ejecutar el código del sitio web sin conexión una vez la cartera esté configurada para generar las claves, además de utilizar una impresora que no esté conectada a una red. Los cajeros automáticos Bitcoin permiten obtener monederos de este tipo, pero en la web algunas conocidas son "BitAddress", "Bitcoin.com" o "Walletgenerator".

En cuanto a las *hot wallets,* son conocidas las carteras de escritorio, las carteras móviles o a través de una aplicación y las carteras web. Las carteras de escritorio son programas informáticos que se instalan en el ordenador y permiten almacenar las claves privadas. Dentro de estas, se diferencia entre *full client* (cliente completo) si supone la descarga de una cadena de bloques en el ordenador del usuario convirtiéndose en un nodo Bitcoin o *lightweight client* (cliente parcial) si no se descarga la cadena de bloques completa, sino sólo la parte que le correspondería (Boar, 2018). Las carteras móviles consisten en una aplicación móvil que permite gestionar bitcoins y realizar pagos a usuarios o comerciantes. Hay carteras de este tipo que son monederos SPV: *simplified Payment Verificación* (Verificación de Pago Simplificado) que supone un híbrido ente los dos tipos de clientes anteriores. Las carteras web funcionan de forma similar a las anteriores, pero utilizan sus propios servidores para almacenar estas claves lo que las hace vulnerables a ciberataques.

Exchange **o Casa de Cambio de Criptomonedas**

En el ámbito de las criptomonedas existen diversas formas de obtener estas monedas virtuales. Así, por ejemplo, se pueden comprar a otras personas utilizando dinero *fiat*, a través de un cajero automático o *Automated Teller Machine* (ATM) de criptomonedas o bien podrían comprarse vales de criptomonedas en comercios habilitados para ello.

Los *Exchange*, casas de cambio o plataformas de intercambio de criptomonedas son negocios que surgen con el propósito de permitir la obtención de criptomonedas[104].

La primera casa de cambio que apareció en la historia de las criptomonedas fue el *exchange* "Liberty", que se creó en el año 2010 y que permitía la compra de bitcoins

[104] A lo largo de este trabajo se empleará mayormente el término "casa de cambio" aunque en ocasiones también se hará uso del término "*exchange*", siempre asegurando que se conoce el significado de dicho término.

empleando moneda fiduciaria. Este hecho supuso, al mismo tiempo, la primera vez que las criptomonedas, en particular una unidad de Bitcoin tenía un precio de forma oficial. Esto favoreció el conocimiento progresivo de la criptomoneda en el año 2011, apareciendo en publicaciones de relevancia como *Forbes* o *The New Yorker*, lo que elevó su popularidad hasta tal punto que llegó a alcanzar ese año un valor de 100 millones de dólares (Domingo, 2018).

En la actualidad, las casas de cambio suelen encontrarse de forma *online*, permitiendo el acceso a través de diversos dispositivos como un ordenador o a través de aplicaciones de móvil. Una vez se accede a estos servicios, disponen de una interfaz gráfica que permite una gestión sencilla de las operaciones con criptomonedas. No obstante, estos negocios no están destinados únicamente a la compra de criptomonedas, sino que también permiten su venta. De esta forma, hay que señalar que existen tres tipos de casas de cambio (Pieters y Vivanco, 2015): *clearing*, descentralizadas y centralizadas. En el primero, el comprador y el vendedor establecen el precio deseado y la plataforma los pone en contacto (p.ej. btc-e, itbit, HitBTC, Kraken y The Rock). En las casas de cambio descentralizadas, los compradores y vendedores seleccionan el usuario con el que desean realizar la transacción de una lista de ofertas en las que aparece el nombre del usuario, el precio de la moneda y un código postal. Esta opción la convierte en la más atractiva para el delito, ya que además ofrece una gran variedad de formas de pago como ingreso en efectivo en una cuenta bancaria, transferencia a través de PayPal o pago en efectivo. Por último, en la opción centralizada la transacción no es realizada por las partes, sino que el dinero es enviado a la casa de cambio y las partes disponen de un tiempo para aceptar o rechazar el dinero propuesto (Pieters y Vivanco, 2015). Finalmente, serán las personas implicadas en la compra o venta las que decidan si se lleva a cabo o no la transacción, pero si se desarrolla esta no quedará reflejada en la *Blockchain*. El minado de esos bitcoins ya tuvo lugar y quedó reflejado en la cadena de bloques, por lo que esta transacción queda almacenada en los sistemas informáticos de la casa de intercambio (Fernández, 2018).

Una vez el usuario accede y se registra en una casa de cambio, se le proporciona una cartera *online* que le permitirá el almacenamiento y la gestión de sus monedas virtuales desde el *exchange* de una forma sencilla, lo que le exime del control y la preservación de sus claves pública y privada. De este modo, se considera que las casas de cambio actúan a su vez de proveedores de servicios de custodia de monederos electrónicos, como “entidades que prestan servicios de salvaguardia de claves criptográficas privadas en nombre de sus clientes, para la

tenencia, almacenamiento y transferencia de monedas virtuales" (Directiva 2018/843, L156/54)[105].

Para facilitar la gestión del usuario de sus criptomonedas y la inversión efectiva de su dinero, también cuentan con servicios de *trading* que muestran estadísticas en tiempo real sobre el valor de varios tipos de criptomonedas, lo que permite no solo la compra con dinero fiduciario, sino también la compra empleando otras criptomonedas que se hayan adquirido empleando el *exchange*.

Aunque Liberty fue la primera casa de cambio conocida, posteriormente han surgido otros *exchange* que fueron relevantes. Una de las casas de cambio más populares fue el *exchange* japonés "Mt. Gox" creado por el programador Jed McCaleb[106]. Los servicios de *exchange* para la criptomoneda Bitcoin fueron introducidos por McCaleb en el año 2010, pero en el año 2011 McCaleb vendió Mt.Gox a Mark Karpeles quien se desempeñaría como Director Ejecutivo (CEO) (mtgox, 2010). En el año 2011 alcanzó una gran popularidad pasando a gestionar más del 70% de todas las transacciones que se realizaban en bitcoins en todo el mundo. No obstante, fue en ese mismo año cuando comenzaron los escándalos relacionados con este *exchange*. Dicha casa de cambio empezó a presentar vulnerabilidades y brechas de seguridad de gran calado que la convirtieron en objeto de *hackers* que accedieron a sus servidores y robaron las credenciales que daban acceso a las claves de sus usuarios. El atacante transfirió el equivalente a 8.750.000 dólares en bitcoins, ocasionando a su vez que el precio de una unidad de Bitcoin pasara de 17,51 dólares a 0,01 (Bastardo, 2019).

El segundo escándalo con el que se relaciona a Mt. Gox tuvo lugar en el año 2014 cuando suspendió todas sus operaciones y se desconectó el sitio web. El motivo fue que la casa de cambio se volvió insolvente tras un supuesto *hackeo* en el que 850.000 bitcoins fueron robados de las cuentas. Aunque más tarde se recuperaron 200.000 bitcoins, la reputación del negocio había quedado comprometida. La casa de cambio suspendió sus operaciones, cerró su sitio web y su servicio de intercambio y se declaró en quiebra. Su CEO, Mark Karpeles, fue acusado por la justicia japonesa de malversación de fondos y manipulación de datos solicitando diez años de prisión. Se le acusaba de haber transferido el

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

[106] El propósito inicial de esta casa de cambio nada tenía que ver con la obtención de criptomonedas, sino que se creó inicialmente como un portal de intercambio de cartas "Magic: The Gathering Online", siendo el nombre "Mt. Gox" una abreviatura de este.

dinero a su cuenta a través de varias transacciones utilizando su computadora personal y alterando los registros de la compañía para ocultarlo. No obstante, se aplicó la suspensión de la pena al haber sido condenado a dos años y medio de prisión y no haber cometido delitos similares (Salgado, 2019). Por último, en esta trama también estuvo implicado Alexander Vinnik, relacionado con la casa de cambio "BTC-e" y que fue acusado de lavar los fondos que se robaron de Mt. Gox (Esparragoza, 2017).

No obstante, después de las casas de cambio Liberty y Mt. Gox, han aparecido muchas otras que operan legalmente en la actualidad. Los datos de la empresa de seguimiento de criptoactivos CoinMarketCap (2021), muestran alrededor de 300 casas de cambio en activo, que ha clasificado según el tráfico, la liquidez, y la confianza en los volúmenes de comercio informados. Según estos criterios, en la actualidad las casas de cambio situadas en los cinco primeros puestos son: Binance, Coinbase Exchange, Kraken, KuCoin, Bitfinex, Bitstamp, OKX, Bybit, Gemini y Bithumb[107].

El proceso para operar en las casas de cambio es similar entre las diferentes plataformas que existen. No obstante, algunas de ellas con objeto de prevenir el blanqueo de capitales y la financiación del terrorismo, bajo lo establecido en la normativa nacional e internacional, están obligadas a exigir al usuario la verificación de su identidad[108]. El objetivo en este caso consiste en obstaculizar aquellas actividades delictivas que se desarrollan aprovechando la opacidad de las transacciones realizadas con criptomonedas, haciendo hincapié en la importancia de la transparencia de estas actividades[109]. En este sentido, se recoge en la directiva que las casas de cambio o *exchanges* y los proveedores de servicios de custodia de monederos estarán obligados a cumplir la normativa y vigilar el uso que se hace de las monedas virtuales a efectos de la lucha contra el blanqueo de capitales y la financiación del terrorismo. Para ello, recoge que tendrán que colaborar para reducir el

[107] Datos obtenidos el 31 de enero de 2023 de la empresa CoinMarketCap https://coinmarketcap.com/es/rankings/exchanges/

[108] Este aspecto será tratado con mayor detalle en el bloque II en los capítulos relativos a la regulación de las criptomonedas y al blanqueo de capitales y su normativa.

[109] Este aspecto es señalado en la Directiva 2018/843, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, que propone la "habilitación para crear y mantener una base de datos central en la que se registren las identidades y las direcciones de monedero electrónico de los usuarios accesibles para las UIF, así como los formularios de autodeclaración destinados a los usuarios de la moneda virtual, y para mejorar la cooperación entre los organismos de recuperación de activos de los Estados miembros y una aplicación basada en el riesgo de las medidas a que se refiere el artículo 20, letra b)" (L 156/72). Con el objetivo de vincular transacciones sospechosas con actividades delictivas, la Unidad de Información Financiera (UIF) requiere de un amplio acceso a la información y al intercambio de datos entre países, que le permita rastrear flujos de capital y prevenir actividades financieras relacionadas con el terrorismo y blanqueo de capitales.

anonimato asociado a estas monedas virtuales y, además, el Estado deberá garantizar que tanto proveedores de servicios de cambio como proveedores de servicios de custodia de monederos electrónicos estarán registrados[110]. De esta forma, si se detecta una dirección bitcoin como sospechosa de participar en un delito, se podría investigar la identidad del autor, ya que se dispone de un registro en el que se ha realizado dicha vinculación. Esto es lo que se conoce como las políticas de "Conoce a tu cliente" o *Know your customer* (KYC).

Cuando el usuario accede al registro en una de estas casas de cambio, se le pedirán datos relativos a su identidad como nombre y apellidos, dirección postal, ciudad, país e incluso una fotocopia o foto ante la cámara web de algún documento de identidad como DNI, pasaporte o permiso de conducir. Otros *exchanges* sin embargo, exigen la aportación de dicha información según la cantidad de criptomonedas que se utilicen, siendo necesario para cantidades elevadas.

Para el registro en el e*xchange* "Coinbase" por ejemplo, según advierten en su página web y lo que se ha podido comprobar, la normativa financiera les exige verificar la identidad mediante la recopilación de datos como la nacionalidad, nombre y apellidos, fecha de nacimiento, DNI, dirección postal, motivo por el que se utiliza el *exchange*, la fuente de fondos utilizada y situación laboral. Una vez se cumplimenta esta información se realizan otras preguntas como la cantidad de criptomonedas que tiene previsto operar al año y el sector en el que trabaja. Finalmente, se exige presentar documentos de identidad como pasaporte, permiso de conducir o el documento nacional de identidad. En el *exchange* "Binance" se exigen los mismos datos que en el anterior, pero a diferencia del anterior, no es necesario presentar ningún documento de identidad a no ser que se requiera aumentar el límite de retiro a 100 BTC o los límites de depósitos en monedas locales seleccionadas.

[110]Modificación del artículo 47 de la Directiva 2015/849, dedicado a la supervisión, en el que se sustituye el texto por lo expuesto en el punto 29 de la Directiva 2018/843: *Los Estados miembros garantizarán que los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias y los proveedores de servicios de custodia de monederos electrónicos estén registrados, que los establecimientos de cambio, las entidades de cobro de cheques y los proveedores de servicios a fideicomisos (del tipo «trust») y sociedades estén autorizados o registrados, y que los proveedores de servicios de juegos de azar estén regulados* (L 156/67).

Capítulo 4. Criptomonedas Alternativas o *Altcoins*

Bitcoin fue la primera criptomoneda que se creó y hasta la fecha sigue siendo la más utilizada con un valor de capitalización de mercado de 411.170.470.637 euros en los inicios del año 2023 (CoinMarketCap, 2023a) [111]. No obstante, su creación y la expansión de su uso dio lugar a la creación de otras criptomonedas existiendo en la actualidad más de 8000 criptomonedas diferentes[112] (CoinMarketCap, 2023a).

Las otras criptomonedas que surgieron a partir de Bitcoin se denominan monedas alternativas o en inglés *altcoins*, que son nuevas monedas virtuales desarrolladas a partir del código abierto de la criptomoneda Bitcoin[113]. De esta forma, se han realizado modificaciones añadiendo nuevas características o funcionalidades con el objetivo de crear una nueva criptomoneda que ofrezca nuevas soluciones a otro tipo de problemas o bien se ha mejorado algún aspecto de la tecnología *Blockchain* o del Bitcoin.

Algunas de esta monedas están supeditadas a la *Blockchain* de Bitcoin, pero la mayoría son *forks*[114] de Bitcoin con *Blockchain* propia, o sistemas independientes que utilizan una o varias *Blockchain* (Ponce de León, 2018).

Aunque todas ellas han surgido a partir de Bitcoin, cada criptomoneda tiene sus propias peculiaridades, por lo que se les ofrece a los usuarios diversas alternativas para escoger según sus intereses. Por ello, será necesario conocer las principales criptomonedas en la actualidad para tomar una decisión y escoger la más conveniente en cada caso. Por ejemplo, en el ámbito de la inversión, el elevado valor de la unidad y la elevada volatilidad de Bitcoin ha motivado a que los usuarios escojan en su lugar criptomonedas alternativas para invertir. Un estudio realizado por Boar (2018) en el que se compara el precio de las principales criptomonedas con respecto al Bitcoin según la capitalización en el mercado, señala que el comportamiento de las criptomonedas Bitcoin Cash y Ethereum es muy similar al del Bitcoin, mientras que la criptomoneda Ripple, aun moviéndose en la misma dirección que Bitcoin, presenta un valor inferior, situándose como una buena alternativa a la volatilidad del primero. Así también expone que la volatilidad de las *altcoins* con respecto a la de Bitcoin

[111] La "capitalización del mercado" en la industria del Blockchain hace referencia al tamaño relativo de una criptomoneda, lo que se calcula multiplicando el precio de mercado actual de una moneda o token por el número total de monedas en circulación (CoinMarketCap, 2023a). Datos actualizados a fecha 31 de enero del 2023 de https://coinmarketcap.com/es/currencies/bitcoin/

[112] Según los datos recogidos por la web CoinMarketCap el 26 de septiembre de 2020.

[113] La primera criptodivisa alternativa creada alternativa a Bitcoin fue "Namecoin" en el año 2011.

[114] Se denomina *fork* al software que se crea a partir del código fuente de otro *software* para crear un nuevo proyecto siguiendo una línea de desarrollo independiente. Para el caso del sistema Bitcoin, estaría hablándose de un *software* o aplicación desarrollados a partir del código de Bitcoin o *Bitcoin core.*

es mucho menor, a pesar de que algunos se muevan en la misma dirección (Boar, 2018). Por ello, en cuanto a obtener beneficios con la inversión de criptomonedas, recomienda no invertir todo el capital en una única criptomoneda ni tampoco únicamente en criptomonedas, combinarlo con otros activos (Boar, 2018). Este ejemplo serviría para ilustrar cómo según el propósito que se persiga con la obtención o utilización de criptomonedas, es recomendable y necesario el estudio de las características de aquellas en las que se esté interesado o al menos de las más significativas. En cuestiones de inversión de capital, al menos, los riesgos son elevados y el daño podría ser irreparable.

Según la capitalización de mercado actual[115], las diez primeras criptomonedas serían: Bitcoin, Ethereum, Tether, BNB, USD Coin, XRP, Binance USD, Cardano, Dogecoin y Polygon (CoinMarketCap, 2023a). Si se comparan estos resultados con los obtenidos para el año 2019, se puede observar que en este año las criptomonedas principales en términos de capitalización de mercado fueron de mayor a menor Bitcoin, Ether, Ripple, Litecoin y Monero (Statista, 2020)[116].

Sin embargo, el objetivo de este trabajo no es ofrecer una revisión exhaustiva de las criptomonedas alternativas que existen, sino exponer las nociones básicas de aquellas seleccionadas. En este caso se tratarán Ether, Litecoin y Monero. Las dos primeras fueron las criptomonedas más conocidas que surgieron después de Bitcoin. La última es una criptomoneda de carácter privado que se utiliza en el ámbito criminal.

Ether (ETH)

El Ether (ETH) es la criptomoneda de la *Blockchain* Ethereum, que fue planteada inicialmente en el año 2013 por su fundador Vitalik Buterin y lanzada finalmente en el año 2015 (Buterin, 2013)[117]. De la misma forma que la criptomoneda Bitcoin, se trata de una moneda virtual protegida con criptografía, sin control centralizado, global, que permite su envío a través de una red peer-to-peer sin intermediarios, abierta a cualquier persona que

[115] Los datos mostrados fueron tomados el 29 de enero de 2023, pudiendo variar dependiendo del momento en el que se consulte la fuente.
[116]Los porcentajes en específico para la capitalización de mercado de las criptomonedas en el año 2019 fueron: 53% Bitcoin, 11% Ether, 9% Litecoin, 3% Ripple y 1% Monero. El 23% restante pertenece al resto de criptomonedas existentes, que en este caso no se ha incluido dentro de la lista porque, aunque el porcentaje sea mayor que las criptomonedas presentadas anteriormente, en el mercado existen más de 3000 criptomonedas diferentes, por lo que si se tiene en cuenta la cantidad de criptomonedas a la que pertenece tal porcentaje el mismo no es tan significativo (Statista, 2020).
[117] Vitalik Buterin presentó la Guía de Ethereum en el año 2013 antes de lanzar el proyecto Ethereum. Esta guía contiene todos los detalles sobre el desarrollo y funcionamiento de la *Blockchain* Ethereum, así como de la criptomoneda asociada, el Ether. Puede ser consultada con detalle en https://ethereum.org/es/whitepaper/

tenga una conexión a Internet y una cartera para ETH y disponible en cantidades flexibles hasta 18 posiciones decimales (Ethereum, 2021a).

En la actualidad tiene un valor de capitalización del mercado de 179.295.990.574 euros, siendo el precio de una unidad de Ether de 1464,12 euros, lo que equivaldría a 0.06881 bitcoins [118] (CoinMarketCap, 2023a).

Difiere de la *Blockchain* de Bitcoin en que está desarrollada con un lenguaje de programación Turing completo[119], lo que permite a cualquier persona que lo desee escribir contratos o crear aplicaciones descentralizadas en las que pueden crear sus propias reglas, determinar sus formatos y funciones. De esta forma, Ethereum se posiciona como la primera plataforma que permite el desarrollo de aplicaciones descentralizadas sobre un registro distribuido y los conocidos como *Smart Contracts* o contratos inteligentes (Buterin, 2013). Se presenta como una *Blockchain* programable, que permite a los usuarios, a través de la *EVM* (en inglés, *Ethereum Virtual Machine*) desarrollar sus propias operaciones.

Además de esto, la *Blockchain* de Bitcoin se diferencia de la *Blockchain* de Ethereum en la arquitectura. A diferencia de Bitcoin, que solo tiene una copia de la lista de transacciones, los bloques de Ethereum disponen de una copia tanto de la lista de transacciones como del estado más reciente (Buterin, 2013). El estado se almacena en la estructura del árbol y después de cada bloque solo una parte pequeña del árbol necesita ser modificada, lo que ese consigue introduciendo un árbol conocido como "árbol Patricia", que añade modificaciones al "árbol de Merkle" empleado en Bitcoin, una estrategia que proporcionaría un enorme ahorro de espacio a Bitcoin (Buterin, 2013).

La moneda de Ethereum, el Ether, tiene un doble propósito, proporcionando una capa de liquidez primaria para permitir el intercambio eficiente entre varios tipos de activos digitales y por otro lado, proporcionar un mecanismo para pagar tarifas de transacción (Buterin, 2013)[120]. Suponen a su vez los incentivos para que los mineros de la *Blockchain* de Ethereum proceses y verifiquen las transacciones.

[118] Datos obtenidos el 31 de enero de 2023 de la página CoinMarketCap https://coinmarketcap.com/es/currencies/ethereum/

[119] Esto significa que el código de la Ethereum *Virtual Machine* o Máquina virtual de Ethereum puede codificar cualquier cómputo que se pueda llevar a cabo, incluyendo bucles infinitos (Buterin, 2013).

[120] Independientemente de sus propósitos generales, el valor que tiene ETH puede depender del usuario que los utilice. Esto es, para la comunidad de Ethereum, el valor del Ether consiste en que permite pagar las tarifas de transacción que permiten mantener en funcionamiento el sistema *Blockchain*. Otros usuarios, ven este valor en que supone una reserva digital y más recientemente, se ha visto el valor del Ether omo garantía para préstamos criptográficos o como sistema de pago. Por supuesto también está el valor que tiene la moneda virtual como una inversión, de la misma forma que otras como el Bitcoin

La filosofía en la que se basa el diseño de Ethereum sigue los principios de simplicidad, universalidad, modularidad, agilidad y no discriminación o censura. Con la simplicidad hace referencia a que el protocolo Ethereum se desarrolló con la intención de que fuera lo más simple posible, de forma que cualquier programador promedio fuera capaz de entenderlo e implementarlo. En relación con su universalidad, Ethereum no tiene "funciones", sino que su lenguaje permite que se pueda desarrollar cualquier contrato inteligente o transacción de cualquier tipo que se pueda definir matemáticamente. La modularidad de Ethereum hace referencia a que las partes del protocolo tienen ser diseñadas de la forma más modular y separable posible, pero al mismo tiempo que permita al resto del ecosistema de criptomonedas beneficiarse de cualquier modificación implementada. También se trata de un protocolo ágil, lo que significa que no es inamovible y que podrían ser consideradas modificaciones que supongan una mejora en la escalabilidad o seguridad. Finalmente, garantiza la no discriminación y censura ya que no debe intentar restringir o prevenir activamente ninguna categoría de uso (Buterin, 2013).

La característica más relevante de Ethereum es que se trata de una plataforma programable, lo que la ha convertido en una tecnología muy versátil con múltiples aplicaciones. De forma general, existen tres tipos de aplicaciones sobre la plataforma Ethereum: aplicaciones financieras (submonedas, derivados financieros, carteras de ahorros e incluso algunas clases de contratos de empleo a gran escala), aplicaciones semifinancieras (por ejemplo, las recompensas autoaplicadas a soluciones a problemas computacionales) y otras aplicaciones no financieras como el voto en línea y el gobierno descentralizado (Buterin, 2013). Dentro de estas aplicaciones son conocidos los sistemas de *Token*, los derivados financieros y la moneda de valor estable, los sistemas de identidad y reputación, el almacenamiento de archivos descentralizado y las organizaciones autónomas descentralizadas (Buterin, 2013). Los sistemas de *tokens* son muy fáciles de implementar en Ethereum y tienen muchas aplicaciones, que van desde submonedas que representan activos como el USD o el oro, acciones de empresas, *tokens* que representan una propiedad inteligente o tokens sin valor solo usados como sistemas de puntos para incentivos.

Los derivados financieros son la aplicación más común de un "contrato inteligente" y una de las más sencillas de implementar en código. Dentro de los sistemas de identidad y reputación se encuentran los sistemas de registro de nombres, que consisten en una base de datos dentro de la red Ethereum a la que se puede añadir datos, pero no modificarlos ni eliminarlos. En relación con el almacenamiento de archivos descentralizado, Ethereum

permite el desarrollo de un ecosistema de este tipo en el que los usuarios individuales pueden ganar pequeñas cantidades de dinero alquilando sus propios discos duros (Buterin, 2013).

Los contratos inteligentes o *Smart contracts* son programas informáticos que se ejecutan en la cadena de bloques Ethereum[121] y que permiten el desarrollo de contratos entre partes y finaliza cuando se cumple lo establecido por ambas. Permiten disponer de saldo y enviar transacciones a través de la red como si se tratara de una cuenta Ethereum, pero no están controlados por ningún usuario, una vez implementados en la red se ejecutan según lo programado[122].

Para poder implementar los contratos inteligentes en la cadena de bloques se emite una transacción especial que ordena su creación. A través de esta transacción se crea una dirección, similar a la dirección de usuario en el sistema Bitcoin, a la que se podrán enviar fondos para ejecutar el contrato[123] (Ponce de León, 2018).

De entre los casos de uso de Ethereum, son muy conocidos los términos DeFi (*DEscentralized finance* o Finanzas descentralizadas)[124], NFTs (*Non-fungible tokens* o *Tokens*

[121] *A "smart contract" is simply a program that runs on the Ethereum blockchain. It's a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain* (Wesley, 2021).
[122] Se han explicado con mayor detalle en el apartado perteneciente a las aplicaciones y tecnologías de la *Blockchain*.
[123] Esta ejecución tiene lugar en la llamada "Máquina Virtual de Ethereum" (*Ethereum Virtual Machine*, EVM) que es ejecutada por cada uno de los nodos completos dentro del proceso de verificación de bloques. De esta forma, toda la red de forma masiva y paralela ejecuta el código de un contrato de forma consensuada y distribuida.
[124] Un DeFi es un término que hace referencia a productos y servicios de un sistema financiero abierto y global construidos como alternativa para los sistemas opacos, estrictamente controlados y unidos por una infraestructura y procesos de la antigüedad. Estos servicios permiten a cualquier usuario que pueda usar Ethereum con conexión a Internet acceder a ellos, dándoles control y visibilidad del dinero (Ethereum, 2021c). No hay autoridades centrales que puedan bloquear los pagos o negar el acceso y los servicios son más seguros ya que son controlados por un código abierto (Ethereum, 2021c). La primera aplicación DeFi surgió con Bitcoin, que ya permitía poseer y controlar el valor del dinero y enviarlo a cualquier parte del mundo sin la necesidad de un intermediario confiable. Ethereum se ha basado en esto pero, añadiendo que este dinero sea programable utilizando los contratos inteligentes, lo que permite en este caso combinar el control y la seguridad de Bitcoin con los servicios de las instituciones financieras como prestar y pedir prestado dinero, programar pagos e invertir en fondos (Ethereum, 2021c).

no-fungibles)[125] y DAOs (*Decentralized autonomous organisations* u Organizaciones descentralizadas autónomas)[126].

Litecoin (LTC)

La criptomoneda Litecoin fue una de las primeras que se crearon a partir del código de Bitcoin. En la actualidad, tiene un valor de capitalización de mercado de 6.279.376.698 euros siendo el precio de una unidad de 87,03 euros (CoinMarketCap, 2023a).

En relación con sus aspectos técnicos, la criptomoneda Litecoin es muy similar a Bitcoin. El LTC consiste en una moneda virtual *peer-to-peer* que permite la realización de transacciones protegidas con criptografía, conforma una red de pago global descentralizada y su software es libre y transparente (Litecoin, 2023).

No obstante, tuvo su origen en la necesidad de una alternativa que diera respuesta al problema de escalabilidad que presenta Bitcoin. Según el diseño de los bloques en la *Blockchain* de Bitcoin, se prevé la emisión de un bloque cada 10 minutos aproximadamente. No obstante, si el número de transacciones es muy elevado, la limitación de tamaño de los bloques obliga a las transacciones en espera a incorporarse en el próximo bloque, siendo el tiempo de espera mucho mayor de 10 minutos (Domingo, 2018). Para solucionar este problema, en el sistema Litecoin el tiempo de generación de un bloque se redujo a 2,5 minutos, lo que suponía un aumento en la frecuencia de generación de los bloques (Litecoin

[125] Consisten en la representación de un activo de forma digital, en este caso basado en la plataforma Ethereum. *Token* no fungible es un término que procede de la economía y que hace referencia a elementos no intercambiables por otros elementos porque tienen propiedades únicas, a diferencia de aquellos fungibles cuyo valor los define más allá de sus propiedades (Ethereum, 2021d). Esto garantiza que en el entorno digital se pueda conseguir propiedades como la escasez, la singularidad y la prueba de propiedad. La generalidad de su aplicación ha permitido la *tokenización* de bienes como arte u objetos de colección. Ha adquirido una elevada popularidad entre los artistas digitales, que han visto cómo aquellas personas interesadas en la criptografía se han interesado también por su trabajo. Un ejemplo de ello es "Foundation", una plataforma en la que creadores pueden participar de una economía creativa en la que se usa la *Blockchain* de Ethereum para dar valor a sus creaciones (Foundation, 2021).

[126] Una organización autónoma descentralizada consiste en una empresa que pertenece y es administrada colectivamente por sus miembros con un funcionamiento horizontal y completamente democratizado (Ethereum, 2021b). De esta forma, se aseguran de que no haya un directivo que pueda manipular los gastos según su propio beneficio. La decisión colectiva para el funcionamiento de determinados aspectos de la empresa se puede ver en una tesorería a la que nadie puede acceder sin la aprobación del grupo o en el desarrollo de propuestas y votaciones para garantizar la representación de todas las voces del grupo en la toma de decisiones (Ethereum, 2021b). Además, todos estos procesos son totalmente transparentes y verificables, lo que supone una gran ventaja en empresas puramente digitales en las que suele ser muy relevante la confianza depositada en la otra parte (Ethereum, 2021b). Su funcionamiento se basa en la tecnología de contratos inteligentes, a partir del cual se definen las reglas de la organización y se mantiene la tesorería, de forma que una vez activo el contrato en Ethereum nadie puede realizar una modificación de las reglas de forma individual, sino que se requerirá la decisión del grupo, de la misma forma que para acceder a la tesorería y gestionar el dinero del grupo (Ethereum, 2021b). Este modelo podría utilizarse por ejemplo en organizaciones benéficas, en las que se aceptan membresías y donaciones de cualquier persona del mundo y será el grupo el que de forma colectiva decida cómo se gastan las donaciones de las que disponen (Ethereum, 2021b).

Wiki, 2019). Esta modificación se tradujo en una mayor capacidad para administrar un mayor volumen de transacciones y por tanto el desarrollo de unas transacciones más rápidas y una mejora en la eficiencia de almacenamiento (Litecoin Project, 2021).

No obstante, a pesar de las mejoras implementadas con respecto al sistema Bitcoin, Litecoin cuenta con algunos inconvenientes que pudieran ser responsables de su baja adopción con respecto a su homóloga. Dos de estos inconvenientes son señalados por Domingo (2018), el primero de ellos, como resultado una generación más rápida de los bloques se ha producido una depreciación del valor de la moneda debido a la mayor cantidad de transacciones que se realizan. Como segundo inconveniente, el hecho de que la comunidad Litecoin sea mucho más pequeña con un líder visible claro e influyente podría generar cierta desconfianza en cuanto si existe una descentralización real. Este hecho queda asegurado en Bitcoin con el consenso de la comunidad, pero dado que esto lleva tiempo, en Litecoin se prioriza la rapidez sobre la confianza en la moneda en ese sentido.

Monero (XMR)

Inicialmente conocida como "BitMonero", la criptomoneda Monero fue creada en abril del año 2014 a partir del protocolo "CryptoNote" (Thankful_for_today, 2014) creado por Nicolas van Saberhagen y diseñado para mitigar riesgos asociados con la reutilización de claves y seguimiento de entrada y salida. En su desarrollo planteaba el uso de firmas de anillo y claves de un solo uso (*one-time keys*) para ocultar el destino y el origen de las transacciones. De esta forma, la creación de Monero no se basó desde el principio en el sistema Bitcoin, sino que se tomó como punto de partida el protocolo de "CryptoNote" que se había inspirado en el de Bitcoin.

En la actualidad, la criptomoneda Monero tiene un valor de capitalización de mercado de 3.057.435.530 euros con un valor por unidad de 167,68 euros (Blockchain.com, 2023)[127].

El objetivo de su creación, a diferencia de otras monedas, no fue el de crear una moneda similar a Bitcoin con algunas mejoras, sino que Monero surgió como una moneda para todas aquellas personas preocupadas por preservar su privacidad en la red. El diseño de Bitcoin permite consultar de forma pública todas las transacciones realizadas y registradas en la *Blockchain*, por lo que con la creación de Monero se pretendía dar respuesta a las

[127] Cifras obtenidas para la criptomoneda Monero el 30 de enero de 2023 de https://www.blockchain.com/explorer/assets/xmr

peticiones de todas aquellas personas que demandaban una moneda virtual realmente anónima.

De esta forma, el desarrollo de Monero y las tecnologías que se le implementaron siguieron en todo momento la filosofía de seguridad, privacidad y descentralización (Monero, 2021b).

El uso de una encriptación más resistente y fuerte permite la realización de transacciones criptográficamente seguras manteniendo a salvo la identidad de los usuarios por defecto (Monero, 2021b). Esto quiere decir que, a diferencia de otras criptomonedas como Bitcoin, la seguridad en Monero no depende de los conocimientos que tenga el usuario sobre la aplicación de técnicas de ocultación y protección de su identidad, sino que el desarrollo de la moneda se ocupó de este aspecto desde el principio.

Para asegurar una mayor descentralización en la creación de la moneda la comunidad Monero creó un algoritmo de consenso o Prueba de trabajo (*Proof-of-Work*) (Monero, 2021b) que se actualiza cada seis meses, lo que evita la utilización de equipos específicos de minado de Monero. Se quiere evitar con esto lo que en el sistema Bitcoin se conoce como "*pool*" o grupos de mineros que a través de la compra y uso de grandes poderes de minado o *Hashpower* monopolizan la creación de nuevas criptomonedas, siendo casi imposible la participación en esta actividad para aquellas personas que disponen de equipos informáticos personales. Así, según autores como Domingo (2018), se asegura un proceso verdaderamente democrático, en el que ninguno de los miembros que participan cuenta con una mayor ventaja con respecto al resto y por tanto pudiendo afirmar que la creación de la cadena es realmente la decisión de la mayoría.

Además, para asegurar la minería y por tanto la seguridad a largo plazo del sistema, la emisión de monedas es infinita, a diferencia del límite de 21 millones de bitcoins. En Monero cada bloque es creado aproximadamente cada dos minutos y no hay un tamaño máximo, sino una penalización de bloque y un tamaño dinámico para garantizar una escalabilidad también dinámica (Monero, 2021b).

En relación con la privacidad que garantiza la moneda, Monero cuenta con una serie de tecnologías que le permiten considerarse como una criptomoneda anónima. Las tres tecnologías principales para conseguir este propósito son las *Ring signatures* o firmas de anillo, *Stealth Addresses* o direcciones ocultas y la técnica "RingCT".

Las firmas de anillo son un tipo de firma digital que puede realizar cualquier miembro de un grupo de usuarios que dispongan de claves. Para su realización se hace uso de las claves de la cuenta de un usuario, así como de las claves públicas extraídas de la cadena de

bloques mediante un método de distribución triangular, así todas las personas del grupo firman una misma transacción siendo iguales y válidos (Monero, 2021a). De esta forma, es computacionalmente inviable determinar cuál de las claves de los miembros de un grupo se utilizó para producir la firma, garantizando que no se pueden rastrear las transacciones (Monero, 2021a).

Las direcciones ocultas, se centran en la privacidad de la persona que recibe el dinero, ya que permiten y requieren que el remitente cree una dirección única aleatoria en nombre del destinatario por cada transacción (Monero, 2021c). Sólo el remitente y el destinatario pueden determinar dónde se envió un pago. Así, el destinatario solo puede publicar una sola dirección, pero todos sus pagos entrantes serán enviados a direcciones únicas en la cadena de bloques, no pueden vincularse a la dirección publicada por el receptor ni a las direcciones de otras transacciones (Monero, 2021c). Al crear una cuenta de Monero, el usuario dispone de una clave de visualización privada (P*rivate view key*), una clave de gasto privada (*Private spend key*) y una dirección pública (*Public Address*). La clave de gasto se usa para enviar pagos, la clave de visualización se utiliza para mostrar las transacciones entrantes destinadas a la cuenta y la dirección pública sirve para recibir pagos (Monero, 2021c). Ambas, tanto la clave de gasto como la clave de visualización se utilizan para formar la dirección Monero.

La implementación en el año 2017 de la técnica "RingCT" (*Ring Confidential Transactions*)[128] en todas las transacciones permite ocultar el importe en cada una de ellas (Koe et al., 2020). El protocolo anterior de Monero se basaba en "CryptoNote", que utilizaba firmas de anillo y claves de un solo uso para ocultar el destino y el origen de las transacciones. Con el protocolo "RingCT" se presenta un nuevo tipo de firma de anillo, que consiste en una firma de grupo anónima, espontánea y de capa múltiple (*A Multi-layered Linkable Spontaneous Anonymous Group signature)* que permitirá ocultar los importes, orígenes y destinos de las transacciones de forma eficiente y generando monedas verificables y sin confianza (Noether et al., 2016). De esta forma, el protocolo RingCT proporciona una criptomoneda fuertemente descentralizada (es decir, no hay ninguna parte privilegiada), fiable y segura (Noether et al., 2016, p.14).

Además de estas tecnologías, las transacciones se realizan sobre la red TOR e I2P para reducir el riesgo de revelar información sensible y el riesgo de censura y también utilizan el protocolo "Dandelion ++" para ocultar la cantidad de dinero que se envía o recibe. Además,

[128]Se puede encontrar toda la información relativa a esta técnica en el trabajo original de sus autores: Noether, S., Mackenzie, A., & Monero Core Team. (2016). Ring Multisignature. *Monero Research Lab*, MRL-0008, 1–7. https://web.archive.org/web/20161023010706/https://shnoe.files.wordpress.com/2016/03/mrl-0008_april28.pdf

las decisiones de desarrollo son claras, abiertas a discusión pública y los registros quedan publicados en línea siendo accesibles y visibles (Monero, 2021b).

Todas estas medidas para mantener la privacidad la convierten en una moneda anónima y fungible, lo que la diferencia de la moneda Bitcoin debido a la transparencia de su *Blockchain* (Koe et al., 2020). De esta forma, una unidad de Monero es igual que otra, algo que no sucede con Bitcoin. Un usuario de Bitcoin que adquiere una unidad de este está adquiriendo de forma indirecta todo el historial de transacciones por el que ha pasado esa moneda, ya que este registro tiene un carácter público. Con la utilización de Monero no es posible conocer con exactitud cuál ha sido el recorrido de las monedas, lo que permite garantizar las propiedades que se le reconocían inicialmente a la Bitcoin *Blockchain* como la inmutabilidad, la contabilidad distribuida y la alta seguridad, pero con transacciones realmente anónimas (Domingo, 2018).

Todas estas medidas para asegurar su privacidad han convertido a Monero en la criptomoneda de los más "puristas" (Domingo, 2018), es decir, aquellas personas que desconfían de la transparencia con la que cuenta la *Blockchain* de criptomonedas como Bitcoin. A pesar de las ventajas que pudiera tener la utilización de Monero sobre la utilización de Bitcoin, lo cierto es que la criptomoneda Monero es mucho menos utilizada, en parte a su menor adaptación ya que no está disponible en una gran cantidad de *Exchanges* y comercios.

BLOQUE II: LAS CRIPTOMONEDAS EN EL ÁMBITO CRIMINAL

Capítulo 5. La Utilización de Criptomonedas Para la Comisión de Delitos.

Estimación de la Delincuencia con Criptomonedas

Las criptomonedas se han convertido en una tecnología que se ha visto involucrada en la comisión de delitos. Son frecuentes sus apariciones en los medios de comunicación en los que las señalan como un instrumento decisivo y de gran interés en el desarrollo de ciertos tipos de delitos. Esta situación ha ocasionado preocupación en ciertas autoridades encargadas de la detección, persecución, investigación y prevención del delito. Un ejemplo de ello, lo ha formado la Oficina Federal de Investigaciones de Estados Unidos, mayormente conocida como *Federal Bureau of Investigations* (en adelante, FBI), que en el año 2012 expresó a través de un informe su preocupación ante la utilización de esta moneda virtual en la comisión de diversos delitos como el blanqueo de capitales e incluso por su utilización como herramienta de estafa para otros usuarios de Bitcoin (Zetter, 2012). Además, en este informe, filtrado en Internet[129], se señalaba la dificultad que existía para rastrear la identidad de los usuarios debido a la utilización de criptografía y a su arquitectura *peer-to-peer* que suprime la existencia de una figura central (Zetter, 2012). Por todo ello, terminan concluyendo que es una herramienta que atraerá a toda aquella persona interesada en la comisión de delitos como el blanqueo de dinero, el tráfico de personas, el terrorismo y otros delitos relacionados con la evasión de sistemas financieros tradicionales a través de las transferencias monetarias globales (Zetter, 2012).

El abordaje de este tipo de criminalidad, su identificación y su estudio no son tareas sencillas debido a las propias características de las criptomonedas. No obstante, a pesar de las dificultades que pudieran existir, esta tarea es necesaria puesto que permite justificar la implementación de medidas exigidas para luchas contra esta criminalidad y que pueden llegar a limitar o prohibir ciertos aspectos del ámbito de las criptomonedas sofocando la innovación y la privacidad de los usuarios. Las personas encargadas de la ley, jueces y Fuerzas y Cuerpos de Seguridad del Estado (FCSE) se muestran interesados en determinar la gravedad de este tipo de criminalidad para valorar la necesidad de elaborar leyes que obliguen a los usuarios de las criptomonedas a limitar su actividad (Schickler, 2022).

[129] Debido a que se trataba de un informe oficial que fue filtrado en Internet en el año 2012, no ha sido posible acceder al documento original que se está tratando, solo a información con carácter parcial o tratada por otros autores que en la fecha sí que tuvieron acceso a dicho documento.

En este sentido, las criptomonedas constituyen una fracción pequeña, pero significativa de las finanzas mundiales (Collins, 2022). A primeros del año 2022, la capitalización total del mercado de las criptomonedas era de aproximadamente 1,3 trillones de dólares, mientras que en el año 2020, los activos totales de los mayores bancos del mundo eran de aproximadamente 128 trillones de dólares y el PIB mundial de 84,5 trillones (Collins, 2022). De forma que, la industria de las criptomonedas representaría alrededor de un 1% de las finanzas globales, lo que resulta una cifra favorable en un panorama en el que las criptomonedas se presentan como un sector que puede facilitar el delito (Collins, 2022).

Sin embargo, todavía en la actualidad existen discrepancias en cuanto al volumen de la actividad con criptomonedas que pertenece al ámbito de la delincuencia. Las estimaciones sobre la proporción de pago con criptomonedas vinculadas a delitos financieros pueden variar entre el 0,15 al 46% (Schickler, 2022). Las diferencias que pueden existir en la determinación del volumen de delitos se deben a las formas tan diversas que existen para medir este tipo de delincuencia. De forma general, las investigaciones realizadas en este sentido se encargan de detectar aquellas direcciones criptográficas sospechosas de haber cometido un delito y estudiar el volumen de transacciones realizadas (Schickler, 2022). Esto es, no se identifican aquellos autores que han estado involucrados en la realización del delito, sino que las estimaciones están basadas en el volumen de actividad de direcciones señaladas como sospechosas.

Generalmente, la estimación del volumen y la gravedad de este tipo de criminalidad son realizados por empresas privadas encargadas del estudio de la *Blockchain* con fines de ciberseguridad. A lo largo del año 2020 se registraron 7,8 billones de dólares que habían sido enviados a direcciones ilícitas, lo que denotaba cierto crecimiento de los delitos basados en criptomonedas con respecto al año anterior. Este crecimiento ha continuado en el año 2021, para el que se ha alcanzado un máximo histórico con una cifra de 14 billones dólares (Chainalysis, 2022). Sin embargo, al mismo tiempo, en el año 2021 se registró un aumento generalizado del uso de las criptomonedas, con un volumen de transacciones de 15,8 trillones de dólares, lo que supone un crecimiento del 567% con respecto al año anterior (Chainalysis, 2022). Esto viene a significar que, aunque en el año 2021 las transacciones ilícitas aumentaron un 79%, en realidad al realizar el ajuste solo se trataría del 0,15% del volumen de transacciones de criptomonedas para el año 2021 (Chainalysis, 2022).

Por su parte, en una investigación en colaboración con la empresa “Elliptic” en materia de blanqueo de capitales se mostró que, a lo largo de los cuatro años de análisis, la fuente de alrededor del 97% de los bitcoins ilegales eran mercados de la *Darknet* (DN)

(Fanusie y Robinson, 2018). Además, el 45% iba destinado a casas de cambio, pero el resto fue destinado a casas de apuestas (25,79%) y servicios de mezclado de criptomonedas (23,40%) (Fanusie y Robinson, 2018).

Otros investigadores han realizado diferentes estimaciones como Foley et al. (2019) que determinaron que la cuarta parte de los usuarios de Bitcoin están involucrados en actividades ilícitas, es decir el 46% de las transacciones de la moneda (76 mil millones de dólares). La diferencia de estos resultados con los de la empresa privada reside en los criterios que han empleado para considerar las direcciones Bitcoin estudiadas. Así, Foley et al. (2019) no se han limitado únicamente a cuantificar la actividad de las direcciones marcadas como sospechosas, sino que han estudiado la red y los comportamientos de los usuarios.

Pero hay otros inconvenientes en las estimaciones de este tipo de criminalidad y es que, por ejemplo, no se consideran aquellos delitos que se desarrollan fuera de los dispositivos y que utilizan criptomonedas como, por ejemplo, la utilización del dinero obtenido a través del tráfico de drogas para la compra de criptomonedas (Schickler, 2022). También en este ámbito hay que considerar el año al que pertenece el estudio consultado, ya que en la investigación de Foley et al. (2019) se ha trabajado con datos pertenecientes al 2017, lo que podría explicar la discrepancia con estudios posteriores e indicar una necesidad de actualización para poder llegar a conclusiones más precisas.

No obstante, aunque sería necesario estimar el volumen de estos delitos para determinar su gravedad, se puede afirmar que el volumen de este tipo de criminalidad no ha superado todavía a los delitos que se cometen utilizando dinero fiduciario (Butler, 2019).

Aspectos que Pueden Favorecer su Utilización en el Crimen

La utilización de las criptomonedas en la criminalidad está aumentando, así como su adopción como forma de pago. No obstante, el número de delitos y de transacciones realizadas con esta tecnología siguen representando una parte limitada de la economía en comparación con el dinero en efectivo y otras formas de pago (Europol, 2022a).

Las criptomonedas han resultado ser útiles para el desarrollo de ciertos delitos, pero atendiendo al panorama actual, resulta demasiado simple considerarlas como una tecnología “excelente” para este propósito, cuando en realidad son un método más de pago (Butler, 2021). Hay muchos usos delictivos que se le podrían dar a las criptomonedas. Pueden ser métodos de pago que sustituyan al dinero en efectivo, o pueden usarse como la forma digital del dinero para realizar transacciones *online* (Butler, 2019). Con su aparición se

ofrecían por primera vez las características del dinero físico de forma digital: transferencia de valor sin intermediarios, de forma descentralizada y persona a persona (Palomo-Zurdo, 2021, p.32).

Por ello, para determinar la gravedad de los delitos cometidos con criptomonedas en el panorama delictivo al completo habría considerar a las criptomonedas en perspectiva con otros métodos de comisión del delito como el dinero fiduciario (Butler, 2019). El dinero en efectivo también ha llegado a considerarse como un facilitador de ciertos tipos de delitos.

Las criptomonedas han sido denominadas en muchas ocasiones como "efectivo digital" y es que el propósito con el que se crearon buscaba imitar algunas de las propiedades del dinero en efectivo (Nakamoto, 2008). las criptomonedas se pueden asemejar al dinero en efectivo debido a sus tres funciones: medio de intercambio, reserva de valor y unidad de cuenta), Además, de la misma forma que el dinero en efectivo, las transacciones realizadas con criptomonedas son irreversibles, ya que no hay intermediarios que puedan restablecerlas. No obstante, en el caso de las criptomonedas las transacciones no son anónimas, sino pseudonanónimas, es posible conocer las direcciones de entrada y salida (Butler, 2019). Mientras que el dinero en efectivo es realmente anónimo, esto es, excepto por los números de serie, es un instrumento al portador, cualquiera que lo posea es su propietario y no hay mecanismos de grabado de las transacciones realizadas (Butler, 2019). Al mismo tiempo, el dinero en efectivo presenta ventajas como un bajo coste, no se necesita una cuenta bancaria ni tener un saldo mínimo o pagar tarifas de mantenimiento, no requiere de una conexión a internet, línea telefónica o incluso electricidad para gastarlo o recibirlo y, sobre todo, otorga un importante grado de privacidad financiera comparado con algunas formas de pago digitales y aquellas que ofrecen los bancos (Hendrickson y Luther, 2022, p.201).

En cuanto a la parte logística del desarrollo de algunos delitos el dinero en efectivo también presenta algunos inconvenientes en relación con las criptomonedas. Su utilización dificulta las transacciones de cantidades elevadas y requiere que ambas partes estén presentes físicamente (Hendrickson y Luther, 2022). Además, es pesado y su transporte supone un reto para los criminales. Por ejemplo, 1 millón en billetes de 500 euros pesa 2 kg, mientras que en billetes de 20 libras pesaría 50 kg (Casciani, 2010). A lo largo de los años, las autoridades han observado, que muchos de los billetes de gran denominación, no son usados en transacciones ordinarias, mientras que sí que eran herramientas útiles para los delincuentes (Casciani, 2010). Por todo ello, se consideró que el efectivo era un facilitador del delito y que debía de limitarse su utilización en muchos casos para reducir la actividad criminal. Este es el caso de

la eliminación del billete de 500 euros a partir del año 2019 porque se consideraba que facilitaba el desarrollo de actividades delictivas (Banco Central Europeo, 2023).

También se han encontrado propuestas en las que se plantea la eliminación total del dinero en efectivo. Sin embargo, de forma paradójica, se ha estudiado de forma empírica una proximidad entre el dinero en efectivo y las criptomonedas, de forma que aquellas medidas que proponen la eliminación del dinero en efectivo para luchar contra la criminalidad podrían ocasionar el desplazamiento a otras formas de pago similares, como la utilización de criptomonedas (Hendrickson y Luther, 2022, p.206).

Se considera por lo tanto que el dinero fiduciario, en particular, el dinero en efectivo constituye una amenaza mayor en la lucha contra la criminalidad que las criptomonedas. Si bien es cierto que se utiliza la tecnología para la comisión de delitos su utilización es muy baja en comparación con otros métodos como la utilización del dinero fiduciario (Butler, 2019). Este permanece como una amenaza latente en el delito de blanqueo de capitales, ya que sigue siendo fácilmente intercambiable, relativamente irrastreable y pseudoanónimo, de la misma forma que las criptomonedas, pero con la diferencia de que estas no han sido adoptadas por un grupo tan numeroso de delincuentes (Europol, 2017). Es muy dudoso que las criptomonedas acaben por sustituir a todos los métodos de pago que existen, no se debería entonces considerar como la amenaza que se suele presentar, y se debería de mantener el foco en la utilización del dinero efectivo en la actividad criminal (Butler, 2019).

Sin embargo, más interesante que el estudio del volumen de estos delitos resultaría el estudio de las motivaciones para su utilización en la criminalidad. Esto es, por qué algunos delincuentes han considerado la incorporación de esta tecnología en el desarrollo de sus actividades delictivas.

Se han realizado estudios sobre el uso de los usuarios de Bitcoin en un ámbito legal. Este es el caso por ejemplo de Bashir et al. (2016), que determinó que la utilización de la moneda estaba más motivada por la novedad de la tecnología e ideologías libertarias que por su anonimato; Zouhair y Kasraie (2019), que hallaron que los factores motivadores de la posesión de criptodivisas fueron las finanzas y la tecnología innovadora (Fintech) con el fin de obtener beneficios; y de Murko y Vrhovec (2019) que además de la utilidad, la facilidad de uso y la norma subjetiva hallaron que influía en la adopción de Bitcoin la confianza en la seguridad.

Pero estas consideraciones no podrían trasladarse directamente a aquellos usuarios de actividades ilegales, que usan foros clandestinos y la red oscura. Desde una perspectiva preventiva es importante comprender las motivaciones políticas o financieras detrás del

desarrollo de las criptomonedas, las oportunidades ilegales y amenazas, así como su inconsistencia legal y reglamentaria (Kethineni y Cao, 2020).

La obtención de este conocimiento supondría la realización de entrevistas con usuarios de las criptomonedas que las hayan utilizado en el desarrollo de algún delito. Sin embargo, hasta la fecha no se ha realizado ningún estudio que permita conocer con exactitud aquellos aspectos de las criptomonedas que motivan a los criminales a utilizar esta tecnología en sus delitos. No obstante, muchos autores han señalado algunas de las características de la moneda virtual como las responsables de atraer a la criminalidad (Ali et al., 2015; Brown, 2016; Kethineni y Dodge, 2018).

Se considera que los criminales utilizarán las criptomonedas, especialmente el Bitcoin que se ha convertido en un objeto para el delito y en una herramienta atractiva para los criminales atraídos por los mismos aspectos que atraen a aquellos usuarios que las utilizan de una forma legal y que han marcado su éxito (Ali et al., 2015). Tradicionalmente se considera que las propiedades clave de estas que han influido en la decisión de los criminales son: anonimato (o pseudoanonimato), velocidad, bajo costo (generalmente), descentralización (sin terceros), auto-soberanía, inmutabilidad de la cadena de bloques y la finalidad (Butler, 2019). Al mismo tiempo, Brown (2016) considera que la falta de regulación y su potencial anonimato son útiles para la actividad delictiva y la convierte en un riesgo existente o al menos potencial. Así, consideran que amenazas delictivas como el lavado de dinero, la evasión de impuestos y otras amenazas como la explotación de la red Bitcoin derivan directamente de su naturaleza anónima y sin confianza, así como de la falta de regulación (Ali et al., 2015). En materia de blanqueo de capitales se consideran facilitadores de la delincuencia la descentralización[130], la privacidad de las transacciones[131], la irreversibilidad[132] y la flexibilidad[133], además de las características propias de la delincuencia

[130] En relación con esto, la nueva directiva orientada a la prevención del blanqueo de capitales va en la línea de determinar medidas para los intermediarios en el negocio de las criptomonedas, como las casas de cambio o *exchanges*. No obstante, en relación con esto, parece no ser suficiente para conseguir frenar considerablemente esta actividad, ya que como se ha expuesto en reiteradas ocasiones, la arquitectura de criptomonedas como Bitcoin permiten operar directamente entre sus usuarios, siendo innecesaria en estos casos, la presencia de intermediarios.

[131] Ciertamente se trata de una pseudonimia y no de un anonimato, ya que como se ha demostrado en estudios como los de (Meiklejohn et al., 2016), se puede seguir el rastro de las transacciones de Bitcoin.

[132] Esta característica ha sido señalada por la UNODC como una de las más relevantes en esta actividad delictiva. Esta irreversibilidad no solo se refiere a la seguridad que le otorga al autor del delito la imposibilidad de retirada de los fondos una vez ya transferidos por la víctima, sino que también dificulta la labor de las fuerzas del orden, reduciendo la investigación a dos opciones (Pérez López, 2017).

[133] Con esto se refiere a que un token, que puede moverse de forma instantánea por la red, podría materializarse si se requiere y almacenarse en un disco duro con el objetivo de salvarlo de cualquier intervención que pudiera

como la instantaneidad, la distancia entre el infractor y el lugar de comisión, el carácter transfronterizo y la inmaterialidad (Pérez López, 2017). Al mismo tiempo, una mayor adopción de las monedas virtuales por parte de las empresas puede ocasionar un mayor espacio de oportunidad para los criminales para emplear las criptomonedas en sus actividades delictivas, obstaculizando la utilización legal (Kethineni y Cao, 2020). Pero no solo en relación con la criptomoneda Bitcoin, ya que, en Ethereum, el desarrollo de *Smart Contracts* también podría fomentar el desarrollo de ciertos tipos de actividades delictivas (Juels et al., 2016) ya que permite asegurar la ejecución de un contrato entre las partes sin intermediarios.

Anonimato

En relación con el anonimato se ha considerado una de las características del Bitcoin más comentadas como facilitador de la actividad criminal. Esta característica consiste en la dificultad de establecer la identidad del usuario que está utilizando una dirección Bitcoin.

Aunque se ha utilizado con frecuencia este término en el ámbito de las criptomonedas, en realidad no se trata de un anonimato al completo, sino de un pseudoanonimato. Esto es, es posible conocer toda la actividad que ha realizado un usuario con Bitcoin si se dispone de información adicional que vincule a este usuario con la dirección de su cartera. En este sentido, diversas investigaciones como Androulaki et al. (2013), Ron y Shamir (2013) y Meiklejohn et al. (2013) han demostrado que el anonimato en la red Bitcoin no es total y que se pueden establecer patrones de actividad e identificar a determinados usuarios. De esta forma, la utilización de técnicas de análisis de la *Blockchain* como la re-identificación o el volcado de sitios web permiten identificar a los usuarios que han utilizado Bitcoin cuya actividad permanece de forma pública en la *Blockchain*.

Estas técnicas y otras similares han dejado entrever que criptomonedas de carácter público como Bitcoin no resultarían a priori tan adecuadas para el desarrollo de determinadas actividades delictivas como, por ejemplo, el blanqueo de dinero. Existen empresas que se dedican profesionalmente al análisis de la *Blockchain* de Bitcoin para ofrecer datos, soluciones o servicios a aquellos usuarios interesados en el conocimiento de la *Blockchain* como agencias gubernamentales, instituciones financieras, compañías de seguros, investigadores en ciberseguridad, etc. Un ejemplo de ello son las empresas "Chainalysis"[134],

realizarse en la red y con una alta probabilidad de no ser interceptado por las fuerzas y cuerpos de seguridad en su transporte (Pérez López, 2017, p. 155).

[134] Chainalysis https://www.chainalysis.com/es/

"Elliptic"[135] o "Ciphertrace"[136]. La primera de ellas elabora un informe con carácter anual sobre los delitos cometidos con criptomonedas o "criptodelitos" como se denominan en estos informes (Chainalysis, 2022). La empresa "Elliptic" también ha participado en el estudio de la criminalidad cometida con criptomonedas. En concreto participó en el estudio del blanqueo de capitales en el que aportó su herramienta de análisis forense que combinaba datos públicos de la *Blockchain* con un conjunto propio de direcciones Bitcoin asociadas a entidades conocidas. La empresa también aportó direcciones marcadas como perteneciente a entidades ilícitas, como mercados de la *Darknet*, *ransomware* y actividades fraudulentas (Fanusie y Robinson, 2018).

Todo ello ha llevado a pensar que el anonimato no debería ser la característica de las criptomonedas que más atraiga a los criminales (Butler, 2019). Si fuera esta la característica que condiciona principalmente a los usuarios para cometer delitos, los sujetos interesados habrían apostado por la utilización de criptomonedas alternativas, especialmente por aquellas de carácter privativo como Monero. Se conoce la utilización de criptomonedas alternativas como Litecoin, que se adoptaron en ocasiones en las que el aumento de la popularidad de Bitcoin ocasionó un aumento del coste en las transacciones y una baja velocidad (Barysevich y Solad, 2018). No obstante, este tipo de criptomoneda es de carácter público como Bitcoin, lo que sugiere que características como el coste o la velocidad de las transacciones han importado más a los usuarios de los foros que el anonimato que pudieran conseguir con la utilización de otra criptomoneda (Barysevich y Solad, 2018).

Al mismo tiempo, las criptomonedas "Monero" y "Zcash", mayormente conocidas por su carácter privado han sido objeto de varias investigaciones en las que se ha estudiado si es tal el anonimato que garantiza su utilización. En el caso de la criptomoneda "ZCash" se ha visto que la utilización que hacen los usuarios de la moneda limita la obtención del anonimato ya que o bien no hacen uso de sus principales propiedades de privacidad o bien hacen uso de estas de una forma que pone riesgo el anonimato de otros usuarios reduciendo el anonimato de conjunto (Kappos et al., 2018). En cuanto a Monero, se ha demostrado una posible debilidad del conjunto de anonimato como métrica de privacidad, ya que en un análisis pasivo de su *Blockchain* se pudieron trazar alrededor del 87% de sus entradas (Kumar et al., 2017). Todo ello, deja entrever la posibilidad de que las criptomonedas de carácter privado pueden presentar en ocasiones riesgos a para la privacidad de la actividad, de forma

[135] Elliptic https://www.elliptic.co/
[136] Ciphertrace https://ciphertrace.com/

que no siempre puede vincularse su utilización con un anonimato total. No obstante, aunque existan criptomonedas que puedan garantizar una mayor privacidad que Bitcoin, hasta la fecha ninguna de las criptomonedas alternativas ha mostrado una utilización mayor que Bitcoin. En el ámbito de su utilización legal, la criptomoneda Bitcoin es la más utilizada y al mismo tiempo, en el ámbito del crimen se ha visto una mayor utilización del Bitcoin debido a la confianza, familiaridad y aceptación más amplia por parte de los usuarios (Kethineni y Cao, 2020).

Al mismo tiempo, hay que puntualizar, que las criptomonedas de carácter privado no aseguran el anonimato total en todo caso. De la misma forma que al utilizar otras herramientas que garantizan la privacidad de la actividad como puede ser TOR (Irwin y Turner, 2018), lo realmente importante de esta tecnología no es el anonimato que pudiera garantizar, sino que el usuario que la utiliza disponga de la habilidad necesaria para conseguirlo. De este modo, el riesgo de este tipo de criminalidad reside por tanto en aquellas formas de utilizar las criptomonedas que permiten seguir manteniendo el anonimato de los usuarios. Algunas de ellas ya se recogían en un informe elaborado en el año 2012 por el FBI (Zetter, 2012). Se pueden señalar, por ejemplo, la creación y uso de nuevas direcciones Bitcoin para cada uno de los pagos realizados, la utilización de programas de anonimización, combinar el saldo de antiguas direcciones de Bitcoin con nuevas direcciones para realizar pago, utilizar servicios especializados en el blanqueo de capitales y utilizar un servicio de cartera electrónica de terceros para consolidar direcciones y crear diversos clientes de Bitcoin (Zetter, 2012).

Esta concepción sobre el anonimato en la utilización de las criptomonedas para la comisión del delito ya es conocida por muchos de los usuarios. Esto se puede ver en investigaciones que estudian las discusiones sobre esta materia en la que los usuarios exponen conocer que el anonimato completo no es posible, sino que se debe aspirar a conseguir la máxima seguridad posible, sin que esta dependa únicamente del método de pago empleado, sino que se logra con la combinación de una serie de medidas (Butler, 2021). En un estudio longitudinal, se ha visto incluso una capacidad de aprendizaje por parte de los usuarios que a lo largo de los años han mostrado una evolución en sus mensajes sobre el anonimato de esta moneda y sobre tecnología como los *mixers* o *tumblers* (Butler, 2021). En cuanto al tipo de criptomonedas empleada, se observó una preferencia en la utilización de Bitcoin sobre otras criptomonedas como Monero, debido entre otras, a cuestiones relacionadas con la disponibilidad de la criptomoneda y la dificultad de uso (Butler, 2021). Además, también se vio que los usuarios son capaces de adaptar sus métodos para poder

utilizar diferentes criptomonedas o incluso continuar con el dinero en efectivo, que sigue teniendo una mayor importancia en las actividades delictivas (Butler, 2021). Por lo tanto, se obtuvo como resultado que el anonimato parecía no ser la principal ventaja de la utilización de las criptomonedas, sino la finalidad que tienen (Butler, 2021). Esto coincide con los resultados obtenidos en otras investigaciones como la de Murko y Vrhovec (2019) que hallaron que ni el anonimato del Bitcoin ni la amenaza de ser víctima de una posible estafa eran factores que influyeran en la adopción de la criptomoneda Bitcoin por parte de los usuarios.

Por todo ello, aunque en capítulos próximos se discute con más detalle, son varios los motivos aquí presentados por los que habría que cuestionar que el anonimato de las criptomonedas sea una característica determinante para su utilización en la criminalidad. En primer lugar, porque en aquellas criptomonedas de carácter público como Bitcoin no existe un anonimato, sino un pseudoanonimato, de forma que con la obtención de información adicional se puede conocer toda la actividad que un usuario ha realizado con esta criptomoneda. En segundo lugar, porque existen indicios que pueden señalar que esta característica no es la preferida por los criminales para la implementación de las criptomonedas en sus actividades delictivas. Por un lado, porque la utilización de criptomonedas de carácter público como Bitcoin es mayor que el uso de criptomonedas de carácter privado como Monero, que garantizarían una mayor privacidad en el desarrollo de la actividad delictiva. Por otro lado, porque, aunque la utilización de criptomonedas en la criminalidad parece haber aumentado en los últimos años, todavía no ha superado al uso de otras formas de pago tradicionales como es el dinero en efectivo. Al mismo tiempo, existe una gran cantidad de delitos que tienen lugar tecnología de anonimización, ni formas de pago anónimas, por lo que la utilización de criptomonedas parece no ser determinante para la comisión de cierto tipo de delitos.

Ausencia de un Marco Normativo Especializado

La ausencia de una regulación uniforme a nivel nacional e internacional en materia de criminalidad y criptomonedas se ha señalado también como otro aspecto de esta tecnología que pudiera estar favoreciendo su utilización en el crimen. Se considera que este hecho supone un riesgo para el sector financiero, pudiendo fomentar delitos como el lavado de dinero, el fraude, la evasión de impuestos y otros (Kethineni y Cao, 2020).

En este ámbito serán los gobiernos de los diferentes países los que de forma discrecional deberán prohibir o restringir, si fuera el caso, la operativa con criptoactivos. En

la Unión Europea, no existe un marco que regule los criptoactivos como el Bitcoin y que pueda garantizar a sus usuarios protección y garantías. Las criptomonedas como los bitcoins no tienen curso legal y no hay ningún requisito para su aceptación por parte de gobiernos y países, por lo que esta falta de regulación y supervisión ocasiona que no haya protección para los consumidores (Choo, 2015). En su lugar, la forma que se ha tenido hasta el momento de responder ante este tipo de criminalidad ha sido utilizar lo que ya se recoge en el ámbito legislativo en lo referente a la lucha contra el blanqueo de capitales y financiación del terrorismo. Esto es, las autoridades nacionales y europeas serán las que tendrán que modificar los marcos legislativos que disponen para poder abordar las cuestiones relativas a las monedas virtuales. Algunos autores han señalado incluso que esta situación constituye un "riesgo regulatorio", que se manifiesta de forma imprevista en forma de prohibiciones, nuevos mecanismos de control, sanciones tributarias, etc. (Palomo-Zurdo, 2021, p. 21).

En este sentido, se debe intentar que las respuestas establecidas no sobrecarguen la innovación financiera con una regulación excesiva, ni restringir el crecimiento de la tecnología al mismo tiempo que se asegure que no se eludan los reglamentos (Kethineni y Cao, 2020). La regulación de este ámbito deberá hallar el límite entre la limitación total de la actividad con criptomonedas y la evitación de la utilización de las criptomonedas en el ámbito delictivo. Esta tarea supondrá sin duda una revolución tecnológica y por tanto la solución establecida, además de lo señalado anteriormente, deberá tener un carácter dinámico y transnacional, que evite tendencias regulatorias de dudosa justificación (Palomo-Zurdo, 2021).

A tal efecto, la cuestión regulatoria se verá influenciada por la consideración que cada país tenga sobre esta tecnología. Hay países que se han mostrado contrarios a la adopción de las criptomonedas como China, Brasil e India. Por el contrario, en Japón y Corea se utilizan de forma masiva, aunque su marco regulatorio no está muy definido. En el año 2021, nueve países incluyendo China, Egipto, Marruecos, Argelia, Túnez, Bangladesh, Nepal, Irak y Catar prohibieron completamente el uso de criptomonedas (The Law Library of Congress, 2021). Otros países, limitaban su utilización de forma implícita a través de otro tipo de como las restricciones bancarias. Estos son Baréin, Benín, Bolivia, Burkina Faso, Burundi, Camerún, República Centroafricana, Chad, Costa de Marfil, República Democrática del Congo, Ecuador, Gabón, Georgia, Guyana, Indonesia, Jordania, Kazajistán, Kuwait, Líbano, Lesoto, Libia, Macao, Maldivas, Malí, Moldavia, Namibia, Níger, Nigeria, Omán, Pakistán, Palaos, Arabia Saudí, Senegal, Tayikistán, Tanzania, Togo, Turquía, Turkmenistán, Emiratos Árabes, Vietnam y Zimbabue (The Law Library of Congress, 2021). Por el contrario, otros países

lejos de prohibir la utilización de cualquier tipo de criptomoneda han impulsado proyectos para crear su propia moneda virtual al mismo tiempo que el resto de los países elaboraban anteproyectos de ley y marcos regulatorios. En algunos casos estas decisiones se deben a razones políticas y de control del capital, mientras que en otros casos el gobierno las utiliza para facilitar la consecución de objetivos geopolíticos o eludir los controles de capital externos (Collins, 2022).

La Unión Europea de forma general, ha mostrado una predisposición a su utilización y disposición de las criptomonedas, motivada por la adopción de la innovación en la cadena de bloques. No obstante, el hecho de que no haya una medida legislativa o reglamentaria en esta materia no significa que no se hayan realizado diversos pronunciamientos de autoridades competentes sobre los riesgos de esta tecnología. En este sentido, la Unión Europea muestra una postura basada en advertir a los usuarios de esta tecnología sobre los riesgos que pudiera presentar como es el caso de los inversores (González, 2021). Pero no solo en cuanto a la inversión, el Banco de España ha señalado otros riesgos de la utilización de las criptomonedas como la financiación de actividades ilícitas y/o blanqueo de capitales, los efectos reputacionales negativos que puedan surgir sobre los medios de pago digitales, las posibles transacciones fraudulentas y el impacto en la estabilidad de los precios y en la estabilidad financiera (Gorjón, 2014). Se deberá mejorar la formación e información en nuevas tecnologías de la sociedad digital para que los ciudadanos de la UE sean capaces de tomar sus propias decisiones al respecto de esta materia (Palomo-Zurdo, 2021, p.26).

En España, no hay una prohibición absoluta ni implícita de las criptomonedas, aunque sí que están sujetas a lo expuesto en la legislación fiscal (sobre el IVA y el impuesto sobre la renta) y en la legislación en materia de blanqueo de capitales y financiación del terrorismo. En relación con la última, la primera regulación relevante sobre "monedas virtuales" tuvo lugar con el "Real Decreto-ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención del blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores". En su contenido trata temas como el cambio entre monedas virtuales y monedas tradicionales y sobre los depositarios de estos activos (monederos electrónicos) (Palomo-Zurdo, 2021, p. 24). En el momento actual se mantiene la legislación anterior en materia de blanqueo de capitales y financiación del terrorismo para abordar la criminalidad en la que se utilizan criptomonedas. El tratamiento regulatorio que se

le da a los delitos de blanqueo de capitales y de financiación del terrorismo con criptomonedas será recogido en apartados posteriores de este trabajo.

Actualmente, se prevé una regulación a nivel europeo conocida como MiCA *(Markets in Crypto Assets)* o Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937. Este tiene como propósito constituirse como un marco legal para los criptoactivos que sea favorable a la innovación y no suponga obstáculos para la aplicación de nuevas tecnologías, protegiendo a consumidores e inversores y la integridad del mercado (Comisión Europea, 2020, p.1)[137]. La propuesta ya ha sido aprobada por el Parlamento Europeo por lo que se espera que las empresas comiencen a aplicarla en el año 2024. En su artículo 2 expone que se dirige a toda persona que emita criptoactivos o preste servicios relacionados con los criptoactivos en la Unión salvo las excepciones contempladas en el segundo punto (Comisión Europea, 2020).

El Reglamento establece normas uniformes en relación con (Comisión Europea, 2020):

a) requisitos de transparencia e información en relación con la emisión y la admisión a negociación de criptoactivos; b) autorización y supervisión de los proveedores de servicios de criptoactivos, los emisores de fichas referenciadas a activos y los emisores de fichas de dinero electrónico; c) funcionamiento, organización y gobernanza de los emisores de fichas referenciadas a activos, los emisores de fichas de dinero electrónico y los proveedores de servicios de criptoactivos; d) normas de protección de los consumidores en relación con la emisión, la negociación, el canje y la custodia de criptoactivos y e) medidas dirigidas a prevenir el abuso de mercado, con el fin de garantizar la integridad de los mercados de criptoactivos (p. 37).

Sin embargo, de la misma forma que se ha comentado anteriormente en el apartado relativo al anonimato, la ausencia de una regulación unánime en esta materia no determinará necesariamente la comisión de delitos con criptomonedas. Aunque puede tratarse de un elemento que favorezca la criminalidad en este sentido, no se puede asumir que los criminales que utilizan criptomonedas estarán motivados en todo caso por una regulación inconsistente o difusa en sus países. Esta suposición estaría considerando que los criminales son conocedores de la legislación y de los diferentes marcos normativos en esta materia. Por ello, será necesario un estudio que determine si este tipo de características atraen y motivan a los criminales en la utilización de criptomonedas.

[137] REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020PC0593&from=ES

Capítulo 6. Delitos en los que Intervienen las Criptomonedas. Criptocrimen.

Las criptomonedas se han posicionado como una tecnología que se utiliza en la criminalidad. Sin embargo, resulta una tara compleja recoger todos aquellos delitos en los que pueden intervenir estas monedas virtuales. Esto puede deberse a las dificultades que existen para detectar este tipo de criminalidad, que presenta una elevada cifra negra. Al mismo tiempo esto ha dificultado la existencia de investigaciones de carácter empírico que tengan como propósito estimar el volumen total de criminalidad que sucede en este sentido.

De esta forma, para recoger aquellos delitos en los que se suelen utilizar las criptomonedas se tendrán que utilizar fuentes de carácter público que hayan registrado este tipo de delitos una vez conocidos. Con dicho fin, en este trabajo se ha empleado la jurisprudencia penal española, los informes de empresas de carácter privado encargadas del análisis de la *Blockchain*, informes de agencias gubernamentales y FCSE, noticias digitales y prensa elaborada por la FCSE (Guardia Civil y Policía Nacional) y órganos encargados de la lucha contra la delincuencia como Europol.

Como resultado del estudio de estas fuentes en cuanto a criminalidad y criptomonedas, se pueden realizar las siguientes observaciones. Por un lado, se han obtenido delitos considerados como tradicionales en los que se han introducido las criptomonedas entre sus formas de actuación. Por otro lado, se han obtenido ciberdelitos en los que la introducción de las criptomonedas ha supuesto un cambio sustancial en la forma en la que se desarrolla.

En relación con esto, muchos autores han denominado "criptocrimen" a la criminalidad cometida con criptomonedas. En inglés se denominaría *cryptocrime* o *bitcoin-related crimes* o *Cryptocurrency-based crime.* Esto es controvertido ya que para utilizar dicho término habría que considerar qué tipo de delitos se incluyen dentro de esta categoría, si solo aquellos que son posibles gracias a la utilización de las criptomonedas o también se incluirían aquellos delitos en los que las criptomonedas solo han supuesto la puesta a disposición de otro medio comisivo. Si se considera que se trata de un tipo de delincuencia específica que solo puede desarrollarse con criptomonedas, habría que realizar previamente un estudio sobre todos los delitos en los que interviene esta tecnología y seleccionar aquellos que solo son posibles gracias a su utilización. No obstante, esta perspectiva presenta un carácter muy limitado, ya que excluiría a una gran cantidad de delitos que, si bien, se cometían con anterioridad a la aparición de las criptomonedas, han experimentado cambios relevantes con la introducción de esta tecnología. Este es el caso de los ataques *ransomware*

que, aunque anteriormente exigían el pago del rescate a través de "Paysafecard", "Ukash" y "Moneypak", la introducción de las criptomonedas cambió su *modus operandi* para mejorar su anonimato y aumentar los beneficios y este cambio se ha mantenido hasta la actualidad (Anderson et al., 2019).

Una de las primeras investigaciones en las que se introduce el término "criptocrimen" es en Ivantsov et al. (2019) en la que se considera como un conjunto de actos socialmente peligrosos cometidos en relación con o con el uso de productos de registros distribuidos (Criptodivisas, tokens y otras formas de activos financieros digitales). Se trata de esta forma, de un concepto amplio en el que se incluirá todo aquel delito en el que se hayan empleado estas tecnologías para su comisión. La amplitud del concepto se apoya además por la consideración de los autores de que los tres sectores del criptocrimen son la venta ilegal de sustancias psicoactivas, el blanqueo de productos del delito y el robo de criptomonedas y otros delitos contra la propiedad (Ivantsov et al., 2019). También se han encontrado otros ejemplos con Anderson et al., (2019) que hace referencia a delitos como ataques *ransomware*, estafas Ponzi y *malware* de criptominado, en los que el uso de criptomonedas como Bitcoin les ha beneficiado. De esta forma, en esta consideración también se observan delitos de carácter tradicional que anteriormente se desarrollaban sin la incorporación de ningún tipo de producto de registro distribuido.

Por lo tanto, en lo que se refiere al desarrollo del presente trabajo, en línea con lo expuesto anteriormente se mantendrá una postura amplia del criptocrimen en la que se incluirán todos aquellos delitos en los que hayan intervenido las criptomonedas de alguna forma. Al mismo tiempo, en este trabajo no se tiene como objetivo elaborar un listado exhaustivo de todos los delitos en los que intervienen las criptomonedas, sino que, a partir del estudio de las fuentes de información mencionadas anteriormente, se pretende mostrar algunos de los delitos que más frecuentemente se han señalado dentro del criptocrimen y exponer la forma en la que las criptomonedas han influido en su desarrollo.

Con este fin, diversas investigaciones han señalado varios tipos de delitos en los que han intervenido las criptomonedas. Así, se han visto un elevado número de casos conocidos de delitos como el lavado de dinero (Roy, 2014)[138], estafas piramidales o esquemas Ponzi

[138] Caso de Charles Shrem director ejecutivo del intercambio de Bitcoin "BitInstant" fue condenado por un delito de prisión por lavar millones de dólares a través de la compra de Bitcoin y que permitió la compra de drogas y otros productos derivados a los usuarios de *Silk Road* (Roy, 2014).

(Sonawane, 2015)[139], compraventa de productos ilegales p.ej. drogas en la *Darknet* (Aldridge and Décary-Hétu, 2014; Greenberg, 2016[140]; Martin, 2014; Ivantsov et al., 2019), la financiación de grupos terroristas (Nauert, 2015)[141] , ataques *ransomware* y utilización de *botnets* (Highbee, 2018), mercados negros, extorsión y *malware* (Ali et al. 2015) y otros delitos contra la propiedad (Ivantsov et al., 2019). Pero no solo se ha convertido en una herramienta útil para el desarrollo de la delincuencia, sino que también ha supuesto un objeto atractivo para los criminales (Ali et al., 2015), por lo que también se han visto casos de robo de criptomonedas (Ali et al., 2015).

La empresa Chainalysis (2020) señala los fondos robados y las estafas como los delitos más cometidos con criptomonedas durante el año 2021. Aunque se ha visto la utilización de esta tecnología en una gran variedad de delitos, son los delitos contra la propiedad aquellos en los que se ha visto una mayor implicación de las criptomonedas (Kethineni y Cao, 2020).

También se han relacionado las criptomonedas con diversos delitos en los informes elaborados anualmente por Europol, como por ejemplo la compraventa en mercados delictivos, el pago de material pornográfico infantil, el blanqueo de capitales, fraudes de inversión, entre otros (Europol, 2021).

A continuación, se explicarán con más detalle algunos de los delitos en los que se ha observado más frecuentemente la utilización de las criptomonedas:

El Blanqueo de Capitales Mediante la Utilización de Criptomonedas

Son muchas las causas que favorecen la existencia y continuidad de las prácticas de blanqueo de dinero, como son la globalización, las tecnologías y las redes sociales, la tardía criminalización de esta actividad, la estrecha relación entre blanqueo y corrupción, la existencia de paraísos fiscales y centros *offshore* o extraterritoriales, la falta de concienciación por parte de ciertos profesionales, la falta de colaboración internacional y la crisis bancaria y la necesidad de liquidez (España Alba, 2016). Como parte de estos factores

[139] Trendon Shavers de Texas protagonizó la conocida como el primer fraude criminal de valores de los Estados Unidos cometido con Bitcoin (Sonawane, 2015). Estafó alrededor de 4,5 millones de dólares a través de la empresa "Savings and Trust" entre 2011 y 2012. Garantizaba a los inversores una ganancia del 1% con la inversión en bitoins, pero en su lugar, se empleaba esta ganancia para pagar a los antiguos inversores. Shavers llegó a controlar un 7% de todos los bitcoins en circulación (Sonawane, 2015).

[140] Ross Ulbritcht dirigía *Silk Road*, el criptomercado más importante de la historia de venta de drogas *online* en la *Darknet* y que cesó su actividad en el año 2013 por la detención de Ulbritch al que se le condenó a 30 años de prisión (Greenberg, 2016).

[141] El grupo de expertos en tecnología *Ghost Security* identificó las cuentas Bitcoin como una de las principales fuentes del terrorismo islámico, siendo la moneda virtual entre el 1 y el 3 por ciento de sus ingresos totales, lo que supone entre 4,7 y 15,6 millones de dólares (Nauert, 2015).

facilitadores, fruto de la globalización y el avance de las nuevas tecnologías, las criptomonedas se han posicionado como una herramienta que facilita el desarrollo del delito de blanqueo de capitales convirtiéndose en uno de sus principales usos en el ámbito criminal. Son un vehículo para delitos financieros como el lavado de dinero y el terrorismo y se requiere una mejora en la regulación en esta materia que permita abordar de forma eficaz estos delitos (Teichmann y Falker, 2021). Características de las criptomonedas como el anonimato o la ausencia de intermediarios parecen favorecer la utilización de esta tecnología en el blanqueo de capitales (Brenig et al., 2015).

No obstante, previamente a considerar la forma en la que las criptomonedas han influido en el delito de blanqueo de capitales, se debería exponer en qué consiste este delito. Según la Ley 10/2010 de Prevención de Blanqueo de Capitales y de Financiación al Terrorismo[142], podrán ser constitutivas de un delito de blanqueo de capitales las siguientes actividades:

> *a) La conversión o la transferencia de bienes, a sabiendas de que dichos bienes proceden de una actividad delictiva o de la participación en una actividad delictiva, con el propósito de ocultar o encubrir el origen ilícito de los bienes o de ayudar a personas que estén implicadas a eludir las consecuencias jurídicas de sus actos. b) La ocultación o el encubrimiento de la naturaleza, el origen, la localización, la disposición, el movimiento o la propiedad real de bienes o derechos sobre bienes, a sabiendas de que dichos bienes proceden de una actividad delictiva o de la participación en una actividad delictiva. c) La adquisición, posesión o utilización de bienes, a sabiendas, en el momento de la recepción de los mismos, de que proceden de una actividad delictiva o de la participación en una actividad delictiva y d) La participación en alguna de las actividades mencionadas en las letras anteriores, la asociación para cometer este tipo de actos, las tentativas de perpetrarlas y el hecho de ayudar, instigar o aconsejar a alguien para realizarlas o facilitar su ejecución* (p.7).

De acuerdo con lo expuesto en dicha ley, la implementación de las criptomonedas en el blanqueo de capitales tiene como finalidad la conversión de bienes que proceden de actividades delictivas o de la participación en estas con el propósito de ocultar o encubrir el origen ilícito de los bienes o ayudar a las personas implicadas a eludir las consecuencias jurídicas de sus actos.

Las criptomonedas también facilitarían lo expuesto en el apartado b) al favorecer la ocultación, encubrimiento, el origen, el movimiento o la propiedad de los bienes obtenidos a partir de una actividad delictiva. Al mismo tiempo, en relación con los apartados c) y d), también se considerarían como parte de un delito de blanqueo de capitales la adquisición, posesión o utilización de bienes, en este caso criptomonedas, que procedan de una actividad delictiva o de la participación en esta o bien la participación o asociación para cometer este

[142] Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. https://www.boe.es/eli/es/l/2010/04/28/10/con

tipo de delitos, la tentativa, el hecho de ayudar, instigar o aconsejar para realizarlas o facilitar su ejecución.

El delito de blanqueo de capitales, de forma general está formado por tres fases: colocación, encubrimiento e integración (Financial Action Task Force, 2022). La fase de colocación consiste en la introducción de los ingresos originados por una actividad delictiva en el sistema financiero; la fase de encubrimiento consiste en el movimiento de los ingresos a través de transacciones financieras que permitan dificultar el trazado del dinero y desvincularlo de su origen y por último, en la fase de integración los fondos con apariencia de ingreso legal vuelven a ingresar en la economía legítima y el sujeto puede invertirlos en bienes, activos de lujo o empresas comerciales (Financial Action Task Force, 2022). En relación con esto, las facilidades que otorgan las criptomonedas están destinadas mayormente a la fase de colocación, que es precisamente aquella en la que la intervención de las autoridades resultaría más eficaz (Pérez López, 2017, p. 156). El criminal introduce las ganancias del delito en el sistema financiero o adquiere instrumentos de valor no monetarios como arte, antigüedades y monedas virtuales (Choo, 2015). En la fase de encubrimiento también podrían tener relevancia de nuevo las criptomonedas al ser utilizadas para comprar otras criptomonedas o enviar los fondos entre diferentes carteras (Choo, 2015).

En definitiva, el núcleo de este tipo de actividad criminal consiste en la compra de criptomonedas utilizando el dinero que se ha obtenido como beneficio de delitos como *carding*, estafas (carta nigeriana, empleos falsos, etc.), tráfico de drogas, etc. Los videojuegos de rol o *multiplayer online role playing games* también se están posicionando como una tendencia en el lavado de dinero. Los criminales crean diversas cuentas falsas en estos videojuegos, utilizan dinero fiduciario para la obtención de la moneda virtual del juego o criptomonedas y luego emplean diversas formas de convertir de nuevo ese dinero a dinero real (Richet, 2013).

De esta forma, en relación con lo expuesto anteriormente, no se considera que la implementación de las criptomonedas en el delito de blanqueo de capitales haya supuesto la creación de un nuevo tipo de delito, sino que se trata de un delito de carácter tradicional cuya novedad ha sido la inclusión de esta tecnología entre las herramientas que utilizan para facilitar el desarrollo de sus actividades delictivas.

Características y Tecnologías que han Favorecido su Uso en el Crimen

En cuanto a los aspectos de las criptomonedas que han favorecido su utilización en el delito de blanqueo de capitales, la independencia de intermediarios como las entidades

bancarias pudiera haber facilitado el desarrollo de este tipo de criminalidad. También puede verse favorecido por su falta de regulación o supervisión, lo que puede haberlas convertido en un instrumento eficaz entre las técnicas para blanquear dinero (España Alba, 2016).

También han sido señalados como facilitadores del lavado de dinero con criptomonedas el anonimato, la evasión y alta negociabilidad y la posibilidad de transferir, utilizar y retirar los fondos en tiempo real (Choo, 2015). Incluso se ha observado que el blanqueo de capitales mediante la utilización de criptomonedas puede reducir los costes en comparación con otros métodos, lo que resulta de interés para la rentabilidad del negocio criminal (Van Wegberg et al., 2018).

En definitiva, todo lo que se busca conseguir es una serie de transacciones privadas anónimas para las que habrá que utilizar servicios especiales que permitan el blanqueo con tal propósito (Ali et al., 2015). Sin embargo, las criptomonedas como el Bitcoin no son anónimas por lo que su utilización en el desarrollo de estos delitos requiere en ocasiones del empleo de técnicas y herramientas que dificulten el rastro de la actividad y la identificación del usuario (Pérez López, 2017). Por este motivo, en su desarrollo han tenido también un papel relevante otras tecnologías relacionadas con el ámbito de las criptomonedas como los *mixers* o mezcladores de criptomonedas, también conocidos como *tumblers* (Soska y Christin, 2015). Estos servicios permiten dificultar el rastreo de las transacciones rompiendo la conexión entre las direcciones (Hong et al., 2018). El usuario que desea utilizar este servicio envía sus fondos a través de una transacción a la dirección del *mixer,* que mezclará las transacciones entrantes de forma que no sea posible asociar las transacciones de entrada con las de salida (Hong et al., 2018). Algunos ejemplos de estos servicios son "BitcoinBlender"[143], "Bitcoin Fog"[144] y "CryptoMixer"[145], los dos primeros únicamente son accesibles a través de la red TOR.

No obstante, estos servicios cuentan cada vez menos con la confianza de los usuarios ya que muchos de ellos han visto involucrados en casos de estafa conocidos como el del *mixer* "Helix" actualmente fuesa de servicio y muchos otros continúan siendo estafas (Crawford y Gleason, 2020). Según las discusiones de los usuarios sobre estos servicios se podía establecer la confianza depositada en cada uno de los *mixers* más conocidos, por lo que alrededor del 19 al 28% eran considerados como probables estafas (Crawford y Gleason, 2020). Al mismo tiempo, en la investigación de Van Wegberg et al. (2018) se utilizaron varios

[143] BitcoinBlender. Onion URL: http://bitblendervrfkzr.onion/
[144] Bitcoin Fog. Onion URL: https://bitcoinfog.info/foggedd3mc4dr2o2.onion
[145] CryptoMixer. https://criptomixer.io/

de estos servicios con el objetivo de comprobar su utilidad como medio de blanqueo de capitales y los investigadores perdieron sus bitcoins en tres de cada cinco intentos.

La confianza de los usuarios en estos servicios también se ha visto reducida porque cuentan con una elevada atención por parte de las FCSE, además de que muchas investigaciones se centran en elaborar algoritmos que les impidan tener éxito en la consecución del anonimato relacionando las direcciones de entrada y las direcciones de salida mezcladas (Hong et al., 2018).

Sin embargo, continúan siendo un servicio que podría ser de utilidad para los criminales, ya que en aquellos casos en los que funcionan correctamente se ha observado que ofrecen un servicio profesional, bien evaluado y a buen coste, por lo que podrían permitir a cualquier usuario el blanqueo de capitales (Van Wegberg et al., 2018).

En una investigación de la empresa "Elliptic" se obtuvo que el 25% de las transferencias ilícitas se enviaban a plataformas de juego y apuestas *online* y a *mixers* (Fanusie y Robinson, 2018). Otro ejemplo es el empleo de redes P2P que facilitan no solo la comunicación entre los miembros de un grupo u organización (Pérez López, 2017). Posteriormente también pueden utilizarse casas de cambio de criptomonedas de carácter descentralizado, es decir, que no requieran de que el usuario aporte su información personal. Este fue el caso de la conocida casa de cambio *Liberty Reserve*, que se tratará en apartados siguientes (Richet, 2013).

Sin embargo, aunque funciona el modelo de lavado de dinero seguido por los criminales utilizando criptomonedas, no es seguro que este pueda servir para grandes cantidades de dinero (Van Wegberg et al., 2018). Ha habido autores que han cuestionado la idoneidad de las criptomonedas en el delito de blanqueo de capitales. Las transacciones realizadas a través de una *Blockchain* de carácter público como la de Bitcoin quedan registradas y existe la posibilidad de consultarlas libremente por cualquier persona interesada. Los grupos criminales implicados en esta actividad necesitarían mover grandes cantidades de dinero, por lo que la posibilidad de que esta transacción quedara registrada de forma pública en la *Blockchain* supondría un riesgo para la permanencia del grupo.

Las capacidades de análisis de la *Blockchain* que disponen las empresas de inteligencia les permitirían detectar y monitorear esta actividad, analizando las transacciones realizadas y ofreciendo esta información a las FCSE y otras entidades encargadas de la persecución de estos delitos (Butler, 2019). Entre otros, se pueden emplear técnicas de agrupamiento mediante las que recogen información de todas las transacciones realizadas en la *Blockchain* para identificar aquellas carteras que pueden estar controladas por la misma

entidad y posteriormente, utilizar rastreadores web y registros manuales para nombrar entidades y asignarles una puntuación de riesgo en relación con su implicación en actividades delictivas (Wolfson, 2018b). Un ejemplo de estas herramientas es la solución "Crystal Blockchain Analytics" desarrollada por el grupo "Bitfury"[146], que establece diferentes niveles en los que una dirección Bitcoin podría haber estado implicada en actividades sospechosas de constituir un delito (Wolfson, 2018b). Algunos sujetos incluso utilizan estas herramientas de forma proactiva para determinar el riesgo de que la actividad legal o ilegal que han planeado pudiera ser detectada por otros usuarios (Wolfson, 2018b).

En relación con la situación de este tipo de delincuencia en España, debido a su carácter desmaterializado y transfronterizo, no es extraño que el perfil que se presenta en este país sea muy similar al encontrado en otros países europeos. Debido a que no hay informes específicos para este país que cuantifiquen el impacto específico del uso de las criptomonedas en el contexto de las finanzas criminales en España, la visibilidad de estas actividades se basa en los informes generales realizados por otras autoridades, la presencia mediática de las actividades de las Fuerzas y Cuerpos de Seguridad del Estado y algunas decisiones judiciales (Pérez López, 2017).

Relevancia de su Persecución. Casos Relevantes en esta Materia

El blanqueo de capitales con criptomonedas ha sido una de las actividades delictivas que más se ha estudiado y perseguido en este ámbito. Diversas autoridades gubernamentales, FCSE y organismos y empresas dedicadas a la seguridad han puesto el foco en la detección, la persecución y el estudio en este tipo de criminalidad, lo que ha supuesto un elevado número de operaciones policiales y una gran variedad de informes que abordan esta temática.

En este sentido, han sido numerosas las instituciones que se han pronunciado al respecto elaborando propuestas o guías de actuación para prevenir este tipo de delincuencia de la forma más efectiva. Ejemplo de ello se pueden señalar las recomendaciones elaboradas por la *Financial Action Task Force* o FATF (en español, Grupo de Acción Financiera Internacional o GAFI), en materia de lavado de dinero y financiación del terrorismo con el objetivo de desarrollar y promover políticas que protejan el sistema financiero global. En los últimos años también se han elaborado diversos informes desde Europol en los que se ha tratado el blanqueo de capitales como parte del cibercrimen mediante la utilización de las criptomonedas con los informes IOCTA. Además, también se señalaron las criptomonedas

[146] Crystal Blockchain Analytics https://crystalblockchain.com/

como un facilitador del blanqueo de capitales entre las actividades delictivas del crimen organizado en los informes SOCTA también elaborados por Europol. A nivel internacional, la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), conocedora de esta práctica, elabora una guía para prevenir el blanqueo de capitales empleando criptomonedas y fomentar la cooperación entre países en la lucha contra este tipo de delincuencia.

A nivel nacional, la Estrategia Nacional de Ciberseguridad ha señalado la utilización de criptomonedas como un desafío debido a su sofisticación y complejidad junto con otros delitos como la evasión de impuestos e incluso en la financiación del terrorismo o del crimen organizado[147]. Entre sus líneas de acción para poder conseguir la neutralización de la economía y otros delincuentes exponen que la utilización de esta tecnología supone una nueva amenaza de naturaleza económica para la que se deberá "impulsar la respuesta normativa y la asunción de compromisos internacionales en materia de supervisión y de investigación (...)" (Consejo de Seguridad Nacional, 2019, p.36). Pero no sólo, ya que también sugiere que será necesario un avance en el conocimiento de estas herramientas en los procesos de blanqueo de capitales, así como su recuperación y gestión "promoviendo normativas que doten de transparencia la operativa en todos los criptoactivos" (Consejo de Seguridad Nacional, 2019, p. 43). En definitiva, propone un trabajo conjunto e internacional entre países, que se centre no únicamente en su detección y persecución sino también en la investigación de este tipo de delitos, para la elaboración de medidas de prevención formadas como la transparencia operativa, además de la formación de los profesionales.

En esta materia se pueden señalar varios casos que han sido relevantes. Uno de los casos de lavado de dinero *online* más relevantes e importantes de la historia fue el caso del servicio de moneda digital centralizado "Liberty Reserve". Se consolidó en el año 2006 y consistía en un transmisor de dinero costarricense que facilitó la distribución, almacenamiento y lavado de las ganancias ilícitas de estafas con tarjetas de crédito, fraude de identidad, estafas de inversión, hacking, tráfico de drogas y pornografía infantil, mediante transacciones anónimas no rastreables. Llegó a contar con más de un millón de usuarios en todo el mundo, realizando alrededor de 55 millones de transacciones, la mayoría de ellas ilegales, suponiendo el movimiento de más de 6.000 millones de dólares en ganancias ilícitas (Financial Action Task Force, 2014). Aunque la plataforma pedía información sobre la identificación del usuario, esta información no era validada, por lo que normalmente se

[147] Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional https://www.boe.es/eli/es/o/2019/04/26/pci487 (p.43443)

empleaban cuentas con nombres y direcciones falsos. Además, para conseguir un mayor anonimato, Liberty Reserve pedía a los usuarios que los depósitos y retiradas de dinero las realizaran a través de *exchanges* externos que no tenían licencia y operaban en países con laxas o inexistentes regulaciones respecto del lavado de dinero como Malasia, Nigeria o Vietnam (Financial Action Task Force, 2014). De esta forma, evitaban cualquier vinculación directa con datos bancarios de los usuarios u otras actividades que pudieran crear un rastro centralizado (Financial Action Task Force, 2014). Por una comisión extra, el usuario podía ocultar también su número de cuenta de Liberty Reserve haciendo incapaces de rastrear las transferencias realizadas entre usuarios de este servicio (Financial Action Task Force, 2014).

Otra de las operaciones más conocidas y notorias, por ser pionera en su tiempo, fue la "Operación Ransom" u "Operación *Ransomware*", en la que se investigó y persiguió a la red responsable del llamado "virus de la policía"[148]. Aunque en este caso el ciberdelito más relevante era el ataque *ransomware*, el pago de numerosas víctimas de la cantidad exigida por los ciberdelincuentes supuso el blanqueo posterior de los beneficios obtenidos eliminar todo rastro de la actividad delictiva. El pago del rescate del equipo era exigido según el país de procedencia, así en Europa obtenían códigos de prepago de *Ukash* o de *PaySafeCard* (proveedores británicos y austríaco de dinero electrónico) y en Estados Unidos obtenían códigos de *MoneyPak*. Una gran parte de los beneficios obtenidos eran convertidos en criptomonedas, en específico bitcoins, que obstaculizaron la investigación de los miembros de la trama al dificultar su trazabilidad [149]. Finalmente, la aprehensión del líder de la operación se realizó de forma *in fraganti* cuando se le sorprendió al mismo con las carteras Bitcoin abiertas en su dispositivo. Esto permitió la incautación del saldo en bitcoins mediante una orden judicial específica, convirtiendo de nuevo estos bitcoins a moneda de curso legal y transfiriendo este producto a la cuenta bancaria de consignaciones judiciales[150] (Pérez López, 2017).

En otro caso, se detuvo a una organización criminal que operaba en diferentes

[148] Aunque se explicará en apartados posteriores con mayor detalle, el "virus de la policía" consistía en un ataque *ransomware* que accedía a sus víctimas a través de un delito de *phishing* por el que suplantaba una página web de las fuerzas y cuerpos de seguridad del país de residencia de la víctima. En esta página se advertía a los usuarios de que habían cometido un delito por el que estaban siendo investigados, por lo que era necesario que accedieran a un enlace para solucionar la situación. Una vez accedían a este enlace, se bloqueaba el contenido del ordenador de la víctima exigiendo para su desbloqueo una cierta cantidad de dinero en forma de criptomonedas, en este caso Bitcoin.

[149] Uno de los mayores errores de los ciberdelincuentes en este caso, fue según X. Pérez (2017) no ofrecer la posibilidad real de desbloqueo del ordenador una vez se pagaba el rescate exigido. De esta forma, muchas de las víctimas que habían pagado la cantidad de dinero que se pedía acudieron a las diferentes comisarías de policía exigiendo el desbloqueo del ordenador.

[150] Este ha sido considerado como el primer caso de incautación de bitcoins en España.

ciudades y que blanqueaba el dinero obtenido en la venta de decodificadores de señales de televisión fraudulentos a través de la compra del equipo necesario para la minería de criptomonedas (EFE, 2016)[151]. De esta forma, crearon diversas "granjas" de minería a través de las que dotaban de criptomonedas a la comunidad y obtenían beneficios de nuevo por medio de dinero fiduciario (EFE, 2016) [152].

Por último, recientemente se detuvo al fundador de la plataforma de intercambio de criptomonedas "Bitzlato" con sede en China por ser sospechoso de haber blanqueado millones de dólares en actividades delictivas (Swissinfo.ch, 2023). Su fundador aseguraba que era necesaria la mínima identificación durante la utilización de su plataforma de cambio, por lo que este servicio se convirtió en un espacio favorable para la criminalidad (Swissinfo.ch, 2023). La gendarmería francesa estimó el total de transacciones registradas en Bitzlato desde 2018 en más de 2000 millones de dólares (Swissinfo.ch, 2023).

Normativa Nacional y Comunitaria

La relevancia de esta criminalidad ha ocasionado que se convierta en una de las principales preocupaciones de los Estados e instituciones. Esto ha quedado reflejado en cierto sentido en el rápido avance que está experimentando la línea de reforma legislativa que se refiere a la prevención del blanqueo de capitales (Pérez López, 2017).

En este sentido, es relevante el Real Decreto Ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención del blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores. Dicha norma, modificaba la Ley 10/2010, de 28 de abril que constituye el marco legal contra el lavado de dinero y lo expuesto en la Directiva 2018/843 del Parlamento Europeo y del Consejo. Así, contemplaba ciertos aspectos de la utilización de criptomonedas que anteriormente no se

[151] Se puede obtener más información sobre el caso en las resoluciones judiciales pertinentes: Auto AP Pontevedra, Sec. 5, n.º 208/2017, de 23 de marzo de 2017; Auto AP Pontevedra, Sec. 5, n. º 515/2017, de 7 de julio de 2017 y Auto AP Pontevedra, Sec. 5, n.º 483/2017, de 30 de agosto de 2017.

[152] De las sentencias de la Audiencia Provincial relacionadas con este caso, se deduce según X. Pérez (2017, p. 185) que para el desarrollo de la actividad delictiva se ha estado robando fluido eléctrico, lo que no solo se entiende por la necesidad de ahorrar en el coste de electricidad, tan elevado en la extracción de bitcoins a gran escala, sino también se entendería como un método para encubrir la actividad ocultando la existencia de las granjas de minería. Añade X. Pérez (2017) que ante esta situación los autores del delito tuvieron que decidir entre dos opciones. La primera de ellas la de ocultar el elevado consumo de electricidad de las granjas de minería y la segunda la de justificar ese elevado consumo de electricidad mediante la realización de otra actividad de carácter lícito.

consideraban en la normativa.

De esta forma, la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (LPBC) será de aplicación para los proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos (Boletín Oficial del Estado, 2010, p.10), debiendo de cumplir con lo expuesto en el texto de la ley en materia de prevención del blanqueo de capitales. Es relevante el artículo 16 de la LPBC, que señala que los sujetos obligados deberán considerar el riesgo de delitos de blanqueo de capitales, analizar el riesgo y tomar medidas:

> *Los sujetos obligados prestarán especial atención a todo riesgo de blanqueo de capitales o de financiación del terrorismo que pueda derivarse de productos u operaciones propicias al anonimato, o de nuevos desarrollos tecnológicos, y tomarán medidas adecuadas a fin de impedir su uso para fines de blanqueo de capitales o de financiación del terrorismo. En tales casos, los sujetos obligados efectuarán un análisis específico de los posibles riesgos en relación con el blanqueo de capitales o la financiación del terrorismo, que deberá documentarse y estar a disposición de las autoridades competentes* (p.20).

A nivel europeo, la Directiva UE 2015/849 del Parlamento Europeo y del Consejo de 20 de mayo de 2015[153] constituía el principal instrumento jurídico de prevención de la utilización del sistema financiero de la Unión para el blanqueo de capitales y la financiación del terrorismo.

Sin embargo, la Directiva 2015/849/UE, no hace mención expresa a las criptomonedas en su texto, ni tampoco habla de forma general de monedas virtuales como herramientas que faciliten el blanqueo de capitales o la financiación del terrorismo. En el Anexo III se señalan factores de riesgo en función del producto, servicio, transacción o canal de distribución como "productos o transacciones que favorezcan el anonimato" o "nuevos productos y nuevas prácticas comerciales, incluidos nuevos mecanismos de entrega, y utilización de tecnologías nuevas o en desarrollo para productos nuevos o ya existentes" (L 141/115). Dentro de este apartado se podrían considerar las criptomonedas como nuevo producto o tecnología nueva, en desarrollo o existente que facilitan las transacciones anónimas. Pero fue necesario emplear para esta materia las disposiciones fruto de la Resolución del Parlamento Europeo, de 26 de mayo de 2016 sobre monedas virtuales, que fue el resultado del mandato dirigido por el Parlamento europeo hacia la Comisión europea, considerando la necesidad de emprender acciones regulatorias en esta materia y que fueron posteriormente incluidas en la Directiva (Pérez López, 2017).

[153] Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) n° 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión (Texto pertinente a efectos del EEE)

Por lo tanto, la Directiva 2015/849/UE necesitaba modificaciones que adaptaran su texto a la utilización en específico de criptomonedas en el blanqueo de capitales. El incremento de la transparencia global del entorno económico y financiero de la Unión podría ser un potente efecto disuasorio, ayudando a prevenir el blanqueo de capitales y la financiación del terrorismo. Por todo ello, se requerían modificaciones en la directiva que se adaptara a los cambios que se estaban produciendo en ambas tipologías delictivas e incluyeran aspectos de la actividad con criptomonedas que no se estaban considerando.

Al año siguiente, el Banco Central Europeo elaboraba un dictamen para proponer una modificación de la Directiva[154] que incluyera aspectos relacionados con la consideración, utilización y regulación de las monedas virtuales. Se amplía la lista de entidades a las que obliga la Directiva (UE) 2015/849 (artículo 2) para "incluir en ella a proveedores que presten principal y profesionalmente servicios de cambio de monedas virtuales por monedas fiduciarias y a los proveedores de servicios de custodia de monederos electrónicos que ofrezcan servicios de custodia de las credenciales necesarias para acceder a monedas virtuales" (C 459/3). Además, obliga a los Estados miembros a que aseguren que estos proveedores estén autorizados o registrados. Estos cambios, se proponen para adaptarse a lo expuesto por el GAFI[155] en relación con la capacidad de grupos terroristas, entre otros para utilizar monedas virtuales para transferir fondos aprovechándose de cierto grado de anonimato del que disponen las plataformas de cambio (Dictamen CON/2016/49).

Finalmente, con el objetivo de incorporar todas las modificaciones propuestas a la Directiva 2015/849/UE, el Parlamento Europeo aprobó la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo[156].

Una de las principales modificaciones de la nueva Directiva en materia de monedas virtuales fue en relación con los proveedores de servicios de cambio de moneda y de custodia

[154] DICTAMEN DEL BANCO CENTRAL EUROPEO de 12 de octubre de 2016 sobre una propuesta de directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica la Directiva 2009/101/CE (CON/2016/49).

[155] Los documentos del GAFI a los que se hace referencia en el dictamen elaborado por el BCE son: «*International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations*» (febrero de 2012); «*Virtual Currencies Key Definitions and Potential AML/CFT Risks*» (junio de 2014), y «*Guidance for a Risk-Based Approach-Virtual Currencies*» (junio de 2015).

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

de monederos electrónicos. En la Directiva anterior ambas entidades no estaban obligadas por la Unión a la detección de actividades sospechosas. Por ello, era necesario ampliar el ámbito de actuación de la Directiva 2015/849 para incluir a estas entidades, que tendrán también la obligación de vigilar el uso de las monedas virtuales a los efectos de la lucha contra el blanqueo de capitales y la financiación del terrorismo. El artículo 2, apartado 1, punto 3 de la Directiva 2018/843, añade estas entidades en sus letras g) proveedores de servicios de cambio y h) servicios de custodia de monederos electrónicos. Ambos como sujetos o entidades obligadas a las que se les aplicará la recogido en la directiva, lo que supone una obligación para aquellos intermediarios en el negocio de las criptomonedas en la Unión Europea[157]. De esta forma, la Directiva dificultaría la continuidad de las casas de cambio o *exchanges* en el territorio europeo al ser sometidas al principio de "conozca a su cliente" para la prevención del blanqueo de capitales (Aránguez, 2020).

Al mismo tiempo, la Directiva 2018/843, hace mención expresa a las monedas virtuales, señalando que estas no deben de ser confundidas con otros términos utilizados en directivas anteriores como "dinero electrónico", "fondos" o "monedas de juegos. El objetivo de esta es abarcar todos los usos de las monedas virtuales, que, aunque también son medios de pago como las anteriores, también pueden ser "medios de cambio, inversión, productos de reserva de valor o uso en los casinos en línea" (L 156/ 45).

Las Criptomonedas en el Cibercrimen

Desde una concepción restringida, se considera cibercrimen a aquellos delitos en los que la tecnología ha tenido un papel esencial (Miró-Llinares, 2012). De acuerdo con esta consideración en este apartado se recogen aquellos delitos en los que las criptomonedas han tenido un papel determinante en su comisión.

La Apropiación de las Criptomonedas. Las Criptomonedas Como Objeto del Delito

El auge de la utilización de las criptomonedas en la última década ha ocasionado que el precio de la unidad de algunas como Bitcoin sea muy elevado. Esto las ha convertido en un objetivo atractivo para los criminales interesados en apropiarse de las criptomonedas de otros

[157]Aunque en la misma Directiva 2018/843, se hace referencia, esta modificación no resolvería totalmente la cuestión del anonimato asociado a las transacciones con monedas virtuales, ya que este se mantendría en gran parte del entorno de la moneda virtual, ya que se pueden realizar transacciones al margen de tales proveedores de servicios. No obstante, para combatir estos riesgos, "las Unidades de Inteligencia Financiera (UIF) nacionales, deberían poder obtener informaciones que les permitan asociar las direcciones de monedas virtuales a la identidad del propietario de la moneda virtual" (L 156/44).

usuarios para obtener elevados beneficios. Al mismo tiempo, características de las criptomonedas como su inseguridad operativa o la irreversibilidad de las transacciones favorecían que los criminales se vieran atraídos por su apropiación (Moore y Christin, 2013). Asimismo, el robo de las carteras de Bitcoin ha supuesto para la comunidad de usuarios de estas monedas junto con la estafa un inconveniente mucho mayor para su utilización que la propia aplicación de la ley (Zetter, 2012).

Existe una correlación entre el precio de criptomonedas como el Bitcoin y la creación de *malware* especializado en el robo de criptomonedas, es decir, a medida que Bitcoin se vuelve más valioso, más autores lo tienen como objetivo (Stewart, 2014). Una mayor divulgación de estos casos a través de la prensa podría sugerir una disminución de la utilización de las criptomonedas y por tanto una reducción del precio de la unidad. Sin embargo, se ha visto que el aumento de los delitos de robo y su comunicación a través de las noticias, al contrario de los que se pudiera pensar, no reduce el precio de las criptomonedas, sino que lo aumenta (Brown y Douglass, 2020). De esta forma, el robo de criptomonedas junto con la estafa se ha constituido como una de las mayores formas de delitos basados en criptomonedas durante el año 2021, la mayoría de los cuales ocurrieron mediante la piratería de empresas de criptomonedas (Chainalysis, 2022).

Existen varias investigaciones dedicadas a estudiar el flujo de monedas robadas, una actividad que es de interés especialmente para las víctimas, pero también para las autoridades encargadas de la persecución de estos delitos, que debido a la complejidad de la tecnología son difíciles de perseguir. Un ejemplo es la investigación de Ahmed et al. (2019) que presentan técnicas de visualización que ayudan a detectar patrones y técnicas operativas de los delincuentes que operan en la red Bitcoin. Pero también se pueden encontrar otras investigaciones que tienen como objeto de estudio las diversas formas que existen para desarrollar este delito.

En este trabajo se han identificado varias formas en las que los sujetos se pueden apropiar de forma indebida de las criptomonedas de otros usuarios. El primer grupo hace referencia a aquellas formas que requieren de la participación de las víctimas como sucede en el delito de *phishing* en el que los criminales utilizan ingeniería social para engañar a las víctimas y obtener sus credenciales. En el segundo grupo se incluyen aquellas formas de apropiarse de las criptomonedas en las que la participación de la víctima no es necesaria para el desarrollo del delito, incluso en varias ocasiones no es consciente del ataque, como sucede en los ataques a las casas de cambio de criptomonedas o en la utilización de *malware* de minado o *cryptojacking* y el empleo de *botnets*.

A continuación, se presentarán con más detalle las diversas formas de apropiación descritas:

Utilización de Técnicas de *Phishing*. Una de las formas de apropiación indebida de las criptomonedas de otros sujetos es a través la utilización de técnicas de *phishing* para engañar a la víctima y obtener las credenciales que dan acceso a sus carteras de criptomonedas.

Para el caso del robo de información personal del usuario, han sido conocidos los casos de las carteras de criptomonedas "Phantom" y "MetaMask" para las que los cibercriminales crearon páginas web muy similares a las originales de estos servicios. El procedimiento en ambas comenzaba con la redirección de los usuarios a estas nuevas páginas web a través de los anuncios del buscador "Google" que situaba la página web falsa en primer lugar, antes que la página oficial de las carteras. En el caso de la cartera "Phantom", al acceder al sitio fraudulento para crear una cartera se podía ver una pregunta de seguridad y un apartado para crear una nueva contraseña. Cuando el usuario accedía a la cartera creada, en realidad estaba accediendo a la cartera de los hackers, por lo que cualquier ingreso de criptomonedas que se realizaba a esta cartera llegaba directamente a los cibercriminales (Barda et al., 2021). En el caso de la cartera "MetaMask", los atacantes robaban las claves privadas de la cartera de los usuarios una vez estos la importaban al sitio web o a través de una frase de seguridad que les permita obtener la respuesta de las víctimas y realizar posteriores transferencias a sus cuentas (Barda et al., 2021).

Al mismo tiempo, los ataques phishing pueden ser utilizados por el criminal con un propósito diferente de la obtención de la información personal del usuario. Otras razones por las que un hacker podría considerar realizar un ataque de este tipo podrían ser para utilizar el dispositivo infectado como parte de una *botnet* o para acceder a este y formar parte de la red (Higbee, 2018, p.15).

Ataques Cibernéticos a Casas de Cambio o *Exchanges*. Otra de las formas de apropiación de las criptomonedas de los usuarios es a través de los ataques a las casas de intercambio de criptomonedas.

Estos servicios permiten convertir dinero fiduciario a criptomonedas y viceversa. Además, disponen de otros servicios como carteras *online* que permiten al usuario almacenar sus fondos en la casa de cambio de forma que se le facilite la posterior conversión sin la necesidad de gestionar claves criptográficas. Sin embargo, esto presenta el riesgo de que en el

caso de que la casa de cambio fuera comprometida, el usuario perdería los fondos custodiados por este servicio, que debido a su naturaleza descentralizada pasarían a ser propiedad del autor del ataque (McCorry et al., 2018). A este tipo de delito se le puede considerar como "el equivalente en criptomonedas a los atracos bancarios" (Ali et al., 2015).

Los motivos por los que suceden este tipo de ataques son muy variados, pudiendo tratarse desde una gestión deficiente de la seguridad por parte de los negocios, así como por su diseño, hasta una posible sofisticación en el desarrollo de las actividades delictivas por parte de los hackers (Ali et al., 2015). Lo cierto es que la utilización de estos servicios puede exponer a los usuarios a ciertos riesgos.

En un estudio que se realizó sobre 40 casas de cambio de Bitcoin se obtuvo como resultado que 18 de estas cerraron antes de lo previsto (Moore y Christin, 2013). Pero lo más interesante fue que los cierres de los servicios no solo se debían a la actuación de los defraudadores, sino que hallaron que el volumen de transacciones era un indicador de la probabilidad del cierre de un intercambio (Moore y Christin, 2013). El volumen de transacciones estaba positivamente correlacionado con la probabilidad de un cierre anticipado, por lo que era más probable que cerraran de forma prematura aquellas casas de cambio más populares (Moore y Christin, 2013).

Algunos de los servicios de conversión de criptomonedas que han sido pirateados incluyen nombres como "Bitcoinca", "BitFloor", "Flexcoin", "Poloniex" y "Bitcurex" (Ali et al. 2015). También ha habido otros casos conocidos como el de "YouBit" un intercambio de criptomonedas de Corea Del Sur que perdió 4000 BTC (alrededor de 64 millones de euros para enero del 2023) (BBC, 2017). No obstante, el caso más importante hasta la fecha ha sido el de la casa de cambio "Mt. Gox", con sede en Tokio, que se posicionó como el intercambio más grande del mundo, gestionando alrededor del 70% de todas las transacciones de Bitcoin mundiales y que se cerró con un robo de 450 millones de dólares en criptomonedas (McCorry et al., 2018).

Las soluciones propuestas para reducir el riesgo de este delito habitualmente presentan un carácter preventivo o proactivo y consisten en el uso de monederos "fríos" para almacenar claves privadas donde los atacantes no puedan acceder, la utilización de módulos seguridad de hardware para salvaguardar el monedero del cliente o el uso de "firmas múltiples" para autorizar los retiros (McCorry et al., 2018). Se ha visto que este tipo de soluciones no resultan suficientes para estos casos, por lo que investigadores proponen soluciones de carácter reactivo con mecanismos que detecten el atraco, congelen los retiros y

permitan recuperarse del compromiso pudiendo destruir las monedas si la clave de recuperación también se ve comprometida (McCorry et al., 2018).

Utilización de *Malware*. *Cryptojacking* y Uso de *Botnets*. La actividad con criptomonedas no requiere de la identificación de los usuarios que intervienen en una transacción. Para enviar criptomonedas, el remitente necesita la clave pública del destinatario y autorizará la transacción firmando con su clave privada. Al no requerir de datos personales, la autoría de las criptomonedas en el sistema Bitcoin se establece a través de la posesión de la clave privada, es decir, aquella persona que posea la clave privada de una cartera será la propietaria de las criptomonedas que contiene.

La clave privada es comparable a una contraseña que necesita el usuario para poder acceder a sus fondos y autorizar sus transacciones. Sin embargo, la longitud que presenta imposibilita el hecho de que el usuario pueda memorizarla por lo que es necesario su almacenamiento de una forma accesible que le permita utilizarla siempre que lo necesite en sus transacciones.

De esta forma, el robo de las criptomonedas en este caso se realiza a través del empleo de un *malware* que accede al ordenador o al móvil de la víctima y obtiene las claves privadas de la cartera almacenadas en estos dispositivos (Bamert et al., 2014). Por lo tanto, el riesgo de robo estará presente en cualquier dispositivo en el que se almacenen las claves privadas de las carteras y disponga de una conexión a Internet (Bamert et al., 2014). Un ejemplo de este tipo de *malware* es "Infostealer.Coinbit" dirigido a los equipos Windows, que se concentraba en buscar la ubicación del archivo estándar para la cartera Bitcoin y luego enviaba por correo electrónico las claves criptográficas privadas al atacante a través de un servidor en Polonia (Poulsen, 2011).

En el año 2014 se contabilizaron 146 especies distintas de *malware* de robo de Bitcoin, frente a las 45 especies registradas en el año anterior y alrededor del 50% de las especies descubiertas evitaban con éxito la detección de los antivirus (Greenberg, 2014). El 99% del *malware* se dirigía a Windows, no a Mac o Linux y el objetivo principal era el robo de Bitcoin, solo un 9% del *malware* robaba otras monedas como Litecoin y un 1% algunas menos conocidas como Dogecoin (Greenberg, 2014).

El *malware* que tiene como objetivo el robo de las carteras es el más común en la apropiación indebida de las criptomonedas (Stewart, 2014). La forma más habitual de operar es mediante la búsqueda de carteras en el sistema del usuario, buscando por términos como "*wallet.dat*" u otras ubicaciones conocidas de almacenamiento de claves de software de

carteras, ya sea comprobando ubicaciones conocidas de archivos o buscando en todos los discos duros nombres de archivos que coincidan (Stewart, 2014). Pero también se ha detectado la utilización de otras formas más sofisticadas como la instalación de registradores de teclas para apuntar billeteras protegidas con contraseña (Ali et al., 2015).

También es habitual el robo de las credenciales que dan acceso a las cuentas de las casas de cambio en las que algunos usuarios almacenan sus fondos en criptomonedas (Stewart, 2014). Otra variante menos conocida es la del "hombre en el medio" en la que, en lugar de robar carteras o credenciales, se altera la dirección del destinatario de la transacción antes de que se firme, enviando directamente los bitcoins al criminal (Stewart, 2014).

El usuario "Allinvain" del foro "BitcoinTalk" en el año 2011 fue una de las primeras personas en sufrir una pérdida importante de sus fondos debido a un hackeo de Bitcoin en el que se comprometió su equipo en el que utilizaba Windows y le robaron la cantidad de 25.000 bitcoins (Allinvain, 2011)[158].

Especialmente eran consideradas de elevado riesgo las carteras en línea a través de las que los usuarios descargaban la responsabilidad de sus fondos a un tercero, facilitando los pagos y reduciendo los conocimientos técnicos necesarios para obtener y almacenar la moneda (Hern, 2014). Este fue el caso del hackeo de la cartera *online* "inputs.io", en el que la empresa sufrió dos ataques en el año 2013 y perdió 4.100 bitcoins y la cartera "BIPS" que perdió 1.295 bitcoins de sus propias cuentas y dinero de varias carteras de consumidores (Hern, 2014). La billetera "Bitstamp" también fue comprometida en el año 2015, lo que le supuso una pérdida de alrededor de 19.000 Bitcoins (Higgins, 2015).

Otra de las formas en las que se obtienen criptomonedas a través de la utilización de un *malware* es mediante el empleo de un *malware* de minería, lo que se conoce como *cryptojacking*. Este consiste en la ejecución de un script de minería de criptomonedas en el equipo de un sujeto sin su conocimiento o permiso (Sigler, 2018). A diferencia del *malware* anterior, en este caso el criminal no se apropia directamente de las criptomonedas de la víctima, sino que hace uso de la capacidad de procesamiento de su equipo para extraer criptomonedas como Bitcoin o Monero a través de la minería.

No obstante, este delito no ocurre de forma aislada. Para que se lleve a cabo es necesaria una infección previa de los equipos informáticos a través del *malware* de minado

[158] Mensaje original de "Allinvain" escrito en el foro "BitcoinTalk": If only the wallet file was encrypted on the HD. I do feel like this is my fault for not moving that money to a separate non windows computer. I backed up my wallet.dat file religiously and encrypted it but that does not do me much good when someone or some trojan or something had direct access to my computer somehow (…) (Allinvain, 2011).

que se introduce en los ordenadores de las víctimas y desarrolla el proceso de minería en segundo plano. Este es un proceso difícil de detectar, sobre todo por usuarios no especializados. El rendimiento del ordenador se ve afectado y su funcionamiento se ralentiza consumiendo una elevada cantidad de energía.

Su propagación se lleva a cabo a través de correos electrónicos o *phishing* con independencia del dispositivo del que se trate (móvil, PC, internet de las cosas, etc.) (Sigler, 2018). Este consistirá habitualmente en herramientas basadas en scripts, que en ocasiones están prefabricadas y requieren de escasas habilidades técnicas y tiempo (Sigler, 2018). Sin embargo, esta no es una técnica que permita un enriquecimiento rápido, ya que probablemente el código ejecutado en una web obtenga menos de un dólar al día (Sigler, 2018).

No obstante, se ha visto que en el desarrollo del *cryptojacking* también es habitual la utilización de *botnets* o redes de robots. Una *botnet* es una red de ordenadores que han sido comprometidos a través de un *malware* y que son controlados por un "Botmaster", que es el sujeto que la utiliza para desarrollar una actividad delictiva para obtener beneficios económicos con un bajo riesgo de ser descubierto (Zareh y Shahriari, 2018). De esta forma, la red de ordenadores estará compuesta por tres elementos que le permiten iniciarse y desarrollar un delito: un atacante, que será el responsable de iniciar la actividad y dar órdenes a los *bots*; los robots o *bots*, que son los ordenadores comprometidos con el código malicioso y que son reclutados como parte de la *botnet* para llevar a cabo el delito y los manipuladores, que son los medios que tienen los atacantes para comunicarse con los robots (Dhayal y Kumar, 2018).

La *botnet* que se utiliza para minar Bitcoin se conoce como "Botcoin" (Zareh y Shahriari, 2018) y permite al *Botmaster* generar bitcoins a gran escala obteniendo beneficios a partir de una pequeña inversión inicial y sin ninguna estructura adicional (Huang et al., 2014). Esto le ha llevado a que algunos criminales lo consideren un delito atractivo que permite obtener beneficios económicos sin exponerse a los riesgos que podrían suponer otros ciberdelitos como, por ejemplo, los ataques *ransomware* (Wolfson, 2018a).

Las actividades delictivas en las que se puede emplear una *botnet* son muy diversas como ataques de denegación de servicio (DDoS), *spam*, recopilación de información confidencial, falsos antivirus, etc. (Huang et al., 2014). En relación con las criptomonedas, se ha visto su utilización para robar los credenciales de carteras Bitcoin en los ordenadores, pero también para el minado de criptomonedas (Plohmann y Gerhards-Padilla, 2012). Este es el ejemplo de la *botnet* "Smominru", que infectó alrededor de 500.000 dispositivos Windows

con el software de minería Monero, generando un beneficio de 2,3 millones de dólares, la cantidad correspondiente a 8.900 unidades de la criptomonedas Monero y con alrededor de 1 millón de víctimas (Cimpanu, 2018). Otro de los principales programas maliciosos de criptominería es "Coinhive", una aplicación de minería que algunos hackers fueron capaces de instalar en los dispositivos de sus víctimas sin su consentimiento utilizando sus baterías y su capacidad de cómputo (Higbee, 2018). Por último, también se puede encontrar el caso del *malware* de minado conocido como "WebCobra", que infectaba el equipo de la víctima instalando el minero "Cryptonight" o el minero "Zcash de Claymore", según las prestaciones del equipo informático, el tipo de arquitectura del ordenador o si disponía de antivirus, lo que suponía que disponía de la capacidad de aprender del sistema del usuario adaptando el ataque (Wolfson, 2018a).

No obstante, esta actividad no se reserva únicamente a ordenadores, también se han detectado aplicaciones móviles infectadas que permitían la realización de esta actividad a través de JavaScript, haciendo el proceso invisible para el usuario (Higbee, 2018, p.14). Además, no solo se ha realizado para la minería de bitcoins, sino que también se han visto un caso en el que una *botnet* utilizó dispositivos de almacenamiento conectados a una red durante un periodo de dos meses para extraer 500 millones de la criptomoneda "Dogecoin" (Tung, 2014).

Aun así, las cifras generadas no se acercan a las que se puede generar con una *botnet* dedicada al *spam* y al fraude (Huang et al., 2014). En un estudio sobre las ganancias de esta actividad se observó que en la operación de minería "ZeroAccess" se recibieron hasta la fecha de la investigación más de 400 BTC en concepto de pagos por minería o en el caso de "DarkSons" se recibió un total de 1.681 BTC a través de transacciones en las que se recibieron recompensas de bloques a través de un monedero intermedio (Huang et al., 2014).

En la investigación de este tipo de delitos se ha estudiado por una multitud de autores la detección de la actividad de las *botnets* a través de diferentes métodos (Dhayal y Kumar, 2018). Un ejemplo de ello es "Botcointrap" un enfoque novedoso para identificar *botnets* mineras de Bitcoin basándose en el comportamiento malicioso (Zareh y Shahriari, 2018).

Las criptomonedas como forma de pago en los ataques ransomware

Un *ransomware* es un tipo de *malware* que se introduce en el sistema del usuario y altera su funcionamiento mediante el desarrollo de actividades maliciosas, exigiendo una cantidad de dinero a cambio de cesar su actividad. Por ello, este tipo de *malware* recibe el nombre de *"ransomware"* ya que en inglés "*Ransom*" significa "rescate" y "*ware*" es una

abreviatura de la palabra “software”, que hace referencia a un programa informático.

En cuanto al impacto financiero del límite inferior de cada familia de *ransomware*, se estima que desde el 2013 hasta mediados de 2017 el mercado de pagos de *ransomware* tiene un valor mínimo de 22.967,94BTC, estando dominado por unos pocos (Paquet-Clouston et al., 2019). De esta forma, el *ransomware* se ha convertido en una amenaza que requiere atención y contención por parte de la comunidad cibernética (Hampton y Baig, 2015).

La historia de los ataques *ransomware* comienza en el año 1989 con el troyano AIDS (también conocido como «PC Cyborg») escrito por Joseph Popp. Aunque surgió hace más de tres décadas, sus estrategias no diferían demasiado de las formas utilizadas en los *ransomware* más recientes. Así, se distribuía electrónicamente a través de un disquete infectado con un *malware* que bloqueaba el acceso a los archivos de los usuarios cifrando su contenido y, finalmente, utilizaba un mensaje de ingeniería social para afirmar que el usuario había incumplido un acuerdo de licencia y que debía pagar 189 dólares (mediante cheque) para que se le enviara un disco de renovación de licencia (y descifrado) (Hampton y Baig, 2015).

A partir de este momento, se dan a conocer otros muchos ataques de este tipo, aunque a diferencia de los ataques llevados a cabo en los años 90 fruto de hackers aficionados, en el *malware* de los años 2000 se comenzó a buscar beneficios económicos y se convirtió en una actividad de negocio (Hampton y Baig, 2015).

En el año 2005, aparece por primera vez un *ransomware* enfocado a la extorsión (No More Ransom, 2020a). En el año 2006 aparecen los gusanos “GPcode”, “TROJ. RANSOM. A”, “Archiveus”, “Krotten”, “Cryzip” y “MayArchive” conocidos porque comienzan a utilizar esquemas de cifrado RSA más complejos (No More Ransom, 2020a). En el año 2008, surge el primer *ransomware* de bloqueo, “Randsom.C”, que bloqueaba el escritorio de la víctima mostrándole un mensaje que aseguraba ser del centro de seguridad de Windows y pidiéndole que llamara a un teléfono (Oz et al., 2021). En el año 2010 aparece el *ransomware* “Winlock” y en el año 2011, surge un gusano *ransomware* que imitaba el aviso de Activación de Productos Windows (No More Ransom, 2020a). En el año 2012 aparece “Reventon”, conocido como “el *ransomware* de la policía”, que intentaba obtener información relevante de la víctima (Oz et al., 2021). En el 2013 aparecieron los gusanos *ransomware* “Stamp. EK” basado en un *exploit kit* y uno específico de MacOS X (No More Ransom, 2020a). A finales del año 2013 el *ransomware* “CryptoLocker” recaudó alrededor de 5 millones de dólares (No More Ransom, 2020a). Posteriormente en el año 2014, aparecieron “CTB-locker” y “CryptoWall” que utilizaban criptografía asimétrica y afectaron alrededor de 500.000

dispositivos (Nadir y Bakhshi, 2018). En este año también apareció el primer *ransomware* de bloqueo para el móvil, “Android Defender”, que accedía a los usuarios a través de la apariencia de una aplicación de antivirus legal (Oz et al., 2021). En el año 2015, aparecen los primeros *ransomware* que atacan a otros dispositivos con “Linux.Encoder” que tenía como objetivo las plataformas GNU/Linux y “KeRanger” que iba dirigido a sistemas operativos Macintosh (Oz et al., 2021) y también surge el *ransomware* “TelsaCrypt”. En 2016, el *ransomware* apareció “Locky” y en 2017 fue relevante la aparición del *ransomware* “WannaCry” que afectó alrededor de 200.000 equipos demandando un rescate de 300 dólares (Nadir y Bakhshi, 2018). En el año 2018, apareció “PureLocker”, que usaba cifrado híbrido y en el que el autor pedía a las víctimas que le contactaran a través del servicio de correo electrónico “Proton” (Oz et al., 2021). En el año 2019, aparece “Ryuk” que tenía como objetivo el ataque a empresas (Oz et al., 2021). Finalmente, en el año 2020, debido a la pandemia, aumentaron los ataques *ransomware* siendo el más conocido “Corona”, que afectaba a la gestión de los pacientes en los hospitales (Wuest, 2020).

Tipos de *ransomware.* No obstante, aunque todos los anteriores se presentan como *ransomware*, dentro de esta categoría se pueden encontrar diversos tipos. El funcionamiento más conocido de los *ransomware* es aquel en el que se cifra parte o la totalidad del equipo de su víctima exigiendo el pago de una cantidad de criptomonedas para su liberación (ciberextorsión). Sin embargo, se pueden encontrar los tipos: *ransomware* de cifrado, *Lock Screen Ransomware – WinLocker, Master Boot Record* (MBR) *Ransomware*, *ransomware* de cifrado de servidores web y *ransomware* de dispositivos móviles (Android) (No More Ransom, 2020b). El *ransomware* de cifrado se encarga de cifrar los archivos personales y las carpetas de sus víctimas (documentos, hojas de cálculo, imágenes, etc.), que se borran y en su lugar los usuarios se encuentran un archivo de texto con instrucciones para realizar el pago. No todos los softwares de cifrado muestran una "pantalla de bloqueo" (No More Ransom, 2020b). Pueden utilizar BTC para requerir el pago del descifrado de los archivos. Ejemplos de este *ransomware*: "Maktub", "CTB-Locker", "CryptoLocker". El "Lock Screen Ransomware – WinLocker" bloquea la pantalla del ordenador impidiendo el acceso a otras ventanas y solicita el pago. En este caso no se cifra ningún archivo personal. Te ofrece la posibilidad de pagar en BTC (No More Ransom, 2020b). El "*Master Boot Record (MBR) Ransomware*" bloquea la "*Master Boot Record*", que es la parte del disco duro del ordenador que permite iniciar el sistema operativo, para interrumpir el proceso de inicio del sistema. Al iniciar el sistema se presenta una pantalla con una orden de rescate (No More Ransom, 2020b). En el *ransomware* de cifrado de servidores web el objetivo es cifrar los archivos de los servidores web. Para ello utilizan vulnerabilidades conocidas en los sistemas de gestión de contenido (No More Ransom, 2020b). Por último, en el *ransomware* de dispositivos móviles (Android) el ataque sucede por medio de la descarga de un archivo o de aplicaciones no oficiales en un dispositivo con un sistema operativo Android (No More Ransom, 2020b).

Según la metodología que emplean, se podrían establecer dos grupos de *ransomware*: el *ransomware* criptográfico que cifra los archivos de la víctima y el *ransomware* de bloqueo, que impide a la víctima acceder al sistema (Oz et al., 2021, p.2).

Si se consideran de forma completa todos los aspectos del ataque *ransomware*, los autores Oz., et al. (2021) desarrollaron una taxonomía del *ransomware* que lo dividen en: 1) objetivo (plataformas o víctimas); 2) Infección (*phishing*, aplicaciones maliciosas, descarga desde el disco duro, vulnerabilidades); 3) comunicación (*Hard-coded IP* o *DGA based*) y 4) Acción maliciosa (cifrado, bloqueo o filtración de datos).

En cuanto a la forma en la que se desarrollan los ataques *ransomware*, su actuación se puede dividir en cuatro fases: 1) infección, en la que el *ransomware* llega al sistema de la

víctima a través de diversos vectores de infección; 2) comunicación con los servidores de Comando & Control (C&C) para intercambiar información relevante con el atacante; 3) destrucción, en la que se desarrolla la acción malintencionada a través del encriptado de documentos o el bloqueo del sistema, y 4) extorsión, en la que se informa a la víctima del ataque a través de una nota de rescate en la que se proporciona los detalles del ataque y las instrucciones de pago (Oz et al., 2021, p.5).

Los mecanismos de propagación pueden consistir en kits de explotación que se compran o alquilan con el propósito de distribuir *malware*; programas de afiliación a través de los que los atacantes subcontratan el *malware* ya existente y la infraestructura de apoyo para distribuirlo y a través de campañas de spam y publicidad de *malware* por correo electrónico que ofrecen el *malware* (Nadir y Bakshi, 2018, p.3). Uno de los vectores de infección más conocidos es a través del correo electrónico, produciéndose la introducción del *malware* al equipo cuando la víctima abre un archivo adjunto (archivo ejecutable, imagen u otro archivo) que está infectado. Una vez abierto, el *malware* se extiende en el sistema del usuario. No suele realizarse de forma inmediata, sino que se suele ejecutar en segundo plano hasta que "despliega un sistema o mecanismo de bloqueo de datos" apareciendo una ventana de diálogo que informa al usuario de que los datos se han bloqueado y solicita un rescate (No More Ransom, 2020a).

Sobre el Pago de los Rescates. En los primeros *ransomware* que aparecieron se exigía a la víctima el pago del rescate a través de métodos muy diversos como el envío de un SMS o de una transferencia a un monedero electrónico. También se podían exigir otras formas de obtener beneficios a través de interacciones del usuario forzándolo a comprar productos en una web, accediendo a determinados enlaces web, etc. (Nadir y Bakhshi, 2018).

Lo cierto es que la forma de pago en el *ransomware* era uno de los principales obstáculos en el desarrollo de esta actividad. Los pagos en aquel momento estaban limitados a determinadas zonas geográficas, además de que tenían el respaldo de las autoridades locales y no garantizaban el anonimato de las transferencias o el envío de grandes cantidades (Oz et al., 2021).

No obstante, este *modus operandi* comenzó a cambiar cuando sucedieron ciertos cambios como la regulación de los sistemas de pago electrónicos, la aparición de la primera criptomoneda y las mejoras en los sistemas de cifrado (Drozhzhin, 2016). Los ciberdelincuentes cambiaron los bloqueadores por el cifrado y añadieron como forma de pago las criptomonedas.

A partir de este momento, la introducción de las criptomonedas en el *ransomware* ha tenido un impacto significativo en el panorama de esta amenaza junto con la introducción de los algoritmos de cifrado criptográficamente seguros y la utilización de redes anónimas como TOR e IP2 (Hampton y Baig, 2015). Se ha situado al Bitcoin como una de las formas de pago no rastreables que incentiva el desarrollo de *ransomware* (Al-rimy et al., 2018), ya que proporciona ventajas técnicas y de privacidad únicas para los criminales, que les permite proteger su anonimato y evitar revelar cualquier información que se use para rastrearlos (Kharraz et al., 2015, p.19).

De forma general, se pueden establecer dos tipos de formas de pago en los ataques *ransomware*: pagos directos y pagos indirectos. Dentro de la primera forma de pago, se incluyen los pagos con transferencias y con criptomonedas. En la segunda forma de pago se incluyen métodos como tarjetas prepago, compras de productos *online*, así como llamadas a número de tarificación adicional (Nadir y Bakshi, 2018).

La primera incorporación de la criptomoneda Bitcoin como forma de pago en un ataque *ransomware* tuvo lugar en el año 2013 con el virus tipo troyano "Cryptolocker", que cifraba los archivos personales de la víctima, retenían una copia de la clave de descifrado en su servidor y pedían el pago de un rescate utilizando "MoneyPak" o Bitcoin dentro de las 72 horas siguientes (Spagnuolo et al., 2014). Se estima que este *ransomware* afectó entre 200.000 y 250.000 sistemas en los 100 primeros días de la amenaza (Jarvis, 2013). Se identificó el pago de 771 rescates por un total de 1.226 Bitcoins, lo que para el año 2013 suponía aproximadamente 1,1 millones de dólares (Spagnuolo et al., 2014, p. 466). En la actualidad, esta cifra ascendería a aproximadamente 20 millones de euros. Otro estudio posterior detectó 968 direcciones Bitcoin implicadas en el pago de los rescates pagados con Bitcoin, estimando el pago de 1.128,40 Bitcoins, lo que en ese momento suponía un daño financiero de más de 310.472,38 dólares, pero podría haber sido hasta 1 millón (Liao et al., 2016). Estudios más recientes estiman que el beneficio de pagos obtenidos por "Cryptolocker" fue de 1.511,71 bitcoins, con un total de 944 direcciones implicada (Paquet-Clouston et al., 2019, p.7). No obstante, se debe señalar que debido a la volatilidad del precio de Bitcoin los beneficios señalados no son estables, pudiendo cambiar en periodos cortos de tiempo. También es habitual encontrar discrepancias en cuanto a estas cantidades dependiendo de la investigación que se trate, ya que hay diversas estimaciones (Paquet-Clouston et al., 2019).

A partir de este momento, el éxito de un ataque *ransomware* estaba determinado por la coincidencia de tres tecnologías básicas (Hampton y Baig, 2015):

> *1) Un cifrado fuerte y reversible para bloquear los archivos de un usuario; 2) Un sistema de comunicación anónima de claves y herramientas de descifrado y 3) la ocultación a través de la configuración de una forma imposible de rastrear para pagar el rescate (p.48).*

Aunque en *ransomware* anteriores se incluía Bitcoin como forma de pago, el primer *ransomware* que consiguió combinar los tres requisitos anteriores fue "CTB-Locker". Esto quedaba reflejado en su propio nombre, que hacía referencia a "Curve, TOR y Bitcoin" por criptografía de curva elíptica para encriptar el contenido, protocolo TOR para comunicarse anónimamente y Bitcoin para conseguir transacciones seguras, no rastreables y similares a la utilización de dinero en efectivo (Hampton y Baig, 2015, p.48).

En definitiva, la introducción de las criptomonedas como forma de pago supuso un cambio significativo en el desarrollo de los ataques *ransomware*. Desde el año 2006 hasta la primera incorporación de las criptomonedas en el 2014 solo el 2,86% de los *ransomware* había ofrecido Bitcoin para el pago del rescate, especialmente aquellos *ransomware* que surgieron posteriormente al año 2014 (Kharraz et al., 2015, p. 17). El resto de los *ransomware* estudiados en este periodo aceptaban otros métodos de pago, el 10% usó números Premium y la mayoría cerca del 88% usó métodos prepago *online* como "Moneypak", "Paysafecard" y "Ukash" (Kharraz et al., 2015, p. 17). En el caso del *ransomware* "Cryptolocker", el 1,1% de las victimas pagó el rescate a través de "MoneyPak" y solo el 0,21% usó Bitcoin (Constantin, 2014).

Sin embargo, desde su incorporación en el año 2014 hasta la actualidad, la mayoría de los *ransomware* han utilizado Bitcoin como forma de pago, incluido el más reciente "Corona" que tuvo su origen en la pandemia ocasionada por la COVID-19 (Oz et al., 2021, p. 13). Todo ello, ha situado al Bitcoin como el método de pago preferente en este tipo de delito en la actualidad (Paquet-Clouston et al., 2019).

No obstante, en este punto hay que señalar que los beneficios de este tipo de delito están determinados por la predisposición de la víctima para pagar el rescate exigido. Aunque la introducción de las criptomonedas como forma de pago ha supuesto una mejora en el delito desde el punto de vista del autor, este hecho no supone que haya aumentado directamente su eficacia.

En este sentido, se ha descubierto que solo unas pocas familias de *ransomware* consiguen obtener los pagos del rescate por valor de millones (Paquet-Clouston et al., 2019). Es decir, se trata de un mercado en el que unos pocos sujetos asumen la mayoría de los pagos de los rescates (Paquet-Clouston et al., 2019). Esto puede deberse a que en su mayoría no presentan un gran potencial destructivo. A pesar de los avances que se han dado en cifrado y

técnicas de comunicación, la mayoría de las familias de *ransomware* bloquean simplemente el ordenador de la víctima o intenta el cifrado o eliminación de documentos de la víctima únicamente utilizando técnicas superficiales (Kharraz et al., 2015).

Investigación por los pagos. El hecho de que la mayoría de los pagos de *ransomware* se lleven a cabo con Bitcoin ha favorecido al mismo tiempo la investigación de este tipo de delitos. El carácter público de la *Blockchain* de Bitcoin ha permitido a los investigadores consultar la actividad realizada por aquellas direcciones Bitcoin que se han vinculado a casos de ataques *ransomware*.

La mayoría de las direcciones que se utilizaban en *ransomware* estaban activas únicamente para recibir el pago de las víctimas (Kharraz et al., 2015). El 73% de las direcciones Bitcoin solo tenían dos transacciones, lo que se debe a que las víctimas realizaban la transacción del pago y el propietario enviaba este dinero a otras direcciones para dificultar el rastreo de la actividad (Kharraz et al., 2015, p.20). Muchos criminales han empleado otras técnicas adicionales que impiden el rastreo de su actividad (utilizar diversas direcciones Bitcoin, pequeñas cantidades de bitcoins, periodo corto de actividad, pequeñas transacciones, etc.) (Kharraz et al., 2015).

De esta forma, se pueden establecer ciertos patrones comunes de comportamiento de las direcciones en la *Blockchain*. Sin embargo, resulta muy complejo determinar direcciones Bitcoin que se dediquen a actividades ilegales basándose únicamente en el historial de transacciones (Kharraz et al., 2015, p.4).

Las investigaciones realizadas en esta materia en su mayoría están destinadas al estudio de los pagos de los rescates con bitcoin, para conocer sus consecuencias financieras (Liao et al., 2016), rastrear los pagos de las víctimas (Huang et al., 2018), identificar y recopilar información sobre transacciones Bitcoin relacionadas con actividades ilícitas (Paquet-Clouston et al., 2019). O para el desarrollo de herramientas de análisis forense de la Bitcoin *Blockchain* como "BitIodine", para la que se comprobó su eficacia con varios casos de *ransomware* como "Cryptolocker" (Spagnuolo et al., 2014). Esta herramienta permite analizar la *Blockchain*, agrupar las direcciones que pueden pertenecer a una misma identidad, clasificar las identidades, etiquetarlas y visualizarlas (Spagnuolo et al., 2014).

Otros Casos Relevantes de *Ransomware.* Desde la incorporación de Bitcoin como forma de pago en el *ransomware* "Cryptolocker", surgieron muchas otras variantes similares[159]. Una de ellas, similar a la anterior fue el *ransomware* "CryptoWall", para el que se estimó que infectó a más de 600.000 sistemas, retuvo 5 billones de archivos como rehenes y generó más de un millón de dólares en Bitcoin con pagos que oscilaron entre 200 y 10.000 dólares (Constantin, 2014).

Otro de los *ransomware* considerables en la historia de estos delitos fue "Ryuk", creado a partir del código fuente del *ransomware* "Hermes", que se encontraba a la venta en foros y que fue utilizado por múltiples actores de amenazas. Sin embargo, "Ryuk" únicamente ha sido utilizado por el grupo criminal "Wizard Spider" y de la misma forma que otros *ransomware* como "Samas" y "BitPaymer" tuvo como objetivo entornos empresariales. La empresa "Crowdstrike" calcula que desde su aparición el grupo criminal de Ryuk ha acumulado más de 705,80BTC en 52 transacciones por un valor de 3.701.893,98 dólares (Hanel, 2019).

También fue muy importante en la historia de estos delitos el *ransomware* "WannaCry". Se creó en el año 2017 y constituyó el "mayor brote de *ransomware* de la historia" afectando a más de 300.000 ordenadores en 150 países diferentes (Sattler, 2017), obteniendo un beneficio de 55,34 bitcoins, lo que suponía aproximadamente 100.000 dólares en bitcoins entre seis direcciones implicadas (Paquet-Clouston et al., 2019, p.7). Este se distribuía a través de *spam* y se propagaba dentro de una organización como un gusano, cifrando todos los archivos del sistema que quedaban inaccesibles hasta que se llegara a pagar la cantidad de 300 dólares en Bitcoin (Sattler, 2017).

En España también han tenido lugar ataques *ransomware* a entidades conocidas tanto de carácter público como privado. Uno de ellos fue el ataque a la empresa "Telefónica" en el 2017 por una variante del *ransomware* "WannaCry" conocida como "WannaDecryptor". Este ataque que fue provocado por una vulnerabilidad del sistema operativo "Windows" que afectó a la red corporativa de toda España bloqueando la intranet de la empresa, cifrando los datos de varios equipos y pidiendo un rescate de 300 dólares en bitcoins para liberarlos (Martí, 2017). Otro ejemplo fue el ataque que sufrió el Ayuntamiento de Jerez que bloqueó el acceso a los servidores internos y a internet, dejando paralizados a los trabajadores que

[159] Véase Hampton y Baig (2015) para una revisión sistemática de los *ransomware* relevantes que han surgido desde el año 1989 hasta el año 2014. Véase también Paquet-Clouston et al. (2019) y Oz et al. (2021) para otros ejemplos de estudios sobre diversas familias de *ransomware*.

utilizaban la red interna. Según fuentes el *malware* responsable ha sido el *ransomware* "Ryuk" que cifró la base de datos del ayuntamiento y pedía un rescate en criptomonedas. Se cree que fue resultado de la instalación de un antivirus gratuito en lugar de uno de pago (Masjerez, 2019; Pérez, 2019). El *ransomware* "Ryuk" también afectó a las plataformas de telecomunicaciones de la empresa de seguridad "Prosegur" en el año 2019 (Prosegur, 2019) y a la "Cadena Ser", que en este caso solo recibió una dirección de correo y el nombre del virus (Pérez, 2019). También el Hospital Universitario de Torrejón de la Comunidad de Madrid confirmó en un comunicado haber sido víctima de un "virus similar al que han tenido otras entidades públicas y privadas en el pasado" (Hospital Universitario de Torrejón, 2020). Fue el primer hospital en España que fue víctima de este ataque que dejó a todos los profesionales sin acceso a los historiales clínicos, que tuvieron que realizar su labor de forma analógica.

Evitar Ser Víctima de un *Ransomware.* Aunque las víctimas suelen ser elegidas al azar en la red, la agencia Europol (2019) ha detectado que en los últimos años los ataques están siendo dirigidos hacia organismos públicos y empresas privadas. Los delincuentes han encontrado que es más probable que este tipo de víctimas pague el rescate por temor la pérdida temporal o permanente de la información y a la paralización de la actividad normal, lo que ocasionaría grandes pérdidas económicas y daños de reputación (INCIBE, 2019). Aunque lo habitual no es dirigirse a grandes empresas como sucedió en el caso de la empresa "Telefónica", sino a pymes y autónomos, donde la ciberseguridad y la repercusión son menores y las posibilidades de extorsión, por lo tanto, mayores (Rodríguez, 2019).

La proliferación del pago con Bitcoin del rescate exigido en el *ransomware* ha ocasionado que las empresas, especialmente aquellas empresas más pequeñas, obtengan reservas de bitcoins como medida proactiva en el caso de que se vean afectadas por una infección de *ransomware* (Higgins, 2016). Los daños que puede ocasionar un ataque de este tipo en una empresa en cuanto a tiempo y dinero se han posicionado entre una de las principales preocupaciones de las empresas, que adoptan medidas para impedir que las consecuencias sean más graves de lo previsto. No obstante, no se recomienda el pago a los criminales. Aunque se devuelvan los datos, no se garantiza que el *malware* ya no esté en el sistema y que pocos meses después vuelva a actuar. Tampoco se garantiza el descifrado y la recuperación de los archivos afectados. Finalmente, también se estaría fomentando la proliferación de estos ataques (No More Ransom, 2020c).

Apropiación de las Criptomonedas Mediante el Engaño. Estafas.

Dentro de todo el panorama de delitos en los que han intervenido de algún modo las criptomonedas, en el año 2021 el delito de estafa fue el delito más registrado seguido del robo, la mayoría de los cuales ocurrieron mediante la piratería de empresas de criptomonedas (Chainalysis, 2022). Esto supuso un aumento del 82% de los delitos basados en criptomonedas durante ese año, lo que se correspondía con el robo de 7800 millones de dólares en criptomonedas a las víctimas (Chainalysis, 2022).

En concreto en España, los delitos de estafa en la criminalidad *online* fueron aproximadamente el 65% del total de todos los procedimientos judiciales para el año 2019 (Fiscal General del Estado, 2021). De acuerdo con esto, los delitos contra el patrimonio, en especial, los delitos de estafa han constituido el delito predominante entre los delitos basados en criptomonedas en España (Aránguez, 2020; Pérez, 2020; Saldaña-Taboada, 2022).

El delito de estafa consiste en que una persona con ánimo de lucro utiliza el engaño bastante para producir error en otro e inducirle a realizar un acto de disposición en perjuicio propio o ajeno (Artículo 248 CP). En el ámbito de las criptomonedas, este delito consistirá en engañar a un sujeto para apropiarse de sus criptomonedas y conseguir beneficios económicos.

Aspectos que Favorecen la Comisión de Estafas con Criptomonedas

Desde una perspectiva criminológica, se ha considera que las criptomonedas presentan ciertas características que podrían favorecer el desarrollo del delito de estafa. Se considera como un producto intangible e ininteligible, que son elementos esenciales en el engaño propio del delito de estafa (Aránguez, 2020, p. 88). Bastaría con asegurar que se trata de un servicio de compra de criptomonedas y apropiarse de la inversión realizada por el sujeto (Aránguez, 2020, p. 88).

El elevado valor del precio de criptomonedas como Bitcoin y su utilización masiva ha podido motivar a la población a obtener este tipo de tecnología para poder beneficiarse de su inversión de igual forma. Sin embargo, en muchas ocasiones la población conoce los beneficios económicos excepcionales de la inversión, pero no son conocedores de sus riesgos. Los riesgos de las inversiones en este tipo de tecnología, en especial en ICOs, han sido señalados por diversos actores tanto a nivel internacional como europeo, como ha sido el caso del Banco de España o la Comisión Nacional del Mercado de Valores. Sin embargo, en muchas ocasiones la promesa de obtener elevados beneficios ha superado a las posibles consecuencias o riesgos de esta actividad.

La relevancia de las criptomonedas en los delitos de estafa ha sido tal, que incluso

algunos autores han llegado a considerar la tecnología como una estada en sí misma, señalando su funcionamiento como una sofisticada estafa piramidal[160], que es compleja de eliminar debido a la dificultad para identificar a sus autores y abarcad su alcance planetario (Aránguez, 2020, p.86-87). No obstante, aunque se hayan visto elevados casos de delitos de estafa en los que intervienen las criptomonedas, en este trabajo no serán consideradas como estafas en sí misma, sino como una herramienta tecnológica que ha podido favorecer el desarrollo de este delito, pero que al mismo tiempo también ha servido a propósitos legales de la utilización de estas monedas virtuales.

Tipos de Estafa Relevantes en los que Intervienen las Criptomonedas

Dentro de este ámbito se han descubierto diversas formas de cometer un delito de estafa en el que estén implicadas de alguna forma las criptomonedas. Vasek y Moore (2015) fueron los primeros en estudiar la presencia de estafas basadas en Bitcoin que, a partir de una muestra de 192 estafas, determinaron que existían cuatro grupos: Esquemas Ponzi o estadas piramidales, estafas de minería, billeteras fraudulentas y casas de cambio fraudulentas. No obstante, señalan que la mayoría de las estafas en este ámbito están centradas en las estafas piramidales, las ofertas iniciales de monedas (ICO) fraudulentas, la manipulación del mercado de criptomonedas, los *honeypots* de *Blockchain* y las estafas de *phishing.*

De esta forma, en este apartado se tratarán mayormente los fraudes de inversión, en especial las estafas piramidales, por la relevancia que han tenido en cuanto al número de casos disponibles, víctimas afectadas y daños económicos. No obstante, también se ha incluido un apartado en el que se tratarán otro tipo de estafas que también han sido importantes en esta materia como las conocidas como *Rug pulls* o "tirones de alfombra" y aquellas relacionadas con la pandemia COVID-19.

[160] Las razones por las que el Prof. Carlos Aránguez considera Bitcoin como una estafa piramidal se describen con detalle en su trabajo "El Bitcoin como instrumento y objeto de delitos" (2020). Pero de forma resumida son: ausencia de un producto real, se genera en bloques o escalones que requieren de nuevos participantes, se requiere de un mayor esfuerzo progresivo para sostener la pirámide, anonimato, fuerte campaña de marketing de promoción del producto, confianza irracional de los consumidores, extrema volatilidad y una ausencia total de garantía (pp.101-102).

Estafas piramidales o Esquemas Ponzi. Fraude de inversión. El delito más reconocido en este ámbito es el de las estafas piramidales o esquemas Ponzi. Este tipo de estafa consiste en el desarrollo de una organización que tiene como objetivo asegurar fondos a los criminales durante un periodo de tiempo determinado a partir del dinero proporcionado por las nuevas incorporaciones a la trama.

Es difícil determinar el impacto económico de los esquemas Ponzi debido a la falta de conjuntos de datos de direcciones de Bitcoin (Bartoletti et al., 2018). Esto es, aunque puedan consultarse de forma pública en la *Blockchain* las direcciones de las carteras, no se dispone de los datos suficientes para determinar que un conjunto de direcciones en específico estuvo implicado en una trama de estafa piramidal con criptomonedas, por lo que es complejo estimar el impacto económico total de estos delitos.

Un ejemplo de un esquema Ponzi basado en Bitcoin fue "Bitcoin Savings & Trust" en el que se captaban a las víctimas prometiéndoles la obtención de altas tasas de interés en sus inversiones. De la misma forma que las estafas piramidales clásicas, en este caso los primeros inversores reciben los rendimientos prometidos para afianzar la confianza en la organización y atraer a nuevos inversores que aportaran el dinero con el que se pagaría a los inversores anteriores. Esta estafa comenzó en noviembre de 2011 y continuó admitiendo nuevos miembros hasta agosto de 2012 en el que el propietario de la estafa "Trendon Shavers" anunció que lo cerraría (Jeffries, 2012).

En España también han tenido lugar diversas estafas piramidales basadas en criptomonedas detectando a finales del año 2021 un incremento en las denuncias por inversiones y transacciones en moneda electrónica (González, 2021). La mayoría de los casos analizados en la jurisprudencia penal española en materia de criminalidad y criptomonedas pertenecen a delitos contra la propiedad, en concreto a delitos de estafa (Aránguez, 2020; Pérez, 2020; Saldaña-Taboada, 2022).

Un ejemplo de esto se puede observar en la jurisprudencia penal española con el caso de la empresa "Cloud Trading & DEVS LTD" que suscribe varios contratos de "Trading de Alta Frecuencia" por los que se compromete a gestionar los bitcoins de cinco personas debiendo reinvertir los eventuales dividendos y entregar las ganancias al vencimiento a cambio de una comisión. No obstante, desde el principio el sujeto no tenía intención ninguna de llevar a efecto lo acordado, como así se demuestra por la inexistencia de operación alguna relacionada con la inversión de las criptomonedas entregadas, siendo su único propósito el de apropiarse de las criptomonedas recibidas (TS (Sala de lo Penal, Sección 1ª), sentencia núm.

326/2019 de 20 junio [RJ 2019\2925] y AP Madrid (Sección 3ª), sentencia núm. 185/2018 de 7 marzo [JUR 2018\133414]).

En el año 2022 se detuvo en Valencia a uno de los mayores estafadores con falsas inversiones en criptomonedas en el ámbito europeo que consiguió con esta actividad un patrimonio superior a 2,5 millones de euros (El País, 2022). El sujeto creó una plataforma de inversión en criptomonedas que ofrecía una rentabilidad mínima del 2,5% semanal a los inversores según la cantidad de dinero aportada. No obstante, las ganancias que obtenían los inversores procedían de otros inversores que habían sido persuadidos a participar en la inversión mediante engaño (El País, 2022).

De esta forma, para el año 2021, la Audiencia Nacional ya investigaba tres grandes casos de criptoestafas: "Arbistar", "Algorithms", "Kualian" (Gálvez, 2021). En el habla hispana se dice que el caso "Arbistar" ha sido el más importante hasta la fecha. Se trataba de una empresa que ofrecía servicios de *trading* automático, comprando y vendiendo criptomonedas empleando un algoritmo (*Community bot*) que aprovechaba las diferencias de cambio que había entre las diferentes empresas dedicadas a convertir criptomonedas en monedas fíat (Aránguez, 2020).

La empresa tinerfeña comenzó en el año 2019 y en el año 2020 comenzaron las primeras denuncias, llegando el caso a la Audiencia Nacional en abril del año 2021. Aunque todavía se siguen sumando afectados, en septiembre de 2021 la cifra de afectados alcanzó 3500 personas y alrededor de 500 millones de euros (Europa Press, 2021). Este caso finalizó antes de lo esperado por los propios autores, ya que la situación de pandemia ocasionada por la COVID-19 aceleró la demanda de los reintegros de los inversores (Aránguez, 2020, p. 90).

En la mayoría de los casos estudiados se han realizado ingentes campañas de publicidad y promesas de rentabilidades desorbitadas de hasta el 15% o 25% (Gálvez, 2021). De esta forma, se puede decir que la publicidad desmesurada es una de las características relevantes para este tipo de delito habiendo invertido mucho más dinero en este aspecto que en ingeniería informática (Gálvez, 2021). El líder del caso "Algorithms", por ejemplo, tenía una gran habilidad con las relaciones sociales, organizaba eventos entre sus inversores e invertía una gran cantidad de dinero en publicidad (Gálvez, 2021).

Este aspecto se ha considerado relevante para influir en la toma de decisiones de un sujeto sobre la inversión en criptomonedas, especialmente porque en España el uso que se hace de las criptomonedas es en su mayoría un uso indirecto. Esto es, los criminales no usan las criptomonedas como medio financiero, sino como un cebo o reclamo en la organización de delitos de estafa con el pretexto de participar en la inversión en criptomonedas o en una

oferta inicial de criptomonedas (Pérez López, 2017). De esta forma, consiguen los fondos de aquellas personas, que poco conocedoras del funcionamiento de las criptomonedas, transfieren sus fondos a los criminales. Tal ha sido la importancia de la publicidad en las criptoestafas que la CMNV elaboró una Circular con la finalidad de desarrollar las normas, principios y criterios a los que debe ajustarse la actividad publicitaria sobre criptoactivos[161].

Otros Tipos de Estafas en los que Intervienen las Criptomonedas. No obstante, las estafas piramidales no son los únicos delitos de estafa en los que se han visto involucradas las criptomonedas.

A nivel internacional, de los 7800 millones de dólares en criptomonedas que perdieron las víctimas, más de 2.800 millones de ese total procedían de delitos como los *Rug Pulls* o "tirón de alfombra" (Chainalysis, 2022). Este tipo de estafa consiste en el desarrollo de un proyecto legítimo de criptomonedas, generalmente de nuevos tokens, para el que se pide la inversión de usuarios interesados en el proyecto. Una vez los desarrolladores han obtenido el dinero de las inversiones, abandonan el proyecto y desaparecen con la liquidez del activo (Chainalysis, 2022).

En este caso se trata de un tipo de estafa del ecosistema de finanzas descentralizadas (DeFi). Sin embargo, no todos los delitos *Rug Pulls* comenzaron como proyectos DeFi. El mayor caso de estafa de este tipo tuvo lugar con "Thodex", una casa de cambio centralizada de Turquía en la que el director ejecutivo (CEO) de la empresa se apropió de cientos de millones de dólares en criptomonedas y desapareció tras impedir que los usuarios pudieran retirar sus fondos (Herrera, 2021). Aunque este caso supuso aproximadamente el 90% del valor de los *Rug Pulls* para el año 2021, el resto de los casos sí que estaban vinculados con proyectos DeFi. Uno de los casos más conocidos y relevantes en este sentido fue el caso "AnubisDAO" que consistía en un proyecto de moneda descentralizada en el que se robaron 58 millones en criptomonedas (Herrera, 2021). Los inversionistas que accedían a participar del proyecto recibían el token "ANKH" a cambio del financiamiento, recaudando así alrededor de 60 millones de inversionistas (Herrera, 2021).

En el año 2020, el aumento del miedo y de la incertidumbre ocasionados por la situación de pandemia de la COVID-19 ocasionaron un aumento de los delitos de estafa en las que estaban involucradas las criptomonedas (FBI, 2020). El contenido de estos delitos se

[161] Circular 1/2022, de 10 de enero, de la Comisión Nacional del Mercado de Valores, relativa a la publicidad sobre criptoactivos presentados como objeto de inversión. https://www.boe.es/boe/dias/2022/01/17/pdfs/BOE-A-2022-666.pdf

asemejaba mucho a los delitos tradicionales de estafa, con la diferencia de que se adaptaban a la temática del COVID-19. De esta forma, se mostraban casos en los que se decía conocer la información personal de una persona y se amenazaba con la infección de COVID-19 si no realizaba el pago exigido; los criminales se hacían pasar por empleadores para pedir donaciones; se ofrecían falsos productos para prevenir la infección del COVID-19 aceptando el pago con criptomonedas o se ofrecían nuevos proyectos de criptomonedas para los que se requería la inversión de las víctimas (FBI, 2020). Un ejemplo de este tipo de delitos lo constituyó una estafa en la que los criminales se hicieron pasar por la Organización Mundial de la Salud para solicitar donaciones con el fin de prevenir la expansión de la COVID-19 (Partz, 2020).

A pesar de que tuvieron lugar en un corto espacio de tiempo, el elevado número de casos que se sucedieron atrajeron el interés de los investigadores, que disponían de información suficiente para el estudio de esta nueva tipología delictiva. La primera investigación en estudiar las estafas con criptomonedas con temática COVID fue el de Xia et al. (2020) que a partir de una muestra de 195 estafas de esta tipología establecieron seis categorías: 1) estafa de tokens; 2) estafa de salida; 3) estafa de chantaje; 4) estafa basada en la utilización de un *malware*; 5) esquema Ponzi o estafa piramidal y 6) estafas de donación en criptomonedas (Xia et al., 2020).

Evitar ser Víctima de un Delito de Estafa Cometido con Criptomonedas

La prevención de estos delitos debería comenzar con una mejor comunicación entre el sector público y privado que permita a los inversores conocer los riesgos de estas actividades y evitar su implicación en proyectos de dudosa fiabilidad (Chainalysis, 2022). Esto resultaría de especial relevancia en España donde el uso que se hace de las criptomonedas consiste en un cebo o reclamo para invertir (Pérez López, 2017). De esta forma, consiguen los fondos de aquellas personas que son poco conocedoras de las criptomonedas y de los riesgos que pudieran suponer para sus fondos la inversión en esta tecnología, por lo que transfieren sus fondos a los criminales y pierden su inversión.

Desde un punto de vista más técnico, otra de las medidas que se podrían tomar en este sentido, podría ser la realización de una auditoría externa del código del contrato inteligente que está detrás de un nuevo token o proyecto DeFi para estudiar el riesgo de que los desarrolladores puedan abandonar el proyecto con los activos de los inversores (Chainalysis, 2022).

No obstante, parece ser relevante en esta materia la elaboración de planes de

prevención que tengan como objetivo principal advertir y educar a la población en los potenciales riesgos que existen en la actividad de inversión en criptomonedas. De esta forma, aunque proliferen las campañas publicitarias centradas en los elevados beneficios que se pueden obtener con esta actividad, la población podría reconocer al mismo tiempo los riesgos existentes y valorar la posibilidad de invertir sus fondos.

La Utilización de Criptomonedas Como Forma de Pago de Productos y Servicios Ilegales

Las criptomonedas han sido utilizadas como forma de pago de productos y servicios ilegales de diversa naturaleza. Las características propias de esta tecnología han permitido a las partes interesadas en la compraventa realizar la transacción garantizando la privacidad de su actividad. Esto ha motivado que las criptomonedas y en especial Bitcoin, se hayan introducido como forma de pago en diversos negocios criminales, sobre todo en aquellos que tienen lugar en los mercados delictivos *online*.

En cuanto al pago de productos, se pueden ver algunos casos en la jurisprudencia penal española en los que se ha utilizado esta tecnología. Se ha observado que se han utilizado criptomonedas para la compra de los materiales o los bienes necesarios para cometer otros delitos, la compra de productos ilegales para su distribución y venta (p.ej. drogas) o el pago de servicios delictivos que permiten el desarrollo de otros delitos. En el primer caso se trataba de una organización criminal dedicada a la falsificación de billetes de 50 euros y que utilizaba las criptomonedas para comprar los materiales necesarios para esta actividad[162]. En otro caso, el sujeto utilizaba las criptomonedas para comprar tarjetas de crédito robadas que posteriormente utilizaba para comprar productos *online*[163]. Por último, otro caso consistía en una organización criminal que fue acusada de delitos contra la salud pública y que utilizó la criptomoneda Bitcoin para comprar anfetaminas en la DN que posteriormente introducían en su negocio de tráfico de drogas[164]. En la mayoría de los casos los productos obtenidos no son legales, por lo que su venta se realiza habitualmente a través del mercado negro ubicado en la *Darknet*.

[162] AP Zaragoza (Sección 3ª), sentencia núm. 84/2019 de 21 febrero [JUR 2019\338758].
[163] AP Lleida (Sección 1ª), sentencia núm. 308/2017 de 14 julio [ARP 2017\1322].
[164] TSJ Islas Canarias, Las Palmas (Sala de lo Civil y Penal, Sección 1ª), sentencia núm. 39/2018 de 28 septiembre [JUR 2018\312883]; AP Santa Cruz de Tenerife (Sección 2ª), sentencia núm. 29/2018 de 29 enero [JUR 2018\204653] y AP Santa Cruz de Tenerife (Sección 2ª), sentencia núm. 294/2018 de 3 octubre [JUR 2019\51117].

No obstante, la utilización de las criptomonedas en el ámbito criminal requiere de cierta formación que puede escapar a las capacidades de muchas personas, especialmente si se desea mantener las medidas de seguridad adecuadas para evitar la detección de las autoridades. O, por el contrario, algunas personas, independientemente de la capacidad que dispongan para utilizar esta tecnología, prefieren delegar la utilización de esta herramienta en otros profesionales. A tal efecto, han surgido negocios que ofrecen como servicio el desarrollo de actividades criminales de forma remunerada, lo que se conoce como *crime-as-a-service* (CaaS) o "delincuencia como servicio".

La primera vez que se menciona el término *crime-as-a-service* o "delincuencia como servicio" fue en un informe IOCTA elaborado por Europol en el año 2014. Tuvo su origen en la economía fragmentada de los grupos delictivos, que presentan un conjunto muy diverso de competencias y áreas de especialización. Esta división del trabajo y la adopción de funcionalidades es lo que impulsa la economía delictiva y ha creado una próspera industria "as-a-service", ya que estas habilidades pueden monetizarse y crear un acceso mucho más amplio a capacidades delictivas que antes habrían requerido habilidades excepcionales (Europol, 2014). En definitiva, se planteaba que los grupos criminales especializados y con habilidades determinadas en un ámbito criminal, pudieran ofrecer estas capacidades como servicio a otros grupos que requieran de esa tarea en su actividad criminal.

El espacio en el que el resto de los delincuentes podían encontrar estos servicios solía ser en sitios web y foros alojados inicialmente en la *Deep Web*, pero que más tarde acabaron alojándose en la *Darknet* (Europol, 2014). En esta última se aprovechan de mecanismos de anonimato que ocultan la identidad de los usuarios, dificultando su rastreo y acceso, lo que ha dado lugar a "servicios ocultos" como foros clandestinos o mercados delictivos (Europol, 2014).

De la misma forma que en la compra de productos ilegales, las criptomonedas tienen un papel relevante en el CaaS como forma de pago de estos servicios. Suponen un mecanismo adicional que junto con los anteriores relativos a la DN permite a los criminales garantizar la privacidad de su actividad.

Según el IOCTA 2014, actividades como el *crime-as-a-service* ofrecen una amplia gama de servicios comerciales que facilitan casi cualquier tipo de delito (Europol, 2014). Los delincuentes podrían obtener servicios como el alquiler de *botnets*, ataques DDoS, desarrollo de *malware*, robo de datos y contraseñas para cometer delitos por sí mismos. Esto ha facilitado el desplazamiento de los grupos tradicionales de delincuencia organizada hacia los ámbitos de la ciberdelincuencia. El beneficio que pueden reportar estos servicios estimula la

comercialización de la ciberdelincuencia, así como su innovación y mayor sofisticación (Europol, 2014). Según el tipo de servicio que se ofrezca, pueden adquirir diversos nombres. Así, se puede encontrar el término *Malware-as-a-Service* (MaaS) cuando se ofrece como servicio el desarrollo o la utilización de *malware* o *Ransomware-as-a-Service* (RaaS) cuando el *malware* concreto que se ofrece es un *ransomware* permitiendo a cualquier persona con bajos conocimientos en la materia ejecutar un ataque *ransomware* utilizando herramientas automatizadas (Nadir y Bakhshi, 2018).

En la jurisprudencia penal española también se puede ver el pago en criptomonedas por algunos servicios como la utilización de una *botnet* AN (Sala de lo Penal, Sección 4ª), auto de 3 octubre 2017. [JUR 2017\243297].

No obstante, en este ámbito resulta especialmente relevante por la dificultad de su persecución y la vulnerabilidad de sus víctimas, el servicio de explotación sexual infantil *online*, que se explica de manera detallada en el apartado siguiente.

Live Distant Child Abuse (LDCA)

De la misma forma que ha sucedido con algunos delitos considerados como tradicionales (p.ej., las estafas), las tecnologías han modificado la forma en la que se distribuye y se crea el material con contenido de explotación sexual infantil. De forma habitual, este tipo de material es compartido y distribuido mediante redes *peer-to-peer* que permiten el contacto entre personas directamente. Sin embargo, esta forma de distribuir el contenido tiene una serie de riesgos para los delincuentes como que estos archivos quedarán almacenados en el dispositivo o incluso que proporcionan un dudoso anonimato.

Aunque se puede encontrar material pornográfico infantil en la DN, la distribución de este material de forma libre no genera beneficios para la persona que lo pone a disposición del resto de usuarios. De esta forma, surgió una nueva tipología delictiva que pretendía beneficiarse del anonimato que ofrece la conexión *streaming* para ofrecer servicios de explotación sexual infantil en directo y así obtener beneficio económico.

Esta nueva tipología delictiva se conoce como *Live Distant Child Abuse* (LDCA) o Abuso Sexual infantil en directo a distancia y es señalada por Europol (2017) como un tipo complejo de explotación sexual infantil *online* a tener muy en cuenta como amenaza emergente por sus peculiaridades y por la gravedad de sus consecuencias.

En el *Live Distant Child Abuse* (LDCA), un sujeto desde cualquier parte del mundo puede pagar para acceder a una conexión en directo en la que un menor es obligado a mostrar comportamientos sexuales o es forzado a ser víctima de abuso sexual delante de una *webcam*

y en directo (ECPAT, 2019). Tiene lugar a través de aplicaciones de vídeo chat o de salas de chat *online* e incluso se le permite al sujeto que ha pagado por la conexión hacer peticiones. Para el buen desarrollo de la actividad, existe la figura del mediador que puede ser un miembro de la familia u otra persona interesada en el negocio. Esta persona se encarga de forzar al menor a enfrentarse a la *webcam* y comunicarse por esta y le da acceso al delincuente para que pueda ver y participar a distancia en el abuso. Normalmente, se acuerda la hora y el medio en el que tendrá lugar la actividad para que la persona que quiere participar a distancia pueda conectarse (ECPAT, 2019).

Para poder pagar por este "servicio" son frecuentes los métodos de pago *online*, los servicios de transferencia de dinero y los centros de pago locales. Además, también se ha detectado el uso de criptomonedas como el Bitcoin (Europol, 2018, p.35). De esta forma, el papel de las criptomonedas en este delito es el de constituir la forma de pago por un servicio, el material pornográfico infantil en directo o por un producto, el menor o la menor víctimas de esta práctica.

Se ha visto algunos negocios estructurados en países no europeos explotando las oportunidades comerciales del LDCA. Sin embargo, aunque es materia de los informes IOCTA, no se considera que los autores de este tipo de delito formen parte de organizaciones criminales, ya que no se trata de un delito especialmente rentable. Los delincuentes en estos casos son mayormente actores solitarios que están poco o nada implicados en las organizaciones criminales de carácter tradicional, pero que se organizan entre ellos, se reúnen en foros en línea donde distribuyen material y comparten técnicas y métodos para escapar de la detección de las fuerzas policiales (Europol, 2018).

Este delito es predominante en países como Filipinas o Kenia donde las familias más pobres aceptan que sus hijos/as menores de edad e incluso menores de 13 años, formen parte de los negocios que se regentan en este país en los que tiene lugar este tipo de delito y desde donde se conecta con otros países (Martínez, 2015). Dado que en la mayoría de los casos no existe un contacto físico entre el adulto y el menor y no hay riesgos físicos, las familias no ven esta actividad perjudicial y favorecen que sus hijos/hijas participen para obtener ingresos extra.

Se trata de un delito de gravedad que ha preocupado a las autoridades debido a que los autores de este son difícilmente detectados y permanecen casi en el anonimato sin dejar rastro. El contenido consumido no se almacena, graba o descarga, los rostros de las personas que contratan el servicio no son visibles al otro lado de la cámara y el método de pago empleado como son las criptomonedas dificulta la detección de estas transacciones. Además,

en ocasiones el contacto con la persona encargada del negocio tiene lugar a través de la *Darknet.* Todo ello, unido a que se trata de víctimas de especial vulnerabilidad, que ven afectados sus derechos además de su desarrollo físico y psicológico.

Mercados Delictivos Online. Criptomercados.

Las actividades delictivas *online* suelen estar relacionadas con espacios de venta ubicados en la Internet profunda, difícilmente accesibles para la mayoría de la población y que permiten ocultar la ilegalidad de los negocios. En este punto, han adquirido gran importancia los mercados delictivos alojados en la *Darknet* (DN) considerada como el espacio en el que los mercados delictivos podrían garantizar la privacidad de su actividad.

Al mismo tiempo, no toda la actividad de compraventa de productos ilegales está ubicada en mercados *online* de la *Darknet,* sino que una gran parte de los negocios, especialmente los de venta de drogas, como las más comúnmente consumidas, pueden encontrarse en la conocida "web superficial", cuyo contenido es fácilmente accesible por cualquier persona que utilice un motor de búsqueda convencional. Los mercados de la DN no permiten el desarrollo de cualquier tipo de actividad delictiva que se desee, además de que requieren de determinadas capacidades para su acceso, por lo que su utilización podría limitar en algunos casos los beneficios esperados por el negocio ilegal.

Sin embargo, la DN y los mercados delictivos que tienen lugar en este espacio merecen una atención especial ya que han supuesto un cambio en la forma en la que se han desarrollado muchos negocios ilegales, especialmente los relacionados con la venta de drogas *online.* Además, aunque la criptomoneda Bitcoin en la actualidad se vincula con una gran variedad de delitos, en sus inicios tuvo su primer reconocimiento en el ámbito criminal con su introducción como forma de pago en los mercados delictivos *online* de la DN. Los mercados ubicados en la DN constituían un espacio que atraía a los criminales interesados en garantizar la privacidad de la actividad en sus negocios criminales.

***Deep Web* y *Darknet*.** Aunque en ocasiones se emplean ambos términos de forma indistinta, *Deep Web* y *Darknet* no son sinónimos. El término *Deep Web* o "web profunda" hace referencia a aquella parte de Internet que no es accesible empleando los motores de búsqueda tradicionales (información y bases de datos protegidas por contraseñas y que pertenecen a agencias gubernamentales, bibliotecas o universidades). Supone la totalidad de todo el contenido de Internet, de forma que la web superficial o el Internet al que se accede habitualmente supone solo un pequeño porcentaje de la totalidad del contenido de Internet. Por otro lado, el término *Darknet* o "red oscura" hace referencia a aquel contenido de la *Deep Web* que está dedicado al desarrollo de algún tipo de actividad delictiva.

Dado que no es posible acceder al contenido de la *Deep Web* y de la *Darknet* empleando los motores de búsqueda tradicionales (p.ej. "Google" o "Yahoo!"), será necesario utilizar la herramienta de cifrado TOR (*The Onion Router).* Se trata de una herramienta de libre acceso y que fue creada por el gobierno de Estados Unidos como parte del proyecto *US Naval Research Laboratory* desde 2004 a 2005 para garantizar el anonimato de los usuarios a través de un mecanismo de encriptado múltiple. Actualmente su desarrollo y mantenimiento está a cargo de TOR Project[165].

Su creación ha sipo posible gracias al desarrollo de tecnologías anteriores que surgieron de diversas investigaciones en la década de 1990 con el propósito de crear una forma de conectarse a Internet sin revelar el usuario, la persona con la que se está contactado o el monitoreo de la red (TOR Project, 2023).

Como resultado de estas investigaciones se desarrolló el *Onion Routing* o "enrutamiento de cebolla" que permitía usar Internet con una mayor privacidad enrutando el tráfico a través de múltiples servidores y cifrando cada paso en el camino (TOR Project, 2023). Si se explica con más detalle, el *Onion Routing* es una red de superposición distribuida diseñada para anonimizar aplicaciones basadas en TCP[166] como navegación web, *Shell* seguro y mensajería instantánea (Dingledine et al., 2004). Los clientes eligen una ruta a través de la red y construyen un circuito en el que cada nodo o *onion routing* en la ruta conoce a su predecesor y sucesor, pero ningún otro nodo en el circuito (Dingledine et al., 2004).

[165] TOR Project https://www.torproject.org/

[166] Un TCP o protocolo de control de transmisión es uno de los principales protocolos en las redes TCP/IP. Permite establecer conexiones en una red de datos compuesta por una red de ordenadores. A diferencia de las IP, el TCP permite que dos *hosts* establezcan una conexión e intercambien flujos de datos. Garantiza que los paquetes se entregarán en el mismo orden en que se enviaron.

En la década de los 2000, Roger Dingledine continuó trabajando en este proyecto y le puso el nombre por el que se le conoce actualmente, *The Onion Routing* (TOR) que lo definió como un servicio de comunicación anónimo de baja latencia basado en circuitos (Dingledine et al., 2004). De forma general, el funcionamiento de TOR se describe como un encriptado múltiple de los datos a través de varios nodos o "TOR *relays*" de la red. Para ello se sirve de una serie de "voluntarios" que pertenecen a la red de servidores y que ocultarán la información de los usuarios eludiendo cualquier actividad de monitoreo. En este punto, comprender el funcionamiento de la red TOR requiere entender en qué consiste el término "*relay*". Este constituye un servidor al que cualquier usuario podrá solicitar que su actividad sea enrutada a través de este. De esta forma, la actividad del usuario pasa a través del servidor y es ocultada ante cualquier observador, que podría ver cómo el tráfico sale del servidor, pero no podría determinar qué usuario es el que está accediendo a un sitio determinado. Este tráfico se dice que está encriptado, lo que garantiza su ocultación. Sin embargo, para evitar que un *relay* sea malicioso y se ponga en riesgo el anonimato y la privacidad, el usuario debería elegir tres servidores y encadenarlos (*Three-hop Tor Circuits*), de forma que se reducen las posibilidades de que un atacante pudiera controlar los servidores (Owen y Savage, 2015).

Sin embargo, aunque TOR ya era utilizado por activistas y usuarios expertos en tecnología, todavía era difícil de utilizar para personas con menos conocimientos, por lo que en el año 2005 se comenzaron a desarrollar otras herramientas más allá del proxy Tor. En el año 2008 se desarrolló el navegador Tor (Tor project, 2023).

El funcionamiento de TOR ha sido descrito de una forma más detallada por Paganini (2012) empleando el clásico escenario entre Bob y Alice. En primer lugar, Alice realiza una conexión no encriptada hacia un servidor centralizado que contiene todas las direcciones de los nodos de TOR. Una vez recibida esta lista, el cliente TOR del software se conecta a un nodo aleatorio por medio de una conexión encriptada (nodo de entrada). El nodo de entrada a su vez se conectará de forma encriptada con un segundo nodo aleatorio y hará lo mismo después con un tercer nodo, así hasta terminar con un nodo de salida. Cada nodo es elegido de forma aleatoria cada vez y no puede elegirse el mismo dos veces, estando establecido también un tiempo fijo de duración en el que cada diez minutos el *software* fuerza el cambio de nodo de entrada (Paganini, 2012).

Por todo ello, se espera garantizar que no pueda ser observada la actividad de ningún usuario, evitando su identificación o el conocimiento de los sitios que ha visitado (Owen y Savage, 2015). Inevitablemente estas propiedades han atraído a aquellas personas que desean

desarrollar sus actividades delictivas lejos de la vigilancia de los gobiernos[167]. Sin embargo, no se trata de una herramienta ilegal, ya que es utilizada por una gran cantidad de personas que están preocupadas por su privacidad en Internet y sus derechos digitales y pretenden escapar a la vigilancia masiva del Estado. Por ejemplo, TOR fue una herramienta fundamental durante la "Primavera Árabe" en el año 2010 porque protegió la identidad de las personas en línea y les permitió acceder a recursos críticos, redes sociales y sitios web que estaban bloqueados (TOR Project, 2023).

No obstante, el anonimato en el acceso no es la única característica relevante de TOR, también se caracteriza por permitir el alojamiento de los servicios ocultos o *Hidden Services* (HSes). Esto consiste en la habilidad de alojar una página web o servicio de Internet de forma anónima tanto para la persona que lo visita como para el espacio visitado (Owen y Savage, 2015). A menudo se denomina *Darknet* al conjunto de servicios ocultos de este tipo, pero también existen otras herramientas menos populares que se pueden incluir de este término como los *Invisible Internet Project* (I2P). La localización de la información en los HSes cambia cada día para hacer más difícil para una persona que controle los *relays* donde se guarda esta información (Owen y Savage, 2015).

De esta forma, la DN ha supuesto en el ámbito criminal un espacio que por sus características ha favorecido el desarrollo de determinadas actividades criminales. Sin embargo, hay que señalar que su utilización no ha estado reservada únicamente para este propósito. La *Deep Web* y en cierto modo la DN, también se han constituido como un espacio en el que se desarrollan actividades legales que pueden beneficiarse del anonimato como compartir información sin censura o impedir el control de la actividad en Internet en aquellos gobiernos más autoritarios (Paganini, 2012).

Criptomercados. Silk Road. Especialmente relevante en el ámbito de las criptomonedas han sido el surgimiento de los criptomercados. El término criptomercado, acuñado en foros de hackers de Internet, hace referencia a un mercado situado en la *Darknet* que utiliza criptografía para ocultar la identidad de los usuarios[168].

De forma más detallada, sus principales características son: 1) Constituye una plataforma de un mercado en línea que ofrece multitud de vendedores que ponen a la venta

[167] Merece la pena señalar el hecho de que aunque se trata de una herramienta que ha permitido escapar al control del gobierno y a su capacidad de censurar determinados lugares o contenidos, la organización "Tor project" encargada de la gestión de esta herramienta ha recibido la mayoría de sus fondos del gobierno de los Estados Unidos (Owen y Savage, 2015).

[168] De acuerdo con Barrat y Aldridge (2016), se prefiere la utilización del término "criptomercado" antes que "mercado de la *Darknet"*. Esto se debe por un lado a que puede haber mercados en la DN que no se ajusten a la

una gran cantidad de bienes y servicios ilegales e ilícitos; 2) tienen la apariencia de cualquier mercado que hayamos podido utilizar en la "web superficial"; 3) permiten realizar comparaciones entre productos y vendedores diferentes y 4) se emplean una serie de estrategias para mantener el anonimato de los usuarios, las transacciones y ocultar la localización de los servidores. Servicios de anonimato como TOR e I2P para ocultar la dirección IP del ordenador, criptomonedas descentralizadas y relativamente poco rastreables como Bitcoin y Litecoin para hacer los pagos y comunicaciones encriptadas entre participantes y mercado vía PGP (Aldridge y Décary-Hétu, 2014).

Además de las anteriores, los criptomercados cuentan con otra serie de sistemas para aumentar la confianza de los usuarios y ganar un mayor número de ventas. En primer lugar, cuentan con sistemas de calificaciones de los vendedores y además permiten que los usuarios puedan dar *feedbacks* o escribir reseñas en los foros sobre las compras realizadas o los vendedores (Garcia Sigman, 2017). En segundo lugar, algunos vendedores para ganar la confianza de los usuarios cuentan con un sistema de pago en diferido o *escrow*. De esta forma, el criptomercado no envía el dinero de la compra al vendedor hasta que el comprador ha recibido el producto y está satisfecho con este (Barratt y Aldridge, 2016). No obstante, debido a las conocidas como "estafas de salida" o *exit scams* algunos criptomercados están ofreciendo *multisignature escrow* ya que intervienen al menos dos o tres partes para finalizar la transacción.

Aunque no son necesariamente ilegales, las posibilidades que ofrecen para ocultar la identidad de los usuarios han atraído a aquellos que buscan realizar alguna actividad delictiva, revolucionando la forma en la que se adquirían productos y servicios ilegales. De esta forma, el contenido de los criptomercados de la DN está relacionado con actividades ilegales como la compraventa de drogas y el abuso infantil (Owen y Savage, 2015). Aunque también se han encontrado criptomercados que ofrecían otros productos como información de tarjetas de crédito robadas, documentos de identidad falsificados, ensayos universitarios plagiados, servicios de piratería informática, blanqueo de dinero, armas de fuego y municiones ilegales e incluso asesinatos por encargo (Martin, 2014, p. 356).

Por todo ello, no cabe duda de que para aquel grupo pequeño de personas que contaba con la capacidad tecnológica necesaria para utilizar este espacio, además de la disposición a

definición propuesta, como los denominados como mercados de "proveedor único". Por otro lado, se considera que todo lo que conlleva el término "dark" u oscuro suele asociarse con algo malo, ilegal, prohibido, etc. (Barrat y Aldridge, 2016, p.2) y en este caso los criptomercados no son espacios ilegales necesariamente, puede hacer referencia a los mercados que, empleando las mismas tecnologías, se dedican a la venta de productos legales.

asumir el riesgo, la utilización de este mercado de drogas *online* ha supuesto una revolución en el ámbito de las drogas (Barrat, 2012). Al facilitar las transacciones virtuales anónimas se superan las peligrosas limitaciones físicas de la droga, como el contacto físico entre comprador y vendedor, lo que reduce el riesgo de posibles delitos violentos (Alridge y Décary-Hétu, 2014).

Diversas investigaciones han intentado estimar la actividad que se llevaba a cabo en la *Darknet*. Entre los años 2013 y 2016 en una investigación en la que se estudió el flujo de alrededor de medio millón de bitcoins de 102 entidades ilícitas se mostró que alrededor del 97% de los bitcoins ilícitos registrados procedían de la DN (Fanusie y Robinson, 2018). Investigaciones posteriores han estimado que al mismo tiempo que estaba en funcionamiento uno de los mayores criptomercados de drogas hasta la fecha, el contenido de abuso infantil comenzó a superar en popularidad a la compraventa de drogas (Owen y Savage, 2015). Esto se demostraba en una investigación en la que se recogieron datos del tráfico de TOR en la DN durante seis meses para analizar la popularidad del contenido, descubriendo que Silk Road recibió poco más de 8000 peticiones al día, siendo más popular el contenido de abuso infantil (Owen y Savage, 2015).

No obstante, en lo que respecta a criptomercados hay que hacer una mención especial al primer criptomercado que apareció, *"*Silk Road*"*, por lo que hablar de los orígenes de los criptomercados supondrá hablar de la aparición de este criptomercado. Constituyó uno de los criptomercados más conocidos y relevantes de la DN, que unía todas las tecnologías que hasta la fecha se conocían para garantizar la privacidad de la actividad criminal, como eran TOR, el pago con criptomonedas y la DN (Christin, 2013). Aunque existieron otros mercados delictivos al mismo tiempo que Silk Road como fueron "Black Market" o "The Armony", este criptomercado contaba con una gran popularidad especialmente fomentada por los medios de comunicación, llegando a disponer de entre 30.000 a 150.000 clientes (Christin, 2013).

Fue creado en el año 2011 por Ross William Ulbricht y supuso un espacio que ponía en común a delincuentes, compradores y vendedores para la venta de productos y servicios ilegales (Christin, 2013). Desde su creación estuvo funcionando durante dos años y medio, hasta que fue cerrado por las autoridades del FBI de Estados Unidos en octubre del año 2013. Estuvo dedicado principalmente a la venta de drogas como cannabis, drogas psicodélicas, drogas estimulantes como la cocaína y medicamentos ilegales (Aldridge y Décary-Hétu, 2014), además de otros productos como armas e identidades robadas o servicios ilegales que facilitaban el desarrollo de otras actividades delictivas.

El diseño de Silk Road era similar al de un mercado *online* habitualmente ubicado en la web superficial (p.ej. "Ebay"), en el que los vendedores recibían valoraciones de los compradores y se mostraban comentarios de los usuarios sobre la calidad de los productos, la rapidez de los envíos, la profesionalidad del vendedor y la discreción de la transacción (Barrat, 2012). Al mismo tiempo, cada producto disponía de una dirección propia, fotografía, nombre y descripción, así como el nombre del vendedor y sus valoraciones (Christin, 2013). Aunque en Silk Road se podían encontrar varios productos ilegales, de una clasificación de los 20 productos más populares del mercado se observó que las drogas se encontraban entre los más populares (Christin, 2013). Estas podían ser agrupadas en seis categorías: cannabis, éxtasis, opioides, prescripciones médicas, psicodélicos y estimulantes; pero el grupo mayoritario era el cannabis (N=2661) (Aldridge y Décary-Hétu, 2014, p.7). De esta forma, puede decirse que se trataba de un criptomercado dedicado fundamentalmente a la venta de drogas.

Este criptomercado permitía el anonimato tanto de compradores como vendedores a través de dos vías. Por un lado, empleaba tecnologías que de forma general permitían el anonimato de los usuarios como la criptomoneda Bitcoin como único sistema de pago (Christin, 2013). Por otro lado, presentaba características propias con las que también conseguía el propósito del anonimato y la dificultad de detección. Así, fue característico el sistema de pago de Silk Road, en el que cada usuario disponía en su página de una cuenta con una cartera Bitcoin y una o varias direcciones proporcionadas por el propio mercado. Esto implicaba que para realizar una compra en el criptomercado primero el usuario debía disponer de criptomonedas en la cartera de su cuenta en el mercado. Para ello, debía comprar criptomonedas con su propia billetera personal y realizar una transferencia a la dirección Bitcoin del monedero proporcionado por el mercado. Estos fondos serían empleados para realizar la compra de los productos ubicados en Silk Road.

Una vez realizada la compra en el mercado, este disponía de otro mecanismo para garantizar una mayor seguridad en la compra y es que el dinero del comprador, antes de llegar al vendedor, se almacenaba en una cuenta *escrow* o fidecomiso hasta que se aseguraba que se había recibido el producto comprado (Financial Action Task Force, 2014). Para una mayor seguridad, Silk Road también empleaba un *tumbler* para cada compra (Financial Action Task Force, 2014).

En cuanto a la localización de los productos, la mayoría de los vendedores ponían a disposición de los usuarios varias opciones de envío a cualquier parte del mundo (49,67% de la muestra) (Christin, 2013). No obstante, había una mayoría de países angloparlantes como

Estados Unidos (43,83%) o Reino Unido (Christin, 2013). El envío o recepción de los productos adquiridos, sobre todo si eran enviados a otros países, suponía un riesgo importante para el funcionamiento del mercado, ya que cabía la posibilidad de que fuera interceptado por las fuerzas policiales (Barrat, 2012).

En un medio en el que se garantizaba el anonimato de los vendedores y no había recursos legales contra el fraude, se esperaba que los compradores tuvieran algún tipo de problema en la obtención de sus productos. Sin embargo, atendiendo a las valoraciones mostradas en el mercado, la experiencia de los compradores era muy positiva. De una muestra de 184.804 *feedbacks* recogidos, el 97,8% eran positivos (entre 4 y 5 en la escala del 1 al 5), y solo un 1,4% eran negativos (1 o 2 de la misma escala) (Christin, 2013). Esto llevaría a pensar en que los vendedores del mercado son de confianza o que al menos el sistema de *escrow* resulta efectivo.

El fin del criptomercado Silk Road tuvo lugar con el arresto de Ross Ulbricht, el creador del criptomercado, en la sección de ciencia ficción de una biblioteca pública desde donde gestionaba el mercado empleando el wifi público que estaba disponible en este espacio. En aquellos momentos este hecho distaba de la imagen que se tenía de los traficantes que gestionan grandes mercados de droga y que están rodeados de guardaespaldas y sicarios (Ali et al. 2015).

Silk Road constituyó una innovación criminal sustancial en el mercado de drogas. Proporcionaba a los traficantes un mercado mundial para sus productos, la capacidad de vender a clientes desconocidos, la posibilidad de comerciar de forma anónima y un entorno de riesgo relativamente bajo (Aldridge y Décary-Hétu, 2014, p.4). Ha supuesto el desarrollo de un modelo de distribución directa en el que no es necesaria la participación de narcotraficantes, intermediarios, mayoristas, minoristas callejeros y otros nodos, sino que ambas partes se encuentran directamente de forma tanto nacional como internacional (Martin, 2014, p.364). Además, permitía reducir riesgos como la violencia asociada con los mercados tradicionales de drogas al resolver conflictos o proteger su territorio (Aldridge y Décary-Hétu, 2014, p.16). También ha supuesto un cambio en las habilidades de los traficantes de drogas que ahora tendrán que considerar las valoraciones y los comentarios de los clientes para adaptar su negocio y ser más competitivos (Aldridge y Décary-Hétu, 2014, p.16). Muchos compradores incluyen en las valoraciones del vendedor los resultados de pureza de la droga adquirida para mostrárselo al resto de los clientes. Esto puede hacer que los vendedores consideren la calidad del producto que ofrecen para ser más competitivos en su negocio y no perder clientela (Christin, 2013; Martin, 2014).

Su cierre impidió el acceso al mercado para obtener más datos. No obstante, se disponía de una gran cantidad de información que había sido recopilada por multitud de investigadores interesados en su estudio lo que les permitió conocer mucho más sobre su funcionamiento, tamaño y características. En el año 2012, Christin (2013), realizó una caracterización del mercado en relación con los productos disponibles, vendedores y compradores con el objetivo de estimar el volumen de la actividad y su relevancia. Se estimó que hubiera podido llegar a obtener alrededor de 22 millones de ventas anuales solo relacionadas con el mercado de drogas (Christin, 2013). En el año 2013, antes de su cierre, Silk Road tenía ventas de 300.000 dólares al día, lo que podía llegar a suponer la obtención de un beneficio económico de alrededor de 100 millones de dólares al año (Soska y Christin, 2015). Estudios posteriores estimaron unos beneficios totales de 84,5 millones de dólares solo con la venta de drogas (Aldridge y Décary-Hétu, 2014). En otro estudio se estimó que el mercado generó unos ingresos totales por el valor de 1,2 billones de dólares (más de 9,5 millones de bitcoins) y aproximadamente 80 millones de dólares (más de 600.000 bitcoins) en comisiones (Financial Action Task Force, 2014). Aunque pueden parecer cifras muy elevadas, merece la pena señalar que estas cifras no son comparables con las registradas para los mercados de drogas en el entorno *offline*, que en el año 2005 contaban con una cifra de aproximadamente 300 billones de dólares (Martin, 2014).

En relación con su tamaño, en el año 2012, el número de vendedores aumentó rápidamente durante los primeros seis meses de 220 a 564 (Christin, 2013) y en 2013 se duplicó a alrededor de los 1000 (Aldridge y Décary-Hétu, 2014). Sin embargo, el número de vendedores no era constante, la mayoría se mantenían operando en el mercado una media de 100 semanas y solo un 9% de la muestra permanecieron a lo largo de todo el intervalo estudiado (Christin, 2013).

Debido al anonimato con el que operaban los usuarios en el mercado, no se pudo conocer demasiado sobre el perfil de los vendedores. No se podía determinar si un mismo vendedor podía operar en varias páginas a la vez, pero sí que se observó que muchos de los vendedores que operaban en el espacio físico ponían a la venta muchos de sus productos en Silk Road (Christin, 2013). También otros estudios han determinado que los vendedores empleaban términos, cantidades y precios que podrían ir dirigidos a clientes con intenciones de revender los productos (Aldridge y Décary-Hétu, 2014). Empleaban en sus *listings* terminología propia de un modelo de *business-to-business,* como, por ejemplo, un vendedor de cannabis exponía “200 gramos de hash de grado comercial de Marruecos” (Aldridge y Décary-Hétu, 2014). También se consideró que los vendedores conocían de la posibilidad de

reventa del producto, por ello, establecían precios bajos, vendían a granel, ofrecían diversas cantidades y hacían descuentos para grandes cantidades (Aldridge y Décary-Hétu, 2014).

Tras el cierre de Silk Road surgieron otros criptomercados como como "Alphabay" que tenía una relevancia y características similares a Silk Road. Después de este surgió "Hansa" que fue considerado como el tercer mayor mercado de la DN y disponía de más de 350000 productos ilícitos como drogas, armas de fuego y *malware* que podían ser comprados utilizando bitcoins y otras criptomonedas. Sin embargo, ambos mercados fueron desarticulados en una operación policial llamada "Bayonet" (Escobar, 2017). Posteriormente surgió el mercado "Sheep", de un tamaño comparable a Silk Road, pero que acabó con un *exit scam*. A lo largo de 2014 los mercados aumentaron su tamaño con "Pandora", "Agora", "Hydra", "Evolution" y Silk Road 2.0 compitiendo por ganar la confianza de los compradores en una época en la que cada vez eran más evidentes las estafas. Más tarde en la operación "Onymous" fueron cerrados Silk Road 2.0, "Cloud 9" e "Hydra" (Aldridge y Décary-Hétu, 2016).

La aparición de los criptomercados supuso un reto para las autoridades, investigadores y fiscales encargados en la lucha contra la distribución de drogas *online.* Sin embargo, la relevancia que tuvo Silk Road en sus inicios se debe a que fue el primer caso de estas características, lo que dificultó frenar rápidamente su avance y el desarrollo de estos mercados *online* (Martin, 2014). La introducción de las criptomonedas como forma de pago en estos mercados, aunque supuso un avance importante en el negocio criminal, ha supuesto al mismo tiempo una vulnerabilidad que facilita la detección por parte de las autoridades que pueden estudiar el rastro de la actividad realizada con esta tecnología (Martin, 2014). No obstante, el envío del producto a través del correo postal continúa siendo la mayor fuente de riesgo de detección de estos negocios (Barrat, 2012: Martin, 2014). Aunque la inspección física del correo sería mucho más efectiva para detectar el delito que el monitoreo *online,* es muy complejo realizar un examen minucioso de todos los paquetes recibidos (Martin, 2014). Por estos motivos, los vendedores han mejorado la forma en la que envían el producto final, evitando que este sea fácilmente por las autoridades en los controles habituales del correo postal ordinario (p.ej. sellar los paquetes al vacío y emplear estilos formales similares a los paquetes ordinarios) (Christin, 2013).

La Utilización de las Criptomonedas en el Crimen Organizado y el Terrorismo

Los avances tecnológicos de la última década y en especial el uso generalizado de Internet han tenido un papel relevante en el proceso de globalización y eliminación de

fronteras. Han supuesto una mejora en la sociedad en lo que respecta a la forma en la que se comunica y comparte información, de tal forma que, en la actualidad, la gran mayoría de las actividades cotidianas implican la utilización de ordenadores, teléfonos móviles o de una conexión a Internet.

No obstante, aunque esta situación ha supuesto grandes beneficios para la sociedad, también ha generado ciertos riesgos. De la misma forma que el resto de la sociedad, los grupos criminales también se ha beneficiado de los avances tecnológicos y los ha incorporado en sus formas de actuación.

Este es el caso de las organizaciones criminales y los grupos terroristas, que se tratarán con mayor detalle a continuación:

Crimen Organizado

En este caso, el crimen organizado también ha incluido en sus formas de actuación herramientas y metodologías propias de los nuevos avances tecnológicos y de la interconexión mundial que ofrece Internet. Esto es, Internet ha facilitado una amplia gama de actividades de la delincuencia organizada relacionadas con su comunicación, investigación, logística, comercialización, captación, distribución y seguimiento (Europol, 2011a). Además, ha facilitado todo tipo de delincuencia organizada *offline* como "la extracción, síntesis y tráfico de drogas ilícitas, la trata de seres humanos con fines de explotación sexual, la migración ilegal, el fraude en la comercialización masiva, el fraude MTIC (IVA), la falsificación del euro y el comercio de armas de fuego prohibidas" (Europol, 2011b).

La Red en sí misma dispone de una serie de características que la hacen atractiva para la delincuencia en general: ofrece seguridad a la persona que comete un delito, permite cometer delitos aprovechando la ingenuidad de las víctimas, pone a disposición de los criminales una gran cantidad de víctimas, permite cometer delitos de forma transnacional y no hay una única legislación que la regule, sino que está supeditada a la interpretación desde muchas legislaciones diferentes (Casas, 2017). De esta forma, las organizaciones criminales han adaptado sus formas de actuación a las nuevas tecnologías porque les permiten llegar a un número mayor de clientes y de víctimas sin importar el espacio ni el tiempo, les permite ampliar su oferta de bienes y servicios debido a los espacios en la red seguros para anunciarse y por la demandas de las herramientas tecnológicas surgidas y por último, los espacios seguros en la red han facilitado el desarrollo de los negocios delictivos dificultando la detección e intervención por parte de las autoridades.

En este contexto, el cibercrimen se ha situado como uno de los mercados delictivos de la criminalidad organizada que más se ha ampliado en los últimos años (Europol, 2017). El desarrollo de este tipo de criminalidad ha afectado a la estructura de los grupos criminales, dejando a un lado el concepto tradicional de organización criminal basada en una estructura jerárquica (Europol, 2011b).

Como parte de la adopción de las nuevas tecnologías en el desarrollo de los delitos tradicionales y los ciberdelitos[169], las organizaciones criminales han incorporado las criptomonedas entre las herramientas que disponen para el desarrollo de sus actividades delictivas. De esta forma, esta tecnología ha sido señalada como un facilitador de aquellos delitos habitualmente relacionados con el crimen organizado (Collins, 2022).

Aunque no se puede determinar con exactitud los motivos por los que las organizaciones criminales han utilizado las criptomonedas en el desarrollo de sus delitos, las propias características de esta tecnología como el anonimato y la descentralización han podido favorecer su utilización entre las organizaciones criminales (Saldaña-Taboada, 2019).

De igual forma, puede que esta utilización también se haya visto favorecida por las particularidades de las organizaciones criminales. De forma general, los rasgos distintivos de las organizaciones criminales son la finalidad económica, la implicación prioritaria en la provisión y suministro de bienes y servicios ilegales, las actividades ilegales complementadas con negocios legales, la continuidad y las medidas de protección, la corrupción y la violencia (Corte y Giménez-Salinas, 2010). Dentro de estas, la motivación económica, es decir, la búsqueda del "puro y crudo lucro económico" es una de las principales motivaciones del crimen organizado, determinando su perduración y pertenencia a la banda (UNODC, 2014). Toda actividad y decisiones que se tomen dentro de la organización criminal se realizarán en torno a la amplificación de las oportunidades para obtener mayores beneficios (Corte y Giménez-Salinas, 2010), sin atender a doctrinas sociales, creencias políticas o preocupaciones ideológicas (lo que la diferencia del terrorismo) (Abadinsky, 2013). Por otro lado, otra de las principales motivaciones del crimen organizado es el suministro de bienes y servicios ilegales, mayormente mediante la explotación de mercados delictivos ofreciendo

[169] En este trabajo se considerará cibercriminalidad tanto a los delitos ciberdependientes o cibernéticos como a los delitos de carácter tradicional cuyo desarrollo se favorece con la utilización de las TICs. A fin de comprender mejor esta apreciación, se considera como "delito ciberdependiente" a aquel que solo puede cometerse usando un ordenador, redes de ordenadores u otras formas de las tecnologías de la información y la comunicación (…), como podrían ser el delito de *malware* o los ataques de denegación de servicio (DoS). Por otro lado, el término cibercriminalidad constituye un concepto más amplio en el además de la anterior, también se incluye la delincuencia considerada como tradicional que se facilita gracias a la utilización de las Tecnologías de la Información y la Comunicación (Fernández y Martínez, 2018, p.152).

productos y servicios bajo demanda (Corte y Giménez-Salinas, 2010). Es decir, la criminalidad organizada adapta su negocio a las demandas de la sociedad, ofreciendo aquellos productos y bienes con los que se podría obtener un mayor número de beneficios. Por último, otra de las principales características de las organizaciones criminales es que disponen de una serie de estrategias para asegurar su permanencia escapando a la detección de las FCSE, además de emplear la corrupción de empleados públicos y responsables políticos y violencia como medio de protección y defensa (Corte y Giménez-Salinas, 2010, p.26).

De esta forma, se puede afirmar que las organizaciones criminales funcionan de la misma forma que una empresa de carácter legal, que busca beneficios económicos y materiales mediante la oferta y demanda de productos y servicios, adaptándose continuamente a los nuevos avances que van surgiendo para mejorar el negocio y obtener mayores beneficios. En este proceso de adaptación se incluyen las criptomonedas, que se presentan como un medio que les permite obtener una mayor rentabilidad en su negocio criminal y obtener beneficios disminuyendo los riesgos de ser detectados por las autoridades.

Aunque no se conoce con total seguridad cuáles son las características de las criptomonedas que motivan a las organizaciones criminales a utilizar esta moneda virtual, se pueden señalar ciertos aspectos de esta tecnología que podrían favorecer esta aceptación: 1) descentralización, es decir, no hay intermediarios, 2) accesibilidad en todo el mundo, 3) Coste mínimo de las transacciones; 4) Permite realizar transacciones internacionales a través de redes *peer-to-peer*; 5) Anonimato; 6) Posibilidad de cambio a dinero *fiat*; 7) Operaciones irreversibles; 8) Falta de regulación entre países; 9) Disponible como forma de pago en los mercados delictivos (Saldaña-Taboada, 2019).

A continuación, se explicarán cada uno de los puntos de manera detallada:

1) La descentralización de la moneda permite a las organizaciones obtener productos o servicios ilegales o bien blanquear dinero sin ningún intermediario implicado, escapando del control de los Estados, gobiernos, autoridades y entidades bancarias.

2) Su fácil acceso desde cualquier lugar permite a la organización utilizar esta moneda en sus actividades trasnacionales y enviar dinero a miembros de la organización de otros países, sin importar el dinero fiduciario del continente o el país en cuestión y sin necesidad de convertirlo a la moneda local.

3)Las organizaciones criminales gestionan grandes cantidades de dinero que requieren del envío entre países, incluso con carácter internacional. Esto puede suponer elevados costes si se realiza a través de una entidad bancaria, además del riesgo de ser detectado por las

medidas de seguridad de la entidad. Las criptomonedas permitirían enviar grandes cantidades de dinero con carácter internacional con unos costes mucho más bajos que a través de una entidad bancaria.

4) La posibilidad de enviar dinero directamente entre las partes interesadas sin intermediarios dificulta la detección de la actividad criminal que tiene lugar por parte de las organizaciones criminales.

5) El anonimato o pseudoanonimato del sistema Bitcoin favorece que los grupos criminales que utilizan criptomonedas gestionen sus negocios delictivos de forma segura, ya que no hay ningún tipo de dato personal vinculado a las direcciones Bitcoin empleadas. Además, para asegurar el anonimato emplean otras estrategias adicionales como la utilización de diversas direcciones Bitcoin.

6) La posibilidad de cambio de criptomonedas a dinero fiduciario permite a las organizaciones criminales gestionar los fondos criminales entre diversos países y distintos miembros y utilizar el dinero obtenido entre la moneda local que sea necesaria.

7) La irreversibilidad de las operaciones realizadas con Bitcoin dota a los grupos criminales de la seguridad de que la transacción realizada no será revertida. Esto es especialmente relevante en negocios criminales en los que no existe una elevada confianza en los acuerdos realizados con la otra parte.

8) La falta de una regulación unificada entre países en esta materia ha podido favorecer la proliferación de la criminalidad organizada que utiliza criptomonedas motivada por la dificultad de respuesta por parte de las autoridades. En este sentido, es relevante la Directiva (UE) 2018/843 que entre las medidas que prevé para la lucha contra el blanqueo de capitales y el terrorismo, recoge que las casas de cambio o *exchanges* y proveedores de servicios de custodia de monederos tendrán que cumplir la normativa y vigilar el uso que se hace de las monedas virtuales, colaborando para reducir el anonimato asociado a estas monedas y además deberán estar registrados.

9)La disponibilidad de criptomonedas, en especial Bitcoin, como forma de pago en los mercados delictivos ha podido motivar a las organizaciones criminales a utilizar esta moneda virtual para obtener productos o servicios ilegales que están disponibles en dichos espacios comerciales.

Por todo ello, las criptomonedas han resultado de interés para las organizaciones criminales que las han utilizado para la comisión de delitos o para facilitar la realización de muchos otros. De esta forma, se pueden encontrar muchos casos de diferentes tipologías

delictivas perpetradas por organizaciones criminales en las que intervienen las criptomonedas de alguna forma.

A continuación, se muestran casos de delitos que han sido relevantes por su perpetración en el seno de una organización criminal que ha utilizado criptomonedas en su desarrollo.

En la lucha contra el crimen organizado y la delincuencia grave la utilización de criptomonedas en el blanqueo de capitales ha supuesto una nueva amenaza que ha de considerarse tal y como se recoge en la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave que expone que la utilización de criptomonedas supone una nueva modalidad de blanqueo de capitales[170]. De esta forma, el blanqueo de capitales constituye uno de los principales motores del crimen organizado junto con el fraude documental y el comercio en línea (Europol, 2018). En esta actividad criminal, las criptomonedas han tenido un gran protagonismo permitiendo la ocultación del rastro del dinero obtenido a través de un delito. Los criminales utilizan el dinero ilegalmente obtenido para comprar criptomonedas, que podrán utilizar como tal o que convertirán de nuevo a dinero fiduciario. En este sentido, en España han sido relevantes los casos "Tulipán Blanco" y "Kampuzo".

En ambas operaciones la Unidad Central Operativa de la Guardia Civil desarticuló una organización criminal dedicada al blanqueo de dinero que otras organizaciones criminales obtenían del narcotráfico. En el primer caso, se trataba de una organización criminal dedicada al narcotráfico que operaba en España y en Colombia y que compraba criptomonedas para blanquear el dinero obtenido de sus actividades relacionadas con el tráfico de drogas. Una vez disponían de las criptomonedas, los miembros de la organización ubicados en España, las enviaban a los miembros del grupo ubicados en Colombia. Una vez en este país, las criptomonedas eran convertidas de nuevo a dinero fiduciario o bien se mantenían en criptomoneda (EFE, 2018). Fue una operación pionera en España en la que se demostró el movimiento internacional de efectivo de una organización criminal dedicada al blanqueo de capitales empleando estas tecnologías en combinación con otras formas tradicionales (Guardia Civil, 2018). En la operación "Kampuzo" los miembros de la organización criminal obtenían bitcoins utilizando el dinero obtenido en su actividad criminal en cajeros automáticos de criptomonedas, en especial Bitcoin, que la organización había

[170] Orden PCI/161/2019, de 21 de febrero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave.

instalado en una “empresa tapadera”. Esta operación supuso la intervención por primera vez en España de cajeros automáticos de criptomonedas de forma física (Guardia Civil, 2018).

En segundo lugar, las organizaciones criminales también han utilizado criptomonedas en el pago de mercados delictivos, constituyendo uno de los métodos de pago que utilizan los grupos junto con las tarjetas prepago y los vales en línea, que permite mover grandes cantidades de fondos criminales (Europol, 2018). Otros métodos de pago digitales como “Paypal” o “Wester Union”, que fueron muy populares antes entre criminales, actualmente cuentan con una amplia variedad de medidas de seguridad para prevenir su utilización en la comisión de delitos, como la disposición de un departamento especializado en antifraude (Casas, 2017). De esta forma, las criptomonedas se han utilizado en la DN para obtener productos como drogas ilegales, armas de fuego, bienes falsificados, documentos fraudulentos, especies en peligro de extinción, etc. (Europol, 2017). Las características de estos mercados criminales unidas a las características propias de las criptomonedas favorecen la utilización de estos espacios por parte de las organizaciones criminales, especialmente porque en muchas ocasiones es necesaria la compra de ciertos productos ilegales para el desarrollo de otros delitos de mayor gravedad. Este es el caso del fraude de tarjeta presente o *Skimming* que requiere los materiales para fabricar las tarjetas de crédito o en el fraude de tarjeta no presente o *Carding* en el que los datos robados permiten la comisión de delitos posteriores de mayor gravedad (Europol, 2017).

En tercer lugar, también se puede encontrar la implicación de las organizaciones criminales en la contratación de servicios delictivos o *Crime-as-a-Service* (CaaS), que ya ha sido tratado en apartados anteriores. De la misma forma que la compra de productos, las organizaciones criminales han utilizado criptomonedas para el pago de servicios criminales. Este es el caso del abuso sexual infantil *online* o LDCA en el que se ha visto la implicación de algunas organizaciones criminales (ECPAT, 2018). Esto se debe a que requieren de los servicios de otros criminales especializados en la comisión de delitos más complejos y elaborados, como sucede cuando se trata de una organización criminal de carácter tradicional interesada en el cibercrimen o en la división de tareas característica de las organizaciones criminales.

Las organizaciones criminales también se han visto involucradas en casos de ciberextorsión y sextorsión. En ambos casos, se exige el pago de una cantidad determinada de criptomonedas a cambio de cesar la actividad maliciosa, que podría ser el secuestro o bloqueo del equipo o parte de este o la difusión de información o imágenes de carácter íntimo y sexual. Los tipos de *malware* más habituales para llevar a cabo este tipo de cibercrimen son el

ransomware y los ataques de denegación de servicio (DDoS), ambos señalados como una ciberamenaza en la que las monedas virtuales como Bitcoin son el medio de pago preferido (Europol, 2017). Un ejemplo de esto lo constituye el grupo criminal "DD4BC" (*Distributed DDoS for Bitcoin*) que fue perseguido por Europol y otros cuerpos policiales por ser uno de los grupos dedicados a atacar plataformas web enviando altas cantidades de tráfico a su red para impedir el acceso a cambio del pago de una determinada cantidad de bitcoins. Este grupo ha sido el responsable de varias campañas de ciberextorsión desde el año 2014 (Hernández, 2016). En cuanto a la sextorsión, se puede ofrecer como ejemplo un caso en el norte de África en el que una organización criminal engañaba y manipulaba a diversos sujetos para obtener fotos con carácter sexual. Una vez se habían obtenido dichas fotos, se amenazaba a las personas en cuestión con distribuirlas a todos sus conocidos si no enviaban la cantidad de criptomonedas exigida por la organización criminal (Casas, 2017).

Otro caso relevante de utilización de *malware* por parte de las organizaciones criminales ha sido el del famoso ciberdelincuente de origen ucraniano dedicado al robo de bancos, creador del *malware* "Carbanak", que protagonizó uno de los casos de ciberdelincuencia en el seno de una organización criminal más importante hasta la fecha tanto por la trascendencia internacional como por la cantidad de dinero sustraída. El *modus operandi* de esta organización comenzaba con el acceso a la red informática de los bancos a través de la utilización de un *malware* que se enviaba mediante correos maliciosos a los trabajadores. Una vez habían accedido al sistema informático del banco, los criminales escalaban hasta los sistemas de seguridad de cajeros y transferencias (Herraiz y Alsedo, 2018). Cuando la organización había infectado la infraestructura del banco robaban el dinero de tres formas diferentes: transfiriendo el dinero a cuentas bancarias en bancos extranjeros, aumentando el dinero de las cuentas bancarias para que pudiera ser retirado del cajero automático y controlando los cajeros automáticos para que expulsaran dinero (Europol, 2018). Por último, el dinero obtenido a través de estos métodos era convertido en criptomonedas, fundamentalmente Bitcoin para dificultar la detección del dinero de origen ilícito (Europol, 2018).

Por último, las organizaciones criminales también se han visto involucradas en el robo de criptomonedas. El elevado valor del Bitcoin y la posibilidad de obtener los fondos únicamente con la clave privada de la billetera convierte al Bitcoin no solo en una herramienta atractiva para su utilización en el delito sino también en un bien valioso. Este es el caso de una organización criminal que hackeó a una empresa y robó seis millones de euros en criptomonedas (Crónica Global, 2022). La empresa fue atacada por un *malware* tipo

Troyano que tuvo su origen en la descarga de un archivo malicioso, en concreto una película, por parte de un trabajador de la empresa afectada (Crónica Global, 2022). Los atacantes se hicieron con el control total del ordenador del empleado y tras seis meses preparando el robo, cuando ya conocían todos los procedimientos, características y estructuras de la empresa los ciberdelincuentes realizaron una transacción de criptomonedas por valor de 6 millones de euros, que fueron enviadas a las billeteras de los criminales (Crónica Global, 2022). Una vez esperaron unos meses para evitar atraer a la policía, crearon un entramado de billeteras electrónicas de blanqueo de capitales que les proporcionaba el anonimato (Crónica Global, 2022).

Terrorismo

De la misma forma que el crimen organizado, los grupos terroristas también han incluido en sus formas de actuación herramientas y metodologías propias de los nuevos avances tecnológicos y de la interconexión mundial que ofrece Internet.

Estas nuevas mejoras están siendo empleadas para diversificar sus modos de financiación, sus comunicaciones y sus operaciones (UNODC, 2021, p.5). Internet se ha convertido en una herramienta de enorme utilidad en la financiación del terrorismo, que permite a los grupos conectar en red con personas que tengan ideas afines y que por tanto les proporcionen apoyo, fundamentalmente de carácter económico (Tierney, 2018). Como parte de los avances tecnológicos que están siendo adoptados por el terrorismo se ha observado que las criptomonedas se han incluido entre las herramientas que utilizan las organizaciones criminales.

La utilización de las criptomonedas por parte de los terroristas es señalada por la UNODC como una amenaza emergente del terrorismo junto con la utilización de drones y de las plataformas de mensajería segura (UNODC, 2021). Junto con las monedas digitales y los servicios de activos virtuales, las criptomonedas han permitido a los terroristas y extremistas abusar de la financiación al mismo tiempo que se obtenía un mayor anonimato para donantes y receptores (Europol, 2022b).

La financiación del terrorismo es el aspecto de esta tipología delictiva en donde las criptomonedas han adquirido un mayor protagonismo y es que, aunque siguen predominando los métodos de financiación tradicionales como el dinero en efectivo, en las organizaciones más avanzadas están recurriendo a las criptomonedas para financiarse (Lindrea, 2022). Se ha visto una utilización de las formas tradicionales de financiación junto con las nuevas formas (Andrianova, 2020). La pérdida del territorio controlado por algunos grupos terroristas les

priva de los beneficios que obtenían a través de actividades ilícitas como la venta de petróleo, el tráfico de personas y los impuestos que les exigían a la población local. Por este motivo, han aumentado su popularidad aquellas formas de financiación que no están vinculadas al territorio, como son el *hawala*, la recaudación de fondos, los pagos electrónicos y las criptomonedas (Andrianova, 2020, p. 29).

Esta tecnología se posiciona como una de las nuevas formas de financiación del terrorismo mediante tecnologías digitales modernas como la microfinanciación o *crowdfunding* o la recaudación de fondos a través de redes sociales y los canales de Telegram (Andrianova, 2020).

El primer caso en el que se vio la utilización de una de estas formas de financiación modernas tuvo lugar en el año 2016, cuando el Centro de Medios de Ibn Taymiyya se convirtió en la primera organización terrorista en lanzar una campaña pública de donación de *crowdfunding* utilizando criptomonedas (Chainalysis, 2020). Esta campaña se nombró como "Jahezona", lo que significa "Equípenos" en árabe, ya que permitía a la sociedad ser partícipes de la adquisición de armas de los grupos terroristas a través de sus donaciones a la dirección Bitcoin del grupo terrorista (Chainalysis, 2020). A partir de este momento han aparecido nuevos casos de financiación en este sentido como el de militantes islámicos que tenían vínculos con células terroristas de Indonesia, les enseñaron a fabricar bombas, organizar ataques y les financiaron empleando Bitcoin y Paypal (Lester, 2017).

No obstante, el primer ejemplo verificado de la implementación de las criptomonedas en una organización terrorista tuvo lugar en el año 2019 con las Brigadas Izz ad-Din al-Qassam (Chainalysis, 2020). Entre los años 2019 y 2020, la organización terrorista Al Qaeda recaudó criptomonedas a través de canales de Telegram y grupos de Facebook y se incautaron más de un millón de dólares a un operador de negocios de servicios monetarios que facilitó las transacciones (Chainalysis, 2022, p.93). Al año siguiente, en la primavera de 2021 las brigadas al-Qassam y los grupos militares de Hamás recaudaron más de 100.000 dólares en donaciones, que fueron confiscadas en julio por el gobierno israelí a los servicios monetarios asociados (Chainalysis, 2022, p.93). En este mismo año también se sancionó a Farrukh Furkatovitch Fayzimatov por haber ayudado y apoyado materialmente a un grupo militante implicado en la guerra civil siria (Hay'et Tahrir al-Sham), para el que solicitó donaciones para que el grupo adquiriera material (Chainalysis, 2022).

Aunque en su mayoría utilizaban la criptomoneda Bitcoin, en el año 2021 tuvo lugar la primera incautación de criptomonedas que incluía una amplia variedad de divisas como

“Ether”, “Tether”, “XRP” y otras en una campaña de donaciones del grupo Hamás (Chainalysis, 2022).

La aparición de diversos casos en los que organizaciones terroristas utilizan las criptomonedas para su financiación ha atraído el interés de las autoridades como Europol que han tratado este tema en diversos informes de carácter europeo (Europol, 2022b). Al mismo tiempo, a nivel nacional se ha demostrado la relevancia de este tema con su incorporación en la Directiva 2018/843 aprobada por el Parlamento Europeo que, junto con la prevención del blanqueo de capitales, también tiene como objetivo la prevención de la utilización del sistema financiero para la financiación del terrorismo.

Sin embargo, aunque se han dado casos relevantes de la utilización de criptomonedas en el terrorismo y se ha visto cierto aumento de estos delitos, su utilización entre los grupos terroristas es muy limitada (Europol, 2022a). Todavía no se dispone de la evidencia suficiente para señalar esta actividad como preocupante (Kethineni y Cao, 2020).

Por todo ello, la investigación empírica en esta materia es escasa. Además, a los inconvenientes de la investigación del terrorismo se le unen los inconvenientes de la investigación de los delitos cometidos con criptomonedas. Salvo en casos conocidos de organizaciones terroristas relevantes que piden financiación, es difícil determinar qué direcciones de las carteras pertenecen a estos grupos. En Azani et al. (2020) utilizando la base de datos de “Bitcoin Abuse”, se identifica una dirección BTC que se ha relacionado con la financiación de una organización terrorista. No obstante, este registro ha sido realizado por una persona que directamente la ha señalado como perteneciente a la organización “Hamás”. Estos resultados pueden carecer de credibilidad, ya que cualquier persona ha podido registrar dicha información y no se disponen de otros registros que puedan apoyar tal afirmación. Por otro lado, la investigación de Andrianova (2020) estudia los principales métodos existentes de financiación actividades terroristas, tanto tradicionales como aquellas desarrolladas a través de tecnologías virtuales y sitúa a las criptomonedas dentro del último grupo.

Capítulo 7: Estado Actual de la Investigación Sobre la Utilización de Criptomonedas en la Criminalidad. Aproximación Desde la Criminología.

La creación de las criptomonedas con la aparición del Bitcoin no tuvo como propósito inicial el desarrollo de una herramienta que favoreciera la comisión de delitos (Finney, 1993)[171]. Tampoco fue este el propósito de ninguna de las propuestas de efectivo digital que le antecedían, que únicamente perseguían la creación de una herramienta que permitiera mejorar la privacidad y la seguridad en un contexto legal (Finney, 1993).

No obstante, la aparición de casos de delitos en los que ha intervenido la criptomoneda ha vinculado esta tecnología con la criminalidad. Algunos investigadores como el danés Vili Lehdonvirta[172] han considerado que el Bitcoin ofrece un nivel de privacidad que especialmente favorece a los criminales, que son los realmente interesados en mover grandes cantidades de dinero garantizando la privacidad de su actividad (Davis, 2011). Esto tenía su apoyo en investigaciones que surgieron en los inicios de Bitcoin como el análisis de la *US Drug Enforcement Administration (DEA)* que mostró que alrededor del 90 % de las transacciones Bitcoin en 2013 estaban relacionadas con actividades criminales (Russo, 2018), lo que sugería que las primeras personas que adoptaron Bitcoin lo hicieron con propósitos ilegales.

Todo ello ha generado un amplio debate sobre los límites que se deberían establecer en la utilización de las criptomonedas para prevenir su utilización en la comisión de delitos.

Contrariamente a todas aquellas personas que señalan a las criptomonedas y en especial a Bitcoin como "el dinero de los criminales", en la actualidad son muchos los usuarios del sistema Bitcoin que utilizan esta tecnología con fines legales, mostrándose como firmes defensores de su uso abierto y libre. Frente a aquellas personas que las vinculan con la criminalidad, estos usuarios exponen diversos argumentos para rehusar la consideración que se tiene de las criptomonedas como una tecnología predestinada para el crimen.

Por un lado, las criptomonedas se podrían considerar como un instrumento más de los muchos que se pueden emplear para cometer delitos, de la misma forma que se ha utilizado la

[171] En palabras de Hal Finney, la primera persona en usar el software de Bitcoin y uno de los desarrolladores clave del proyecto, se desconocía si el Bitcoin sería utilizado para el desarrollo de delitos, no siendo este el propósito inicial de la moneda: "I don't know whether this system could be used to support illegal actions, tax evasion, gambling, or whatever. That is not the purpose of this proposal. It does offer the prospect of improving personal privacy and security, in a framework that might even be legal, and that's not bad" (Finney, 1993).
[172] Vili Lehdonvirta ha sido sospechoso de ser Satoshi Nakamoto. Es investigador del Helsinki Institute for Information Technology con una formación en desarrollo de videojuegos y estudios de monedas virtuales. Además, forma parte del comité de expertos de la organización Electronic Frontier Finland, que trabaja entre otras cosas, por motivas la privacidad *online*.

conexión a Internet o un ordenador, y para los que no se plantea una prohibición total de su utilización (Boar, 2018). Existe una gran variedad de tecnologías que se están empleando en el desarrollo de actividades delictivas por lo que la supresión de las criptomonedas no supondría la eliminación de la mayoría de los mercados delictivos que existen en la actualidad. Este hecho pudo observarse con la caída del criptomercado Silk Road en el año 2013. La criptomoneda Bitcoin constituía la moneda de este mercado, por lo que fue considerada como la principal forma de pago de drogas y otros servicios ilegales en esa fecha. Sin embargo, el cierre del mercado no supuso el cese por completo de la utilización de la criptomoneda, sino que poco a poco fue empleada en otros mercados delictivos que fueron apareciendo (Ammous, 2018).

Controlar y medir la cantidad exacta de delitos que se llevan a cabo con criptomonedas no es una tarea fácil. La investigación que se lleva a cabo en esta materia consiste mayormente en la identificación de direcciones criptográficas que parecen sospechosas y en calcular su volumen, por lo que resulta difícil determinar la identidad de los usuarios (Schickler, 2022). Dependiendo del tipo de investigación que se realice la proporción de pagos con criptomonedas que se vinculan a delitos financieros puede variar enormemente entre el 0,15 y el 46% (Schickler, 2022). Por lo tanto, coincidiendo con lo que exponía Janze (2017) en su investigación, todavía en la actualidad no se ha podido demostrar empíricamente que las criptomonedas constituyan una tecnología mayormente empleada por criminales. De esta forma, sería negligente afirmar que el Bitcoin, se trata de una herramienta criminal que en su mayoría es utilizada para cometer actividades delictivas.

Por otro lado, el anonimato es habitualmente una de las características de las criptomonedas que se relaciona con la utilización de esta tecnología en la criminalidad. Sin embargo, diversas investigaciones han demostrado que criptomonedas como el Bitcoin no garantizan el anonimato que se espera, además de que se han desarrollado técnicas de desanonimización que permitirían, con la información adecuada, conocer la identidad del usuario, además de la actividad al completo realizada con la moneda virtual. Así, Reid y Harrigan (2013) determinaron que las criptomonedas no eran anónimas, sino pseudoanónimas a partir uno de los primeros análisis de anonimato en el sistema Bitcoin en el que se atribuía información de identificación externa a las direcciones; Androulaki et al. (2013), evaluó la privacidad de Bitcoin demostrando que las técnicas de agrupación de clústeres basadas en el comportamiento y en las transacciones podían desanonimizar hasta el 40% de los usuarios; Ron y Shamir (2013) realizaron un análisis de todas las transacciones para examinar el comportamiento de los usuarios de Bitcoin y los medios por los que

protegían su privacidad en el sistema Bitcoin; Meiklejohn et al. (2013) utilizaron heurísticas de agrupación para clasificar a los propietarios de carteras de Bitcoin y discutir el anonimato del protocolo Bitcoin. Todas estas investigaciones cuestionaban la existencia de un anonimato real en el protocolo Bitcoin y en las criptomonedas de carácter público en general, ya que demostraban que era posible conocer varios aspectos de la actividad realizada con criptomonedas que, con la obtención de la información adicional necesaria permitirían identificar a los usuarios dentro del sistema.

De esta forma, no se podría hablar de anonimato, sino de un pseudoanonimato del sistema Bitcoin, lo que supone que aquellos usuarios interesados en utilizar esta tecnología en la criminalidad que tendrán que conocer los riesgos que podría suponer su uso para su privacidad. Por lo tanto, este pseudoanonimato, al contrario de los que se pudiera pensar, en lugar de favorecer la criminalidad, supone un inconveniente sobre todo para aquellos usuarios más especializados. Para proteger su identidad y la privacidad de su actividad delictiva, la utilización de criptomonedas tendrá que ir acompañada del empleo de servicios de anonimización como mezcladores de criptomonedas para asegurar que las transacciones realizadas no son rastreables a través de la *Blockchain* o bien utilizar técnicas para dificultar el rastreo como el envío de fondos entre diferentes carteras o incluso realizar la transacción de forma física entre las personas interesadas (Bancroft y Scott Reid, 2017). Todos estos métodos añadidos a la utilización de criptomonedas, lejos de facilitar el desarrollo de la criminalidad supondrían un obstáculo añadido a los propósitos de los criminales.

Por todo ello, se considera que los criminales que son conocedores de este riesgo para su privacidad estarán interesados en la utilización de criptomonedas de carácter privado sobre aquellas criptomonedas de carácter público, que gozan de transparencia en la *Blockchain*. Por este motivo, se considera que la propuesta de prohibición o limitación de las criptomonedas que sostienen aquellos que sostienen posturas más restrictivas en la lucha contra este tipo de criminalidad, no deberían dirigirse hacia todos los tipos de criptomonedas de la misma forma. Debido a las diferencias en su diseño, hay ciertos tipos de criptomonedas que garantizan una mayor privacidad con su uso, como es el caso de la criptomoneda Monero. Por este motivo, Domingo (2018) considera que no se debería generalizar y señalar a todas las criptomonedas como potenciales instrumentos para la comisión del delito, ya que habría ciertos tipos de criptomonedas más atractivos para la criminalidad

Al mismo tiempo, el anonimato no se considera determinante en delitos como aquellos relacionados con el comercio de drogas en línea, ya que muchos de estos negocios se desarrollan en la Internet superficial e incluso en redes sociales sin ocultar la identidad de los

participantes, es decir, no requieren del acceso a la DN o la utilización de servicios de anonimización (Bancroft y Scott Reid, 2017). La venta en los mercados de la DN se considera que es una cuestión de mantener la imagen de los vendedores ofreciendo profesionalidad, capacidad y responsabilidad, difícilmente demostrable en persona, más que garantizar el desarrollo de una compraventa segura (Bancroft y Scott Reid, 2017).

Por lo tanto, puede que, aunque los criminales puedan asegurar el anonimato de su actividad criminal, este aspecto no sea determinante para utilizar las criptomonedas en el desarrollo de sus actividades delictivas.

Toda esta discusión motiva a conocer el propósito con el que los criminales utilizan las monedas virtuales en sus actividades delictivas. La obtención de esta información permitiría el desarrollo de políticas de prevención adecuadas y precisas, además de la elaboración de medidas de seguridad adaptadas a la gravedad real de este tipo de criminalidad. Para encargados de la ley, jueces y FCSE, resulta de interés determinar la gravedad de la delincuencia cometida con criptomonedas, ya que, permitiría valorar si son necesarias aquellas leyes que puedan obligar a los usuarios de las criptomonedas a limitar su actividad (Schickler, 2022).

En el ámbito legal, la motivación para utilizar las criptomonedas ha sido ampliamente estudiada. Este es el caso de Bashir et al. (2016) que estudió la consideración que tenía la población del Bitcoin a través de una muestra de 7500 estudiantes. Los resultados que se obtuvieron mostraban que no existía una consideración unánime para todas las personas, de forma que la criptomoneda Bitcoin era utilizada en cada caso por motivos muy diversos como elementos políticos, el anonimato o la novedad de la moneda (Bashir et al., 2016, p.362). En estos resultados se observó que la novedad era un elemento que predisponía más fuertemente al sujeto a poseer bitcoins que el anonimato (Bashir et al., 2016, p.362). Lo que parecía indicar que los usuarios estaban más interesados en poseer criptomonedas por curiosidad que para involucrarse en actividades clandestinas (Bashir et al., 2016, p.362). En otro estudio sobre el interés que se tiene en las criptomonedas como activo o como moneda, se determinó que los usuarios especialmente desinformados se acercaban a las monedas digitales no porque las consideraban como un sistema de transacciones alternativo, sino porque buscaban participar en un vehículo de inversión alternativo (Glaser et al., 2014).

No obstante, si se han encontrado diferencias en las investigaciones anteriores en cuando a las actitudes de las personas que utilizan las criptomonedas en un entorno legítimo, no se consideraría adecuado realizar afirmaciones rotundas sobre la utilización de las criptodivisas en la criminalidad. Este último es un campo menos investigado, de forma que la

realidad de esta tecnología en el ámbito criminal tal y como señala Butler (2021), podría ser más matizada y variada y se debería de profundizar en este aspecto.

Si bien pueden señalarse algunas características de las criptomonedas que podrían motivar a algunas personas a utilizarlas en la criminalidad, hasta el momento no se ha observado una tendencia significativa hacia su uso (Brown, 2016). Puede que esto se deba a la necesidad de especialización en esta materia, a la falta de consideración, a que no se ha investigado realmente sobre este aspecto o a que el volumen real de este tipo de delitos no está todavía en el radar de las autoridades (Brown, 2016). Sin embargo, será necesaria una investigación de carácter criminológico que tenga como propósito estudiar los motivos de su utilización criminal, si pueden señalarse estas como una herramienta para la criminalidad y la forma en la que ha influido su utilización en los aspectos del crimen como el *modus operandi*, las víctimas, el autor o el delito.

Antecedentes en Materia de Criptomonedas y Criminalidad

Antes de iniciar la investigación será necesario en primer lugar, revisar aquellos trabajos que se han realizado anteriormente en esta materia. Por este motivo, en este apartado se presenta una visión general sobre las investigaciones realizadas hasta la fecha que han tenido como objeto de estudio la utilización de las criptomonedas en el ámbito criminal.

Posteriormente, se seleccionarán aquellas que presenten una perspectiva criminológica, esto es, si han estudiado aspectos que pudieran motivar a los criminales a utilizar esta tecnología, las motivaciones para utilizarla, la forma en la que han podido influir en los elementos del crimen u otra información que pudieran afirmar o desmentir que se trata de una herramienta creada para la comisión del delito. Esta información será útil sin duda para una posterior detección y prevención del delito. El resultado de esta tarea será la presentación de un panorama general de la investigación sobre criminalidad y criptomonedas que permita ubicar la presente investigación.

Para ello, se ha realizado una revisión de toda la literatura que se ha podido obtener en *Scopus, Google Scholar* y *Dialnet* a partir de la introducción de los términos “crime”, “Bitcoin”, “Cryptocurrencies” y en español “delito” y “Criptomonedas”.
De todos los resultados obtenidos de las diferentes búsquedas se seleccionaron los trabajos que tenían como objetivo principal el estudio de algún aspecto de las criptomonedas relacionado con el ámbito criminal, los que proponían mejoras para la prevención de algún delito y los que trataban la utilización de las criptomonedas en el crimen de forma general. Esto es, se evitaban aquellas investigaciones que, aunque trataban las criptomonedas en algún

momento, no era su objeto de investigación principal.

Como resultado de las búsquedas se obtuvo que, de forma general, la investigación en cuanto a criptomonedas y criminalidad está enfocada a la detección de las transacciones ilícitas, la identificación de los autores, el estudio de los patrones delictivos en las transacciones, la creación de herramientas de permitan detectar la actividad ilícita en la *Blockchain* y la elaboración de propuestas de mejora en la investigación. Es decir, en su mayoría se trata de investigaciones de carácter técnico con una perspectiva de investigación forense digital.

El grupo mayoritario lo forman aquellas investigaciones que estudian las transacciones de la Bitcoin *Blockchain* con el objetivo de desanonimizarlas. Aunque esta información tiene un carácter público y es fácilmente accesible por cualquier persona interesada, no recoge datos personales que permitan vincular una dirección con una persona en concreto. De esta forma, las investigaciones en esta materia buscan un desanonimizar estas transacciones a través de diversos métodos. Uno de ellos consiste el desarrollo de técnicas, métodos o herramientas que permitan obtener la información adicional necesaria para conocer la identidad de una dirección y poder determinar su identidad a través del estudio de sus transacciones. En otros casos, las investigaciones se centran en determinar aquellas direcciones de carteras que son sospechosas de haber cometido actividades ilegales. Otros métodos consisten en el estudio de los patrones de la actividad ilícita para determinar el comportamiento del criminal, aunque se desconozca la identidad del autor.

En este sentido, Yan Wu et al. (2019) extraen patrones de transacción utilizando casos conocidos y crean un modelo llamado "Bitcoin Transaction Net" para identificar direcciones sospechosas; Lee et al. (2020) utilizan técnicas de *machine learning* para detectar y clasificar aquellas direcciones de la *Blockchain* que son ilegales; Lin et al. (2019) proponen nuevas características del sistema (detectadas mediante *machine learning)* para elaborar un modelo de clasificación que detecte anomalías en las direcciones de la red Bitcoin para identificar las direcciones empleadas por los delincuentes; Zheng et al. (2018) intentan rastrear las transacciones maliciosas de Bitcoin y adquieren un nuevo método de agrupación heurística; Bang y Choi (2019) proponen el desarrollo de un sistema de monitoreo para detectar y rastrear transacciones ilegales recolectando y analizando información de la red *Blockchain*; Yang et al. (2019) detectan usuarios sospechosos de haber cometido un delito a través de las características de las transacciones de los usuarios en el sistema Bitcoin y establecen una clasificación para distinguir a los usuarios normales de los sospechosos y agrupar a los usuarios empleando un modelo gaussiano para detectar a los sospechosos; Turner y Irwin

(2018) señalan por un lado, las técnicas heurísticas y de análisis de grafos para construir una imagen del comportamiento de las direcciones y las transacciones Bitcoin y por otro, los métodos de *Big Data* y redes sociales para aumentar los datos sobre transacciones potencialmente ilícitas empleando *machine learning* para la clasificación y agrupación de transacciones sospechosas y Zhao y Guan (2015) proponen un método basado en análisis de grafos para analizar la agrupación de identidades en el sistema Bitcoin y estudiar las propiedades del flujo de divisas de las transacciones.

Otro de los grupos obtenidos de investigaciones es aquel que se refiere a la investigación de delitos concretos desde un punto de vista técnico. Así Zareh y Shahriari (2018), presentan un enfoque para identificar *botnets* mineras de Bitcoin (Botcoins); Akcora et al. (2020) proponen un marco para predecir automáticamente nuevas transacciones de *ransomware* en una familia conocida y predecir la aparición de nuevas familias; Phetsouvanh et al. (2018) proponen técnicas de minería de grafos para explorar las relaciones entre las direcciones de carteras sospechosas de pertenecer a una trama de extorsión que utiliza Bitcoin; Al-Hashedi et al. (2021) realizan una revisión del estado del arte de las técnicas de detección del fraude financiero, incluyendo el fraude de criptomonedas.

Por último, se encuentra el grupo de investigaciones que presentan o desarrollan mejoras para la investigación de este tipo de criminalidad desde una perspectiva técnica en el análisis forense digital. Se incluyen aquí Kuzuno y Karam (2017) que proponen un entorno local de soluciones para analizar direcciones relacionadas con actividades sospechosas y un sistema que gestiona los datos en tiempo real con diversas técnicas de rastreo y visualización (estadísticas, relaciones gráficas entre direcciones, agrupación de direcciones conocidas, etc.); Balaskas y Franqueira (2018) realizan una revisión de las herramientas de análisis de la *Blockchain*, establecen una taxonomía temática basada en sus aplicaciones y presentan los retos para el desarrollo y la investigación; Zollner et al. (2019) que proponen combinar el análisis *postmortem* de lugares específicos (monederos, dispositivos móviles, etc.), habitualmente utilizado en la investigación forense actual del Bitcoin con el análisis de datos en vivo; Sun et al. (2019) que crea "BitVis", un sistema interactivo de visualización de la relación entre las cuentas Bitcoin, a través del cual se pueden filtrar las transacciones bajo demanda, interactuar con las redes de transacciones para buscar información y analizar el comportamiento de estas, lo que facilita la vigilancia de los delitos financieros por parte de las autoridades y Wang et al. (2020) proponen un sistema de denuncia de delitos a través de la *Blockchain* para conseguir un mayor anonimato.

Sin embargo, aunque no constituyeran un grupo numeroso, los resultados que han sido

de interés para este trabajo son aquellas investigaciones que abordan la criminalidad cometida con criptomonedas desde una perspectiva criminológica. Esto es, aquellas investigaciones que estudian este tipo de criminalidad de forma general realizando estimaciones de los delitos cometidos, las que estudian si las criptomonedas favorecen la realización de determinados delitos, aquellas que se centran en estudiar los usuarios que intervienen en esta criminalidad, las que abordan las motivaciones de los usuarios para involucrarse en esta actividad y las que se centran en estudiar delitos específicos que se cometen con esta tecnología. En definitiva, todas aquellas que en términos generales abordan los diferentes aspectos del crimen en relación con esta criminalidad, es decir, delito, víctima, autor y control social.

En primer lugar, se encuentran aquellos estudios destinados a determinar si las criptomonedas constituyen una herramienta que favorece el desarrollo de la criminalidad y estiman el volumen y la gravedad de esta delincuencia. Así, se puede encontrar Brown (2016) que estudia si las criptomonedas favorecen la criminalidad constituyendo una amenaza potencial para la sociedad y un riesgo que deba preocupar a los legisladores; Janze (2017) que estudia si las criptomonedas son una tecnología empleada principalmente por criminales; Ali et al. (2015) estudian cómo el Bitcoin ha sido una herramienta de utilidad para los criminales y lucrativa para el crimen; Saldaña-Taboada (2019) presenta cómo las criptomonedas disponen de determinadas características que pudieran favorecer el desarrollo de delitos a las organizaciones criminales; Kethineni y Cao (2020) estudian la influencia de las criptomonedas en la actividad criminal como facilitador de ciertos delitos, la situación de su regulación y lo desafíos actuales; Foley et al., (2019) realizan una estimación sobre la cantidad de transacciones con Bitcoin que se pueden relacionar con actividades ilegales; Kethineni et al., (2018) estudian los factores que contribuyen a la utilización del Bitcoin en la criminalidad, así como la aplicación de conceptos criminológicos tradicionales para explicar estas actividades delictivas y Pieters y Vivanco (2017) estudiaron si la variación en el precio del Bitcoin entre diferentes casas de cambio podía explicarse por la utilización de estos servicios en la actividad criminal, hallando que aquellos que no disponían de políticas de KYC presentaban precios diferentes.

Otro grupo recoge aquellas investigaciones que se centran en los usuarios de este tipo de criminalidad. Así, Yelowitz y Wilson (2015) estudiaron el interés de los usuarios en el Bitcoin hallando que la programación informática y las actividades ilegales estaban relacionadas con un interés por las criptomonedas, mucho más que los motivos políticos o de inversión; Buil y Saldaña-Taboada (2021) estudiaron el comportamiento de los usuarios de

estos delitos y hallaron que la mayoría de las actividades delictivas cometidas con criptomonedas se concentran en unos pocos usuarios.

En cuanto al grupo de investigaciones que abordan delitos concretos en los que se utilizan criptomonedas, se pueden señalar Aránguez (2020), Pérez (2020) y Saldaña-Taboada (2022) que estudiaron el panorama general español de este tipo de criminalidad a partir de un análisis jurisprudencial centrándose en los delitos de estafa, que son los que mayormente se obtuvieron; Pérez López (2017) que estudia cómo las criptomonedas son un instrumento para la comisión de delitos de blanqueo de capitales; Brenig et al. (2015) estudian si existen incentivos económicos que puedan favorecer la adopción de las criptomonedas en el blanqueo de capitales; Vasek y Moore (2015) estudiaron las estafas basadas en Bitcoin estimando su relevancia y estableciendo una clasificación de estas (estafas Ponzi, estafas de minería, billeteras e intercambios fraudulentos) y Xia et al. (2020) estudian las estafas de criptomonedas relacionadas con el COVID-19 (estafas de token, estafas de chantaje, estafas de *malware*, estafas de esquema Ponzi y estafas de donaciones).

En cuanto a las motivaciones de los usuarios para utilizar las criptomonedas, de acuerdo con Butler (2021) se ha encontrado que existe un vacío en la literatura sobre actitudes y motivaciones de los usuarios de criptomonedas con fines ilícitos. En este sentido se recoge la investigación del propio Butler (2021) que aborda las actitudes y motivaciones del uso de las criptomonedas para la actividad ilícita desde la perspectiva de los usuarios en foros clandestinos y de la red oscura. Para ello, parte de tres preguntas de investigación: 1) propiedades importantes de las criptomonedas para los usuarios de actividades ilícitas; 2) actitudes y experiencias de los usuarios al utilizar criptomonedas para actividades ilícitas; 3) hasta qué punto las CC son un facilitador de la actividad ilegal clandestina y de la red oscura.

La Necesidad de Más Investigación Criminológica

Con respecto a los antecedentes de la investigación en materia de criptomonedas y criminalidad, se ha podido observar un predominio de estudios de carácter técnico tendentes a la detección y monitoreo de transacciones ilícitas o el desarrollo de técnicas o herramientas que faciliten el análisis de la *Blockchain* desde un punto de vista forense y que faciliten la visualización de los resultados. En definitiva, se muestra un predominio en el abordaje de este fenómeno desde el análisis forense digital y el asesoramiento y apoyo a aquellas autoridades encargadas de su detección y persecución.

Se ha identificado la necesidad de desarrollar un estudio integral que aborde el fenómeno de las criptomonedas en la criminalidad desde una aproximación criminológica. En

este caso, lejos de centrarse en los aspectos técnicos de estos delitos, lo que se persigue es obtener una visión general que permita comprender el fenómeno y sus causas y generar el conocimiento necesario para elaborar políticas de prevención adaptadas a las necesidades existentes, además de orientar a los profesionales encargados de elaborar medidas de prevención consistentes en la limitación o prohibición del uso legal de las criptomonedas.

Aunque se han encontrado estudios con esta perspectiva que han realizado una estimación de este tipo de criminalidad, han estudiado si las criptomonedas son facilitadores del delito o han buscado comprender por qué se utiliza esta tecnología en la criminalidad, también presentan inconvenientes que han motivado la realización de estudios posteriores. En primer lugar, en comparación con la totalidad de los estudios en esta materia, este grupo de investigaciones son minoritarias y fueron realizadas hace dos años mínimo, por lo que podría ofrecerse un conocimiento más actualizado. En segundo lugar, son investigaciones realizadas por diferentes autores, en periodos temporales separados y en las que abordan diferentes aspectos de esta criminalidad utilizando datos muy dispares. No se dispone de una visión global e integral de todos los aspectos relacionados con este tipo de criminalidad. En tercer lugar, aunque muchas de estas investigaciones estudian si esta tecnología favorece la criminalidad, en su mayoría no presentan una metodología de carácter empírico que les permita obtener dichas afirmaciones más allá de la supuesta idoneidad de la tecnología. Además, aunque muchas de estas sí que persiguen los objetivos señalados anteriormente, emplean una metodología basada en la utilización de técnicas y herramientas de detección automática, lo que limita la obtención de nuevo conocimiento basado en características sustanciales del fenómeno.

Por todo ello, será necesario el estudio integral del fenómeno en el que se aborden los siguientes aspectos que se consideran clave para su comprensión de forma global. Están basados en una aproximación al fenómeno desde el conocimiento criminológico y son: un estudio sobre el tipo de delitos que se comete de forma mayoritaria, victimización, aspectos de la tecnología que favorece su uso criminal, motivaciones de los autores.

De esta forma, se hace hincapié en su perspectiva criminológica porque podrá aportar un enfoque global del fenómeno criminal mediante el estudio del delito, las causas, autores y víctimas y formas de evitar y prevenir el delito. Dando un paso más allá del descubrimiento del delito o de su autor y la evitación de delitos futuros.

En este sentido, permitirá el estudio y la identificación de los costes y beneficios que se pueden observar en la utilización de esta tecnología con fines delictivos. Aunque se requiere de un estudio que profundice en este aspecto, los costes que se podrían considerar

estarían relacionados con la detección de las autoridades o la no obtención de los beneficios esperados. Los beneficios que aportaría su utilización podrían estar relacionados con aquellos que se observan en su utilización con carácter legal como el pseudoanonimato, los bajos costes, la posibilidad de cambio en cualquier tipo de divisa de forma global, etc. En definitiva, se trata de aportar respuestas que permitan determinar si las criptomonedas constituyen una herramienta criminal, en lugar de basar este hecho en suposiciones de idoneidad.

Por lo tanto, se ampliará el conocimiento existente de este fenómeno criminal en relación con su volumen, facilitadores, motivaciones y características. Todo ello será de utilidad para justificar y adaptar las medidas de prevención que consistan en la limitación o prohibición de la utilización de las criptomonedas. Esta tecnología no tiene un carácter ilegal, es decir, su existencia no se basa en la comisión de actividades delictivas. Las medidas adoptadas deberán adaptarse a los derechos y libertades de los usuarios interesados en utilizar esta tecnología de forma legal para respetar su privacidad. La obtención de un conocimiento que permita comprender el fenómeno de forma global permitirá una detección y persecución del delito más adecuada y precisa, especialmente en el desarrollo de herramientas y tecnologías que sirvan de apoyo a las autoridades encargadas de la lucha contra este tipo de criminalidad. Además, permitirá mejorar las políticas de prevención, que podrán dirigirse específicamente hacia aquellas necesidades que se deban cubrir, en todo caso incluyendo también a los usuarios implicados. Esto es, el conocimiento obtenido también se utilizará con el fin de educar a la población en las nuevas formas delictivas existentes, de forma que no solo se centren los esfuerzos en el desarrollo de tecnologías avanzadas que detecten y persigan estas actividades.

BLOQUE III: CUESTIONES METODOLÓGICAS Y ANALÍTICAS SOBRE EL ESTUDIO DE LA DELINCUENCIA COMETIDA CON CRIPTOMONEDAS.

Capítulo 8. Diseño de la Investigación

Según lo visto en capítulos anteriores, son conocidos los casos de delitos en los que se han empleado criptomonedas para facilitar su desarrollo y asegurar su rentabilidad. Sin embargo, tal y como se ha mostrado en el capítulo 7, las investigaciones que giran en torno a esta materia están más centradas en la persecución y detección de las transacciones ilícitas en la *Blockchain* y en el desarrollo de tecnologías capaces de realizar estas acciones de forma automática. Hasta el conocimiento del que se dispone, no se ha encontrado un contenido científico en el que se hayan estudiado en su conjunto los actores intervinientes en estos delitos, así como los tipos de delitos, la victimización, los roles de las criptomonedas y las motivaciones criminales.

El objetivo que se persigue con el presente trabajo es el de realizar una aproximación criminológica al fenómeno de utilización de las criptomonedas en la comisión del delito. Consistirá en el estudio de los autores, tipos de delitos, víctimas, los roles de las criptomonedas y las motivaciones criminales.

Todo ello sugiere la necesidad de una investigación con un carácter exploratorio, que permita conocer más acerca del fenómeno y desarrollar conocimiento de interés para contrastar hipótesis (Bows, 2018). No obstante, esta elección no exime de cierto carácter descriptivo en algunos puntos de la investigación en los que se realiza la descripción de determinadas personas o situaciones. Una investigación de carácter exploratorio, como se han realizado en concreto con estudios centrados en el delito de robo, buscaría comprender las experiencias de victimización de este delito, mientras que una investigación de carácter descriptivo examinaría la prevalencia y naturaleza de estos delitos durante un tiempo o área geográfica determinadas (Bows, 2018, p. 95).

Por tanto, teniendo en cuenta el carácter exploratorio de la investigación que se plantea y la materia de la que se trata, se parte de una primera hipótesis, sin que esto pueda significar la aparición de hipótesis posteriores derivadas del estudio y análisis que se plantean. La hipótesis de partida es que una comprensión global del fenómeno criminal desde todos los elementos del delito permite determinar su importancia como herramienta criminal, esto es, si se trata de "dinero criminal" y dirigir las actuaciones de intervención y prevención hacia los aspectos clave.

Por todo ello, la presente investigación seguirá una metodología de carácter mixto que combina métodos cuantitativos y cualitativos. Este tipo de metodología permite una mejor comprensión de los fenómenos complejos y multifacéticos (Valls-Prieto, 2022), examinando

al mismo tiempo su extensión y su naturaleza (Heap y Waters, 2018). De este modo, resulta adecuada para la elaboración de una investigación sobre criminalidad cometida con criptomonedas. Este fenómeno goza de una enorme complejidad y de multitud de aspectos que se han de considerar para poder comprenderlo en su totalidad. Al carácter poliédrico del delito, se le añaden las dificultades de investigar esta delincuencia que facilita a los autores la ocultación de su identidad y la comisión efectiva del delito (Miró-Llinares, 2012). Además, la utilización de las criptomonedas en estos delitos supone algunas dificultades añadidas. Las características propias de estas criptomonedas como el anonimato, su utilización global o el cambio a cualquier divisa aumentan la complejidad de investigación de este fenómeno. Por ello, se ha considerado el desarrollo de la metodología mixta, ya que las fortalezas de un método pueden compensar las debilidades del otro y empleando ambos pueden proporcionar un panorama completo de este fenómeno tan complejo cuya explicación resultaría insuficiente únicamente empleando un método cuantitativo o cualitativo. La metodología mixta permitirá que ambos métodos complementen sus debilidades ofreciendo una respuesta más completa a la pregunta de investigación planteada, de carácter criminológico, así como también permite responder a preguntas de investigación diferentes fomentando finalmente la integridad de los resultados.

El desarrollo de una metodología de carácter mixto implica considerar dos cuestiones: la cuestión de prioridad y la cuestión de secuencia (Bryman, 2016). La cuestión de prioridad hace referencia a la importancia que tendrán los componentes cualitativo y cuantitativo en la investigación, si un componente tiene un peso mayor que otro y por tanto es dominante. La cuestión de secuencia se refiere al orden en el que se desarrollan los componentes de la investigación, si se desarrollan unos antes que otros o si, por el contrario, se desarrollan varios de forma simultánea.

Para el desarrollo de la metodología de esta investigación se proponen cinco experimentos, dos de ellos presentan una metodología de carácter cuantitativo y los restantes de carácter cualitativo. En relación con la cuestión de prioridad, se considera que los experimentos 2, 3 y 4 son dominantes y tienen mayor relevancia dentro del proyecto de investigación, mientras que los experimentos 1 y 5 tendrán menor importancia que los anteriores (Tabla 1)[173]. El primer experimento (cuanti) se considera de menor relevancia porque la obtención de los resultados esperados supondrá un complemento para el

[173] Esta importancia se muestra en las abreviaturas empleadas: “cuanti” o “CUANTI”. Los caracteres que se muestran en mayúsculas significan que ese experimento tiene una prioridad mayor. Por el contrario, los caracteres en minúscula indican que el experimento tiene una prioridad menor.

conocimiento generado con el resto de los experimentos. Esto es, permitirá complementar, apoyar o negar los posibles resultados obtenidos con el resto de las metodologías planteadas. El segundo experimento (CUALI) se considera relevante porque, aunque sus resultados se refieren al panorama español, puede dar una visión completa del fenómeno que podría suponer un punto de referencia para el estudio del fenómeno a nivel internacional. El tercer experimento (CUANTI) se considera relevante porque permite explorar las variables tiempo y espacio en este tipo de criminalidad, hecho que no es fácil si se considera su dificultad de detección y la complejidad para obtener bases de datos oficiales. El cuarto experimento (CUALI) se considera relevante puesto que permite obtener información sobre el fenómeno, sus motivaciones y el desarrollo del delito a partir del testimonio de los propios autores en una comunidad anónima en la que se estimula este intercambio de información sin temor a ser detectado. Por último, el quinto experimento (cuali) se considera de menor relevancia que los anteriores porque constituye un caso de estudio sobre algunas de las características que pueden motivar a la utilización de criptomonedas en el delito. Este aspecto es estudiado de una forma mucho más amplia en el cuarto experimento, por lo que en este caso tendría un alcance menor. Sin embargo, su desarrollo es importante ya que permite estudiar de forma empírica algunas de las motivaciones delictivas en un entorno en el que, a diferencia de otros países, se puede obtener el producto de forma legal en establecimientos gestionados por el gobierno.

En cuanto a la cuestión de secuencia, la metodología presenta un diseño simultáneo en el que los componentes de la investigación son desarrollados prácticamente al mismo tiempo sin que haya influencia de ninguno de ellos en la recogida de datos de los otros (Tabla 1). Se trataría de un diseño integrado, en el que alguno de los componentes puede tener prioridad, pero lo importante es que el trabajo se basa en ambos enfoques (Bryman, 2016). En este caso, se trataría de un diseño simultáneo, pero este tipo de diseño también permite el diseño secuencial. El desarrollo de este diseño es típico en investigaciones en las que ambos componentes son insuficientes por separado para comprender el fenómeno de interés. Por tanto, resulta adecuado para el diseño de una investigación que aborda diferentes aspectos del complejo fenómeno de la criminalidad cometida con criptomonedas.

De esta forma, el diseño completo de la investigación, según sus cuestiones de prioridad y secuencia, podría sintetizarse de la siguiente forma: cuanti/ CUALI/ CUANTI/ CUALI/ cuali} → Integración → Resultados[174]

Tabla 1.

Diseño de la metodología de la investigación.

Experimento	Método	Prioridad	Secuencia
1	Cuantitativo	Cuanti	Simultáneo
2	Cualitativo	CUALI	Simultáneo
3	Cuantitativo	CUANTI	Simultáneo
4	Cuantitativo	CUALI	Simultáneo
5	Cualitativo	Cuali	Simultáneo

Fuente: Elaboración propia

El desarrollo de los diferentes componentes de la investigación se combinará a través del proceso de complementariedad. En este, varios métodos se combinan para investigar aspectos distintos, pero a menudo superpuestos de un fenómeno, otorgando una mayor comprensión (Heap y Waters, 2018). Se ha considerado apropiado este diseño para esta investigación porque el objetivo perseguido es el estudio y análisis de diversos aspectos del fenómeno de la criminalidad cometida con criptomonedas, por lo que se trata de un fenómeno complejo que requiere de varios métodos para conseguir una mayor comprensión. Para ilustrar esto, un ejemplo de lo anterior se puede ver en la investigación de Waters (2009) en la que se emplean datos secundarios de la "*British Crime Survey*" (CUANTI) para estudiar aspectos demográficos de los consumidores de drogas mayores de 50 junto con entrevistas semiestructuradas (cuali) para comprender las motivaciones y actitudes hacia el consumo de drogas.

Cada uno de los componentes de esta investigación seguirá una metodología, herramientas y datos diferentes con diversos propósitos. A continuación, se describen en detalle los cinco experimentos que se desarrollarán en la presente investigación:

El experimento primero consiste en una metodología de carácter cuantitativo basada en la utilización de los sistemas inteligentes en un conjunto de datos de delitos cometidos con criptomonedas por grupos criminales.

[174] Esta fórmula sintetiza las cuestiones de prioridad y de secuencia en la investigación. Posteriormente indica que los resultados obtenidos de los experimentos se integrarán para obtener los resultados finales de la investigación.

La hipótesis de partida es que la utilización de estas herramientas y metodologías permiten obtener un mejor conocimiento sobre el fenómeno criminal permitiendo el desarrollo posterior de actuaciones más efectivas por parte de las FCSE.

El objetivo general de este experimento consiste en aplicar las técnicas de los sistemas inteligentes a este fenómeno criminal para descubrir nuevo conocimiento sobre los aspectos criminológicos del delito como son los autores, las víctimas y el tipo de delitos cometidos. Este conocimiento podría servir al mismo tiempo para la evaluación y la adaptación de las herramientas policiales basadas en técnicas de IA.

De esta forma, se planteó una metodología formada por tres etapas, comenzando por el estudio de la criminalidad con criptomonedas cometida por grupos, seguido del estudio de las metodologías y herramientas actuales en la lucha contra el delito y, finalmente, la utilización de sistemas inteligentes en conjuntos de datos de criminalidad con criptomonedas.

Sin embargo, se anticipa que dicho experimento no pudo llevarse a cabo de la forma propuesta debido a una serie de inconvenientes que se encontraron durante su desarrollo. Se propuso la utilización de herramientas de análisis de criptoactivos que permiten estudiar de forma interactiva los flujos monetarios. Sin embargo, no fue posible obtener los datos necesarios por parte de las autoridades y los proyectos de investigación relacionados, por lo que no se dispuso de una muestra suficiente y válida que permitiera obtener los resultados esperados. Al mismo tiempo se detectó la incapacidad de determinar lo que se considera como organización criminal únicamente por la observación de los datos. Se podía extraer información sobre sobre las transacciones realizadas, pero ningún contexto adicional de interés criminológico.

El segundo experimento consiste un análisis cualitativo del contenido de la jurisprudencia penal española del año 2017 al 2022 sobre delitos cometidos con criptomonedas, especialmente Bitcoin. Se trata de un método de carácter cualitativo en el que se estudia y analiza la información obtenida para codificarla y extraer los temas de interés. En este caso, se ha operado de forma deductiva, ya que previamente al proceso de codificación se han determinado las categorías de interés en el análisis de los datos: tipo de delitos, *modus operandi*, tipo de autores y víctimas, así como el rol de las criptomonedas en cada caso. Se ha considerado la elección de este método de investigación debido a su carácter flexible y relativamente sistemático, que permite estudiar y analizar los datos pertenecientes a varios años y obtener la información necesaria para las variables previamente establecidas.

La fuente de los datos es de carácter documental oficial, en específico la jurisprudencia penal española elaborada por el Poder Judicial español. Por ello, los datos que

se trabajarán son datos primarios, que no se han obtenido de otras investigaciones, entidades o grupos. El motivo por el que se ha escogido esta fuente de datos es que el carácter oficial de la información dota de fiabilidad a los resultados obtenidos. Además, permite obtener información detallada sobre aspectos de este tipo de delincuencia que no hubiera sido posible obtener por otros medios sin contacto con las víctimas o los autores.

Los resultados de este experimento podrán aportar una primera aproximación al fenómeno desde la situación actual en el panorama español. Debido al carácter transnacional de la utilización de la criptomoneda y la globalidad de la cibercriminalidad, las fronteras entre países son difusas y aunque se trate de casos españoles, esto puede ser un reflejo de actuaciones muy similares en países externos. Además, en algunos de los casos con los que se ha trabajado, se ha encontrado que la actividad delictiva excede las fronteras de España, viéndose culpables en otros países.

El tercer experimento consiste en un análisis descriptivo de los datos obtenidos de un repositorio web sobre registros de víctimas de delitos cometidos con criptomonedas. Se trata de un método de carácter cuantitativo a través del que se obtiene información sobre los patrones temporales y espaciales de la victimización, la frecuencia según el tipo de delitos, así como su correlación con otros factores. El motivo por el que se ha escogido este método es doble. En primer lugar, de acuerdo con el propósito de la investigación, el análisis de los patrones espaciotemporales requiere de un método de carácter cuantitativo. El segundo, es que un método de carácter cuantitativo era el adecuado para el estudio y análisis del tipo de datos obtenidos en este caso.

La fuente de datos empleada es el repositorio de la página web “Bitcoin Abuse”. En este caso la página web se presenta como fuente de datos, pero no por su contenido, sino porque constituye el medio para descargar la base de datos almacenada. De esta forma, no cabe el riesgo de que el contenido pueda ser modificado o eliminado por parte de los administradores y se puede acceder a los datos de una forma estructurada. La elección de esta fuente de datos se debe a que es el único repositorio conocido que dispone de registros de victimización de esta delincuencia para usuarios con un carácter internacional. Esto ha podido evitar algunos de los problemas que se suelen presentar en la obtención de datos sobre este tipo de delitos. El primero es que de la misma forma que sucede con los ciberdelitos en general, la mayoría de los usuarios que han sido víctimas de algún tipo de ciberataque cometido con criptomonedas no registran este incidente empleando un cauce oficial, por lo que no se dispone de repositorios oficiales donde puedan consultarse estos datos. El segundo es que puede que la víctima no sea consciente de su victimización, pues en muchas ocasiones

estos ataques se presentan en forma de correo electrónico no deseado y no llegan a culminar sus motivaciones delictivas.

Los datos obtenidos son de carácter secundario. Las víctimas realizan el registro a través del formulario de la página web y estos quedan almacenados en el servidor. La descarga de los datos se realiza a través de la API de Bitcoin Abuse, por lo que no han sido recolectados por la investigadora de este proyecto, sino que se descarga una base de datos que han sido registrados por las propias víctimas y almacenados y estructurados por la empresa que gestiona la página web. En la base de datos se pueden encontrar varios tipos de delitos, las direcciones Bitcoin del autor, información adicional sobre este, así como información sobre el lugar, la hora y el día en el que se realizó el registro. Se dispone por tanto de ciberdelitos tradicionales como de ciberdelitos independientes.

Los resultados que se esperan son los patrones temporales y espaciales de la victimización con criptomonedas, así como los tipos de delitos más denunciados y su estudio espaciotemporal.

El cuarto experimento consiste en el estudio de las discusiones sobre la utilización de criptomonedas en un foro de la *Darknet* que se desarrollará conforme a un enfoque de la Teoría Fundamentada o *Grounded Theory Approach* (GT).

La Teoría Fundamentada constituye en un método de análisis cualitativo creado por Glasser y Strauss (1967) que se caracteriza porque la teoría emerge de los datos recogidos y analizados durante el proceso de investigación (Clark et al., 2021). Se caracteriza por dos elementos: 1) La teoría se desarrolla a partir de los datos; 2) es una aproximación iterativa en la que la recogida de los datos y su análisis están haciéndose referencia constantemente (Clark et al., 2021, p. 361). De esta forma, se trata de una metodología de carácter inductivo en la que, de manera inversa al proceso de investigación convencional, la investigación comienza con la recogida de datos y su continua comparación con la teoría y solo se accede a aquella literatura que será más relevante para el tema (Davies & Francis, 2018, p.71).

El carácter iterativo de este enfoque resulta de interés para explorar el contenido dinámico de las conversaciones que se mantienen en el foro. Los comentarios de una discusión pueden ser eliminados o modificados por un usuario o por el moderador del foro, además, resulta casi imposible conocer con exactitud el contenido su totalidad. Por lo tanto, este enfoque permite iniciar el estudio a partir de una pregunta de investigación y comenzar elaborando conceptos y categorías sin cerrar la posibilidad de redefinir y crear otras nuevas.

De forma general, el proceso de desarrollo de la investigación ha tenido lugar según lo expuesto para el enfoque *Grounded Theory* por Clark et al. (2021, p. 530). El proceso

comienza con una pregunta de investigación, que en este caso ha consistido en las características de las criptomonedas que motivan a los criminales a utilizarlas en el desarrollo de sus actividades delictivas. Se ha accedido al foro de la *Darknet* y se ha realizado un muestreo de discusiones que incluían el término "Bitcoin". Se han recogido los datos de las discusiones y se ha realizado una primera codificación de la que han comenzado a extraerse algunos conceptos. A partir de estos resultados se generaron las primeras categorías, incluyendo temas como la utilización de las criptomonedas para escapar a la detección de las autoridades. Estos resultados han sido comparados con información externa sobre la temática y se ha continuado con la recogida de datos y su agrupación en categorías hasta llegar a la saturación de categorías. Una vez explorada la relación entre las categorías se han generado ciertas hipótesis que han motivado continuar con la recogida de datos hasta llegar a la saturación de categorías. Finalmente, se comprueban las hipótesis y se comparan con información externa para crear una teoría formal.

La operacionalización de los datos ha tenido un carácter inductivo, de lo particular hacia lo general, de acuerdo con el enfoque de la Teoría Fundamentada. Se comenzó accediendo a la fuente de la información y recopilando los datos formando algunas categorías para ir añadiendo nuevas categorías posteriormente. Esto ha permitido la exploración de este ámbito de forma iterativa, lo que resultada de interés debido a la falta contenido prestablecido en esta materia.

La fuente de recogida de los datos ha sido el foro *online*. Los datos obtenidos son de carácter primario, ya que se han recogido por la investigadora de este proyecto a partir de la lectura y el análisis de las discusiones del foro. La elección del foro como fuente de los datos se debe a que el análisis de su contenido puede ofrecer información directamente proporcionada por el sujeto, que puede encontrarse mucho más motivado a compartirla debido al carácter anónimo de los foros, unido al anonimato de la *Darknet*. Esto para el investigador supone la oportunidad de conocer las diferentes interacciones de un grupo en su contexto habitual en la red sin que se haya alterado o perdido la información suministrada.

La recogida se ha llevado a cabo a través del método de la observación no participante porque se ha accedido a las discusiones del foro sin la participación de la investigadora ni su identificación. Este tipo de participación es propia de la Teoría Fundamentada y se ha considerado adecuada en este caso por varios motivos. El primero de ellos tiene que ver con la naturaleza de la materia que se está tratando. Las discusiones objeto de estudio describen cómo llevar a cabo una actividad ilegal de la forma más efectiva para escapar de las autoridades, no ser detectada y obtener el máximo beneficio económico. Se ha considerado

que la advertencia a los usuarios del foro de la participación en una investigación podría suponer un elevado riesgo de perder el contenido por la autocensura por parte de estos o bien por la restricción del acceso al foro por parte de los moderadores. El segundo motivo, es que se ha considerado que debido a que se trata de un foro en la *Darknet*, únicamente accesible a través de la red TOR, el diseño de este entorno ya está destinado a respetar la privacidad de todos los usuarios que participan, además de la utilización de un *nickname*. Así, es casi imposible la identificación de ninguno de los participantes en estas discusiones. En tercer lugar, al tratarse de una investigación en la que la investigadora accede al entorno objeto de estudio, la identificación y puesta en conocimiento de la investigación podrían poner en riesgo a la investigadora (Castro-Toledo, F. J., & Gómez-Bellvís, A. B., 2022). Por último, la obtención de un consentimiento informado resultaba de gran complejidad debido a la propia estructura del foro y a la organización de los temas y las discusiones. El contenido del foro "Dread" se organiza según temas, que pueden estar incluidos dentro de comunidades diferentes. Cada comunidad tiene asignados diferentes moderadores anónimos que están encargados de la gestión del contenido de las discusiones de diferentes temáticas dentro de una misma comunidad. En este caso, la búsqueda del término "Bitcoin" dentro del foro "Dread" ha recopilado diferentes discusiones que pertenecían a diferentes temas dentro de diferentes comunidades del foro. La recopilación del consentimiento informado en cada una de las discusiones estudiadas hubiera sido una tarea altamente compleja. Por todo ello, se consideró adecuado continuar con el método de la observación no participante en la recogida de los datos.

Los resultados de este experimento podrán aportar información detallada sobre las motivaciones de los sujetos para usar las criptomonedas en el desarrollo de un delito, así como de los detalles de esta utilización en la actividad criminal.

El quinto y último experimento consiste en un análisis cualitativo del contenido de páginas web canadienses de venta de cannabis y productos derivados. De la misma forma que en el cuarto experimento, se seguirá el enfoque de la Teoría Fundamentada (Glasser y Strauss, 1967) en el que la teoría emerge de los datos recogidos y analizados durante el proceso de investigación (Clark et al., 2021).

De forma general, el proceso de desarrollo de la investigación ha tenido lugar según lo expuesto para el enfoque *Grounded Theory* por Clark et al. (2021, p. 530). El proceso comienza con una pregunta de investigación, que en este caso ha consistido en determinar cuáles son las características de las criptomonedas que atraen a los criminales. Para ello, se estudiará el sistema de pago disponible en los mercados objeto de estudio. En cada una de las

tiendas online se simulará la compra de algún producto hasta finalizar en el apartado "método de pago", en el que aparece si está disponible el pago en Bitcoin u otro método. Se ha registrado el método de pago disponible para cada tienda online, de forma que finalmente se ha elaborado una base de datos en la que se incluyen elementos relevantes de la tienda online junto con la forma de pago disponible.

La fuente de datos en este caso es la web superficial en la que se ubican las tiendas online de cannabis. Se trata de páginas a las que se puede acceder fácilmente empleando alguno de los buscadores web tradicionales e introduciendo los términos clave relacionados. Los motivos por los que se ha elegido esta fuente de datos son varios. El primero de ellos es que este contenido es fácilmente accesible y presenta un carácter público y transparente. Aunque existe el riesgo de que el contenido pueda ser modificado o eliminado, durante el desarrollo de la investigación se registraron todos los datos clave en una base de datos, de forma que se actuó de forma previa ante la posibilidad de este riesgo. Cualquier modificación en dichas páginas no afectaría a la elaboración de la investigación. En segundo lugar, esta fuente de datos permite la obtención de una gran cantidad de datos solo con introducir algunos de los términos clave en la materia. Por lo que, si se controlan los riesgos que puedan surgir, se trata de una interesante posibilidad para obtener información relevante. Por último, los negocios criminales de venta de cannabis y derivados se ubican en la Internet superficial. Esto es, al tratarse del lugar en el que están ubicados estos negocios, la web superficial como fuente de datos se considera fiable, puesto que el vendedor necesita que el comprador disponga de la información necesaria para ejecutar eficazmente la compra y recibir los beneficios.

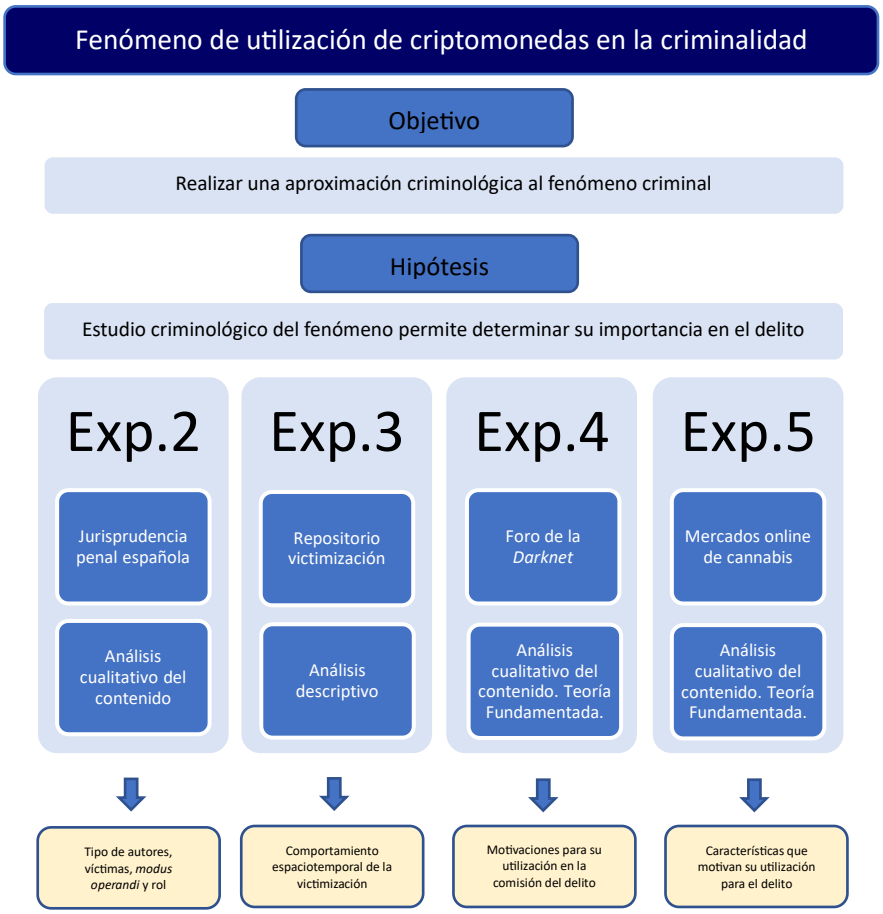
Los datos obtenidos son datos de carácter primario, ya que han sido recogidos y almacenados por la investigadora de este trabajo, no habiendo sido obtenidos de otros investigadores, entidades u organizaciones. A partir de estos, se espera estudiar el rol de la criptomoneda más conocida como sistema de pago en un entorno en el que la compra del cannabis es legal y está regulada por el gobierno.

Los resultados de este experimento serán relevantes para el estudio de las motivaciones de los criminales para la utilización de las criptomonedas, afirmando o negando aquellas concepciones previas sobre las características de esta tecnología más relevantes para la comisión de un delito.

Todo el procedimiento de la metodología de la investigación que se ha descrito a lo largo de este apartado se recoge y se presenta en el diagrama siguiente:

Figura 1.

Diagrama del diseño de la investigación.



Fuente: Elaboración propia

En primer lugar, se muestran el objetivo general y la hipótesis de la investigación. En segundo lugar, se muestran cada uno de los experimentos, incluyendo la fuente de los datos que se utilizó, la metodología empleada y los resultados esperados (Figura 1). El primer experimento no se incluye en este diagrama debido a que los resultados fueron negativos.

Capítulo 9. El Estudio de la Criminalidad Cometida Con Criptomonedas Usando Sistemas Inteligentes (Experimento 1)

Introducción

De entre todos los tipos de delincuencia existentes, el crimen organizado mantiene la atención de las autoridades y se encuentra en el foco de sus actuaciones para luchar contra la criminalidad. Este tipo de criminalidad preocupa a las autoridades por el alcance que pueden tener sus acciones, la diversidad de delitos que tienen asociados y la dificultad de detección y persecución que presenta.

Sus formas de actuación se han adaptado a los avances actuales con el objetivo de hacerse más eficientes, en términos de obtener mayores beneficios evitando los riesgos de detección. La expansión de la utilización de Internet ya supuso un cambio sustancial en la estructura de las organizaciones criminales hacia la formación de redes con carácter transnacional (Corte-Ibáñez y Giménez-Salinas, 2010). Esto no solo les ha facilitado la comunicación, la fijación de objetivos y la organización de delitos, sino que, en primer lugar, les ha facilitado el desarrollo de delitos tradicionales empleando las TIC, como el blanqueo de capitales. En segundo lugar, les ha permitido la comisión de delitos ciberdependientes, únicamente posibles gracias a la aparición y desarrollo de Internet, como la compraventa con criptomonedas en los criptomercados de la *Darknet* (Europol, 2018; Casas, 2017).

De esta forma, el cibercrimen se ha situado como uno de los mercados delictivos en auge en los grupos criminales. Se considera como parte de este fenómeno aquellos delitos ciberdependientes o puramente cibernéticos (Europol, 2018), así como los delitos de carácter tradicional en los que se emplean las Tecnologías de la Información y la Comunicación (TICs) (Fernández Bermejo y Martínez Atienza, 2018).

Como parte de la adopción de los grupos criminales a las nuevas tecnologías existentes, se ha observado la utilización de criptomonedas, en especial de Bitcoin. De esta forma, las criptomonedas se convirtieron en una amenaza emergente en la lucha contra la delincuencia y en este caso, contra los grupos criminales, algo que se comenzó a señalar en el informe IOCTA para el año 2014 (Europol, 2014). Desde entonces, su utilización ha sido tratada en los diversos informes de Europol hasta la actualidad.

Así, a la especialización, opacidad, trasnacionalidad y gravedad de la criminalidad organizada se les une la posibilidad de emplear una moneda que permite la realización de transacciones anónimas, descentralizadas (sin intermediarios), internacionales y a través de

Internet, que se pueden cambiar a cualquier moneda fiduciaria y que tienen bajos costes (Fernández, 2018). Esto ha generado especial preocupación en las agencias de seguridad y cuerpos policiales ya que, lógicamente, a las dificultades de detección de las organizaciones criminales se les unen aquellas derivadas de la utilización de las criptomonedas.

El uso más frecuente de las criptomonedas en los grupos criminales se ha observado mayormente en el blanqueo de dinero, pero también se han visto involucradas en la financiación (Kruisbergen et al., 2019). Los informes de la Europol, tanto los IOCTA (2019) como los SOCTA (2018), nos permiten ver la realidad de la actividad del crimen organizado en sus modalidades *online* y *offline* y la tendencia del uso de las criptomonedas. La utilización criminal de criptomonedas se ha extendido no solo a otros países, sino también a otros actores, haciendo de esta actividad un fenómeno internacional que no se circunscribe únicamente al territorio de un país (Pérez López, 2017). Este es el caso de la compraventa de productos ilegales en mercados delictivos de la *Darknet* utilizando criptomonedas (Europol, 2021).

Ahora bien, de la misma forma que la criminalidad ha actualizado sus formas de comisión del delito, se hace necesario que las autoridades adapten sus estrategias y herramientas para poder situarse al mismo nivel al que está sucediendo el crimen.

Así, en el ámbito de la lucha contra el crimen organizado se ha observado la necesidad de dejar de centrarse únicamente en estrategias de carácter reactivo dirigidas únicamente a la detención de los delincuentes y la puesta a disposición ante las autoridades, que tienen un escaso efecto preventivo (Redondo y Garrido, 2013). Son necesarias soluciones proactivas que den respuesta a los problemas criminológicos que presentaba este tipo de criminalidad (Medina, 2011). Aunque en su momento surgieron estrategias centradas en el análisis delictivo para dar respuestas específicas a problemas delictivos, como fueron los *Policing Oriented Problems (POP)* (Goldstein, 1990), estas tenían un carácter local, por lo que no se ajustaban a las necesidades actuales de una criminalidad transnacional.

Con los acontecimientos terroristas del 11-S se evidenciaron las limitaciones de las estrategias policiales anteriores y la necesidad de gestionar la información y los datos policiales como herramientas que permitieran una mejora en la toma de decisiones vinculadas a la seguridad. Por todo ello, se desarrolló el modelo *Intelligence-led policing* o vigilancia basada en la inteligencia, una estrategia proactiva que consistía en la recogida y el análisis de datos para obtener inteligencia criminal con la finalidad de conseguir una toma de decisiones orientada a la reducción e irrupción del delito (Ratcliffe, 2008). Especialmente, esta aproximación se centraba en comprender las causas económicas, sociales, culturales, políticas

y tecnológicas que posibilitaban la aparición y emergencia del delito (Valls-Prieto y Gómez-Romero, 2016). Además, hacía participe a la comunidad y a otras agencias de investigación, de forma que presentaba un carácter colaborativo.

Relacionado con el anterior, surgió el *Predictive policing* o vigilancia predictiva (Perry et al., 2013). Consiste también en la estimación o predicción de los delitos con la finalidad de poder actuar previamente a su desarrollo. A diferencia del *Intelligence-led policing,* la vigilancia predictiva se centra en el dónde y en el cómo del delito, esto es, analiza grandes cantidades de datos de delitos para un área geográfica determinada con el propósito de anticipar dónde y cuándo ocurrirá el delito (Perry et al., 2013). Por el contrario, el *Intelligence-led policing* identifica víctimas potenciales y posibles delincuentes y trabaja con la comunidad para prevenir la victimización (Ratcliffe, 2008). Aunque, dentro de este último pueden a veces incluirse estrategias de *Predictive Policing*, ambas constituyen estrategias independientes.

Este planteamiento sobre la posibilidad de predecir el delito se basa en el conocimiento de la Criminología, que con las teorías de la oportunidad sostiene que el delincuente no actúa de forma aleatoria, sino que tiende a actuar desde una zona de *confort*, repitiendo aquellas actividades delictivas que fueron exitosas (Brantingham, 2009). Esto permitiría identificar patrones delictivos y factores que influyen en la comisión del delito haciendo que sea posible predecir el comportamiento futuro a partir del comportamiento anterior del delincuente.

En los últimos años, las estrategias que estudian, analizan y estiman el delito como el *Intelligence-led policing* y el *Predictive Policing* han vuelto a adquirir importancia con el desarrollo de nuevas tecnologías como el análisis de datos masivo o *Big Data,* las técnicas de aprendizaje automático en Inteligencia Artificial (IA) o, en general, los sistemas computacionales inteligentes.

El análisis de datos masivo o *Big Data* consiste en el aprovechamiento del gran volumen de datos heterogéneos surgidos en la actualidad gracias a las mejoras de los sistemas de recogida, almacenamiento y procesamiento de datos y al fenómeno de la datificación. Estas nuevas capacidades de procesamiento masivo de datos han sido de gran utilidad para descubrir patrones y tendencias desconocidas (Mayer-Schönberger y Cukier, 2013).

Por otro lado, la inteligencia artificial (IA) "tiene por objeto que los ordenadores hagan la misma clase de cosas que puede hacer la mente" (Boden 2017, p.11). John McCarthy, uno de los padres fundadores de la disciplina, describió en 1955 la IA como la

capacidad “de hacer que una máquina se comporte de formas que serían llamadas inteligentes si un ser humano hiciera eso” (Kaplan 2017, p.1).

De esta forma, existen una multitud de definiciones de IA, ya que cada una se plantea desde un enfoque diferente. En este trabajo no se tiene como objetivo una revisión exhaustiva de la IA ni de los sistemas inteligentes. Por lo tanto, en este caso, de acuerdo con Valls-Prieto (2021), se ha considerado más interesante hacer referencia a los puntos clave de esta para poder comprender cómo se aplicaría al ámbito criminal. De esta forma, se recogen cuatro puntos de interés (Valls-Prieto, 2021, p.25): 1) la IA está desarrollada por humanos que establecen unos patrones de origen o el procedimiento para descubrirlos; 2) los algoritmos de toma de decisiones de los sistemas inteligentes requieren de datos para poder funcionar, lo que puede suponer un riesgo para la privacidad de los usuarios; 3) cada sistema de IA tiene un objetivo concreto por lo que los riesgos o inconvenientes de estos dependen de cada sistema en específico y 4) toda predicción o estimación que realicen estas herramientas tendrá su fundamento en datos o situaciones conocidas anteriores, viéndose reducida su efectividad ante situaciones completamente desconocidas.

La utilización de la Inteligencia Artificial ha demostrado tener grandes beneficios en la detección de problemas y en la toma de decisiones en diversos ámbitos. Sus técnicas se pueden aplicar a multitud de áreas de actuación “siendo posible su utilización en cualquier campo en el que se requiera de la toma de decisiones por humanos” (Valls-Prieto, 2021, p. 27). Por ello, existen muchos y muy diversos avances basados en técnicas de IA, hasta el punto de que “desgraciadamente hay drones militares recorriendo los campos de batalla [pero], por suerte, también hay robots dragaminas” (Boden 2017, p. 12).

Aunque anteriormente ya se permitía la extracción de patrones de los datos utilizando técnicas estadísticas, la novedad del *Big Data* es “la gran escala y algunas de las nuevas técnicas de computación que parecen imitar ciertos aspectos del cerebro humano (…)” (Kaplan 2017, p. 33). De esta forma, el análisis masivo de datos se apoya en los algoritmos de Inteligencia Artificial que estudiarán el comportamiento de un fenómeno y estimarán o predecirán su futuro. Y viceversa, la Inteligencia Artificial actual debe su éxito a la capacidad aumentada de cómputo del Big Data.

Existen dos enfoques principales dentro del ámbito de la Inteligencia Artificial: el que basa su aprendizaje en reglas lógicas y el que se basa en datos. La investigación propuesta se centraba en este último. La Inteligencia Artificial basada en el procesamiento de datos consiste en el desarrollo de sistemas adaptativos que mejoran su rendimiento conforme se les presentan más datos, lo que se conoce habitualmente como aprendizaje máquina o *machine*

learning y que es la aproximación mayoritaria en el área en la actualidad (Valls-Prieto, 2021, p.20).

Volviendo al tema que nos ocupa, para el caso de la investigación de la criminalidad con criptomonedas, el carácter público de la *Blockchain* de Bitcoin sugiere que sería posible analizar estos datos para conocer mejor los comportamientos de los grupos criminales. Cabe señalar, no obstante, que se requerirá de información adicional que permita la identificación de autores o conocer el tipo de delito o las víctimas implicadas. Tal y como se expuso en el bloque II, en el apartado relativo a la investigación, la mayoría de las investigaciones realizadas en esta materia están dirigidas a la desanonimización de las transacciones a través de diferentes métodos o herramientas que permitan obtener la información adicional necesaria para conocer la identidad de una dirección y determinar el usuario con el que se corresponde un patrón de actuación (Turner e Irwin, 2018).

En esta labor, se ha visto que eran de utilidad las técnicas basadas en IA. Este es el caso de las técnicas heurísticas y de análisis de grafos, que permiten construir una imagen del comportamiento de las direcciones y transacciones Bitcoin, y mediante métodos de *Big Data* y redes sociales aumentan los datos sobre las transacciones parcialmente ilícitas, empleando *machine learning* para la clasificación y agrupación de transacciones sospechosas (Turner e Irwin, 2018). No obstante, plantean que la solución ideal para este fenómeno constaría de una herramienta con capacidad predictiva que de forma automática recoja y analice datos de la Bitcoin Blockchain y fuentes de datos externas y aplique criterios de búsqueda, indexación y agrupación para identificar comportamientos sospechosos (Irwin y Turner, 2018).

En general, en el marco de las estrategias de vigilancia IOCTA y SOCTA mencionadas, se ha destacado la necesidad del desarrollo de herramientas integrales de detección, análisis y estimación del delito que sirvan de apoyo a las autoridades encargadas de la lucha contra el crimen. Así, la prevención policial y la seguridad han sido dos áreas en las que se ha propuesto la utilización de la IA para mejorar las actuaciones de las autoridades encargadas de la lucha contra la criminalidad (Miró- Llinares, 2018).

De esta forma, los algoritmos están siendo utilizados para estimar los riesgos de delitos en relación con el lugar o las características de las personas y mejorar la toma de decisiones en cuanto a su prevención, la investigación y la persecución (Miró-Llinares, 2020). Se persigue con ello mejorar la estimación de eventos futuros basados en el conocimiento de eventos anteriores (Miró-Llinares, 2020).

En determinados tipos de delincuencia, como la desarrollada por grupos criminales, se consideran oportunos el estudio de la criminalidad, la detección de sus actividades delictivas

y la monitorización, además del establecimiento de evaluaciones de riesgo de amenazas que permita una actuación de carácter prospectivo (Andrews et al., 2013). Es el caso de la creación de escáneres ambientales o *Environmental Scanning,* que son herramientas basada en IA que permiten la detección y predicción de amenazas delictivas (Valls-Prieto y Gómez-Romero, 2016). España ha participado en proyectos en este sentido como el proyecto CASPER o el ePOOLICE (2015) que se presentaban como escáneres ambientales que facilitaban la toma de decisiones y la gestión de los recursos policiales generando alertas de riesgo delictivo geolocalizadas y clasificadas por colores en función del nivel de riesgo.

A este respecto, se toman como ejemplo de herramientas de detección, análisis, predicción o estimación del delito: ePOOLICE, COPKIT y TITANIUM[175].

En primer lugar, el "ePOOLICE" (*early Pursuit against Organized crime using envirOnmental scanning, the Law and IntelligenCE systems*) era un sistema de detección de actividades delictivas organizadas y de predicción de la evolución de esta delincuencia. Sus objetivos consistían, por un lado, en la detección del crimen organizado a través del descubrimiento de actividades delictivas típicamente vinculada a este y de organizaciones criminales subyacentes para evitar la formación de sistema criminales más fuertes y resistentes (ePOOLICE, 2015). Por otro lado, perseguía la predicción de la evolución del crimen organizado a través de un sistema de escaneo ambiental para analizar y desarrollar escenarios de posibles amenazas en el futuro (ePOOLICE, 2015).

El resultado del proyecto ePOOLICE fue un sistema de alerta y vigilancia estratégica que permitía a las autoridades encargadas de la lucha contra el delito apreciar, evaluar y anticipar delitos emergentes, monitorear el entorno y capturar en tiempo real información relevante de fuentes heterogéneas (la ley, informes gubernamentales, web, redes sociales, etc.) (ePOOLICE, 2015).

En segundo lugar, el "COPKIT" (*Technology, training and Knowledge for Early-Warning/ Early-Action led Policing in fighting Organised Crime and Terrorisms*) aborda el problema existente al analizar, prevenir, investigar y mitigar el uso de las nuevas tecnologías de la información y la comunicación por parte del crimen organizado y los grupos terroristas (COPKIT, 2022). Propone un sistema de alerta y acción tempranas basado en la vigilancia dirigida por inteligencia o *Intelligence-led policing*, lo que ofrece un marco para guiar

[175] Todas ellas han recibido fondos de diversas ayudas de la Unión Europea para poder desarrollarse, como es el caso del programa de investigación e innovación Horizonte 2020 de la Unión Europea. Esto podría indicar que a nivel europeo existe interés por parte de los estados en utilizar estas herramientas en la estimación de la criminalidad.

operaciones, priorizando las necesidades y optimizando los recursos (COPKIT, 2022). El sistema de alerta rápida o intervención temprana utiliza una serie de técnicas de Inteligencia Artificial (IA) y aprendizaje automático para recopilar y analizar datos con pequeños y grandes volúmenes (COPKIT, 2022). El analista utilizará estos datos para identificar tendencias, advertencias o señales delictivas, observando potenciales amenazas y tomando decisiones (COPKIT, 2022).

Por último, y más cercano a esta investigación, el proyecto "TITANIUM" (*Tools for the Investigation of Transactions in Underground Markets*) tenía como objetivo la investigación, el desarrollo, la implementación y la validación de técnicas y soluciones basadas en datos que sean de utilidad para aquellas agencias encargadas de cumplir la ley que tengan como objetivo la investigación de actividades delictivas o terroristas que involucren monedas virtuales y/o mercados clandestinos en la red oscura (TITANIUM Project, 2020a). Se presenta como un proyecto de necesidad debido al carácter seudónimo de las monedas virtuales y el secreto de los mercados delictivos (TITANIUM Project, 2020a). Los resultados de TITANIUM consistieron en un conjunto de servicios y herramientas forenses que podían ser utilizadas para la investigación de: "1) el monitoreo de tendencias en ecosistemas del mercado de monedas virtuales y *Darknet*; 2) el análisis de transacciones en diferentes libros de contabilidad de moneda virtual y 3) la generación de informes de prueba para tribunales basados en procedimientos analíticos reproducibles y legalmente compatibles" (TITANIUM Project, 2020b).

Por todo ello, junto con las estrategias de *Intelligence Led Policing*, la vigilancia predictiva está adquiriendo popularidad en el uso policial. Aunque es utilizada en este ámbito, no se debe caer en un optimismo ni en un pesimismo extremos sobre su utilización en el ámbito criminal (Miró-Llinares, 2020). Por un lado, permitiría analizar grandes cantidades de información de una forma más rápida que una persona, añadiendo transparencia a la decisión del analista e incluso puede que redujeran los sesgos que pudiera tener una persona en la toma de decisiones (Miró-Llinares, 2020, p. 10). No obstante, todavía no se dispone de suficiente evidencia empírica sobre si la utilización de esta tecnología contribuye realmente a la prevención del delito (Miró-Llinares, 2020).Tampoco se debe caer en posturas extremadamente pesimistas que relacionan la utilización de esta tecnología directamente con la vigilancia y el control de la sociedad por parte del Estado y que estos datos además, sean utilizados en la vigilancia policial ocasionando discriminación y dinámicas de poder (Miró-Llinares, 2020). Estas tecnologías no son neutras, pero tampoco son algo definido imposible de cambiar, por lo que habrá que adoptar una actitud "realista, ética y empíricamente

informada" ante las herramientas de IA, algoritmos de BD y la vigilancia policial (Miró-Llinares, 2020, p. 18).

Por todo lo anterior, se consideró de utilidad el estudio, análisis y aplicación de herramientas basadas en sistemas inteligentes que permitan la lucha contra la criminalidad con criptomonedas cometida por grupos criminales. No obstante, previamente era necesario conocer el funcionamiento de estas herramientas y obtener el conocimiento suficiente sobre este tipo de criminalidad para adaptar las herramientas al abordaje de este fenómeno. Además, en este propósito sería también de utilidad la aplicación de técnicas de *Big Data* y aprendizaje automático en Inteligencia Artificial, que permitiera generar el conocimiento nuevo mencionado anteriormente y estimar el comportamiento de este fenómeno en el futuro. Anticipamos que no se puedo llevar a cabo porque se careció de los datos necesarios sobre transacciones fraudulentas con criptomonedas para la investigación.

Metodología

Frente al fenómeno de la criminalidad cometida con criptomonedas por grupos organizados, el objetivo general que se tenía inicialmente en esta investigación era el de aplicar las técnicas de los sistemas inteligentes a este fenómeno criminal para descubrir nuevo conocimiento sobre los aspectos criminológicos del delito como son los autores, las víctimas y el tipo de delitos cometidos. Este conocimiento podría servir al mismo tiempo para la evaluación y adaptación de las herramientas policiales basadas en técnicas de IA.

La hipótesis inicial consistía en que la utilización de estas herramientas y metodologías permite obtener un mejor conocimiento sobre el fenómeno criminal que posibilita el desarrollo de actuaciones más efectivas, eficientes y rápidas para las FCSE y otras autoridades, además de mejorar la prevención del delito mediante el conocimiento anticipado obtenido de los modelos predictivos.

En cuanto a los datos que se esperaba obtener, estarían formados por los casos delictivos proporcionados por proyectos europeos como COPKIT o TITANIUM, además de casos de delitos de la prensa digital e informes policiales. También se esperaba disponer de un conjunto de direcciones Bitcoin pertenecientes a delitos cometidos por grupos criminales y proporcionadas por las FCSE.

De esta forma, se planteó una metodología formada por tres etapas, comenzando por el estudio de la criminalidad con criptomonedas cometida por grupos, seguido del estudio de las metodologías y herramientas actuales en la lucha contra el delito y, finalmente, la utilización de sistemas inteligentes en conjuntos de datos de criminalidad con criptomonedas.

De forma detallada, primero se estudiaría la criminalidad desarrollada con criptomonedas por grupos criminales. Para ello, se realizaría una revisión bibliográfica y un estudio de casos. La fuente de datos empleada serían la jurisprudencia, los informes de agencias de seguridad y FCSE, noticias digitales y casos delictivos conocidos y aportados por Policía Nacional, Guardia Civil y *Mossos d'Esquadra*. Con todo ello, se elaborarían criterios relevantes sobre la criminalidad con criptomonedas que posteriormente se utilizarían en la utilización de los sistemas inteligentes.

En segundo lugar, se propuso el estudio y análisis de las herramientas existentes en la lucha contra este tipo de criminalidad. Se centraría en aquellas que utilizaran sistemas inteligentes debido a la capacidad de predicción y estimación de los delitos.

Por último, se aplicarían diversas técnicas relacionadas con el análisis de datos de delitos en los que intervienen las criptomonedas con el objetivo de descubrir nuevos conocimientos en forma de patrones que no se habían considerado en un estudio previo sobre el fenómeno. Todo ello serviría para establecer comparaciones entre el comportamiento observado y el conocimiento existente y establecer criterios relevantes para la identificación de esta criminalidad.

El nuevo conocimiento generado anteriormente permitiría proponer mejoras y una adaptación de las herramientas empleadas en la persecución del crimen. Esto permitiría conseguir una herramienta de detección, análisis y predicción de este tipo de criminalidad que fuera adecuada para este fenómeno criminal al mismo tiempo que fuera respetuosa con los derechos fundamentales y adaptada a las necesidades de las personas encargadas de la lucha contra esta criminalidad.

Resultados

Los resultados que se obtuvieron durante las primeras etapas de la investigación indicaron que no sería posible obtener los resultados esperados de acuerdo con la metodología planteada inicialmente. Los motivos de esto se pueden dividir en dos grupos. El primero tiene relación con una serie de inconvenientes que surgieron durante el proceso de la investigación que dificultaron o impidieron el desarrollo de la estrategia planteada. El segundo tiene relación con una serie de descubrimientos que surgieron del proceso de investigación que plantearon la necesidad de dar una nueva dirección a al proyecto.

En relación con el primer grupo, la obtención de los datos necesarios fue el principal inconveniente que se encontró en la investigación. Esto se debió a la incapacidad de las autoridades para proporcionar datos específicos sobre grupos criminales que utilizaran

criptomonedas. Se solicitaron estos datos a Policía Nacional, Guardia Civil y *Mossos d'Esquadra* y las respuestas obtenidas en los tres casos fueron muy similares, y es que no disponían de los datos. Aunque disponían de algunas direcciones Bitcoin sospechosas de haber cometido un delito, no contaban con registros o con una base de datos sobre direcciones Bitcoin relacionadas con delitos, ni con el tipo de delito con el que se les relacionaba. Además, tampoco contaban con la información relativa a los individuos, por lo que no era posible determinar si se trataba de un grupo criminal. Únicamente se ofrecieron algunas direcciones que pertenecían a casos ampliamente conocidos que habían sido resueltos, en los que, debido a la investigación por otros medios, se había podido determinar que se trataba de una organización criminal y se habían podido recolectar las direcciones pertenecientes a sus carteras Bitcoin.

Al mismo tiempo, aunque se tenía contacto con algunos de los miembros de los proyectos ePOOLICE y COPKIT, tampoco fue posible obtener los datos requeridos. Se pudo conocer algunos de los casos de uso empleados por los investigadores para desarrollar la herramienta; sin embargo, debido a la confidencialidad de esta información y a los diferentes propósitos de la investigación, tampoco se obtuvieron datos sobre direcciones Bitcoin o sobre grupos criminales que utilizaran estas herramientas en sus delitos. De hecho, estas dificultades eran mostradas de forma explícita en la página web del proyecto TITANIUM, en la que se recogía que la mayoría de los datos, herramientas y resultados del proyecto no estaban disponibles de manera abierta. Además, puesto que las herramientas habían contado con inversión privada y/o estaban destinadas a ser utilizadas por agencias de aplicación de la ley, no podían divulgarse al público general (TITANIUM Project, 2020a).

En este sentido, cabe señalar que el procedimiento del proyecto de TITANIUM estaba formado por siete etapas o pasos y que se tuvo acceso a la herramienta del paso 3, "GraphSense" [176], dedicada al seguimiento del dinero y que mostraba las transacciones realizadas por los criminales permitiendo rastrearlas (TITANIUM Project, 2020b). Concretamente, GraphSense es una plataforma de análisis de criptoactivos que se puede utilizar para investigaciones interactivas de flujos monetarios (Haslhofer et al., 2021), por ejemplo, para identificar grupos de direcciones que probablemente pertenezcan a la misma entidad del mundo real. La instalación y configuración del software Graphsense pudo

[176] En el momento de realización de esta investigación se tuvo acceso anticipado a la versión de prueba de esta herramienta. Sin embargo, en la actualidad ya se puede acceder a la herramienta públicamente por cualquier persona interesada https://graphsense.info/

realizarse de forma satisfactoria, pero aún no se disponía de direcciones Bitcoin para realizar el análisis.

En consecuencia, se decidió recopilar manualmente direcciones Bitcoin de casos delictivos conocidos que mostraban públicamente estos datos. De esta forma, se accedió a periódicos digitales y a informes de agencias de seguridad y FCSE y se recopilaron algunas direcciones, que pertenecían mayormente a casos de ataques *ransomware*. Esto se debe a que en esta tipología delictiva el criminal requiere del pago de la víctima, por lo que muestra la dirección de la cartera Bitcoin con el propósito de recibir el dinero exigido a cambio de liberar el equipo afectado. Sin embargo, el conjunto de direcciones recopiladas también presentaba inconvenientes como que mayormente estaban limitadas a ataques ransomware, se trataba de casos conocidos antiguos y ya resueltos y, además, constituía un número muy limitado de registros, lo que dificultaba la realización de un análisis amplio. Por último, aunque eran casos conocidos en su mayoría, no era posible obtener más información relativa a la pertenencia a un grupo criminal.

En relación con el segundo grupo de inconvenientes, y a partir del análisis limitado realizado con Graphsense, se obtuvieron varios resultados negativos. Así, fue posible obtener aquellas carteras con las que se relacionaban las direcciones proporcionadas, además de patrones temporales y la interacción con entidades registradas como casas de cambio o mercados de la *Darknet*. Sin embargo, al tratarse de una muestra muy reducida e incompleta, no se pudo conocer el tipo de actividad delictiva realizada, quiénes eran los autores o información sobre las víctimas (en caso de haberlas). Esto imposibilitó la obtención de resultados de interés criminológico que pudieran ser empleados en la elaboración de estrategias de actuación y prevención de este tipo de delitos. En definitiva, solo se podía obtener información sobre las transacciones realizadas entre carteras, la relación con algunas entidades y su información temporal, pero ningún contexto adicional.

Finalmente, en un plano teórico, se descubrió que resulta complejo determinar qué es un grupo criminal en cuanto a la criminalidad cometida con criptomonedas. En su mayoría, los grupos criminales que se conocen en este ámbito fueron identificados a partir de otras fuentes, habiéndose descubierto la actividad con criptomonedas posteriormente. Es decir, no se puede realizar la identificación de un grupo criminal únicamente a partir del rastreo de su actividad con criptomonedas como Bitcoin. Será necesaria información adicional que vincule a una persona sospechosa de pertenecer a un grupo criminal con una cartera de criptomonedas. Tal y como se expuso en el bloque II, se han desarrollado investigaciones capaces de agrupar carteras de criptomonedas que pertenecen a una misma entidad; sin

embargo, no es posible afirmar solo con dicha información que se trata de un grupo criminal, ya que puede tratarse de una única persona que es la propietaria del conjunto completo de direcciones. Además, esto se dificulta aún más cuando se considera el hecho de que las criptomonedas constituyen una tecnología legal, por lo que en el estudio de las transacciones pudieran aparecer sujetos que utilizan las monedas de forma legal.

De esta forma, se ha adoptado una postura amplia en relación con las consideraciones de grupo criminal. Es decir, en lugar de limitar el estudio de las criptomonedas solo a aquellas actividades delictivas cometidas por grupos criminales, se ha considerado cualquier fenómeno de la delincuencia cometida con criptomonedas. Así, se busca obtener información valiosa que, en su caso, también podría ser utilizada en investigaciones posteriores en las que se requiera de la identificación o al menos la presunción de que se trata de un grupo criminal.

Discusión

Por todo ello, se detectó la necesidad de abordar el fenómeno de la delincuencia con criptomonedas desde una aproximación criminológica. La estrategia planteada anteriormente hubiera podido ofrecer conocimiento nuevo sobre la actividad realizada con carteras de criptomonedas a través de la implementación de sistemas inteligentes. No obstante, además de los inconvenientes de los datos mencionados anteriormente, se consideró que se requería el desarrollo de una investigación previa que desde una aproximación desde la Criminología pudiera abordar este fenómeno delictivo de una forma holística. Esto es, se observa una necesidad de disponer de información sobre los autores, las víctimas y las actividades delictivas, con el propósito de conseguir una prevención efectiva.

De acuerdo con posturas como la de Miró-Llinares (2020), los desarrollos científicos sobre tecnologías como la IA y su utilización en el entorno policial deberán basarse lo máximo posible en conocimiento por lo que, la utilización de este tipo de herramientas para la investigación y prevención de la delincuencia "deben partir necesariamente de una visión social y criminológica de los fenómenos implicados (…)" (p. 21). Aunque en la utilización de las técnicas de IA son necesarios elevados conocimientos de informática y estadística, las ciencias sociales comienzan a adquirir importancia en este ámbito, de forma que se considera que la tecnología no debería ser el elemento central de estas herramientas, sino que también habría que considerar la comunidad y el funcionamiento de la policía (Miró-Llinares, 2020).

De la misma forma que se planteó en la estrategia anterior, se pretende obtener conocimiento que pueda ser de utilidad en el desarrollo de sistemas inteligentes que puedan abordar este tipo de criminalidad. No obstante, en este caso, en lugar de obtener esa

información de forma automática a través del análisis de datos masivo como se había previsto, se aportará el conocimiento obtenido de diversos experimentos desarrollados a través de una metodología mixta desde una aproximación criminológica. La combinación de los resultados obtenidos será de utilidad para cuestionar el conocimiento que se tiene actualmente sobre este fenómeno delictivo y para apoyar el desarrollo posterior de herramientas de lucha contra el delito.

En definitiva, se identificó la necesidad de desarrollar una investigación que excediera la obtención de información que fuera el soporte para el desarrollo de herramientas de análisis forense de este tipo de criminalidad. Esto daría soporte a futuras investigaciones que propongan soluciones basadas en la utilización de sistemas inteligentes.

La lucha contra el crimen y los avances en su predicción requieren de una investigación criminológica que encuentre soluciones a los retos y problemas que plantea a la sociedad. Un análisis delictivo y de riesgo constituye una parte importante de los objetivos finales de la investigación. Por ello será importante también tener en cuenta el factor humano en el desarrollo y aplicación de estas herramientas.

Capítulo 10. Estudio de la Jurisprudencia Española en Materia de Criminalidad y Criptomonedas (Experimento 2).

En este experimento se tiene como objetivo general conocer el panorama delictivo español en cuanto a la delincuencia en la que se utilizan las criptomonedas. Para el desarrollo de los objetivos propuestos y en relación con la literatura que se ha tratado en capítulos anteriores, se parten de las siguientes hipótesis:

H1. La complejidad tecnológica de las criptomonedas y la *Blockchain* da lugar al desarrollo de un tipo de criminalidad técnicamente especializada.

H2. El principal rol de la criptomoneda en la delincuencia es su utilización como sistema de pago.

H3. Debido a su capacidad para ocultar el rastro de la actividad delictiva, se emplearán en su mayoría criptomonedas que permitan una privacidad más elevada.

H4. Su mayor utilización como sistema de pago produce que mayormente no sea posible identificar a las víctimas, que serán de carácter difuso.

H5. La mayor utilización de la criptomoneda Bitcoin como sistema de pago ocasiona que el autor implicado en el delito presente un carácter individual.

Métodos y Materiales

Estrategia de Investigación

La metodología de este experimento consiste en el análisis cualitativo del contenido de la jurisprudencia penal española en materia de criptomonedas y criminalidad, que fue descrita anteriormente en el apartado general de metodología.

Para la obtención de la información necesaria se ha empleado la base de datos de jurisprudencia "Aranzadi". Considerando lo expuesto en la literatura sobre el tema, en la búsqueda se emplearon las palabras clave "criptomoneda", "blockchain" y "bitcoin"[177]. Los resultados obtenidos se filtraron seleccionando la jurisprudencia del área de derecho penal entre los años 2017 y 2022.

[177] De entre todos los tipos de criptomonedas existentes se decidió el empleo del término "Bitcoin", porque dicha criptomoneda además de ser la pionera es actualmente la más utilizada, la más conocida y por tanto la criptomoneda de mayor relevancia en cuanto a su capitalización de mercado. Esto puede consultarse en la web https://coinmarketcap.com/es/

Una vez realizada la búsqueda se obtuvieron 48 resultados para "criptomoneda", 51 para "Bitcoin" y 4 para "Blockchain"[178] obteniendo una muestra total de 103 resultados. No obstante, fue necesario un proceso de limpieza previo al desarrollo de la base de datos con el conjunto de sentencias que se van a utilizar. Primero, porque algunas de las resoluciones obtenidas aparecen en varios de los términos de búsqueda realizados[179]. Segundo, porque había que eliminar aquellas resoluciones judiciales en las que, aunque aparecía alguno de los términos clave, el contenido no guardaba relación con el tema, o bien, no contaba con la información necesaria para la consecución de los objetivos de la investigación[180].

Descripción de la Muestra

Finalmente, se obtuvo una muestra de 70 resoluciones judiciales (n=70). El listado de todas las resoluciones judiciales según el término de búsqueda empleado y el año de la resolución se pueden consultar en el Apéndice 1.

Si se observa la Tabla 2 elaborada a partir de los resultados obtenidos, se puede ver que el término "Bitcoin" ha sido el que más resultados ha proporcionado (n=37), seguido del término "criptomoneda" (n=35). El año en el que se han producido más resoluciones judiciales en esta materia fue el 2021 (n=38), siendo el año 2017 el que ha tenido menos resoluciones.

[178] Resultados actualizados para la fecha 21 de febrero de 2022.

[179] Se encontró un total de 14 resoluciones que aparecían en varias búsquedas al mismo tiempo. Como, por ejemplo, la AP Barcelona (Sección 21ª), auto núm. 2128/2021 de 4 noviembre [JUR 2022\55708]; la AP de Barcelona (Sección 21ª) Auto núm. 1565/2020 de 19 de noviembre [JUR\2021\173486]; la AP de Álava (Sección 2ª) Sentencia núm. 4/2021 de 15 de enero [ARP 2021\679] o la TS (Sala de lo Penal, Sección 1ª) Sentencia núm. 326/2019 de 20 junio [RJ\2019\2925].

[180] Se eliminó un total de 16 resoluciones judiciales: AP de Valladolid (Sección 4ª) Sentencia núm. 100/2020 de 3 junio [JUR 2020\204806]; AP de Barcelona (Sección 5ª) Auto núm. 329/2020 de 30 junio [JUR 2020\232831]; AP de Barcelona (Sección 7ª) Auto núm. 728/2020 de 26 noviembre [JUR 2021\112825]; AN (Sala de lo Penal, Sección 3ª) Auto núm. 327/2021 de 10 septiembre [JUR 2021\306954]; AN (Sala de lo Penal, Sección 3ª) Auto núm. 349/2021 de 1 octubre [JUR 2021\325511]; AP de Madrid (Sección 4ª), auto núm. 333/2021 de 26 de mayo [JUR 2021\374627]; AN (Sala de lo Penal, Sección 4ª), auto núm. 14/2022 de 11 de enero [JUR 2022\48689]; AN (Sala de lo Penal, Sección 4ª), auto núm. 49/2022 de 31 de enero [JUR 2022\59716]; AN (Sala de lo Penal, Sección 4ª), auto núm. 48/2022 de 31 de enero [JUR 2022\60334]; AP de Pontevedra (Sección 5ª) Auto núm. 388/2018 de 23 julio [JUR\2018\295137]; AP de Castellón (Sección 2ª) Auto núm. 505/2017 de 10 noviembre [JUR\2018\42298]; AP de Pontevedra (Sección 5ª) Auto núm. 527/2018 de 31 octubre [JUR\2019\3713]; AP de Barcelona (Sección 5ª) Sentencia núm. 403/2020 de 22 de julio [JUR\2020\293115]; AP de Valencia (Sección 5ª) Auto núm. 230/2021 de 2 marzo [JUR\2021\152431]; AP de Guadalajara (Sección 1ª) Auto núm. 33/2021 de 27 enero [JUR\2021\154453]; AN (Sala de lo Penal, Sección 2ª) Auto núm. 26/2021 de 21 junio [JUR\2021\223783].

Tabla 2.

Resoluciones judiciales obtenidas según año y término de búsqueda.

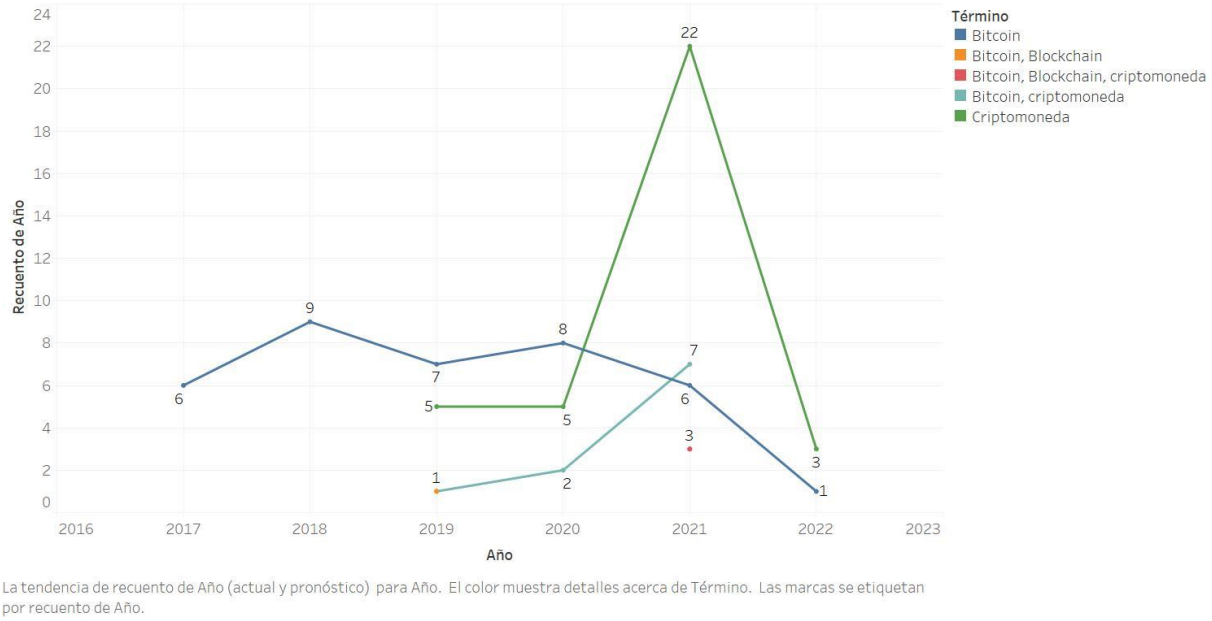
Término de búsqueda	2017	2018	2019	2020	2021	2022	Total
Bitcoin, Blockchain			1				1
Bitcoin, Blockchain, criptomoneda					3		3
Bitcoin, criptomoneda			1	2	7		10
Criptomoneda			5	5	21	3	35
Bitcoin	6	9	7	7	6	1	37
Total	**6**	**9**	**14**	**15**	**38**	**4**	**86**

Fuente: Elaboración propia a partir de los resultados obtenidos empleando la base de datos jurídica Aranzadi.

Si se observa la Figura 2 se puede ver que los resultados para el término "criptomoneda" presentan un pico pronunciado en el año 2021 con 22 resultados, a la vez que parece haber un descenso de resoluciones en las que aparece el término "bitcoin". La aparición de resoluciones con el término "Bitcoin" se mantiene constante desde el primer año del que se dispone para los datos hasta el año 2022 en la actualidad. Sin embargo, las resoluciones con el término "criptomoneda" comienzan a aparecer desde el año 2019. Las resoluciones que combinan ambos términos, "bitcoin" y "criptomoneda", comienzan a aparecer en el año 2019 con una aparente tendencia a su crecimiento. Por último, es puntual (no parece que siga ninguna tendencia) la aparición de resoluciones judiciales en las que aparecen el término "Blockchain", no habiéndose hallado ninguna resolución en la que aparezca únicamente este término, sino en combinación con alguno de los anteriores.

Figura 2.

Resoluciones judiciales según año y término de búsqueda.



Fuente: Elaboración propia a partir de los resultados obtenidos empleando la base de datos jurídica Aranzadi.

En la base de datos elaborada se incluyeron las siguientes variables (entre paréntesis el indicador de cada variable): identificador principal de la resolución judicial (ID), identificador secundario de la resolución judicial (ID2), si se incluye o no en la muestra (¿Se incluye?), término de búsqueda (Término), año de la resolución judicial (Año), tipo de delito que se está enjuiciando según lo expuesto en el Título del Código penal (Delito), tipo de delito según el capítulo del Código penal (Delito_capítulo), otra información relacionada con el delito que se está enjuiciando (Delito_adicional), el tema general que trata la resolución (Tema), el tipo de criptomoneda implicada en el suceso (Criptomoneda), tipo de autor implicado (Autor), si se trata de una empresa (¿empresa?), información adicional sobre el autor implicado (Autor_des), país en el que se desarrollaron los hechos (País), víctima del hecho delictivo (Víctima), información adicional sobre la víctima/as implicadas (Víctima_des), la motivación por la que se ha empleado la criptomoneda en el desarrollo de la actividad delictiva (Rol_cripto), si se justifica en la resolución judicial el motivo por el que se usan las criptomonedas en el delito (Motivación_resol) y la forma en la que se llevaron a cabo los hechos delictivos (Modus operandi). La elección de estas variables tiene relación con el objetivo general del experimento, así como con las hipótesis planteadas.

Resultados

Como resultado de la investigación se obtuvo finalmente una muestra de 70 resoluciones judiciales. Del estudio y el análisis de la muestra en relación con el objetivo de la investigación se agruparon los resultados obtenidos en diferentes apartados que son: 1) Delitos en los que se utilizan las criptomonedas; 2) Rol que desempeñan las criptomonedas en los delitos; 3) Tipo de criptomoneda implicada en la actividad delictiva; 4) Victimario implicado en la actividad delictiva y 5) Autor responsable de los hechos (individual o grupal).

A continuación, se presentan de forma detallada los resultados obtenidos en relación según los apartados expuestos anteriormente:

Delitos en los Que se Utilizan las Criptomonedas

Los tipos de delitos que se han extraído de las resoluciones judiciales estudiadas se han clasificado según el título y el capítulo al que pertenecen los hechos según el Código penal español.

Se debe tener en cuenta que el tipo del delito del que se trata es el que se señala en las resoluciones judiciales, es decir, no se trata del delito en específico en el que interviene directamente la utilización de las criptomonedas. Por ejemplo, la resolución judicial puede indicar que se trata de un delito de estafa, pero la utilización de las criptomonedas que se está describiendo en la resolución podría tener relación con un delito de blanqueo de capitales.

Los delitos predominantes son aquellos recogidos en el Título XIII de los delitos contra el patrimonio y contra el orden socioeconómico (n=55), seguidos de los delitos contra la seguridad colectiva (n=4) y los delitos contra la Administración pública (n=4) (Tabla 3).

Tabla 3.

Tipo de delito según el Título del Código penal español.

Tipo de delito	Total
Delitos contra el patrimonio y contra el orden socioeconómico. Delitos contra la hacienda pública y contra la seguridad social.	1
Delitos contra la libertad e indemnidad sexuales	1
Delitos de homicidio y sus formas	1
Delitos de las falsedades	1
Delitos contra el patrimonio y contra el orden socioeconómico. Delitos contra la seguridad colectiva.	3
Delitos contra la Administración pública	4
Delitos contra la seguridad colectiva	4
Delitos contra el patrimonio y contra el orden socioeconómico	55
Total	**70**

Fuente: Elaboración propia a partir de los resultados obtenidos empleando la base de datos jurídica Aranzadi.

Si se estudia en detalle el delito cometido dentro de la categoría de delitos contra el patrimonio y contra el orden socioeconómico (Tabla 4), se obtiene una mayoría de delitos de estafa (n=34) ubicados en el capítulo perteneciente a las defraudaciones. A estos les siguen los delitos de receptación y blanqueo de capitales (n=4) y los delitos de estafa junto con los delitos de apropiación indebida (n=4).

Tabla 4.

Tipo de delito contra el patrimonio y contra el orden socioeconómico según el capítulo del CP.

Tipo de delito	Total
Delitos de los daños: Delito de daños informáticos	1
Delito de daños informáticos. Delito de las defraudaciones: de fluido eléctrico y análogas.	1
De las defraudaciones: Delito de estafa. Delito de receptación y blanqueo de capitales	1
De las defraudaciones: Delito de estafa. De las falsedades documentales. De la receptación y el blanqueo de capitales.	1
De las defraudaciones: delito de estafa. De la receptación y el blanqueo de capitales. Delito de descubrimiento y revelación de secretos. Delito contra la propiedad industrial.	1
De las defraudaciones: Delito de estafa, delito de apropiación indebida. De las falsedades: De las falsedades documentales.	1
De las defraudaciones: Delito de estafa, delito de administración desleal y delito de apropiación indebida. Delitos contra la hacienda pública y contra la seguridad social. Delito de receptación y blanqueo de capitales.	1
De las defraudaciones: De las defraudaciones de fluido eléctrico y análogas	1
De las defraudaciones (delito de estafa). De la receptación y el blanqueo de capitales	1
De la receptación y el blanqueo de capitales. Delito contra la salud pública.	1
Delito de falsificación de moneda y efectos timbrados. Delito contra la salud pública.	2
De la receptación y el blanqueo de capitales	2
De las defraudaciones: Delito de apropiación indebida	3
Delito de receptación y blanqueo de capitales	4
De las defraudaciones: Delito de estafa y delito de apropiación indebida	4
De las defraudaciones: Delito de estafa	34
Total	**59**

Fuente: Elaboración propia a partir de los resultados obtenidos empleando la base de datos jurídica Aranzadi.

En su mayoría los delitos de estafa estudiados tratan sobre falsas ventas de productos a través de aplicaciones de compraventa en las que la persona interesada en la compra contacta con el vendedor para acordar la venta y una vez se ha realizado la transacción no se recibe el producto comprado ni se devuelve el dinero invertido. En estos casos la transferencia realizada por el comprador no se envía realmente al autor de la venta falsa, sino que se acuerda el envío hacia personas dedicadas profesionalmente a la compraventa de criptomonedas. De esta forma, se pretende emplear el dinero de la transferencia para la

compra de criptomonedas y eliminar el rastro de ilegalidad del dinero obtenido. Han sido numerosos los casos obtenidos en los que se ha empleado este *modus operandi* y en los que se han ofrecido diversos productos como una cámara de fotos (sentencia del JP de Zamora núm. 122/2020 de 9 junio, [JUR\2020\368548]), un perro (AP de Salamanca (Sección 1ª), sentencia núm. 24/2021 de 25 junio [JUR\2021\247102]) una fuente de alimentación (sentencia de la AP de Murcia (Sección 5ª) núm.104/2020 de 14 julio, [JUR\2020\264175]), un coche (Auto del TS (Sala de lo Penal, Sección 1ª) de 24 octubre de 2019, [JUR 2019\298172]).

En relación con el resto de los delitos que no pertenecen a los delitos contra el patrimonio y contra el orden socioeconómico, si se observa la tabla 5, se puede ver una prevalencia de los delitos contra la salud pública, en especial del tráfico de drogas (n=4). La mayoría de estos casos tratan delitos en los que en el seno de un grupo criminal se han empleado las criptomonedas como sistema de pago para la compra de drogas a través de la *Darknet* (sentencia del TSJ Islas Baleares (Sala de lo Civil y Penal, Sección 1ª), núm. 30/2021 de 5 de octubre [JUR\2021384193]).

Tabla 5.

Tipo de delito según los capítulos del CP (excluyendo delitos contra el patrimonio y contra el orden socioeconómico).

Tipo de delito	Total
Delito contra la salud pública. Tráfico de drogas	4
Delito de tráfico de influencias. Delito de malversación. Delito de prevaricación de los funcionarios públicos y otros comportamientos injustos. Delito de las negociaciones y actividades prohibidas a los funcionarios públicos y de los abusos en el ejercicio de su función.	2
Delito de falsificación de moneda y efectos timbrados	1
Delito de malversación de caudales públicos	1
Delito de tráfico de influencias y delito de malversación	1
Delitos de homicidio y sus formas	1
Delitos relativos a la prostitución y a la explotación sexual y corrupción de menores.	1
Total	**11**

Fuente: Elaboración propia a partir de los resultados obtenidos empleando la base de datos jurídica Aranzadi.

Rol Que Desempeñan las Criptomonedas en los Delitos.

Los roles de las criptomonedas que se han extraído del estudio de las resoluciones judiciales guardan relación con el propósito por el que el autor del delito utilizaba esta tecnología en el desarrollo de su actividad criminal. Así, esto no estaría relacionado con el tipo de delito que se señala en las resoluciones judiciales. Por ejemplo, para los delitos de estafa en los que se lleva a cabo una falsa venta, aunque se esté tratando dicho delito en la resolución judicial, en realidad la motivación por la que se ha utilizado la criptomoneda es para la ocultación del rastro ilegal del dinero obtenido mediante el delito de estafa, lo que está más relacionado con un delito de blanqueo de capitales.

De esta forma, del estudio del *modus operandi* de los delitos cometidos en la jurisprudencia, se ha determinado que los diversos roles que desempeñan las criptomonedas en la actividad criminal son: lucro, ocultación del rastro ilícito del dinero y sistema de pago (Tabla 6). El primero hace referencia a la búsqueda de un enriquecimiento ilícito del autor, que incorpora las criptomonedas de alguna forma en el desarrollo de su actividad delictiva con el propósito de obtener beneficios económicos. La ocultación del rastro ilícito del dinero hace referencia a la utilización de las criptomonedas con el propósito de evitar la detección del dinero que se ha obtenido de forma ilegal. Por último, la utilización de las criptomonedas como sistema de pago consiste en su utilización como moneda para pagar por productos o servicios ilegales. Como propósito secundario se ha visto también la utilización de esta tecnología como reclamo para atraer a potenciales víctimas, que frecuentemente debido al desconocimiento de la actividad y de sus riesgos acceden a participar en la actividad propuesta[181].

Si se observan los resultados presentados en la tabla 6, el papel que desempeñan las criptomonedas es mayormente el de ocultar el rastro ilícito del dinero (n=37). Le sigue su utilización como medio para atraer a las potenciales víctimas junto con el ánimo de lucro (n=12). Esto es, conseguir que se impliquen en su actividad delictiva y así apropiarse de su dinero o de sus criptomonedas y obtener beneficio económico. El tercer lugar lo ocupa la utilización de las criptomonedas como sistema de pago (n=10).

[181] Como excepción se ha encontrado un caso en el que se hace mención a las criptomonedas como parte del desarrollo de un ataque cibernético. Sin embargo, no se tenía intención real de utilizar las criptomonedas para recibir dinero a cambio del cese de esta actividad y es que no era correcto el número para la cartera Bitcoin proporcionada en el contenido del mensaje y tampoco pertenecía al autor.

Tabla 6.

Rol de la criptomoneda en el desarrollo del delito.

Tipo de rol	Total
Es parte del ataque (no lucro)	1
Atracción de la víctima, lucro y ocultación del rastro ilícito del dinero	2
Lucro y ocultar rastro ilícito del dinero	3
Lucro	5
Sistema de pago	10
Atracción de la víctima y lucro	12
Ocultar el rastro ilícito del dinero	37
Total	**70**

Fuente: Elaboración propia a partir de los resultados obtenidos empleando la base de datos jurídica Aranzadi.

Debido a su prevalencia, se han estudiado con una mayor profundidad aquellos casos en los que el rol de las criptomonedas era la ocultación del rastro ilícito del dinero. Como resultado se han obtenido diversas formas en las que se ha desarrollado la actividad delictiva con este propósito. La primera consiste en la compra de criptomonedas empleando el dinero que se obtuvo en otra actividad delictiva. Se utilizaban tarjetas de crédito duplicadas o robadas para extraer dinero en efectivo[182] o digital[183] y realizar la compra posterior de bitcoins. La segunda forma consiste en la simulación de la venta de productos a particulares a través de plataformas de compraventa online como "Wallapop" o "Milanuncios". La persona interesada en la compra contactaba con el vendedor y realizaba una transferencia a su favor, que una vez recibida utilizaba este dinero para comprar criptomonedas. También se han encontrado casos en los que el vendedor proporciona al comprador el número de cuenta de una persona que se dedica profesionalmente a la compraventa de criptomonedas a través de dinero fiduciario. Finalmente, la persona que realizó la transacción para la compra del producto no recibe ninguna entrega ni el dinero que pagó por este[184]. En este caso, cabe señalar que en varias ocasiones la criptomoneda no desempeña ningún rol en el desarrollo de la actividad delictiva, sino que únicamente forma parte de la justificación que se emplea por parte del acusado para explicar la recepción de la transferencia. Así, son numerosos los casos

[182] *Vid.,* entre otras, la sentencia de la AN (Sala de lo Penal, Sección 1ª) 22/2021 de 5 julio, [JUR 2021/230837], en la que el dinero en efectivo se obtiene a través del hackeo de cajeros automáticos.
[183] Sentencia de la AP de Salamanca (Sección 1ª) 24/2021 de 25 junio, [JUR\2021\247102]
[184] En este sentido hay una gran cantidad de casos muy similares que se diferencian únicamente en el producto que se ofrece. Entre otros, por ejemplo, un perro en la SAP de Navarra (Sección 1ª) 267/2019 de 10 diciembre, [JUR 2020\49196]; una cámara de fotos en la SAP de Navarra (Sección 1ª) 241/2019 de 22 octubre, [JUR 2020\15005]; un coche en el auto del TS (Sala de lo Penal, Sección 1ª) Auto de 24 octubre 2019, [JUR 2019\298172] o una videoconsola en la SAP de Barcelona (Sección 7ª) 646/2019 de 18 octubre, [JUR\2020\213591].

en los que se alude a la posesión o participación en un negocio de compraventa de criptomonedas para recibir tales cantidades[185], pero no se ha llevado a cabo finalmente dicha conversión a la moneda virtual. En este sentido también se han encontrado casos en los que se ha empleado el dinero obtenido ilegalmente para la compra de material o tecnología de minado de criptomonedas[186].

En cuanto al propósito de lucrarse u obtener un beneficio económico, los resultados obtenidos pertenecen en su mayoría al desarrollo de falsos negocios de inversión de criptomonedas con el objetivo de lucro. De forma general, esta actividad consiste en el depósito de cierta cantidad de dinero fiduciario hacia personas o empresas que han asegurado estar especializadas en generar importantes beneficios económicos a través de la actividad de inversión. Sin embargo, el dinero o las criptomonedas invertidas no son destinados a la inversión en el arbitraje, sino que estos sujetos se apropian indebidamente de estos fondos y no son devueltos a la víctima en ninguna de sus formas. De forma detallada, se han estudiado tres formas en las que se ha llevado a cabo esta actividad. La primera, a través de falsos *brókeres* que se encargaban de persuadir a las víctimas sobre los beneficios económicos que se podrían generar con la inversión en criptomonedas[187]. La segunda, a través de la realización de las conocidas como estafas piramidales o "esquemas Ponzi", en las que se introduce a una persona en el negocio de inversión que a su vez estará en cargada de introducir de forma sucesiva a más personas, de forma que los supuestos beneficios generados por la actividad están reservados únicamente a las personas que ocupan las posiciones más altas en la pirámide. El resto de las personas que forman parte de la estafa tienen que intentar introducir a más personas para tener alguna rentabilidad[188]. Por último, a través de la inversión realizada por las víctimas en páginas web dedicadas a tal fin, que resultaban ser falsas[189], algunas de ellas desapareciendo una vez recibida la inversión.

---

[185] *Vid.,* entre otras, la sentencia de la AP de Cantabria, núm. 235/2020 de 27 de mayo [JUR 2020\334253] y el auto de la AP de Vizcaya (Sección 2ª), núm. 90189/2020 de 12 de mayo [JUR 2021\81590]

[186] En el auto de la AP de Pontevedra (Sección 5ª) 142/2018 de 20 marzo, [JUR\2018\193971]

[187] *Vid.,* el auto del TS (Sala de lo Penal, Sección1ª), auto de 28 septiembre 2021, [JUR 2021\326865], en el bróker de "Grandefex" persuade a otra persona por teléfono para que invierta en criptomonedas, realizando una transferencia de 336.999 euros.

[188] *Vid.,* el auto de la AN (Sala de lo Penal, Sección 4ª), 488/2021 de 8 septiembre [2021\307100], en el que se expone cómo la entidad "Kuailian Bank" había creado un sistema de inversión en criptomonedas con ganancias exponenciales para atraer a inversores. Como parte de su estrategia, había creado una forma de mostrar lo beneficios obtenidos a los potenciales inversores. Sin embargo, no se trataba de beneficios reales sino que era parte de una trama para hacer creer al inversor que su actividad había generado beneficios y así motivarle para continuar en esta y atraer a más inversores.

[189] *Vid.,* el auto del Tribunal Supremo (Sala de lo Penal, Sección1ª) Auto de 3 junio 2021, [JUR 2021\198719] en el que un grupo criminal desarrolló un negocio en el que se ofrecían elevados beneficios a través de la inversión en bitcoins, entregando a las víctimas una pequeña cantidad de capital como prueba de estos beneficios y

En cuanto al papel de las criptomonedas como sistema de pago se han estudiado dos formas de utilizarlas. La primera y la más conocida es su utilización como sistema de pago en los negocios ilegales ubicados en la *Darknet.* Por un lado, para la compra de diversos productos como drogas[190] o billetes falsos[191] o en el pago de servicios ilegales[192]. Por otro lado, para la compra de herramientas o productos que permitan el desarrollo de actividades delictivas posteriores, por ejemplo, la compra de tarjetas robadas[193] o los materiales necesarios para llevar a cabo la falsificación de billetes[194]. También se ha visto la utilización de Bitcoin como sistema de pago para acceder a material pornográfico infantil de la *Darknet* [195].

Si se ponen en relación los delitos que tratan las resoluciones judiciales con los roles de las criptomonedas se obtienen los siguientes resultados (Tabla 7). Las criptomonedas son empleadas con el propósito de ocultar el rastro ilícito en una mayoría de delitos contra el patrimonio y contra el orden socioeconómico (n=31), seguidos de los delitos contra la Administración pública (n=4). La utilización de las monedas virtuales con la intención de atraer a potenciales víctimas y obtener beneficio económico se lleva a cabo fundamentalmente en delitos contra el patrimonio y contra el orden socioeconómico (n=12). La utilización como sistema de pago queda reservada para delitos contra la seguridad colectiva (n=3) y delitos contra el patrimonio.

conseguir la captación de más víctimas. Finalmente, se comunicaba la supuesta pérdida de la inversión, siendo imposible para la víctima la retirada del dinero invertido y el supuesto beneficio generado.

[190] *Vid.,* sentencia del TSJ Islas Canarias, Las Palmas (Sala de lo Civil y Penal, Sección 1ª) 39/2018 de 28 septiembre, [JUR 2018\312883]; la sentencia de la AP Santa Cruz de Tenerife (Sección 2ª) 29/2018 de 29 enero, [JUR 2018\204653] y AP Santa Cruz de Tenerife (Sección 2ª) 294/2018 de 3 octubre, [JUR 2019\51117]. Los acusados constituían una organización criminal que compraba droga en la *Darknet* utilizando criptomonedas y una vez la recibía en sus domicilios la distribuía y vendía por la isla de Tenerife.

[191] *Vid.,* la sentencia de la AP de Zaragoza (Sección 6ª) 188/2021 de 11 de mayo, [JUR/2021/185786], en la que el acusado adquiere 12 billetes falsos por 20 euros cada uno a través de la *Darknet* en la que emplea como sistema de pago el Bitcoin. También la sentencia de la AP de Madrid (Sección 3ª) 388/2020 de 7 de octubre, [JUR\ 2020\ 367249], en la que se adquieren 50 billetes falsos de 10 euros pagando con bitcoins.

[192] *Vid.,* la sentencia de la AP de Málaga (Sección 3ª), núm.189/2021 de 12 de mayo [JUR 2021\335126], en la que el autor utilizaba la criptomoneda Bitcoin como sistema de pago en una página web de la Darknet dedicada a la visualización y descarga de pornografía infantil.

[193] *Vid.,* la sentencia de la AP Lleida (Sección 1ª) 308/2017 de 14 julio, [ARP 2017\1322], sobre la compra de tarjetas comprometidas, robadas o clonadas y la posterior utilización para obtener dinero en efectivo y comprar criptomonedas.

[194] *Vid.,* la sentencia de la AP de Zaragoza (Sección 3ª) 84/2019 de 21 febrero, [JUR\2019\338758] en la que una organización criminal se dedicaba a la fabricación de billetes de 50 euros y a su puesta en circulación.

[195] *Vid*.; la sentencia de la AP de Málaga (Sección 3ª), núm.189/2021 de 12 de mayo [JUR 2021\335126]

Tabla 7.

Delitos según rol de las criptomonedas.

	Rol criptomoneda							
Delito título	Parte del ataque	Atracción, lucro y ocultación del rastro ilícito	Lucro y ocultación del rastro ilícito	Lucro	Sistema de pago	Atracción de la víctima y lucro	Ocultación del rastro ilícito	**Total**
Delitos contra el patrimonio y contra el orden socioeconómico	1	2	3	4	2	12	31	**55**
Delitos contra el patrimonio y contra el orden socioeconómico. Delitos contra la hacienda pública y contra la seguridad social.				1				**1**
Delitos contra el patrimonio y contra el orden socioeconómico. Delitos contra la seguridad colectiva.					2		1	**3**
Delitos contra la Administración pública							4	**4**
Delitos contra la libertad e indemnidad sexuales					1			**1**
Delitos contra la seguridad colectiva					3		1	**4**
Delitos de homicidio y sus formas					1			**1**
Delitos de las falsedades					1			**1**
Total	**1**	**2**	**3**	**5**	**10**	**12**	**37**	**70**

Fuente: Elaboración propia a partir de los resultados obtenidos en la búsqueda realizada con la base de datos jurídica Aranzadi.

Tipo de Criptomoneda Implicada en la Actividad Delictiva.

En cuanto al tipo de criptomoneda utilizado en los delitos es mayoritario el empleo del Bitcoin (n=48) (Tabla 8). Solo se han encontrado dos resoluciones en las que se han empleado otras criptomonedas, como son Ethereum[196] y Litecoin[197]. Esta última, es empleada al mismo tiempo que Bitcoin. También se han obtenido algunas resoluciones en las que se habla de criptomonedas de una forma general y no se especifica el tipo de criptomoneda empleada. No obstante, la cantidad de resoluciones judiciales en la que sucede esto es mucho menor que aquellas en las que se utiliza el Bitcoin (n=19). De esta forma, en el supuesto caso de que se tratara en realidad de otra criptomoneda, esta no superaría la cantidad de resoluciones en las que se ha utilizado la criptomoneda Bitcoin.

Tabla 8.

Tipo de criptomoneda implicada en el delito.

Tipo de criptomoneda	Total
Bitcoin y Litecoin	1
Ethereum	1
Otra (falsa)	1
No se dice	19
Bitcoin	48
Total	70

Fuente: Elaboración propia a partir de los resultados obtenidos en la búsqueda realizada con la base de datos jurídica Aranzadi.

En relación con el tipo de delito en el que está involucrado cada tipo de criptomoneda, el Bitcoin se utiliza mayoritariamente en delitos contra el patrimonio y contra el orden socioeconómico (Tabla 9). De igual formas, las criptomonedas Ethereum y Litecoin también se utilizan en este tipo de delitos, pero en la última se desarrolla en conjunto con un delito contra la hacienda pública y contra la seguridad social (Tabla 9).

[196] *Vid.,* el auto de la AN (Sala de lo Penal, Sección 4ª) núm. 488/2021 de 8 de septiembre [JUR 2021/307100]
[197] *Vid.,* el auto de la AP de Barcelona (Sección 6ª) núm. 631/2021 de 17 septiembre [JUR 2022/10473]

Tabla 9.

Tipo de criptomoneda según el tipo de delito según el título del CP.

Delito título	Bitcoin	Bitcoin y Litecoin	Ethereum	No se dice	Otra (falsa)	Total
Delitos contra el patrimonio y contra el orden socioeconómico. Delitos contra la hacienda pública y contra la seguridad social.		1				**1**
Delitos contra la libertad e indemnidad sexuales	1					**1**
Delitos de homicidio y sus formas	1					**1**
Delitos de las falsedades	1					**1**
Delitos contra el patrimonio y contra el orden socioeconómico. Delitos contra la seguridad colectiva.	2			1		**3**
Delitos contra la Administración pública	3			1		**4**
Delitos contra la seguridad colectiva	4					**4**
Delitos contra el patrimonio y contra el orden socioeconómico	36		1	17	1	**55**
Total	**48**	**1**	**1**	**19**	**1**	**70**

Fuente: Elaboración propia a partir de los resultados obtenidos en la búsqueda realizada con la base de datos jurídica Aranzadi.

Si se relacionan estos resultados con la motivación para emplear las criptomonedas (Tabla 10) se ha obtenido una mayoría de resoluciones en las que se ha empleado la criptomoneda Bitcoin con la intención de ocultar el rastro del dinero ilegalmente obtenido (n=25). En segundo lugar, se obtienen aquellas resoluciones en las que no se menciona el tipo de moneda empleada, pero en las que también existe una motivación de blanqueo del dinero (n=12). Son puntuales los resultados en los que se han encontrado otras criptomonedas como Litecoin (n=1) y Ethereum (n=1), ambas utilizadas en casos en los que se tenía la intención de atraer a potenciales víctimas y lucrarse. En tercer lugar, se sitúa la motivación de la atracción de la víctima y lucro, siendo mayoritaria para aquellas resoluciones en las que se ha empleado la criptomoneda Bitcoin (n=6) o que no se especifica el tipo de criptomoneda empleada (n=4). Por último, es de interés el hecho de que el caso en el que el autor utiliza una criptomoneda falsa presenta una motivación de atracción a la víctima y lucro (n=1).

Tabla 10.

Tipo de criptomoneda según la motivación del autor.

Rol criptomoneda	Tipo criptomoneda					
	Bitcoin	Bitcoin y Litecoin	Ethereum	No se dice	Otra (falsa)	**Total**
Parte del ataque	1					**1**
Atracción, lucro y ocultación del rastro ilícito	1			1		**2**
Lucro y ocultación del rastro ilícito	2			1		**3**
Lucro	4	1				**5**
Sistema de pago	9			1		**10**
Atracción y lucro	6		1	4	1	**12**
Ocultación del rastro ilícito	25			12		**37**
Total	**48**	**1**	**1**	**19**	**1**	**70**

Fuente: Elaboración propia a partir de los resultados obtenidos en la búsqueda realizada con la base de datos jurídica Aranzadi.

Victimario Implicado en la Actividad Delictiva.

Para el estudio de las víctimas se han establecido varias categorías atendiendo a si la víctima fue una sola persona, un grupo de personas o una empresa. También se han establecido dos categorías adicionales en las que se incluyen, por un lado, aquellos casos en los que no hay víctima directa de la utilización de criptomonedas. Por otro lado, aquellos en los que, aunque se menciona expresamente la intención de utilizar las criptomonedas en el delito, finalmente no se utilizan.

De los resultados obtenidos, en la tabla 11 se puede ver que la mayoría de las víctimas lo han sido de forma individual (n=25), seguidas de aquellos casos en los que no hay una víctima directa (n=19) y de los casos en los que las víctimas son múltiples (n=17).

Tabla 11.

Tipo de víctima implicada en el delito.

Víctima	Total
No se utiliza	**4**
Empresa	**5**
Múltiple	**17**
No hay víctima	**19**
Individual	**25**
Total	**70**

Fuente: Elaboración propia a partir de los resultados obtenidos en la búsqueda realizada con la base de datos jurídica Aranzadi.

Si se pone en relación con el tipo de delito (Tabla 12), se obtiene que la mayoría de las víctimas lo han sido individualmente por un delito contra el patrimonio y contra el orden socioeconómico (n=25). De igual forma sucede para aquellas víctimas múltiples (n=15).

Para el caso de la victimización de empresas, la totalidad de las empresas que han sido víctima de un delito de este tipo lo han sido en el desarrollo de un delito contra el patrimonio y contra el orden socioeconómico (n=5).

Tabla 12.

Tipo de víctima implicada según el tipo de delito.

	Víctima					
Delito título	No se utiliza	Empresa	Múltiple	No hay víctima	Individual	**Total**
Delitos contra el patrimonio y contra el orden socioeconómico. Delitos contra la hacienda pública y contra la seguridad social			1			**1**
Delitos contra la libertad e indemnidad sexuales			1			**1**
Delitos de homicidio y sus formas				1		**1**
Delitos de las falsedades				1		**1**
Delitos contra el patrimonio y contra el orden socioeconómico. Delitos contra la seguridad colectiva.				3		**3**
Delitos contra la Administración pública	4					**4**
Delitos contra la seguridad colectiva				4		**4**
Delitos contra el patrimonio y contra el orden socioeconómico		5	15	10	25	**55**
Total	**4**	**5**	**17**	**19**	**25**	**70**

Fuente: Elaboración propia a partir de los resultados obtenidos en la búsqueda realizada con la base de datos jurídica Aranzadi.

Si se estudian en detalle los delitos contra el patrimonio y contra el orden socioeconómico (Tabla 13) se obtiene que la mayoría de las personas son víctimas de delitos de estafa individualmente (n=21), seguidos de aquellos casos en los que la víctima es múltiple (n=9). En segundo lugar, se sitúan los delitos de recepción y blanqueo de capitales para los que no hay víctima directa (n=6).

Tabla 13. *Tipo de víctima implicada según los delitos contra el patrimonio y contra el orden socioeconómico.*

	Tipo de víctima				
Delito capítulo	Empresa	No hay	Múltiple	Individual	Total
De la receptación y el blanqueo de capitales. Delito contra la salud pública.		1			1
De las defraudaciones (delito de estafa). De la receptación y el blanqueo de capitales			1		1
De las defraudaciones: De las defraudaciones de fluido eléctrico y análogas	1				1
De las defraudaciones: Delito de estafa, delito de administración desleal y delito de apropiación indebida. Delitos contra la hacienda pública y contra la seguridad social. Delito de receptación y blanqueo de capitales.			1		1
De las defraudaciones: Delito de estafa, delito de apropiación indebida. De las falsedades: De las falsedades documentales.			1		1
De las defraudaciones: delito de estafa. De la receptación y el blanqueo de capitales. Delito de descubrimiento y revelación de secretos. Delito contra la propiedad industrial.			1		1
De las defraudaciones: Delito de estafa. De las falsedades documentales. De la receptación y el blanqueo de capitales.			1		1
De las defraudaciones: Delito de estafa. Delito de receptación y blanqueo de capitales			1		1
Delito de daños informáticos. Delito de las defraudaciones: de fluido eléctrico y análogas.		1			1
Delitos de los daños: Delito de daños informáticos	1				1
Delito de falsificación de moneda y efectos timbrados. Delito contra la salud pública.		2			2
De las defraudaciones: Delito de apropiación indebida			1	2	3
De las defraudaciones: Delito de estafa y delito de apropiación indebida	2			2	4
Delito de receptación y blanqueo de capitales		6			6
De las defraudaciones: Delito de estafa	1	3	9	21	34
Total	**5**	**13**	**16**	**25**	**59**

Fuente: Elaboración propia a partir de los resultados obtenidos en la búsqueda realizada con la base de datos jurídica Aranzadi.

Autor Responsable de los Hechos: Individual o Grupal.

Los resultados obtenidos para el tipo de autor involucrado se han agrupado en tres categorías: empresa, grupo e individual. La primera hace referencia a aquellos casos en los que la actividad delictiva ha sido desempeñada por una empresa u otra entidad similar. El segundo se refiere a aquellos casos cuyo autor es parte de un grupo u organización criminal en la que utilizan criptomonedas como parte del desarrollo efectivo de algún delito. Por último, la categoría individual hace referencia a aquellos casos en los que el autor del delito ha actuado de forma individual o, al menos, no se conoce de su colaboración con otras personas para la comisión efectiva del delito. En la elaboración de las categorías se consideró importante realizar una distinción entre la categoría individual y la categoría empresa debido a que en el estudio y análisis de los casos se encontraron elementos característicos propios de los delitos cometidos por empresas que debían ser tenidos en cuenta.

Los resultados obtenidos muestran que prevalecen las resoluciones judiciales en las que la actividad delictiva ha sido realizada como parte de la criminalidad desarrollada por un grupo u organización criminal (n=31) (Tabla 14). Aunque la diferencia no es muy elevada con respecto a aquellas en las que el autor ha actuado de forma individual, estando la diferencia únicamente en un resultado (n=30). Por último, se sitúan los resultados en los que se ha visto involucrada una empresa u otra entidad similar (n=9).

Tabla 14.

*Tipo de autor implicado en los hechos delictivos***.**

Tipo de autor	Total
Empresa	9
Individual	30
Grupo	31
Total	**70**

Fuente: Elaboración propia a partir de los resultados obtenidos en la búsqueda realizada con la base de datos jurídica Aranzadi.

Según el tipo de delito que se trata en la resolución (título y capítulo), se han obtenido los resultados recogidos en la Tabla 15. En relación con los delitos contra el patrimonio y contra el orden socioeconómico, predomina la autoría individual con respecto a las otras categorías (n=26). Presentan una mayoría de delitos de estafa (n=18), seguidos de los delitos de receptación y blanqueo de capitales (n=2), delitos de apropiación indebida (n=2), delitos de estafa junto con delitos de apropiación indebida (n=2) y, por último, delitos de daños informáticos (n=1) y delitos de las defraudaciones de fluido eléctrico y análogas (n=1).

En cuanto a la autoría grupal, hay que señalar que reúne la totalidad de los delitos contra la Administración pública (n=4) con delitos como tráfico de influencias, malversación de caudales públicos y prevaricación. De igual manera sucede con los delitos contra la seguridad colectiva (n=4) relativos a la salud pública (tráfico de drogas).

Es necesario señalar que, salvo una resolución, la totalidad de los delitos cometidos por empresas pertenecen a la categoría de los delitos contra el patrimonio y contra el orden socioeconómico (n=8), es específico se refiere a delitos de estafa y de apropiación indebida.

Tabla 15.

Tipo de autor según tipo de delito según título y capítulo en el CP.

Delito título	Delito capítulo	Autor			
		Empresa	**Grupo**	**Individual**	**Total**
Delitos contra el patrimonio y contra el orden socioeconómico	De las defraudaciones: Delito de estafa	6	10	18	34
	Delito de receptación y blanqueo de capitales		4	2	6
	De las defraudaciones: Delito de estafa y delito de apropiación indebida	2		2	4
	De las defraudaciones: Delito de apropiación indebida		1	2	3
	Delitos de los daños: Delito de daños informáticos			1	1
	Delito de daños informáticos. Delito de las defraudaciones: de fluidos eléctricos y análogos.		1		1
	De las defraudaciones: Delito de estafa. Delito de receptación y blanqueo de capitales		1		1
	De las defraudaciones: Delito de estafa. De las falsedades documentales. De la receptación y el blanqueo de capitales.		1		1
	De las defraudaciones: delito de estafa. De la receptación y el blanqueo de capitales. Delito de descubrimiento y revelación de secretos. Delito contra la propiedad industrial.		1		1
	De las defraudaciones: Delito de estafa, delito de apropiación indebida. De las falsedades: De las falsedades documentales.		1		1
	De las defraudaciones: De las defraudaciones de fluido eléctrico y análogas			1	1
	De las defraudaciones (delito de estafa). De la receptación y el blanqueo de capitales		1		1
	Total	**8**	**21**	**26**	**55**
Delitos contra el patrimonio y contra el orden socioeconómico. Delitos contra la hacienda pública y contra la seguridad social.	De las defraudaciones: Delito de estafa, delito de administración desleal y delito de apropiación indebida. Delitos contra la hacienda pública y contra la seguridad social. Delito de receptación y blanqueo de capitales.	1			1
	Total	**1**			**1**
Delitos contra el patrimonio y contra el orden socioeconómico. Delitos contra la seguridad colectiva.	Delito de falsificación de moneda y efectos timbrados. Delito contra la salud pública.			2	2
	De la receptación y el blanqueo de capitales. Delito contra la salud pública.		1		1
	Total		**1**	**2**	**3**

Delitos contra la Administración pública	Delito de tráfico de influencias. Delito de malversación. Delito de prevaricación de los funcionarios públicos y otros comportamientos injustos. Delito de las negociaciones y actividades prohibidas a los funcionarios públicos y de los abusos en el ejercicio de su función.		2		2
	Delito de tráfico de influencias y delito de malversación		1		1
	Delito de malversación de caudales públicos		1		1
	Total		**4**		**4**
Delitos contra la libertad e indemnidad sexuales	Delitos relativos a la prostitución y a la explotación sexual y corrupción de menores.			1	1
	Total			**1**	**1**
Delitos contra la seguridad colectiva	Delito contra la salud pública. Tráfico de drogas		4		4
	Total		**4**		**4**
Delitos de homicidio y sus formas	Delitos de homicidio y sus formas			1	1
	Total			**1**	**1**
Delitos de las falsedades	Delito de falsificación de moneda y efectos timbrados		1		1
	Total		**1**		**1**
	Total	**9**	**31**	**30**	**70**

Fuente: Elaboración propia a partir de los resultados obtenidos en la búsqueda realizada con la base de datos jurídica Aranzadi.

Si se relacionan el tipo de autor con el rol de la criptomoneda empleada (Tabla 16), se obtiene una mayoría de grupos criminales que han utilizado esta tecnología con la intención de ocultar el rastro ilícito del dinero (n=19). Muy próximos a estos se sitúan también los casos en los que, con la misma motivación, la autoría es individual (n=18). Los roles que desempeñan las criptomonedas cuando el autor del delito es una empresa son el lucro y su utilización para atraer a potenciales víctimas (n=9).

Tabla 16.

Tipo de autor según el rol de la criptomoneda.

	Tipo de autoría			
Rol de la criptomoneda	Empresa	Grupo	Individual	Total
Parte del ataque sin ánimo de lucro			1	1
Atracción de la víctima, lucro y ocultación del rastro ilícito del dinero		2		2
Lucro y ocultar rastro ilícito del dinero			3	3
Lucro	4		1	5
Sistema de pago		5	5	10
Atracción de la víctima y lucro	5	5	2	12
Ocultar el rastro ilícito del dinero		19	18	37
Total	**9**	**31**	**30**	**70**

Fuente: Elaboración propia a partir de los resultados obtenidos en la búsqueda realizada con la base de datos jurídica Aranzadi.

Discusión

Criminalidad Técnicamente Especializada (H1)

Si se atiende al tipo de delito cometido, los resultados obtenidos no se corresponderían con las consideraciones generales que se tienen sobre la tecnología *Blockchain* y las criptomonedas. Habitualmente, se asume que este tipo de tecnologías requieren de una elevada capacidad técnica para su utilización. Esto es debido en parte a su relativa novedad y a la escasa familiarización de la población general con su utilización. Por ello, se pensaría que la delincuencia en la que intervienen las criptomonedas se corresponde con un tipo de delincuencia no convencional que requiere de cierta especialización criminal y no podría ser desarrollada por cualquier persona motivada para ello. Su utilización quedaría reservada para aquellas personas altamente formadas en el manejo de las nuevas tecnologías.

Sin embargo, los resultados obtenidos para el marco español muestran que el tipo de delito predominante son los delitos contra el patrimonio y contra el orden socioeconómico, en especial el delito de estafa. Este tipo de delito es considerado de carácter

tradicional, que no requiere necesariamente de la utilización de tecnologías para su comisión. Esto coincidiría con los resultados obtenidos en los que en su mayoría las criptomonedas no realizan el papel principal como son las falsas ventas de productos a través de aplicaciones de compraventa. En estos la criptomoneda es una forma que utiliza el vendedor para eliminar el rastro de ilegalidad del dinero obtenido.

De esta forma, se cuenta con un autor que siendo consciente de la capacidad de las criptomonedas para la ocultación del rastro criminal ha incorporado este elemento en el desarrollo de su actividad delictiva para evadir su detección. Este último paso en el desarrollo del delito podría llevarse a cabo empleando otros métodos que permitan la ocultación de la actividad criminal, sin que fuera imprescindible la utilización de criptomonedas. No es necesario que el autor disponga de los conocimientos necesarios para la utilización de las criptomonedas ni para su compraventa, delegando esta tarea en un tercero especializado.

En el caso del resto de delitos que no pertenecen al título de los delitos contra el patrimonio y contra el orden socioeconómico se puede observar una situación diferente. La mayoría de estos delitos consisten en la utilización de criptomonedas para la compra de drogas a través de la *Darknet*. Esta actividad criminal requiere de una mayor especialización que la criminalidad mencionada anteriormente ya que requiere de conocimientos especializados relativos a la compraventa de criptomonedas (en especial Bitcoin) y a la utilización de la *Darknet* para la compra de productos y servicios ilegales.

No obstante, estos últimos casos constituyen una pequeña cantidad en comparación con la tipología delictiva anterior. De esta forma, no se podría considerar la hipótesis 1 que expone que la delincuencia cometida con criptomonedas en este caso presente una elevada complejidad técnica relacionada con el funcionamiento de las criptomonedas. El delito de estafa es considerado como un delito de carácter tradicional, para el que en estos casos se ha introducido un elemento tecnológico. No obstante, este no sería imprescindible, por lo que la supresión de la criptomoneda en estos casos no impediría que se finalizara la comisión del delito de estafa empleando otros métodos más tradicionales.

Utilización de las Criptomonedas Como Sistema de Pago (H2)

De los diversos roles de las criptomonedas que se han detectado, la ocultación del rastro ilícito ha sido el más frecuente. La compra de criptomonedas con este fin ha supuesto el último paso en el desarrollo de un delito que es muy diverso y que en ocasiones no ha llegado a llevarse a cabo.

En segundo lugar, se sitúa la motivación de lucro y obtención de beneficio económico. Esta motivación se basa en el elevado valor que ha adquirido en los últimos años la criptomoneda Bitcoin[198]. Se han convertido en un el objetivo de muchos criminales que buscan apropiarse de ellas indebidamente de forma directa o a través de falsos negocios creados para tal fin[199]. De forma general, la víctima podía enviar dinero fiduciario con el propósito de invertirlo en criptomonedas o por otro lado podía enviar sus criptomonedas al autor para obtener un mayor beneficio. La razón de ser de esta motivación es que una vez el dinero ha sido invertido en criptomonedas o se han enviado al autor, es compleja su persecución y devolución, lo que aumenta el interés por su obtención. Por último, en cuanto al rol de sistema de pago ha sido uno de los usos de esta tecnología más conocidos y tratados en la literatura. Sin embargo, si se observan los resultados obtenidos, aunque los casos para sistema de pago son muy similares a los de ocultación de la actividad criminal, lo cierto es que el primero queda por debajo del segundo. Se han obtenido una elevada cantidad de casos de estafas relacionadas con falsas compras de productos, falsos negocios de inversión y estafas piramidales. De esta forma, se puede decir que no se acepta la H2 ya que la moneda virtual no constituye únicamente un medio de pago, dejando a un lado la opinión que se tiene en muchos círculos que la etiquetan como "dinero criminal", siendo más notoria su utilización en casos de lavado de dinero y de lucro a través de la actividad de inversión.

Tipo De Criptomoneda Utilizada (H3)

La utilización de las criptomonedas en la criminalidad podría sugerir un mayor uso de criptomonedas privadas para conseguir ocultar la actividad criminal. Este tipo de criptomonedas debido a su diseño garantizan el desarrollo de la actividad delictiva de forma más privada que el resto de las criptomonedas como Bitcoin. Sin embargo, si se observan los resultados obtenidos, se puede ver que hay una mayoría de casos en los que se ha utilizado la criptomoneda Bitcoin, que permite consultar su actividad de forma pública. De esta forma, no se puede admitir la tercera hipótesis (H3) ya que no se da una mayor utilización de

[198] Las criptomonedas tienen como características que tienen una enorme volatilidad, siendo su inversión atractiva para aquellas personas que buscan generar beneficios económicos. Como ejemplo, el 22 de febrero de 2022 una unidad de Bitcoin tiene un valor de 32,860 euros. Recuperado de https://coinmarketcap.com/es/currencies/bitcoin/

[199] Como caso aislado, se ha estudiado también una resolución judicial en la que el autor se estaba lucrando a través de la actividad ilegal de minería de criptomonedas debido a que el desarrollo de la misma se realizaba en la empresa en la que trabajaba, la cual no tenía conocimiento de la actividad (SAP de Málaga (Sección 2ª) 373/2019 de 25 octubre, [JUR 2020\118664]).

criptomonedas de carácter privado[200].

Identificación de las Víctimas en los Delitos Con Criptomonedas (H4)

En cuanto a la victimización, predominan las víctimas de carácter individual para delitos contra el patrimonio y contra el orden socioeconómico. Se trata en su mayoría de delitos de estafa en los que las víctimas desconocían los riesgos asociados a la utilización de las criptomonedas, en especial en actividades de inversión. Esto sugiere que se trataría de un tipo de delincuencia que podría evitarse mediante la elaboración de estrategias preventivas con potenciales víctimas dirigiendo los esfuerzos hacia aquellas personas interesadas en la compraventa e inversión de criptomonedas. Sin embargo, para garantizar el éxito de estos planes es necesaria la identificación de la potencial víctima. Esta tarea no es sencilla y es que existen una serie de dificultades por las que resulta compleja o inviable la identificación de las personas afectadas.

Si se atiende a la definición de "víctima" que se recoge en el artículo 2 del Estatuto de la víctima del delito (Ley 4/2015, de 27 de abril, del Estatuto de la víctima del delito), una víctima directa sería "toda persona física que haya sufrido un daño o perjuicio sobre su propia persona o patrimonio, en especial lesiones físicas o psíquicas, daños emocionales o perjuicios económicos directamente causados por la comisión de un delito" (p.9). Por lo tanto, si se consideran los tres roles mencionados anteriormente –lucro, ocultación del rastro ilegal y sistema de pago– se puede ver que la determinación de la víctima no es igual de compleja para todos ellos. En los casos en los que la criptomoneda se utiliza como sistema de pago, no se encontraría una víctima directa afectada, no hay una persona física que haya sufrido el daño o perjuicio ocasionado, sino que se hablaría en todo caso de una víctima indirecta. De igual forma sucedería en aquellos casos en los que la moneda virtual se emplea para la ocultación del rastro del delito. Lo que se pretende impedir o dificultar en este caso es la persecución de la actividad delictiva, por lo que no se encuentra tampoco una víctima directa, sino que podría hablarse de una víctima difusa o indirecta que podría ser el Estado.

No obstante, en el caso de la utilización de la criptomoneda para lucro personal, se puede identificar como víctima a todas aquellas personas que destinaron su dinero para la realización de las diferentes actividades de inversión. Debido a que la gran mayoría de los delitos conocidos del estudio de la jurisprudencia penal española se corresponden con delitos

[200] En este sentido habría que tener precaución en relación con las limitaciones de investigación de las criptomonedas de carácter más privado. Esto es, puede que esta característica sea a su vez la que dificulta la denuncia de actividades delictivas en las que se han visto implicadas estas monedas virtuales.

contra el patrimonio y contra el orden socioeconómico, en específico delitos de estafa, sería interesante en este sentido considerar los elementos de esta tipología delictiva como son el ánimo de lucro y el "engaño bastante"[201].

Aunque el delito de estafa es considerado como un delito de carácter tradicional (Miró-Llinares, 2012), la inclusión de las criptomonedas en su desarrollo ha potenciado su efectividad en cuanto a la obtención del lucro y a la consecución del considerado como "engaño bastante". El primero es debido a la capacidad que tienen para dificultar la identificación de los autores y la persecución de la actividad criminal, lo que facilita la obtención de los elevados beneficios de su apropiación indebida. El segundo a causa de que es presentado como un atractivo reclamo para potenciales víctimas, que siendo poco conocedoras de los riesgos de la actividad de inversión acceden a participar de la proposición. Esto es, el autor del delito, valiéndose del desconocimiento generalizado sobre el funcionamiento de las criptomonedas y los riesgos asociados, propone la actividad de inversión asegurando una elevada rentabilidad que atraería a la potencial víctima. En la mayoría de los casos se ha podido observar cómo la víctima incluso pudo facilitar el desarrollo del delito de forma exitosa.

Por todo ello, sería admitida de forma parcial la hipótesis 4, que sostiene que, debido a su mayor utilización como sistema de pago, las víctimas de delitos cometidos con criptomonedas tendrán un carácter difuso. La razón es que, su utilización no se reserva únicamente como sistema de pago, sino que también es un medio para ocultar el rastro criminal, donde se encuentra una víctima difusa o indirecta. Sin embargo, la mayoría de los casos delictivos estudiados en este sentido pertenecen a una actividad de inversión fraudulenta, por lo que la consideración de las víctimas de carácter difuso no incluiría a la gran mayoría de la muestra.

El Carácter Individual de los Delitos Con Criptomonedas (H5)

La utilización de las criptomonedas en los delitos ha estado habitualmente relacionada con su papel como sistema de pago. Esto ha llevado a pensar que la autoría de esta delincuencia tendría un carácter individual debido a que es el comprador el que de forma individual utiliza esta tecnología para obtener productos o servicios de un vendedor. Sin

[201] Según el tenor literal del artículo 248.1 del Código penal, se dice "Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno" Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. https://www.boe.es/buscar/pdf/1995/BOE-A-1995-25444-consolidado.pdf

embargo, en apartados anteriores se ha podido determinar que el rol frecuente de las criptomonedas no es el de sistema de pago, sino el de ocultación del rastro criminal. Esto cuestiona el tipo de autoría más frecuentemente implicado en estos delitos.

Los resultados para este apartado muestran que la autoría frecuente en los delitos cometidos con criptomonedas está formada por grupos criminales.

En su mayoría los delitos cometidos por estos grupos criminales son delitos contra el patrimonio y contra el orden socioeconómico, en especial, estafas y blanqueo de capitales. Este hecho coincide con los casos conocidos de estafas piramidales y grupos criminales de tráfico de drogas.

Se ha utilizado el término grupo criminal para hacer referencia de forma general a un grupo de personas que se ha determinado a partir del número de personas que se exponían en el contenido de las resoluciones judiciales. A partir de esta fuente de datos, no se puede conocer en detalle la continuidad de la actividad delictiva realizada como para determinar si se trata de una organización criminal. La mayoría de estos grupos han utilizado las criptomonedas con el propósito de ocultar el rastro ilícito del dinero. Esto coincide con el uso habitual que se le suele dar a las criptomonedas en estos casos para blanquear el dinero ilegalmente obtenido a través de otra de las actividades del grupo criminal (p.ej. el tráfico de drogas).

Por todo ello, no podría aceptarse la hipótesis 5 (H5) en la que se asumía una autoría individual en la utilización de las criptomonedas para el desarrollo de actividades delictivas.

Limitaciones del Segundo Experimento

Este experimento contribuye de forma empírica al estudio del panorama español de los delitos cometidos con criptomonedas. Sin embargo, también presenta una serie de limitaciones.

En relación con el estudio de la jurisprudencia penal, la primera limitación es que la utilización de esta fuente de información, aunque puede ofrecer una visión general sobre la criminalidad cometida en esta materia, no constituye la totalidad de todos los delitos cometidos con criptomonedas en España. Por ello, habría que tener precaución en la consideración de los resultados mostrados, ya que no podrían realizarse generalizaciones o rotundas afirmaciones sobre este tipo de criminalidad. Por otro lado, el contenido de las resoluciones judiciales en ocasiones está muy limitado en cuento a la información disponible sobre el desarrollo del delito. Sería necesario complementar la información obtenida con otras fuentes como informes de organismos oficiales o denuncias de víctimas. Por último, en

relación con el estudio de los casos delictivos hay que considerar que la muestra está formada por resoluciones judiciales y no por casos delictivos, lo que podría suponer que un mismo caso sea tratado en varias resoluciones judiciales al mismo tiempo. Esto dificulta el estudio cuantitativo y cualitativo de la delincuencia cometida con criptomonedas en España, así como la determinación de grupos criminales y el estudio de los patrones de victimización.

Capítulo 11. Estudio de las Denuncias de Víctimas Online de Delitos Con Criptomonedas (Experimento 3).

El objetivo del experimento consiste en estudiar espaciotemporalmente la victimización de los delitos cometidos con criptomonedas. La pregunta general de investigación es si este tipo de criminalidad se concentra en determinados lugares o períodos.

Método y Materiales

Estrategia de Investigación

La metodología de este experimento consiste en un análisis descriptivo de la victimización de los delitos cometidos con criptomonedas. Para ello, se dispone de datos obtenidos a través de "Bitcoin Abuse", un repositorio de carácter público creado en el año 2017[202] que permite a sus usuarios denunciar aquellos incidentes delictivos de los que han sido víctimas y en los que se ha utilizado la criptomoneda Bitcoin[203]. Se trata de un proyecto que surge de la necesidad de hacer públicas aquellas direcciones Bitcoin que utilizan los delincuentes para exigir el pago en bitcoins. De esta forma, dificultan a los delincuentes el gasto posterior de los delincuentes por un lado y, por el otro ayudan a los usuarios a identificar este tipo de engaños (Bitcoin Abuse, 2019).

Los datos recogidos en este repositorio han sido utilizados en investigaciones anteriores como Azani et al. (2020) para consultar direcciones Bitcoin relacionadas con la financiación de actividades terroristas; en Bambuch (2020), como una fuente de datos más para crear una plataforma que recoja y muestre información sobre direcciones criptográficas afectadas por ciberdelitos; en Oggier et al. (2020) para comprobar el origen delictivo y algunas características de algunas direcciones Bitcoin implicadas en el estudio de redes de transacciones Bitcoin de estafadores implicados en una campaña de sextorsión; en Wang et al. (2020) para obtener las etiquetas necesarias para la implementación de técnicas de *clustering* y en Xia et al. (2020) para comprobar el origen delictivo de dos direcciones Bitcoin (una de ellas "giveaway scam" y la otra de "COVID Blackmail scam") como parte del estudio de las estafas con temática COVID.

No obstante, la única investigación que se conoce hasta la fecha en la que se ha empleado esta base de datos para un propósito de carácter criminológico ha sido en la investigación de Buil-Gil y Saldaña-Taboada (2021) con el objetivo de estudiar la

[202] Los datos relativos a la creación de la página web se han consultado en el siguiente enlace https://whois.domaintools.com/bitcoinabuse.com
[203] Se puede acceder a la página web y al repositorio a través de este enlace https://www.bitcoinabuse.com/

concentración de delitos cibernéticos de esta categoría e identificar los grupos de delincuentes involucrados.

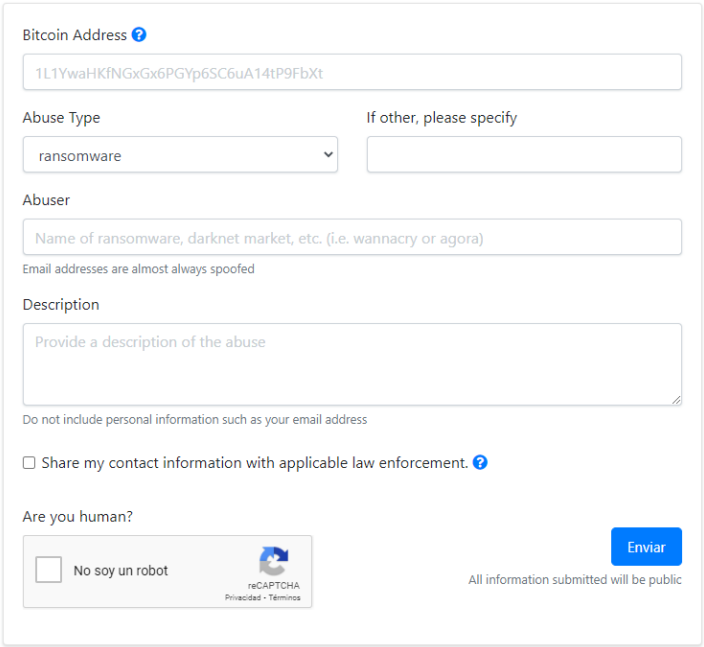
La investigación presente también utiliza los datos recogidos en el repositorio "Bitcoin Abuse" con fines criminológicos para el estudio de los patrones espaciotemporales de los delitos cometidos con criptomonedas que, al mismo tiempo, nos muestran hábitos de utilización de las criptomonedas por parte de los autores.

A través del formulario disponible en la página web los usuarios pueden registrar la dirección Bitcoin recibida, el tipo de delito, información sobre el autor y otra información adicional (Figura 3)[204]. Además de los datos registrados por la víctima, esta base de datos también ofrece información sobre el país de residencia y la hora de cada registro. La descarga de los datos se realizó empleando la API del sitio web[205].

A lo largo de la investigación, se utilizará el término "victimización" para hacer referencia a la frecuencia de denuncias que han sido interpuestas por los usuarios. De esta forma, cuando se hace referencia a la victimización según el país, se está refiriendo al número de denuncias registradas por los usuarios de "Bitcoin Abuse" según el país desde el que se realiza el registro.

Figura 3.

*Formulario de autodenuncia de la página web Bitcoin Abuse***.**



Fuente: Página web "Bitcoin Abuse".

[204] Se puede acceder al formulario de denuncia a través del siguiente enlace https://www.bitcoinabuse.com/reports/create

[205] La API permite la descarga de un archivo ".csv" en un periodo de tiempo seleccionado entre: un día, u mes o desde siempre. Toda la información está disponible en https://www.bitcoinabuse.com/api-docs

Una vez se disponía de la base de datos, se realizó un proceso de organización de los datos para prepararlos para el estudio posterior. Se adaptaron los datos pertenecientes a la fecha y hora a un formato estándar. También, la variable perteneciente a los delitos estaba estructurada conforme a una serie de códigos, de forma que cada número se correspondía con un tipo de delito. Por ello, se realizó la traducción de los códigos y se sustituyeron por el tipo de delito con el que se correspondían.

El estudio de los datos se realizó utilizando el *software* "Tableau", que permite gestionar y visualizar datos para obtener nuevo conocimiento. Se establecieron diversas relaciones entre los datos como el tipo de delito según el país desde el que se registró la denuncia o el tipo de delito según el día o la hora en la que se registraron las denuncias.

Descripción de la Muestra

Se dispone de una muestra de 219.672 denuncias que fueron registradas entre el 16 de mayo del año 2017 y el 15 de abril del año 2021. Las variables que se incluyen en la muestra son nueve[206]:

1. Dirección: conjunto de direcciones Bitcoin que adjunta el delincuente para recibir el dinero exigido.
2. Id_delito: tipo de delitos registrados. Se dispone de seis categorías: *ransomware, blackmail scam, sextorsión, Darknet market, bitcoin tumbler* y otro.
3. Id_delito_otros: cualquier otro tipo de información adicional que el usuario aporta sobre el ataque.
4. Infractor: información que el usuario dispone sobre el autor del delito. Puede ser una dirección de correo electrónico que aparece en el mensaje recibido, nombre del ransomware o mercado al que se hace alusión, etc.
5. Descripción: información sobre el mensaje recibido. En su mayoría los usuarios adjuntan la información idéntica recibida o realizan una descripción sobre el incidente.
6. País: lugar desde el que el usuario ha realizado la denuncia.
7. Id_país: código del país desde el que el usuario ha realizado la denuncia
8. Fecha: a la que el usuario ha registrado la denuncia (DD/MM/AAAA)
9. Hora: a la que el usuario ha registrado la denuncia (HH:MM)

[206] Se han traducido al español las variables que en la base de datos inicial se correspondían con: *address, abuse_type_id, abuse_type_other, abuser, description, from_country, from_country_code, created_at.*

En relación con la variable perteneciente al tipo de delito, en relación con el desarrollo de esta investigación será necesario explicar los elementos que caracterizan a cada delito. En este caso, se incluyen seis categorías que se corresponden con delitos que habitualmente se han visto relacionados con el uso de criptomonedas como Bitcoin:

- *Ransomware*: tipo de programa maligno o código malicioso que se ejecuta en forma de software y puede bloquear o encriptar el sistema o bien algunos documentos. A cambio de su liberación, el autor exige el pago de una determinada cantidad en dinero digital o en criptomonedas (especialmente Bitcoin) como en este caso. Esta categoría incluye registros en los que las víctimas han sido afectadas por este programa maligno descargado a través de correo electrónico o a través de la visita de páginas web que han bloqueado el sistema del usuario o encriptado sus documentos.
- *Blackmail scam*: consiste en que la víctima recibe un mensaje, generalmente vía correo electrónico en el que se asegura que se ha accedido a su sistema o ha sido hackeado. El autor del delito amenaza a la víctima con publicar información comprometedora de esta o detalles personales a menos que se pague la cantidad en bitcoins requerida. Se suele añadir algún dato real de la víctima para darle credibilidad a la amenaza.
- Sextorsión: es un tipo de extorsión de carácter sexual en la que la que el autor exige a la víctima el pago de alguna cantidad monetaria a cambio de no difundir material de contenido sexual de la víctima (imágenes, vídeos, texto, etc.). En esta categoría se incluyen casos en los que el extorsionador asegura tener información comprometedora de carácter sexual de la víctima y pide el pago de una cantidad en Bitcoin.
- Mercado de la *Darknet*: se refiere a mercados online de la Darknet en los que se puede comprar productos ilegales (mayormente drogas, pero también armas de fuego, *malware,* tarjetas de crédito robadas y otros) o pagar por servicios ilegales usando criptomonedas como Bitcoin y Monero. En estos datos, los registros hacen referencia especialmente a fraudes cometidos por vendedores de la Darknet que no entregaron el producto o servicio por el que había pagado la víctima. Algunos registros también hacen referencia a mercados de la Darknet que ofrecen servicios ilegales y cuentas de Bitcoin con enlaces a productos ilegales anunciados en los mercados de la Darknet.
- *Bitcoin tumblers*: son servicios que mezclan bitcoins que son potencialmente identificables para oscurecer la ruta que ha seguido desde su fuente original, que de otra forma sería públicamente accesible desde *Blockchain*. En la muestra de la que se

dispone, en esta categoría se incluyen aquellos servicios de mezcladores de criptomonedas que resultaron ser fraudulentos.

- Otros: recoge aquellos incidentes relacionados con Bitcoin que los usuarios no han clasificado en ninguna de las categorías anteriores.

Resultados

Los resultados se dividen en cuatro grupos según la variable para la que se haya estudiado la victimización por este tipo de delitos: 1) Victimización según el tipo de delito denunciado: 2) Victimización según el país desde el que se denuncia; 3) Victimización según el país y el tipo de delito y 4) Victimización en el tiempo.

A continuación, se presentan de forma detallada los resultados obtenidos en relación con las diferentes variables:

Victimización Según el Tipo ee Delito Denunciado

Una vez obtenidos los resultados, se dispone de una muestra de un total de 219.672 delitos denunciados en los que han intervenido las criptomonedas de alguna forma. De estos delitos, el tipo más denunciado ha sido el de *Blackmail scam* o extorsión (N=86.532), seguido de los delitos de sextorsión (N=68.002) y de los ataques *ransomware* (N=48.256), mientras que la proporción de denuncias para los mezcladores de Bitcoin (N=3.875) y los mercados de la *Darknet* (N=1.447) fueron mucho menores (Tabla 17).

Tabla 17.

Tipo de delitos en la base de datos Bitcoin Abuse.

Tipo de delito	Frecuencia	Porcentaje
Blackmail scam	86.532	39%
Sextorsión	68.002	31%
Ransomware	48.256	22%
Otros	11.560	5%
Bitcoin tumbler	3.875	2%
Mercados de la Darknet	1.447	1%
Total	**219.672**	**100%**

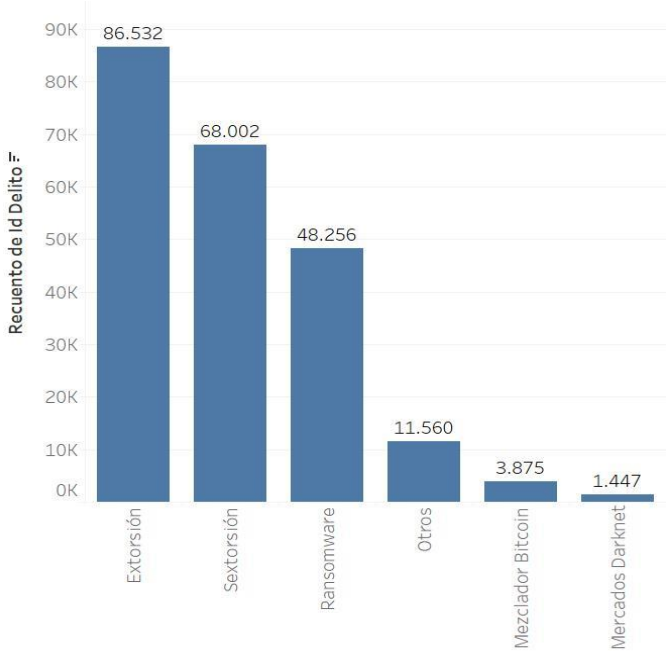
Fuente: Elaboración propia a partir de los datos obtenidos en el repositorio Bitcoin Abuse.

Al representar estos resultados a través de un gráfico de barras (Figura 4), se aprecia que no existen diferencias importantes entre el número de registros para los delitos de

extorsión, sextorsión y *ransomware*. Sin embargo, sí se aprecia una diferencia significativa con respecto a los delitos de mezcladores BTC y de los mercados de la *Darknet* (Figura 4).

Figura 4.

Victimización según el tipo de delito.



Fuente: Elaboración propia a partir de los datos obtenidos en el repositorio Bitcoin Abuse.

Victimización Según el País Desde el que se Denuncia

Se dispone de un total de 203 países desde los que los usuarios de la página Bitcoin Abuse han registrado una denuncia. De los 10 países con más registros, más del 40% de los delitos fueron denunciados por usuarios que residían en Estados Unidos (n= 57.161), seguidos de los residentes de Reino Unido, Canadá, Alemania, Francia que también presentan un elevado número de registros (Tabla 18). Estos países suponen el 62,23% del total de denuncias realizadas por países, lo que supone que más de la mitad de las denuncias están realizadas por los diez países que se recogen en la tabla. En la posición número 11 después de Japón se encontraría España con 4.230 denuncias en total.

Tabla 18.

Los 10 países con más denuncias según la residencia de la víctima.

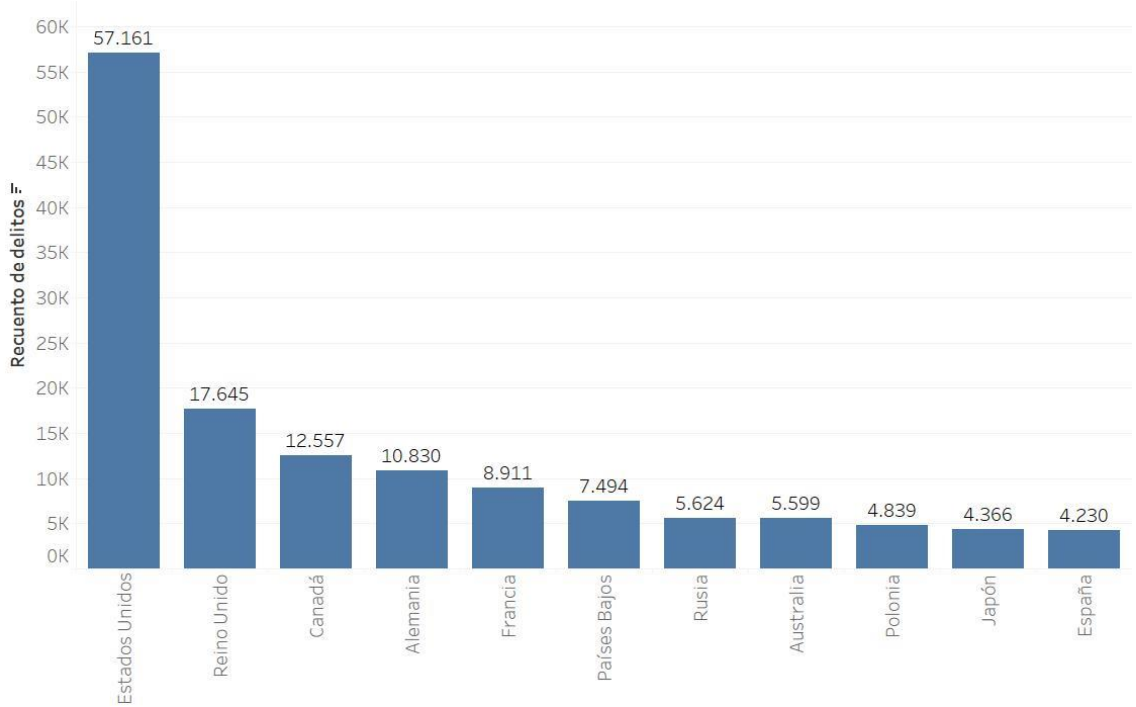
País	Frecuencia	Porcentaje del total*
Estados Unidos	57.161	26,35%
Reino Unido	17.645	8,13%
Canadá	12.557	5,79%
Alemania	10.830	4,99%
Francia	8.911	4,11%
Países Bajos	7.494	3,45%
Rusia	5.624	2,59%
Australia	5.599	2,58%
Polonia	4.839	2,23%
Japón	4.366	2,01%

*Este porcentaje se corresponde con el porcentaje del total de todos los países registrados
Fuente: Elaboración propia a partir de los datos obtenidos en el repositorio Bitcoin Abuse.

Al representar estos resultados en un gráfico de barras se puede ver la gran diferencia que existe en la frecuencia de denuncias entre Estados Unidos con respecto al resto de países (Figura 5).[207]

Figura 5.

Frecuencia de denuncias según el país.



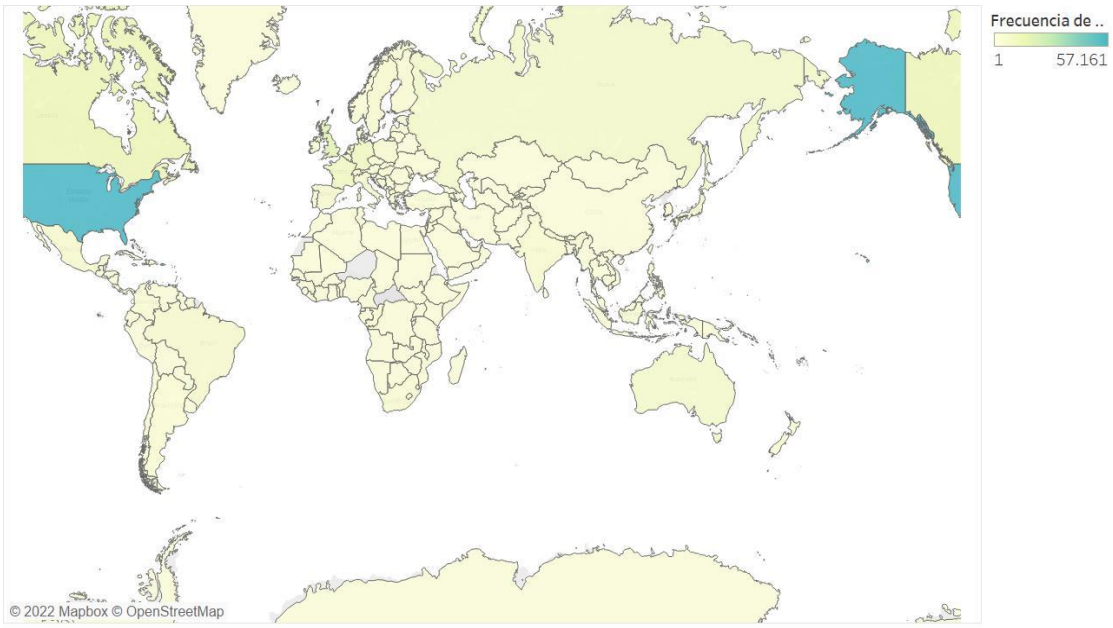
Fuente: Elaboración propia a partir de los datos obtenidos en el repositorio Bitcoin Abuse.

[207] Aunque España no se encuentra entre los 10 países con el mayor número de denuncias, se ha querido incorporar en el gráfico de barras para que se pudiera realizar una comparación y determinar la situación de nuestro país en este ámbito.

Se pueden observar de una forma más visual los resultados para la victimización según países en el mapa de la Figura 6. Estados Unidos se representa con el color azul siendo el país con un mayor número de denuncias. Conforme el número de denuncias se va reduciendo los países adquieren tonalidades amarillas hasta grises.

Figura 6.

Mapa de frecuencia de denuncias por países.



Mapa basado en Longitud (generado) y Latitud (generado). El color muestra recuento de Id Delito. Se muestran detalles para País1 (copia).

Fuente: Elaboración propia a partir de los datos obtenidos en el repositorio Bitcoin Abuse.

Victimización Según el País y el Tipo de Delito

Al relacionar las denuncias por países con los tipos de delitos denunciados se obtiene lo siguiente (Tabla 19). Para Estados Unidos el tipo de delito más frecuente es el delito de extorsión o *Blackmail scam* (N=23.222), seguido del delito de sextorsión (N=16.520). De igual forma sucede para Reino Unido, Alemania y Países Bajos. No obstante, en Canadá y Francia son más frecuentes los delitos de sextorsión.

Tabla 19.

Top 10 de países en Bitcoin Abuse según el tipo de delito.

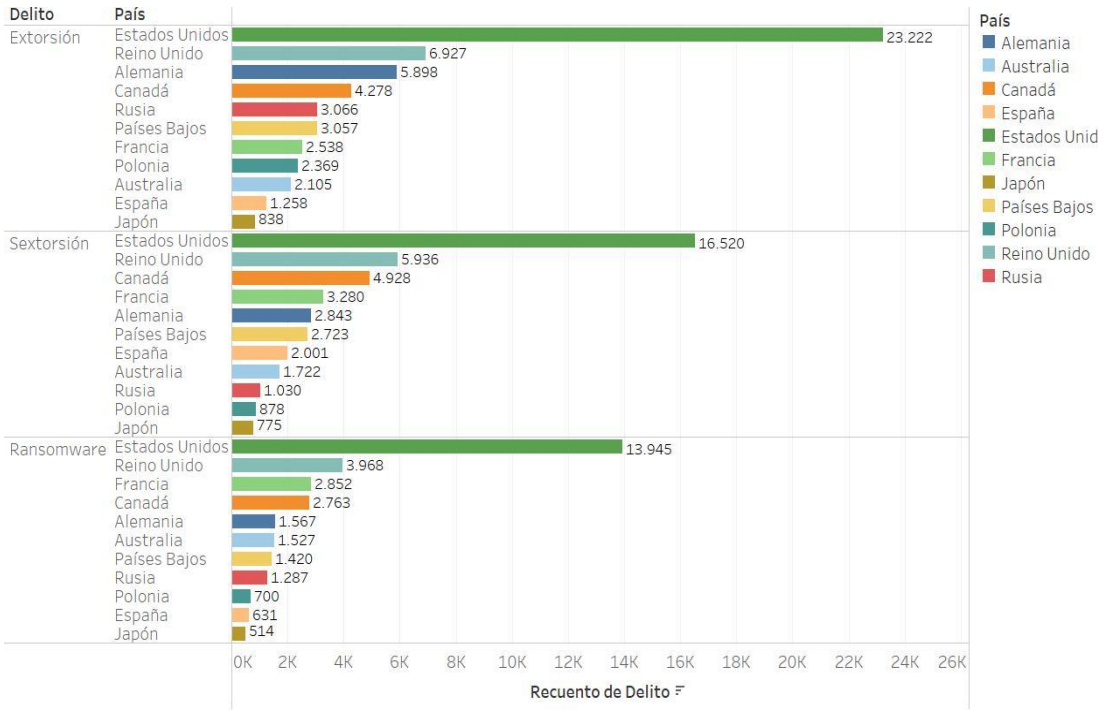
	Tipo de delito						
País	BTC *tumbler*	*Blackmail scam*	Mercados DN	Otro	*Ransomware*	Sextorsión	**Total**
Estados Unidos	703	23.222	340	2.431	13.945	16.520	**57.161**
Reino Unido	119	6.927	80	615	3.968	5.936	**17.645**
Canadá	91	4.278	41	456	2.763	4.928	**12.557**
Alemania	142	5.898	43	337	1.567	2.843	**10.830**
Francia	62	2.538	27	152	2.852	3.280	**8.911**
Países Bajos	87	3.057	31	176	1.420	2.723	**7.494**
Rusia	33	3.066	37	171	1.287	1.030	**5.624**
Australia	42	2.105	37	166	1.527	1.722	**5.599**
Polonia	696	2.369	68	128	700	878	**4.839**
Japón	135	838	14	2.090	514	775	**4.366**

Fuente: Elaboración propia a partir de los datos obtenidos en el repositorio Bitcoin Abuse.

Si se representan los resultados según el tipo de delito y el país de residencia se puede observar lo siguiente (Figura 7). Se observa una cantidad elevada de delitos para Estados Unidos en comparación con el resto de los países.

Figura 7.

Victimización según el tipo de delito y el país.



Fuente: Elaboración propia a partir de los datos obtenidos en el repositorio Bitcoin Abuse.

Victimización en el Tiempo

Se han registrado las denuncias desde el año 2017 al año 2021. Si se observan los resultados de forma general, el año 2020 es el que ha acumulado un mayor número de denuncias (N=102.717) (Tabla 20).

Tabla 20.

Número de denuncias según el año de su registro.

Año	Total
Nulo	3
2017	14
2018	20.640
2019	77.219
2020	102.717
2021	19.079
Total	**219.672**

Fuente: Elaboración propia a partir de los datos obtenidos en el repositorio Bitcoin Abuse.

Si se relacionan los datos de los delitos según el año en el que se registró la denuncia (Tabla 21), se puede observar que los delitos más frecuentes son la extorsión, la sextorsión y los ataques *ransomware*. Se ha visto que los delitos de extorsión han tenido una cifra mayor para el año 2019 (N=36.195), mientras que los delitos de sextorsión (N=40.060) y los delitos de ataques *ransomware* (N=21.002) han repuntado en el año 2020 (Tabla 20).

Tabla 21.

Victimización según el tipo de delito y el año.

Delito	Año					Total
	2017	2018	2019	2020	2021*	
Extorsión		12.262	36.195	31.628	6.446	**86.531**
Sextorsión			22.582	40.060	5.359	**68.001**
Ransomware	7	7.598	16.595	21.002	3.053	**48.255**
Otros	5	559	1.200	7.093	2.703	**11.560**
Mezclador Bitcoin		129	453	2.092	1.201	**3.875**
Mercados Darknet	2	92	194	842	317	**1.447**
Total	**14**	**20.640**	**77.219**	**102.717**	**19.079**	**219.669****

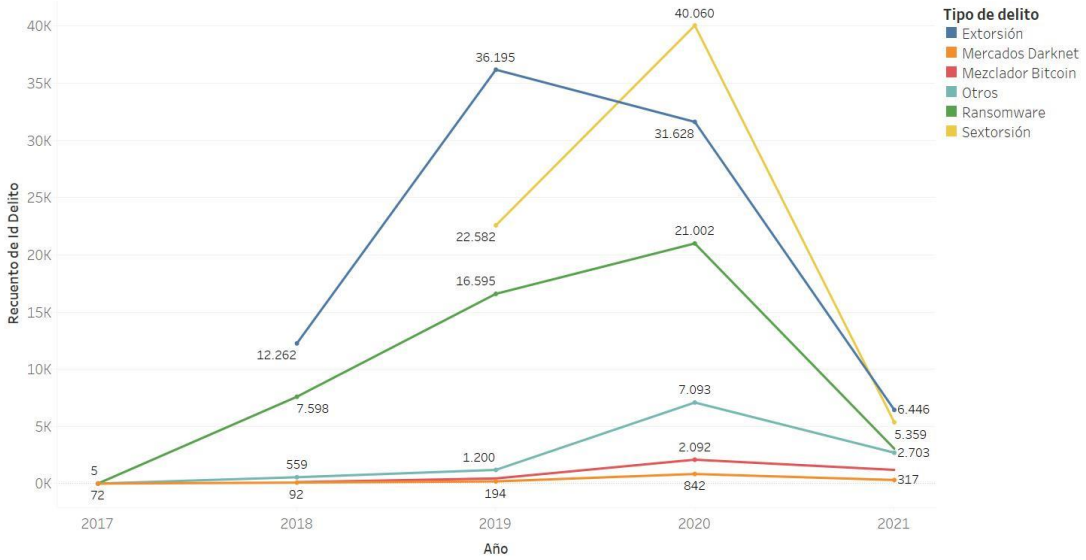
Fuente: Elaboración propia a partir de los datos obtenidos en el repositorio Bitcoin Abuse.

*Debido a las cuestiones relacionadas con los tiempos en la investigación, los datos registrados para este año no pertenecen al año 2021 en su totalidad.
**Se han eliminado del total tres registros de los que no se disponía del año.

Estos resultados se pueden ver de una forma más visual en la Figura 8, en la que se representan los valores más elevados para los delitos de extorsión (color azul), sextorsión (color amarillo) y ataques *ransomware* (color verde).

Figura 8.

Tipo de delito según año del registro en Bitcoin Abuse.

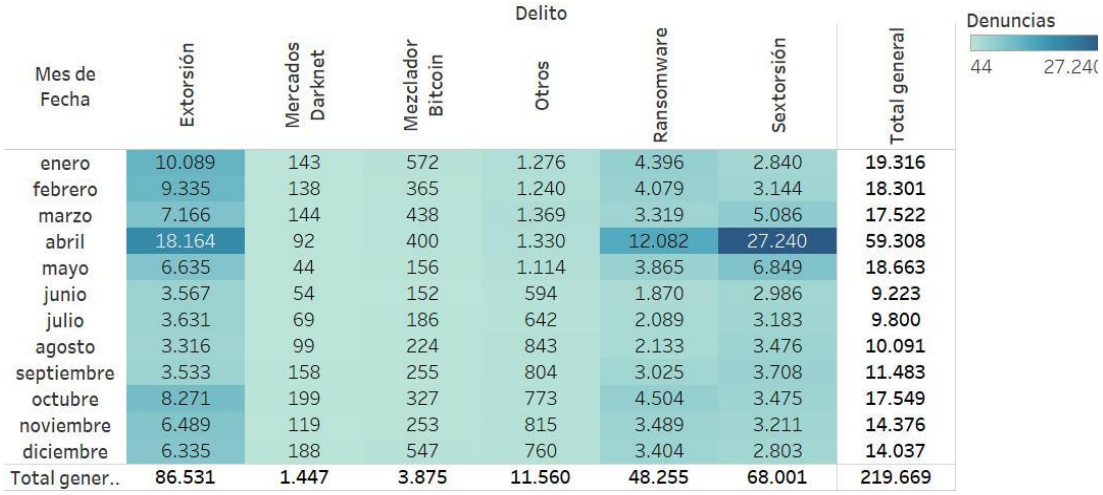


Fuente: Elaboración propia a partir de los datos obtenidos en el repositorio Bitcoin Abuse.

La victimización según los meses del año (Figura 9), presenta un intervalo con un mayor número de denuncias entre los meses de enero (19.316) y mayo (N=18.663). El mes de abril es el que acumula la mayor cantidad de denuncias (N=59.308) y en el que se encuentra el valor máximo de la muestra con los delitos de sextorsión (N=27.240). El valor mínimo se registra en el mes de mayo para los delitos relacionados con los mercados de la *Darknet* (N=44). En segunda posición se sitúa el mes de enero (N=19.316), siendo el mes de junio el que reúne el menor número de denuncias (N=9.223).

Figura 9.

Frecuencia de delitos denunciados según el mes.



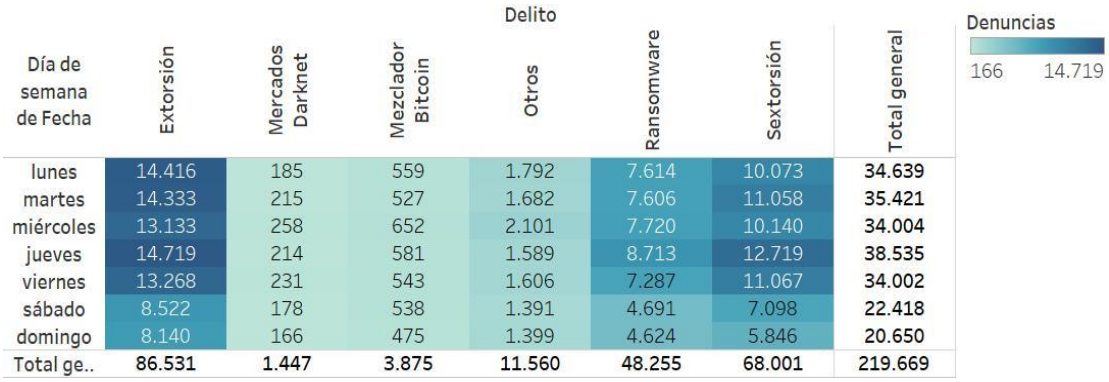
Mes de Fecha	Extorsión	Mercados Darknet	Mezclador Bitcoin	Otros	Ransomware	Sextorsión	Total general
enero	10.089	143	572	1.276	4.396	2.840	19.316
febrero	9.335	138	365	1.240	4.079	3.144	18.301
marzo	7.166	144	438	1.369	3.319	5.086	17.522
abril	18.164	92	400	1.330	12.082	27.240	59.308
mayo	6.635	44	156	1.114	3.865	6.849	18.663
junio	3.567	54	152	594	1.870	2.986	9.223
julio	3.631	69	186	642	2.089	3.183	9.800
agosto	3.316	99	224	843	2.133	3.476	10.091
septiembre	3.533	158	255	804	3.025	3.708	11.483
octubre	8.271	199	327	773	4.504	3.475	17.549
noviembre	6.489	119	253	815	3.489	3.211	14.376
diciembre	6.335	188	547	760	3.404	2.803	14.037
Total gener..	86.531	1.447	3.875	11.560	48.255	68.001	219.669

Tabla de frecuencias de denuncias según el tipo de delito y los meses del año para el conjunto de los años que forman la muestra. El color representa la frecuencia de denuncia de esos delitos siendo el color oscuro una mayor frecuencia de denuncias y el color claro una menor frecuencia. La cifra de delitos totales varía de la cifra de delitos representada en la tabla 17 porque no se dispone de la fecha en la que se realizaron esos registros. Fuente: Elaboración propia a partir de los datos obtenidos en el repositorio Bitcoin Abuse.

En cuanto a la victimización según los días de la semana (Figura 10), se puede observar que hay un mayor número de denuncias los jueves (N=38.535) con un valor máximo de la muestra en los delitos de extorsión (N=14.719), seguidos de los delitos de sextorsión (N=12.719). En segundo lugar, presentan también valores elevados los martes (N=35.421), en los que del mismo modo destacan los delitos de extorsión (N=14.333) y sextorsión (N=11.058). El menor número de denuncias tiene lugar los domingos (N=20.650), con un valor mínimo para los delitos relacionados con los mercados de la *Darknet* (N=166).

Figura 10.

Frecuencia de delitos denunciados según día de la semana.



Día de semana de Fecha	Extorsión	Mercados Darknet	Mezclador Bitcoin	Otros	Ransomware	Sextorsión	Total general
lunes	14.416	185	559	1.792	7.614	10.073	34.639
martes	14.333	215	527	1.682	7.606	11.058	35.421
miércoles	13.133	258	652	2.101	7.720	10.140	34.004
jueves	14.719	214	581	1.589	8.713	12.719	38.535
viernes	13.268	231	543	1.606	7.287	11.067	34.002
sábado	8.522	178	538	1.391	4.691	7.098	22.418
domingo	8.140	166	475	1.399	4.624	5.846	20.650
Total ge..	86.531	1.447	3.875	11.560	48.255	68.001	219.669

Tabla de frecuencias de denuncias según el tipo de delito y los días de la semana para el conjunto de los años que forman la muestra. El color representa la frecuencia de denuncia de esos delitos siendo el color oscuro una mayor frecuencia de denuncias y el color claro una menor frecuencia. La cifra de delitos totales varía de la cifra de delitos representada en la tabla 17 porque no se dispone de la fecha en la que se realizaron esos registros. Fuente: Elaboración propia a partir de los datos obtenidos en el repositorio Bitcoin Abuse.

En relación con la victimización según las horas del día (Figura 11), se puede observar cómo comienzan a aumentar los valores a partir de las 14h (N=10.369) y disminuyen a partir de las 23h (N=10.563), mostrando el valor más elevado en este intervalo a las 17h (N=11.856) para los delitos de extorsión (N=4.753). Los valores mínimos totales se registran entre las 3h (N=6.649) y las 7h (N=6.292), siendo el valor mínimo a las 6h para los delitos relacionados con la *Darknet* (N=98). El valor máximo se registra a las 17h para los delitos de extorsión (N=4.753) y el valor mínimo a las 2h para los delitos relacionados con la *Darknet* (N=30).

Figura 11.

Frecuencia de delitos denunciados según día de la semana.

Hora d..	Extorsión	Mercados Dark..	Mezclador Bitc..	Delito Otros	Ransomware	Sextorsión	Total general
0	3.383	55	189	527	2.525	3.269	9.948
1	3.041	52	121	453	1.909	2.773	8.349
2	2.651	30	118	381	1.602	2.464	7.246
3	2.324	31	95	398	1.438	2.363	6.649
4	2.218	49	107	359	1.351	1.962	6.046
5	2.429	45	87	315	1.205	1.729	5.810
6	2.014	33	98	322	1.309	1.572	5.348
7	2.469	71	123	345	1.400	1.888	6.296
8	3.486	49	132	382	1.700	2.382	8.131
9	3.922	74	147	427	2.000	2.632	9.202
10	3.964	46	141	497	1.997	2.720	9.365
11	3.735	52	116	473	1.896	2.631	8.903
12	3.416	51	149	499	1.919	2.452	8.486
13	3.814	62	195	423	1.952	2.510	8.956
14	4.329	76	225	596	2.272	2.871	10.369
15	4.617	64	217	598	2.386	3.092	10.974
16	4.584	97	194	600	2.494	3.372	11.341
17	4.753	81	232	621	2.608	3.561	11.856
18	4.294	77	219	536	2.410	3.328	10.864
19	4.390	75	196	524	2.435	3.706	11.326
20	4.363	66	195	558	2.379	3.588	11.149
21	4.339	60	199	557	2.313	3.770	11.238
22	4.136	80	205	594	2.463	3.776	11.254
23	3.860	71	175	575	2.292	3.590	10.563
Total ..	86.531	1.447	3.875	11.560	48.255	68.001	219.669

Denuncias: 30 – 4.75

Tabla de frecuencias de denuncias según el tipo de delito y las horas del día para el conjunto de los años que forman la muestra. El color representa la frecuencia de denuncia de esos delitos siendo el color oscuro una mayor frecuencia de denuncias y el color claro una menor frecuencia. La cifra de delitos totales varía de la cifra de delitos representada en la tabla 17 porque no se dispone de la fecha en la que se realizaron esos registros. Fuente: Elaboración propia a partir de los datos obtenidos en el repositorio Bitcoin Abuse.

Discusión

Victimización por Delitos

De estudio empírico de la victimización por delitos con criptomonedas, se ha obtenido que los delitos más denunciados son los de extorsión también conocidos como *blackmail scam.* Este tipo de delitos consisten mayormente en el envío de mensajes a través de correo electrónico en el que se intentan convencer a la víctima de que se encuentra en una situación comprometida para su integridad moral o física que solo se podría evitar mediante el pago de una cantidad de dinero en criptomonedas. El éxito del ataque depende de la decisión última que tome la víctima sobre el pago de la cantidad requerida. Por ello, será necesario el envío

masivo de estos mensajes para asegurar una mínima cantidad de respuestas. Este puede ser uno de los motivos por los que el *blackmail scam* ha sido uno de los más denunciados, es decir, uno de los más recibidos por los usuarios y al mismo tiempo, uno de los más reconocibles por la población.

De igual forma sucedería con el delito de sextorsión o extorsión sexual, que ha sido el segundo delito más denunciado. Constituye una variante del delito anterior de extorsión, por lo que se desarrolla de forma similar salvo que el contenido del mensaje recibido tiene un marcado carácter sexual. Se trataría también de un mensaje frecuentemente recibido y fácilmente identificable por la población, lo que facilita la denuncia por parte de la víctima.

En cuanto a los delitos de *ransomware* que ocupan la tercera posición, de la misma forma que en los anteriores también se requiere del envío a una gran cantidad de personas para asegurar tener éxito, aunque fuera con un bajo porcentaje. Habitualmente las autoridades recomiendan no pagar la cifra que se exige en este tipo de ataques por lo que, aunque la recepción parece ser elevada, su éxito es bajo.

Victimización en el Espacio

Si se estudia la victimización por países se obtiene que ha sido Estados Unidos el país que acumula un mayor número de denuncias. La cantidad de denuncias presenta una diferencia altamente significativa en comparación con los países que ocuparían la segunda y la tercera posición, que son Reino Unido y Alemania.

Por un lado, esto podría significar que es Estados Unidos el país con más víctimas por delitos de extorsión, sextorsión y ataques *ransomware*. Por otro lado, podría suponer un mayor conocimiento de este tipo de delitos y de la plataforma de denuncia en estos países lo que se ha traducido en una mayor implicación en las denuncias. Sin embargo, a pesar de las dificultades para determinar si se trata de una posibilidad u otra, lo cierto es que la tasa de denuncias en Estados Unidos es muy elevada triplicando la cifra para Reino Unido que ocupa el segundo lugar, por lo que tiene relevancia para su estudio.

Victimización en el Tiempo

El año en el que se han recibido un mayor número de denuncias ha sido el 2020. No obstante, debido a las limitaciones de la disponibilidad en los datos de los años siguientes, no se dispone de suficientes datos para establecer tendencias al aumento o descenso de este tipo de delitos. Al observar la representación de los datos en los gráficos se podría estimar un aumento en la tendencia de todos los delitos salvo en el de extorsión que parece disminuir.

Además, el delito de sextorsión aumenta significativamente el año 2019 lo que podría suponer un aumento abrupto para los próximos años. No obstante, debería disponerse de los datos para los años siguientes para poder extraer conclusiones.

Si se realiza un estudio en detalle considerando los meses, los días y las horas en cada año se puede observar lo siguiente. El mes con un mayor número de denuncias ha sido el mes de abril, lo que en principio no arrojaría ninguna conclusión de interés en la materia. No obstante, sí son de gran interés los meses de junio, julio y agosto para los que se ha obtenido el menor número de denuncias. Estos se corresponden con los meses de verano en los que habitualmente las personas abandonan sus trabajos y modifican sus rutinas de forma temporal. De esta forma, los resultados podrían indicar por un lado que las denuncias de estos delitos disminuyen durante los meses de verano porque las personas están alejadas de sus dispositivos y no han reparado en los ataques recibidos, o bien, si han reparado en estos su nueva rutina no les permite dedicar su tiempo en la denuncia. Por otro lado, podría significar que los autores de los delitos también se ven afectados por los cambios en las actividades sociales que se producen durante estos meses, reduciendo su actividad criminal durante este período.

Estas conclusiones coinciden con los resultados obtenidos para los días de la semana, ya que fueron los sábados y los domingos los días en los que menos denuncias se registraban. Estos días se corresponden con el fin de la semana, habitualmente dedicado al descanso y al ocio de las personas. Por lo tanto, también podría indicar que los patrones de actividad tanto de las víctimas como de los autores pudo afectar a la recepción del ataque o al registro de la denuncia.

En cuanto al estudio de la victimización según las horas del día, los valores más elevados se presentan entre las 14h y las 23h de la tarde, con una máxima a las 17h. Esto podría tener relación con la jornada laboral de las víctimas, que pudiendo haber recibido el ataque o el mensaje por la mañana o en la tarde del día anterior, dedicarían la tarde del día siguiente para denunciar el incidente.

De esta forma, se puede observar en el estudio temporal de la victimización que hay una influencia de las actividades cotidianas de víctimas y/o autores de los delitos en la prevalencia de estos.

Como conclusiones, se puede decir que el tipo de criminalidad cometida con criptomonedas que se ha estudiado depende de los patrones de actuación de las víctimas para garantizar su éxito. El primer lugar, se ha visto que son más denunciados aquellos delitos que requieren de envíos masivos de mensajes para poder captar a más víctimas. La efectividad de

este delito dependerá del pago de la víctima de la cantidad solicitada. Por otro lado, la recepción y denuncia de estos delitos también está influenciada por las actividades rutinarias o cotidianas de las víctimas y de los autores. Se mostrarán menos receptivos al ataque fuera de aquellos meses, días y horas en los que no se espera que el usuario pueda estar utilizando un dispositivo apropiado como, por ejemplo, durante su jornada laboral.

Limitaciones del Tercer Experimento:

Este experimento contribuye de forma empírica al estudio de la victimización de delitos con criptomonedas. Sin embargo, también se han encontrado algunas limitaciones. En primer lugar, los datos obtenidos recogen información de una muestra no probabilística y autoseleccionada de víctimas de ciberdelitos relacionados con Bitcoin que no es necesariamente representativa de todo el universo de víctimas. Por lo tanto, la muestra de datos que se dispone no necesariamente refleja todo el universo de víctimas de estos delitos. Puede que el acceso a la página Bitcoin Abuse sea más familiar para algunos usuarios en concreto por diversos motivos como el idioma o su publicidad. O también puede suceder que solo accedan aquellos usuarios más capacitados para el uso de la tecnología (Buil-Gil & Saldaña-Taboada, 2021). Además, la clasificación del tipo de incidente recibido se ha realizado por la víctima, por lo que puede suceder que haya clasificaciones erróneas (Buil-Gil & Saldaña-Taboada, 2021).

Por otra parte, debido al trascurso de la investigación, la recogida de datos tuvo que realizarse a mediados de 2021 por lo que no se disponen de la totalidad de datos para ese año. Se espera que en futuras investigaciones se pueda ampliar la muestra de datos y realizar un estudio más detallado de las tendencias de victimización a lo largo de los años.

Sin embargo, a pesar de estas limitaciones se ha considerado una fuente de obtención de datos extremadamente valiosa que permite la medición de un fenómeno que por sus características es difícilmente cuantificable.

Capítulo 12. Estudio de las Motivaciones Para Utilizar Criptomonedas en un Foro de Discusión de la *Darknet* (Experimento 4)

El objetivo del experimento consiste en el estudio de las motivaciones de los sujetos para utilizar las criptomonedas en el desarrollo de sus actividades delictivas. Para ello será también necesario conocer la forma en la que utilizan esta tecnología en sus delitos, así como las criptomonedas que emplean con una mayor frecuencia. La pregunta general desde la que se parte es si las características de estas tecnologías son relacionadas con un favorecimiento de la actividad criminal y, por tanto, se asume que serán utilizadas por los criminales en todo caso para obtener más beneficios.

Métodos y Materiales

Estrategia de Investigación

La metodología de este experimento consiste en el análisis del contenido de un foro de la *Darknet* conforme a un enfoque *Grounded Theory* anteriormente descrito.

La fuente de obtención de los datos es un foro de la *Darknet* conocido como "Dread". Se presenta como el sucesor de un foro que inicialmente se ubicaba en "Reddit" creado por el usuario "HugBunter", que desapareció en el año 2018 cuando "Reddit" eliminó cientos de comunidades en las que se realizaban discusiones que podían incitar o facilitar la comisión de un delito. El foro se divide a su vez en diversos subforos que se especializan en temáticas específicas como, por ejemplo, el fraude o un mercado australiano en la *Darknet*. La información contenida en el foro se ha utilizado anteriormente en otra investigación realizada por Simon Butler (2021). No obstante, difiere de la presente investigación en que Butler utiliza una base de datos ya elaborada, "CrimeBB" que se corresponde con otro periodo temporal. Además, analiza el contenido del foro de una forma automatizada y emplea otro programa de análisis cualitativo conocido como "QDA Miner Lite".

La recogida de los datos se realizó en dos periodos de tiempo separados en dos años con una duración de cuatro meses. El primero tuvo lugar durante el mes de diciembre del año 2020. El segundo periodo se corresponde con el período entre los meses de julio y septiembre del año 2021.

Los pasos de este proceso se desarrollaron conforme al enfoque *Grounded Theory* que se han explicado de una forma más detallada en el apartado perteneciente a la metodología general del experimento. De forma resumida, consisten en el acceso al foro, la recolección de los datos, el codificado de los datos, la revisión de los datos obtenidos y la recodificación. El acceso al foro estaba condicionado por la resolución de diversos puzles a través de la medida

de seguridad CAPTCHA. La recolección de las discusiones se llevó a cabo a través de la introducción del término de búsqueda “Bitcoin”.

El proceso de codificación se realizó utilizando el software de análisis cualitativo “NVivo”. Se comenzó con el estudio y el análisis de un grupo de la muestra para obtener los primeros códigos. Estos fueron revisados y se observó su aplicación al resto de las discusiones, obteniendo al mismo tiempo nuevos códigos (Apéndice 2). Como resultado se obtuvieron diferentes temas y subtemas en los que podrían agruparse las discusiones estudiadas.

Descripción de la Muestra

De esta forma se recopiló una muestra de 254 discusiones que fueron almacenadas en un formato de texto e imagen para su posterior estudio y análisis. La estructura de estas discusiones consta de un comentario principal realizado por un usuario que realiza una consulta o comentario y por las respuestas del resto de miembros del foro en relación con el comentario principal siguiendo un formato de pregunta-respuesta (Figura 12). Las discusiones obtenidas pueden pertenecer a diversos subforos de los que se divide el foro principal. El número de respuestas de las que consta cada discusión es indeterminado siendo al mismo tiempo muy numerosas, lo que ha dificultado su recuento a efectos del presente apartado.

Figura 12.

Ejemplo de una de las discusiones del foro.

Esta información ha sido eliminada por cuestiones de privacidad y seguridad. Se podrá acceder a estos datos por medio de una solicitud ante el órgano competente de la Universidad de Granada.

Captura de pantalla de una de las discusiones que se han recopilado para esta investigación. Fuente: Elaboración propia a partir del contenido del foro de la DN.

Resultados

Como resultado de la recopilación de datos durante los cuatro meses entre el año 2020 y 2021 se obtuvo una muestra de 254 discusiones.

Del estudio y análisis de las discusiones obtenidas en relación con el objetivo de las investigaciones se identificaron varios temas. Al mismo tiempo, se han podido encontrar

otros temas y subtemas que no se habían previsto pero que resultan de interés para el desarrollo de la investigación.

Finalmente, el resultado consiste en la obtención de seis temas con sus respectivos subtemas en los que se podrían agrupar todas las discusiones estudiadas. Estos temas son: 1) Evitar la detección de la actividad ilegal; 2) Utilización de las criptomonedas para cometer delitos; 3) Lecciones sobre ciberseguridad y utilización de las criptomonedas; 4) Regulación de las criptomonedas; 5) Evitar la victimización y 6) Reflexiones, quejas y casos relevantes.

A continuación, se presentan de forma detallada los resultados obtenidos en relación con las diferentes temáticas:

1. Evitar La Detección de la Actividad Ilegal

De entre todas las discusiones estudiadas, son mayoritarias aquellas que versan sobre evitar la detección de la actividad ilegal cometida con criptomonedas. El objetivo que persiguen los usuarios en estos grupos de discusión es evitar la detección de la actividad realizada con criptomonedas, esto es, desde la obtención hasta la conversión a dinero en efectivo. Esto no solo se limita a la detección por parte de las autoridades policiales, sino que se extiende hacia otros usuarios de la comunidad del foro. De forma general, la comunidad de las criptomonedas es plenamente conocedora de la capacidad de rastreo de la actividad con Bitcoin a través del análisis de la *Blockchain*. Por ello, siendo en algunos casos irremplazable la utilización de Bitcoin, estos grupos de discusión se sustentan sobre formas de reducir o evitar toda probabilidad de un rastreo en el futuro.

Dentro de esta temática, se han agrupado las diferentes conversaciones estudiadas según los aspectos que se consultan. Si se ordenan de mayor a menor frecuencia estos grupos son: (1) obtención de las criptomonedas, (2) consejos para escapar de las autoridades o responder ante estas, (3) rutas de conversión entre criptomonedas (4) tipos de criptomonedas preferentes para el crimen, (5) tecnología empleada para ocultar la actividad; (6) técnicas específicas de *cashout* y (7) reparar riesgo ocasionado. De esta forma, el grupo con una frecuencia mayor ha sido el de consultas sobre la obtención de criptomonedas, seguido del grupo con discusiones sobre consejos para escapar de las autoridades y responder ante estas.

Obtención de las Criptomonedas. La obtención o compra de las criptomonedas es el primer paso que debe dar toda persona interesada en una posterior utilización de esta tecnología tanto con fines ilegales como legales. Para el caso de que la persona desee incorporarla en sus actividades delictivas, tendrá como objetivo la protección de su actividad delictiva y su anonimato.

Este paso constituye la primera relación que se establece entre un sujeto y la moneda virtual, por lo que su obtención se debe realizar de la mejor forma posible para que no se pueda establecer un vínculo entre ambos en los pasos posteriores de su actividad delictiva. Cualquiera de los delitos que se conoce que incorporan esta tecnología en alguna de sus etapas comenzará inevitablemente por su obtención.

Por todo ello, el modo para obtener o comprar criptomonedas ha adquirido una elevada importancia entre los usuarios de la comunidad de criptomonedas:

> *never done this online before, where specifically should i buy and store monero, and how do i buy? i dont see buying on listings only messaging on their profile. this is probably the dumbest question ever asked but whatever* (U1, 2021[208]).

Este tema ha sido uno de los más frecuentemente discutidos en el foro, especialmente con consultas sobre diversas formas de realizar este primer paso de una forma segura que permita evitar riesgos de detección, rastreo y persecución del delito posterior.

De forma anónima y segura:

> *Hello, can someone guide me how to buy BItcoin/Monero anonymously with carded credit/debit cards. The safe way to do it. Thanks* (U2, 2021).

Sin que se requiera un documento de identidad:

> *Could someone point in the direction of a website where i can purchase crypto with cards without ID* (U3, 2021).

Que no dispongan de políticas de KYC:

> *Hello, i want to purchase approximately $2,000 in bitcoin, but the majority of exchangers are having really low limit. I want to pay with my own cc/debit card and just receive the btc to my electrum wallet (...) What is the best way to purchase fast and instantly bitcoin with cc (...) Most need KYC and but i prefer to purchase from direct exchange where you don't even have to make account, just pay with cc and receive to your btc address* (U4, 2021).
>
> *Anywhere to buy in the UK at the moment? Used to be able to buy £200 or less without KYC thru cryptomate but seems to have changed and don't even allow you to buy XMR anymore* (U5, 2021).

Que esté disponible en un país en concreto y que permita realizar la compra con dinero en efectivo:

> *do I really need to find a way to buy crypto from an exchange that IS AVAILABLE IN NY, US, allows fiat<->crypt<->fiat, handles monero, accepts debit or prepaid cash card or cashapp, with no KYC 2-factor, that doesn't charge an excessive deposit or withdrawal fee, that can transact with my wallet on*

[208] La abreviatura U1 significa "Usuario 1". Se utilizará la letra "U" para denominar a los usuarios del foro junto con su correspondiente número por orden de aparición en el texto.

> *my computer. is that a realistic? does that exist? if not, PLEASE tell me what are the minimum currency/wallet/exchange requirements for anonymous shopping?* (U6, 2021).

Que además sea un método barato, efectivo y sencillo:

> *What is the easiest and cheapest way to buy bitcoin. I got booted from cash app which was only $2 for every $100 so looking for something like that. Am doing illegal stuff but need no advice other than place to purchase the bit coin. Thanks* (U7 en U8, 2020).

Las respuestas a estas consultas pueden presentar un carácter muy variado y dependerán del propósito que se tenga para su posterior utilización, es decir, si se quiere permanecer oculto, cometer un delito o solamente evadir impuestos (U9 en U8, 2020). El siguiente usuario explica esto en detalle con la forma en la que se debería actuar en cada caso. Lo divide en si desea ocultar lo que se está comprando, si se desea ocultar al gobierno que se dispone de criptomonedas Monero o si desea ocultar al gobierno que se posee cualquier tipo de criptomoneda:

> *It all depends. If you just want to hide what you're purchasing, I recommend buying LTC on some exchange, send it to elude, change to xmr, use as desired. Once it's xmr it's like it goes *poof* into the ether. This will hide all transactions once you've switched to xmr.If you're trying to prevent the government from being able to find out that you have monero, the previous steps will also suffice. Just don't send the xmr to any kyc wallet/exchange. Use a hardware wallet/XMR GUI wallet/cake wallet. You can keep it on elude if you want but that would personally make me nervous. If you're trying to prevent the government from knowing you have any crypto at all, your options are local monero cash by mail, any local btc/crypto atms that don't do kyc (I have no idea about specific availability in US/NY, sorry, but there are searchable location lists on the clearnet) or mine your own XMR either solo or through a pool. You can find more specific mining help on Reddit* (U10 en U6, 2021).

De forma general, del estudio de las conversaciones, los aspectos que interesan a los usuarios en la obtención de criptomonedas con propósitos delictivos se pueden agrupar en: evitar toda política de KYC (medidas de seguridad, límites de dinero, etc.) y en obtener la mayor rentabilidad por su actividad (tasas de conversión, disponibilidad en su localidad, rapidez, etc.). En relación con estas necesidades los usuarios del foro responden a los comentarios recomendando diferentes formas de obtener o comprar las criptomonedas. Están constituidos por: casas de cambio o plataformas de compra de criptomonedas, cajeros automáticos o ATM, tarjetas regalo o prepago, tarjetas de crédito y débito.

Casas de Cambio o Exchanges. De forma general, en el foro se desaconseja la compra de criptomonedas a través de casas de cambio con políticas de KYC. Se expone que si en una operación policial se cierra un criptomercado y se obtienen todas las direcciones que realizaron transacciones hacia los vendedores se podría seguir el rastro hasta el punto en el que se obtuvieron las criptomonedas en la casa de cambio e identificar a la persona (U11 en U12, 2020). Un ejemplo de este tipo de casas de cambio es "Coinbase", que ha sido reiteradamente desaconsejada en los foros para la compra de bitcoins que posteriormente se utilicen en criptomercados:

> *As you mentionned it's because of the financial regulations in your country. You can't bypass them. If you don't want to have to fill in these infos then don't use big exchanges like Coinbase, localbitcoins and stuff. Even if you raised any security flag, you'll never notice it. Such things are always hidden due to EU global laws. My best advices would be to not use exchanges like Coinbase at all. Also use XMR over BTC* (U13, 2020).

En su lugar, se aconseja la utilización de casas de cambio descentralizadas en las que la compra de criptomonedas no supondría la superación de políticas de KYC. Por ejemplo, el intercambio "Bisqnetwork" cuenta con una amplia variedad de formas de pago entre las que se encuentra una anónima (U15 en U16, 2021). También "Kilos" es otro intercambio sin políticas de KYC que no almacena direcciones IP en el sistema por lo que no se podrá vincular el intercambio con una identidad, IP o información KYC (U17 en U18, 2021).

Plataformas de Compra de Criptomonedas Peer-To-Peer (P2P). Otra de las opciones recomendada son las plataformas de compraventa de criptomonedas peer-to-peer (P2P) que ponen en contacto a personas que deseen obtener criptomonedas con aquellas personas que desean venderlas o viceversa. Los dos servicios más discutidos en el foro han sido "LocalBitcoins" y "LocalMonero" consultando cuándo es adecuado utilizarlos y las razones por las que se recomienda uno sobre el otro.

Algunos usuarios hacen referencia a la utilización de "LocalBitcoins" para delitos que no revistan de una elevada gravedad como la compra de pequeñas cantidades de droga (U12, 2020). Otros usuarios aseguran que su utilización no es útil actualmente porque requiere de la identidad y recomiendan opciones alternativas como "Agoradesk" (U19 en U12, 2020). El motivo es que, aunque anteriormente se podía utilizar este servicio sin medidas de KYC, en la actualidad han sido añadidas:

> *I'm now looking to going back to buying my crypto anonymously and am looking at localmonero. I used to use localbitcoins back when it was anonymous but now that can't be* done (U20, 2021).

> *Yes the good old days when you set a trade up on Localbitcoins and had 1 hour to run to the bank with NO ID and deposit cash into the bitcoin traders account. 1 bitcoin = £90 back then lol* (U21en U5, 2021).

De esta forma, aunque se adquiera Bitcoin de forma legal y luego se convierta a otras criptomonedas siguiendo diversos caminos, la transacción realizada siempre quedará grabada en la *Blockchain* y si se accede a este se podrá conocer la identidad. Se pueden tomar algunas medidas para utilizar este servicio y evadir las políticas de KYC como utilizar documentos de identidad falsos, teléfonos desechables o encargar la tarea a una tercera persona. Sin embargo, estos inconvenientes unidos a las altas tasas de conversión de estos lugares han motivado a la comunidad de las criptomonedas a recomendar otros servicios para obtener criptomonedas más rentables.

En lugar de la criptomoneda Bitcoin se recomienda utilizar Monero, que se puede obtener del servicio "LocalMonero". Se trata de otra plataforma de compraventa de criptomonedas con *escrow y peer-to-peer* (P2P) que permite obtener la criptomoneda Monero directamente de un intercambio con otro usuario. Goza de una amplia confianza por parte de la comunidad ya que es posible operar sin políticas de KYC y además ofrece *Onion Service* (U22, 2020). Dispone de una amplia variedad de vendedores que aceptan diversas formas de pago como tarjetas de débito (a veces crédito), efectivo en el correo, *Wester Union*, transferencia bancaria, etc. (U23 en U24, 2021). Por ejemplo, tarjetas prepago de Amazon o tarjetas de videojuegos como "Fornite" (U25 en U26, 2021). El usuario puede escoger al vendedor que desee, no obstante, se recomienda reiteradamente contactar con aquellos vendedores con puntuaciones altas y valoraciones positivas por parte de los clientes.

De entre todos los métodos de pago que pudieran estar disponibles en LocalMonero, los usuarios del foro recomiendan comprar Monero a través del envío de dinero en efectivo por correo postal, lo que se conoce como *cash by mail:*

> *(…) Localmonero cash by mail. There are reputable vendors and I have a solid guy I've used many times without a hiccup. I know people are wary of cash by mail and being ripped off, but is it really any worse that the markets. Really? I've been ripped off on the markets when I thought I had protection which we don't really. You register anonymously, send the cash by express and you've got it in your localmonero account within two days (…) But I love the mail as you stay totally out of sight (…)* (U27 en U26, 2021).

> *Then for Monero you won't find better than localmonero and buy with cash (cash in person, cash by mail, etc.) or through gift cards and stuff if you're comfortable with* (U29 en U30, 2021).
> *Localmonero cash by mail. 100% anonymous and not tracked. Need a verified email to get a localmonero account. Get a cellphone burner to obtain the verified email to make the account* (U28 en U31, 2021).

> *Cash by mail is the safest way to go, just make sure you follow the instructions given to you by the vendor down to the tee or they could fuck up. Not many people do cash by mail compared to just buying off an exchange and converting for obvious reasons but if you're fine with waiting a few days to a week then go for it* (U32 en U20, 2021).

La forma en la que se desarrolla este método de compra de Monero es la siguiente: el usuario accede a la plataforma, selecciona el vendedor que ofrece *cash by mail* como forma de pago, envía la cantidad de dinero en efectivo a través del correo postal y cuando el vendedor reciba el dinero enviará las criptomonedas a la cuenta del comprador. Este funcionamiento permite garantizar un mayor anonimato, lo que ha motivado a la comunidad del foro a recomendar este método más frecuentemente. El registro anónimo y el carácter privado de la criptomoneda Monero unidos a la utilización del dinero en efectivo fuera de la red garantizan que no sea posible su rastreabilidad. Aunque puede pedir en ocasiones la verificación de la cuenta, se podrán emplear técnicas como la utilización de un teléfono desechable y este método con unas tasas menores y menos utilizado que otros servicios será mucho más rentable.

Cajeros Automáticos o ATM. Otra forma de obtener criptomonedas es a través de la utilización de cajeros automáticos o *Automated Teller Machines* (ATM). Se presentan con una opción comentada en el foro porque permiten la compra de criptomonedas utilizando dinero en efectivo, por lo que ofrecen posibilidades de preservar el anonimato.

> *idk if this is the right sub to ask in but ever since some laws u cant put cash in a btc atm without having to verify your id or whatever. how can i buy bitcoin anonymously? thanks guys* (U33, 2021).

Sin embargo, aunque de forma generalizada se considera como una opción deseable para garantizar el anonimato de la actividad, esta opción ha sido muy debatida. El motivo es que, aunque permite obtener fácilmente criptomonedas empleando efectivo, dispone de algunas medidas de KYC que habrá que considerar. Este es el caso de las medidas que se establecen una vez superado el límite de dinero por transacción (datos personales, documento de identificación, número de teléfono, etc.) o las medidas de seguridad en el propio establecimiento (cámaras de vigilancia). Han sido muy criticados por la severidad de las medidas, aunque se trata de una forma legal de obtener criptomonedas (U6, 2021). De esta forma, las consultas realizadas y la mayoría de las respuestas dadas tratan sobre la forma de beneficiarse de los servicios de los ATM sin que se descubra la identidad. Hay ATMs que todavía no disponen de políticas KYC como “CoinFlip”, que además permite la compra de varios tipos de criptomonedas (U34 en U35, 2021). Pero de forma general, los consejos en este caso están orientados a salvar el tipo de medidas de seguridad que se pueden encontrar en los ATM (teléfonos desechables, identificaciones falsas, cara cubierta, etc.) sin poner en riesgo el anonimato del usuario.

También se han planteado otras cuestiones más generales como, por ejemplo, la forma en la que deben enviarse las monedas obtenidas a la cartera del usuario (/u/bartard86, 2020). Recomiendan emplear una de las carteras que se conoce que respetan la privacidad, obtener el código QR de esta y cuando en el cajero se pida este código mostrarlo para enviar las criptomonedas a esa cartera (U36 en U37, 2020). Para encontrar los cajeros más cercanos a la zona se recomienda la utilización de coinradar.com.

Tarjetas Regalo o Prepago. Las tarjetas prepago y tarjetas regalo se presentan como una alternativa para aquellas personas que desean convertir dinero en efectivo a criptomonedas como Bitcoin sin que la actividad sea detectada (U38, 2021).

> *(...) After lurking and taking notes I concluded that my personal method would be to buy a giftcard for as high and I can and trading it for bitcoin. I don't give a fuck about the bank locking shit cause the giftcard will already be in my hands. I'll admit I haven't researched enough to know if the bank reversing the transaction will lock the giftcard or not but I dead do not care (...)* (U39, 2021).

Consisten en un soporte similar a las tarjetas de crédito o débito que al que se le puede cargar dinero fiduciario para poder utilizarlo de forma digital.

> *In my opinion it is best to use options which do not even ask for a name, like cash or gift cards, than use an option where you are asked for your name (even if you are able to lie)* (U40 en U38, 2021).

De esta forma, constituyen una opción interesante en este ámbito porque pueden utilizarse para comprar criptomonedas con dinero digital o a través de algún vendedor que acepte esta forma de pago:

> *Buy giftcards, amazon, paypal, ... and change it with bitcoin. not good for investing since it loses its value* (U41en U30, 2021).

> *Find a reputable vendor who accepts gift card codes, then send them gift card codes you bought with cash. If you pick a big company cards, like Amazon, moving $1k around per week should not be too hard* (U40en U38, 2021).

Algunos vendedores de plataformas como “LocalBitcoins” o “LocalMonero” aceptan tarjetas regalo como forma de pago, por lo que se puede utilizar dinero en efectivo para la compra de las tarjetas (p.ej. tarjetas de Amazon) y posteriormente utilizarlas como forma de pago de criptomonedas (U40 en U38, 2021).

Aunque esta opción resulta interesante para obtener criptomonedas mediante dinero efectivo de una forma que permite conseguir cierto anonimato, lo cierto es que las tasas y tarifas de las tarjetas prepago en muchas ocasiones son muy elevadas y no resulta rentable, por lo que no es uno de los métodos más recomendados en el foro:

> *Do cash by mail with localmonero. If it's gift cards you are referring to as prepaid the fees they tax you are insane and not worth it* (U28 en U42, 2021).

Además, constituyen una opción difícil de conseguir ya que actualmente se encuentran pocos vendedores que acepten esta forma de pago y pocos sitios que vendan estas tarjetas pagando con criptomonedas (U43, 2020).

Tarjetas de Crédito y Débito. Es habitual también encontrar en el foro comentarios de usuarios que desean comprar criptomonedas utilizando tarjetas de crédito o de débito:

> *Hello, can someone guide me how to buy BItcoin/Monero anonymously with carded credit/debit cards. The safe way to do it. Thanks* (U2, 2021).

> *I was planning on buying bitcoin with prepaid cards and then exchanging it for monero but everywhere says to avoid useing bitcoin at all. It doesn't seem like you can use prepaids to buy monero, you can mail in cash but im not trying to do that. So should I just buy monero directly with my debit card?* (U42, 2021).

Aunque las tarjetas de crédito y debido están conectadas a una cuenta bancaria que dispone de datos personales del usuario hay varias razones para consultar su utilización en este ámbito. La primera es que se trata de una forma de comprar online con la que los usuarios están familiarizados, por lo que se puede utilizar más fácilmente que otros métodos menos conocidos como las casas de cambio o los servicios de compra P2P. Además, no requiere del registro ni la apertura de nuevas cuentas en otros servicios. La segunda es que es una forma más accesible que no requiere de la disposición, gestión y manipulación de dinero en efectivo. De esta forma, suprime los inconvenientes de acudir a un cajero automático a retirar grandes cantidades de efectivo que habrá que manipular o enviar.

Por estos motivos, se puede utilizar la tarjeta de crédito para comprar criptomonedas en algunas casas de cambio como “Binance”, pero hay que saber que tienen políticas de KYC. Habrá que verificar una cuenta mediante el escaneo de una identificación, descargar una foto, etc.:

> *you can buy with cc from binance , its the safest place to buy btc , BUT you need to verify your account first > id scan + utility bill + selfie* (U44 en U24, 2021).

De esta forma, requerirá de tomar una gran cantidad de precauciones y realizar acciones destinadas a superar las medidas establecidas por las políticas de KYC. La verdadera clave de esta forma de obtener criptomonedas reside en la habilidad para el robo de identidad más que en la utilización del dinero (U43, 2020).

Puede también realizarse la compra utilizando la propia cuenta bancaria de los usuarios. Esto resulta especialmente arriesgado por lo que deberá seguir un método concreto para no asumir riesgos:

> *(…) how I go about doing this is getting quality CCs with fullz info. I make a bank drop and age it for several months. Together with the creation of the drop I create an account at an exchange, verify all the documents and let it sit. When I am ready to card it I will use funds that I have been*

> *depositing/using in my bank drop and make several purchases for bitcoin (…)* (U43, 2020).

Muchos usuarios no recomiendan la compra de criptomoneda con tarjeta de crédito por ser difícil y compleja a no ser que se encuentre un nuevo método (U45 en U2, 2021). Además, algunos bancos han bloqueado la opción de pago con tarjeta de crédito, únicamente estando disponible el pago con tarjeta de débito:

> *You're not going to be able to buy crypto with a credit card because banks blocked all crypto purchases through credit cards. You're going to have to use a debit card* (/u/ U46 en U24, 2021).

No obstante, aunque sea posible, la utilización de tarjetas de débito para la compra de criptomonedas también es desaconsejada por la comunidad del foro. De forma general, se desaconseja toda opción para adquirir criptomoneda que pueda vincular la identidad de un usuario con su actividad posterior. Aunque se utilice una tarjeta de débito para comprar una criptomoneda de carácter privado como puede ser Monero, si en el futuro se consiguen rastrear las transacciones que se realizan con esta se podrá relacionar la identidad del usuario con la actividad realizada:

> *getting the monero with your debit card just ties your identity more closely to the monero which isnt what you want... even though the transactions are private today, the quantum computers will eventually be able to trace it all :)* (U47 en U42, 2021).

En el caso de los registros bancarios, se disponen de medidas de seguridad como el factor de doble autentificación o un sistema de dispositivo OTP. Si el sujeto se hace con uno de estos registros, tendrá que saber cómo superar este tipo de controles. Cuando se quiere utilizar una cuenta para comprar criptomonedas, en el caso de que el banco pida el OTP se han comentado en el foro estrategias para poder superar esto. Si se dispone el número de teléfono de la víctima consiste en llamarla haciéndose pasar por personal del banco y reclamando el código que se le ha enviado por SMS. Una vez se consiga realizar la transacción, mover el fondo hacia la billetera “Electrum” y luego limpiar las monedas con un cajero de BTC (U48 en U49, 2021).

Escapar de la Detección de las FCSE y Otras Autoridades. La utilización de las criptomonedas puede incrementar el anonimato y la privacidad de la actividad ilegal realizada, pero su simple utilización no es eficaz en todo caso. Para conseguir reducir el riesgo de detección de un delito, los usuarios han de conocer cuáles son las estrategias de persecución empleadas por las autoridades. Por ello, son objeto de discusión en el foro las actuaciones de las FCSE y otras autoridades encargadas de la persecución de este tipo de criminalidad.

En primer lugar, se debe tener en cuenta que, aunque la observación de la *Blockchain* permite conocer la actividad de cualquier dirección Bitcoin, esto no supone que pueda conocerse la identidad del usuario. Para ello será necesario obtener información adicional que permita vincular la actividad de una cartera a una identidad en específico. Esta tarea se dificulta con aquellas criptomonedas de carácter privado, en las que incluso no es posible conocer la actividad realizada por ninguna de las carteras implicadas.

De esta forma, se podría decir que las estrategias de persecución este tipo de delitos se dividen en dos etapas. Por un lado, estaría el estudio y obtención del patrón de actividad de las direcciones que se deseen investigar. Por otro, la obtención de información adicional que permita vincular de forma inequívoca la dirección de una cartera con la identidad de un usuario en concreto. Sin la obtención de dicha información, no podría señalarse a una persona como autora de un delito de estas características.

Por lo tanto, el primer paso que pueden dar las autoridades en la investigación es el de señalar como sospechosas determinadas carteras que pudieran estar implicadas en alguna actividad delictiva.

> *Worse case you are simply put on a list until police can gather more info on you to convict you of something. But for a small order just once, its probably not worth going after* (U50 en U51, 2021).

Uno de los indicios que pudiera llevar a considerar una dirección como sospechosa de cometer un delito es la cantidad empleada de dinero fiduciario para comprar criptomonedas. Aunque a priori no es ilegal comprar una elevada cantidad, las autoridades pueden marcar estas direcciones como sospechosas e iniciar una investigación más detallada para obtener la identidad del usuario y determinar si su actividad era legal. Para ello son determinantes las políticas de *Know your customer* (KYC) o "Conoce a tu cliente" de algunas casas de cambio, que exigen información personal a todo aquel usuario que desee comprar criptomonedas empleando sus servicios. De esta forma, disponen de información que puede vincular a un usuario con la dirección de su cartera. Esta información podrá ser requerida por las FCSE

cuando necesiten identificar a los usuarios que gestionan direcciones calificadas como sospechosas de cometer un delito.

> *In order to confirm 100% a transaction from wallet A to wallet B, LE would have to have both sender and reciever wallets. which is why sending from a kyc enchange directly is bad, because LE can/will get those easy. just assume LE own KYC wallets. so, if they get yours too, game over* (U47 en U52, 2021).

Por este motivo, las políticas KYC son frecuentemente discutidas en el foro por aquellos usuarios que quieren evitar que se les identifique en su actividad con criptomonedas. De forma general, la comunidad del foro recomienda que se evite utilizar cualquier casa de cambio que tenga este tipo de políticas para adquirir criptomonedas. Sin embargo, en ocasiones no es posible evitar utilizar una casa cambio de estas características, por lo que los usuarios ofrecen consejos para minimizar el riesgo de identificación. El primero de ellos consiste en no enviar las criptomonedas obtenidas a través de un *Exchange* con políticas KYC directamente a otra dirección, ya sea de un mercado o de una dirección privada.

> *If you sent the exact or similar amount from a KYC exchange to yourself and then to vendor then police can make a guess and say that it was you who made the transaction. The closer your exchange withdrawal is to the vendor transaction in time and amount the more certain they are that it was you who made it* (U53, 2021).

Si las otras direcciones comienzan a ser investigadas, podrían fácilmente acceder a la actividad que ha desarrollado y obtener las otras direcciones involucradas. Si estas proceden directamente de políticas KYC, se podrá conocer la identidad del usuario y la actividad realizada. Esto cuando un vendedor o mercado han sido aprehendidos por las autoridades y se obtienen todas las direcciones implicadas en sus actividades.

> *Dont use exchanges that need KYC. If a market got busted they will investigate every adress and every transaction, if they found your wallet and see connections with exchanges they will investigate and will found you. If you want to be really safe use monero* (U11 en U12, 2020).

La utilización de carteras privadas podría evitar que, aunque se conozca la actividad, no se pueda relacionar con un usuario en concreto, siempre que no se proporcione información adicional.

> *At the end of the day, they cannot prove that you are the owner of the private/local wallet's address, and (most likely) nothing bad would happen to you so long as you kept your mouth shut and never admitted you are the owner of the local address* (U54 en U55, 2021).

El segundo consejo más frecuentemente dado en el foro consiste en la compra de la criptomoneda Monero que, al ser de carácter privado, no se puede acceder públicamente al registro de transacciones realizadas y se asegura la privacidad. Aunque puedan cometerse riesgos en la ocultación de la identidad vinculada a una dirección, no podrá conocerse el patrón de actividades completo. No obstante, su utilización tiene que guardar también ciertas precauciones. Aunque se rompa la trazabilidad con la utilización de Monero, la obtención de

una elevada cantidad a través de una casa de cambio con KYC podría levantar sospechas y se podría abrir una investigación (U56 en U57, 2021). Este sería el caso del usuario que, aunque ha decidido utilizar Monero, compra una elevada cantidad empleando una casa de cambio con políticas KYC y posteriormente lo envía a un vendedor que inmediatamente lo convierte en dinero fiduciario en un intercambio KYC (se pone en riesgo la privacidad del usuario (U58, 2021):

> *If let's say you bought exactly 1 XMR at a KYC exchange, and then within 1 hour sent that amount to a vendor, who immediately cashes out at a KYC exchange, it wouldn't take a detective to figure out where the coins came from* (U58, 2021).

Del mismo modo, habría que tener precaución con la cantidad de dinero fiduciario que se extrae o ingresa en transacciones bancarias procedentes de una venta de criptomonedas. Por ejemplo, el ingreso de una cantidad de 10000 dólares podría poner señalar a un usuario como sospechosos y ponerlo bajo vigilancia (U28 en U59, 2021). Si aun conociendo los riesgos de esta actividad se desea realizarla, se tiene que estar preparado para explicar en cualquier momento de dónde vienen tales cantidades de dinero, porque incluso 900 dólares a la semana podrían levantar sospechas (U60 en U61, 2021). Especialmente si se trata de Bitcoin, ya que esta inversión no desaparece nunca de la *Blockchain* y las FCSE u otras autoridades podrían requerir una justificación de la cantidad de criptomonedas Bitcoin obtenidas (U62, 2021).

> *When you keep buying BTC tied to your identity you'll have to be creative if you ever get this question. As long as they can't directly tie the btc's your bought to the drugs you've purchased you should be relatively fine, but still very suspicious. The best thing would obviously be to find an anonymous way to purchase BTC. Have a look if there are any BTC ATM's in your area or give local bitcoin a try* (U63 en U64, 2020).

De esta forma, las estrategias desarrolladas para evitar el riesgo de detección no se centran únicamente en evitar la actividad con un tipo de criptomoneda o la utilización de ciertos servicios. En su lugar, se ofrecen diferentes formas de dificultar que las FCSE puedan relacionar la actividad de una dirección con la identidad de un usuario. Hacer diversas rutas de conversión// no traficar con cantidades demasiado grandes// no mantener todo el registro al completo de transacciones.

Aunque estas estrategias siempre pueden conllevar ciertos riesgos, la comunidad recomienda ser lo más cauto posible y transmite tranquilidad a los usuarios.

> *You'll be fine... you're a VERY small fish in a very big pond. The fact that you're posting shows you learned, so just don't do it again. Nobody is after you for some one-time little order* (U65en U51, 2021).

> *your isp now has a record of you connecting to a monero node, but thats not illegal, so nothing to be worried about* (U66 en U67, 2021).

Por ejemplo, consideran que no suponen demasiado riesgo las cantidades pequeñas de droga adquiridas una sola vez. Exponen que en este caso no se trata de un delito muy grave y que el gobierno y las autoridades no tienen la capacidad para perseguir cada transacción realizada. Por ello, centrarían sus recursos en aquella actividad que revista de una gravedad mayor.

No obstante, mucha gente no es tan experta y cometen errores por los que sí que funcionan estas medidas (U78 en U68, 2021). Esto también ha llevado a que muchos usuarios se muestren escépticos en cuanto a la efectividad de las medidas impuestas para prevenir este tipo de delincuencia, como las políticas de KYC.

> *It literally takes me few hours to get KYC'ed via Homeless person and then another few more to cash out my money. I'm the average joe. How long will it take to the average criminal? It's not like they don't know the term money mule. I will never support this clownery, how come people believe that this is supposed to prevent crime or tax evasion? Hilarious. I will never support this KYC nonsense. It does nothing. It's useless surveillance to track normies, this won't stop criminals. How can someone be this naive?* (U68, 2021).

Hacen referencia a la ineptitud del gobierno, consideran que ese tipo de medidas tiene lugar cuando se elaboran medidas sobre algo de lo que se desconoce (U69 en U68, 2021) y lo acusan incluso de dejar que el crimen pase.

Ante la posibilidad de que se produzca una detección, los usuarios han deliberado sobre la mejor forma de responder a las FCSE en el caso de que sus actividades ilegales fueran descubiertas. Aconsejan, por ejemplo, que si se diera el caso podrían responder con excusas como la rentabilidad de obtener la criptomoneda Monero sobre Bitcoin debido a las estadísticas del mercado:

> *If anyone asks why you are buying monero you could surely just say you heard it was going to be like the next btc so you thought it would be a good idea to invest in buying some. but yea really depends on the scale, if its just personal i wouldn't get too paranoid about the whole thing if i were you, sure keep yourself safe, but if you are just picking up the odd wee thing for yourself don't stress yourself out about the process too much*" (U70 en U64, 2020).

En este mismo sentido, los usuarios también advierten que las autoridades locales tienen una mayor facilidad para obtener información de los usuarios cuando las empresas de conversión de criptomonedas están ubicadas en el mismo país en el que se está realizando la actividad. Por este motivo, aconsejan que, si se tiene la intención de depositar el dinero en una casa de cambio, sería menos arriesgado para la privacidad hacerlo en una empresa extranjera:

> *(...) then I'd suggest cancelling the order if possible, as it is easy for local law enforcement to get information from the companies in the same country* (U71en U72, 2020).

No obstante, siempre se recomienda mejor comprar las criptomonedas con dinero en efectivo a través de servicios como "Localbitcoins" o "Localmonero" o similares y se

desaconseja la utilización de servicios como los mezcladores, *mixers o tumblers* (U71en U72, 2020), casas de cambio como Coinbase o utilizar el dinero directamente en el mercado (U13 en U14, 2020).

En cuanto a las técnicas empleadas por las FCSE para la investigación de este tipo de delincuencia, se han expuesto en el foro diversas formas en las que se desarrollan. De este modo, los usuarios aprenden dichas estrategias y quedan advertidos para actuar en consecuencia y adaptar su actividad ilegal. Una de estas técnicas se conoce como ataque "dust" o "ataques de polvo". El usuario expone que son técnicas empleadas por las FCSE, entre otros, para identificar la asociación de múltiples direcciones a una sola cartera (U73 en U74, 2020) [209]. Por lo general se recomienda que para estar seguro se utilicen diferentes carteras para diferentes usos. No obstante, en el sistema de Monero es difícil realizar este ataque debido a la forma que tiene de oscurecer las entradas y salidas en una cartera.

Sin embargo, la preocupación de los usuarios por la detección de las FCSE no ha quedado limitada a lo anterior, sino que también han deliberado en diversas discusiones sobre la posibilidad de que finalmente consigan hacer Monero trazable (U75, 2020). Aunque esta posibilidad parece estar todavía alejada de la realidad algunos usuarios en el foro han comentado la oferta de gobiernos como el de Estados Unidos que ofrece una recompensa a todo aquel que sea capaz de rastrear transacciones con Monero:

> *I read today the US Government is still offering a bounty of $650,000 to anybody who can work out how to trace XMR transactions. They're still pretty private. Unlike bitcoin.* (U76 en U79, 2021).

> *The IRS was offering like 625k for anyone who could break monero last year I don't know how successful they were* (U35, 2021).

Conocidas empresas de análisis de la *Blockchain* como "Ciphertrace" o "Chainalysis" suelen colaborar con las autoridades en la identificación de direcciones sospechosas, así como en la identificación de los usuarios. Sin embargo, todavía no se conocen casos de éxito en los que algunas de estas empresas hayan conseguido comprometer la privacidad de Monero:

> *Monero has been placed under scrutiny by multiple organizations, who have been unable to compromise the private nature of Monero. This includes Ciphertrace, Chainalysis, and the United States IRS. Should any future attacks succeed, Monero would attempt to develop a solution, and likely succeed* (U77, 2020).

[209] Este ataque consiste en enviar una pequeña cantidad de criptomonedas a una de las direcciones sospechosas. Cuando el usuario quiera enviar la cantidad de una cartera hacia otra, si elige la opción "enviar todo" enviará la cantidad que tenía prevista junto con la cantidad enviada anteriormente (U73 en U74, 2020).

Todavía no se cuenta con pruebas de ninguna transacción que haya sido trazada y sea el único motivo por el que se ha detenido e imputado a alguien por un delito:

> *CipherTrace has not provided a single piece of proof or transaction they have traced. There has never been a conviction, in a court of law, of someone who exclusively used Monero AND did''t snitch. Of course monero is not going to be secure forever, but I think it will be the top privacy coin for at least another 5-7 years* (U80 en U75, 2020).

Sin embargo, aunque esto fuera posible, de la misma forma que como se ha comentado con Bitcoin, no se esperaría su utilización para todas las transacciones realizadas (U81 en U57, 2021). El esfuerzo en cuanto a recursos como el tiempo dedicado y el dinero invertidos son elevados, por lo que se centrarían en aquella actividad sospechosa que revistiera de mayor importancia (U46 en U82, 2021), no en el usuario medio que adquiere pequeñas cantidades de droga en un mercado (U83 en U18, 2021).

Rutas Para Mantener el Anonimato y/o la Privacidad Utilizando las Criptomonedas. La comunidad del foro recomienda mayormente la utilización de la criptomoneda Monero para mantener el anonimato y la privacidad. No obstante, esto no supondrá la evitación en cualquier caso de todos los riesgos posibles para la privacidad:

> *That being said, Monero (or privacy coins) will not 100% protect you from being exposed to law enforcement. You should still take proper precaution when you're buying or selling in the Darknet (...)* (U58, 2021).

Será necesario considerar una serie de precauciones antes de la utilización de esta criptomoneda para la comisión de un delito.

Según lo expuesto en el apartado anterior, la mejor forma de disminuir el riesgo de detección en este tipo de criminalidad es evitando el vínculo entre la actividad realizada y toda información personal que pueda relacionar una dirección con una identidad. Para ello, se recomienda dificultar la trazabilidad de esta actividad a través de su fragmentación, especialmente en aquellos casos en los que se va a utilizar la criptomoneda Bitcoin. Esto se le conoce como ruta o *path* y están formadas por una serie de pasos que siguen los usuarios antes de utilizar las criptomonedas en el desarrollo de una actividad delictiva o posteriormente a esta para limpiar el rastro delictivo. Pueden suponer la conversión entre diversas criptomonedas, así como la utilización de herramientas que permitan conseguir una mayor privacidad. Pude consistir, por ejemplo, en la compra de un tipo de criptomoneda, la posterior conversión a otro tipo, el envío de este a una cartera privada, la posterior conversión de nuevo a otro tipo de criptomoneda y finalmente la utilización en un criptomercado. Así, al fragmentar la actividad de un mismo usuario se dificulta el rastreo de su actividad al completo.

Todo ello ha motivado que muchas de las consultas del foro se llevaran a cabo por sujetos que, aunque eran conocedores de la privacidad de Monero y otras tecnologías relacionadas, preguntaban sobre la mejor ruta para mantener la privacidad y por tanto la seguridad de su actividad. Este tipo de discusiones comienza habitualmente con un usuario que muestra una ruta y pregunta a los miembros del foro si resulta adecuada para su privacidad. También se encuentran consultas de algunos usuarios que, una vez han tomado las medidas para que su actividad se desarrolle de forma anónima, prefieren consultar si la ruta tomada ha sido la adecuada. Por ejemplo, sobre la configuración de la cartera de Monero en Tails (U84, 2020). Las respuestas recibidas comentan las soluciones propuestas o proponen otras que resultarían más efectivas.

De forma general, las rutas más recomendadas comienzan con la obtención de la criptomoneda Bitcoin, su cambio a la criptomoneda Monero y la utilización de esta en el mercado delictivo. O bien, si el mercado no acepta Monero, pero sí Bitcoin, añaden a la ruta anterior la opción de volver a cambiar a Bitcoin antes de usar en el mercado.

Hay usuarios que aseguran que no es necesario seguir una ruta de conversión excesivamente compleja y larga, ya que la conversión a Monero, por sus características permite conseguir que la actividad sea difícil de rastrear (U85 en U86, 2021). Sin embargo, en el foro se ofrecen multitud de alternativas que añaden otros pasos como el depósito en carteras privadas o públicas, la utilización de cursos en TOR, la utilización de diferentes intercambiadores y la obtención de otras criptomonedas alternativas. A continuación, se muestran las rutas más frecuentemente recomendadas:

- BTC (ID) – cartera web superficial – XMR – cartera Tails – Mercado (U64, 2020).
- XMR (Kraken) – cartera XMR GUI (web superficial) – cartera XMR GUI (Tails) – mercado[210](U64, 2020).
- BTC (Kraken) – cartera Electrum (web superficial) – Cartera Tails (TOR) – XMR (Elude) – cartera Tails – mercado (U64, 2020).
- BTC – cartera Cake – XMR (Cake) – Cartera Monero (Tails) – mercado (U87en U64, 2020).
- BTC – cartera Cake – XMR – BTC (Cake en Tails) – mercado (U87en U64, 2020).
- BTC (Localbitcoins) – mezclador (cartera online) – cartera Tails – XMR (Unlink) – cartera XMR GUI – mercado (U88, 2020).
- BTC (Exodus) – XMR (Cake) – BTC (Cake) – cartera XMR GUI (Rails) – mercado (U89 en /U88, 2020).
- LTC – cartera Electrum – XMR (Kilos o Elude) – Mercado (U90en U91, 2021).
- BTC (tarjeta crédito) – Cartera Electrum pc (total dinero) – Cartera Electrum Tails (parte dinero) – XMR (Feather) – Mercado (U92, 2021).
- BTC (Exodus) – XMR (cartera Cake) – cartera XMR GUI (Tails) – Mercado (U89 en /U88, 2020).
- LTC – XMR cartera temporal – cartera principal – eliminar cartera temporal (U17 en U18, 2021).
- BTC (ATM) – cartera – XMR (Elude o Kilos) Cartera XMR – mercado (U93 en U94, 2021).
- BTC (ATM) – cartera teléfono – cartera pc – XMR (Elude, Localcripto o bisq.network) (U95en U1, 2021).

- ETH – XMR – cartera (U97 en U96, 2021)

La mayoría de las rutas comienzan con la obtención de la criptomoneda Bitcoin a través de diversas opciones de compra como casas de cambio, carteras privadas, servicios *peer-to-peer*, etc. Posteriormente, se convierte a Monero a través de diversos tipos de carteras como Exodus o casas de cambio como Kraken y LocalMonero entre otros. Al final de la ruta se encuentra el mercado delictivo, para el que se recomienda no enviar pagos directamente desde una casa de cambio (U95 en U1, 2021).

De esta forma, no se prohíbe totalmente la utilización de Bitcoin, sino que se recomienda seguir una serie de medidas para evitar la detección debido a la transparencia de su *Blockchain*. Por ejemplo, si se compran los bitcoins en casas de cambio públicas es recomendable seguir un proceso de blanqueo de las monedas (U97 en U12, 2020). No obstante, este proceso no debería consistir en el traslado reiterado de diferentes cantidades de Bitcoin de una cartera a otra, ya que esto no impide que esta actividad siga siendo trazable desde la *Blockchain* de Bitcoin (U63 en U64, 2020). Además, utilizar el monedero a través de TOR evita el rastreo de la IP y que se pueda revelar la ubicación.

De forma general, es recomendable cambiar la criptomoneda Bitcoin a Monero para utilizar este último en el criptomercado. Además, aunque comprar Monero con dinero *fiat* no es una actividad ilegal, también se recomienda no unir directamente la identidad de una persona con una cuenta Monero antes de usar este en el mercado (U63 en U64, 2020). En este caso, las FCSE podrían considerarlo como una actividad sospechosa.

Tipo de Criptomoneda Preferente. En la actualidad existen más de mil tipos de criptomonedas diferentes. En este sentido, es habitual que se realicen consultas sobre cuál es la mejor criptomoneda para evitar tanto como sea posible la detección del delito:

> *Which cryptocurrency would you all say is the best? id say moreno is the best personally but you also cant beat bitcoin and how reliable it is, thought?* (U98, 2020).

Las criptomonedas Monero (XMR) y Zcash (ZEC) son privadas, mientras que Bitcoin (BTC) y Ethereum (ETH) son transparentes. Varios usuarios han señalado la importancia de utilizar criptomonedas privadas en lugar de otras con mayor disponibilidad como Bitcoin (U58, 2021)[211]. En la última, el registro de transacciones tiene un carácter público, así que

[211] Las criptomonedas privadas son aquellas que mantienen la privacidad por defecto. Es cierto que se puede conseguir que criptomonedas como Bitcoin puedan ser mucho más anónimas y privadas de lo que son, pero se recomienda no asumir estos riesgos. Otras criptomonedas como Dash no ofrecen esa opción como defecto, sino

una vez se vincula una dirección Bitcoin con una identidad se podrá conocer todo el historial de transacciones realizadas[212].

No obstante, pese al elevado número criptomonedas que existen, las consultas realizadas en el foro giraban en torno a la elección entre Bitcoin y Monero. La primera de ellas porque es la más conocida y ampliamente utilizada en el mundo de las criptomonedas. La segunda porque garantiza el respeto por la privacidad de la actividad del usuario.

De forma general, se recomienda la utilización de la criptomoneda Monero sobre Bitcoin. Se considera a Bitcoin como una de las criptomonedas más rastreables que existen, que además registra las transacciones de forma permanente y permite realizar el rastreo con posterioridad:

> *You should never use Bitcoin on the Darknet markets. Nobody should be using Bitcoin anymore. It's unsafe and the most traceable means of exchange the world has ever seen. Every transaction is recorded forever. Even if the process right now is safe it can be broken later and then everyone gets fucked. Just use Monero and fuck Bitcoin* (U73 en U74, 2020).

> *bitcoin in actually very traceable. Best thing to do is to use monero. If you have to buy btc, even with a know your customer exchange, just swap for monero with a service like kilos or elude, transfer to your own monero wallet, then to the market. Monero is untraceable and safest way to do it* (U93 en U94, 2021).

Por todos estos motivos se recomienda cambiar esta criptomoneda a Monero, que dispone de la tecnología necesaria para garantizar un anonimato real y la privacidad de la actividad, solo el emisor y el receptor pueden determinar dónde es enviada la transacción:

> *(…)Monero provides a true anonymity. Monero uses ring signatures, Ring Confidential transactions, and stealth addresses. Ring signatures hide information about the sender. Ring Confidential Transactions, Alice can send Bob some Monero, and the only people that will ever know the amount sent will be Alice and Bob. Although the transaction is visible on the Blockchain, there is no way to determine the amount transacted. Stealth addresses is used by the receiver to display incoming transactions. This method means that while a transaction is recorded on the Blockchain, only the sender and the receiver can determine where the payment was actually sent (…)* (U41, 2021).

Pero su trazabilidad no es el único motivo por el que se desaconseja la utilización de Bitcoin. Sus elevadas tasas de conversión y la atención que le prestan las FCSE son otros de los motivos que se exponen:

> *Why not, but I wouldn't use btc if i were you. Stick to xmr as much as you can. Btc is an oudated currency, hight fees, LE is all over it, pushing mixer, anonymous wallet, exchange to track down users* (U99 en U84, 2020).

> *XMR is fast, cheap and private, in my opinion its better than bitcoin. Bitcoin conversion and withdrawal fee is too high, you buy 10K worth BTC from an exchange or P2P and realize it just costs*

---

que debería ser configurada, por lo que tampoco se recomienda, ya que puede haber usuarios que no sean capaces de configurarla (U58, 2021).

[212] Un ejemplo de esto se puede ver en el popular caso de "Dread Pirate Roberts", más conocido como Ross Ulbricht, creador del criptomercado *Silk Road*, que una vez detenido por el FBI no pudo ocultar las transacciones que había realizado con Bitcoin a lo largo de toda su actividad.

> *2K to withdraw to your personal wallet. Don't talk about transaction or network fee. Its a good investment. Don't use it to buy drugs* (U100, 2021).

Además, a lo largo de la historia de Bitcoin se han presentado una serie de fallas en su sistema que han comprometido el anonimato y su integridad. Posteriormente estos errores se tomarían como base para la creación de la criptomoneda Monero. Por este motivo, muchos usuarios del foro consideran que la criptomoneda Monero es el futuro de las criptomonedas y que supone todo aquello que debería haber sido el proyecto Bitcoin:

> *Monero is what Bitcoin should have been from the start* (U80 en U75, 2020).

Por todo ello, la criptomoneda más frecuentemente recomendada en el foro es Monero. se aconseja la utilización de Monero para el desarrollo de toda actividad para la que se desea ocultar su rastro, recomendando que no se utilice Bitcoin o bien que se reserve para otro tipo de actividades legales como son las actividades de inversión:

> *Bitcoin is great for legit investments but use monero if you wanna have nothing connected to you* (U98, 2020).

Sin embargo, en algunas ocasiones ciertos negocios prefieren ofrecer Bitcoin como sistema de pago en lugar de Monero, porque consideran que esta última no es una criptomoneda que pueda ser ampliamente utilizada fácilmente (U101 en U102, 2020). Las respuestas a esto siguen la línea de señalar esta decisión como poco inteligente debido a la transparencia de la *Blockchain* y a la capacidad que muestra Bitcoin para que la actividad sea rastreada.

Se considera que Monero es una criptomoneda muy segura, sin embargo, esto no significa que su utilización en todo caso vaya a suponer la evasión de las FCSE. Por ejemplo, se puede comprometer la privacidad si se compra una elevada cantidad en Monero en una casa de cambio con políticas de "conoce a tu cliente" y más tarde se envía este dinero a un vendedor que inmediatamente la convierte en dinero fiduciario en un intercambio con las mismas políticas KYC (U58, 2021).

El riesgo de detección por parte de las FCSE ha llevado a que muchos usuarios consulten sobre la posibilidad de rastreo de Monero y la trazabilidad de su actividad al completo (U75, 2020). No obstante, de forma general los usuarios se muestran escépticos a que esta posibilidad llegue a ocurrir. Consideran que las tecnologías que conforman el sistema de Monero como *ring signatures, stealth addresses* y las continuas actualizaciones de sus algoritmos de encriptado, etc. (U75, 2020) se presentan como elementos robustos y seguros capaces de mantener la ocultación de la actividad y por tanto la protección de la privacidad.

Además, en relación con las grandes empresas de análisis de la *Blockchain*, los usuarios han señalado en varias discusiones que Ciphertrace y Chainalysis no han sido capaces todavía de comprometer la privacidad que otorga Monero (U80 en U75, 2020; U77, 2020). Además, hasta la fecha todavía no se ha conocido ningún caso o persona que haya sido enjuiciada y llevada a prisión únicamente por haber sido descubierta su actividad ilegal realizada con Monero (U80 en U75, 2020). De esta forma, todavía se espera que la criptomoneda sea segura contra la detección de las autoridades.

No obstante, aunque la mayoría de las discusiones en el foro giran en torno a la utilización de Bitcoin o Monero, también son mencionadas otras criptomonedas alternativas o *alternative coins* (altcoins). Se presentan como una alternativa que permite solventar algunos de los inconvenientes de Bitcoin o Monero en la utilización con fines ilícitos. En este caso, la criptomoneda alternativa más comentada en el foro es Litecoin (LTC), que ha sido consultada por algunos usuarios:

> *I see a couple vendors accept litecoin, is this just as secure as BTC??. Using LTC im guessing i can save on transfer fees alot . I kno i should use xmr and i guess i will when the time comes i go back to WHM* (U103, 2021).

De forma general, se recomienda la utilización de Litecoin como una alternativa a las elevadas tarifas de servicio que presenta Bitcoin, además de una mayor rapidez para completar las transacciones:

> *(…) the other way could be buy litecoin (you can also use bitcoin but its network fees is much higher) at any trading platform transfer it to cake wallet and then convert it to monero and use it anyway you want... i prefer litecoin because its transactipn fees is much lower and much faster transfer (…)* (U104, 2021).

> *stop buying bitcoin. the fees are high & its slow. Buy LTC and convert to XMR. LTC withdrawal fees sit at 0.001 LTC which is sitting at a pretty low 23 cents atm. youll barely lose anything on the exchange* (U105).

Litecoin es considerada como una criptomoneda de carácter no privativo, es decir, que en cuestión de anonimato es comparable a Bitcoin por la transparencia de su Blockchain. Por ello, una vez se ha obtenido Litecoin la comunidad del foro recomienda convertirlo a Monero para volver a garantizar la privacidad de la actividad:

> *BTC and LTC are the same in terms of security and traceability. So yes using LTC will save fees and be no different than BTC* (U106 en U103, 2021).

> *some yes but u can buy litecoin bitcoin or etherum most , if you can choose buy litecoin because lowest exchange fee and just change it to monero in some application* (U107en U108, 2021).

> *In my opinion you should buy LTC.Very very low fees,fast transactions.Then convert it to XMR.You can use temporary wallets for extra security. LTC>Exchange to xmr (temp wallet)>To your main xmr wallet. then delete the temporary wallet.Dont forget to backup your temp wallet seeds just in case. You can swap it on our Kswap service on Kilos* (U17).

En este sentido otros usuarios afirman que, aunque los precios puedan variar excesivamente, Litecoin no es tan ventajoso como se cree en comparación con Monero.

> *the transaction fees for XMR are already very very low. About the same as litecoin. There is no benefit to using litecoin over XMR. as litecoin is easily traced just like bitcoin* (U103, 2021).

Utilización de Tecnologías Adicionales Para Incrementar la Privacidad.

Junto con la utilización de las criptomonedas, aquellos usuarios interesados en la comisión de delitos han empleado otras herramientas o soluciones para asegurar su anonimato y la privacidad de su actividad. Entre ellas, están el uso de los mezcladores o *mixers*, los *tumblers* y las carteras privadas.

Los *mixers* o mezcladores permiten oscurecer el rastro de las transacciones mediante el mezclado de las criptomonedas de los usuarios que tienen este objetivo. Desde su aparición se consideraron como servicios de utilidad para conseguir una capa extra de privacidad en la comisión de delitos con criptomonedas. De esta forma, se ha situado como un tema frecuentemente tratado en las discusiones del foro:

> *whats the best and safety way to tumble coins? im kind of a noob so i need a little bit insight anything will help* (U109, 2020).

Aunque algunos usuarios consideran la utilización de un mezclador como uno de los pasos en sus rutas de conversión, no se trata de una tecnología ampliamente utilizada, siendo además objeto de numerosos debates en las discusiones del foro:

> *If you cannot hold monero for some reason (like hard drive size requirements stopping you from running a monero node or something like that) only then should you use a bitcoin tumbler (...)* (U110 en U109, 2020).

> *Bitcoin mixers are a waste of time and money. it was designed to be traceable. you'd be better off converting between different coins but be mindful what service you use* (U55, 2021).

Del estudio de las discusiones se ha visto que en los últimos años existe cierta desconfianza al uso de los mezcladores por diversos motivos. Uno de ellos es que algunos usuarios aseguran que ciertas empresas de mezcladores han trabajado o trabajan junto con las FCSE:

> *Remember that's one mixer worked with LE month ago, to burst user down. I wouldn't trust any mixer at this point, also simply using one will get your btc adress red flagged* (U99 en /U88, 2020).

Exponen que las direcciones vinculadas a un mezclador son marcadas en rojo por las FCSE. Una vez que alguna de estas direcciones se relacione con cualquier casa de cambio con políticas de KYC se detectaría la actividad realizada y se podría trazar al completo:

> *Look for the news, October mixer bust, as exemple. Also using any kind of anonymous service, such as mixer, will get your adress flagged, so as soon as you re use this adress and linking it to any exchange or KYC related services, you got flagged and linked* (U99 en /U88, 2020).

Otro de los motivos para su desconfianza son los casos de "estafa de salida" que se han registrado en los últimos años en las que si las carteras son custodiadas pueden suponer la pérdida de las monedas invertidas:

> *There's no reason to use a custodial tumbler anymore. The operators tend to exit scam with user coins* (U109, 2020).

Muchos usuarios han justificado el aumento de la utilización de esta tecnología como una consecuencia del desarrollo de herramientas de rastreo y violación de la privacidad por parte de empresas como "Elliptic":

> *At the end of the day one can only conclude and agree that Governments and Analysis Firms themselves are the ones to blame. Mixers have for the most part grown in prominence thanks to increased privacy violating and tracking technologies from firms like Elliptic* (U111, 2020).

Por todos estos motivos, se desaconseja la utilización de los mezcladores. En su lugar, se proponen otras formas de conseguir una mayor privacidad empleando rutas de conversión otras herramientas como las carteras privadas.

Las carteras privadas son aquellas que permiten oscurecer el rastro de la actividad realizada permitiendo el mezclado de las criptomonedas depositadas entre diferentes carteras de este tipo. Se han relacionado con la actividad criminal porque dificultan la identificación de los usuarios. Aunque se envíe una cantidad de dinero a un mercado desde una cartera, no se podría obtener la identidad del usuario a menos que la persona desvele su identidad:

> *The thing with sending to a private wallet first is IF it came down to a court of law, there would be no way for anyone to prove that you are the owner of the private/local wallet you sent your funds to* (U54 en U55, 2021).

Según un informe de la empresa de análisis de Blockchain "Elliptic", alrededor del 13% del delito cometido con Bitcoin es blanqueado a través de la utilización de carteras privadas, lo que ha supuesto el crecimiento de un 11% con respecto al año anterior. Esta empresa estima que la cifra representa más de 160 millones de dólares procedentes de mercados de la Darknet, robos y estafas (U111, 2020).

Algunos ejemplos son las carteras Wasabi[213] o Samourai[214] (U111, 2020[215]). Son consideradas como carteras "no custodiadas", lo que da la habilidad de conectar con un nodo completo propio y preservar la privacidad sin confiar en terceras partes. El propósito de estas herramientas no es servir para su utilización para el delito, tal y como ha expuesto Ricardo Masutti portavoz de Wasabi wallet (U111, 2020).

***Cashout* o Retiro de las Criptomonedas.** En el ámbito de las criptomonedas el proceso de *cashout* o retirada consiste en la materialización de los fondos obtenidos en estas monedas virtuales a través de su conversión a dinero fiduciario en efectivo o digital.

Constituye un paso importante para todas aquellas personas que han empleado las criptomonedas en la comisión de un delito y que desean utilizar el beneficio obtenido fuera del ámbito digital. Pero al mismo tiempo presenta un elevado riesgo para la identidad del usuario y su privacidad ya que establece de nuevo una relación entre la actividad digital y el mundo no virtual.

Las políticas de prevención de este tipo de delitos tienen como objetivo establecer un vínculo entre la identidad real de los usuarios y la actividad desarrollada con las criptomonedas por lo que este paso será también de gran importancia para las autoridades encargadas de su detección. Por este motivo, la realización de este paso de la forma más segura y efectiva posible es uno de los temas más frecuentemente tratados en el foro:

> *Bonjour, je recherche a retirer mes crypto en cash (liquide) sans etre tracer avait vous une solution? (Stop Troll) Merci* (U113, 2021)

> *how to anonymously cash out btc in EU? 1 million eur. what are the ways to cash it out from offline wallet?* (U112, 2021).

[213] Consiste en una tecnología que permite el desarrollo de "CoinJoin" sobre la red Tor. Esto consiste en que varios participantes combinan sus monedas (UTXO en específico) creando una gran transacción con múltiples entradas y múltiples salidas. De esta forma, no se puede determinar qué entrada pertenece a qué salida, dificultado a partes externas rastrear dónde se compró una moneda o dónde se envió Para llevar esto a cabo es necesario que varias personas que deseen realizar una transacción se pongan de acuerdo para realizar una transacción conjunta. https://wasabiwallet.io/

[214] Se trata de una cartera que además de ofrecer las prestaciones habituales para este tipo de tecnología, también garantiza la privacidad del usuario. Cuenta con diversas prestaciones que le permiten conseguir esto. La forma en la que garantiza esto consiste en que una vez se realiza una transacción con esta cartera, el envío no se realiza directamente hacia la cartera destino, sino que pasa por diferentes carteras antes de llegar a su receptor. A diferencia de otros servicios relacionados, esta cartera no hace la trazabilidad de las transacciones imposible, sino más costosa en cuanto a tiempo y dinero https://samouraiwallet.com/

[215] Según este Usuario, en su hilo de discusión plantea que las carteras que garantizan una mayor privacidad que las ordinarias están siendo utilizadas por criminales que desean ocultar su actividad y proteger su identidad. Plantea también cuestiones interesantes como que por ejemplo, los servicios de CoinJoin como puede ser Wasabi, podrían ser conocedores del principal uso que se le está dando a sus servicios entre la esfera criminal, pero que pretenden seguir obteniendo un beneficio mediante los costos de las transacciones realizadas, sin importar la procedencia.

Del estudio del foro, se han obtenido dos formas de realizar el retiro o *cashout*. La primera de ellas consiste en su conversión a dinero fiduciario, ya sea de forma física o en digital. La segunda consiste en la conversión a bienes o productos que se obtienen utilizando las criptomonedas como forma de pago.

En el primer grupo son frecuentes las recomendaciones sobre cuentas bancarias, cajeros automáticos y métodos de compraventa de criptomonedas P2P. En relación con las cuentas bancarias, el usuario puede obtener una cuenta bancaria que pertenece a otra persona o que ha abierto utilizando una identificación falsa. Este método presenta mayores dificultades porque requiere de estrategias de evitación de las medias de seguridad como el factor de doble autentificación. También puede tenerse acceso al dinero a través del robo o falsificación de la tarjeta de crédito o débito mediante *carding.* En cualquier caso, una vez se dispone del dinero, se utilizará para comprar criptomonedas que posteriormente convertirá a efectivo.

En este último paso será necesario utilizar una ATM para retirar el dinero en efectivo. Son muy comentadas, aunque no son el método preferido entre la comunidad por los inconvenientes que ocasionan sus altas tasas de retirada en efectivo y sus medidas de seguridad por políticas KYC que comprometen la privacidad de los usuarios:

> *What I usually do is just withdrawing from BATM but: 1- I feel like there are ways way cheaper than spending 10% on fees for withdrawing; 2- I don't really feel "secure" withdrawing from BATMs because of the cameras and the last thing I want is being retraced to a TX where the ATM "caught me in 4K"* (U114, 2021).

Además de las medidas que se pueden encontrar de forma física en la ATM, se deberán tener en cuenta las relacionadas específicamente con la retirada de efectivo como son los límites de dinero a partir de los cuales se requiere la aplicación de las políticas de KYC:

> *Si il y a des limites italie 2000 € par tickets et espagne 2500€ (tu peux en faire autant que tu veux). No KYC en dessous de la limite (c'est ce qui permet de faire plusieurs tickets)*. Au dessus, pas de KYC ils te renvoient les coins. Attention a rester toujours en dessous.Si tu as 10 ou 20k a sortir fais autant de tickets que nécessaire (U115 en U113, 2021).

En algunas ocasiones será necesaria la utilización de identificación falsa para poder retirar el dinero de forma segura. Por ello, se recomienda que previamente al paso de *cashout* el usuario tiene que “limpiar” las monedas siguiendo alguna de las rutas comentadas en apartados anteriores. Se pretende conseguir que, aunque se descubra la identidad real del sujeto no se permita el rastreo de la actividad ilegal.

No obstante, la forma más recomendada en el foro para la retirada de los fondos es la venta de las criptomonedas a través de un particular. Esto supone la realización de forma inversa del proceso descrito en el apartado de obtención de criptomonedas a través de una

compra P2P. Se vuelven a mencionar las plataformas "LocalMonero" y "LocalBitcoins" y el envío de dinero en efectivo a través del correo postal:

> *I don't do crypto->fiat so I can't give much advice there, but your best bet for monero is to go to Local Monero, the. onion is on DDF, and do cash/xmr by mail. I can't personally vouch for it, but bisq.network is peer to peer for BTC and they don't have kyc as far as I can tell* (U116 en U6, 2021).

De esta forma, el usuario ofrece en la plataforma la venta de una cantidad de criptomonedas, estableciendo las condiciones que prefiere para la compra (transferencia bancaria, dinero en efectivo a través del correo, etc.). También se han encontrado comentarios que hacen referencia a la compraventa entre particulares utilizando cuentas de la empresa "Paypal", en la que un usuario recibe en su cartera las criptomonedas y el otro recibe en su cuenta "Paypal" el dinero fiduciario correspondiente (U117, 2021).

En cuanto al segundo grupo, también se ha comentado en el foro la posibilidad de comprar bienes o productos con las criptomonedas obtenidas de una actividad ilícita. Aunque es considerada como una de las mejores formas de realizar este proceso, será necesaria mucha preparación y contar con buenas medidas de seguridad (U43, 2020).

Se comenta sobre una amplia variedad de productos como tarjetas regalo, joyas u otro tipo de inversiones de valor:

> *Many gift card websites accept crypto. Make sure it's clean prior (...)* (U28 en U118, 2021).

> *Ola amigo! Achète des bijoux avec tes bitcoins, pas plus de 5000 euros et go vers les exchanger partout en france pour échanger ça contre du liquide ou des virements propre. Les bijoux ne sont taxé qu'à 6 % et les pièces d'or à zéro mais ça dépend lesquel, par contre l'or c'est 11,5% de taxe ça pique. Ciao!* (U113, 2021).

Son frecuentes también los comentarios sobre páginas como "Craiglist" en las que adquirir los artículos (teléfonos de gama alta, ordenadores portátiles, productos electrónicos caros más pequeños, etc.) utilizando criptomonedas como forma de pago (/u/toshiba666 en U114, 2021). De esta forma, una vez se dispone de los bienes adquiridos se ofertan en el mercado legal para obtener dinero fiduciario ya sea en efectivo o en digital. Se recomienda no poner en venta los productos adquiridos en grandes plataformas de venta como Amazon, Apple, etc. (U43, 2020).

La retirada de los fondos obtenidos con criptomonedas es un paso clave en toda ruta de conversión tras su utilización en actividades delictivas. Por este motivo son muy codiciadas las discusiones en las que se comentan formas de llevar a cabo esta actividad de la forma más segura y efectiva para el usuario. Sin embargo, los usuarios del foro, que son conocedores del valor de estos comentarios exponen que no será fácil encontrar estos métodos de forma explícita en el foro:

> *This is what every carder is looking for, so unfortunately nobody will tell you his method. You'll have to find a method or a target website by yourself or have to pay to have the information* (U119 en U120, 2021).

Entre ellos, un usuario consulta sobre cómo se podría realizar este proceso empleando un teléfono desechable (U121, 2020). En este sentido se recomienda la opción de comprar números de verificación online antes que utilizar una cuenta bancaria o tarjeta de débito.

Enmendar el Riesgo de Detección. Los foros de la *Darknet* suelen constituir un espacio en el que hay disponible una gran cantidad de información para aprender cómo desarrollar una actividad delictiva de la forma más eficaz y efectiva posible. Sin embargo, puede suceder que durante el desarrollo de su actividad en la *Darknet* algún usuario cometa un error que suponga un riesgo para la privacidad de su actividad o su anonimato. En estos casos son los propios usuarios afectados los que advierten el riesgo de ser detectados por las autoridades además del riesgo de perder su dinero (U122, 2020) y escriben en el foro consultando su gravedad y la forma en la que podrían solucionar la situación. De forma habitual, estas conversaciones comienzan con el usuario describiendo la situación y realizando la consulta a la que responden el resto de los miembros del foro. Los errores cometidos y por tanto las situaciones recogidas son muy variadas. Por ejemplo, comprar un producto ilegal de un mercado de la *Darknet* utilizando directamente una cartera verificada, es decir, que se obtuvo aportando algún tipo de dato identificativo:

> *Hello. What if somebody made a mistake and bought something illegal from the Darknet with their own verified wallet. Is there any way to kill the wallet / change the wallet to make it look like it belongs to a dead person? So the person who bought the stuff doesn't get arrested?* (U82, 2021).

En este caso el usuario consulta si existe alguna forma de eliminar la cartera en cuestión o realizar algún tipo de cambio que dificulte su utilidad. Si se realizó una compra con una criptomoneda de carácter no privativo se relacionó directamente una cartera con datos personales con un mercado delictivo. En el caso de que las autoridades intervinieran el mercado podrían tener acceso a la cartera de este usuario y conocer su identidad.

Otro error similar al anterior sería el de un usuario que compra criptomonedas directamente al criptomercado en el que las usaría:

> *So, I made a huge mistake earlier this day by ordering bitcoins directly to a Darknet site (200 dollars) from (copenhagenbitcoins) (dont flame me. I know Im a idiot). The order has not gone accepted yet though. Are there a big risk of me getting busted or is it common they simply just deny me the coins?* (U72, 2020).

En este caso se podría establecer una relación directa ente la billetera de la persona que ha comprado las criptomonedas y el mercado. De la misma forma que en la situación

anterior, si el mercado es intervenido por las autoridades, se podría conocer la billetera del sujeto y sus datos.

Asimismo, se podría establecer una relación con el usuario en la situación en la que compra criptomonedas utilizando una cartera personal y las envía directamente y sin mezclar a una cartera "sucia" que utiliza para gestionar su actividad delictiva en la *Darknet*:

> *hey guys i bought btc from an exchange and usually i would use coin tumbler but i accidentally did not copy the tumbler address and sent it to the dirty wallet i use for Deepweb transactions . how bad is it ? can someone see all the transactions i made with the dirty wallet ?? . i asssumed since it happenned already i sent from the dirty wallet to the tumbler to another dirty wallet . i will not use any of these wallets again but can someone tell me am i in danger ??* (U123, 2021).

El usuario afectado en este caso, de forma similar a conversaciones anteriores, pregunta en el foro si es grave el error y si está en peligro o si se podría conocer toda la actividad delictiva que ha realizado con su cartera "sucia".

Muchos de ellos se han mostrado arrepentidos por los errores cometidos como, por ejemplo, aquellos que, aun conociendo los riesgos a los que se exponían, utilizaron la casa de cambio "Coinbase":

> *I bought a small amount of weed on coinbase one time (I know, stupid to use coinbase*).*Could I use coinbase for clean btc investment, and then LocalBitcoins for drug money? Is it suspicious/compromising to have my identity linked to both larger amounts of BTC from one site, as well as a different btc site where I buy smaller amounts for Darknet use? (…)* (U12, 2020).

Las respuestas de los lectores en las discusiones suelen agruparse en dos temáticas. La primera de ellas es intentando aconsejar a la persona para enmendar el error cometido o explicarle la gravedad o la irrelevancia de la situación. La segunda consiste en reprochar al usuario su conducta a través de insultos, burlas, humillaciones u otro tipo de comentarios que pretenden ponerlos en evidencia y hacer ver su incapacidad e ineficacia en esta materia considerando que las dudas o consultas realizadas son cuestiones básicas para aquellos usuarios más especializados[216]. Un ejemplo de ello se puede ver en la respuesta de un usuario al comentario de un sujeto que compró Bitcoin en una casa de cambio con políticas de KYC y lo usó directamente en un criptomercado (U124 en U12, 2020):

> *(…) It took me over 1000 hours of research and preparation before I started doing my illegal hustle. But then you got dudes like you who just buy drugs straight from their coinbase accounts!?!?!? Idk is it confidence or big balls or something?? (…)* (U124 en U12, 2020).

2. Utilización de las Criptomonedas Para Cometer Delitos

El anonimato y la especialización de su contenido convierten a los foros en un espacio proclive a consultas sobre la forma más eficaz de cometer un delito. En específico en la

[216] Para más información sobre esto consultar el apartado de "quejas" de este capítulo.

utilización de criptomonedas, se refiere a la forma de obtener un mayor beneficio por su actividad ilegal o al desarrollo de esta de una forma rentable sin la detección de las autoridades.

Por lo tanto, en este apartado se incluyen aquellas discusiones que se centran en la comisión de delitos en específico. En primer lugar, se presenta un apartado sobre las explicaciones y consejos que se muestran en el foro para desarrollar cierto tipo de delitos. Puede tratarse tanto de ciberdelitos como de delitos de carácter tradicional, pero ambos tienen en común que en algún punto utilizan criptomonedas. En segundo lugar, se incluye un apartado relativo a la forma de operar en los criptomercados delictivos, en concreto a la utilización de las criptomonedas en estos (utilización, formas de pago, cantidades adecuadas, mercados recomendados, etc.). Las peculiaridades de estos negocios ubicados en la *Darknet* requieren de un apartado específico en el que se traten aquellos aspectos de la comisión del delito que pertenecen especialmente a este entorno. El último apartado hace referencia a los negocios que surgen en relación con la utilización de las criptomonedas por parte de otras personas para cometer delitos.

Comisión de Delitos en Específico. Las criptomonedas se pueden utilizar durante el desarrollo de una gran variedad de delitos. Por ello, muchas de las consultas realizadas en el foro tratan diversas cuestiones de la utilización de esta tecnología en determinados delitos. El objetivo es conocer todos los detalles de su desarrollo de forma que el usuario pueda obtener el máximo beneficio posible y evitar la detección de la actividad.

Se han encontrado algunas discusiones sobre delitos de fraude en relación con la venta de determinados productos falsificados, por ejemplo, relojes (U125, 2021). Se consulta la viabilidad que tendría la venta de este producto en la *Darknet*:

> *Are counterfeit watches something that would be worth selling on the Darknet. Considering buying a vendor bond and wondering if I'd have the market for it* (U125, 2021).

Las respuestas que se realizan este tipo de comentario aconsejan tener suficiente stock del producto que se desea a vender. El motivo es que la volatilidad de los precios del Bitcoin en este caso podría afectar la rentabilidad del negocio y la confianza de los clientes que esperan la entrega del producto (/u/rambouk2uk en U125, 2021).

Sin embargo, la mayoría de las discusiones que se centran en la comisión de delitos en específico tratan los delitos de blanqueo de capitales, *carding* y ataques *ransomware* en los que las criptomonedas tienen un papel relevante. Las recomendaciones y consejos realizadas sobre estos están relacionadas con la protección de la privacidad y el anonimato, explicando

cuáles son las formas más efectivas de desarrollar los delitos en específico para evitar cualquier riesgo de detección.

En relación con el delito de blanqueo de capitales o lavado de dinero, los consejos para proteger la privacidad y el anonimato se han centrado en aspectos como la cantidad de monedas que se deben comprar, las casas de cambio que utilizar, el tipo de criptomonedas, patrones de actuación, tipo de carteras, etc. Todo ello con el objetivo de que las partes que intervienen en los criptomercados puedan realizar su actividad de forma que no se descubra la actividad ilegal realizada (U58, 2021). El dinero obtenido a través de otro delito será utilizado en la compra de criptomonedas, de forma que se "limpia" el rastro delictivo del dinero. Posteriormente este dinero podrá ser conservado como criptomoneda o bien convertido de nuevo a dinero fiduciario.

De la misma forma que delito de blanqueo de capitales tradicional, el desarrollo de este delito con criptomonedas también consta de una serie de etapas. En el foro se realizan diversas consultas que se corresponden con las diferentes etapas que forman el proceso de blanqueo de dinero y las diferentes técnicas que se pueden utilizar.

Una de las técnicas empleadas en el desarrollo de este delito es la utilización de un ATM de criptomonedas como Bitcoin. Consiste en la utilización del dinero procedente de un delito para comprar criptomonedas a través de un cajero de criptomonedas:

> *looking for a very good and scannable fake ID. id like to get more into washing my cash with crypto through both atms and cashapp/zelle/whatever (i used elude mixers and exchanges and create new wallets so im gucci on that. any reccomendations? im pretty sure i remember in college theyd use a clearnet site, but im not fs* (U126, 2021).

En la mayoría de los ATM la identificación no será necesaria siempre que no supere el límite establecido. De esta forma, para obtener más dinero del límite mínimo establecido por las políticas de KYC será necesaria la obtención de una identificación falsa:

> *You should get the log with email access. Plaid will send you a code and if you have email access you can get the code and verify. Since cashapp's limit is $2500 I believe you should have a fake ID so you can buy bitcoin. The limit is $10k but obviously do it in chunks* (U127 en U128, 2021).

Por este motivo, en muchos casos será necesario comprar credenciales en la *Darknet* ya que también serán de utilidad para superar las medidas de KYC de algunas casas de cambio, tarjetas prepago o evitar las elevadas tasas de los cajeros:

> *You can go to a Bitcoin ATM and get crypto anonymously. At some Bitcoin ATMs they only require you to give name (you can give fake one) and a phone number(you can get a burner phone from walmart). Wear a mask. If you go to fakeidreview.com it is a verified list of fake ID vendors. Ive bought from several vendors and never had any problems. You need to also buy some identity credentials off White House Market marketplace on the dark web. Go to Dark.fail and then click on White House Market URL. Learn how to do PGP and create an account. I know this is a lot of steps but you are going to need identity credentials to be able to do KYC for a lot of prepaid cards and crypto exchanges if you dont want to pay the fees at bitcoin atms. Look up coin flips in your area. This is a brand of bitcoin*

> *ATMS with the lowest fees I have seen. Its 7 percent to buy crypto. If you get identity credentials you can use their credentials or use crypto NO KYC exchanges like Bisq or Local Monero (…)* (U129 en U130, 2021).

Otra forma que se comenta recientemente para el blanqueo de criptomonedas es a través de las plataformas de compraventa P2P como LocalMonero y LocalBitcoin:

> *Yeah I agree! Make sure to block the people who ask for ID and then only the ID'less? (Ones that don't ask for ID) will pop up in the search results. A lot of people use Localmonero to launder drug money into monero :)* (U131 en U5, 2021).

Tanto para operar con los ATM como para utilizar los servicios de compraventa P2P será necesaria la verificación de la cuenta creada. Estas credenciales también se pueden obtener en el mercado negro de la misma manera que la identificación falsa mencionada anteriormente. se pueden comprar los números de verificación necesarios en muchas de las operaciones realizadas con ATM (U132 en U121, 2020). De igual forma con las cuentas verificadas de Localbitcoins se venden por 350 dólares en el mercado WHM (U133 en U134, 2021).

De forma general, las recomendaciones se centran sobre todo en formas de evitar la detección de la actividad de blanqueo a través de la superación de medidas de seguridad relacionadas con las políticas de KYC. Esto es, por ejemplo, el factor doble de autenticación, los códigos de verificación que se envían por correo electrónico, el límite de obtención de bitcoins sin identificación, etc. Estas medidas se han tratado con mayor detalle en apartados anteriores pertenecientes a la evitación de la actividad ilegal.

Una vez terminado todo el proceso de blanqueo del dinero será necesario convertir de nuevo dicha cantidad a dinero fiduciario. Para ello es necesario realizar un proceso de *cash out* en el que se requiere de una elevada precaución para no poner en riesgo la privacidad. Este tema es tratado en apartados anteriores de forma más detallada.

Otro de los delitos más frecuentemente comentados en el foro es el delito de *carding*. Se trata de un ciberdelito que consiste en la falsificación de tarjetas bancarias u obtención de la información de las tarjetas de crédito o débito con el objetivo de hacerse con los fondos de la víctima. Las criptomonedas están relacionadas con este delito porque son utilizadas como forma de pago de las cuentas bancarias, las tarjetas de crédito o débito o la información financiera necesaria o bien son compradas con el dinero fiduciario obtenido. De esta forma, se encuentran en el foro discusiones que relacionan ambos términos:

> *i haven't carded before and because i don't live in us my only way to card is carding btc and converting it to xmr. like i said i haven't carded before so didn't try to bypass the kyc system but is it so hard to do? and exactly what i need to do it? is binance good for this shit? oh and all transactions will be below 200$. i'm not after big money. even 400$ per month is enough for me* (U134, 2021).

En este sentido, son frecuentes las discusiones en las que los usuarios recomiendan formas de realizar el *carding* superando las medidas de KYC obteniendo beneficios y evitando la detección de las autoridades. Explicando los aspectos principales de la utilización de los métodos que se utilizan habitualmente para cometer este delito como son las tarjetas de regalo, PayPal, giros postales, *Tranferwise*, *Western Union* o productos físicos (U43, 2020). Todas estas medidas se comentan de una forma más detallada en apartados anteriores. Según el foro, se puede decir que para obtener criptomonedas a través del cardado se requiere: paciencia, envejecimiento de las cuentas, buena falsificación de documentos y preferiblemente, acceso a una cuenta bancaria antigua con el nombre del titular de la tarjeta de crédito (U43, 2020).

Sin embargo, de la misma forma que se hablan de las ventajas del *carding* también se han comentado los riesgos que pudiera tener esta actividad delictiva. Muchos usuarios no lo recomiendan porque consideran que se asume un riesgo elevado de que la tarjeta pudiera ser bloqueada. Otros opinan que no se deberían comprar tarjetas clonadas o prepago porque habitualmente constituyen una estafa (U135 en U136, 2021). En su lugar, se proponen otras soluciones como la utilización de tarjetas regalo por el valor más elevado posible y luego cambiarlas por bitcoin (U138, 2021) o la obtención de una criptomoneda, aunque sea con verificación y luego su conversión a través de la cartera Cake a XMR y luego a BTC de nuevo para usarla en el mercado (U135 en U136, 2021).

Por último, también se han encontrado discusiones en las que se comenta el papel de las criptomonedas en los ataques *ransomware*. Se trata de un ciberdelito en el que se exige el pago de cierta cantidad de criptomonedas a cambio de la liberación total o parcial de un equipo informático. Algunos usuarios interesados en el desarrollo de esta actividad delictiva han consultado en el foro sobre la forma en la que debería llevarse a cabo:

> *Where do I get a Ramsonware that I can personalise it and put my Bitcoin address on it to ask for payment to remove the encryption?* (U137, 2021).

Consultan sobre la forma en la que personalizar el ataque e introducir sus direcciones personales de Bitcoin para poder recibir los pagos de sus víctimas. Pero no solo se ha consultado cómo ser autor de un ataque *ransomware*, sino que también se comenta sobre la posibilidad de ser víctima. Aunque se comentará con más detalle en apartados posteriores, este es el caso de un usuario que recibe un correo electrónico en el que se le amenaza con revelar a la policía la información de sus compras de drogas a menos que pague la cantidad de 150 dólares en bitcoin (U139, 2020). En ocasiones obtienen los contactos de las víctimas

de los registros de mercados que los venden para conseguir dinero o bien que no disponían de medidas de seguridad suficientes para protegerlos (U139, 2020).

Operar en los Criptomercados de la *Darknet.* Aunque no se limitan únicamente a la *Darknet* la mayoría de los mercados delictivos online se ubican en este entorno. La *Darknet* o "red oscura" garantiza una mayor privacidad de la actividad de sus usuarios al emplear en su funcionamiento la red TOR. De esta forma, se pueden encontrar los llamados criptomercados, en los que se utilizan las criptomonedas como sistema de pago.

Las particularidades que se pueden ver en la utilización de los criptomercados y en especial de la utilización de las criptomonedas en estos, ha motivado a muchos usuarios a escribir en los foros para consultar determinados aspectos relativos en específico a esta temática. Por ello, se dedica un apartado exclusivo para la utilización y operación en los criptomercados de la *Darknet.* En este se incluyen discusiones sobre temáticas como el pago en los criptomercados, la valoración de estos por parte de la comunidad del foro, detalles sobre la utilización de las criptomonedas en estos, etc.

Utilización de un Criptomercado. De forma general, en el foro se recomienda que previamente al acceso y utilización de un criptomercado se realice el estudio detenido de la "Biblia DNM" de "Dread":

> *hey mate, dont do anything on the DN until you've read the DNM bible. it runs you through everything opsec related along with the things you should do and avoid. there is a link in the banner and on the sidebar. stay safe* (U140 en U1, 2021).

Este documento elaborado por los administradores del foro "Dread" contiene recomendaciones de carácter básico relacionadas con la seguridad de la actividad en un criptomercado, detallando lo que se debe hacer y lo que se debe evitar.

En primer lugar, la utilización de un criptomercado tendrá que comenzar con la elección de una criptomoneda como forma de pago, que de forma general se trata de la criptomoneda Monero. Además, también se realizan otro tipo de recomendaciones como la utilización de la firma PGP y la necesidad de comprobar que los enlaces de los criptomercados son oficiales para evitar el riesgo de ser víctima de *phishing* (U93 ,2021).

Hay usuarios que consultan sobre la utilización en general de los criptomercados. El perfil de estos usuarios puede ser muy variado. Por ejemplo, puede tratarse de una persona interesada en convertirse en proveedor del mercado que pregunta acerca de cuál es el mejor mercado, cómo realizar el envío del producto, qué información se debe proporcionar y cómo utilizar las criptomonedas, especialmente para transferir los fondos a la billetera personal

(U141, 2021). Otros usuarios piden a la comunidad del foro tutoriales o explicaciones detalladas sobre cómo encargar un producto en un mercado en concreto, comenzando por la utilización de PGP, el cambio de Bitcoin a Monero en aquellos que se da el caso hasta el pedido:

> *Hi, im somewhat new to the marketplace. Me and my partner have been paying someone to do orders for us cause i just cant figure it out. Would anyone be interested in giving me a step by step tutorial on how they order? its costing me a fortune having to pay someone to to do the PGP and then transfer bitcoin to xmr. What is the best way i can learn so i dont have to pay then give half my profit for payment? I mean this can be tedious and im doing my best but IM BEGGING for someone to give me the STEP BY STEP order process. I use WHitehouse Market. i purchase hulks like 1000. I like the deals . But also if anyone else has a better website i can order from that uses bitcoin that would be good, also the easiest PGP site for a beginner like me* (U142, 2021).

Aunque estas peticiones no son las más frecuentes, reciben comentarios de usuarios interesados en ayudar. Por ejemplo, en el caso anterior se responde que la ruta general para comprar en el mercado WHM empieza por registrarse y obtener una clave PGP2, se selecciona el artículo que se desea, se consulta al proveedor en caso de dudas, se compran criptomonedas Monero en LocalMonero, se realiza este pedido en el mercado, se envían las criptomonedas a la billetera del mercado (U142, 2021).

En otras ocasiones también se realizan explicaciones sobre el funcionamiento de otro tipo de mercados menos convencionales como es el caso del criptomercado ruso “Hydra”, que ha supuesto una revolución en el ámbito de los mercados de drogas de la *Darknet* por la forma en la que se realizan los pedidos:

> *The Russian DNM Hydra pioneered the drop gang sistem. In short, it's a system using Tor or encrypted apps to set up anonymous local purchases and dilveries. After a bitcoin payment the customer receives a message stating the location of their delivery, ie. taped behind a utility box, often with a pic of the exact spot. In some locations in US they can now be found on Telegram operating independently of markets. A Google search on Hydra will get you started and there have been posts on the subject here that I can no longer find* (/u/U143 en /u/U144, 2021).

Este mercado de drogas online utiliza TOR para garantizar el anonimato de la compra y la entrega. Después del pago en Bitcoin el cliente recibe un mensaje en el que se le indica la localización exacta en la que se encontrará su pedido, a menudo acompañada de una fotografía del lugar (/u/U143 en /u/U144, 2021).

No obstante, los consejos para proteger la privacidad y el anonimato de la actividad en la *Darknet* no quedan únicamente reservados para los compradores. Siendo conscientes del riesgo al que pueden exponerse los vendedores de los criptomercados, algunos usuarios han expuesto diversas pautas que estas figuras deberían seguir en el desarrollo de su actividad. Entre ellos, se les recomienda no cobrar inmediatamente el dinero recibido, utilizando Monero, esperando varios días e intentando mezclar las transacciones antes de convertir las monedas virtuales a dinero fiduciario, especialmente si se trata de una cantidad elevada:

> *Don't cash out immediately (Or better yet, don't cash out at all. Use the Monero as money instead). This can prevent linking transactions. Try to wait several days and mix transactions before cashing out* (U58, 2021).

Además, se aconseja que, si por algún motivo se debiera aceptar Bitcoin, se debería realizar esa transacción a una nueva dirección y enviar este dinero a una cartera Monero a través de un intercambio descentralizado:

> *If you must accept Bitcoin for some reason, let the buyer send it to a new address. Then convert that Bitcoin to Monero through a decentralized exchange* (U58, 2021).

Pagar en Criptomercados. Para poder adquirir los productos o servicios ofertados en los criptomercados es necesario obtener previamente alguna de las criptomonedas disponibles como forma de pago. La elección del tipo de criptomoneda que se utilizará es un tema importante para aquellas personas que desean proteger la privacidad de su actividad, especialmente si se trata de una actividad ilegal. Por ello, es habitual que algunos usuarios acudan a los foros para preguntar cuál es la mejor forma de obtener estas criptomonedas, cómo usarlas en el criptomercado para que su identidad no quede al descubierto o sobre la disponibilidad de alguna en determinados criptomercados:

> *do most sites accept monero as a payement method like they do bitcoin?* (U145, 2020).

Los usuarios que han participado en estas discusiones exponen de forma general que Monero es una de las criptomonedas disponibles como forma de pago en los criptomercados y aunque no es tan accesible como Bitcoin, se recomienda su utilización frente a esta porque protege la privacidad de la actividad (U145, 2020). En el caso de que el mercado que se desea utilizar no tenga disponible una criptomoneda en específico, ya sea Bitcoin o Monero, se recomienda comprar la criptomoneda que le sea más habitual y finalmente realizar el cambio a la otra criptomoneda. No obstante, Monero se ha convertido en la criptomoneda estándar en los criptomercados de la DN (U140 en U146, 2021) de forma que aquellos criptomercados que solo tengan disponible Bitcoin como forma de pago requerirán de un cambio a Monero.

Una vez se conoce la disponibilidad en un mercado de una criptomoneda en particular, la realización del pago en estos espacios también presenta una serie de peculiaridades. Para pagar en los criptomercados de la *Darknet* se requiere del envío de una transferencia con la cantidad exacta del precio del producto o servicio. Esto ha generado diversas dudas a los compradores que, han consultado en el foro sobre cómo se debería de realizar el pago de forma que las tasas que se aplican en la conversión de divisas no supongan una reducción en la cantidad enviada. Si finalmente el vendedor recibe una cantidad menor, el envío sería cancelado y el comprador podría perder el dinero invertido (U147, 2020). La

solución que proponen el resto de los usuarios en este caso es que se realice este pago directamente señalando en la cartera la cantidad de bitcoins que se desea enviar, y que sea la cartera la que realice la conversión y determine la tarifa (U147, 2020).

Cantidad Adecuada de Compra de Criptomonedas. Previamente a la utilización de un criptomercado será necesaria la adquisición de criptomonedas. Sin embargo, la compra de criptomonedas para la posterior utilización en los negocios de la Darknet también ha generado diversas discusiones en el foro. El motivo es que la compra de criptomonedas en una casa de cambio y su posterior utilización para la compra de droga u otros productos ilegales podría señalar esta actividad como sospechosa y aumentaría el riesgo de detección por parte de las autoridades policiales. Por ello, muchos usuarios han consultado cuál sería la cantidad necesaria de bitcoins que deberían comprar para que su actividad en los criptomercados no fuera señalada (U12, 2020).

De forma general, las respuestas que se han aportado sobre este tema señalan que se debe obtener siempre más cantidad de criptomonedas de la que se necesita para emplear en la compra. Si se adquiere y envía exactamente la misma cantidad que se necesita para la compra de un producto se podría detectar fácilmente al usuario. En el caso de que no se pueda adquirir más de la cantidad que se necesita, se recomienda espaciar el tiempo entre la adquisición de la moneda y su utilización (U58, 2021). En este sentido también habrá que considerar que el precio indicado de los productos supone una cifra orientativa. Finalmente habrá que pagar el producto utilizando la criptomoneda requerida, por lo que no se debe centrar todo el proceso en la cantidad de dinero fiduciario mostrada en el mercado ya que este valor cambiará durante la conversión y se debe asegurar que se dispone de suficientes fondos:

> *Yes just forget fiat when paying. The thing you pay attention to is the amount of BTC or XMR you are requested to send. Fiat is there for reference only as in, this item cost 60 dollars i look at my btc wallet and make sure i have enough if not a bit more according to the fiat balance, that way you have a rough idea if you have enough from one day to the next or even hour the way btc fluctuates* (U147, 2020).

Recomendación de Criptomercados. La oferta de mercados ilegales que se pueden encontrar en la Darknet es muy amplia y variada, lo que ha motivado que muchas de las discusiones del foro traten sobre recomendaciones de mercados basadas en las experiencias previas de los usuarios.

Aunque son más habituales los criptomercados dedicados a la venta de drogas, las recomendaciones no solo se limitan a estos, yendo desde mercados donde comprar productos ilegales, como plataformas de pornografía o *streaming* y TV en vivo (U148, 2021).

Son frecuentes las discusiones en las que un usuario ofrece una lista de mercados que recomienda. Por ejemplo, Monopoly, White House, Cypher, Torrez, ASAP, Dark0de, Tor2door, etc. (U93, 2021). En ocasiones se buscan recomendaciones sobre mercados o vendedores de los que obtener productos en específico, especialmente relacionados con el delito de carding, buscando comprar tarjetas clonadas o robadas (U136, 2021).

En este apartado también incluyen aquellas discusiones en las que los usuarios consultan sobre el normal funcionamiento de un criptomercado. Esto es, por ejemplo, la retirada de fondos de la billetera que se utiliza en estos mercados.

> *Is anyone else having issues with their withdrawals? I tried to withdraw XMR from my account once and XMR was taken from my account, but I never had XMR show up to my wallet and it didn't even show up as a withdrawal in my XMR transactions on the site. I contacted staff and they refunded me saying "Failed withdrawals will be auto-refunded in your account.". What is this supposed to mean? Why did it fail in the first place? (...) I am by no means trying to spread FUD. Just want to know if anyone is experiencing this like I am* (U149, 2021).

Aunque este aspecto es tratado de una forma más amplia en apartados posteriores relativos a la victimización de los usuarios, merece la pena señalarlo también en este apartado, ya que un mercado que finalmente resulte fraudulento supondrá una recomendación negativa por parte de los usuarios del foro. En este sentido son habituales los comentarios que tienen como objetivo comprobar si se ha sido víctima de las conocidas como "estafas de salida" en las que el mercado cesa su actividad de forma repentina apropiándose de los fondos depositados por el usuario para realizar su compra.

Por este motivo, los usuarios también han creado listas sobre criptomercados para los que no se recomienda su utilización. Así, crean hilos de discusión en los que exponen el nombre de un criptomercado y describen su experiencia o exponen diversos argumentos en contra de su utilización. Se han encontrado diferentes comentarios relacionados con esta temática. Este es el caso por ejemplo del criptomercado "RPD Canada":

> *I have noticed several high profile guides on here which have RDP Canada as a recommendation. I purchased an RDP with some one of upgrades several days ago from them, and I am still waiting for them to show the invoice is paid and activate my service. I have sent them emails, messages, spoken to live chat, all to no avail. In total with the one off extras it was nearly $50, bitcoin was through the confirmations in 20mins, so watch when you are reading these guides, the ability to scam is all around!! Do Not Waste Your Money On RDP Canada–- and these so called guides should be removing them!!!* (U150, 2020).

Sin embargo, aunque las experiencias negativas de los usuarios deben ser tomadas como una advertencia están abiertas a debate. Muchos usuarios han participado en estas discusiones rebatiendo los comentarios negativos y aportando sus buenas experiencias de compra en el mismo mercado objeto de debate. Señalan que, aunque puede que haya habido problemas, estos se han resuelto por el personal del mercado no tratándose de una estafa y

además exponen que este tipo de riesgos también podría tener lugar en mercados de la web superficial (U151 en U152, 2021). También hay casos en los que las respuestas a los comentarios negativos son realizadas por el personal del mercado en cuestión, discutiendo la veracidad de las afirmaciones que se están realizando y cuestionando la calidad de las medidas de seguridad empleadas por el usuario (U110 en U153, 2021).

Contratar a Otra Persona Para Utilizar las Criptomonedas. Los aspectos técnicos de las criptomonedas han motivado a algunos usuarios del foro a buscar a otras personas más especializadas que sean capaces de utilizar esta tecnología en su lugar (Europol, 2018). También se han realizado algunas publicaciones de personas que se ofrecen para trabajar como expertos en alguna materia relacionada (Europol, 2018). Tal es el interés de ambos que en el foro se ha incluido un subtema en el que se recogen todas las publicaciones relacionadas con ofertas de empleo y ofertas de trabajadores. Este tipo de publicaciones requieren de un formato en específico en el que se incluye el tipo de empleo en el título, se detallan las características del empleo o bien las cualidades del demandante de empleo y la cantidad de criptomonedas que demanda o bien que se pagaría por el trabajo (U154 en U155, 2021). Emplean los términos [JOB] para ofertas de empleo y [LFW] para usuarios que se ofrecen para trabajar. Tienen también como regla que el *hacking for hire* no está permitido y advierten sobre los riesgos de las transacciones en bitcoin y recomiendan la utilización de Monero.

Las discusiones que se han encontrado en este sentido pueden agruparse en dos tipos. Por un lado, aquellas relacionadas con usuarios que buscan personas que se ofrezcan o acepten desarrollar una actividad delictiva o una parte de esta a cambio del pago en criptomonedas. Por otro lado, se agrupan aquellas discusiones en las que se ofrece o se busca alguna persona que realice una actividad de carácter técnico relacionada con las criptomonedas y que permita la realización de un delito posterior.

El primer tipo consiste en aquellos usuarios que buscan a personas para utilizar las criptomonedas como parte del desarrollo de una actividad delictiva. Esto puede consistir en el desarrollo de la actividad delictiva al completo o de alguno de los pasos necesarios.

En una discusión sobre la obtención de criptomonedas empleando un cajero automático, el usuario, con algunas dudas sobre la utilización de la tecnología, sugiere que sería mucho más sencillo solucionar sus inconvenientes si pagara a otra persona para adquirir su pedido:

> *I have a few different ones. Paxful, exodus, coinbase. Just trying to figure best one to use till I can get my bank account fixed, just wanna make my damn order, I got plenty of money lol. If I scan the qr code and say, send it to paxful wallet. Could I then send it to him or? Shit is frustrating the hell out of me. How about I pay someone to do an order for me lol. Keep everything opsec as possible lol* (U37, 2020).

En la respuesta proporcionada a este comentario se le recomienda al usuario que para mantener la privacidad de su actividad y mantener las opciones de seguridad, no debería implicar a terceras personas (U37, 2020).

Se incluyen las discusiones en las que se ofrecen las criptomonedas como forma de pago por el desarrollo de una actividad delictiva. Este es el caso del usuario que busca a alguien con acento estadounidense para realizar llamadas telefónicas a casinos en línea y conseguir verificar la identidad de forma telefónica a cambio del pago en Bitcoin o Monero (U156, 2021). O el caso de un usuario que ofrece el pago en Bitcoin o Monero por realizar una llamada telefónica que consiga convencer a una persona y a los otros miembros de una estancia de que tienen que desalojarla para poder entrar a recuperar unos bienes supuestamente robados a otro grupo criminal (U157, 2021).

También puede darse el caso de que sean los usuarios los que se ofrezcan para realizar un delito a cambio del pago de una cantidad de criptomonedas. Por ejemplo, el usuario que se ofrecía a realizar el envío de transacciones "Paypal" a cambio del pago en bitcoins a su cartera (U117, 2021). Se presenta como un vendedor que permitía obtener dinero en efectivo para todos aquellos usuarios que desearan convertir sus fondos obtenidos con criptomonedas.

En ciberdelitos se han encontrado casos en los que se utilizan las criptomonedas como forma de pago de programas maliciosos empleados para el desarrollo de delitos posteriores (U158, 2021). En ocasiones esto también ha supuesto el trabajo conjunto con el usuario encargado del desarrollo de este programa. De esta forma, aunque el beneficio obtenido es menor se reduce el riesgo de detección sobre todo si no se cuenta con la especialización necesaria (U158, 2021).

También puede ocurrir que se trate de un trabajo complejo que requiera de refuerzos y aunque no sea imprescindible la participación de la otra persona, se ofrezca la participación en este delito a cambio de un porcentaje o cantidad de los beneficios que se esperan obtener:

> *Looking for someone to distribute malware software that replaces copied BTC addresses from clipboard and replaces them with another address (mine). I'll split whatever profit I get from the stolen BTC 50/50. So the more you spread the software, the more you'll get in return. This software is proven to bring in thousands if utilized well* (U159, 2021).

O el caso de un usuario que dispone de una plataforma falsa de *escrow* de criptomonedas y que necesita a alguien para que atraiga mediante ingeniería social a una persona con mucho dinero en criptomonedas para que deposite sus fondos en la plataforma

(U160, 2021). Finalizado el trabajo se repartirían el dinero disponible en la cuenta de la víctima como beneficio del delito realizado, haciendo desaparecer la plataforma empleada.

El segundo tipo consiste en aquellos usuarios que buscan personas con la capacidad de desarrollar los aspectos técnicos de un ciberdelito estrechamente relacionados con el funcionamiento de las criptomonedas a cambio del pago en esta moneda:

> *We are a small team of professionals developers and hackers ready to do almost every job included: Desktop and smartphone surveillance (Active and passive), server and Web-Application hacking (SQLi, XSS, LDAP, Xpath, etc.), social Engineering (Spear-phishing, Whaling, Smishing, etc.), personalized Malware and 0-Day exploit development and deployment (...) and much more for our customers. We accept many type of cryptocurrencies included: Bitcoin (BTC), Bitcoin Cash (BCH), Etherum (ETH) and XMR (Monero)* (U161, 2020).

Por ejemplo, son frecuentes los comentarios de algunos usuarios buscando personas que sean capaces de ayudarles con alguno de los aspectos de carácter técnico necesarios para el desarrollo de un mercado online. Exponen que el desarrollo de este trabajo será recompensado con el pago en criptomonedas como Bitcoin o Monero. También algunas personas se ofrecen como demandantes de empleo para este tipo de trabajo:

> *I'm able to build vendor shops, static pages, etc. Anything web application you need I can probably build it, no matter the complexity. I don't care what the morals of your application are (except CP and harm). (...) Disclaimer: Vendor shop pricing will start in the k's (...) I will also not accept full payment in the form of a commission of site profits although I will accept a percentage of the payment to be payed this way. An exact quote will be given after contact (...)* (/u/U162, 2020).

3. Lecciones Sobre Ciberseguridad y Utilización de las Criptomonedas

El carácter técnico de las criptomonedas y de las tecnologías que habitualmente se utilizan junto con estas ha llevado a muchos usuarios a realizar consultas sobre algunos de sus aspectos más especializados, tanto en su utilización legal como ilegal. Al mismo tiempo, el riesgo que puede suponer para la privacidad y el anonimato el desconocimiento de algunos de los puntos clave en su utilización, ha motivado a los usuarios a escribir en el foro explicaciones, consejos y recomendaciones sobre una mejor utilización de estas tecnologías.

Por todo ello, en este apartado se incluyen las discusiones relativas a las lecciones sobre privacidad y anonimato, consultas sobre aspectos del uso legal de las criptomonedas, consultas sobre aspectos de la tecnología en general y otras consultas relacionadas.

Lecciones Sobre Delitos en General. En relación con el carding, ha experimentado multitud de cambios en los últimos años. Las medidas de seguridad aplicadas impulsan cambios frecuentes en el desarrollo de este delito. Por ello, algunos usuarios ofrecen consejos y recomendaciones para facilitar la búsqueda y aplicación de métodos. Conocer los límites de cada usuario (habilidades, conexión y geolocalización); medir el tamaño del comerciante, aunque los pequeños comerciantes agoten rápido la estrategia, permite hacer menos movimientos con un beneficio mayor; no ser testarudo, midiendo en cada actividad si el coste o riesgo que se asume compensa al beneficio que se espera obtener; buscar mercados que incluyan pasarelas de pago, lo que nos indica que la tienda no es muy avanzada (U163, 2021).

Lecciones Sobre Privacidad y Anonimato. En el ámbito de las criptomonedas existen muchos usuarios preocupados por mantener el anonimato de su identidad y la privacidad de su actividad. Los motivos pueden ser varios, el que se ha encontrado de una forma más habitual en el foro suele estar relacionado con la comisión de delitos con criptomonedas, pero también puede tratarse de personas que están preocupadas por mantener su privacidad y que no tienen intención de cometer actividad delictiva alguna. Estos motivos pueden favorecer la utilización además de la red TOR y de los foros ubicados en la *Darknet*.

Por todo ello, la protección y aseguramiento de estos dos términos, anonimato y privacidad, es un tema muy discutido en el foro. Tal es el caso, que se han recogido algunas discusiones en las que los usuarios, de forma desinteresada ofrecían lecciones sobre dichos términos para asegurarse de que la comunidad los comprendían y no cometían errores. Este es el ejemplo de la discusión sobre la diferencia entre anonimato y privacidad, para la que un usuario emplea un ejemplo muy ilustrativo sobre una persona que viaja en autobús (U58, 2021). Considera que se hablaría de anonimato cuando una persona accede al autobús con la cara y el cuerpo cubiertos. En este caso las personas de dentro y fuera del autobús podrían ver que está viajando en el autobús, pero nadie conocería su identidad. Por el contrario, se trataría de privacidad cuando la misma persona viaja en un autobús sin ventanas para el que solo el conductor sería conocedor de su actividad.

Al contrario de lo que se piensa, Bitcoin no es anónimo, se puede consultar la cantidad de bitcoins enviados y recibidos en la *Blockchain* de forma pública y se puede trazar la actividad realizada por determinadas direcciones. Esto se agrava si se han obtenido los bitcoins de casas de cambio centralizadas con políticas de "conoce a tu cliente" (*Know your customer*, en inglés). Además, Bitcoin tampoco es privado porque toda la actividad que se realiza con esta criptomoneda queda registrada en la *Blockchain*, mientras que con

criptomonedas como Monero los registros quedan ocultos, por lo que el historial no puede ser consultado por nadie.

En estas discusiones también es frecuente que se trate lo recogido en otras publicaciones sobre la privacidad de las criptomonedas. Si los usuarios del foro conocen cómo están respondiendo las empresas de ciberseguridad y otras autoridades en la lucha del crimen cometido con criptomonedas, podrán trabajar en el aseguramiento de su privacidad. Este es caso de los informes de empresas como "Elliptic" la primera que señaló las carteras privadas como una de las principales herramientas de lavado de dinero en los últimos años considerando que la empresa creadora de la tecnología facilita de forma indirecta el desarrollo de estos delitos (U111, 2020) Este tipo de discusiones suscitan amplios debates en los que se consideran que las medidas de prevención establecidas se dirigen casi fundamentalmente hacia "el pez pequeño" dejando a un lado las actuaciones de grandes bancos que, son conocedores de las elevadas transacciones con origen delictivo que se realizan en sus servicios (U111, 2020).

En específico para las criptomonedas también se han dado consejos para mantener el anonimato y la privacidad. Aunque puede parecer similar a lo recogido en apartado anteriores, en este apartado se consideran aquellas recomendaciones que dan los usuarios a la comunidad de forma libre y sin haber sido requeridas previamente. Exponen la importancia de escoger criptomonedas que sean privadas, evitando criptomonedas que no son anónimas como BTC o ETH ya que, aunque no se muestren datos personales, se podrían relacionar los patrones de actividad con la dirección empleada:

> *if any of the addresses in a transaction's past or future can be tied to an actual identity, it might be possible to work from that point and guess who may own all of the other addresses since whole the Blockchain is public then all the history attached to an address is visible. There are many companies and website who could de-anonymize Bitcoin transactions with a high degree of accuracy* (U41, 2021).

Pero se debe tener cierta precaución porque no toda criptomoneda que se presenta como privada puede asegurar en todo caso el anonimato. Es importante escoger aquellas criptomonedas que tienen configuradas su privacidad por defecto, ya que algunas como por ejemplo la criptomoneda "Dash", tienen una configuración opcional para la privacidad, por lo que aquellos usuarios que desconozcan este aspecto no activarán la opción (U58, 2021). Además, la forma en la que se utilicen también puede ser determinante en la preservación de su privacidad. Por ello, se ofrecen consejos relativos a la cantidad de criptomonedas que se debe comprar, el tipo, la forma en la que se deben enviar o cobrar, tipos de billetera, intercambios, etc. (U58, 2021) dirigidos a que el usuario evite cometer errores y asumir riesgos en la protección de su privacidad y anonimatos.

Consultas Sobre Aspectos Generales del Uso de las Criptomonedas. En este apartado se incluyen consultas sobre aspectos generales del uso de las criptomonedas, pudiendo ser el propósito posterior su utilización en actividades ilegales, pero no necesariamente han de estar centradas en la comisión de delitos. Muchos de los usuarios que han iniciado estas discusiones justifican su consulta aludiendo a su baja formación en la tecnología o a encontrarse en una etapa muy inicial de su aprendizaje en esta materia.

En este sentido, son habituales las preguntas relacionadas con el tiempo que se estima para la retirada de cierta cantidad de criptomonedas como Bitcoin:

> *Hi guys, I am inquiring if its normal that my withdraw is showing pending? If so, how long does the withdraw get processed to my wallet? Thank you!* (U164, 2020).

Esto es, el tiempo que transcurre desde que se compra un tipo de criptomoneda en una casa de cambio hasta que esta cantidad queda reflejada en la cartera del usuario. El motivo por el que esta consulta es habitual es porque los usuarios temen haber sido víctimas de una estafa o haber cometido algún error en el proceso y perder sus fondos.

Las respuestas a estos comentarios suelen ir en la línea de explicar al usuario cómo se realizan este tipo de operaciones. Señalan que suelen llevar tiempo ya que en aquellos momentos en los que la red está congestionada (picos en el precio de Bitcoin), los mineros seleccionan primero aquellas transacciones cuyas comisiones son más elevadas, ocasionando retrasos en el peor de los casos de hasta 6-12 horas para el resto de transacciones (U164, 2020).

Otras consultas están relacionadas con la adquisición de bitcoins y su utilización para realizar compras:

> *Any knowledge on how i can acquire some bitcoin, and how to use is to purchase things* (U8, 2020).

Como respuesta a este tipo de pregunta el resto de usuarios cree necesario conocer el motivo de la obtención de las monedas, es decir, si se adquieren para su utilización en servicios ilegales, para mantener oculta su actividad ilegal o para pagar menos tasas (U165 U8, 2020). Según el propósito por el que se obtengan, pueden existir diferentes posibilidades para su obtención.

Por último, también se recogen algunas discusiones sobre posibles alternativas a las criptomonedas para el caso de que se desarrollen leyes que regulen determinados aspectos de su utilización en ciertos países. Por ejemplo, sobre la obtención de bitcoins a través de las casas de cambio de Reino Unido o usando cuentas bancarias inglesas:

> *9th January is the start of the ban on bitcoin in the UK. Any advice on new exchanges, which ones or countries maybe? Will any via UK bank transfer internationally?*
> *I think the ban is on all crypto currencies?* (U166, 2020).

Hacerse una cartera para enviar y recibir bitcoins siendo menor de edad:

> *Yo, whats the deal... I'm 16 and was wondering how I can personally make my own btc wallet that can send and receive btc anywhere. Every transaction on the dark web that I have made is thru an IRL friend that I pay with cash for him to pay the vendor. Any help/explanation is much appreciated :)* (/u/U167, 2020).

Sobre cómo hacer diferentes direcciones en una cartera GUI de Monero:

> *So basically when I sent xmr from my clear net wallet to my tails wallet, I make a new address in the Tails wallet every time to make it harder to track, right?*
> *But when I send xmr from my tails wallet into a DNM do I also need to make a new sending address every time? If so, I can't figure out how to do this on GUI wallet. I can only make new receiving addys and I can't figure out how to make a new address to send from. Wasnt bitcoin electrum you could make both? I can't remember exactly tho, it's been a few years since I've used it* (U168, 2020).

Otro Tipo de Lecciones. Para acceder a los mercados de la *Darknet* es necesario utilizar un enlace conocido como enlace "onion" que se utiliza de forma general en cualquiera de los lugares ubicados en TOR. Para evitar que otros usuarios sean víctimas de delitos phishing, algunos usuarios ofrecen consejos como comprobar que la dirección onion a la que se va a acceder es confiable o (U93, 2021).

El personal de algunos criptomercados ha iniciado discusiones en el foro en las que aportan consejos para poder solucionar posibles problemas que se presenten con los fondos depositados. De esta forma, aconsejan a los usuarios guardar el comprobante de intercambio firmado por PGP, la clave de firma del mercado (para asegurar que no se trata de phishing), etc. (U110 en U153, 2021). En relación también con los criptomercados, otros usuarios han aconsejado que para evitar ser víctimas de phishing se debe verificar los enlaces onion que habitualmente se utilizan para acceder a estos espacios (U93, 2021).

4. Regulación de las Criptomonedas

Otro de los temas que ha sido frecuentemente tratado en el foro es la regulación de las criptomonedas. Resultan relevantes este tipo de discusiones ya que aquellos usuarios motivados para la comisión de un delito con criptomonedas se mostrarán interesados en conocer aquellas reglas o normas vigentes en un determinado país. De esta forma, modificarán o limitarán sus actividades delictivas según la información obtenida o idearán nuevas formas de conseguir sus propósitos superando las restricciones implementadas.

Las discusiones que se pueden encontrar en este tema giran en torno a comentar la legislación existente en determinados países, las modificaciones que se prevén realizar y cómo afectarían al desarrollo de ciertos delitos o también conversaciones cuestionando la utilidad de algunas de las medidas de prevención del delito.

Aunque las criptomonedas pueden ser utilizadas con carácter global y transnacional, las medidas de prevención que se elaboran para luchar contra la criminalidad en la que se utilizan están limitadas a un país o países en específico. Este hecho ha motivado que algunos usuarios del foro consulten sobre aquellas medidas de seguridad que podrían estar vigentes en un determinado país o sobre el alcance que podrían tener las afirmaciones realizadas por los gobiernos:

> *the good OL USA is announcing putting large amounts of funds, and time into investigating money laundering in crypto. they are labeling it a priority. This can potentially be very bad for the darkweb for buyers and Sellers. how bad can this problem be, and what can be done about it?* (U96, 2021).

Pero no se centran únicamente en conocer las medidas vigentes de una forma descriptiva, sino que una vez disponen de la información sobre las medidas, buscan conocer cómo deberían modificar la forma en la que operaban anteriormente para adaptarse a los nuevos cambios:

> *9th January is the start of the ban on bitcoin in the UK. Any advice on new exchanges, which ones or countries maybe? Will any via UK bank transfer internationally? I think the ban is on all crypto currencies?* (U166, 2020).

Además, la mayoría de los usuarios no muestran posiciones neutras ante este tipo de información. La intervención de los gobiernos en la regulación de las criptomonedas ha sido considerada como un envilecimiento que aleja a las criptomonedas de su propósito inicial de transferir dinero y las acerca a convertirse en una herramienta para invertir y "hacerse rico" (U68 en U169, 2021). Las criptomonedas deberían considerarse como una tecnología que obligara a la legislación a adaptarse a su funcionamiento y no al revés:

> *If it must kow-tow to politicians and lawmakers, it's rootings lie on swampy ground. Crypto, the true crypto that follows its original goal, must not depend on legislation. Nothing short of shutting down internet can stop it. The true crypto is not supposed to adapt to legislation, but instead force legislation to adapt to the new rules. If not, it's game over for crypto* (U169, 2021).

Pero sobre todo son habituales en el foro las conversaciones en las que se cuestiona la utilidad de aquellas medidas de prevención del delito que han resultado de los cambios legislativos. Este es el caso del endurecimiento de las políticas de KYC para prevenir delitos como el blanqueo de capitales. Muchos usuarios se han mostrado escépticos ante la utilidad que pudieran tener algunas acciones al respecto como, por ejemplo, el control en la retirada de dinero, que podría ser fácilmente evitado mediante la utilización de terceras personas conocidas como "mulas":

> *It literally takes me few hours to get KYC'ed via Homeless person and then another few more to cash out my money. I'm the average joe. How long will it take to the average criminal? It's not like they don't know the term money mule. I will never support this clownery, how come people believe that this is supposed to prevent crime or tax evasion? Hilarious. will never support this KYC nonsense. It does nothing. It's useless surveillance to track normies, this won't stop criminals. How can someone be this naive?* (U68, 2021).

En este sentido, las respuestas a este tipo de intervenciones han sido variadas. Ante la afirmación de que ese tipo de medidas carecen de efectividad y en relación con el descontento de la actuación por parte del gobierno, varios usuarios han expuesto que en realidad se trata de medidas cuestionables que aumentan la vigilancia de la población (U170 en U68, 2021). Exponen que ante la elaboración de este tipo de medidas los gobiernos parecen carecer del conocimiento suficiente para el desarrollo de propuestas que realmente contribuyan en la prevención de la delincuencia (U69 en U68, 2021). Lo que puede sugerir que incluso dejan que el crimen simplemente suceda (U171 en U68, 2021). Este desarrollo legislativo habitualmente no se fundamenta en cifras delictivas reales, sino que tal y como sugiere la comunidad, endurecen sus medidas de prevención impulsados por el estigma que se tiene sobre la mera utilización de criptomonedas.

No obstante, aunque en menor medida, también se han encontrado algunos comentarios que, en relación con la efectividad de las medidas, sostienen que puede que las medias sean efectivas con aquellos usuarios menos experimentados que no disponen de la habilidad ni de la previsión para proteger sus identidades en este tipo de controles de seguridad (U78 en U68, 2021).

Otros comentarios sugieren que realmente es posible que el gobierno limite la utilización de las criptomonedas hasta que resulte compleja su utilización en el crimen. Exponen que no hay que subestimar el alcance de las medidas que se proponen. Por ello, la comunidad del foro se muestra previsora y algunas discusiones giran en torno a casos hipotéticos en los que se produce un intenso endurecimiento de la legislación. Se incluyen discusiones relacionadas con el cierre de plataformas de intercambio como LocalMonero y Agoradesk, sobre el funcionamiento del mercado de la DN con la prohibición de las criptomonedas o la monitorización de bitcoin y prohibición de Monero (U173, 2020). Las respuestas a estas discusiones son muy variadas, pero de forma general se plantea que la regulación difícilmente podrá ir orientada a una prohibición total del uso de criptomonedas, de la misma forma que no se podría prohibir el uso de internet (U172 en U173, 2020). Al mismo tiempo, hay que considerar que muchos de los delitos que ahora se desarrollan empleando criptomonedas ya existían anteriormente. Por ejemplo, se comenta que el primer negocio de drogas en internet fue en Usenet[217] en 1973, donde se vendió marihuana por valor

[217] Abreviatura de “Users network” o red de usuarios que constituye un sistema global de discusiones en Internet.

de cinco dólares en un campus universitario (U174 en U173, 2020). Simplemente se encontrarán otras formas de desarrollar la actividad delictiva obteniendo sus beneficios:

> *Well except for dropshippers vendors already find creative ways just to be vendors, like moving product, stealth and what ever it is that they are doing. I doubt moving some data from here to there and exchanging it for cash will be much of a problem. I'm quite sure smart ones will be just fine* (U172 en U173, 2020).

Esta capacidad de adaptación a las modificaciones se puede ver incluso en países con restricciones duras como es el caso de China:

> *Let's use China as an example, they have been cracking down on Bitcoin ever since it's creation. What do the Chinese do? Use a VPN and buy through a neighboring exchange and sell it through a neighboring bank (…) That's why Bitcoin will never be toppled. All attempted bans have been unsuccessful even in an extreme Country (…)* (U175 en U173, 2020).

Aunque el país ha desarrollado en los últimos años una regulación muy estricta para la criptomoneda Bitcoin, la población en China ha encontrado nuevas formas de continuar utilizándola.

5. Evitar la Victimización

Puede ocurrir que los usuarios que participan en el foro sean al mismo tiempo usuarios de la *Darknet* que utilizan las criptomonedas para diversos fines. De esta forma, se muestran como usuarios preocupados por su propia seguridad y han realizado consultas en el foro con el objetivo de evitar ser víctimas de delitos, en específico de ciberdelitos.

En primer lugar, se ha encontrado que los usuarios realizan consultas relacionadas con la posibilidad de ser víctimas de una estafa. Habitualmente se valora en grupo la fiabilidad de servicios o lugares de la *Darknet* que podrían ser fraudulentos. Este es el caso, por ejemplo, de los servicios que garantizan multiplicar la cantidad de criptomonedas de la que se dispone y así obtener elevados beneficios. Aunque muchos usuarios conocen la falsedad de estos servicios, los elevados beneficios que se aseguran han llevado a otros usuarios a asegurarse de que no es cierto lo que se promete:

> *Does anyone know if "Underground 10x Bitcoin" actually works? Sounds kinda sus* (U176, 2021).

Las respuestas a estos comentarios coinciden de forma unánime en señalar a este tipo de servicios como una estafa:

> *Every website that pretends to multiply cryptos or anything are a scam buddy, stay aware. If easy money existed everyone would be Jeff Bezos :)* (U29 en U176, 2021).

No obstante, la mayoría de las consultas realizadas sobre esta temática tratan la posibilidad de haber sido víctima de estafa en un mercado online fraudulento. En este sentido, preguntan sobre la fiabilidad de determinados mercados o sobre si son normales ciertas situaciones que se han producido durante el desarrollo de su actividad. Para realizar la

compra de un producto en un criptomercado es necesario depositar una cantidad determinada de criptomonedas en la dirección de la cartera del mercado. Una vez se haya finalizado la transacción y se haya confirmado en el sistema, ese dinero aparecerá en la cartera de la cuenta creada en el mercado y se podrá realizar la compra. Sin embargo, una elevada demora en la aparición del dinero en la cuenta del mercado podría suponer un indicio de estafa, cuestionando la fiabilidad del mercado en el que se ha operado:

> *On Sunday I create and verify my account on World market. I made 2 deposits with bitcoins but till now can't see my deposit in my profil on World market. Can't find anybody to help me. I spoke with wallet company that I send deposit on world market and they told me that all are right and the money are now on the address that game me world market. Can somebody help me?* (U177, 2021).

Esto sucede sobre todo cuando se comprueba que se han realizado varias confirmaciones de la transacción en la red Bitcoin y no se ha recibido aún el dinero en la billetera del mercado:

> *It took me to a working site, seemed fine, but when I put in a small deposit it says "Confirming... Your deposit, 0.0031 Bitcoin has been recognized by our system and is now confirming. Once the required amount of confirmations is reached, it will be added to your account balance and you will be able to make another deposit. Reaching the required amount of confirmations can take several minutes up to several hours. Thank you for your patience. "but it has 3 confirmations already. Did I get fucked?* (U178, 2021).

Los usuarios exponen sus experiencias en el foro para conocer si se trata de un suceso habitual para ese mercado y le ha sucedido de la misma forma a otras personas, o si por el contrario han sido víctimas de una estafa.

Junto con lo anterior, es posible que el usuario también haya sido víctima de un delito de *phishing*. Como ya se conoce, la *Darknet* no dispone de un buscador a través del que se puedan encontrar los mercados online o criptomercados. Por ello, será necesario disponer de los enlaces necesarios para poder acceder a los mercados que el usuario desee. En ocasiones estos enlaces son creados por los cibercriminales para dirigir a los usuarios hacia réplicas de mercados online originales:

> *Generally if you can not create a ticket it is possible that you are on a phishing site (...)* (U179 en U177, 2021).

La víctima cree estar operando en el mercado habitual y realiza el depósito a la dirección de la billetera proporcionada. Sin embargo, ese dinero nunca se deposita en la cartera del mercado ya que al tratarse de un falso mercado la dirección proporcionada es la del criminal. Por todo ello, se recomienda frecuentemente entre los usuarios del foro comprobar los enlaces *onion* antes de acceder y depositar dinero en un mercado.

En segundo lugar, el caso más común entre los usuarios es el del delito de *blackmail* o chantaje. Muchos usuarios escriben exponiendo que han recibido correos electrónicos en los

que se les exige el pago de una determinada cantidad de bitcoins a cambio de no revelar sus identidades o información comprometida de su actividad delictiva:

> *I recently received a mail threatening to reveal my informations (mostly drugs that I bought online) to the local authorities. I already have trouble with the justice (I am awaiting trial right now) so this could be really bad for me... The guy want that I send 150$ worth of BTC to his wallet address within 2 weeks and I don't know what to do right now, should I send it? (U139, 2020).*

Aunque el hecho de recibir este tipo de mensajes puede ocasionar preocupación en cualquier usuario de Internet, en este caso los usuarios realizan la consulta especialmente preocupados porque han participado en actividades de compra en criptomercados delictivos de la *Darknet.* Por este motivo, preguntan al resto de usuarios sobre determinados aspectos que pudieran resultar sospechosos de constituir actividades delictivas. Estas consultas se realizan en muchas ocasiones antes incluso de realizar ninguna acción al respecto.

Las respuestas a este tipo de consultas son muy variadas, pero de forma generalizada los usuarios recomiendan no pagar nunca la cantidad exigida. Como argumento, los usuarios señalan la falsedad de los mensajes recibidos, cuestionando el hecho de que los autores de los mensajes arriesguen su propio anonimato al denunciar las actividades ilegales realizadas por otros usuarios (U180 en U139, 2020). En este sentido, el comentario de otro usuario:

> *(…) how is he going to send that to the Police department anonymously? What does he get from that except for risking his own identity being known? It must be someone who truly hates you a lot then, and even if thats the case, what Do they got on you? technically? Just your name and address that ordered a product online that is illegal* (U181 en U139, 2020).

Otras respuestas tienen el propósito de hacer ver al usuario la falsedad del mensaje recibido. Es el caso, por ejemplo, del usuario que expone que se exige una cantidad en Bitcoin, una criptomoneda que es conocida por la posibilidad de rastrear toda su actividad. Considera que podría haber gozado de una mayor credibilidad si se hubiera exigido el pago en Monero (U182 en U139, 2020).

Por último, también hay respuestas de usuarios que explican a la persona que realiza la consulta cómo ha podido ser su dirección implicada en el ataque. De esta forma, intentan hacer ver que no se trata de un ataque dirigido y que por tanto no merece mayor preocupación. Así, por ejemplo, le hacen ver que se trata de un mensaje que ha sido enviado de la misma forma a otros muchos usuarios de la *Darknet* (U183 en U139, 2020). También otros aseguran que podría tratarse de los mismos vendedores del criptomercado en el que compró droga, por lo que carece de sentido el hecho de que se pongan en contacto con las autoridades y pongan en riesgo sus propias actividades delictivas (U184 en U139, 2020).

6. Reflexiones, Quejas y Casos Relevantes

En relación con las criptomonedas, en especial con Bitcoin, se han encontrado discusiones dedicadas por un lado a reflexionar sobre diversos aspectos de esta tecnología y por otro, a mostrar descontento o desaprobación sobre actuaciones relacionadas con su utilización.

Aunque algunos de los cometarios incluidos en este apartado ya habían sido tratados en apartados anteriores, se ha decidido su incorporación también aquí por dos motivos. El primero es que se pretende resaltar que el foro es un espacio dedicado al debate y a la reflexión entre sus miembros. Se incluyen sobre todo aquellas discusiones de interés para la comunidad que son polémicas o que abiertamente llaman al debate al resto de usuarios. El segundo motivo es que también se han encontrado otras discusiones que, aunque tratan temas interesantes para el ámbito de las criptomonedas, no tienen cabida en ninguno de los apartados anteriores. Por ello, sería conveniente que se expongan en este apartado por su utilidad para comprender la línea de pensamiento y de actuación de la comunidad del foro.

Uno de los temas sobre los que más se ha reflexionado ha sido sobre la regulación de las criptomonedas, el alcance de las medidas de seguridad y las limitaciones que pueden generar estas decisiones en las formas de actuación actuales. Aunque ya se han tratado estos temas en el apartado de la regulación, aquí se pretende destacar que se trata de un tema que suscita amplios debates entre los miembros del foro. Por ello, es de interés mencionar brevemente el tipo de reflexiones que se han desarrollado más frecuentemente en las discusiones.

Como parte de la estrategia de detección, persecución y prevención de este tipo de criminalidad se ha discutido sobre la justificación que pudiera tener la persecución por parte de las autoridades de toda la actividad realizada utilizando criptomonedas, así como el desarrollo de medidas tendentes a restringir su utilización. En este sentido, muchos usuarios consideran que la persecución que se está realizando por parte de las FCSE no está justificada y que se están dirigiendo estos esfuerzos contra los objetivos equivocados. Así, por ejemplo, un usuario acusa a las grandes firmas bancarias de conocer e ignorar la procedencia delictiva de muchos de sus fondos y de su utilización para la financiación terrorista y gobiernos corruptos (U111) suponiendo esta cifra alrededor de 10.1 veces más la capitalización total de Bitcoin o casi 6 veces la capitalización total del mercado de criptomonedas. Por ello, sostiene que no está justificada la persecución que se está realizando de las actividades desarrolladas con criptomonedas, porque es ampliamente conocido que solo el 1% de todas las

transacciones realizadas con criptomonedas están dedicadas a actividades delictivas (U111, 2020). Continúa exponiendo, que la continua lucha contra las criptomonedas rastreándolas y localizándolas, supone un malgasto de recursos contra los "peces pequeños", a la vez que otorga una mala imagen de las criptomonedas y su comunidad:

> *Instead of stopping the real source of all the problems, pain and misery in this world by going after the big fish they are still wasting resources on the little fish, tracking, tracing and stopping enouvation while at the same time painting a bad picture of cryptocurrancy and its community* (U111, 2020).

Por otra parte, también son objeto de críticas las grandes empresas dedicadas al análisis de la Blockchain como son "Chainalysis", "Ciphertrace" y "Elliptic" que obtienen una elevada suma de dinero por su actividad al mismo tiempo que trabajan con aquellas personas encargadas de regular el uso de las criptomonedas. Consideran que se está persiguiendo el desarrollo de un sistema que controlará cada movimiento, mensaje y transacción, vigilando, rastreando y monitorizando a los usuarios sin que esto pueda tener una justificación real desde la persecución de la delincuencia:

> *Laws which at the end will only contribute to the shaping of a more draconian and totalitarian system which will eventually be the end and down fall of democracies as we know it and will start a world in which every move, messages and transaction is being watched, tracked, monitored and followed. As privacy becomes more of a necessity than a luxury in the crypto space as a whole, it is understandable that criminals would want to get inventive and use privacy wallets* (U111, 2020).

Por este motivo, los propios usuarios justifican que se utilicen tecnologías como las carteras privadas para ocultar el rastro de su actividad para la que consideran que tienen derecho a mantenerla privada.

En este sentido también se ha reflexionado sobre la posibilidad de que surjan herramientas o se desarrollen medidas que permitan finalmente un control o monitoreo total de la actividad con criptomonedas. Se ha expuesto que Rusia en conjunto con una importante compañía de servicios financieros y bancarios parece estar desarrollando un sistema de monitoreo de diversas criptomonedas como Bitcoin a través del Servicio de Monitoreo Financiero de Rusia. Este sistema les permitiría identificar patrones de actuación en el mercado e identificar usuarios, así como crear una base de datos de billeteras relacionadas con actividades ilegales y financiación del terrorismo (U111, 2021). También se ha debatido sobre cuál sería la situación de los usuarios en el caso de que se consiga rastrear toda la actividad de una billetera de Monero (U75, 2020) y cómo sería la profundidad de la información que podría obtener de las billeteras (U52, 2021) o si la aparición del ordenador cuántico podría acabar con toda la criptografía existente y por tanto con la funcionalidad de las criptomonedas (U137, 2021).

Por otro lado, también han sido objeto de reflexión otras cuestiones de las criptomonedas como su verdadero valor en comparación con el dinero fiduciario. Se compara esta tecnología con el dinero fiduciario y se explica cómo ha sido la evolución del valor de este desde el patrón oro y sus orígenes (U185 y U186 en U187, 2021). También se trata cómo ha aumentado el precio de las criptomonedas (BTC, EH, XMR, etc.) y cómo cada vez es más difícil comprar algún producto (p.ej. ilegal como la marihuana) sin sentir que se está perdiendo dinero y sobre todo sin pensar que en el futuro esa inversión perdería su valor (U188, 2021).

Por todo lo anterior, el foro se muestra como un espacio en el que los usuarios hacen consultas, comparten dudas, dan recomendaciones y proporcionan ayuda a usuarios menos experimentados. No obstante, algunos usuarios han participado en varias discusiones en las que exponen que no es admisible cualquier comportamiento en el foro y responden a ciertos comentarios de forma directa, crítica e incluso descortés. Aunque de forma general muchos usuarios se muestran inconformistas y muestran su descontento hacia muchos temas, en este apartado se recogen aquellos comentarios que responden a los comentarios previos de otros sujetos. Los motivos para la respuesta pueden ser varios. El primero es dejar ver que, aunque se puede consultar sobre casi cualquier tema en el foro, en ocasiones hubiera sido apropiado tener un mínimo de formación previamente a realizar preguntas excesivamente básicas en el foro:

> *All of this can be read on moneros FAQ (on their official website), low effort posts will receive low effort responses* (U50 en U189, 2021).

En segundo lugar, se encuentran las respuestas a aquellos usuarios que con baja experiencia en la utilización de criptomercados y tecnologías relacionadas deciden escribir en el foro exponiendo sus problemas y cuestionando la fiabilidad del mercado utilizado:

> *Stop trying so hard to bring down this service. At this point is clear that you are you talking shit. Wanna get all this fixed? Show the pgp signed msg from your transaction! is so hard to follow the instructions? If you cant then you should not be here. **Newbies, always READ and do what the fucking instructions say* (U190 en U59 ,2021).

En tercer lugar, se han encontrado respuestas de usuarios que señalan a aquellas personas a las que consideran que por los servicios o productos que ofertan están estafando a la comunidad:

> *What kind of idiot do you think will deposit above 1 bitcoin into an unverified escrow service? Jesus fucking Christ, at least show some creativity if you want to be a scamming piece of shit* (U191 en U160, 2021).

Por último, se recogen los comentarios de aquellos usuarios que culpan y responsabilizan a las personas que en sus discusiones dejan ver una baja formación y

actuaciones negligentes que ponen el riesgo su identidad o incluso la seguridad del resto de los miembros:

> *I don't understand how people can break the law so easily without any kind of preparation or research. It took me over 1000 hours of research and preparation before I started doing my illegal hustle. But then you got dudes like you who just buy drugs straight from their coinbase accounts!?!?!? Idk is it confidence or big balls or something?? Sometimes I wish I had that ability to just say "fuck it" and just hope for the best* (U124 en U12, 2020).

Además de las quejas y reflexiones, también es habitual encontrar en el foro algunas discusiones en las que se exponen casos de personas relevantes e influyentes para la *Darknet* y sus mercados delictivos. El motivo es que el resto de la comunidad de las criptomonedas pueda conocer los detalles de su actividad que los expusieron a un elevado riesgo de ser detectados y detenidos por las autoridades y de esta forma, no cometer los mismos errores y mantener la seguridad.

Son frecuentes las discusiones en las que se trata el caso de Ross William Ulbritch conocido como "Dread Pirate Roberts" que se convirtió en una persona muy relevante por crear en 2011 el criptomercado de la *Darknet* "Silk Road", el primer mercado web basado en TOR y el primero en usar Bitcoin como forma de pago. Las discusiones giran en torno a la pena desproporcionada a la que fue condenado, considerada como injusta por la comunidad y sobre la forma en la que lo detuvieron (U192, 2021).

Tal es el interés de los miembros del foro en que se conozcan estos casos paradigmáticos, que hay algunos usuarios que hacen una recopilación de los más relevantes con todo detalle. Junto con el anterior, incluyen también al cofundador del mercado Alphabay (U193, 2020). Además, en relación con los casos también se ofrecen consejos para evitar asumir los mismos riesgos que los detenidos. Del caso del cofundador de Alphabay se expone lo siguiente:

> *Lesson we can learn from that is to avoid using anything personal when testing, and to ensure you don't leave anything sensitive in. Another lesson is keep everything seperate. Don't mix your real identity with your dark web one* (U193, 2020).

Y del caso de Silk Road para la detención de Ross Ulbritch:

> *What can we learn. Don't reuse usernames. And be careful when marketing a hidden service. Keep the accounts totally seperate. Don't talk to much about beliefs. don't order multiple fake ID's at the same time. And there are probably a couple more* (U193, 2020).

También hacen referencia al caso de la detención del propietario de un mercado cocido como "Insta" del que se obtuvo su billetera Ethereum y se pudo tener acceso a toda la actividad realizada con esta moneda. Los consejos en este caso se dirigían especialmente a la utilización de monedas privadas como Monero:

> *If "Insta" was using Monero with that exchange guy. The agent couldn't find out his wallet address on Blockchain network even after searching his phone device. So please save your life, use Monero and remove bitcoin and other coins from your life completely. Even in 20 years they can find a wallet that was attached to you and then come after you* (U41, 2021).

Discusión

Los resultados del cuarto experimento han contribuido de forma empírica al conocimiento sobre las motivaciones y las formas en las que se utilizan las criptomonedas en el desarrollo de una actividad delictiva.

Aunque el propósito inicial de la investigación era la búsqueda de las motivaciones delictivas, como resultado de la investigación se han identificado seis temas frecuentemente tratados en el foro y que han sido de interés.

Uno de los temas mayormente tratados y por tanto del que más discusiones se ha obtenido ha sido el relativo a evitar la detección ilegal de la actividad. Dentro este tema a su vez se han incluido otros subtemas: obtención de las criptomonedas, cómo escapar de la detección de las FCSE y otras autoridades, rutas para mantener el anonimato, tipo de criptomonedas preferentes, utilización de tecnologías adicionales, retiro de las criptomonedas y formas de enmendar el riesgo de detección. El subtema más tratado ha sido el de la obtención de criptomonedas. De forma general, para la obtención o compra de criptomonedas se recomienda no utilizar casas de cambio que dispongan de políticas de KYC. Si estos servicios fueran intervenidos por las autoridades, se podría tener acceso a las identidades de los usuarios vinculadas a las direcciones por lo que se podría trazar el patrón de actuación. En su lugar, se recomienda la utilización de casas de cambio descentralizadas o servicios P2P como, por ejemplo, “LocalMonero” con la utilización de la criptomoneda Monero. Este permite el intercambio de criptomonedas entre dos usuarios interesados en la compraventa, sin que haya intermediarios. Si se dispone de algún tipo de medida como la verificación de la cuenta, se recomienda en el foro la utilización de identificación falsa. Los cajeros de criptomonedas son otro medio interesante para la obtención de criptomonedas, porque permite la compra utilizando dinero en efectivo. No obstante, disponen de diversas medidas de seguridad tanto físicas como las cámaras de vigilancia en los establecimientos, como durante el servicio. Al mismo tiempo, las tarjetas prepago son una opción interesante para la compra porque también permiten el uso de dinero en efectivo, sin embargo, presentan unas tasas más elevadas y no gozan de tanta disponibilidad de uso como otros medios. En cuanto a las tarjetas de crédito y débito, resultan un método de compra de criptomonedas atractivo para aquellos usuarios que prefieren utilizar un método de pago con el que ya estén

familiarizados. Las casas de cambio o los servicios de compra P2P resultan más difíciles de utilizar para la mayoría de los usuarios. Además, son más accesibles y no requieren de la disposición, gestión y manipulación de dinero en efectivo (tienen también medidas KYC).

Por todo lo anterior, en relación con la obtención o compra de las criptomonedas, las discusiones giran en torno a consultar y aconsejar formas de superar las medidas de seguridad que derivan de las políticas de KYC presentes en diferentes medios (ATM, tarjetas de débito y crédito, etc.). Así, se realizan propuestas como la obtención de identidades falsas, teléfonos desechables, protección física como la cara cubierta, etc. En este sentido es interesante que, aunque hay unas formas más recomendables que otras para comprar criptomonedas, en general se han considerado las ventajas e inconvenientes de cada una de las propuestas, atendiendo a la disponibilidad que cada usuario pueda tener para utilizar un método u otro. Se considera que será el sujeto interesado el que tendrá que valorar qué método es más favorable para su caso considerando aspectos como los riesgos para la detección, los beneficios que le puede reportar el delito y la disponibilidad de cada método.

En cuanto a las formas de escapar de las FCSE y otras autoridades, es interesante el hecho de que los usuarios han afirmado que conocer el funcionamiento de estos organismos les permitirá prepararse y modificar sus actuaciones. Las detenciones que se producen en este ámbito no se deben al rastreo y la monitorización que las autoridades realizan de las actividades con criptomonedas. Es necesaria una información adicional que vincule la dirección de una cartera con una identidad en concreto. En este punto es donde tienen especial relevancia las políticas de KYC que tienen como objetivo recopilar la información suficiente que permita a las autoridades establecer este vínculo. Los usuarios del foro, que son conocedores de este hecho, advierten sobre las medidas que serán necesarias para impedir esta detección, como son la evitación de las casas de cambio con políticas KYC, la utilización de la criptomoneda Monero y controlar la cantidad de criptomonedas que se transfiere. De esta forma, es interesante el hecho de que se marcan los límites a las actuaciones de detección y persecución por parte de las autoridades de este tipo de criminalidad. Una vez conocidos estos límites, se recomiendan formas de actuar para evitar las medidas de las políticas de KYC sin que esto pueda suponer la evitación por parte de los usuarios de la utilización de las criptomonedas.

En cuanto a las rutas de conversión entre criptomonedas, se trata de una forma de operar con criptomonedas muy popular entre los usuarios del foro. Supone una forma de protección ante posibles rastreos y monitorizaciones de las criptomonedas, de forma que la fragmentación no permita el descubrimiento de la actividad al completo. Aunque se disponen

de diversas alternativas de rutas, una gran mayoría de las propuestas encontradas comienzan con la compra de la criptomoneda Bitcoin. Este hecho resulta de interés porque pese a que es conocida la transparencia de la Blockchain de Bitcoin, no se prohíbe la utilización de esta criptomoneda. En aquellas rutas en las que se comienza con la compra de Bitcoin se añaden más elementos de conversión que puedan asegurar la posterior protección de la privacidad. De igual forma sucede con la utilización de las carteras privadas, que no son tan frecuentes como aquellas de carácter público. Se puede observar mucha flexibilidad en la elaboración de las diferentes rutas de conversión, siendo dos los puntos que siempre permanecen constantes y que además son señalados por los usuarios como los más importantes: convertir las criptomonedas públicas a otras privadas antes de enviar a un mercado y no utilizar las criptomonedas en un mercado justo después de haberlas comprado. Todo ello resulta de interés porque suponen formas de evitar la detección que no se centran únicamente en la prohibición de una tecnología en concreto. Por ello, se considera la amplia disponibilidad de la criptomoneda Bitcoin como forma de pago y teniendo en cuenta este hecho se ofrecen posibilidades para que los usuarios puedan utilizarla protegiendo su privacidad y evitando la detección por parte de las autoridades.

La criptomoneda más frecuentemente recomendada en el foro para la evitación de la detección ilegal es Monero. Su utilización es recomendada en la mayoría de todas las discusiones analizadas ya que su diseño permite garantizar una mayor privacidad. Además, señalan que Bitcoin presenta elevadas tasas y tienen una mayor atención por parte de las FCSE y otras autoridades. Hasta la fecha, ni las autoridades ni las empresas privadas han podido rastrear Monero y descubrir su actividad, lo que la dota de una elevada seguridad. También, aunque en menor medida, se ha visto la utilización de la criptomoneda alternativa Litecoin que ha supuesto una opción de criptomoneda pública con menores tasas que Bitcoin. Sin embargo, los resultados que se han obtenido del estudio del foro arrojan que, aunque se recomienda la utilización de Monero para una mayor seguridad de la actividad, en ocasiones se asume que esta utilización no es posible por diversos motivos como la dificultad de uso para algunos usuarios, así como la no disponibilidad de esta criptomoneda como forma de pago o por parte de otros usuarios para realizar las transacciones. Por ello, es más deseable establecer diferentes rutas de conversión de criptomonedas en las que se asegura la protección de diversas formas.

En cuanto a las tecnologías adicionales para ocultar la actividad delictiva, en el foro son frecuentemente comentados los *mixers* y las carteras privadas. Se presentan como tecnologías capaces de añadir una capa extra de privacidad a la actividad delictiva realizada

con criptomonedas. Sin embargo, es interesante el hecho de que, aunque estas tecnologías han sido señaladas en diversas ocasiones por considerar que facilitan la actividad criminal, su utilización no goza de una amplia popularidad en el foro e incluso se desaconsejan en diversas ocasiones. Se han visto numerosos casos en los que los *mixers* resultaron ser estafas en las que los creadores se apropiaban del dinero de los usuarios. Además, el interés que se le presupone para la criminalidad ha ocasionado que las autoridades pongan el foco sobre estas tecnologías por lo que su utilización contribuye a señalar una dirección como sospechosa de haber realizado un delito. Por todo ello, se ha desaconsejado su utilización y al contrario de lo que se puede pensar, no son tan frecuentemente empleadas.

Por último, el *cashout* o conversión de nuevo al dinero fiduciario supone uno de los pasos importantes para obtener los beneficios del dinero obtenido en criptomonedas mediante el desarrollo de un delito. Para los criminales se trata de una actividad de riesgo, ya que supone de nuevo la conexión de las criptomonedas con una identidad real que será la que obtenga el dinero fiduciario. En el foro este proceso es muy comentado y se proponen dos formas de llevarlo a cabo: utilizándolas para comprar dinero fiduciario o utilizándolas para comprar bienes de valor. En el primer caso se utilizan cuentas bancarias ajenas o cajeros automáticos, sin embargo, las medidas de seguridad son similares a las señaladas en la obtención de las criptomonedas. En el segundo caso, la dificultad reside en la disponibilidad de compra de dichos objetos con criptomonedas, esto es, no hay tanta oferta de compra de productos de valor como joyas o tarjetas regalo utilizando criptomonedas. Ha sido mucho más discutido en el foro el primer caso, en el que se señalan las medidas de seguridad que se tendrán que superar si se elige dicha opción. Se recomiendan de nuevo otras formas de vender las criptomonedas a través de servicios P2P. De esta forma, al igual que la compra de las criptomonedas, la venta de estas supone la superación de las medidas de seguridad derivadas de las políticas de KYC. Los sujetos tienen que valorar estos riesgos antes de la utilización de la tecnología en sus actividades delictivas. No obstante, en el caso de los productos de valor, la posibilidad de que se realice esta compra está sujeta a la disponibilidad de la oferta, por lo que puede que en algunas ocasiones no sea posible.

Aunque se supone su utilización en una gran variedad de delitos, se ha visto que esta tecnología se ha relacionado con mayor frecuencia en el foro con delitos de ataques *ransomware*, *carding* y blanqueo de capitales. En los dos primeros ocupa el rol de sistema de pago y en el último el de ocultación del rastro ilícito del dinero. Es habitual que se describa la forma en la que es más efectiva la realización del delito, no solo en cuanto a beneficios, sino también en relación con mantener la privacidad, el anonimato y evitar el riesgo de detección.

Por ejemplo, el delito de blanqueo consta de varias etapas y si intervienen las criptomonedas habrá que considerar la superación de medidas de seguridad en algunas de estas como, por ejemplo, en la utilización de un ATM y los límites que se pudieran imponer. Además de la forma en la que se desarrollan, también se tratan los riesgos que pueden ocasionar como, por ejemplo, ser víctima de un delito como una estafa. Por tanto, es interesante en este caso el hecho de que, aunque se presume que la utilización de las criptomonedas sería favorable en todo tipo de delito, los usuarios realmente solo estarían interesados en su implementación en ciertos delitos en específico.

Sin embargo, en relación con su utilización en la criminalidad ha sido más discutido en el foro la implicación de la criptomoneda en las operaciones realizadas en los criptomercados de la *Darknet*. En este tipo de discusiones, además de detallar la forma en la que se debe llevar a cabo esta actividad, se habla del funcionamiento de diversos tipos de mercados. El foro contiene una gran cantidad de información dirigida tanto a compradores como a vendedores para utilizar y gestionar el mercado. De la misma forma que en apartados anteriores, la actividad en los mercados habrá de seguir unas medidas de seguridad dirigidas a evitar la detección de los usuarios y su identificación. Por ejemplo, son importantes el hecho de no utilizar criptomonedas después de su compra o vigilar el límite de transacciones que se realizan.

Las características técnicas de las criptomonedas han ocasionado que su utilización sea compleja para algunos usuarios. Por ello, se ha visto en el foro la posibilidad de pagar a otras personas por el desarrollo de algunas tareas que conllevan la utilización de criptomonedas, como, por ejemplo, su implementación en un mercado delictivo. También se ha observado que existen ofertas de trabajo para aquellas personas que estén interesadas en desarrollar alguno de los pasos de un delito a cambio del pago en criptomonedas. Este tipo de discusiones, al contrario de lo que se pudiera pensar no han sido las más frecuentes. La complejidad con la que puede ser vista en algunas ocasiones las criptomonedas ha ocasionado que se asuma la necesidad de un usuario más especializado que permita a aquellas personas menos experimentadas incluir esta tecnología en el desarrollo de sus delitos. Sin embargo, el foro presenta un carácter ampliamente didáctico en el que cualquier persona interesada en el tema podría aprender a utilizarlas. De hecho, son más frecuentes las discusiones en las que se consulta cómo realizar algunos delitos o cómo utilizar las criptomonedas de alguna forma en específico que aquellas en las que se ofrecen “contratos” para la realización de estas tareas.

Muy relacionado con lo anterior se encuentra el apartado sobre lecciones de ciberseguridad y la utilización de criptomonedas. Aunque puede parecer similar a lo ya

expuesto, en este caso se hace hincapié en que son los miembros de la comunidad del foro los que ofrecen explicaciones, consejos y recomendaciones en este espacio sin que haya habido una petición previa por parte de otros usuarios. Lo que resulta interesante de este hecho es que se puede observar una predisposición general por parte de los usuarios del foro en enseñar a sus miembros a utilizar las criptomonedas tanto de forma legal como ilegal, favoreciendo el aprendizaje autodidacta. Son habituales las lecciones sobre anonimato y privacidad de una forma teórica a través de la explicación de algunos conceptos y de una forma práctica a través de las explicaciones sobre las políticas KYC de algunas casas de cambio, tipos de criptomonedas que utilizar, carteras, etc. Pero esta intención no solo se observa en este apartado, sino que, de forma general, en los diversos apartados del foro se puede ver que los usuarios responden de forma altruista a las dudas planteadas, en ocasiones con información muy detallada con el propósito de que se comprenda la respuesta y se aprenda. Este es el caso también de las formas de operar en los mercados de la *Darknet* para los que los propios gestores del foro han elaborado un manual de uso dirigido tanto a los clientes como a los vendedores. También coincide esta motivación con el apartado de la evitación de la victimización. Aquellos usuarios implicados en estas actividades pueden ser al mismo tiempo autores y víctima de este tipo de delitos. En este entorno podrían ser víctimas de estafa por la utilización de un falso mercado, víctimas de *phishing* por utilizar enlaces *onion* fraudulentos o víctimas de *blackmail* recibiendo mensajes en los que se pide una determinada cantidad de dinero a cambio de no revelar información comprometida. En estos casos, muchos de los usuarios exponen su victimización y consultan su situación en el foro. Muchos de los miembros del foro están predispuestos a explicarles la situación y ayudarles a evitar que la victimización adquiera una mayor gravedad. Para evitar tanto como sea posible la victimización por parte de los mercados de la DN también suelen exponer aquellos que se consideran poco fiables y para los que se desaconseja su utilización. Si bien es cierto que la mayoría de los miembros del foro explican de forma paciente y detallada la consulta realizada, los errores cometidos o el riesgo asumido y proponen soluciones, este no es el único perfil de usuario que se puede encontrar. Aunque en menor medida, hay otro grupo de usuarios que señala los errores cometidos como inadmisibles, señalan a los usuarios que han cometido tales riesgos y en ocasiones favorecen su humillación.

Por todo lo anterior, no sería necesaria la contratación o pago a otros usuarios para utilizar las criptomonedas en los delitos. En el caso de que se realizara este pago, sería por motivos de delegación de la carga de trabajo en el grupo criminal o porque el sujeto no está

predispuesto al aprendizaje de las técnicas, por lo que no se podría hablar de una necesidad real.

En cuanto a la regulación de las criptomonedas, los usuarios se muestran interesados en conocer los cambios legislativos y las nuevas regulaciones en materia de criptomonedas para poder adaptar sus actuaciones. Por ello, consultan sobre las medidas vigentes en un país o sobre su alcance, en especial, sobre aquellas que consisten en políticas de KYC. Lo interesante en este caso han sido las discusiones que se han generado al respecto en las que se han formado diversos grupos de opinión. Por un lado, se contaba con grupos que se mostraban escépticos a la efectividad de las medidas, que eran consideradas como fácilmente superables. Por otro, aquellos usuarios que exponían que las medidas harían efecto para los sujetos menos experimentados en la materia. Esto puede dejar entrever el hecho de que los sujetos del primer grupo consideran que las medidas de KYC no inhiben de la utilización de esta tecnología, sino que motivan para asumir los riesgos y mejorar la seguridad personal. Esto es, todavía consideran que las medidas dejan una oportunidad para adaptar las formas de comisión y continuar con la actividad delictiva. Es por esto por lo que al mismo tiempo sostienen que dichas medidas no están basadas en evidencia delictiva real y que solo responden a las peticiones populares de las autoridades, constituyendo un monitoreo y una persecución exacerbada de los ciudadanos sin que haya un problema real con este tipo de criminalidad. Muchos de los delitos que se cometen con criptomonedas ya existían mucho antes de la incorporación de esta tecnología, por lo que una nueva regulación en este sentido solo ocasionaría una nueva modificación en la forma en la que son desarrollados.

Por último, es importante señalar la relevancia que tiene el foro como un espacio de discusión y debate que ha supuesto una fuente de información muy valiosa. El formato en el que se presenta este espacio, además de las medidas de seguridad que garantiza por estar ubicado en la red TOR, favorece que los usuarios compartan este tipo de contenido de forma amplia y con detalle. Esto ha quedado reflejado en el apartado dedicado a las reflexiones y quejas en el que se tratan temas como el presente de las criptomonedas, las actuaciones de detección más recientes, la situación de la moneda en el futuro e incluso se debate sobre la justificación de su persecución y monitoreo. Al mismo tiempo, ha permitido tener acceso a la información sobre este tipo de criminalidad directamente de sujetos que han estado implicados.

Como conclusiones, se ha podido observar que de forma general la utilización de las criptomonedas en la criminalidad está basada en una valoración de costes y beneficios. Si los beneficios que reporta la realización de un delito son mayores que los costes que presenta, se

favorece la motivación por cometerlo. Del estudio realizado se han identificado diversos costes que influyen en este balance. El primero de ellos consiste en la superación de las medidas de seguridad que se derivan de las políticas de KYC. La compra y venta de criptomonedas está condicionada por la superación de estas medidas, por lo que, en lugar de evitar totalmente su utilización, se ayuda al resto de usuarios a reducir los riesgos para la privacidad y la identidad que se afrontan con estas medidas. Si la superación de estas medidas supone un coste mayor que el beneficio que reportaría el delito se podría abandonar la actividad delictiva.

En segundo lugar, otro de los costes que se han detectado ha sido la baja disponibilidad de la tecnología. Aunque la criptomoneda Monero es más segura para la privacidad que Bitcoin, esta última no se encuentra disponible como forma de pago en muchos de los mercados de la DN. Esto limita las posibilidades de su uso y supone la inclinación por otras formas de pago disponibles, aunque puedan suponer algún riesgo para la privacidad. De igual forma sucede con el blanqueo de las criptomonedas a través de la compra de productos de valor, ya que en muchas ocasiones no está disponible el pago de bienes con esta tecnología.

En tercer lugar, otro de los costes que se han valorado ha sido una alta probabilidad de detección del delito por parte de las FCSE y otras autoridades. Se busca conocer la forma en la que las autoridades detectan y persiguen este tipo de criminalidad para tomar medidas de precaución. La percepción de una alta probabilidad de ser detectados puede suponer un elevado coste que no compense los beneficios esperados. Esto se puede ver en la utilización de los *mixers* que, aunque se espera que puedan ser una herramienta favorable para mantener la privacidad, son objeto de estudio constante por parte de las FCSE. Para reducir la probabilidad de detección se elaboran rutas de conversión entre criptomonedas que fragmentan la actividad realizada. De esta forma, para reducir este riesgo se eligen métodos más complejos para ocultar la identidad a través de la compra de diferentes tipos de moneda, el cambio a dinero en efectivo y posterior compra de criptomonedas, etc.

En cuarto lugar, una baja familiarización y una elevada dificultad de uso de la tecnología o la forma de pago puede limitar los beneficios percibidos. Así, por ejemplo, la utilización de la criptomoneda Monero se ha visto en muchas ocasiones limitada por la dificultad de uso y su baja familiarización en comparación con Bitcoin. Por este motivo, muchos usuarios han asumido los riesgos de utilización de Bitcoin y han utilizado esta criptomoneda en lugar de Monero. Esto también puede observarse en los métodos de compra cuando los usuarios obtienen criptomonedas con métodos con los que ya están familiarizados,

aunque estos puedan suponer un riesgo para su privacidad como, por ejemplo, las tarjetas de crédito o débito. Los riesgos para la privacidad no son tan elevados para los usuarios como el coste que les supone la familiarización e implementación de nuevas formas de pago.

Por último, también se ha considerado como un coste la probabilidad de ser víctima de un delito, como por ejemplo sucede con la utilización de *mixers*, que en ocasiones han sido objeto de "estafas de salida". Esto es, aquellas actividades que son percibidas por los usuarios con una alta probabilidad de ser víctimas de un delito como, por ejemplo, la utilización de mezcladores, serán evitadas, aunque puedan aparentemente ser más beneficiosas para el desarrollo de su propia actividad delictiva.

No obstante, se han encontrado usuarios en el foro que han contribuido en la reducción de los costes esperados de la actividad delictiva. Por ejemplo, en el caso de la dificultad de uso o la familiarización, se encuentran usuarios predispuestos a ayudar y a dar lecciones sobre la mejor forma de utilizar las criptomonedas con fines tanto legales como ilegales. Esto permite el aprendizaje autodidacta y reducir la necesidad de disponer de otras personas más capacitadas para realizar estas tareas. Todo esto ha llevado a que su utilización sea más frecuente en aquellos delitos que permiten gestionar los posibles costes mencionados anteriormente.

Limitaciones del Cuarto Experimento

Este experimento ha contribuido de forma empírica al conocimiento existente sobre las motivaciones para utilizar criptomonedas. La metodología cualitativa ha permitido profundizar en las discusiones y generar nuevo conocimiento que no se había considerado desde el principio. Sin duda estos resultados complementarán a los resultados de carácter cuantitativo que se obtengan en esta materia.

Sin embargo, esta investigación también presenta algunas limitaciones. En primer lugar, se encuentran las limitaciones relacionadas con las medidas de seguridad que presenta la *Darknet* y el foro "Dread" para proteger y garantizar la privacidad de sus usuarios. El acceso a este espacio requiere de la resolución de un complejo CAPTCHA que se modificaba pasados unos minutos y cada vez que se accedía de nuevo al foro. Esto imposibilitó la tarea de desarrollo de un *escrow* que recopilara de forma automática todas las discusiones que contenían el término de búsqueda empleado. En su lugar, se estudió y analizó el contenido del foro de forma analógica, sistemática e individualizada, seleccionando manualmente los resultados adecuados según los criterios establecidos. En segundo lugar, debido al funcionamiento mismo del foro, todas aquellas discusiones que ocupaban las últimas páginas

eran eliminadas cada semana. Por lo tanto, fue necesario el acceso reiterado para la recolección de las discusiones y actualmente no es posible acceder al mismo contenido salvo que se utilicen los enlaces conservados para tal fin. Esto ha imposibilitado la forma en la que se pueden compartir de forma pública los datos obtenidos para que puedan ser replicados por otros investigadores. Por último, en el último lapso de esta investigación el foro cambió su diseño y eliminó el buscador que se utilizaba para recopilar las discusiones que eran de interés. Por ello, aunque se tenía prevista una tercera etapa de búsqueda con una etapa adicional de recogida de datos, esto no fue posible debido a la imposibilidad de buscar en específico las discusiones o comentarios que son de interés. Se espera que en futuras investigaciones se permita la recolección automática del contenido para poder ampliar los resultados y el tiempo de análisis y descubrir patrones que puede que no se tuvieran en cuenta en esta investigación. Además, aunque el foro al estar ubicado en la *Darknet* ha permitido el acceso a información valiosa sobre estos delitos, en el futuro se espera poder ampliar esta investigación con el estudio de discusiones de otros foros ubicados en la internet superficial.

Capítulo 13. Estudio de la Utilización de las Criptomonedas Como Forma de Pago en Mercados *Online* de Cannabis y Productos Derivados (Experimento 5)

En este experimento se tiene como objetivo general conocer aquellas características de las criptomonedas que motivan a los criminales a utilizarlas en sus actividades delictivas. Para ello, se estudiará la implementación de esta tecnología como sistema de pago en los mercados online de cannabis y otros productos derivados en el territorio de Canadá. La pregunta de investigación general desde la que se parte es si las características de esta tecnología que favorecen la privacidad del usuario podrían motivar a una utilización con fines delictivos.

Métodos y materiales

Estrategia de investigación:

La metodología de este experimento se desarrolla conforme al enfoque de la Teoría Fundamentada descrito en el apartado general de metodología. De forma general, tiene como objeto de estudio de la utilización de criptomonedas en los mercados *online* de cannabis y otros productos derivados ubicados en Canadá.

La fuente de recogida de los datos han sido los mercados online de cannabis ubicados en Canadá. La elección de esta fuente de datos se debe a que permite conocer la información directamente proporcionada por el personal encargado de gestionar el mercado online. Además, en Canadá es legal la compra de cannabis online y de forma física siempre que el negocio sea gestionado por el gobierno o disponga de una licencia privada según los casos previstos (Tabla 22).

Tabla 22.

Legalidad de la venta de cannabis en Canadá.

Provincia[218]	En persona	Tienda online
Alberta	Licencia privada	Gestionada por el gobierno
British Columbia	Gestionada por el gobierno o licencia privada	Gestionada por el gobierno
Manitoba	Licencia privada	Licencia privada
New Brunswick	Gestionada por el gobierno	Gestionada por el gobierno
Newfoundland and Labrador	Licencia privada	Gestionada por el gobierno
Northwest Territories	Gestionada por el gobierno	Gestionada por el gobierno
Nova Scotia	Gestionada por el gobierno	Gestionada por el gobierno
Nunavut	-	Gestionada por el gobierno
Ontario	Licencia privada	Gestionada por el gobierno
Prince Edward Island	Gestionada por el gobierno	Gestionada por el gobierno
Quebec	Gestionada por el gobierno	Gestionada por el gobierno
Saskatchewan	Licencia privada	Licencia privada
Yukon	Licencia privada	Gestionada por el gobierno

Fuente: Elaboración propia a partir de los datos oficiales aportados por el Gobierno de Canadá en https://www.canada.ca/en/health-canada/services/drugs-medication/cannabis/laws-regulations/provinces-territories.html

De esta forma, serán excepciones las siguientes provincias o territorios: British Columbia, New Brunswick, Northwest territories, Nova Scotia, Prince Edward Island y Quebec. Además de aquellas tiendas que requieran del usuario un permiso para consumir cannabis con propósitos médicos[219]. Por lo tanto, entendemos que aquellas tiendas online que se encuentran en territorios donde la venta online de cannabis no está permitida de forma privada será considerada de carácter ilegal y podrá ser objeto de esta investigación.

Los datos para esta investigación han sido recopilados de forma primaria por medio de una serie de búsquedas en la web superficial empleando los buscadores "Google" y "Duckduckgo". Los términos de búsqueda empleados fueron: "cannabis canada", "buy weed in Canada", "order cannabis online nb", "weed online Canada" y "order weed Quebec". Se seleccionaron aquellas páginas web que pertenecían a tiendas online de cannabis y otros productos derivados cuya sede estuviera ubicada en cualquier territorio de Canadá.

Una vez se disponía de la base de datos, el contacto con los vendedores de las tiendas online se realizó a través de tres métodos: el chat de la página de la tienda, correo electrónico o por medio del teléfono móvil que ponían a disposición del cliente en el apartado "contáctanos". Esta tarea se llevó a cabo en dos etapas diferenciadas o contactos. En la

[218] Alberta: https://albertacannabis.org/; British Columbia: https://www.bccannabisstores.com/; New Brunswick: https://www.cannabis-nb.com/; Newfoundland and Labrador: https://www.shopcannabisnl.com/; Northwest territories: https://www.releafnt.ca/#/menu; Nova Scotia: https://cannabis.mynslc.com/; Nunavut: https://nunacannabis.com/; Ontario: https://ocs.ca/#/verify-age; Prince Edward Island: https://peicannabiscorp.com/; Quebec: https://www.sqdc.ca/en-CA/; Yukon: https://cannabisyukon.org/

[219] https://www.canada.ca/en/health-canada/topics/accessing-cannabis-for-medical-purposes.html

primera etapa, una de las investigadoras contactaba con las tiendas de la primera mitad de la base de datos, mientras que la segunda investigadora realizaba el mismo proceso con la segunda mitad. En la segunda etapa, las investigadoras intercambiaban sus roles. De este modo, se persigue obtener las respuestas de las tiendas de una forma acumulativa, esto es, intentando obtener el mayor número de respuestas posible. El motivo por el que en la recogida de datos participan dos investigadores en dos etapas diferentes es porque se pretende asegurar una variedad de estrategias para obtener respuestas de los vendedores.

Las conversaciones que se mantuvieron durante los diferentes contactos tuvieron lugar en la lengua inglesa y aunque se tenían previstas algunas de las preguntas que podrían realizarse, en cada contacto se aprendía del anterior para realizar modificaciones o generar nuevas preguntas. El tipo de pregunta realizada también cambiaba dependiendo de si se trataba de una tienda que aceptaba criptomonedas o no. El contenido de las preguntas estaba orientado a conocer por qué se utilizan las criptomonedas como forma de pago. Un ejemplo de algunas de las preguntas que se formularon se encuentra en la tabla 23.

Tabla 23.

Preguntas realizadas a las tiendas online de cannabis.

Tiendas que aceptan criptomonedas
Hi! It's super cool that you accept payment in BTC! Just out of curiosity, why can I use it here and not in other stores?
I am surprised that you have bitcoin as a payment option. Just out of curiosity, why can I use my crypto in your shop and not in other similar shops? Stay safe!
Hi! I have been recommended your store and I am amazed! I can pay with my cryptocurrencies! it is not easy to find a store where I can use them. Just out of curiosity, why did you decide to introduce Bitcoin as a payment method? It would be great if I could convince the other stores to use it too :P
Tiendas que no aceptan criptomonedas
Hi! I'm interested in your store; can I pay my order with BTC?
Will you accept BTC in the future?
What is the reason why I can't pay with BTC in this shop, but I can in other similar shops?
You have good prices. Why BTC is not accepted? I would really like to buy here…
Hi! I have a question about the order. I would like to know if I can pay with BTC.
Hi, I would like to buy from your shop, but I don't see any option to pay with BTC. Can I pay my order with BTC?

El análisis de las conversaciones se llevó a cabo utilizando "NVivo", un software informático de análisis de datos cualitativo cuya función principal es el análisis de los datos en diversos formatos como texto, imágenes, audio y vídeo con carácter no estructurado. De acuerdo con el enfoque de la Teoría Fundamentada se realizó una primera lectura de todas las conversaciones partiendo de la pregunta general de investigación sobre las motivaciones para utilizar las criptomonedas. De esta primera lectura se elaboraron unos códigos que se introdujeron en el programa, comenzando a agrupar los datos en estos. Del posterior análisis de la totalidad de la muestra se extrajeron los temas tratados y se elaboraron el resto de los códigos, que fueron introducidos en el programa (Apéndice 3). Estos se dividen en dos grupos según si la tienda acepta o no criptomonedas como forma de pago y las abreviaturas han sido realizadas a partir de su significado en inglés.

Descripción de la Muestra

La base de datos creada constaba de 205 páginas web con variables que se pueden dividir en tres grupos (Se puede ver el listado en el Apéndice 4). El primero incluye variables sobre la búsqueda realizada como las palabras claves o el motor de búsqueda empleado. El segundo grupo incluye datos relevantes de la tienda online como el sistema de pago con criptomonedas o no, envíos, localización, métodos de contacto, enlace a la web y otros comentarios. En el último grupo se incluyen las variables relativas al proceso de contacto con las tiendas online, esto es, investigadoras encargadas de contactar, respuestas obtenidas, primer y segundo contacto y fecha y método de contacto.

Una vez creada la base de datos se realizó una limpieza de aquellos registros que no eran válidos para el fin de esta investigación. En este caso son de interés sobre todo las variables relacionadas con el sistema de pago en cada tienda. De esta forma, se ha considerado eliminar cuatro registros de tiendas para las que la forma de pago no estaba disponible de forma visible, siendo necesario aportar información personal que hubiera puesto en peligro la identidad de las investigadoras. Las páginas eliminadas son: "Acreage Pharms", "CannMart", "Herbal dispatch" y "Weed canada".

Finalmente, se dispone de un total de 201 páginas relativas a tiendas online de cannabis en Canadá. Si se consideran las criptomonedas como método de pago en estos mercados estas quedan divididas en 153 tiendas que no aceptan criptomonedas y 48 tiendas que sí las aceptan, siendo estas en su mayoría Bitcoin (Tabla 24).

Tabla 24.

Aceptación de criptomonedas como forma de pago en las tiendas.

¿Aceptan criptomonedas?	Total
NO	153
SÍ	48
Total	**201**

El número de respuestas obtenidas al contactar con las tiendas se presenta en dos tablas diferentes según si se trata del primer o el segundo contacto con la tienda. En el primer contacto se obtuvieron 104 respuestas frente a 72 tiendas de las que no se obtuvo respuesta. Un total de 21 páginas web eran inaccesibles en el momento en el que se realizó la toma de contacto por lo que tampoco se obtuvo respuesta. Además, también se obtuvo que 4 de las páginas web se correspondían con tiendas online que, aunque realizaban envíos a Canadá, no estaban ubicadas en territorio canadiense, por lo que no eran objeto de este estudio (Tabla 25).

Tabla 25.

Respuestas obtenidas en el primer contacto con las tiendas.

¿Aceptan criptomonedas?	¿Respondieron a las preguntas?				
	No	*No funciona*	*EE. UU*	*Sí*	**Total**
NO	58	15		80	**153**
SÍ	14	6	4	24	**48**
Total	**72**	**21**	**4**	**104**	**201**

En el segundo contacto se obtuvieron 88 respuestas frente a 89 contactos para los que no se obtuvo respuesta. En este caso, fueron 20 las páginas web que no estaban operativas y de las que no se pudo establecer contacto (Tabla 26).

Tabla 26.

Respuestas obtenidas en el segundo contacto con las tiendas.

¿Aceptan criptomonedas?	¿Respondieron a las preguntas?				
	No	*No funciona*	*EE. UU*	*Sí*	**Total**
NO	70	14		69	**153**
SÍ	19	6	4	19	**48**
Total	**89**	**20**	**4**	**88**	**201**

La variación de las respuestas en el segundo contacto con respecto al primero puede deberse a varios motivos. El primero de ellos puede estar relacionado con las diversas estrategias empleadas por las investigadoras para obtener las respuestas de los vendedores. Puede que algunas de las utilizadas en el primer contacto fueran mucho más efectivas que las que se emplearon en el segundo. El segundo motivo puede deberse a un conocimiento por parte de las tiendas sobre la realización de una investigación, lo que llevó al personal a mostrarse menos predispuesto a colaborar que en anteriores ocasiones. Por último, puede haberse visto afectado por otro tipo de circunstancias incontrolables por los investigadores como las relacionadas con la actividad del mercado, esto es, su disponibilidad, cese de la actividad, etc. En cualquier caso, como se mencionó en apartados anteriores el fin de estos contactos es obtener respuestas de forma acumulativa, por lo que no resulta determinante la variación obtenida entre ambos contactos.

Las conversaciones mantenidas con las tiendas fueron recogidas tanto en formato texto como en captura de pantalla y almacenadas para su posterior análisis. Además del contenido de las conversaciones también se registraron otros datos como el nombre de la tienda, el enlace web, el día y la hora en los que tuvo lugar el contacto y si la tienda seguía operativa. Se pueden ver ejemplos de las conversaciones que se han mantenido con los mercados durante la investigación en el Apéndice 5.

Resultados

Como resultado de la investigación se obtuvo una muestra de 201 respuestas. Del estudio y el análisis de las respuestas obtenidas en relación con el objetivo de la investigación se identificaron varios temas. Al mismo tiempo, se han podido encontrar otros temas y

subtemas que no se habían previsto pero que han resultado de interés para el desarrollo de la investigación.

Finalmente, los resultados consisten en la obtención de los siguientes temas con sus correspondientes subtemas en los que se podrían agrupar todas las conversaciones estudiadas. Para aquellas tiendas que aceptan las criptomonedas como forma de pago: 1) Motivos por los que son aceptadas las criptomonedas; 2) Recomendación de otras formas de pago; 3) Situación de otros mercados respecto a la aceptación de las criptomonedas; 4) Obtención de otra información no relevante y negativas a responder. Para las tiendas que no aceptan criptomonedas como forma de pago: 1) Inconvenientes técnicos del mercado; 2) Características de las criptomonedas que dificultan la implementación; 3) Inconvenientes de la adopción para el negocio; 4) Excepción a la aceptación de criptomonedas en el mercado; 5) Persuasión para la utilización de medios de pago disponibles; 6) Probabilidad de aceptación de las criptomonedas en el futuro y 7) Respuestas no colaborativas, poco relevantes o negativas.

Los resultados se dividen en dos grandes grupos según si las tiendas aceptan criptomonedas o no como forma de pago. Dentro de cada uno de los grupos se presenta una descripción de los temas más discutidos en las conversaciones.

A continuación, se presentan de forma detallada los resultados obtenidos en relación con las diferentes temáticas:

Tiendas que Aceptan Criptomonedas Como Forma de Pago (ACC)

Motivos por los que son aceptadas las criptomonedas. En este apartado se incluyen aquellas respuestas que explicaban los diversos motivos por los que cada tienda aceptaba criptomonedas, en especial Bitcoin, como una forma de pago. Así, han surgido diversos motivos como respuestas en las conversaciones:

Mejora Para la Rentabilidad del Negocio (ACC_buss). La introducción de las criptomonedas como forma de pago en los mercados también ha venido motivada por la búsqueda de la mejora del negocio para obtener una mayor rentabilidad.

En este sentido, su introducción se debe por un lado a la intención del mercado de disponer de una amplia variedad de formas de pago novedosas y actualizadas. De esta forma, los vendedores pretenden que este aspecto no pueda suponer una limitación para realizar la compra en su mercado y así atraer a un mayor número de potenciales clientes:

> *Me: Hi! I have been recommended your store and I am amazed! I can pay with my cryptocurrencies! It is not easy to find a store where I can use them. Just out of curiosity, why did you decide to introduce Bitcoin as a payment method? It would be great if I could convince the other stores to use it too :P*

Them: We introduced the option to pay via Bitcoin simply to provide our customers with another easy option of payment (M1[220]).

Me: Sorry to bother you. I think it's great that I can use my cryptocurrencies in your shop!!It's not easy to find a good weed shop to use them in. Just out of curiosity why did you decide to introduce BTC?
Them: Glad to hear that! We are constantly looking to improve our company to provide the best experience possible for our customers. We decided to offer a different type of method, that being bitcoin, as it gives everyone other options than just our interac e-transfer. Especially with the increase in cryptocurrencies being used around the world, we wanted our system to stay up to date (M2).

Consideran que la disponibilidad del pago con Bitcoin en su mercado solo constituye una opción más que ofrecer a las personas interesadas en comprar sus productos, pero al mismo tiempo muestran preocupación por las necesidades de los clientes:

Me: Hi! I have been recommended your store and I am amazed! I can pay with my cryptocurrencies! it is not easy to find a store where I can use them. Just out of curiosity, why did you decide to introduce Bitcoin as a payment method? It would be great if I could convince the other stores to use it too :P
Them: It's as good as any other currency to us so why not, it also adds a little extra privacy to buyers (M3)

Pero también consideran que la utilización de las criptomonedas en su actividad comercial podría suponer una mejora en el mercado. Estas mejoras aumentarían la confianza de los usuarios en esa tienda y podrían atraer a un mayor número de potenciales clientes para aumentar sus beneficios. Se trata en este caso de mejoras como la seguridad o la efectividad del negocio:

Me: oh that's great!! It's difficult to find a store! Why did you add Bitcoin as a form of payment?
Them: We accept Interac Bitcoin as this is a safe payment method for the nature of our business! (M4).

Me: Ah ok… why do you decide to accept BTC?
Them: We think it is the safest for our customers and us, also the fastest (M5, Figura 13, Apéndice 5).

Petición de los Clientes de la Inclusión de las Criptomonedas (ACC_cust). Aunque algunas tiendas no las incluyeron en sus orígenes, la creciente demanda de los clientes que deseaban utilizar criptomonedas en su compra las motivó para incluirlas entre las opciones disponibles. Estas peticiones han sido realizadas de forma general hacia el mercado, sin ofrecer demasiados detalles:

Me: Just curiosity, why did you choose this option in the end? I have been waiting a long time for this store to accept BTC.
Them: We noticed that a lot of people asked about BTC so we decided to put it. Thank you for being patient and we're happy that you can use this option for payment now! (M6, Figura 14, Apéndice 5).

[220] La abreviatura M1 significa "mercado 1". Se utilizará la letra "M" para denominar a los mercados junto con su correspondiente número por orden de aparición en el texto.

Aunque en algunas ocasiones se pide la inclusión de las criptomonedas como alternativa a otras formas de pago más tradicionales que se usan habitualmente en estos mercados como es en Canadá el pago con "e-transfer":

> *Me: Hey! I am surprised that you have bitcoin as a payment option. Just out of curiosity, why can I use my crypto in your shop and not in other similar shops? Stay safe!*
> *Them: Hello! My sincerest apologies for the delayed response! That is a good question! We decided to start accepting bitcoin due to the volume of customers who asked for an alternative to etransfer. Bitcoin and Ethereum were the most requested payment options, and our goal is to be able to serve our com community as easily and effectively as possible. Please let me know if you have any further questions and I will be more than happy to help!* (M7).

O bien porque asumen que los clientes conocen ciertas características de las criptomonedas que los podrían beneficiar en el desarrollo de sus negocios. Por eso, relacionan esta petición de uso con la necesidad de disfrutar de estas ventajas, como el supuesto anonimato o la sensación de seguridad al utilizarlas:

> *Me: Hi! So cool that I can pay with crypto in your store! It's not easy to find a store like this! Why did you introduce it? Do you know why other stores similar to this one doesn't introduce it? Stay safe!!*
> *Them: Hello, most other dispensaries do offer cryptocurrency payments as well. We introduced it for convenience as a lot of our customers want to remain anonymous* (M8).

> *Me: Hey! It's great that you accept bitcoin! I tried to buy in your shop last year and it was not possible to use this currency. Just out of curiosity, why did you introduce this payment method? I can't use my cryptocurrencies in other similar shops.*
> *Them: Hi there, I am not sure of the specifics but I'm sure one of the reasons would be because of how crypto cannot be traced therefor some customers feel safer paying this way.*

Aspectos de las criptomonedas que motivan su aceptación. Aunque han sido menos frecuentes, también se han obtenido respuestas en las que se hace alusión a algunas características de las criptomonedas que específicamente han motivado su inclusión en el mercado.

Este es el caso de aquellas tiendas que han expuesto que las criptomonedas son más seguras que otras opciones de pago, lo que motivaría a los vendedores a ponerlas a disposición de aquellos usuarios que estén interesados en utilizarlas:

> *Me: Can I pay with BTC? I've seen the Bitcoin option in the payment part of my order. So I'm just asking If that's sure*
> *Them: Hi, yes, works well and it is secure* (M9).

> *Me: I would like to try your products, but I'm not really comfortable to share my info. I hear that crypto is much safer than e-transfer. Do you think that is the case? I am not very familiar with crypto. Can you guide me on what you think would be best? (…)*
> *Them: Yes, cryptocurrency would be the safest option if you prefer not to share your info. You can select cryptocurrency and you'll save an extra 7% on your order. Once you select cryptocurrency on the checkout page there will be a wallet address displayed on the next page with the exact amount to send. Once you send the exact amount to the provided address, we will process your order* (M8).

Incluso equiparan este nivel de seguridad con otro tipo de criptomonedas alternativas como la criptomoneda Ethereum:

> *Me: Thank you for the fast response, I really appreciate it. I have heard that BTC is more secure than e-transfer. I am not very familiar with Ethereum, is it better than BTC?*
> *Them: My apologies for the delayed response. As for as security I would say both BTC and Ethereum are similar as they are both cryptocurrencies* (M10).

Recomendación de Otras Formas de Pago. En algunos casos, la disponibilidad de las criptomonedas como forma de pago no ha supuesto que sea el método preferido por el mercado. Aunque las ofrecían como una opción de pago, algunos mercados han señalado los inconvenientes de su utilización y han recomendado otras opciones sobre el pago con criptomonedas.

Son frecuentes las respuestas en las que se recomienda a los usuarios evitar la utilización de las criptomonedas como forma de pago si no se dispone de la suficiente experiencia y especialmente si se trata de la primera transacción:

> *Me: Hi, Thanks for the quick response! Great. I'm not familiar with the process, but I really don't want to share my information. I've heard that btc is much safer than e-transfers. Do you think this is the case? Would you recommend me to pay in btc?*
> *Them: Hi Loremm, If it's your first time paying with bitcoin I don't recommend it. Bitcoin is for advanced users and we do not recommend it if it is going to be your first transaction. Have to be very careful on how you send it or it may not go through* (M11).

Los mercados explican que el pago con estas monedas virtuales requiere de una preparación previa para superar sus inconvenientes habituales como, por ejemplo, la necesidad de realizar una transacción con una cantidad de dinero exacta o sus elevadas tarifas:

> *Me: Hi, I would like to place an order in your shop but I'm not very sure about if I could use BTC to pay my order.*
> *Them: Hi there, You can use Bitcoin to pay but if you are not experienced with it then I recommend paying by e transfer. Crypto requires a lot of due diligence when sending payment. You need to send the exact amount or else it will not process automatically and apply payment to the order. You have to remember to take into account any ATM fees* (M12, Figura 23).

En ocasiones el consejo de no utilizar criptomonedas va seguido de la recomendación de otros métodos de pago más habituales como e-transfer, con el que se compara frecuentemente. Se presenta e-transfer como un método seguro, útil y fácil, habitualmente utilizado por los clientes, pero se señala que la opción de pago con criptomonedas está disponible si se prefiere:

> *Me: Hi, I would like to try your products, but I'm not really comfortable to share my info. I hear that crypto is much safer than e-transfer. Do you think that is the case? I am not very familiar with crypto. Can you guide me on what you think would be best?*
> *Them: Hi, Our e-transfer transactions are secure, convenient, and easiest to do so we always suggest using that payment method to most of our customers. But, if you're uncomfortable using it, you can pay through crypto or cash in mail. Let me know, if you've chosen which payment method to use and I'll assist you with it* (M13).

> *Me: Hi, I would like to try your products, but I'm not really comfortable to share my info. I hear that crypto is much safer than e-transfer. Do you think that is the case? I am not very familiar with crypto. Can you guide me on what you think would be best?*
> *Them: Both crypto and etransfer work the same way in a sense, once you send the transfer it is not reversible unless the receiving parts decides to send it back (…). Crypto is a more difficult to explain and I would only recommend that form of payment to people that are experienced in it as it takes many steps to setup and is mitral vulnerable to scams when trying to acquire (…)* (M3).

Exponen que las ventajas que se pudieran obtener con la utilización de las criptomonedas, como es la protección de la privacidad, puede conseguirse con métodos como e-transfer, que no son tan complejos y cuyas transacciones son más rápidas y no son tan costosas:

> *Me: I would like to try your products, but I'm not really comfortable to share my info. I hear that crypto is much safer than e-transfer. Do you think that is the case? I am not very familiar with crypto. Can you guide me on what you think would be best?*
> *Them: I understand your concerns. I have heard crypto is more secure as it doesn't show your information as much as an e-transfer does. I am not too familiar with crypto as I haven't tried it myself but have heard much about it from customers. I would like to warn you that crypto payments take some time to process and are more complicated than e-transfers. When we receive an e-transfer before 12:30pm (PST), it will be accepted right away and we process your order sooner. Simply because we receive e-transfers and can process them faster. However we do our best to make sure your form of payment (e-transfer or crypto) is accepted and to ship out your order that day if everything goes well before 12:30pm (PST) as that it our last call for shipping out orders same day (…)* (M2).

Situación de Otros Mercados Respecto a la Aceptación de las Criptomonedas.

Como parte del objetivo de comprender por qué los mercados ofrecen criptomonedas como forma de pago, también se les ha preguntado a las tiendas que tienen disponible esta opción por qué creen que otros mercados no la ofrecen. Esta es una forma de conocer aquellas características de las criptomonedas que, al contrario de lo expuesto en el apartado anterior han motivado a los mercados a su no inclusión. Esto puede ser considerado como inconvenientes para la adopción de las criptomonedas en el mercado. Consideran que otros mercados puede que no hayan incluido las criptomonedas como forma de pago porque no están dispuestos a lidiar con inconvenientes como la fluctuación de sus precios.

> *Me: Hi! It's super cool that you accept payment in BTC! Just out of curiosity, why can I use it here and not in other stores?*
> *Them: I can't speak for other stores but if I have to guess, they don't want to deal with the price fluctuations with crypto* (M14,Figura 15, Apéndice 5).

La adopción de esta tecnología puede ser más compleja y difícil de gestionar que las formas de pago tradicionales como e-transfer y, por tanto, los mercados que no están familiarizados con esta deciden no adoptarla entre sus opciones de pago:

> *Me: Yeah, you're right! Why other shops won't offer that option?*
> *Them: I'm not too sure. My guess would be that the set up for crypto payments is more complex and harder to manage than e-transfers* (M2).

Me: Thank you very much for answering! That's great! So if it's becoming popular, why do you think other stores similar to yours don't accept it?
Them: They're probably not familiar with taking in payments for crypto (…) (M11).

Respuestas No Colaborativas, Poco Relevantes o Negativas. En ambos contactos realizados con los mercados se han realizado preguntas similares a todas las tiendas. En algunos casos, aunque se han respondido a las preguntas, esta respuesta no guardaba relación con la pregunta realizada. Esto es, se obtenía información adicional, pero no se correspondía con la información que se requería, lo que ha sido considerado como información no relevante para la investigación. El motivo de esto puede estar relacionado con la elevada competitividad existente entre las tiendas de cannabis y otros productos, que las obliga a mantener unos altos estándares en cuanto al trato con los clientes. Por ello, se ofrecía una respuesta, aunque esta no guardara relación con la pregunta realizada.

Por otro lado, también se han obtenido respuestas que pudieran entenderse como una negativa a colaborar con el interés del usuario por conocer más allá de lo que está disponible en la página web de la tienda:

Me: Hi, I was shopping on your site and while doing the checkout I realized that it only had etransfer. Is it possible to pay by bitcoin?
Them: Yes (M12).

Me: Oh great!!! I didn't see the option! It is not easy to find a store where I can use my cryptocurrencies Why did you decide to introduce this payment method?
Them: I'm not entirely sure I'm not really involved with those decisions. my apologies (M15).

Tiendas que No Aceptan Criptomonedas Como Forma de Pago (DACC)

De los resultados obtenidos se observa que son mayoritarias aquellas tiendas que no aceptan criptomonedas como forma de pago. De esta forma, en este apartado se muestran los temas que se han extraído de las respuestas dadas a las preguntas realizadas a aquellos mercados que no disponían de criptomonedas entre sus opciones de pago.

Inconvenientes Técnicos del Mercado. En ocasiones, la no disponibilidad de las criptomonedas como forma de pago ha estado relacionada con algunos inconvenientes de carácter técnico en los mercados que dificultaban su implementación.

Habitualmente no se ofrecen detalles sobre el tipo de inconvenientes técnicos que tendría que afrontar el mercado para llevar a trámite esta implementación, en su mayoría exponen únicamente que existe y que el sistema no está preparado para aceptar pagos con criptomonedas en esos momentos y que no sabrían cómo gestionar este pago:

Me: Excuse me, but what is the reason? I am very interested in the prices of your store and I need to buy a large quantity of weed…

> *Them: Hi Kat, we unfortunately are not accepting BTC as our system is not set up to accept it at this time. Sorry for the inconvenience* (M16, Figura 16, Apéndice 5)

> *Me: oh god. Why is this? I really like your prices but man, I'm worry about my privacy...*
> *Them: I understand your worried about your privacy and btc would be the better option but for us btc just isn't something that we can set up at the moment as we have never dealt with btc and have no idea what we're doing with it to be honest* (M17).

En algunas ocasiones se han señalado algunos aspectos de manera concreta. Por ejemplo, se ha señalado que el mercado no dispone de una cartera Bitcoin en la que se pueda recibir la transferencia:

> *Me: oh god. Why is this? I really like your prices but man, I'm worry about my privacy.*
> *Them: Unfortunately, we don't have a crypto wallet. It's something we haven't integrated yet. We understand your concerns* (M18).

Otras respuestas no están tan relacionadas con cuestiones técnicas como con otro tipo de dificultades del mercado que impiden la incorporación de esta opción. Es el caso de aquellos mercados que han expuesto carecer de una licencia oficial del gobierno, lo que dificultaría que fueran elegibles para ofrecer otro tipo de opciones legales de pago:

> *Me: ohhh God. Why is that?*
> *Them: The banks see the funds as going to an illicit source because we do not hold a license from the government, so they choose to not take us on as clients for debit/credit payments* (M19, Figura 17, Apéndice 5).

In another case it is stated that the market owner was not familiar with cryptocurrencies and therefore was not willing to include them as a payment option:

> *Our owner is a senior citizen*
> *That likely has something to do with it*
> *You know how the older generation is with new technology like crypto*
> *I think it's neat and I hold crypto myself, but it's not for everyone* (M19, Figura 18, Apéndice 5).

Características de las Criptomonedas que Dificultan la Implementación. Algunas de las características propias de las criptomonedas pueden dificultar su introducción en determinados mercados. Los propietarios de las tiendas online que son conocedores de estas características han señalado muchas de ellas como la razón por la que no han decidido introducir esta moneda virtual entre sus opciones de pago.

Uno de los aspectos más comentados es el pseudoanonimato de criptomonedas como Bitcoin. Muchas de las respuestas obtenidas han sugerido que la mayoría de las tiendas no están interesadas en Bitcoin como forma de pago porque es posible conocer el rastro del dinero y se puede poner en riesgo la privacidad de la actividad comercial:

> *Me: Oh my, why is that? I really like your products and your prices, but I appreciate my privacy. I think that BTC is the safest way of payment. It's hard to find a store to use my cryptocurrencies in, I don't understand why.*
> *Them: Thank you for the kind words. We apologize for not accepting bitcoin but bitcoin transactions are also traceable. So, it isn't fully anonymous like many people think it is. Interac e-transfers are very*

safe because your bank will protect its customers and they spend hundreds of millions into preventing their customers from fraud and identity theft (…) (M20).

Thank you, at the moment we don't accept BTC! Also just for your knowledge, BTC can be traced, it is just really hard to do so. Regarding your information, you are able to put a fake name, but we will need to check your ID at the door :) (M21).

Señalan que, aunque algunos clientes piden la utilización de las criptomonedas como forma de pago con el objetivo de proteger la privacidad de su actividad, muchos de ellos no conocen la posibilidad de rastreo de la moneda.

Otro de los aspectos de las criptomonedas al que se ha hecho referencia en las conversaciones ha sido su volatilidad:

Me: oh, that's a pity. I really like your prices. Will you accept it in the future?
Them: Unlikely, as Bitcoin has been volatile (M22).

Este aspecto las convierte en una opción de pago arriesgada y difícil de gestionar para los mercados, que tendrían que asumir continuos altibajos en su precio exponiéndolos a la pérdida de beneficios:

Me: just curiosity, what could be the drawback?
Them: The drawback? What did you mean by this
Me: for you to accept payment with bitcoins
Them: We're just not really into have BTC as it's a gamble it seems like
Them: We don't like the up and downs of the market of btc
Them: So never got into it, to each there own though (M17, Figura 19, Apéndice 5).

Por último, también se han señalado las elevadas tasas en sus transacciones como otro aspecto para tener en cuenta en su implementación en un mercado:

Me: Hi! I just need help. I've prepared my order and I thought that I could pay with crypto, but I can't.
Them: We did used to accept crypto, but the merchant fees were extremely high, and almost no one used it, so we stopped offering it. We're working towards rolling out card payments later this year, but right now it's only e-transfer (M23).

El trabajo que supondría su implementación asumiendo todos los inconvenientes que pudiera ocasionar sería mucho mayor que los beneficios que pudiera aportar, especialmente cuando esa opción de pago podría ser sustituida por otra de las más habitualmente utilizadas en estos mercados. Por ello, muchos propietarios de los mercados después de considerar este balance de beneficios e inconvenientes han decidido no introducir esta opción de pago:

Me: Ohh, What a pity! Why is that?
Them: We do not have the internal infrastructure for it. Also crypto is dicey. Owner doesn't want to deal with the hassle. Fair enough I say (M24).
Me: Oh :-(what a pity! I really like your prices! But I appreciate my privacy... Why don't you accept BTC?
Them: We don't accept any forms of electronic payments, too much hassle. too easy to cancel transactions, paper trails etc. (M25).

Este balance de beneficios e inconvenientes se posiciona aún más hacia la no implementación cuando se trata de tiendas ubicadas en Canadá. Dado que en Canadá el

consumo de marihuana es legal, las tiendas no tienen una elevada necesidad de ofrecer bitcoin como opción de pago, siendo el esfuerzo de su adopción mucho mayor en comparación con los beneficios que pudiera ocasionar:

> *Them: We do not accept bitcoin because weed is legal in Canada and slowly legalizing in other places of the world. There isn't the need to use bitcoin transactions for it. We do not take bitcoin because it will be too much hassle and the price is too volatile. Once we receive bitcoin payments, we will need to send it to our bank account immediately because of the price volatility. That is just too much work for us and not necessary* (M20).

Inconvenientes de la Adopción Para el Negocio. En algunos casos la implementación de las criptomonedas como forma de pago no se ha llevado a cabo porque no suponía una opción ventajosa para el desarrollo del negocio. Los motivos por los que se ha considerado que su inclusión no sería beneficiosa son diversos, siendo de nuevo relevante el balance entre el coste de su adopción en comparación con el beneficio que les pudiera reportar.

En varios de los casos se ha encontrado que el propietario del mercado no está familiarizado con la tecnología por diversos motivos, entre ellos su avanzada edad. La inclusión de Bitcoin como forma de pago supondría un coste mayor en comparación con el beneficio que le pudiera reportar, además de disponer de opciones ya disponibles que le otorgan igual beneficios:

> *Me: yes, but I can't find the same variety of products there...and those prices! Do you know if you will accept BTC in the future?*
> *Them: There's always a tradeoff isn't there haha. Honestly probably not. The owner is around 70+ years old, it's not something they're interested in going through from what I've heard/discussed with them* (M24).
> *Me: Ah sure I understand.... and there is no way to find out about it, right?*
> *Them: Nope! Our owner is a senior citizen. That likely has something to do with it. You know how the older generation is with new technology like crypto. I think it's neat and I hold crypto myself, but it's not for everyone* (M26).

En relación con esto, han llegado a exponer que se trata de una tecnología que está limitada para las personas de ese rango de edad, señalando que las criptomonedas "no son para todo el mundo".

En otras ocasiones, la demanda actual de las criptomonedas como forma de pago no es suficiente para algunos negocios como para incluir esta opción de pago. En efecto se ha señalado en algunas tiendas que anteriormente se disponía de la opción de pago con Bitcoin, pero debido a la escasa demanda de esta opción en comparación con su costoso mantenimiento tuvo que retirarse:

> *Hello Kat, though we had carried this option in the past, the demand for cryptic currency is simply not great enough to warrant the expense of placing a processor for this on our checkout page. We will for*

sure keep your email on file and contact you should we accept crypto currently again at some point. In the meantime, we do accept e-transfer as well as credit card payment options (M27).

Se considera que esta opción de pago no es todavía suficientemente popular como para asumir los costes de su implementación:

Me: And you don't know why? I'm trying to understand the reasons. I've spent much time trying to find a shop.
Them: I am not certain; I'd have to try and find out. I just don't think it's been popular enough to set up. Most seem to be ok paying with e transfer or credit card. Sorry we can't help you out today (M28).

Them: It's rare that clients ask for BTC. The number of clients we have that understand how to use it is even lower it's not fully adopted. so, we will not be using it not everyone is tech savvy (M29).

Excepción a la Aceptación de Criptomonedas en el Mercado. El número de mercados que no aceptan las criptomonedas como forma de pago es mucho mayor que el de aquellos mercados que sí incluyen esta moneda virtual entre sus opciones. Sin embargo, se ha encontrado que muchos de los mercados con los que se ha contactado, aunque no disponían de esta opción, se han mostrado predispuestos a recibir transacciones con criptomonedas si se les comunicaba el deseo de utilizarlas.

Una vez se simulaba la compra de un producto en la página de la tienda y se comprobaba que no se ofrecían las criptomonedas como forma de pago, se contactaba con el servicio al cliente pidiendo la utilización de Bitcoin. Aunque muchos mercados se negaron a ofrecer esta opción, muchos otros accedieron a permitir esta transacción y mostraron interés en que la compra se finalizara:

Them: We can try to arrange something just for you to be paid in btc if you'd like. We can see if our friend can allow btc to be sent to their account for you if you want to do something like that? (M17).
Me: Hi, I really like your prices, can I pay my order with BTC?
Them: Absolutely, send us a text message to 647-660-7351 and one of our operators will be able to help you (M30).

Al tratarse de una opción que no se encuentra disponible en la página web de la tienda, en algunas ocasiones ha sido necesario realizar esta petición a través de correo electrónico para el personal encargado. Una vez recibido el correo electrónico, la persona encargada de gestionar este servicio responde explicando el procedimiento que se debería seguir. Esto es, una vez iniciada la compra, cuando se disponga del número de pedido se deberá enviar un correo electrónico indicándolo. Una vez realizado esto, se recibirá otro correo electrónico en el que se indica el precio de la moneda y el número de la cartera a la que se debería realizar la transacción.

Me: Oh, great! But why isn't the option available when I go to finalize my payment.
Them: Please place the order normally and then let us know here when you are ready to send payment and I will tell you the conversion and wallet ID (M31, Figura 20 y Figura 21, Apéndice 5).

El valor de la transacción no incluiría únicamente el precio de la criptomoneda, sino que también se le podrían añadir tasas de la gestión de la transacción. Por ello, no se realiza de forma automática, sino que el mercado propone un precio para la transacción y es el cliente el que decide si continuar con el proceso. Será en ese momento cuando se le envíen los datos de la cartera y el resto de las instrucciones necesarias:

> *Me: Oh that's great, thank goodness! But I'm confused, why don't I get the option in the shop, how should I do it?*
> *Them: Yes we can accept bitcoin. Would you like to place an order? :) Place an order and email us we will give you a real time price, we agree on it, we will send you the wallet ID :)* (M32).

En algunos casos, aunque los mercados se han mostrado favorables a realizar una excepción en el pago, han establecido ciertos requisitos. Se ha encontrado que es habitual reclamar como requisito el tamaño de la compra realizada. Han señalado que, aunque no se aceptan normalmente los pagos con esta criptomoneda, se hace una excepción cuando se trata de pedidos de gran cantidad:

> *Me: Sorry, what is the reason for only accepting BTC on bulk orders?*
> *Them: We don't normally take BTC but will do it for bigger orders since it's harder to send payment via e-transfer* (M33, Figura 24, Apéndice 5).
> *Me: Hi, I was shopping on your site and while doing the checkout I realized that it only had etransfer. Is it possible to pay by bitcoin?*
> *Them: How big is your order Loremm? We don't normally accept bitcoin but I can look into it if your order is substantial* (M34).

En ocasiones cuando se pide utilizar Bitcoin para pagar el pedido, incluso se pregunta cuál será la cantidad que se espera pagar y así decidir si aceptan el pago con esta moneda:

> *Me: I would like to know if I can pay with BTC*
> *Them: how much are you thinking?*
> *Me: a large amount. Around 500 dollars.*
> *Them: ok, shouldn't be a problem. Please put an order together, I will pass you the wallet key* (M35).
> *Me: Oh my, why is that? I really like your products and your prices, but I appreciate my privacy. It's hard to find a store to use my cryptocurrencies in, I don't understand why.*
> *Them: We will be able to accept crypto on a case by case basis if the order is above $1000, just send us an email and we can arrange* (M36).

Todo ello podría indicar que se trata de una opción disponible siempre y cuando el cliente lo pida. Algunos mercados incluso señalan esta posibilidad durante el proceso de compra indicando que está disponible en caso de que se requiera (M37, Figura 22, Apéndice 5).

Persuasión Para la Utilización de Medios de Pago Disponibles. Los mercados que no aceptan criptomonedas como forma de pago intentan persuadir a los clientes para que utilicen las formas de pago disponibles y así conseguir que se lleve a efectivo la compra.

Para ello emplean diversas estrategias como por ejemplo explicar al cliente el funcionamiento de la opción y enumerar las ventajas de su utilización, muchas veces

comparándolas con el funcionamiento de las criptomonedas. En estos casos, la opción de pago disponible más utilizada y recomendada por el mercado es “e-transfer”:

> *I apologize, Kat. E-transfer is a simple and convenient way to send and receive money. Interac e-Transfer is one of the safest digital money transfer services in the world. When you send money using Interac e-Transfer, the money is transferred using established and secure banking procedures that financial institutions have used for years to settle cheques, bank machine deposits and withdrawals* (M38).

Aunque también se ha seguido el mismo procedimiento con otras de las opciones de pago que disponen como, por ejemplo, el pago en efectivo:

> *The management have not found a way yet to integrate BTC payment options yet. Our cash delivery method has proven very secure and our drivers always notify you when they arrive!* (M18).
> *No idea about our future plans. But yes you can do cash on door if you are not comfortable with interac. Where are you located?* (M39).

Otra de las estrategias para convencer al cliente consiste en asegurar la profesionalidad de la tienda y la seguridad de los métodos de pago disponibles. Es habitual que expongan que no se compartirá ni almacenará información personal del cliente ni de la compra realizada:

> *Me: I want to buy a big amount of drugs and I don't want my activity to be discovered...*
> *Them: We follow a standard protocol for how most MOMS operate online. Your information is not shared and we delete all photo IDs once we verify you* (M40).

> *Our company does not share any information outside to anyone. We also keep your privacy 100% safe and secure. Offshore servers that keep no logs and purge daily ensures your total security* (M41).

De esta forma quieren asegurar y convencer al cliente de que se disponen de formas de compra tan seguras y fiables como se pudiera pensar de las criptomonedas y que por lo tanto merece la pena utilizar alguna de estas para finalizar la compra en la que mostraba interés.

Probabilidad de Aceptación de las Criptomonedas en el Futuro. En cuanto a los mercados que no aceptan Bitcoin como forma de pago ha sido de interés conocer si cabe la posibilidad de que acepten esta opción en el futuro. Las respuestas obtenidas pueden dividirse en dos grupos: mercados que incluirán criptomonedas en el futuro y mercados que no están interesados en su implementación.

En relación con al grupo de mercados favorables a su implementación, estos exponen estar dispuestos a incluir esta opción en el futuro por lo que habitualmente se disculpan por no tener la opción disponible, pero aseguran que están trabajando en esos momentos para su implementación o que están haciendo todo lo posible para conseguirlo y tendrán la opción disponible próximamente:

> *Me: Oh, that's super interesting. So you consider that to be sufficient? Better than using cryptocurrencies?*

Them: We are looking into crypto however this payment option has not yet been implemented in our company yet. We are still evolving ☺ (M40).
Me: Hi, I would like to buy Animal Cookies, can I pay it with BTC?
Them: Hi Kate, we are so sorry, unfortunately at this time we are unable to accept BTC. We hope to add this payment method soon so stay tuned! We apologize for any inconvenience this may cause and we hope that you will still try us again (M42).

No obstante, han sido más frecuentes las respuestas de los mercados que señalaban no estar interesados en incluir esta opción de pago en el futuro. Habitualmente se disculpaban por no disponer de esta opción y exponían que no era posible el pago con Bitcoin:

Me: What a pity! I would really like to buy in your store, but I am quite worried about my privacy (problems with previous orders in other stores) and I am very aware of the use of BTC…do you know if you will accept it soon?
Them: Hi Kitty, at the moment we don't have any timelines as to when we will be accepting BTC. Thank you. (M16).
Me: Do you know if you will accept it soon? before the end of the sales, for example.
Them: Sorry, I don't think there's a plan to accept BTC in the future (M18).

En estos casos no es habitual obtener detalles sobre el motivo por el que no se va a incorporar las criptomonedas como forma de pago en el futuro. Aunque en algunos mercados se ha hecho alusión brevemente a algunas de las características del Bitcoin que se han mencionado en apartados anteriores como la volatilidad y la seguridad:

Me: Hi, do you plan to accept it in the near future? I would like to try your products, but I'm not really comfortable to share my info (…)
Them: Sorry, But with the volatility of crypto at the moment, we can't be accepting it as payment (…) (M43).

Es más habitual que, tras señalar que no incluirán la opción con Bitcoin, comenten la posibilidad de utilizar cualquiera de las otras opciones que tienen disponibles y señalen las ventajas que presentan también como forma de pago:

Me: Do you plan to accept it in the near future? I would like to try your products, but I'm not really comfortable to share my info (…)
Them: We do not have any immediate plans to use bitcoin. We can assure you the ID Upload for the credit card processor is on a secure site, we only see that it was uploaded, not the information attached. We understand your reluctance and recommend you use the Interac E-Transfer option as it is the most secure if you wish to place an order (…) (M44).

Me: Hi! I would like to buy Purple Dream, can I pay it with BTC?
Them: Hi Kate, Thanks for reaching out. Unfortunately BTC is not yet a payment method, but you will be glad to know that it will soon be available here within the coming weeks. In the meantime we do offer eTransfer as a payment option, which you are welcome to use to complete any current orders (M45, Figura 25, Apéndice 5).

Respuestas no Colaborativas, Poco Relevantes o Negativas. De la misma forma que para el grupo que aceptaba Bitcoin como forma de pago, en este grupo también se han obtenido respuestas que no aportaban la información necesaria o que mostraban desinterés o molestia por parte del personal encargado de las tiendas. No obstante, en este caso se dispone de un mayor número de respuestas en comparación con el grupo anterior. Las respuestas que se han obtenido en este grupo se pueden agrupar a su vez en los siguientes grupos.

En primer lugar, se encuentran aquellos mercados que únicamente responden que no aceptan criptomonedas y exponen la forma de pago disponible, sin añadir ninguna información adicional:

> *Me: Hi, I would like to buy some weed. Can I pay my order with BTC?*
> *Them: Sorry we only accept etransfer as a form of payment* (M46, Figura 26, Apéndice 5).

> *Me: Hi, I was shopping on your site and while doing the checkout I realized that it only had etransfer and credit. Is it possible to pay by bitcoin?*
> *Them: Unfortunately, we do not currently take bitcoin sorry* (M47).

En segundo lugar, se encuentran aquellos mercados que responden que no aceptan criptomonedas, pero además añaden no conocer la razón exacta para ello:

> *Me: Can I pay with BTC?*
> *Them: Sorry no, only Interac E-transfer*
> *Me: Oh ☹ Why??*
> *Them: I wish I knew ☺* (M48, Figura 27, Apéndice 5).

También se encuentran aquellas tiendas de las que se ha recibido una respuesta poco amistosa, no colaborativa y se han mostrado molestas por las preguntas realizadas:

> *Me: Hi, I saw that you only accept interact transfer. Can I ask why you don't accept BTC? I'm not comfortable to share my info.*
> *Them: Interac is currently our only accepted form of payment. Apologies, our reasons are also private* (M49).

> *Me: Hi sorry to bother you again, my browser shut down. I'd rather pay in crypto... Why don't you accept them?*
> *Them: We choose not to do so- We apologize for the inconvenience* (M50).

Por último, se encuentran aquellas tiendas que a través de sus respuestas hacen ver que no están predispuestas a continuar con la conversación:

> *They haven't set up the infrastructure to do so, not really too sure why. Not my call!* (M51).
> *Hey sorry to cut you off but is a bit too much. This is a brand new conversation and a lot of questions, for someone who values privacy, please understand* (M52).

Discusión

Los resultados de esta investigación estudian empíricamente la aceptación de las criptomonedas en los mercados online de cannabis en el territorio de Canadá contribuyendo empíricamente al conocimiento de la utilización de las criptomonedas en el desarrollo de una actividad delictiva. En este caso, se realiza la investigación en mercados de cannabis y otros productos derivados en Canadá, que tienen como peculiaridad que la venta de estos productos de forma *online* es legal por la gestión del propio gobierno. Por lo tanto, en esta situación, se supone que los mercados aceptarían criptomonedas debido a los beneficios que puede aportar al desarrollo y la seguridad de su actividad delictiva. Sin embargo, los resultados generales obtenidos son interesantes porque muestran que la mayoría de los mercados no aceptan criptomonedas, especialmente Bitcoin, como forma de pago. Esto desafía las suposiciones sobre que la adopción de esta tecnología será beneficiosa en cualquier caso para los delincuentes. Se ha visto que los costos de la aceptación de criptomonedas superan los beneficios de la aceptación de criptomonedas. Además, entre este grupo de negocios se ha asegurado no estar predispuestos a incluir esta forma de pago en el futuro. Todo ello indica que en este panorama son más utilizadas otras opciones de pago más conocidas como el pago a través de "*e-transfer*".

Los mercados que disponían de Bitcoin como forma de pago presentan una frecuencia menor, pero han arrojado valiosos resultados. Ha sido interesante el hecho de que la aceptación de esta tecnología ha estado más relacionada con la mejora del negocio y la atracción de clientes potenciales que con una motivación para utilizar criptomonedas por sus características. La introducción de esta forma de pago ha supuesto la ampliación de las opciones disponibles permitiendo a los clientes tener una amplia variedad de opciones y facilitando el acceso a todo tipo de clientes. Al considerarse un método de pago seguro, se les ofrece a los clientes una mejor experiencia de compra y una mayor confianza, aumentando la probabilidad de futuras compras. Por otro lado, también han decidido su aceptación debido a la alta demanda de los clientes que han solicitado alternativas a los métodos de pago tradicionales y buscaban más seguridad. Ante las crecientes demandas de los clientes, los mercados adoptan esta tecnología para poder conseguir más ventas ya que, aunque se trate de negocios ilegales también existe la competitividad entre las tiendas y las demandas para adaptarse a las necesidades de los clientes.

En este grupo han sido también interesantes los resultados en los que se recomiendan otras formas de pago con preferencia a Bitcoin. Aunque disponen de la opción, recomiendan

abiertamente a los usuarios que les contactan con dudas utilizar otras de las opciones especialmente si tienen poca experiencia o si se trata de su primera transacción. Motivan a la utilización de los otros métodos incluso realizando comparaciones y señalando los beneficios que presentarían con respecto a Bitcoin, como el mismo nivel de protección de la privacidad con menos costes y mayor velocidad. Una mala experiencia de este tipo podría socavar los posibles beneficios futuros.

Las recomendaciones de otras formas de pago y la implementación con motivo de mejorar el negocio y atender a las demandas de los clientes pueden indicar que la utilización de las criptomonedas en el mercado no se debe a una preferencia por las características propias de la tecnología. En estos casos, se presentaría como una de las opciones más ofrecidas por los mercados delictivos, pero al mismo tiempo recomendarían otras opciones que facilitarán la experiencia del usuario y reducirá por tanto la probabilidad de perder clientes o perjudicar al negocio con experiencias negativas por parte de los clientes.

Algunos mercados han reconocido la aceptación de Bitcoin porque es una forma de pago segura, pero no son frecuentes los casos en los que se presentan las características de las criptomonedas para valorar su aceptación en el mercado. Sin embargo, reconocen aquellos inconvenientes de Bitcoin que pueden influir en la decisión en relación con otros mercados. Afirman que otros mercados pueden no estar utilizando esta moneda virtual debido a su volatilidad, la fluctuación de los precios o la falta de familiaridad con su funcionamiento. En este caso, se confirma que reconocen que están presentes estas cualidades en el funcionamiento de Bitcoin, pero, sin embargo, podría considerarse más una expresión de competitividad con respecto a mercados que no asumieron estos inconvenientes y limitarán su clientela con respecto a los mercados que sí que las utilizan.

En el caso de las tiendas que aceptan Bitcoin como forma de pago, los beneficios de su implementación superan a los inconvenientes. Estos beneficios están relacionados con atraer a un mayor número de clientes que puedan tener buenas experiencias de compra en sus negocios y así aumentar los beneficios económicos. No consideran necesaria la aceptación de las criptomonedas como forma de pago para beneficiarse de sus propiedades en el desarrollo de su actividad delictiva (por ejemplo, del pseudoanonimato o de la inmutabilidad de sus transacciones).

También han sido interesantes los resultados obtenidos para aquellas tiendas en las que no se aceptaban criptomonedas como forma de pago. En estos casos, si se solicitaba el pago con Bitcoin, ocurrían dos situaciones. La primera es que la tienda convencía al usuario de los beneficios y la idoneidad de utilizar alguno de los medios de pago ya disponibles. Para

ello garantizaban la seguridad de las otras opciones e incluso las comparaban con la utilización de Bitcoin. Otra de las situaciones que ocurrían y la más frecuente es que las tiendas ofrecían el pago con Bitcoin si se les solicitaba. Aunque en determinados casos establecían requisitos como la cantidad del pago, no se presentaban inconvenientes a utilizar este método si era lo que el cliente deseaba.

Esto mostraría que la no aceptación de la tecnología no se debe a las propias convicciones sobre las cualidades de las criptomonedas, sino en que puede ser una forma de aumentar las ventas y por tanto obtener más beneficios. Los mercados intentan desviar el uso a formas de pago disponibles que son ampliamente utilizadas y les brindan ganancias en lugar de implementar una nueva opción que les exige un gran esfuerzo y menos facilidad de uso. Sin embargo, si el cliente insiste en su uso, la utilidad percibida de la tecnología aumenta, lo que compensa el esfuerzo percibido y lo lleva a usarla para aumentar sus ganancias.

En estos casos no se ofrecen demasiados detalles sobre la razón para no incluir criptomonedas entre las opciones de pago. Sin embargo, las respuestas obtenidas se pueden dividir en tres grupos, que en orden de frecuencia se presentan como: inconvenientes de mercado, características de las criptomonedas e inconvenientes para el negocio. En cuanto a los inconvenientes del mercado, se hacía alusión a la falta de capacidad y la estructura necesaria para realizar pagos con Bitcoin, además de carteras Bitcoin o la licencia del gobierno necesarias para las transferencias bancarias. Las características de las criptomonedas que se señalaban como responsables de la no implementación eran la volatilidad, las elevadas tasas de las transacciones además del hecho de que sus operaciones no eran realmente anónimas. Todas ellas, se presentaban como inconvenientes demasiado costosos de superar para los posibles beneficios que pudieran ofrecer. Finalmente, los inconvenientes para el negocio de la adopción estaban relacionados con la baja popularidad del uso de Bitcoin, que no podía compensar el esfuerzo que le tomaría al mercado familiarizarse con él, entre otros. Por lo tanto, estos son tres inconvenientes que aumentan los costos requeridos para la aceptación de Bitcoin.

En resumen, todo esto ha demostrado que la implementación de criptomonedas en un mercado de drogas online no viene determinada por las características de esta tecnología. Han sido más importantes los aspectos relacionados con la prosperidad del negocio, la captación de clientes y la mejora de la experiencia de compra. Los mercados que aceptaron Bitcoin no lo eligieron por la necesidad de proteger su privacidad o la de sus clientes, sino que las demandas de los clientes aumentaron la utilidad percibida de esta tecnología. Las criptodivisas eran una opción más cuyos inconvenientes se conocían y a veces incluso no se

recomendaba su utilización. De igual forma sucedía en los mercados que no aceptaban la criptodivisa, donde su escasa usabilidad y el elevado esfuerzo que suponía su implementación se veían mermados por la utilidad percibida que aumentaba cuando un cliente demandaba su uso. Los riesgos que dificultan su uso en una situación de legalidad como la volatilidad de su precio, la posibilidad de ser victimizado o el riesgo de cometer errores no superaban en estos casos la utilidad percibida detectada en su uso delictivo para un mercado.

Limitaciones del Quinto Experimento

Aunque los resultados presentados en este documento contribuyen a la comprensión de la aceptación de las criptomonedas en los mercados criminales de cannabis en Canadá, esta investigación no está exenta de limitaciones. En primer lugar, los datos se han obtenido de mercados ubicados en territorios de Canadá, donde existe una situación específica sobre la regulación del cannabis. La situación de legalidad en la venta de estos productos a través de la gestión gubernamental sugiere que las ventas fuera de esta situación requieren el uso de criptodivisas para ocultar su actividad ilícita. Futuras investigaciones podrían dirigirse a estudiar la actividad de este tipo de comercios en zonas donde la regulación de este ámbito sea diferente. En segundo lugar, la investigación se centra en los mercados que venden específicamente cannabis y otros productos derivados del cannabis. Aunque este comercio es interesante debido a su especial regulación en este territorio, estudios posteriores podrían ampliar la investigación a mercados que vendan otros productos diferentes o incluso servicios ilegales. En tercer lugar, se estudia el uso de criptomonedas como sistema de pago, pero este no es el único uso que se le suele dar a esta tecnología en la actividad delictiva. Además del pago de productos y servicios, también se utiliza para ocultar el rastro de actividades ilícitas y para el lucro personal. Los resultados obtenidos no han podido extenderse al resto de usos de las criptodivisas. Por lo tanto, nuevos estudios podrían ampliar esta investigación a otros usos de las criptodivisas para obtener una visión global del uso de esta tecnología en la delincuencia. No obstante, se considera que proporciona resultados valiosos sobre la aceptación de las criptomonedas en los mercados delictivos y el uso de esta tecnología en la delincuencia.

BLOQUE IV: DISCUSIÓN Y CONCLUSIONES

Discusión

En las últimas décadas, el avance de las Tecnologías de la Información y la Comunicación (TICs), el uso generalizado de Internet y la globalización han supuesto multitud de beneficios para la sociedad, especialmente en relación con la comunicación e interconexión entre personas de una forma más rápida y efectiva.

Dentro de este avance tecnológico surgieron las criptomonedas que tenían como propósito conseguir que el comercio electrónico no estuviera sujeto a la intervención de intermediarios como las entidades bancarias. De esta forma, se creó una moneda virtual protegida con criptografía que permitía realizar transacciones entre personas sin la intervención de terceros y sin conocer la identidad de las partes implicadas. Esto conllevó grandes beneficios para aquellas personas interesadas en mantener la privacidad de su actividad financiera, que consideraban que estaba controlada por las entidades bancarias.

No obstante, de la misma forma que los avances tecnológicos han beneficiado a la sociedad, también han favorecido el desarrollo de actividades delictivas. Las criptomonedas se han utilizado para la comisión de una gran variedad de delitos tanto delitos de carácter tradicional en los que no son necesarias las TICs para su desarrollo, como delitos ciberdependientes que solo son posibles mediante la utilización de la tecnología. Además, han adquirido diferentes roles, ya que se han utilizado como forma de pago, para ocultar el rastro de la actividad delictiva y con el propósito de lucrarse y obtener beneficios económicos.

La realización de transacciones de carácter anónimo, la falta de una regulación uniforme entre países, su alcance global y la posibilidad de adquirir cualquier tipo de moneda fiduciaria han favorecido la utilización de las criptomonedas en el ámbito criminal.

Esta situación ha ocasionado preocupación entre las autoridades encargadas de la lucha contra la criminalidad. Las características de las criptomonedas unidas a las peculiaridades de los grupos criminales están propiciando un tipo de delincuencia difícil de detectar, perseguir y eliminar. Esto ha motivado el desarrollo de investigaciones sobre las transacciones de la *Blockchain* dirigidas al descubrimiento de la identidad de las carteras sospechosas de haber cometido un delito. Además, con el propósito de que la información obtenida pueda asistir en las actuaciones de las FCSE, se han creado herramientas como la elaborada en el proyecto TITANIUM, que incluyen técnicas de análisis de datos masivos y otras basadas en Inteligencia Artificial y sistemas inteligentes.

Los beneficios que ha supuesto la utilización de la Inteligencia Artificial en ámbitos como la medicina han motivado que se extienda a otras áreas de la sociedad. El desarrollo de

este tipo de máquinas permite tomar decisiones de la misma forma que un humano basándose en el conocimiento de situaciones anteriores. Estiman la situación futura de un fenómeno, lo que permite descubrir aspectos que puede que no se hubieran considerado con anterioridad a través del estudio realizado por una persona. Esto ha impulsado que se integren estas técnicas en herramientas creadas para el desarrollo de estrategias policiales basadas en la vigilancia dirigida por inteligencia y la vigilancia predictiva.

Por todo lo anterior, el fenómeno de la criminalidad cometida con criptomonedas se consideró adecuado para la utilización de este tipo de herramientas. Su utilización podría alcanzar aquel conocimiento que no es posible para los investigadores actuales debido a las complejidades de la moneda y de su utilización en grupos criminales.

De esta forma, la presente investigación tuvo como objetivo general realizar una aproximación criminológica al fenómeno criminal con criptomonedas para obtener una visión completa sobre sus autores, víctimas, tipo de delitos y motivaciones delictivas.

Para la consecución del objetivo propuesto se planteó una metodología de carácter mixto formada por cinco experimentos, tres con metodologías de carácter cualitativo y dos con una metodología de carácter cuantitativo. Aunque en el bloque de metodología se pueden encontrar las discusiones de cada uno de los experimentos realizados, se ha decidido realizar una breve exposición de estas y de sus limitaciones para poder disponer del contexto necesario para comprender las conclusiones.

El experimento primero tenía como objetivo utilizar sistemas inteligentes en conjuntos de datos de delitos cometidos con criptomonedas que permitieran obtener nuevo conocimiento sobre este fenómeno delictivo y que al mismo tiempo sirvieran para evaluar y adaptar las herramientas de vigilancia predictiva basadas en Inteligencia Artificial. Finalmente, no fue posible conseguir el objetivo propuesto debido a los inconvenientes que surgieron durante la investigación, en su mayoría relacionados con la incapacidad de las autoridades y de los investigadores de los proyectos para proporcionar los datos necesarios o bien porque no se disponía de estos.

La investigación en esta área requería de la formación y el conocimiento del tipo de datos e información de los que se dispone. Las direcciones de las carteras de criptomonedas no ofrecen datos personales sobre los usuarios, el tipo del delito en el que pudieran estar implicadas o las posibles víctimas.

En este sentido, tal como se vio en el bloque II en el capítulo siete, la investigación sobre criptomonedas se centra mayormente en desarrollar métodos y herramientas que permitan, por un lado, estudiar los patrones de actividad de las transacciones en la

Blockchain. Por otro lado, obtener la información adicional necesaria para poder vincular la dirección de una cartera con la identidad de un usuario en particular. Esto es, de forma general, se busca una mejora en la eficiencia de estas tareas, bien por la tecnología empleada para el estudio de los patrones, bien por la utilización de nuevas técnicas y estrategias.

Sin embargo, aunque este tipo de investigaciones puedan obtener nuevo conocimiento que anteriormente se desconocía sobre este tipo de delitos, la naturaleza de los datos y la forma en la que se opera en la *Blockchain* no permite que con esta forma de proceder se pueda estudiar el fenómeno delictivo en su totalidad. Se está dirigiendo el foco de las investigaciones a la tecnología empleada y a la importancia de disponer de amplios conocimientos de informática y estadística. Se considera que se está descuidando el estudio del fenómeno delictivo objeto de estudio, desatendiendo otras áreas de este que puede que no fueran abordadas únicamente con la utilización de nuevas tecnologías emergentes.

En este sentido adquiere valor la investigación en Criminología, cuyo conocimiento y métodos, basados en las ciencias sociales, permiten un conocimiento completo del fenómeno delictivo. De esta forma, permitiría que investigaciones posteriores pudieran conocer la importancia del delito que se pretende abordar, si es necesario su estudio y si lo es, qué aspecto de todo el fenómeno es más interesante. A partir de este punto, sería cuando la utilización de técnicas de IA y otros sistemas inteligentes podrían ofrecer conocimiento nuevo sobre el fenómeno que no se hubiera considerado previamente, pero hasta entonces, el estudio previo se considera de utilidad para conocer la dirección que debería llevar la investigación posterior. Esto es, si este fenómeno tiene la relevancia social o delictiva como para su estudio, si la problemática está vinculada con el estudio de los autores, de las víctimas o del contexto espaciotemporal del delito.

Por todo ello, se continuó en la investigación con el desarrollo de cuatro experimentos conforme a una metodología de carácter mixto que permitiera desde una aproximación criminológica conseguir una visión del fenómeno delictivo en su conjunto.

En relación con el segundo experimento, se realizó un estudio sobre el panorama español de la criminalidad cometida con criptomonedas. Para ello, se emplearon datos obtenidos de la jurisprudencia penal española para obtener detalles sobre autores, delitos víctimas y posibles motivaciones de los delitos.

Se obtuvo que el delito mayoritario en el marco español en este ámbito son los delitos contra el patrimonio y contra el orden socioeconómico, en especial el delito de estafa. Estos resultados coincidirían con los obtenidos en otras investigaciones similares como Aránguez (2020); Kethineni y Cao (2020); Pérez (2020) y Saldaña-Taboada (2022).

Se trata de un tipo de delito de carácter tradicional, es decir, que no se requiere necesariamente de la utilización de las nuevas tecnologías para su comisión. Se observó que en los casos de falsas ventas de productos las criptomonedas no tenían un papel relevante en el delito de estafa, sino que se utilizaban porque permitían la ocultación del rastro ilegal del dinero obtenido. Al mismo tiempo, tampoco eran utilizadas en otros casos de estafas en los que solo suponían un reclamo para conseguir la inversión de la víctima en un falso negocio de inversión. Aunque también se han obtenido casos de utilización de las criptomonedas en la compra de productos de la *Darknet,* estos casos fueron minoritarios. Por lo tanto, según los resultados obtenidos las criptomonedas no eran una herramienta determinante en los delitos de estafa ya que la supresión de esta tecnología no impedía que se pudiera finalizar la comisión del delito empleando otros métodos.

En cuanto al rol de las criptomonedas en el desarrollo del delito, se ha observado que es predominante su utilización para la ocultación del rastro ilícito. La forma más habitual para realizar esto se ha visto que ha sido utilizando el dinero ilegalmente obtenido para comprar criptomonedas. Le sigue la motivación de lucro y obtención de beneficio económico. Esto se debe al elevado valor que ha adquirido en los últimos años la criptomoneda Bitcoin, además de la posibilidad de apropiarse de estas monedas de forma definitiva. Esto ha llevado a que los criminales busquen apropiarse de las monedas de forma directa o a través de falsos negocios creados para tal fin.

De forma general, casos delictivos estudiados tratan sobre falsas compras de productos, falsos negocios de inversión y estafas piramidales. De esta forma, la víctima envía su dinero o sus criptomonedas al delincuente con la intención de comprar un producto o invertir en un negocio, pero el criminal se apropia del dinero. Por lo tanto, la realidad de las criptomonedas se encuentra lejos de su rol único como medio de pago dejando a un lado su etiqueta de "dinero criminal" y siendo más frecuente su utilización en casos de blanqueo de dinero y de obtención de beneficio económico y lucro.

En cuanto al tipo de criptomoneda más utilizado, se esperaría una mayor utilización de criptomonedas de carácter privado como Monero. No obstante, los resultados han señalado que la criptomoneda más utilizada ha sido Bitcoin que, a diferencia de la anterior, permite acceder al historial de transacciones públicamente.

En relación con las víctimas implicadas en este tipo de criminalidad, predominan aquellas víctimas que con carácter individual se han visto afectadas por un delito contra el patrimonio y contra el orden socioeconómico, en su mayoría por estafas relacionadas con falsas inversiones en criptomonedas. Esto podría sugerir la necesidad de medidas preventivas

que consistan en advertir y formar a las potenciales víctimas sobre los riesgos de estas actividades y dirigidas hacia aquellas personas interesadas en la compraventa e inversión de criptomonedas.

Por último, en relación con la autoría de este tipo de delitos, los resultados de este experimento han mostrado una mayoría de grupos criminales, mayormente implicados en los delitos contra el patrimonio y contra el orden socioeconómico, en especial, estafas y blanqueo de capitales. Esto coincide con lo expuesto en los sucesivos informes de Europol (2014, 2018, 2019, 2021, 2022) sobre la utilización de criptomonedas por parte de los grupos criminales o de otras investigaciones como Collins (2022). También es de interés el hecho de la implicación de los grupos criminales en casos de estafas piramidales y tráfico de drogas. Por lo tanto, no podría asumirse una autoría individual en este tipo de criminalidad.

El tercer experimento consistía en un estudio espacio temporal de la victimización por delitos cometidos con criptomonedas. Los resultados fueron agrupados por victimización según el delito, el espacio y el tiempo.

En cuanto al tipo de delito, los delitos más denunciados por las víctimas fueron los delitos de extorsión, seguidos de los delitos de sextorsión y de *ransomware*. En los tres casos se trata de delitos en los que los criminales exigen el pago a la víctima de una cantidad de criptomonedas por lo que el éxito del delito estará determinado por la decisión de la víctima de realizar el pago. Por ello, uno de los motivos por los que han sido los delitos más denunciados por las víctimas es porque requerían el alcance a una gran cantidad de víctimas para conseguir el pago de cierta cantidad. Por otro lado, también podría tratarse de delitos que son fácilmente reconocibles por las víctimas, por lo que detectan el ataque y lo denuncian.

En cuanto a la victimización según el espacio, los resultados muestran que Estados Unidos es el país con un mayor número de denuncias, siendo esta cantidad muy significativa en comparación con los países que ocupan la segunda y la tercera posición, que son Reino Unido y Alemania. Esto podría suponer que este país es el que reúne un mayor número de víctimas por delitos de extorsión, sextorsión y *ransomware*, pero también podría significar que esta población tiene un mayor conocimiento de esta plataforma de denuncias. En cualquier caso, la cifra de victimización es tan elevada que debería ser considerada.

Por último, en relación con la victimización según el tiempo, los resultados muestran que hay un menor número de denuncias en aquellos meses, días y horas que se consideran no laborables. Esto es, los meses de verano de junio, julio y agosto, los días de fin de semana y las horas fuera de la jornada laboral. Todo ello podría indicar que se producen menos delitos debido a una menor disponibilidad de los criminales, o bien que los usuarios al no estar

disponibles en el entorno laboral no son víctimas de estos ataques o se muestran menos predispuestos a denunciar.

El cuarto experimento consiste en un estudio de las motivaciones y las formas de utilización de las criptomonedas en un foro de discusión de la *Darknet.* Los resultados obtenidos se han dividido en siete grupos según la temática tratada.

Uno de los temas mayormente tratados y del que más discusiones se ha obtenido ha sido el relativo a evitar la detección ilegal de la actividad. Al mismo tiempo, dentro de este tema se identificaron otros subtemas, como son: la obtención de las criptomonedas, cómo escapar de la detección de las FCSE y otras autoridades, rutas para mantener el anonimato, tipo de criptomonedas preferentes, utilización de tecnologías adicionales, retiro de las criptomonedas y formas de enmendar el riesgo de detección. El subtema más tratado ha sido el de obtención de las criptomonedas, en el que de forma general se recomienda que la compra de criptomonedas se realice en un lugar que no disponga de políticas de KYC para evitar la detección de las autoridades. Sin embargo, si esto no fuera posible, la mayoría de las discusiones de esta temática giran en torno a consultar y aconsejar sobre formas de superar las medidas de seguridad que derivan de las políticas de KYC presentes en diferentes medios (cajeros, las tarjetas prepago, las tarjetas de crédito y débito). En su lugar, recomiendan la utilización de casas de cambio descentralizadas o servicios P2P como “LocalMonero” con la utilización de la criptomoneda Monero. Se considera que será el sujeto interesado el que tendrá que valorar qué método es más favorable para su caso considerando aspectos como los riesgos para la detección, los beneficios que le puede reportar el delito y la disponibilidad de cada método.

En cuanto a las formas de escapar de las FCSE, los usuarios señalan cuáles son las formas mediante las que las autoridades son capaces de conocer las identidades de las carteras BTC como, por ejemplo, a través de la información recopilada con las políticas de KYC. A partir de este conocimiento, aconsejan cuál es la mejor forma de evitar que se obtenga esta información como utilizando casas de cambio descentralizadas, criptomonedas privadas y controlando la cantidad de criptomonedas transferidas.

Las rutas de conversión entre criptomonedas permiten evitar el rastreo y la monitorización de la actividad completa. En su mayoría se aconsejan las rutas que comienzan con la compra de la criptomoneda Bitcoin, añadiendo posteriormente elementos de conversión que aseguren la protección de la privacidad. Se observa una gran flexibilidad en la elaboración de estas rutas, siendo siempre recomendable la conversión a criptomonedas privadas antes de su utilización en un mercado.

La criptomoneda Monero es ampliamente recomendada en el foro como la mejor opción para escapar a la detección de las autoridades, además de que presenta tasas menores que las que se obtienen con Bitcoin. Se trata de una criptomoneda que hasta la fecha no ha podido ser rastreada, por lo que presenta una elevada seguridad.

En cuanto a las tecnologías adicionales para ocultar la identidad, son ampliamente tratados los *mixers* y las carteras privadas, que constituyen tecnologías que pueden añadir una capa extra de privacidad a la actividad delictiva realizada con criptomonedas. No obstante, su utilización no goza de popularidad en el foro e incluso se desaconsejan por la posibilidad de ser víctimas de estafas o por la elevada atención que las autoridades han depositado en estas.

Por último, el *cashout* supone uno de los pasos más importantes de la actividad delictiva, ya que conecta de nuevo la actividad con criptomonedas con la identidad del usuario. Comentan la posibilidad de realizarlo a través de la compra de dinero fiduciario o a través de la compra de bienes de valor. En el primer caso se deberán seguir las medidas de seguridad que se expusieron en el apartado de obtención de las criptomonedas. En la segunda opción será importante la disponibilidad de la criptomoneda Bitcoin como forma de pago en los bienes de valor.

El segundo tema más tratado en el foro fue la utilización de las criptomonedas en el crimen. De esta forma, los delitos más discutidos fueron los ataques *ransomware*, el carding y el blanqueo de capitales. Se describen formas en las que es más efectiva la realización del delito en cuanto a beneficios y en relación con mantener la privacidad, el anonimato y el riesgo de detección. También ha sido muy comentada la utilización en mercados delictivos de la *Darknet*, haciendo referencia a la forma en la que operan y a la mejor forma de utilizarlos para evitar la detección de las autoridades. Por otro lado, la necesidad de ciertos conocimientos para utilizar las criptomonedas ha llevado a que se hayan observado usuarios en el foro que se ofrecen para realizar estas tareas a cambio de una cantidad de criptomonedas. A su vez, también se ofrece el pago en criptomonedas para realizar otras actividades delictivas que requieren de cierta especialización como los ciberdelitos.

En relación con lo anterior, el tercer tema más discutido en el foro tenía relación con las lecciones sobre ciberseguridad y sobre la utilización de criptomonedas. Esto consiste en que los miembros de la comunidad del foro ofrecen explicaciones, consejos y recomendaciones en este espacio sin que haya habido una consulta previa. Se favorece de esta forma, el aprendizaje autodidacta. De forma general, los usuarios responden de forma altruista a las dudas planteadas, con información detallada y con una intención real de que la comunidad aprenda.

Muchos usuarios también han aprovechado este espacio para consultar sobre la veracidad de mensajes recibidos de los que se sospechaba que consistían en un delito. Aunque la mayoría de los usuarios responden de forma paciente y detallada explicando la situación, también ha habido usuarios que señalan públicamente la ineptitud de otros e incluso acceden a la humillación. Por todo ello, no sería realmente necesaria la contratación de otra persona para utilizar las criptomonedas en ciertos ámbitos.

Otro de los temas tratados en el foro es la regulación de las criptomonedas. Los usuarios se muestran interesados en conocer los cambios legislativos y las nuevas regulaciones para poder adaptar sus actuaciones. También se han generado debates sobre la efectividad de las medidas propuestas por los gobiernos con relación a si son realmente efectivas para prevenir este tipo de delincuencia o si suponen un medio más de control de la población por parte del Estado. En este punto resulta interesante el hecho de que haya usuarios que aseguran que no tienen ninguna efectividad y que en realidad existen otras formas de adaptar su actuación y llevar a cabo la actividad delictiva con criptomonedas sin ser descubierto por las autoridades.

Con todo ello, el foro ha sido un espacio de discusión y debate que se ha posicionado como una fuente de información muy valiosa. Las medidas que dispone para proteger la identidad de los usuarios y su ubicación en la *Darknet*, han motivado a los usuarios a compartir consejos, recomendaciones, reflexiones y críticas sobre la utilización de las criptomonedas en el ámbito delictivo, de una forma detallada y amplia. Esto ha permitido tener acceso a la información sobre este tipo de criminalidad de sujetos directamente implicados en estas actividades.

El quinto experimento consiste en un estudio de la utilización de las criptomonedas como forma de pago en mercados online de cannabis y productos derivados.

La actividad de venta de cannabis online es legal si está gestionada por el gobierno a través de sus páginas web oficiales. Por lo tanto, aquellos mercados *online* que no disponen de una licencia de venta serán considerados como mercados ilegales. De esta forma, se asume que, al tratarse de una actividad ilegal fácilmente accesible a través de la web superficial, se utilizarán criptomonedas de carácter privado para proteger la identidad de las partes que realizan la compra de cannabis.

Sin embargo, los resultados obtenidos muestran que la mayoría de los mercados estudiados, aunque son considerados ilegales, no aceptan criptomonedas como forma de pago. Se ha observado que los costos de la implementación de las criptomonedas han superado a los beneficios, por lo que en su mayoría han continuado utilizando otras formas de

pago tradicionalmente empleadas y ampliamente conocidas por la población, aunque no garantizaran el nivel de privacidad que puede asegurarse con la utilización de las criptomonedas.

Los mercados que aceptaban criptomonedas como Bitcoin basaban su decisión en la mejora del negocio y la atracción de potenciales clientes y no en características propias de estas monedas. Bitcoin suponía una opción más que ofrecer a los clientes, que debido a la disponibilidad de una amplia variedad de opciones de pago podrían decidirse por la utilización de un mercado en particular. También se ha aceptado la criptomoneda debido a las altas demandas de muchos clientes que exigían formas de pago alternativas a las tradicionales. De nuevo, la decisión del mercado de aceptar la criptomoneda está basada en el rendimiento del negocio y la obtención de un mayor número de clientes para mostrarse competitivos con respecto al resto de mercados. Estas decisiones no se deben a preferencias por las características propias de las criptomonedas, aunque reconocen los inconvenientes de su implementación cuando consideran el hecho de que otros mercados no hayan aceptado las criptomonedas. Señalan como características de las criptomonedas que no favorecen su implementación su volatilidad, la fluctuación de los precios y la no familiarización con su funcionamiento.

Para el caso de los mercados que aceptan Bitcoin como forma de pago, los beneficios de su implementación han superado a los costes. Estos beneficios consisten en atraer un mayor número de clientes y aumentar los beneficios económicos.

Los mercados que no aceptaban Bitcoin como forma de pago constituían la mayoría de los resultados. Sin embargo, si se le pedía al mercado la posibilidad de pagar el producto con criptomonedas, algunos de estos se mostraban favorables a ofrecer dicha opción. Resultaba como una excepción a la norma habitual del mercado que se hacía con la intención de captar aquellos clientes que se habían mostrado interesados en utilizar ese mercado en específico. No obstante, suelen establecer como requisito que se obtenga una cantidad elevada de productos.

De esta forma, se demuestra de nuevo, que la no aceptación de la criptomoneda no se debe a características propias de esta, sino a criterios de rentabilidad en el negocio.

En este caso, los costes de la implementación de las criptomonedas han superado a los beneficios esperados. Los costes consisten en su mayoría en inconvenientes para el mercado como que no disponer de la capacidad suficiente y la estructura necesaria para realizar los pagos con Bitcoin, además de una cartera o de la licencia del gobierno. También, aunque en menor medida que la anterior, se señalaban algunas características de las criptomonedas

como su volatilidad, las altas tasas de las transacciones y el bajo anonimato que garantiza Bitcoin. Por último, se hacía alusión a una baja popularidad del pago con Bitcoin, que no podía compensar el esfuerzo de su implementación

Ahora bien, aunque esta investigación ha permitido obtener conocimientos valiosos sobre el fenómeno de la criminalidad cometida con criptomonedas, también presenta algunas limitaciones.

Las limitaciones de la investigación están formadas por un conjunto de las limitaciones de todos los experimentos que se han desarrollado. De igual forma sucede con las futuras líneas de investigación.

En el primer experimento las limitaciones tuvieron que ver con la incapacidad de las autoridades para proporcionar datos sobre grupos criminales que utilizaran criptomonedas, bien porque no se disponía de estos datos, bien porque no tenían información que les permitiera conocer si se trataba de un grupo criminal. Además, debido a la confidencialidad de la información, tampoco fue posible obtener datos de los proyectos que desarrollaban herramientas para la detección y estimación de este tipo de criminalidad. Al mismo tiempo, aunque se tuvo acceso a una plataforma de análisis de criptoactivos, no se disponía de direcciones Bitcoin para realizar el análisis. La muestra era muy reducida e incompleta, por lo que no era posible conocer el tipo de actividad realizada, quiénes eran los autores u obtener información sobre las víctimas. Por último, no se pudo determinar la existencia de un grupo criminal únicamente con el estudio de las transacciones realizadas por una entidad, ya que podría tratarse de un mismo usuario que dispone de varias carteras.

En el futuro sería deseable comparar el conocimiento obtenido en esta investigación con los resultados obtenidos en investigaciones que utilicen sistemas inteligentes en esta misma materia. Posteriormente, se elaborarían criterios clave en la detección y persecución de este tipo de criminalidad que serían considerados en el desarrollo de herramientas para la lucha contra la criminalidad que utilicen sistemas inteligentes.

En relación con el segundo experimento, los resultados han sido obtenidos de las resoluciones judiciales de la jurisprudencia española. Por lo tanto, no se podrían extender las conclusiones a toda la criminalidad cometida con criptomonedas. Tampoco podría considerarse que los resultados se corresponden con todo el universo de la criminalidad de este tipo cometida en España. En el futuro se espera ampliar esta investigación realizando un análisis jurisprudencial de otros países y comparar los resultados obtenidos.

En el tercer experimento los datos recogen información de una muestra no probabilística y autoseleccionada de víctimas de ciberdelitos con Bitcoin, lo que no se

corresponde necesariamente con todo el universo de víctimas de estos delitos. Puede que la plataforma de denuncia haya sido más accesible para aquellas personas con más formación técnica o que dominaban el idioma o para aquellos países más conocedores de este servicio. Además, la clasificación de los delitos ha sido realizada por las propias víctimas, por lo que pudiera suceder que se encontraran clasificaciones erróneas. Sin embargo, a pesar de estas limitaciones se ha considerado una fuente de obtención de datos extremadamente valiosa que permite la medición de un fenómeno que por sus características es difícilmente cuantificable. Además, en esta investigación se disponía de datos solo para los años del 2017 al 2021. En el futuro se espera poder recopilar datos de victimización para los próximos años y poder realizar estudios longitudinales.

El cuarto experimento ha contribuido de forma empírica al conocimiento de las motivaciones para utilizar criptomonedas y la forma en la que se utilizan. No obstante, también presenta algunas limitaciones. Por un lado, para acceder al foro se necesitaba resolver un complejo CAPTCHA que se modificaba al pasar unos minutos y cada vez que se accedía al sitio web. Esto impidió la posibilidad de automatizar la recogida de los datos, que finalmente se realizó de forma manual. Por otro lado, el contenido del foro presentaba un elevado dinamismo, ya que cada semana se eliminaban todas aquellas discusiones de mayor antigüedad. Esto ocasionó que fuera necesario el acceso reiterado para recopilar las discusiones, que actualmente no están disponibles. Además, en la última etapa de la investigación el foro cambió su diseño y eliminó su buscador, por lo que se limitó la recogida de datos.

En el futuro se espera poder tener acceso a foros similares en los que se pueda recopilar una mayor cantidad de datos durante más tiempo, además de ampliar el estudio a foros ubicados también en la web superficial.

Por último, en relación con el quinto experimento, sus limitaciones consisten en que la investigación se ha restringido al territorio de Canadá, a los mercados de cannabis y al rol de la criptomoneda como forma de pago. De esta forma, no podrían generalizarse los resultados obtenidos para mercados de otros productos cuya sede se encuentre en territorios con una situación legislativa diferentes a Canadá. No obstante, se considera que este experimento proporciona resultados valiosos sobre la aceptación de las criptomonedas en los mercados delictivos y el uso de esta tecnología en la delincuencia.

En este sentido, estudios posteriores deberían de ampliar esta investigación con el abordaje de otros territorios y otros mercados que vendan productos diferentes o incluso

servicios ilegales, además de considerar otros roles de las criptomonedas diferentes a su utilización como sistema de pago.

Conclusiones

La decisión de utilizar las criptomonedas en el delito se basa en el resultado de realizar un balance de costes y beneficios, de acuerdo con lo establecido en la teoría de la elección racional de Cornish y Clarke (1986). Los criminales decidirán utilizar esta tecnología en sus actividades criminales si los beneficios que esperan de su utilización son mayores que los costes que les pudiera ocasionar.

Tradicionalmente, se ha considerado que los criminales utilizan las criptomonedas motivados por el anonimato y su falta de regulación. Sin embargo, los resultados obtenidos han mostrado que han sido más valorados otros aspectos ajenos a las características intrínsecas de esta tecnología como, por ejemplo, su disponibilidad como forma de pago en los mercados delictivos. Por este motivo, las criptomonedas de carácter público como Bitcoin son mucho más utilizadas en el crimen que criptomonedas de carácter privado como Monero. Aunque esta última garantizaría la privacidad de la actividad delictiva muestra al mismo tiempo una menor disponibilidad como forma de pago.

Otros aspectos que también han sido valorados por los usuarios son la familiaridad, la preferencia de uso y la accesibilidad. Esto se ha podido observar en las rutas de conversión de criptomonedas, en las que se comenzaba con la compra de Bitcoin que tiene una mayor disponibilidad y accesibilidad que otras criptomonedas de carácter privado. Estos aspectos eran considerados como beneficios de mayor importancia que los costes de que el delito fuera detectado por las autoridades encargadas de la lucha contra el crimen.

En relación con los mercados delictivos, la adopción de las criptomonedas ha sido determinada por aspectos relacionados con la prosperidad del negocio como una mayor captación de clientes y la capacidad para ofrecerles una experiencia de compra satisfactoria. Los mercados que ofrecían Bitcoin como forma de pago no habían basado esta decisión en la protección de su privacidad o la de sus clientes, sino en un aumento de la demanda de esta moneda. De igual forma sucedía en aquellos mercados en los que no se aceptaba el Bitcoin como forma de pago. Se consideraba que esta opción de pago no era muy popular entre los clientes, por lo que la baja utilización esperada no superaría los costes que suponía su implementación como la volatilidad en los precios.

Todo ello indica que los criminales no se muestran firmemente motivados a la utilización de estas monedas por las características que pudieran presentar, sino que el Bitcoin constituye una opción adicional para el desarrollo de sus actividades delictivas. Por este motivo, no se evita la utilización del Bitcoin, sino que se emplean diversas formas de asegurar la privacidad que no se garantiza con el mero hecho de utilizar la moneda. Este es el caso de las rutas de conversión de criptomonedas mencionadas anteriormente o la adaptación de los criminales a los cambios en la regulación de esta materia buscando nuevas formas de cometer el delito y ajustándose a las nuevas modificaciones legislativas propuestas.

Sin embargo, entre las formas de asegurar la privacidad, se ha visto que los servicios *mixers* que permiten añadir una capa extra de seguridad a la actividad realizada no son populares entre los criminales. El motivo es que se han visto implicados en diversos casos de estafas de salida y además han atraído la atención de las FCSE, que los investigan para evitar que sean utilizados con fines criminales.

Por todo ello, las criptomonedas se presentan como una opción que los criminales tienen disponible cuando lo consideren oportuno y no se considera una herramienta imprescindible en la mayoría de los delitos. Por lo tanto, en aquellas ocasiones en las que su utilización no sea beneficiosa para los criminales continuarán con el empleo de otros medios de pago como, por ejemplo, el dinero en efectivo, que continúa siendo la forma de pago más utilizada en el ámbito criminal, en especial, en el blanqueo de capitales.

Respecto a lo anterior, se ha visto su mayor utilización en delitos que ya existían con anterioridad a la utilización de las tecnologías, que son los delitos de estafa y los delitos de extorsión. En ambos, el Bitcoin solo suponía un elemento más del delito con el que se esperaba conseguir mejores resultados. En cuanto a los delitos de extorsión, como la sextorsión o el *ransomware*, el pago con criptomonedas supone una nueva opción que ha sustituido a formas de pago anteriores, pero que no ha sido un medio de pago único en el desarrollo de este delito. Aunque se eliminara la criptomoneda se podrían buscar nuevas formas de continuar con el desarrollo de este tipo de criminalidad.

También se ha visto que, aunque intervienen en el delito en muchas ocasiones no es necesaria la utilización de las criptomonedas para el desarrollo de la actividad delictiva. Por ejemplo, se utiliza como reclamo en los falsos negocios de inversión para atraer a potenciales víctimas que no son conocedoras de los riesgos de esta actividad. De esta forma, la víctima adquiere importancia en el desarrollo efectivo del delito. Este tipo de criminalidad depende de los patrones de actuación de las víctimas para garantizar el éxito del delito. Se ha observado que son más denunciados aquellos delitos que requieren de envíos masivos de

mensajes (*ransomware*, extorsión y sextorsión) para poder llegar a aquellas víctimas que estuvieran dispuestas a realizar el pago. Por otro lado, se ha detectado que la victimización de estos delitos también se ha visto influenciada por las actividades rutinarias o cotidianas de las víctimas y de los autores. La victimización será menor durante aquellos meses, días y horas que habitualmente están vinculados con periodos festivos, como vacaciones, fines de semana o el fin de la jornada laboral. Por ello, se considera que el Bitcoin es una opción que se utilizará cuando se briden la oportunidad para ello.

En relación con los autores, se ha encontrado una mayoría de grupos criminales dedicados a esta actividad delictiva, lo que coincide con la preocupación de las autoridades y el desarrollo de sus herramientas de análisis y estimación del delito. No obstante, resulta interesante que se ha observado un perfil de autor individual que no se inició en el ámbito criminal con un perfil especializado en esta tecnología, sino que ha aprendido de forma autodidacta cómo utilizarla para cometer un delito. Esto es posible debido a que existe una oferta muy amplia de opciones para aprender cómo utilizar las criptomonedas con este propósito. Además, hay una predisposición elevada por parte de los usuarios de la comunidad de las criptomonedas a enseñar a sus miembros en el uso legal e ilegal de la tecnología, favoreciendo el aprendizaje. Por lo tanto, se ha observado una baja popularidad en la contratación de los servicios de expertos que utilicen criptomonedas en actividades delictivas.

En definitiva, se trata de una investigación que ha centrado su atención en los autores, las víctimas, las formas comisivas del delito y las motivaciones. Se ha realizado una aproximación criminológica a estos aspectos empleando metodologías cualitativas y cuantitativas propias de la disciplina de las ciencias sociales. A diferencia de la mayoría de las investigaciones en esta materia, se ha alejado el foco de la tecnología y se ha obtenido información relevante sobre los autores y sus motivaciones y las víctimas.

Sin duda, constituirá un conocimiento de valor para la elaboración posterior de políticas de prevención en esta materia. Especialmente serviría para elaborar políticas de prevención dirigidas a aquellas personas interesadas en la inversión de criptomonedas para poder advertirles sobre los riesgos de esta actividad. La formación en esta materia sería clave para prevenir un aumento en la creación de oportunidades delictivas, ya que el conocimiento del usuario sobre los riesgos en los ciberdelitos es determinante para ser víctima. Pero además también podría servir para la información y orientación de herramientas que permitan la lucha contra la criminalidad.

El conocimiento obtenido en la investigación será de utilidad para las autoridades y la elaboración de herramientas de detección, análisis y estimación de esta criminalidad.

Teniendo como base los resultados obtenidos, sus actuaciones se podrían centrar en lo siguiente. Se ha visto una presencia significativa de mercados delictivos ubicados en la web superficial, de forma que habrá que extender la persecución de los delitos más allá de la *Darknet*. Habitualmente las actuaciones de las FCSE tienen como objetivo de estudio las organizaciones criminales especializadas en la utilización de las criptomonedas en el delito, pero según los resultados obtenidos también tendrán que considerar aquellos usuarios que han aprendido a utilizar ilegalmente las criptomonedas de una forma autodidacta. También deberán investigar aquellas fuentes en las que se encuentra la información necesaria para ello. Esto pone de manifiesto la importancia del aprendizaje autodidacta sobre la contratación de personas especializadas en el uso criminal de las criptomonedas. Al mismo tiempo, la victimización de estos delitos se ve influenciada por las rutinas y los patrones del autor y de la víctima, por lo que deberán considerar los patrones espaciotemporales en sus herramientas desarrolladas para la lucha contra este tipo de criminalidad.

Por último, la aplicación de sistemas inteligentes en la detección, estudio, análisis y persecución de este tipo de criminalidad también habrá que decidirse en base a un balance de costes y beneficios de su utilización. Los antecedentes de éxito de estas tecnologías no pueden ocasionar que se asuman los beneficios de su utilización en todo caso. El desarrollo de investigaciones como la que se presenta en este trabajo tiene utilidad como paso previo al planteamiento de tecnologías y herramientas de análisis y estimación del delito más sofisticadas que utilicen sistemas inteligentes. Sus resultados permitirán centrar los esfuerzos en aquellos aspectos que realmente preocupen a la sociedad y cuyo tratamiento sea determinante en la prevención del delito. Por ello, serán necesarios grupos de trabajo interdisciplinares, que aparten el foco de atención de la investigación de la tecnología, y que combinen metodologías propias de ciencias sociales con aquellas más usadas en informática para obtener una visión global del fenómeno delictivo.

Síntesis de las Conclusiones

A continuación, se presenta una síntesis de las principales conclusiones de este trabajo:

1. Las criptomonedas no son la opción preferente para todos los criminales, solo constituyen una opción más para cometer delitos.

Los criminales deciden utilizar las criptomonedas cuando podrían reportarles algún tipo de beneficio. En aquellos casos en los que no fueran útiles, recurrirían a otro tipo de herramientas que les permitieran el desarrollo del delito. Por lo tanto, no se muestran especialmente motivados a utilizar esta tecnología por sus características, sino que esto dependerá de la valoración de los beneficios que pudiera aportarle.

2. La utilización de las criptomonedas en el ámbito criminal no supone un aumento de los delitos de carácter técnico.

El uso de las tecnologías en el crimen a menudo se vincula con delitos que requieren de un elevado dominio tecnológico. Por ello, la utilización de criptomonedas se ha relacionado con una criminalidad especializada en el uso de las tecnologías y delitos ciberdependientes. Sin embargo, se ha observado que predomina la utilización de las criptomonedas en aquellos delitos que ya existían con anterioridad a su aparición como, por ejemplo, los delitos de estafas.

3. La criminalidad cometida con criptomonedas muestra un predominio de la utilización del Bitcoin frente a criptomonedas de carácter privado.

Popularmente se ha asumido que las criptomonedas de carácter privado como Monero son las más utilizadas en el crimen. En comparación con Bitcoin, Monero garantiza una mayor privacidad de la actividad financiera por lo que podría ser más atractiva para los criminales. Sin embargo, se ha observado que Bitcoin sigue siendo todavía la criptomoneda más utilizada. Esto se debe a que los criminales prefieren otros aspectos como la disponibilidad en los mercados criminales. Este beneficio es mucho más valorado que la posibilidad de que la actividad criminal sea detectada por las autoridades.

4. Un bajo dominio en la utilización de criptomonedas no supone una limitación para los criminales.

La complejidad técnica que pudieran presentar las criptomonedas y la *Blockchain* no ha supuesto una limitación para aquellas personas con un bajo dominio de las tecnologías, pero

con una alta motivación para cometer un delito. Esto se debe a una amplia disponibilidad de contenido didáctico sobre la utilización de las criptomonedas en el crimen. Los usuarios podrán acceder al contenido de fuentes abiertas y formarse por ellos mismos. También se ha observado que los usuarios de la comunidad se han mostrado predispuestos a ayudar a otros en el aprendizaje de las criptomonedas ofreciendo consejos, recomendaciones e incluso resolviendo las dudas que les plantean.

5. No es necesario el pago a criminales especializados en criptomonedas para poder involucrarse en este tipo de criminalidad.

La posibilidad de llevar a cabo un aprendizaje autodidacta de la utilización criminal de las criptomonedas ha sugerido que no es necesario el pago a usuarios especializados para cometer delitos con esta tecnología. Por ello, se ha observado una baja popularidad del conocido como *Crime-as-a-Service* en este ámbito.

6. El Bitcoin no es solo una moneda para adquirir productos ilegales.

Popularmente las criptomonedas han sido consideradas como la moneda que utilizan todos los criminales para adquirir productos y servicios ilegales. Sin embargo, no es predominante su rol como forma de pago, sino que son más frecuentes otros roles como el de ocultar el dinero ilegalmente obtenido o el de utilizarla para obtener beneficios económicos. El primer rol se corresponde con los delitos de blanqueo de capitales, en los que los criminales utilizan el dinero ilegalmente obtenido para comprar criptomonedas y dificultar el rastreo del delito. En el segundo rol las criptomonedas se utilizan como un reclamo para que los usuarios inviertan en falsos negocios de inversión de criptomonedas u otras estafas relacionadas.

7. Las criptomonedas no han sustituido a los medios de pago tradicionales.

Aunque han adquirido una gran popularidad por haber sido vinculadas al crimen, las criptomonedas no son el medio de pago más utilizado por los criminales. La decisión de utilizar el Bitcoin en el delito no está influenciada únicamente por las características de la moneda. Serán considerados otros aspectos ajenos a la tecnología como su disponibilidad en mercados criminales, su familiaridad, la facilidad de acceso o la dificultad de uso. Además, si se trata de un negocio criminal, se tendrán en cuenta aspectos relacionados con la rentabilidad del negocio y la obtención de beneficios económicos. Por lo tanto, si los beneficios esperados por el uso de la moneda no superan los aspectos anteriores, los criminales utilizarán los medios de pago que

sí los garanticen. Esta es la razón por la que el dinero en efectivo continúa siendo la forma de pago más utilizada en el crimen.

8. La victimización por este tipo de delitos se ha visto influenciada por las actividades cotidianas del autor y de la víctima.

Muchos de los delitos que se cometen con criptomonedas requieren del pago de una cantidad determinada por parte de las víctimas. Por lo tanto, los criminales envían estos ataques a una gran cantidad de usuarios con el propósito de que realicen ese pago el mayor número de usuarios posibles. No obstante, dado que la mayoría de estos delitos tienen lugar a través de un entorno *online*, se ha observado que la victimización está influenciada por las actividades cotidianas del autor y de la víctima. Se han registrado un menor número de denuncias en aquellos días, horas y meses en los que se espera que una persona se encuentre fuera de su horario laboral. Esto puede incluso significar que muchos de estos ataques son recibidos por la víctima en el propio entorno laboral. Por lo tanto, por un lado, se produce una menor victimización debido a una menor disponibilidad de los criminales para realizar el ataque. Por otro lado, los usuarios al no estar disponibles en el entorno laboral no son víctimas de estos ataques o se muestran menos predispuestos a denunciar.

9. La víctima adquiere un papel importante en el éxito de la mayoría de los delitos cometidos con criptomonedas.

La mayoría de los delitos denunciados por las víctimas eran delitos de sextorsión, extorsión y *ransomware*. Este tipo de delitos tiene la peculiaridad de que requiere del pago de la víctima para que el criminal pueda obtener beneficios económicos con su desarrollo. De esta forma, la decisión de la víctima de realizar el pago exigido será determinante en el éxito del delito. De igual manera sucede con los delitos de estafa que consisten en falsos negocios de inversión de criptomonedas o en estafas piramidales. La participación de la víctima en esta actividad sin conocer los riesgos determina el éxito del delito y la obtención de beneficios económicos. Por lo tanto, sin ánimo de culpar a las víctimas del surgimiento de estos delitos, se detecta la necesidad de intervenir con potenciales víctimas para que conozcan los riesgos y las limitaciones del uso de las criptomonedas.

10. Se deben elaborar medidas preventivas que se dirijan a personas interesadas en la inversión en criptomonedas.

Se ha observado que hay una gran cantidad de personas que han sido víctimas de falsos negocios de inversión en criptomonedas por lo que existe la necesidad de elaborar planes de prevención que estén dirigidos a que las potenciales víctimas de este delito conozcan los riesgos de la inversión en criptomonedas antes de involucrarse.

11. No hay que asumir que la adopción de una tecnología será favorable para el criminal en todo caso.

Los supuestos beneficios de la utilización de una tecnología en el delito no pueden ocasionar que se asuma su utilización en todo caso. Los criminales toman la decisión de utilizarla realizando un balance de costes y beneficios de su implementación. En este análisis se incluyen otros factores que son valorados por los criminales y que puede que no estén relacionados con las características de tecnología. En el caso de las criptomonedas fueron más importantes para el criminal la disponibilidad de la moneda, su accesibilidad, su facilidad de uso o la familiaridad. En aquellos casos en los que se trate de un mercado criminal se valorarán aspectos relacionados con la rentabilidad de negocio y la obtención de beneficios. Al mismo tiempo, no han sido populares las herramientas que permiten reforzar la privacidad como los mezcladores o *mixers*. Por lo tanto, no hay que asumir que se utilizarán las tecnologías en todos los delitos ya que esto dependerá de los aspectos que los criminales consideren beneficiosos para su actividad delictiva.

12. La flexibilidad y la capacidad de adaptación de los criminales limita la efectividad de las medidas de prevención del delito que consisten en la prohibición del Bitcoin.

Se ha observado una elevada capacidad y predisposición de los criminales para adaptar sus métodos a los nuevos cambios en las tecnologías y a los límites en la detección de la actividad criminal. De hecho, a pesar de su carácter pseudoanónimo, el Bitcoin sigue siendo la criptomoneda más utilizada en el delito. En lugar de abandonar por completo su utilización por el riesgo de ser detectada la actividad criminal, se ha observado una adaptación constante de los criminales que utilizan formas muy diversas de continuar protegiendo su identidad al mismo tiempo que siguen utilizando esta moneda. Un ejemplo de ello son las diversas rutas de conversión de criptomonedas en las que combinan la utilización de diversas criptomonedas y realizan una multitud de cambios entre ellas. Por lo tanto, se cree que la prohibición absoluta del Bitcoin, además de ser casi imposible por cuestiones técnicas, no sería completamente efectiva para terminar con este tipo de criminalidad.

13. Los foros constituyen una gran fuente de datos de interés criminológico.

La información contenida en los foros ha supuesto una fuente de datos de gran valor para realizar investigaciones criminológicas. Las características propias de este entorno unidas a las medidas para proteger la identidad de la red TOR en la *Darknet* han permitido a los usuarios expresarse con libertad y detallar sus actividades de una forma que ha posibilitado obtener la información suficiente para el desarrollo de la investigación.

14. Las investigaciones en Criminología sobre esta materia tienen un gran valor para obtener información relevante del delito.

Se ha observado un gran valor de la investigación en Criminología, cuyas teorías y métodos basados en las ciencias sociales han permitido obtener un conocimiento completo del fenómeno criminal. Esto ha permitido que las investigaciones posteriores que se realicen en esta materia puedan conocer la importancia de esta criminalidad y establecer si es necesario su estudio y qué aspectos sería más interesante abordar. A partir de este punto, la utilización de técnicas de IA y otros sistemas inteligentes podrían ofrecer conocimiento nuevo sobre el fenómeno que no se hubiera considerado previamente. Hasta entonces, se requiere de un estudio previo que permita identificar los puntos de interés del delito, centrar los esfuerzos y conocer mejor el fenómeno criminal favoreciendo su prevención y aprovechando todas las bondades de la aplicación de estas tecnologías.

Conclusions

The decision to use cryptocurrencies in crime is based on the outcome of a cost-benefit analysis, in line with Cornish and Clarke's (1986) rational choice theory. Criminals will decide to use this technology in their criminal activities if the benefits they expect from its use are greater than the costs they might incur.

Traditionally, criminals have been seen as using cryptocurrencies because of their anonymity and lack of regulation. However, the results obtained have shown that other factors unrelated to the intrinsic characteristics of this technology, such as, for example, its availability as a form of payment in criminal markets, have been more highly valued. For this reason, public cryptocurrencies such as Bitcoin are much more widely used in crime than private cryptocurrencies such as Monero. Although the latter would guarantee the privacy of criminal activity, it shows a lower availability as a form of payment.

Other aspects that have also been valued by users are familiarity, preference of use and accessibility. This could be seen in cryptocurrency conversion paths, which typically started with the purchase of Bitcoin, which is more widely available and accessible than other privately held cryptocurrencies. These aspects were seen as more important benefits than the costs of the crime being detected by crime-fighting authorities.

Regarding criminal markets, the adoption of cryptocurrencies has been driven by aspects related to the prosperity of the business, such as increased customer acquisition and the ability to offer them a satisfactory shopping experience. Marketplaces that offered Bitcoin as a form of payment had not based this decision on the protection of their privacy or that of their customers, but on an increase in demand for the currency. The same was true for those marketplaces that did not accept Bitcoin as a form of payment. This payment option was not very popular with customers, so the expected low usage would not outweigh the costs of implementing it, such as price volatility.

This suggests that criminals are not strongly motivated to use these currencies because of their potential characteristics. Bitcoin is an additional option for their criminal activities. For this reason, the use of Bitcoin is not avoided, but various ways are employed to ensure the privacy that is not guaranteed by using the currency. This is the case of cryptocurrency conversion routes or the adaptation of criminals to changes in the regulation of this area by seeking new ways of committing crime and adjusting to the proposed new legislative changes.

However, among the ways of securing privacy, it has been found that mixer services that allow an extra layer of security to be added are not popular with criminals. This is because they have been implicated in several cases of exit scams and have also attracted the attention of the LE, which is investigating them to prevent them from being used for criminal purposes.

For all these reasons, cryptocurrencies are presented as an option that criminals have available to them if they wish and are not considered an essential tool in most crimes. Therefore, on those occasions when their use is not beneficial for criminals, they will continue to use other means of payment, such as cash, which continues to be the most widely used form of payment in the criminal field, especially in money laundering.

Regarding the above, there has been a greater use in crimes that already existed prior to the use of the technologies, namely fraud and extortion crimes. In both, Bitcoin was only one element of the crime that was expected to achieve better results. For extortion crimes, such as sextortion or *ransomware*, payment with cryptocurrencies is a new option that has replaced previous forms of payment but has not been a unique means of payment in the development of this crime. Even if cryptocurrency were to be eliminated, new ways could be sought to continue the development of this type of crime.

It has also been seen that, although they are often involved in the crime, the use of cryptocurrencies is not necessary for the development of the criminal activity. For example, it is used as a lure in fake investment businesses to attract potential victims who are not aware of the risks of this activity. In this way, the victim becomes important in the actual development of the crime. This type of crime depends on the victims' patterns of behaviour to ensure the success of the crime. It has been observed that crimes that require the sending of mass messages (*ransomware*, extortion, and sextortion) to reach victims who are willing to pay are more frequently reported. On the other hand, victimisation of these crimes has also been found to be influenced by the routine or everyday activities of victims and perpetrators. Victimisation will be lower during those months, days and times that are usually linked to non-working periods, such as holidays, weekends, or the end of the working day. Bitcoin is therefore seen as an option to be used when the opportunity to do so arises.

In relation to the offenders, many criminal groups have been found to be dedicated to this criminal activity, which is in line with the concern of the authorities and the development of their tools for analysing and estimating crime. However, it is interesting that an individual offender profile has been observed who did not start out in the criminal field with a specialised profile in this technology, but who has self-taught himself how to use it to commit

a crime. This is possible because there is a very wide range of options for learning how to use cryptocurrencies for this purpose. In addition, there is a high willingness on the part of users in the cryptocurrency community to teach their members about the legal and illegal use of the technology, which is favourable for learning. Therefore, low popularity has been observed in hiring the services of experts who use cryptocurrencies in criminal activities.

In short, this research has focused its attention on the perpetrators, the victims, the ways in which crime is committed and criminal motivations. A criminological approach to these aspects has been carried out using qualitative and quantitative methodologies typical of the discipline of social sciences. Unlike most research in this area, the focus has been shifted away from technology and relevant information has been obtained on the offenders and their motivations and the victims.

It will undoubtedly provide valuable knowledge for the subsequent development of prevention policies in this area. It would serve to develop prevention policies aimed at those interested in investing in cryptocurrencies to warn them about the risks of this activity. Training in this area would be key to preventing an increase in the creation of criminal opportunities, as the user's knowledge of the risks of cybercrime is a determining factor in becoming a victim. But it could also be used to provide information and guidance on tools to fight crime.

The knowledge obtained in the research will be useful for the authorities and the development of tools for detecting, analysing, and assessing this criminality. Based on the results obtained, their actions could focus on the following. There has been a significant presence of criminal markets located on the surface web, so it will be necessary to extend the prosecution of crimes beyond the Darknet. Usually, the LE's actions are aimed at criminal organisations specialised in the use of cryptocurrencies in crime, but depending on the results obtained, they will also have to consider those users who have learned to use cryptocurrencies illegally in a self-taught manner. They will also have to investigate those sources where the necessary information can be found. This highlights the importance of self-learning over hiring people specialised in the criminal use of cryptocurrencies. At the same time, the victimisation of these crimes is influenced by the routines and patterns of the perpetrator and the victim, so they should consider spatiotemporal patterns in their tools developed to fight this type of crime.

Finally, the application of intelligent systems in the detection, study, analysis and prosecution of this type of crime will also have to be decided on the basis of a cost-benefit balance. The successful track record of these technologies cannot mean that the benefits of

their use are assumed in any case. The development of research such as this work is useful as a steppingstone to the development of more sophisticated crime analysis and estimation technologies and tools using intelligent systems. Its results will allow us to focus our efforts on those aspects that are of real concern to society and whose treatment is decisive in crime prevention. For this reason, interdisciplinary working groups will be necessary, shifting the focus of attention away from research into technology, and combining methodologies from the social sciences with those most used in computer science to obtain a global vision of the criminal phenomenon.

Summary of Conclusions

The following is a synthesis of the main findings of this work:

1. Cryptocurrencies are not the preferred option for all criminals, they are just another option for committing crimes.

Criminals choose to use cryptocurrencies when they could bring them some kind of benefit. In cases where they would not be useful, they would use other tools that would allow them to carry out the crime. Therefore, they are not particularly motivated to use this technology because of its characteristics, but this will depend on their assessment of the benefits it could bring them.

2. The use of cryptocurrencies in crime does not imply an increase in tech-savvy crime.

The use of technologies in crime is often linked to crimes that require a high level of technological proficiency. Thus, the use of cryptocurrencies has been linked to specialised tech-savvy crime and cyber-dependent crime. However, it has been observed that cryptocurrencies are predominantly used in crimes that already existed prior to their emergence, such as scam crimes.

3. Crime committed with cryptocurrencies shows a predominance of the use of Bitcoin as opposed to private cryptocurrencies.

It has been popularly assumed that private cryptocurrencies such as Monero are the most widely used in crime. Compared to Bitcoin, Monero ensures greater privacy of financial activity and could therefore be more attractive to criminals. However, it has been observed that Bitcoin is still the most widely used cryptocurrency. This is because criminals prefer other aspects such as its availability in criminal markets. This benefit is much more highly valued than the possibility of criminal activity being detected by the authorities.

4. The mastery of cryptocurrency technology is not a constraint for criminals.

The technical complexity that cryptocurrencies and the *Blockchain* may present has not been a constraint for those with a low mastery of the technologies, but with a high motivation to commit a crime. This is due to the wide availability of educational content on

the use of cryptocurrencies in crime. Users will be able to access open-source content and learn for themselves. It has also been observed that other users in the community have shown a willingness to help users learn about cryptocurrencies by offering advice, recommendations and even answering their questions.

5. It is not necessary to pay criminals specialised in cryptocurrencies to engage in this type of criminality.

The possibility of self-taught training in the criminal use of cryptocurrencies has suggested that it is not necessary to pay specialised users to commit crimes using this technology. As a result, the popularity of crime-as-a-service has been observed to be low in this area.

6. Bitcoin is not just a currency for acquiring illegal goods.

Cryptocurrencies have been popularly considered as the currency used by all criminals to acquire illegal products and services. However, its role as a form of payment is not predominant; other roles are more frequent, such as hiding illegally obtained money or using it to obtain economic benefits. The first role corresponds to money laundering crimes, where criminals use illegally obtained money to buy cryptocurrencies and make it difficult to trace the crime. In the second role, cryptocurrencies are used as a lure for users to invest in fake cryptocurrency investment businesses or other related scams.

7. Cryptocurrencies have not replaced traditional means of payment.

Although they have become very popular because they have been linked to crime, cryptocurrencies are not the most common means of payment used by criminals. The decision to use Bitcoin in crime is not only influenced by the characteristics of the currency. Other aspects outside the technology will be considered, such as its availability in criminal markets, its familiarity, ease of access or difficulty of use. In addition, if it is a criminal business, aspects related to the profitability of the business and the achievement of economic benefits will be considered. Therefore, if the expected profits from the use of the currency do not outweigh the above aspects, criminals will use the means of payment that do guarantee them. This is why cash continues to be the most common form of payment used in crime.

8. Victimisation by this type of crime has been influenced by the routine activities of the offender and the victim.

Many of the crimes committed with cryptocurrencies require the payment of a certain amount by the victims. Therefore, criminals send these attacks to many users with the aim of getting as many users as possible to make the payment. However, since most of these crimes take place in an online environment, victimisation has been found to be influenced by the routine activities of the perpetrator and the victim. Fewer reports have been recorded on those days, times, and months when a person is expected to be out of working hours. It may even mean that many of these attacks are received by the victim in the working environment itself. Therefore, on the one hand, there is less victimisation due to less availability of criminals to carry out the attack. On the other hand, users who are not available in the work environment are not victims of these attacks or are less inclined to report them.

9. The victim plays an important role in the success of most cryptocurrency crimes.

Most of the crimes reported by victims were sextortion, extortion, and *ransomware* crimes. This type of crime is unique in that it requires payment from the victim for the criminal to be able to profit financially from its development. Thus, the victim's decision to make the required payment will be decisive in the success of the crime. The same is true for scam crimes consisting of fake cryptocurrency investment deals or pyramid schemes. The victim's participation in this activity without knowing the risks involved determines the success of the crime and therefore the obtaining of economic benefits. Therefore, without blaming the victims for the emergence of these crimes, it is necessary to work with potential victims so that they are aware of the risks and limitations of the use of cryptocurrencies.

10. Preventive measures should be developed to target people interested in investing in cryptocurrencies.

It has been observed that many people have been victims of fake cryptocurrency investment businesses, so there is a need to develop crime prevention plans that are aimed at making potential victims of this crime aware of the risks of investing in cryptocurrencies before they become involved.

11. It should not be assumed that the adoption of a technology will be favourable to the criminal in every case.

The supposed benefits of the use of a technology in crime cannot lead to the assumption of its use in all cases. Criminals make the decision to use it by balancing the costs

and benefits of its implementation. This analysis includes other factors that are valued by criminals and may not be related to the characteristics of the technology. In the case of cryptocurrencies, the availability of the currency, its accessibility, ease of use or familiarity were more important for the criminal. In cases where a criminal market is involved, aspects related to business profitability and profit-making will be valued. At the same time, tools to enhance the privacy of the activity, such as mixers, have not been popular. Therefore, it should not be assumed that technologies will be used in all crimes as this will depend on the aspects that criminals consider beneficial to their criminal activity.

12. The flexibility and adaptability of criminals limits the effectiveness of crime prevention measures consisting of a Bitcoin ban.

Criminals' ability and willingness to adapt their methods to new changes in technologies and limits in the detection of criminal activity has been observed to be high. Indeed, despite its pseudo-anonymous nature, Bitcoin remains the most widely used cryptocurrency in crime. Rather than abandoning its use altogether because of the risk of criminal activity being detected, there has been a steady adaptation of criminals using a variety of ways to continue to protect their identity while continuing to use this currency. An example of this is the various cryptocurrency conversion routes where they combine the use of various cryptocurrencies and perform a multitude of exchanges between them. Therefore, it is believed that an outright ban on Bitcoin, in addition to being almost impossible due to technical issues, would not be completely effective in ending this type of criminality.

13. The forums are a great source of data of criminological interest.

The information contained in forums has been a valuable source of data for criminological research. The characteristics of this environment, together with the measures to protect the identity of the TOR network in the Darknet, have allowed users to express themselves freely and to detail their activities in a way that has made it possible to obtain enough information for the development of the investigation.

14. Criminology research in this area is of great value in obtaining relevant information on crime.

Research in Criminology has been of great value, and its theories and methods based on social sciences have enabled a complete understanding of the criminal phenomenon. This has enabled subsequent research in this area to understand the importance of this criminality

and to establish whether it is necessary to study it and which aspects would be more interesting to address. From this point, the use of AI techniques and other intelligent systems could offer new knowledge about the phenomenon that had not previously been considered. Until then, a prior study is required to identify the points of interest of the crime, focus efforts and better understand the criminal phenomenon, favouring its prevention and taking advantage of all the benefits of the application of these technologies.

Referencias

Abadinsky, H. (2013). *Organized crime*. Wadsworth Cengage Learning (10th ed.).

Ahmed, M., Shumailov, I., & Anderson, R. (2019). Tendrils of Crime: Visualizing the Diffusion of Stolen Bitcoins. In G. Cybenko, D. Pym, & B. Fila (Eds.), *Graphical Models for Security. GraMSec 2018. Lecture Notes in Computer Science* (Vol. 11086, pp. 1–12). Springer, Cham. https://doi.org/10.1007/978-3-030-15465-3_1

Akcora, C. G., Li, Y., Gel, Y. R., & Kantarcioglu, M. (2020). BitcoinHeist: Topological Data Analysis for Ransomware Prediction on the Bitcoin Blockchain. *Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence*, 4439–4445. https://doi.org/10.24963/ijcai.2020/612

Aldridge, J., & Décary-Hétu, D. (2014). Not an "Ebay for Drugs": The Cryptomarket "Silk Road" as a Paradigm Shifting Criminal Innovation. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.2436643

Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. *Computer Science Review*, *40*, 100402. https://doi.org/10.1016/j.cosrev.2021.100402

Ali, S. T., Clarke, D., & McCorry, P. (2015). Bitcoin: Perils of an Unregulated Global P2P Currency. In A. J. Christianson B., Švenda P., Matyáš V., Malcolm J., Stajano F. (Ed.), *Security Protocols XXIII. Security Protocols 2015. Lecture Notes in Computer Science* (Vol. 9379, pp. 283–293). Springer, Cham. https://doi.org/10.1007/978-3-319-26096-9_29

[Allinvain] (2011, June 13). *I just got hacked - any help is welcome! (25,000 BTC stolen)* [Online forum post]. BitcoinTalk. https://bitcointalk.org/index.php?topic=16457.0

Al-rimy, B., Maarof, M. & Shaid, S. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security,* 74. 10.1016/j.cose.2018.01.001.

Amat, O. (2018). El Bitcoin: Burbuja o revolución. En *Descubriendo el Bitcoin: cómo funciona, cómo comprar, invertir, desinvertir...* (pp. 111–126). Profit.

Ammous, S. (2018). *El patrón bitcoin: la alternativa descentralizada a los bancos centrales*. Deusto.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Hernandez Ganan, C., Grasso, T., Levi, M., Moore, T., & Vasek, M. (2019). Measuring the Changing Cost of Cybercrime. In *The 2019 Workshop on the Economics of Information Security (WEIS*

2019) https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_25.pdf

Andrews, S., Akhgar, B., Yates, S. J., Stedmon, A. W., & Hirsch, L. (2013). Using formal concept analysis to detect and monitor organised crime. En H. L. Larsen et al. (Eds.), *Flexible Query Answering Systems (FQAS 2013),* LNAI 8132 (pp. 124-133). Berlin, Heidelberg: Springer.

Andrianova, A. (2020). Countering the Financing of Terrorism in the Conditions of Digital Economy. In: Ashmarina, S., Mesquita, A., Vochozka, M. (eds) Digital Transformation of the Economy: Challenges, Trends and New Opportunities. *Advances in Intelligent Systems and Computing,* vol 908. Springer, Cham. https://doi.org/10.1007/978-3-030-11367-4_2

Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., & Capkun, S. (2013). Evaluating user privacy in Bitcoin. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7859 LNCS*, 34–51. https://doi.org/10.1007/978-3-642-39884-1_4

Antonopoulos, A. M. (2015). *Mastering bitcoin: unlocking digital crypto-currencies.* (First edit). O'Reilly. https://granatensis.ugr.es/permalink/34CBUA_UGR/1p2iirq/alma991014010607204990

Antonopoulos, A. M. (2017). *Mastering bitcoin: Programming the Open Blockchain* (2nd ed). O'Reilly.

Aránguez, C. (2020). El Bitcoin como instrumento y objeto de delitos. *Cuadernos de Política Criminal*, 2(131), 75-103.

Azani, E., Barak, M., Landau, E., & Liv, N. (2020). *Identifying Money Transfers and Terror Finance Infrastructure In the Service of the Popular Resistance Committees in Gaza Co-Authors: Cobwebs Tech*. https://doi.org/10.2307/resrep25874

Back, A. (1997, March 28). *hash cash postage implementation*. http://www.hashcash.org/papers/announce.txt

Balaskas, A., & Franqueira, V. N. L. (2018). Analytical Tools for Blockchain: Review, Taxonomy and Open Challenges. *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 1–8. https://doi.org/10.1109/CyberSecPODS.2018.8560672

Bambuch, V. (2020). *Platform for Cryptocurrency Address Collection* [Master's Thesis, Brno University of Technology]. https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=216179

Bamert, T., Decker, C., Wattenhofer, R., Welten, S. (2014). BlueWallet: The Secure Bitcoin Wallet. In: Mauw, S., Jensen, C.D. (eds.) *Security and Trust Management. STM 2014. Lecture Notes in Computer Science* (vol 8743). Springer, Cham. https://doi.org/10.1007/978-3-319-11851-2_5

Banco Central Europeo (2023). *Billetes.* https://www.ecb.europa.eu/euro/banknotes/html/index.es.html#500

Banco Santander (12 de septiembre de 2019). *Blockchain: qué es y cómo afecta al sector financiero.* https://www.santander.com/es/stories/blockchain-seguridad-y-transparencia-al-servicio-de-la-banca

Banco Santander (2021). *One Pay: transferencias internacionales al instante - Banco Santander.* https://www.bancosantander.es/particulares/banca-digital/one-pay

Bancroft, A., & Scott Reid, P. (2017). Challenging the techno-politics of anonymity: the case of cryptomarket users. *Information, Communication & Society*, *20*(4), 497–512. https://doi.org/10.1080/1369118X.2016.1187643

Bang, J., & Choi, M.-J. (2019). Design and Implementation of Storage System for Real-time Blockchain Network Monitoring System. In *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)* (pp. 1–4). IEEE. https://doi.org/10.23919/APNOMS.2019.8892967

Barda, D., Zaikin, R., & Vanunu, O. (2021, November 4). *CPR alerts crypto wallet users of massive search engine phishing campaign that has resulted in at least half a million dollars being stolen*. Check Point Research. https://research.checkpoint.com/2021/cpr-alerts-crypto-wallet-users-of-massive-search-engine-phishing-campaign-that-has-resulted-in-at-least-half-a-million-dollars-being-stolen/

Barrat, M. J. (2012). Silk Road: Ebay for drugs. *Addiction*, *107*(3), 683–683. https://doi.org/10.1111/J.1360-0443.2011.03709.X

Barratt, M. J., & Aldridge, J. (2016). Everything you always wanted to know about drug cryptomarkets* (*but were afraid to ask). *International Journal of Drug Policy*, *35*, 1–6. https://doi.org/10.1016/J.DRUGPO.2016.07.005

Bartoletti, M., Pes, B. & Serusi, S. (2018). Data mining for detecting Bitcoin Ponzi schemes. *IEEE 2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* - Zug, Switzerland, (), 75–84. doi:10.1109/cvcbt.2018.00014

Barysevich, A. & Solad, A. (2018). *Litecoin Emerges as the Next Dominant Dark Web Currency*. https://go.recordedfuture.com/hubfs/reports/cta-2018-0208.pdf

Bashir, M., Strickland, B., Bohr, J. (2016). What Motivates People to Use Bitcoin? In: Spiro, E., Ahn, YY. (eds) *Social Informatics. SocInfo 2016. Lecture Notes in Computer Science (),* vol 10047. Springer, Cham. https://doi.org/10.1007/978-3-319-47874-6_25

Bastardo, J. (2019, April 28). *Mark Karpelès: ¿Mt Gox fue un robo o un gran fraude?* Criptonoticias. https://www.criptonoticias.com/seguridad-bitcoin/mark-karpeles-mt-gox-robo-fraude/

Bayer, D., Haber, S., & Stornetta, W. (1999). *Improving the Efficiency and Reliability of Digital Time-Stamping*. https://doi.org/10.1007/978-1-4613-9323-8_24

Bayer, D., Haber, S., & Stornetta, W. (1999). Improving the Efficiency and Reliability of Digital Time-Stamping. https://doi.org/10.1007/978-1-4613-9323-8_24

BBC (2017, December 19). *Bitcoin exchange Youbit shuts after second hack attack.* BBC News, https://www.bbc.com/news/technology-42409815

BBC (2019, February 6). *Child abuse images hidden in crypto-currency blockchain.* BBC News. https://www.bbc.com/news/technology-47130268

bit2me Academy (15 de noviembre de 2016). *Qué son las Hardware Wallets*. https://academy.bit2me.com/hardware-wallets/

bit2me Academy (1 de agosto de 2018). *Qué es una wallet o monedero de criptomonedas*. https://academy.bit2me.com/wallet-monederos-criptomonedas/

bit2Me Academy (12 de diciembre de 2019). *¿Qué es Timestamp?* https://academy.bit2me.com/timestamp-blockchain/

bit2me Academy (5 de mayo de 2020a). *¿Qué es un nodo?* https://academy.bit2me.com/que-es-un-nodo/

bit2me Academy (9 de julio de 2020b). *¿Qué es una red P2P?* https://academy.bit2me.com/que-es-una-red-p2p/

Bitcoin Project (2020). *Vocabulario.* https://bitcoin.org/es/vocabulario#bitcoin

BitcoinAbuse (2019). *Frequently Asked Questions.* Retrieved November 5, 2019, from https://www.bitcoinabuse.com/faq.

BitInfoCharts (2023). *Litecoin (LTC) price stats and information*. https://bitinfocharts.com/litecoin/

Blázquez, S. (2 de enero de 2019). ‘Blockchain’, el notario de la educación. *El País*. https://elpais.com/economia/2018/12/28/actualidad/1545995900_480941.html?outputType=amp

Blockchain.com (2021a). *Bloque: 0 | Explorador de Blockchain*. https://www.blockchain.com/btc/block/0

Blockchain.com (2021b). *Gráficos de la Blockchain*. https://www.blockchain.com/charts#block

Blockchain.com (2023). *Monero*. https://www.blockchain.com/explorer/assets/xmr

Boar, A. (2018). *Descubriendo el bitcoin: cómo funciona, cómo comprar, invertir, desinvertir.* Profit.

Bows, H. (2018). Methodological approaches to criminological research. En P. Davies y P. Francis (eds.) *Doing criminological research* (pp.94-109). SAGE.

Bratingham, P. J. (2009). *Statistical Models of Criminal Behavior: The Effects of Law Enforcement Actions.* UCLA.

Boden, M. A. (2017). *Inteligencia Artificial.* Turner.

Brenig, C., Accorsi, R., & Müller, G. (2015). Economic Analysis of Cryptocurrency Backed Money Laundering. In J. Becker, J. V. Brocke and M. de Marco (Eds.) *23rd European Conference on Information Systems, ECIS 2015.* https://doi.org/10.18151/7217279

Brown, M. S. & B. Douglass, B. (2020). An Event Study of the Effects of Cryptocurrency Thefts on Cryptocurrency Prices. In F. J. Barros, X. Hu, H. Kavak and A. A. Del Barrio (Eds.), *2020 Spring Simulation Conference (SpringSim)*, (pp. 1-12). IEEE. https://doi.org/10.22360/SpringSim.2020.CSE.001

Brown, S. D. (2016). Cryptocurrency and criminality: The Bitcoin opportunity. *The Police Journal: Theory, Practice and Principles*, *89*(4), 327–339. https://doi.org/10.1177/0032258X16658927

Bryman, A. (2016). *Social Research Methods* (5ª Ed.) Oxford University Press.

Buil-Gil, D. y Saldaña-Taboada, P. (2021). Offending Concentration on the Internet: An Exploratory Analysis of Bitcoin-related Cybercrime. *Deviant Behavior*, 43, https://doi.org/10.1080/01639625.2021.1988760

Buterin, V. (2013). *Guía de Ethereum*. https://ethereum.org/es/whitepaper/

Butler, S. (2019). Criminal use of cryptocurrencies: a great new threat or is cash still king? *Journal of Cyber Policy*, *4*(3), 326–345. https://doi.org/10.1080/23738871.2019.1680720

Butler, S. (2021). Cyber 9/11 Will Not Take Place: A User Perspective of Bitcoin and Cryptocurrencies from Underground and Dark Net Forums. In Groß, T., Viganò, L. (eds) *Socio-Technical Aspects in Security and Trust. STAST 2020. Lecture Notes in Computer Science* (), vol 12812. Springer, Cham. https://doi.org/10.1007/978-3-030-79318-0_8

Cambridge University Press. (2020). Cryptocurrency. In *Cambridge Dictionary*. https://dictionary.cambridge.org/es/diccionario/ingles-espanol/cryptocurrency

Carrascal, J. (2021). Experiencia de usuario y modelo de incentivos. En J. M. Corchado y J. L. Tejedor (Ed.), *C1b3rWall Academy- Módulo 0*. Universidad de Salamanca. https://youtu.be/B0PE71FbPy4

Carrefour (2018). *Blockchain alimentario.* https://actforfood.carrefour.es/Por-queactuar/BLOCKCHAIN-ALIMENTARIO

Casas, E. (2017). *La red oscura: En las sombras de Internet. El cibermiedo y la persecución de los delitos tecnológicos*. La esfera de los libros.

Casciani, D. (2010, May 13). *500 euro note - why criminals love it so.* BBC *Magazine,* http://news.bbc.co.uk/2/hi/8678979.stm

Castro-Toledo, F. J., & Gómez-Bellvís, A. B. (2022). Bad outcomes, good intentions: approaching the potential misuse of crime data by policymakers. https://doi.org/10.31235/osf.io/g7dhp

Chainalysis (2020, January 17). *Terrorism Financing in Early Stages with Cryptocurrency But Advancing Quickly*. Chainalysis. https://blog.chainalysis.com/reports/terrorism-financing-cryptocurrency-2019/

Chainalysis (2022). *The 2022 Crypto Crime Report. Original data and research into cryptocurrency-based crime.* https://go.chainalysis.com/2022-Crypto-Crime-Report.html

Choo, K.K.R. (2015). Cryptocurrency and virtual currency: corruption and money laundering/terrorism financing risks. In D. L. K. Chen (Ed.), *Handbook of Digital Currency* (pp. 283-307). Academic Press. https://doi.org/10.1016/B978-0-12-802117-0.00015-1

Christin, N. (2013). Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace. In *WWW '13: Proceedings of the 22nd international conference on World Wide Web* (pp. 213–224). Association for Computing Machinery. https://doi.org/10.1145/2488388.2488408

Cimpanu, C. (2018, February 1). *Smominru Botnet Infected Over 500,000 Windows Machines*. Bleeping Computer. https://www.bleepingcomputer.com/news/security/smominru-botnet-infected-over-500-000-windows-machines/

Clark, T., Foster, L., Sloan, L., & Bryman, A. (2021). *Bryman's social research methods*. Oxford University Press.

Coinbase (2023). *Predicting Bitcoin fees for transactions*. https://bitcoinfees.earn.com/

CoinMarketCap (1 de febrero de 2023b). *Bitcoin.* https://coinmarketcap.com/currencies/bitcoin/

CoinMarketCap (29 de enero de 2023a). *Principales 100 Criptomonedas por capitalización de mercado*. https://coinmarketcap.com/es/

CoinMarketCap (2021). *Exchange Ranking*. https://support.coinmarketcap.com/hc/en-us/articles/360052030111-Exchange-Ranking

Cointelegraph (2023). *Halving de Bitcoin - ¿Cómo funciona el ciclo de halving y por qué es importante?* https://es.cointelegraph.com/bitcoin-for-beginners/bitcoin-halving-how-does-the-halving-cycle-work-and-why-does-it-matter

Collins, J. (2022). *Crypto, crime and control: Cryptocurrencies as an enabler of organized crime.* Global Initiative Against Transnational Organized Crime. https://globalinitiative.net/wp-content/uploads/2022/06/GITOC-Crypto-crime-and-control-Cryptocurrencies-as-an-enabler-of-organized-crime.pdf

Comisión Europea (2020) REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937. Bruselas. https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0003.02/DOC_1&format=PDF

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

Consejo de Seguridad Nacional (2019). *Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave*. Gobierno de España. https://www.dsn.gob.es/es/documento/estrategia-nacional-contra-crimen-organizado-delincuencia-grave

Constantin, L. (2014, August 29). *CryptoWall ransomware held over 600K computers hostage, encrypted 5 billion files.* PCWorld. https://www.pcworld.com/article/434991/cryptowall-held-over-halfamillion-computers-hostage-encrypted-5-billion-files.html

COPKIT (2022). Technology, training and knowledge for Early-Warning / Early-Action led policing in fighting Organised Crime and Terrorism. https://cordis.europa.eu/project/id/786687/es.

Cornish, D. B., & Clarke, R. V. (Eds.). (1986). *The reasoning criminal: Rational choice perspectives on offending*. Springer-Verlag.

Corte Ibáñez, L. y Giménez-Salinas, A. (2010). *Crimen.org: evolución y claves de la delincuencia organizada*. Editorial Ariel.

Crawford, J., & Guan, Y. (2020). Knowing your Bitcoin Customer: Money Laundering in the Bitcoin Economy. In *2020 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE)* (pp. 38–45). IEEE. https://doi.org/10.1109/SADFE51007.2020.00013

Crónica Global (23 de febrero de 2022). *Cae la organización criminal que hackeó y robó a una empresa de criptomonedas seis millones de euros*. Crónica Global. https://cronicaglobal.elespanol.com/vida/cae-organizacion-criminal-hackeo-robo-criptomonedas_608331_102.html

Dai, W. (1998, November). *b-money*. Satoshi Nakamoto Institute. https://nakamotoinstitute.org/b-money/

Davies, P. & Francis, P. (2018). *Doing criminological research* (3ª ed.). SAGE.

Davis, J. (2011, October 3). The Crypto-Currency. *The New Yorker*. https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency

Dhayal, H., & Kumar, J. (2018). Botnet and P2P Botnet Detection Strategies: A Review. In *2018 International Conference on Communication and Signal Processing (ICCSP)* (pp. 1077–1082). IEEE. https://doi.org/10.1109/ICCSP.2018.8524529

Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The Second-Generation Onion Router. *13th USENIX Security Symposium*, 1-18. https://www.usenix.org/legacy/publications/library/proceedings/sec04/tech/full_papers/dingledine/dingledine.pdf

Domingo, C. (2018). *Todo lo que querías saber sobre bitcoin, criptomonedas y blockchain y no te atrevías a preguntar*. Planeta.

Drozhzhin, A. (2016). *Historia y evolución del ransomware: datos y cifras*. Kaspersky. https://latam.kaspersky.com/blog/ransomware-blocker-to-cryptor/7295/.

ECPAT (2019). *Live streaming of child sexual abuse in real-time*. Retrieved January 23, 2019, from https://ecpat.org/resource/factsheets-on-online-child-sexual-exploitation-ocse-manifestations-live-streaming-of-child-sexual-abuse-in-real-time/.

EFE (25 de mayo de 2016). *Descubren el mayor productor ilegal de bitcoin para blanquear un fraude de TV*. Agencia EFE. https://web.archive.org/web/20220618041912/https://www.efe.com/efe/espana/sociedad/descubren-el-mayor-productor-ilegal-de-bitcoin-para-blanquear-un-fraude-tv/10004-2935598

EFE (9 de abril de 2018). Once detenidos de una red que blanqueaba dinero del narcotráfico a través de criptomonedas. *El Mundo.* https://www.elmundo.es/espana/2018/04/09/5acb154ee2704eef6b8b4603.html

El País (2 de enero de 2022). Detenido en Valencia uno de los mayores estafadores en inversiones con criptomonedas de Europa. *El País*. Consultado el 30 de enero de 2021 en https://elpais.com/economia/2022-01-02/detenido-en-valencia-uno-de-los-mayores-estafadores-en-inversiones-con-criptomonedas-de-europa.html?event=go&event_log=go&prod=REGCRART&o=cerrado

ePOOLICE (2015). *early Pursuit against Organized crime using envirOnmental scanning, the Law and IntelligenCE systems.* https://cordis.europa.eu/project/id/312651/reporting/es

Escobar, V. (22 de julio de 2017). *Cae Hansa: Operación policíaca internacional desmantela el tercer mayor mercado de la Deep Web.* Criptonoticias. https://www.criptonoticias.com/sucesos/cae-hansa-operacion-policiaca-internacional-desmantela-tercermayor-mercado-deep-web/

España Alba, V. M. (2016). *Criptodivisas: Bitcoin y el blanqueo de capitales.* ElDerecho, https://elderecho.com/criptodivisas-bitcoin-y-el-blanqueo-de-capitales

Esparragoza, L. (2017, July 26). *Casa de cambio BTC-e involucrada en robo multimillonario a MtGox*. Criptonoticias. https://www.criptonoticias.com/judicial/casa-cambio-btc-e-involucrada-robo-multimillonario-mtgox-arrestado/

Ethereum (2021a). *¿Qué es el ether (ETH)?* https://ethereum.org/es/eth/

Ethereum (2021b). *Decentralized autonomous organizations (DAOs).* https://ethereum.org/en/dao/

Ethereum (2021c). *Decentralized finance (DeFi). Ethereum Use Cases.* https://ethereum.org/en/defi/

Ethereum (2021d). *Non-fungible tokens (NFT).* https://ethereum.org/en/nft/

Ethereum. (2020, October 14). *What is Ethereum*. https://ethereum.org/es/what-is-ethereum/

Europa Press (27 de septiembre de 2021). *Uno de los investigados por la presunta 'criptoestafa' de Arbistar reconoce al juez su papel de cambista.* Europa Press. Consultado el 30 de enero de 2022 en https://www.europapress.es/nacional/noticia-investigados-presunta-criptoestafa-arbistar-reconoce-juez-papel-cambista-20210927115531.html

Europol (2011b). *Threat Assessment on Internet Facilitated Organised Crime (iOCTA) 2011*. https://www.europol.europa.eu/activities-services/main-reports/threat-assessment-internet-facilitated-organised-crime-iocta-2011

Europol (2014). *The Internet Organised Crime Threat Assessment (iOCTA) 2014*. https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web.pdf

Europol (2017). *Serious and organised crime threat assessment: Crime in the age of technology*. 60. https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017

Europol (2018). *Internet Organised Crime Threat Assessment (IOCTA) 2018*. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

Europol (2019). *Internet Organised Crime Threat Assessment (IOCTA)*. *IOCTA report*. https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf.

Europol (2021). *Internet Organised Crime Threat Assessment (IOCTA) 2021*. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021

Europol (2022a). *Cryptocurrencies: Tracing the Evolution of Criminal Finances*. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

Europol (2022b). *European Union Terrorism Situation and Trend Report 2022*. https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf

Europol (3 de Abril de 2020). *Catching the virus cybercrime, disinformation, and the COVID-19 pandemic.* https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic

Fanusie, Y. J., & Robinson, T. (2018). *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services*. Elliptic, Center on Sanctions & Illicit Finance. https://cdn2.hubspot.net/hubfs/3883533/downloads/Bitcoin%20Laundering.pdf

FBI (2020, April 13). *FBI Expects a Rise in Scams Involving Cryptocurrency Related to the COVID-19 Pandemic*. FBI News. https://www.fbi.gov/news/press-releases/fbi-expects-a-rise-in-scams-involving-cryptocurrency-related-to-the-covid-19-pandemic

Fernández, A. F. (2018). *Guía Bitcoin 2018: La guía más práctica, completa y actualizada para iniciarse y avanzar en el mundo bitcoin.* Independently published.

Fernández Bermejo, D. y Martínez Atienza, G. (2018). *Ciberseguridad, ciberespacio y ciberdelincuencia*. Aranzadi.

Financial Action Task Force (2014). *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*. https://www.fatf-gafi.org/content/dam/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.coredownload.pdf

Financial Action Task Force (2021). *Who we are*. http://www.fatf-gafi.org/about/whoweare/#d.en.11232

Financial Action Task Force (2022). Money Laundering - Financial Action Task Force (FATF). https://www.fatf-gafi.org/faq/moneylaundering/

Finney, H. (1993a, August 19). *Digital Cash & Privacy*. Satoshi Nakamoto Institute. https://nakamotoinstitute.org/digital-cash-and-privacy/

Finney, H. (1993b, October 15). *Detecting Double Spending*. Satoshi Nakamoto Institute. https://nakamotoinstitute.org/detecting-double-spending/

Finney, H. (2013, March 19). *Bitcoin and me (Hal Finney)*. [Online forum post]. BitcoinTalk. https://bitcointalk.org/index.php?topic=155054.0

Fiscal General del Estado (2021). *Memoria de la fiscalía general del Estado de 2021.* Recuperado el 27 de enero de 2021 de https://www.fiscal.es/memorias/memoria2021/FISCALIA_SITE/index.html

Fleder, M., Kester, M. S., & Pillai, S. (2015). *Bitcoin transaction graph analysis.* arXiv. https://doi.org/10.48550/arXiv.1502.01657

Foley, S., Karlsen, J. R., & Putniņš, 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

Foundation (2021). *About.* https://foundation.app/about

Gálvez, J. J. (2021). El nuevo auge de las criptoestafas copia el viejo fraude piramidal. *El País.* https://elpais.com/economia/2021-07-24/el-auge-de-las-criptoestafas.html#?rel=mas

García Meras, T. (2021). Blockchain: Introducción, casos de uso y casos de abuso. En J. M. Corchado y J. L. Tejedor (Ed..), *C1b3rWall Academy- Módulo 0*. Universidad de Salamanca.

Garcia Sigman, L. I. (2017). Narcotráfico en la Darkweb: los criptomercados/ Illicit Drug Trafficking on the Darkweb: Criptomarkets. *URVIO - Revista Latinoamericana de Estudios de Seguridad*, (21), 191–206. https://doi.org/10.17141/urvio.21.2017.2824

García, J. (31 de agosto de 2019). *Napster: inicio, auge y caída del servicio que puso en jaque a la industria musical.* Xataka. https://www.xataka.com/historia-tecnologica/napster-inicio-auge-caida-servicio-que-puso-jaque-a-industria-musical

Glaser, F., Zimmermann, K., Haferkorn, M., Haferkorn, M. and Weber, M. C. & Siering, M. (2014). Bitcoin - Asset or Currency? Revealing Users' Hidden. *ECIS 2014,* (Tel Aviv). https://ssrn.com/abstract=2425247.

Glasser, B. G. & Strauss, A. L. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research.* Aldine.

Goldstein, H. (1990). *Problem-oriented policing.* New York: McGraw-Hill.

González, A. (2021). Blockchain como inicio de la revolución tecnológica del sector financiero. En J. M. Corchado y J. L. Tejedor (Ed..), *C1b3rWall Academy- Módulo 0*. Universidad de Salamanca.

González, G. (6 de octubre de 2021). Aumentan las víctimas de estafas por inversiones y transacciones en criptomonedas. *El Mundo.* Consultado el 30 de enero de 2022 en https://www.elmundo.es/cataluna/2021/10/06/615d6d1521efa0ff2b8b4608.html

González-Meneses, M. (2019). *Entender Blockchain: una introducción a la tecnología de registro distribuido* (2a ed.). Thomson Reuters Aranzadi.

Gorjón, S. (2014). *Divisas o Monedas Virtual: El caso de Bitcoin*. Banco de España. https://www.in-diem.com/wp-content/uploads/2017/12/Nota_informativa_Bitcoin_enero2014.pdf

Greenberg, A. (2014, February 26). Nearly 150 Breeds of Bitcoin- Stealing Malware in The Wild, Researchers Say. *Forbes.* http://www.forbes.com/sites/andygreenberg/2014/02/26/nearly-150-breeds-of-bitcoin-stealing-malware-in-the-wild-researchers-say/

Greenberg, A. (2015, February 4). *Silk Road Mastermind Ross Ulbricht Convicted of All 7* Charges. Wired. https://www.wired.com/2015/02/silk-road-ross-ulbricht-verdict/

Guardia Civil (2018, April 9). *La Guardia Civil desarticula una organización criminal dedicada al blanqueo de capitales procedentes del narcotráfico mediante el uso de criptomonedas*. https://www.guardiacivil.es/es/prensa/noticias/6552.html

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology*, 3(2), 99–111. https://doi.org/10.1007/BF00196791

Hampton, N., & Baig, Z. (2015). Ransomware: Emergence of the cyber-extortion menace. In *13th Australian Information Security Management Conference* (pp. 47–56). SRI Security Research Institute, Edith Cowan University. https://doi.org/10.4225/75/57b69aa9d938b

Hanel, A. (10 enero de 2019). *Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware*. CrowdStrike. https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

Heap, V. y Waters, J. (2018). Using mixed methods in criminological research. En P. Davies y P. Francis, *Doing criminological research* (pp. 114-134). SAGE.

Hendrickson, J. R., & Luther, W. J. (2022). Cash, crime, and cryptocurrencies. *The Quarterly Review of Economics and Finance*, *85*, 200–207. https://doi.org/10.1016/j.qref.2021.01.004

Hern, A. (2014, March 18). A history of bitcoin hacks. *The Guardian.* https://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency

Hernández, A. (13 de enero de 2016). *EUROPOL y otros cuerpos policiales ejecutan operaciones contra un grupo de ataques cibernéticos.* Criptonoticias. https://www.criptonoticias.com/seguridad-bitcoin/europol-y-otros-cuerpos-policiales-ejecutan-operaciones-contra-un-grupo-de-ataques-ciberneticos/

Herraiz, P. y Alsedo, Q. (27 de marzo de 2018). Cae en España el "hacker" de los 10.000 millones, el ciberladrón más importante del mundo: Carbanak. *El Mundo*. http://www.elmundo.es/espana/2018/03/26/5ab8bdeb268e3ed01d8b4636.html:

Herrera, J. (2021, December 17). *Rug Pulls, un tipo de estafa con criptomonedas que prevalece en DeFi y ha crecido este año*. Criptonoticias. https://www.criptonoticias.com/comunidad/rug-pulls-tipo-estafa-criptomonedas-prevalece-defi-crecido-este-ano/

Higbee, A. (2018). The role of crypto-currency in cybercrime. *Computer Fraud & Security*, *2018*(7), 13–15. https://doi.org/10.1016/S1361-3723(18)30064-2

Higgins, S. (2015, February 5). *Bitstamp claims $5 million lost in hot wallet hack*. *CoinDesk*. http://www.coindesk.com/bitstamp-claims-roughly-19000-btc-losthot-wallet-hack/

Higgins, S. (2016, June 9). *Ransomware Concerns Prompt UK Businesses to Buy Bitcoins, Survey Finds*. *CoinDesk.* https://www.coindesk.com/markets/2016/06/09/ransomware-concerns-prompt-uk-businesses-to-buy-bitcoins-survey-finds/

Hong, Y., Kwon, H., Lee, J., & Hur, J. (2018). *A Practical De-mixing Algorithm for Bitcoin Mixing Services*. *BCC '18: Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts*, 15–20. https://doi.org/10.1145/3205230.3205234

Hospital Universitario de Torrejón (27 de enero de 2020). *El Hospital Universitario de Torrejón avanza en el restablecimiento de sus sistemas informáticos*. Recuperado el 31 de enero de 2020 de https://www.hospitaldetorrejon.es/noticia/el-hospital-universitario-de-torrejon-mantiene-su-actividad-asistencial-tras-sufrir-una-incidencia-informatica/255/

Huang, D., Dharmdasani, H., Meiklejohn, S., Dave, V., Grier, C., Mccoy, D., Savage, S., Weaver, N., Snoeren, A. & Levchenko, K. (2014). Botcoin: Monetizing Stolen Cycles, *Network and Distributed System Security Symposium '14,* 23-26 February 2014, San Diego, CA, USA 10.14722/ndss.2014.23044.

Huang, D. Y., Aliapoulios, M. M., Li, V. G., Invernizzi, L., Bursztein, E., McRoberts, K., Levin, J., Levchenko, K., Snoeren, A. C., & McCoy, D. (2018). Tracking Ransomware End-to-end. *Proceedings - IEEE Symposium on Security and Privacy*, *2018-May*, 618–631. https://doi.org/10.1109/SP.2018.00047

Hughes, E. (1993, March 9). *A Cypherpunk's Manifesto*. https://www.activism.net/cypherpunk/manifesto.html

IBM (2021a). *Farmer Connect + IBM.* https://mediacenter.ibm.com/media/1_8nksvgym

IBM (2021b). *TradeLens and Blockchain Technology Supply Chain Demo.* https://mediacenter.ibm.com/media/t/1_8rzr58wb

IBM (2021c). *What is Blockchain for Business?* https://www.ibm.com/topics/blockchain-for-business

INCIBE. (2019). *Servicio AntiRansomware.* Retrieved October 23, 2019, from https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware.

Irwin, A. S. M., & Turner, A. B. (2018). Illicit Bitcoin transactions: challenges in getting to the who, what, when and where. *Journal of Money Laundering Control*, *21*(3), 297–313. https://doi.org/10.1108/JMLC-07-2017-0031

Ivantsov S.V., Sidorenko E.L., Spasennikov B.A., Berez- kin Yu.M., Sukhodolov Ya.A. (2019). Cryptocurrency-related crimes: key criminological trends. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 13(1), 85-93. https://doi.org/10.17150/2500-4255.2019.13%281%29.85-93

Janze, C. (2017). Are cryptocurrencies criminals best friends? examining the co-evolution of bitcoin and darknet markets. *AMCIS 2017 - America's Conference on Information Systems: A Tradition of Innovation*, *2*. https://aisel.aisnet.org/amcis2017/InformationSystems/Presentations/2

Jarvis, K. (2013, December 18). *CryptoLocker Ransomware*. Securework. https://www.secureworks.com/research/cryptolocker-ransomware

Jeffries, A. (2012, August 27). *Suspected multi-million dollar Bitcoin pyramid scheme shuts down, investors revolt*. The Verge. https://www.theverge.com/2012/8/27/3271637/bitcoin-savings-trust-pyramid-scheme-shuts-down

Jgarzik. (2010, August 15). *Strange block 74638*. [Online forum post]. BitcoinTalk. https://bitcointalk.org/index.php?topic=822.0

Juels, A., Kosba, A., & Shi, E. (2016). The Ring of Gyges: Investigating the Future of Criminal Smart Contracts. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 283–295. https://doi.org/10.1145/2976749.2978362

Kaplan, J. (2017). *Inteligencia artificial: lo que todo el mundo debe saber.* Teel.

Kappos, G., Yousaf, H., Maller, M., and Meiklejohn, S. (2018). An Empirical Analysis of Anonymity in Zcash. In *Proceedings of the 27th USENIX Security Symposium*. https://www.usenix. org/conference/usenixsecurity18/presentation/kappos.

Kethineni, S., & Cao, Y. (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review*, *30*(3), 325–344. https://doi.org/10.1177/1057567719827051

Kethineni, S., Cao, Y. & Dodge, C. (2018). Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes. *Am J Crim Just* 43, 141–157. https://doi.org/10.1007/s12103-017-9394-6

Khandelwal, S. (2017). *Petya Ransomware Spreading Rapidly Worldwide, Just Like WannaCry*. The Hacker News. https://thehackernews.com/2017/06/petya-ransomware-attack.html

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., Kirda, E. (2015). Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. In: Almgren, M., Gulisano, V., Maggi, F. (eds) *Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2015. Lecture Notes in Computer Science (),* vol 9148. Springer, Cham. https://doi.org/10.1007/978-3-319-20550-2_1

Koe, Alonso, K. M., & Noether, S. (2020). *Zero to Monero: Second Edition. A technical guide to a private digital currency; for beginners, amateurs, and experts.* (2º). https://www.getmonero.org/es/library/Zero-to-Monero-2-0-0.pdf

Kruisbergen, E. W., Leukfeldt, E. R., Kleemans, E. R., & Roks, R. A. (2019). Money talks money laundering choices of organized crime offenders in a digital age. *JOURNAL OF CRIME & JUSTICE*, 42(5), 569-581. https://doi.org/10.1080/0735648X.2019.1692420

Kryskova Kuksa, T. (2017). El bitcoin. La cibermoneda que reta al legislador. En F. B. de Mata (Ed.), *FODERTICS 6.0: los nuevos retos del derecho ante la era digital* (6th ed., pp. 325–335). Comares. https://dialnet.unirioja.es/servlet/articulo?codigo=6200960

Kumar, A., Fischer, C., Tople, S., Saxena, P. (2017). A Traceability Analysis of Monero's Blockchain. In: Foley, S., Gollmann, D., Snekkenes, E. (eds) *Computer Security – ESORICS 2017. ESORICS 2017. Lecture Notes in Computer Science* (), vol 10493. Springer, Cham. https://doi.org/10.1007/978-3-319-66399-9_9

Kuzuno, H., and Karam, C. (2017). Blockchain explorer: An analytical process and investigation environment for bitcoin. In *2017 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 9-16). IEEE. https://doi.org/10.1109/ECRIME.2017.7945049

Lage, Ó. (2021). Privacy-preserving computing: compartición y explotación segura del dato. En J. M. Corchado y J. L. Tejedor (Ed..), *C1b3rWall Academy- Módulo 0*. Universidad de Salamanca.

Laszlo (2010a, May 10). *Generating Bitcoins with your video card (OpenCL/CUDA)*. [Online forum post]. BitcoinTalk. https://bitcointalk.org/index.php?topic=133.msg1103#msg1103

Laszlo (2010b, May 18). *Pizza for bitcoins?* [Online forum post]. BitcoinTalk. https://bitcointalk.org/index.php?topic=137.msg1195#msg1195

Laszlo (2010c, May 22). *Re: Pizza for bitcoins?* [Online forum post]. BitcoinTalk. https://bitcointalk.org/index.php?topic=137.msg1195#msg1195

Lee, C., Maharjan, S., Ko, K., & Hong, J. W.-K. (2020). Toward Detecting Illegal Transactions on Bitcoin Using Machine-Learning Methods. In *1st International Conference on Blockchain and Trustworthy Systems, BlockSys 2019* (pp. 520–533). https://doi.org/10.1007/978-981-15-2777-7_42

Lester, C. (2017, January 9). *Terrorists use bitcoin and PayPal in Indonesia, AML official claims.* CCN.com. https://www.ccn.com/terrorists-use-bitcoin-and-paypal-in-indonesia-agency-official-claims/.

Liao, K., Zhao, Z., Doupe, A., and G. Ahn, G. J. (2016). Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin. *2016 APWG Symposium on Electronic Crime Research (eCrime)*, Toronto, ON, Canada, pp. 1-13, doi: 10.1109/ECRIME.2016.7487938.

Lin, Y.-J., Wu, P.-W., Hsu, C.-H., Tu, I.-P., & Liao, S. (2019). An Evaluation of Bitcoin Address Classification based on Transaction History Summarization. *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 302–310. https://doi.org/10.1109/BLOC.2019.8751410

Lindrea, B. (31 de octubre de 2022). *Los terroristas están financiando sus horribles actos con criptomonedas, dice una funcionaria de la ONU*. Cointelegraph. https://es.cointelegraph.com/news/tech-savvy-terrorists-are-using-crypto-to-finance-their-horrible-deeds-un-official

Litecoin (2023). *Sobre nosotros: ¿Qué es Litecoin?* Litecoin. https://litecoin.org/es/

Litecoin Project. (2021). *¿Qué es Litecoin?* https://litecoin.org/es/

Litecoin Wiki. (2019). *Litecoin*. Litecoinwiki. https://litecoin.info/index.php/Main_Page

Lopp, J. (2016, April 9). *Bitcoin and the Rise of the Cypherpunks*. Cypherpunk Cogitations. https://blog.lopp.net/bitcoin-and-the-rise-of-the-cypherpunks/

Martí, A. (16 de mayo de 2017). *Un ciberataque deja fuera de juego la intranet de Telefónica en toda España.* Xataka. https://www.xataka.com/seguridad/un-ciberataque-deja-fuera-de-juego-la-intranet-de-telefonica-en-toda-espana#comments

Martin, J. (2014). Lost on the Silk Road: Online drug distribution and the 'cryptomarket.' *Criminology and Criminal Justice*, *14*(3), 351–367. https://doi.org/10.1177/1748895813505234

Martínez, A. (5 de octubre de 2015). El indestructible monstruo del cibersexo infantil. *El País.* https://elpais.com/elpais/2015/10/02/planeta_futuro/1443780472_354261.html

Masjerez (3 de octubre de 2019). *Ciberataque al Ayuntamiento de Jerez: caos y datos expuestos por instalar un antivirus gratuito*. Recuperado el 1 de febrero de 2020 de https://masjerez.com/noticias/ciberataque-al-ayuntamiento-de-jerez-caos-y-datos-expuestos-por-instalar-un-antivirus-gratuito

Matzutt, R. et al. (2018). A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin. In: Meiklejohn, S., Sako, K. (eds) *Financial Cryptography and Data Security. FC 2018. Lecture Notes in Computer Science* (), vol 10957. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-58387-6_23

May, T. C. (1992, November 22). *The Crypto Anarchist Manifesto*. https://activism.net/cypherpunk/crypto-anarchy.html

Mayer-Schönberger, V. y Cukier, K. (2013) *Big Data: La revolución de los datos masivos*. Turner.

McCorry, P., Möser, M., Ali, S.T. (2018). Why Preventing a Cryptocurrency Exchange Heist Isn't Good Enough. In: Matyáš, V., Švenda, P., Stajano, F., Christianson, B., Anderson, J. (eds) Security Protocols XXVI. Security Protocols 2018. *Lecture Notes in Computer Science ()*, vol 11286. Springer, Cham. https://doi.org/10.1007/978-3-030-03251-7_27

Medina, J. (2011). *Políticas y estrategias de prevención del delito y seguridad ciudadana.* Edisofer.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of bitcoins: characterizing payments among men with no names. *Proceedings of the 2013 Conference on Internet Measurement Conference - IMC '13*, 127–140. https://doi.org/10.1145/2504730.2504747

Miró-Llinares, F. (2012). El cibercrimen. Marcial Pons.

Miró-Llinares, F. (2018). Inteligencia artificial y Justicia Penal. Más allá de los resultados lesivos causados por robots, *Revista de Derecho Penal y Criminología,* 20, pp.87-130. https://doi.org/10.5944/rdpc.20.2018.26446

Miró-Llinares, F. (2020). Predictive policing: Utopia or dystopia? On attitudes towards the use of big data algorithms for law enforcement, *IDP revista de Internet, derecho y política = revista d'Internet, dret i política*, 30, http://dx.doi.org/10.31235/osf.io/a7juk

Monero (2021a). *Ring Signature*. Moneropedia. https://www.getmonero.org/resources/moneropedia/ringsignatures.html

Monero (2021b). *Sobre Monero*. https://www.getmonero.org/es/resources/about/

Monero (2021c). *Stealth Address*. Moneropedia. https://www.getmonero.org/resources/moneropedia/stealthaddress.html

Moore, T. & Christin, N. (2013). Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. In: Sadeghi, AR. (eds) Financial Cryptography and Data Security. *FC 2013. Lecture Notes in Computer Science,* vol 7859. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-39884-1_3

Mtgox (2010). *New Bitcoin Exchange (mtgox.com)*. [Online forum post]. BitcoinTalk. https://bitcointalk.org/index.php?topic=444.0

Murko, A. & Vrhovec, S. L. R. (2019). Bitcoin adoption: Scams and anonymity may not matter but trust into Bitcoin security does. In S. Vrhovec (Ed.), *Proceedings of the Third Central European Cybersecurity Conference (CECC 2019)* (pp. 1–6). Association for Computing Machinery. https://doi.org/10.1145/3360664.3360679

Nadir, I. & Bakhshi, T. (2018). Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques. In *2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)* (pp. 1-7). IEEE. https://doi.org/10.1109/ICOMET.2018.8346329

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. www.bitcoin.org

Nauert, H. (2015, November 25). *ISIS parks its cash in bitcoin experts say*. Fox News Tech. https://www.foxnews.com/tech/2015/11/25/isis-parks-its-cash-in-bitcoin-experts-say.html

Nieto, A. (18 de febrero de 2018). *Cuál es la diferencia entre criptomoneda, moneda virtual y dinero digital*. Xakata. https://www.xataka.com/criptomonedas/cual-es-la-diferencia-entre-criptomoneda-moneda-virtual-y-dinero-digital

No More Ransom (2020a). *Preguntas más frecuentes: Las historia del Ransomware.* https://www.nomoreransom.org/es/ransomware-qa.html

No More Ransom (2020b). *Preguntas más frecuentes: Tipos de ransomware.* https://www.nomoreransom.org/es/ransomware-qa.html

No More Ransom (2020c). *Sobre el proyecto*. https://www.nomoreransom.org/es/about-the-project.html

Noether, S., Mackenzie, A. & Monero Core Team (2016). Ring Confidential Transactions. *Monero Research Lab*. https://web.getmonero.org/resources/research-lab/pubs/MRL-0005.pdf

Oggier, F., Datta, A., & Phetsouvanh, S. (2020). An ego network analysis of sextortionists. *Social Network Analysis and Mining, 10*(1), 44. https://doi.org/10.1007/s13278-020-00650-x

Owen, G., & Savage, N. (2015). The Tor Dark Net. In *Global Commission on Internet Governance Paper Series: NO.20* (No. 20). https://www.cigionline.org/sites/default/files/no20_0.pdf

Oxford University Press. (2020a). Cryptocurrency. In *Oxford Advanced Learner's Dictionary.* https://www.oxfordlearnersdictionaries.com/definition/english/cryptocurrency?q=cryptocurrency

Oxford University Press. (2020b). Cryptocurrency. *Oxford English Dictionary.* https://www.oed.com/view/Entry/79224404?redirectedFrom=cryptocurrency#eid

Oz, H., Aris, A., Levi, A., & Uluagac, A.S. (2021). A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. *ACM Computing Surveys (CSUR), 54*, 1 - 37.

Paganini, P. (2012, September 17). *The good and the bad of the Deep Web*. Security Affairs. http://securityaffairs.co/wordpress/8719/cyber-crime/the-good-and-the-bad-of-the-deep-web.html

Palomo-Zurdo, R. (2021). Las criptomonedas en la sociedad digital: ¿visión o transgresión? En B. Belando Garín (Dir.), *Las criptomonedas a debate* (pp. 13–34). Aranzadi.

Panda Security (2010). *¿Qué es peer-to-peer (P2P)?* http://resources.pandasecurity.com/enterprise/solutions/8.%20WP%20PCIP%20que%20es%20p2p.pdf

Paquet-Clouston, M., Bernhard Haslhofer, B. & Benoît Dupont, B. (2019). Ransomware payments in the Bitcoin ecosystem. *Journal of Cybersecurity*, 5 (1), tyz003. https://doi.org/10.1093/cybsec/tyz003

Partz, H. (2020, March 19). *Scammers Impersonate World Health Organization to Steal BTC COVID-19 Donations*. Cointelegraph. https://cointelegraph.com/news/scammers-impersonate-world-health-organization-to-steal-btc-covid-19-donations

Pérez López, X. (2017). Las criptomonedas: consideraciones generales y empleo de las criptomonedas como instrumento de blanqueo de capitales en la Unión Europea y en

España. *Revista de Derecho Penal y Criminología*, *18*, 141–187. http://e-spacio.uned.es/fez/view/bibliuned:revistaDerechoPenalyCriminologia-2017-18-7030

Pérez, D. (2020). Blockchain, criptomonedas y los fenómenos delictivos: entre el crimen y el desarrollo. *Boletín criminológico,* 26 (197). https://doi.org/10.24310/Boletin-criminologico.2020.v27i.11283

Pérez, E. (4 de octubre de 2019). *Paralizan el Ayuntamiento de Jerez encriptando su base de datos con un virus informático y piden un rescate para liberarlo*. Xataka. https://www.xataka.com/seguridad/paralizan-ayuntamiento-jerez-encriptando-su-base-datos-virus-informatico-piden-rescate-para-liberarlo

Pérez, J. (4 de noviembre de 2019). Un virus de origen ruso ataca a importantes empresas españolas. *El País.* https://elpais.com/tecnologia/2019/11/04/actualidad/1572897654_251312.html?ssm=TW_CM_TEC

Perry, W. L., McInnis, B., Price, C. C., Smith, S. C. y Hollywood, J. S (2013). *Predictive Policing.* RAND OFFICES.

Phetsouvanh, S., Oggier, F., & Datta, A. (2018). EGRET: Extortion Graph Exploration Techniques in the Bitcoin Network. In H. Tong, Z and Li, F. Zhu (Eds.), *2018 IEEE International Conference on Data Mining Workshops (ICDMW)* (pp. 244–251). IEEE. https://doi.org/10.1109/ICDMW.2018.00043

Pieters, G. C. & Vivanco, S. (2017). Financial regulations and price inconsistencies across Bitcoin markets. *Information Economics and Policy,* 39, 1-14, https://doi.org/10.1016/j.infoecopol.2017.02.002

Plohmann, D., & Gerhards-Padilla, E. (2012). Case study of the Miner Botnet. In C. Czosseck, R. Ottis and K. Ziolkowski (Eds.), *4th International Conference on Cyber Conflict (CYCON 2012)*. https://ieeexplore.ieee.org/document/6243985/authors#authors

Ponce de León, P. J. (2018). Blockchain, un nuevo patrón tecnológico. En *Blockchain: Aspectos Tecnológicos, Empresariales y Legales* (1º, pp. 35–77). Thomson Reuters Aranzadi.

Poulsen, K. (2011, June 16). *New Malware Steals Your Bitcoin*. Wired. https://www.wired.com/2011/06/bitcoin-malware/.

Prosegur (27 de noviembre de 2019). *Actualización sobre incidencia de seguridad informática.* Recuperado el 31 de enero del 2020 de https://twitter.com/Prosegur/status/1199731997947711492?s=20

Quarmby, B. (2021). *Una pareja se casa en la blockchain de Ethereum por 587 dólares.* Cointelegraph. https://es.cointelegraph.com/news/couple-gets-married-on-ethereum-blockchain-for-587-in-transaction-fees

RAE (2020). Moneda. En *Diccionario de la lengua española.* https://dle.rae.es/moneda?m=form

RAE (2023). Criptomoneda. *Diccionario de la lengua española.* https://dle.rae.es/criptomoneda

Ratcliffe, J. (2008). *Intelligence- Led Policing*. Cullompton, UK: Willan.

Rauchs, M., Glidden, A., Gordon, B., Pieters, G. C., Recanatini, M., Rostand, F., Vagneur, K., & Zhang, B. Z. (2018). Distributed Ledger Technology Systems: A Conceptual Framework. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3230013

Redondo, S. y Garrido, V. (2013). *Principios de Criminología.* Tirant Lo Blanch.

Reid, F., & Harrigan, M. (2013). An Analysis of Anonymity in the Bitcoin System. In Y. Altshuler, Y. Elovici, A. Cremers, N. Aharony, & A. Pentland (Eds.), *Security and Privacy in Social Networks* (pp. 197–223). Springer New York. https://doi.org/10.1007/978-1-4614-4139-7_10

Richet, J.-L. (2013). Laundering Money Online: a review of cybercriminals methods. In *Tools and Resources for Anti-Corruption Knowledge, June, 01, 2013. United Nations Office on Drugs and Crime (UNODC).* https://arxiv.org/ftp/arxiv/papers/1310/1310.2368.pdf

Rodríguez, P. (3 de julio de 2019). *Cuando una empresa sufre un ataque de ransomware, me llaman para solucionarlo: la difícil lucha contra el malware del momento.* Xataka. https://www.xataka.com/seguridad/cuando-empresa-sufre-ataque-ransomware-me-llaman-para-solucionarlo-dificil-lucha-malware-momento

Romero, P. (16 de junio de 2015). Pablo Soto vuelve a ganar a las discográficas: crear tecnología P2P es legal. *El Mundo.* https://www.elmundo.es/tecnologia/2014/04/09/5345682322601d2c688b4580.html

Ron, D., Shamir, A. (2013). Quantitative Analysis of the Full Bitcoin Transaction Graph. In A. R., Sadeghi (eds) *Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science*, vol 7859. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-39884-1_2

Roy, J. (2014, January 27). BitInstant CEO Charlie Shrem Arrested for Alleged Money Laundering. *Time*. https://time.com/1892/bitinstant-ceo-charlie-shrem-arrested-for-alleged-money-laundering/

Russo, C. (7 de agosto de 2018). *Bitcoin Speculators, Not Drug Dealers, Dominate Crypto Use Now.* Bloomberg. https://www.bloomberg.com/news/articles/2018-08-07/bitcoin-speculators-not-drug-dealers-dominate-crypto-use-now#xj4y7vzkg

Saldaña-Taboada, P. (2019). ¿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/view/20883

Saldaña-Taboada, P. (2022). La victimización en los delitos cometidos con criptomonedas: Aproximación al panorama español. En M. Olmedo Cardenete, N. Castelló Nicás, M. J. Jiménez Díaz, C. Aránguez Sánchez y J. Barquín Sanz (Coords.), *Estudios en homenaje al Profesor Dr. D. Jesús Martínez Ruiz*. Dykinson.

Salgado, Z. (2019, March 15). *CEO de Mt Gox es hallado culpable de uno de sus cargos*. Criptonoticias. https://www.criptonoticias.com/judicial/ceo-mtgox-hallado-culpable-cargos/

Satoshi Nakamoto Institute. (2021). *Hal Finney*. https://nakamotoinstitute.org/finney/

Satoshi. (2010). *Added some DoS limits, removed safe mode (0.3.19)*. [Online forum post]. BitcoinTalk. https://bitcointalk.org/index.php?topic=2228.msg29479#msg29479

Sattler, J. (2017, May 12). *WannaCry, the Biggest Ransomware Outbreak Ever*. F-Secure. https://blog.f-secure.com/wannacry-may-be-the-biggest-cyber-outbreak-since-conficker/

Schickler, J. (2022, May 9). *How Big Is Crypto Crime, Really?* CoinDesk. https://www.coindesk.com/policy/2022/05/09/how-big-is-crypto-crime-really/

Schueffel, P., Groeneweg, N., & Baldegger, R. (2019). *The Crypto Encyclopedia Coins, Tokens and Digital Assets from A to Z*. Growth Publisher, Bern. https://www.researchgate.net/publication/335290055_The_Crypto_Encyclopedia_Coins_Tokens_and_Digital_Assets_from_A_to_Z

Sigler, K. (2018). Crypto-jacking: how cyber-criminals are exploiting the crypto-currency boom. *Computer Fraud & Security*, *2018*(9), 12–14. https://doi.org/10.1016/S1361-3723(18)30086-1

Sonawane, V. (2015, September 22). *Bitcoin Fraud: Texas Man Pleads Guilty In Ponzi Scheme*. International Business Time. https://www.ibtimes.com/bitcoin-fraud-texas-man-pleads-guilty-ponzi-scheme-2107889

Soska, K., & Christin, N. (2015). Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. *24th USENIX Security Symposium*, 33–48.

https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/soska

Spagnuolo, M., Maggi, F., Zanero, S. (2014). BitIodine: Extracting Intelligence from the Bitcoin Network. In N., Christin, R. Safavi-Naini (eds.) Financial Cryptography and Data Security. FC 2014. *Lecture Notes in Computer Science (),* vol 8437. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-45472-5_29

Statista. (2020, June 12). *Distribution of leading cryptocurrencies from 2015 to 2020, by market capitalization*. Recuperado el 25 de noviembre de 2020 de https://www.statista.com/statistics/730782/cryptocurrencies-market-capitalization/

Stelzer, K. (2021). *Driving auto supply chains forward with blockchain.* IBM. https://www.ibm.com/case-studies/renault/

Stewart, J. (2014, February 26). *Cryptocurrency-Stealing Malware Landscape.* Secureworks. https://www.secureworks.com/research/cryptocurrency-stealing-malware-landscape#end1

Sun, Y., Xiong, H., Yiu, S. M., & Lam, K. Y. (2019). BitVis: An Interactive Visualization System for Bitcoin Accounts Analysis. *2019 Crypto Valley Conference on Blockchain Technology (CVCBT),* 21–25. https://doi.org/10.1109/CVCBT.2019.000-3

Swissinfo.ch (18 de enero de 2023). *Redada global en torno a plataforma de criptomonedas Bitzlato acusada de blanqueo.* Swissinfo.ch. https://www.swissinfo.ch/spa/redada-global-en-torno-a-plataforma-de-criptomonedas-bitzlato-acusada-de-blanqueo/48215908

Szabo, N. (1995). *Smart Contracts Glossary*. Satoshi Nakamoto Institute. https://nakamotoinstitute.org/smart-contracts-glossary/

Szabo, N. (1997). *The Idea of Smart Contracts*. Satoshi Nakamoto Institute. https://nakamotoinstitute.org/the-idea-of-smart-contracts/

Szabo, N. (2001). *Trusted Third Parties are Security Holes.* Satoshi Nakamoto Institute. https://nakamotoinstitute.org/trusted-third-parties/

Szabo, N. (2002). *Shelling Out: The Origins of Money.* Satoshi Nakamoto Institute. https://nakamotoinstitute.org/shelling-out/

Szabo, N. (2005, December 29). *Bit Gold*. Satoshi Nakamoto Institute. https://nakamotoinstitute.org/bit-gold/

Szabo, N. (2021). *Literature. Satoshi Nakamoto Institute*. https://nakamotoinstitute.org/authors/nick-szabo/

Teichmann, F.M.J. & Falker, M.C. (2021). Cryptocurrencies and financial crime: solutions from Liechtenstein. *Journal of Money Laundering Control*, 24 (4), 775-788. https://doi.org/10.1108/JMLC-05-2020-0060

Thankful_for_today (2014). *[ANN][BMR] Bitmonero - a new coin based on CryptoNote technology - LAUNCHED*. [Online forum post]. BitcoinTalk. https://bitcointalk.org/index.php?topic=563821.0

The Law Library of Congress (2021). *Regulation of Cryptocurrency Around the World: November 2021 Update*. https://tile.loc.gov/storage-services/service/ll/llglrd/2021687419/2021687419.pdf

Tierney, M. (2018). #TerroristFinancing: An Examination of Terrorism Financing via the Internet. *International Journal of Cyber Warfare and Terrorism (IJCWT), 8*(1), 1-11. http://doi.org/10.4018/IJCWT.2018010101

TITANIUM Project (2020a). *Frequently Asked Questions.* https://www.titanium-project.eu/faq/index.html

TITANIUM Project (2020b). *TITANIUM PROJECT.* https://www.titanium-project.eu/

TOR Project (2023). *About: History.* https://www.torproject.org/about/history/

Torrero, J. A. (2021). Blockchain: ¿Pero eso qué es? Blockchain para Dummies. En J. M. Corchado y J. L. Tejedor (Ed.), *C1b3rWall Academy- Módulo 0*. Universidad de Salamanca.

Tung, L. (2014, June 18). *NAS device botnet mined $$600,000 in dogecoin over two months.* ZDnet. http://www.zdnet.com/article/nas-device-botnet-mined-600000-in-dogecoin-over-two-months/

Turner, A., & Irwin, A. S. M. (2018). Bitcoin transactions: a digital discovery of illicit activity on the blockchain. *Journal of Financial Crime, 25*(1), 109–130. https://doi.org/10.1108/JFC-12-2016-0078

UNODC (2004). *Convención de las Naciones Unidas contra la delincuencia organizada transnacional y sus protocolos*. Naciones Unidas. https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

UNODC (2021). *Estrategia UNODC 2021-2025.* Naciones Unidas. https://www.unodc.org/res/strategy/full-strategy_html/full-strategy-ES.pdf

Valls-Prieto, J. y Gómez-Romero, J. (2016). Use of Big Data and the prediction of organized crime. AA. VV. *Building a European Digital Space* (pp.365-380). Estudis de Dret i Ciencia Politica.

Valls-Prieto, J. (2021). Inteligencia artificial, Derechos Humanos y bienes jurídicos. Editorial Aranzadi.

Valls-Prieto, J. (2022). *Un ejemplo de análisis empírico en el derecho penal basado en una metodología mixta. La orden europea de investigación*. Editorial Comares.

Van Wegberg, R., Oerlemans, J.-J. & Van Deventer, O. (2018). Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, 25 (2), 419-435. https://doi.org/10.1108/JFC-11-2016-0067

Vasek, M. & Moore, T. (2015). There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. In: Böhme, R., Okamoto, T. (eds) Financial Cryptography and Data Security. FC 2015. *Lecture Notes in Computer Science ()*, vol 8975. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-47854-7_4

Wang, H., He, D., Liu, Z., & Guo, R. (2020). Blockchain-Based Anonymous Reporting Scheme With Anonymous Rewarding. *IEEE Transactions on Engineering Management*, *67*(4), 1514–1524. https://doi.org/10.1109/TEM.2019.2909529

Wang, M., Ichijo, H., & Xiao, B. (2020, March 30). *Cryptocurrency Address Clustering and Labeling*. ArXiv. http://arxiv.org/abs/2003.13399

Waters, J. (2009). *Illegal Drug Use Among Older Adults* [PhD dissertation, University of Sheffielf]. EThOS Import Sheffield. https://etheses.whiterose.ac.uk/14974/1/522511.pdf

Wesley (2021, June 18). *Introduction to smart contracts.* Ethereum. https://ethereum.org/en/developers/docs/smart-contracts/

Wolfson, R. (2018a, November 13). Cryptojacking On the Rise: WebCobra Malware Uses Victims' Computers To Mine Cryptocurrency. *Forbes.* https://www.forbes.com/sites/rachelwolfson/2018/11/13/cryptojacking-on-the-rise-webcobra-malware-uses-victims-computers-to-mine-cryptocurrency/?sh=7e0c7d71c336

Wolfson, R. (2018b, November 26). Tracing Illegal Activity Through the Bitcoin Blockchain to Combat Cryptocurrency-Related Crimes. *Forbes.* https://www.forbes.com/sites/rachelwolfson/2018/11/26/tracing-illegal-activity-through-the-bitcoin-blockchain-to-combat-cryptocurrency-related-crimes/?sh=7058301433a9

Wu, Y., Luo, A., & Xu, D. (2019). Forensic Analysis of Bitcoin Transactions. *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 167–169. https://doi.org/10.1109/ISI.2019.8823498

Wuest, C. (2020, April 28). *Digital CoronaVirus: Yet Another Ransomware Combined with Infostealer*. Acronis. https://www.acronis.com/en-us/blog/posts/digital-coronavirus-yet-another-ransomware-combined-infostealer/

Xia, P., Wang, H., Luo, X., Wu, L., Zhou, Y., Bai, G., Xu, G., Huang, G., & Liu, X. (2020, July 27). *Don't Fish in Troubled Waters! Characterizing Coronavirus-themed Cryptocurrency Scams*. ArXiv. http://arxiv.org/abs/2007.13639

Yang, L., Dong, X., Xing, S., Zheng, J., Gu, X., & Song, X. (2019). An Abnormal Transaction Detection Mechanim on Bitcoin. In H. Xuanwen & W. Zhenqiang (Eds.), *2019 International Conference on Networking and Network Applications (NaNA)*, (pp. 452–457). IEEE. https://doi.org/10.1109/NaNA.2019.00083

Yelowitz, A. & Wilson, M. (2015). Characteristics of Bitcoin users: an analysis of Google search data. *Applied Economics Letters*, 22 (13). https://doi.org/10.1080/13504851.2014.995359

Zareh, A., & Shahriari, H. R. (2018). BotcoinTrap: Detection of Bitcoin Miner Botnet Using Host Based Approach. *2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)*, 1-6. https://doi.org/10.1109/ISCISC.2018.8546867

Zarracina, M. (2020, November 11). *Reopening venues with contactless blockchain digital ticketing*. IBM. https://www.ibm.com/blogs/blockchain/2020/11/reopening-venues-with-contactless-blockchain-digital-ticketing/

Zetter, K. (2012, September 8). *FBI Fears Bitcoin's Popularity with Criminals*. Wired. https://www.wired.com/2012/05/fbi-fears-bitcoin/

Zhao, C., Guan, Y. (2015). A GRAPH-BASED INVESTIGATION OF BITCOIN TRANSACTIONS. In G. Peterson and S. Shenoi (eds) *Advances in Digital Forensics XI. DigitalForensics 2015. IFIP Advances in Information and Communication Technology*, vol 462, (pp. 79–95). Springer, Cham. https://doi.org/10.1007/978-3-319-24123-4_5

Zheng, B., Zhu, L., Shen, M., Du, X., Yang, J., Gao, F., Li, Y., Zhang, C., Liu, S., & Yin, S. (2018). Malicious Bitcoin Transaction Tracing Using Incidence Relation Clustering. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and*

Telecommunications Engineering, LNICST, 313–323. https://doi.org/10.1007/978-3-319-90775-8_25

Zheng, B. *et al.* (2018). Malicious Bitcoin Transaction Tracing Using Incidence Relation Clustering. In: J. Hu, I. Khalil, Z. Tari, S. Wen (eds), Mobile Networks and Management. MONAMI 2017. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol 235, (pp. 313-323). Springer, Cham. https://doi.org/10.1007/978-3-319-90775-8_25

Zollner, S., Choo, K.-K. R., & Le-Khac, N.-A. (2019). An Automated Live Forensic and Postmortem Analysis Tool for Bitcoin on Windows Systems. *IEEE Access*, *7*, 158250–158263. https://doi.org/10.1109/ACCESS.2019.2948774

Zouhair, A. & Kasraie, N. (2019). Disrupting Fintech: Key Factors for Adopting Bitcoin. *Business and Economic Research, Macrothink Institute, 9*(2), 33-44. https://ideas.repec.org/a/mth/ber888/v9y2019i2p33-44.html

Legislación y Normativa

Circular 1/2022, de 10 de enero, de la Comisión Nacional del Mercado de Valores, relativa a la publicidad sobre criptoactivos presentados como objeto de inversión. https://www.boe.es/boe/dias/2022/01/17/pdfs/BOE-A-2022-666.pdf

DICTAMEN DEL BANCO CENTRAL EUROPEO de 12 de octubre de 2016 sobre una propuesta de directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica la Directiva 2009/101/CE (CON/2016/49) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016AB0049&from=ES

DIRECTIVA 2009/110/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 16 de septiembre de 2009 sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE https://www.boe.es/doue/2009/267/L00007-00017.pdf

Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) N.º 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión (Texto pertinente a efectos del EEE) https://www.boe.es/buscar/doc.php?id=DOUE-L-2015-81123

Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE. https://www.boe.es/buscar/doc.php?id=DOUE-L-2018-81022

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. https://www.boe.es/eli/es/lo/1995/11/23/10/con

Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. https://www.boe.es/eli/es/l/2010/04/28/10/con

Ley 21/2011, de 26 de julio, de dinero electrónico. https://www.boe.es/eli/es/l/2011/07/26/21

Ley 4/2015, de 27 de abril, del Estatuto de la víctima del delito. https://www.boe.es/eli/es/l/2015/04/27/4/con

Orden PCI/161/2019, de 21 de febrero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave. https://www.boe.es/eli/es/o/2019/02/21/pci161

Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional https://www.boe.es/eli/es/o/2019/04/26/pci487

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020PC0593&from=ES

Discusiones del Foro de la *Darknet*

Esta información ha sido eliminada por cuestiones de privacidad y seguridad. Se podrá acceder a estos datos por medio de una solicitud ante el órgano competente de la Universidad de Granada.

Apéndice

Apéndice 1. *Listado de las resoluciones judiciales*

ID	ID2	Término	Año
AN (Sala de lo Penal, Sección 4ª), auto núm. 14/2022 de 11 de enero	JUR 2022\48689	Criptomoneda	2022
AN (Sala de lo Penal, Sección 4ª), auto núm. 48/2022 de 31 de enero	JUR 2022\60334	Criptomoneda	2022
AN (Sala de lo Penal, Sección 4ª), auto núm. 49/2022 de 31 de enero	JUR 2022\59716	Criptomoneda	2022
TS (Sala de lo Penal, Sección 1ª), auto núm. 20039/2022 de 19 enero	JUR 2022\41407	Bitcoin	2022
AN (Sala de lo Penal, Sección 1ª) Auto núm. 548/2021 de 7 julio	JUR 2021\255684	Criptomoneda	2021
AN (Sala de lo Penal, Sección 1ª) Sentencia núm. 22/2021 de 5 julio	JUR 2021\230837	Criptomoneda	2021
AN (Sala de lo Penal, Sección 2ª) Auto núm. 26/2021 de 21 junio	JUR\2021\223783	Bitcoin, criptomoneda	2021
AN (Sala de lo Penal, Sección 3ª) Auto núm. 237/2021 de 30 junio	JUR\2021\253475	criptomoneda	2021
AN (Sala de lo Penal, Sección 3ª) Auto núm. 241/2021 de 30 junio	JUR 2021\254141	Criptomoneda	2021
AN (Sala de lo Penal, Sección 3ª) Auto núm. 248/2021 de 6 julio	JUR 2021\253689	Criptomoneda	2021
AN (Sala de lo Penal, Sección 3ª) Auto núm. 327/2021 de 10 septiembre	JUR 2021\306954	Criptomoneda	2021
AN (Sala de lo Penal, Sección 3ª) Auto núm. 349/2021 de 1 octubre	JUR 2021\325511	Criptomoneda	2021
AN (Sala de lo Penal, Sección 4ª) Auto núm. 488/2021 de 8 septiembre	JUR 2021\307100	Criptomoneda	2021
AP Barcelona (Sección 21ª), auto núm. 2128/2021 de 4 noviembre	JUR 2022\55708	Bitcoin, Blockchain, criptomoneda	2021
AP Barcelona (Sección 21ª), auto núm.2123/2021 de 4 de noviembre	JUR 2022\56042	Bitcoin, Blockchain, criptomoneda	2021
AP Barcelona (Sección 6ª), auto núm. 631/2021 de 17 septiembre	JUR 2022\10473	Bitcoin, criptomoneda	2021
AP Barcelona (Sección 8ª), auto núm. 768/2021 de 28 octubre	JUR 2022\55796	Criptomoneda	2021
AP de Álava (Sección 2ª) Sentencia núm. 4/2021 de 15 de enero	ARP 2021\679	Bitcoin, criptomoneda	2021
AP de Barcelona (Sección 21ª) Auto núm. 265/2020 de 21 enero	JUR\2021\149183	Bitcoin, Blockchain, criptomoneda	2021
AP de Barcelona (Sección 21ª), auto núm. 289/2021 de 28 de enero	JUR 2021\367571	Criptomoneda	2021
AP de Burgos (Sección 1ª) Sentencia núm. 96/2021 de 23 marzo	JUR\2021\166930	Bitcoin, criptomoneda	2021
AP de Burgos (Sección 1ª) Auto núm. 93/2021 de 8 febrero	JUR\2021\100808	Bitcoin, criptomoneda	2021
AP de Guipúzcoa (Sección 3ª) Auto núm. 48/2021 de 23 febrero	JUR 2021\206850	Criptomoneda	2021
AP de Islas Baleares (Sección 2ª) Sentencia núm. 80/2021 de 24 de febrero	JUR 2021\200435	Criptomoneda	2021
AP de Madrid (Sección 4ª), auto núm. 333/2021 de 26 de mayo	JUR 2021\374627	Criptomoneda	2021

AP de Ourense (Sección 2ª) Auto núm. 66/2021 de 4 febrero	JUR 2021\128921	Criptomoneda	2021
AP de Salamanca (Sección 1ª) Sentencia núm. 24/2021 de 25 junio	JUR\2021\247102	Bitcoin, criptomoneda	2021
AP de Zaragoza (Sección 6ª) Auto núm. 132/2021 de 16 marzo	JUR 2021\169420	Criptomoneda	2021
AP de Badajoz (Sección 3ª) Sentencia núm. 52/2021 de 6 abril	JUR\2021\164300	Bitcoin	2021
AP de Zaragoza (Sección 6ª) Sentencia núm. 188/2021 de 11 mayo	JUR 2021\185786	Criptomoneda	2021
AP Islas Baleares (Sección 2ª), sentencia núm. 378/2021 de 7 de octubre	JUR 2021\381016	Criptomoneda	2021
AP Pontevedra (Sección 5ª), sentencia núm. 352/2021 de 21 octubre	JUR 2022\27662	Criptomoneda	2021
Tribunal Superior de Justicia de País Vasco, (Sala de lo Civil y Penal, Sección1ª)	JUR 2021\252222	Bitcoin, Criptomoneda	2021
AP de Guadalajara (Sección 1ª) Auto núm. 33/2021 de 27 enero	JUR\2021\154453	Bitcoin	2021
TS (Sala de lo Penal, Sección 1ª) Auto de 29 junio 2021	JUR 2021\221511	Criptomoneda	2021
TS (Sala de lo Penal, Sección 1ª) Auto de 3 junio 2021	JUR 2021\198719	Criptomoneda	2021
TS (Sala de lo Penal, Sección1ª), auto de 28 septiembre 2021.	JUR 2021\326865	Criptomoneda	2021
AP de Málaga (Sección 3ª), sentencia núm.189/2021 de 12 de mayo	JUR 2021\335126	Bitcoin	2021
TSJ Islas Baleares (Sala de lo Civil y Penal, Sección 1ª), sentencia núm. 30/2021 de 5 octubre	JUR 2021\384193	Criptomoneda	2021
AP de Pontevedra (Sección 4ª) Auto núm. 120/2021 de 1 marzo	JUR\2021\169311	Bitcoin	2021
AP de Pontevedra (Sección 5ª) Auto núm. 276/2021 de 12 mayo	JUR\2021\293991	Bitcoin	2021
AP de Valencia (Sección 5ª) Auto núm. 230/2021 de 2 marzo	JUR\2021\152431	Bitcoin	2021
AP de Barcelona (Sección 5ª) Sentencia núm. 403/2020 de 22 de julio	JUR\2020\293115	Bitcoin	2020
AP de Cantabria (Sección 3ª) Sentencia núm. 235/2020 de 27 de mayo.	JUR\2020\334253	Bitcoin	2020
AP de Madrid (Sección 3ª) Sentencia núm. 388/2020 de 7 de octubre	JUR\ 2020\ 367249	Bitcoin	2020
AP de Tarragona (Sección 2ª) Auto núm. 108/2020 de 20 febrero	JUR\2020\136359	Bitcoin	2020
AP de Vizcaya (Sección 2a) Auto núm. 90189/2020 de 12 de mayo	JUR\2021\81509	Bitcoin	2020
AP de Vizcaya (Sección 2ª) Auto núm. 90453/2020 de 3 de diciembre	JUR\2021\73840	Bitcoin	2020
AP de Vizcaya (Sección 2ª) Auto núm. 90454/2020 de 3 de diciembre	JUR\2021\76878	Bitcoin	2020
JP de Zamora Sentencia núm. 122/2020 de 9 junio	JUR\2020\368548	Bitcoin	2020
AP de Barcelona (Sección 21ª) Auto núm. 1565/2020 de 19 de noviembre	JUR\2021\173486	Bitcoin, criptomoneda	2020
AP de Barcelona (Sección 5ª) Auto núm. 329/2020 de 30 junio	JUR 2020\232831	Criptomoneda	2020
AP de Barcelona (Sección 7ª) Auto núm. 728/2020 de 26 noviembre	JUR 2021\112825	Criptomoneda	2020
AP de León (Sección 3ª) Auto núm. 620/2020 de 10 julio	JUR 2020\253332	Criptomoneda	2020

AP de Murcia (Sección 5ª) Sentencia num.104/2020 de 14 julio	JUR\2020\264175	Bitcoin, criptomoneda	2020
AP de Valladolid (Sección 4ª) Sentencia núm. 100/2020 de 3 junio	JUR 2020\204806	Criptomoneda	2020
AP de Zaragoza (Sección 6ª) Auto núm. 569/2020 de 3 diciembre	JUR 2020\366005	Criptomoneda	2020
AP de Barcelona (Sección 7ª) Sentencia núm. 646/2019 de 18 octubre	JUR\2020\213591	Bitcoin	2019
AP de Madrid (Sección 29ª) Auto núm. 292/2019 de 11 abril	JUR\2019\185439	Bitcoin	2019
AP de Madrid (Sección 29ª) Auto núm. 482/2019 de 20 junio	JUR\2019\310539	Bitcoin	2019
AP de Madrid (Sección 29ª) Auto núm. 704/2019 de 10 octubre	JUR\2019\326886	Bitcoin	2019
AP de Zaragoza (Sección 3ª) Sentencia núm. 84/2019 de 21 febrero	JUR\2019\338758	Bitcoin	2019
JP de Cartagena (Provincia de Murcia), núm. 1, sentencia núm. 150/2019 de 23 de mayo	JUR\2021\4698	Bitcoin	2019
JP de Logroño (Provincia de La Rioja) Sentencia núm. 44/2019 de 13 febrero	JUR\2020\361813	Bitcoin	2019
TS (Sala de lo Penal, Sección 1ª) Sentencia núm. 326/2019 de 20 junio	RJ\2019\2925	Bitcoin, Blockchain	2019
AP de Málaga (Sección 2ª) Sentencia núm. 373/2019 de 25 octubre	JUR 2020\118664	Criptomoneda	2019
AP de Navarra (Sección 1ª) Sentencia núm. 241/2019 de 22 octubre	JUR 2020\15005	Criptomoneda	2019
AP de Navarra (Sección 1ª) Sentencia núm. 267/2019 de 10 diciembre	JUR 2020\49196	Criptomoneda	2019
AP de Zaragoza (Sección 3ª) Sentencia núm. 291/2018 de 9 julio	JUR 2018\265629	Criptomoneda	2019
TS (Sala de lo Penal, Sección 1ª) Auto de 24 octubre 2019	JUR 2019\299203	Criptomoneda	2019
TS (Sala de lo Penal, Sección 1ª) Auto de 24 octubre 2019	JUR 2019\298172	Bitcoin, criptomoneda	2019
AP de Ávila (Sección 1ª) Auto núm. 150/2018 de 15 junio	JUR\2018\231870	Bitcoin	2018
AP de Cantabria (Sección 1ª) Auto núm. 520/2018 de 11 diciembre	JUR\2019\290704	Bitcoin	2018
AP de Madrid (Sección 3ª) Sentencia núm. 185/2018 de 7 marzo	JUR\2018\133414	Bitcoin	2018
AP de Pontevedra (Sección 5ª) Auto núm. 142/2018 de 20 marzo	JUR\2018\193971	Bitcoin	2018
AP de Pontevedra (Sección 5ª) Auto núm. 388/2018 de 23 julio	JUR\2018\295137	Bitcoin	2018
AP de Pontevedra (Sección 5ª) Auto núm. 527/2018 de 31 octubre	JUR\2019\3713	Bitcoin	2018
AP de Santa Cruz de Tenerife (Sección 2ª) Sentencia núm. 29/2018 de 29 enero	JUR\2018\204653	Bitcoin	2018
AP de Santa Cruz de Tenerife (Sección 2ª) Sentencia núm. 294/2018 de 3 octubre	JUR\2019\51117	Bitcoin	2018
TSJ de Islas Canarias, Las Palmas (Sala de lo Civil y Penal, Sección 1ª) Sentencia núm. 39/2018 de 28 septiembre	JUR\2018\312883	Bitcoin	2018
AN (Sala de lo Penal, Sección 4ª) Auto de 3 octubre 2017	JUR\2017\243297	Bitcoin	2017
AP de Castellón (Sección 2ª) Auto núm. 505/2017 de 10 noviembre	JUR\2018\42298	Bitcoin	2017
AP de Lleida (Sección 1ª) Sentencia núm. 308/2017 de 14 julio	ARP\2017\1322	Bitcoin	2017

AP de Pontevedra (Sección 5ª) Auto núm. 208/2017 de 23 marzo	JUR\2017\126220	Bitcoin	2017
AP de Pontevedra (Sección 5ª) Auto núm. 483/2017 de 30 junio	JUR\2017\226944	Bitcoin	2017
AP de Pontevedra (Sección 5ª) Auto núm. 515/2017 de 7 julio	JUR\2017\215738	Bitcoin	2017

Apéndice 2. *Libro de códigos de la investigación sobre discusiones de un foro en la DN.*

Nombre	Descripción	Archivos	Referencias
AVOID	Evitar la detección de la actividad criminal	143	469
AVOID_cashout	Formas de convertir las criptomonedas	19	40
AVOID_get	Formas de obtener criptomonedas de la mejor manera para que no se pueda detectar la actividad criminal	64	130
AVOID_LE	Discusiones sobre cómo evitar la detección en específico sobre las FCSE y otras autoridades.	46	86
AVOID_path	Rutas que seguir con criptomonedas para conseguir evitar la detección de la actividad criminal	42	72
AVOID_repair	Formas de reparar el daño cometido para su privacidad	10	10
AVOID_tech	Discusiones sobre las tecnologías que tienen como propósito facilitar el anonimato y la privacidad usando criptomonedas (p.ej. mixers)	31	61
AVOID_typeC	Discusiones sobre cuál es la mejor criptomoneda para evitar la detección.	46	70
ALT_CRYPTOS	Utilización de criptomonedas alternativas	15	28
GENERAL	Discusiones sobre criptomonedas en general	24	30
LESSON ó EXPLAIN	Explicaciones o recomendaciones sobre criptomonedas	16	25
LESSON_crypto	Discusiones en las que los usuarios ofrecen consejos y recomendaciones sobre diversos temas relacionados con las criptomonedas.	3	4
LESSON_other	Otro tipo de lecciones	9	15
LESSON_privacy	Discusiones en las que los usuarios ofrecen consejos, recomendaciones y resuelven dudas a otros usuarios sobre cuestiones relacionadas con la privacidad y el anonimato. Tienen como objetivo evitar que asuman riesgos.	5	6
OTHER	Se incluyen otros temas más amplios relativos a quejas y reflexiones	31	46
OTHER_cases	Discusiones sobre casos conocidos e importantes para la comunidad	6	9
OTHER_complain	Discusiones en las que los usuarios se quejan sobre algún tema relacionado con el ámbito de las criptomonedas.	10	12
OTHER_reflection	Discusiones en las que los usuarios reflexionan sobre algún tema relacionado con las criptomonedas.	15	25
REGULATION	Discusiones sobre regulación de las criptomonedas	8	22
USE	Utilización de las criptomonedas para cometer delitos	93	129
USE_CaaS	Utilización de las criptomonedas en el desarrollo o comisión de delitos como un servicio que se ha contratado (puede que pagando con cripto).	21	25

USE_crime	Utilización de las criptomonedas para cometer un delito en particular	36	45
USE_market	Utilización de criptomonedas en un criptomercado en particular	38	59
VICTIM	Evitar convertirse en víctima de un delito	5	7
VICTIM_blackmail	Víctima de *blackmail*	1	1
VICTIM_phishing	Víctima de *phishing*	3	4
VICTIM_scam	Víctima de estafa	1	2

Apéndice 3. *Códigos y sus definiciones para la investigación.*

Aceptan criptomonedas (ACC)	
Definición	*Código*
Las aceptan porque muchos clientes se lo han pedido o porque esperan que sean utilizadas por muchas personas.	ACC_cust
Las aceptan porque consideran que será una buena opción para mejorar y expandir el negocio.	ACC_buss
Hablan sobre las razones por las que creen que otros negocios no las aceptan	ACC_otmrkt
Razones por las que aceptan un tipo de criptomoneda	ACC_cryptype
No recomiendan la utilización de bitcoin aún incluso cuando lo aceptan	ACC_rec*
Explican las ventajas y los inconvenientes de utilizar criptomonedas	ACC_crypto
Respuestas no colaborativas	ACC_noncol

No aceptan criptomonedas (DACC)	
Definición	*Código*
No las aceptan debido a inconvenientes del mercado	DACC_mrkt
No las aceptan porque no es una buena opción para el negocio	DACC_buss
No las aceptan debido a algunas características de las criptomonedas	DACC_crypto
No las aceptan, pero las ofrecen como forma de pago si se insiste en utilizarlas	DACC_insist
No las aceptan, pero ofrecerán la opción en el futuro	DACC_future
No las aceptan y no ofrecerán estas como opción de pago en el futuro	DACC_nofuture
Ofrecen información sobre los métodos de pago que tienen disponibles para convencer a los usuarios de que los usen en lugar de las criptomonedas.	DACC_conv
No aportan información sobre la pregunta que se les ha realizado	DACC_noinfo**
Respuestas no colaborativas	DACC_noncol

Apéndice 4. *Listado de tiendas online de cannabis que constituyen la muestra.*

Esta información ha sido eliminada por cuestiones de privacidad y seguridad. Se podrá acceder a estos datos por medio de una solicitud ante el órgano competente de la Universidad de Granada.

Apéndice 5. *Ejemplos de conversaciones que se han mantenido con los mercados de cannabis online de Canadá.*

Esta información ha sido eliminada por cuestiones de privacidad y seguridad. Se podrá acceder a estos datos por medio de una solicitud ante el órgano competente de la Universidad de Granada.