FACULTAD DE TURISMO Y FINANZAS

GRADO EN FINANZAS Y CONTABILIDAD

CRIPTOMONEDAS, ICOs Y STABLECOINS, LA PROBLEMÁTICA DEL USO ILÍCITO

Trabajo de Fin de Grado presentado por Ignacio de Larriva Álvarez, tutorizado por Félix Jiménez Naharro.

Alumno: Vº. Bº. del Tutor:

Fdo.: Ignacio de Larriva Álvarez Fdo.: Félix Jiménez Naharro

Sevilla, mayo de 2021

FACULTAD DE TURISMO Y FINANZAS

GRADO EN FINANZAS Y CONTABILIDAD

TRABAJO DE FIN DE GRADO

CURSO ACADÉMICO 2020-2021

TÍTULO
Criptomonedas y stablecoins, la problemática del fraude fiscal

AUTOR
Ignacio de Larriva Álvarez

TUTOR
Félix Jiménez Naharro

DEPARTAMENTO
Economía Financiera y Dirección de Operaciones

ÁREA DE CONOCIMIENTO
Economía Financiera

RESUMEN
El uso de las criptomonedas está cada vez más extendido en un ámbito internacional; promovidas originalmente por el mercado negro, actualmente su versatilidad es empleada por gobiernos, bancos, grandes empresas y particulares por igual. Dada su accesibilidad, privacidad, rapidez y anonimato, presentan una gran oportunidad para las economías sumergidas, el lavado de dinero y el fraude fiscal, a una escala e inmediatez nunca antes vistas. Las criptomonedas proporcionan seguridad, transparencia y privacidad para los usuarios, pero son un rompecabezas para el rastreo y seguimiento del dinero, lo que supone un cambio necesario en la política impositiva tradicional de los países. En este Trabajo de Fin de Grado analizaremos en profundidad el surgimiento, uso actual, variaciones, posibles riesgos y la relación con los usos ilegales de las criptomonedas en su conjunto, con especial mención al Bitcoin. Como conclusión, usaremos estos parámetros estudiados para determinar si realmente representan un riesgo para los países y Bancos Centrales y su viabilidad como activo alternativo al dinero fiat.

PALABRAS CLAVE
Criptomoneda, blockchain, Bitcoin, stablecoin, ICOs, especulación, evasión, impuesto, lavado de dinero, rastreo de dinero, fraude fiscal.

ÍNDICE

INTRODUCCIÓN

En este Trabajo de Fin de Grado estudiaremos el origen y funcionamiento de las criptomonedas, con especial mención a la moderna derivación de las mismas, llamadas stablecoins. Además, se perfilará y documentará la situación actual de las características inherentes que poseen este tipo de activos que facilitan su uso como herramientas para el fraude fiscal.

A pesar de que las criptomonedas, y en especial, el blockchain, son temas complejos y extensos, se expondrán únicamente los puntos principales y suficientes para el entendimiento del funcionamiento, funcionalidad, e integración actual de estas monedas en la sociedad, así como de los posibles riesgos que sufren los bancos centrales y la dificultad de regulación y seguimiento.

La primera criptomoneda que empezó a ser operada fue el Bitcoin en 2009, tras la época de la Gran Recesión, por lo que abundaban las opiniones desfavorables en cuanto a bancos, gobiernos, transparencia y seguridad, lo que hizo que esta moneda ganara rápidamente usuarios asiduos que querían mantener su dinero a salvo de las instituciones financieras, dado el nivel extremo de desconfianza. Su rápida expansión provocó que su tecnología comenzara a usarse extensamente en redes de cibercrimen y en organizaciones y foros del mercado negro.

Las stablecoins son una derivación de las criptomonedas que poco a poco es más popular, y presentan un riesgo real para el orden monetario internacional, ya que reducen uno de los mayores problemas que presentan las criptomonedas a la hora de conservar su valor: la volatilidad extrema en el precio.

La gran volatilidad en el precio de las criptomonedas ha hecho que, en principio, éstas sean descartadas como activos que mantienen el valor y como posible alternativa al dinero tradicional, puesto que, la fiebre existente es tal, que un rumor puede hacer caer o subir estos valores un 50% o más en tan solo unos días, lo que supone pérdidas y ganancias multimillonarias, en un entorno que a simple vista parece carecer de control y estabilidad, presa de la pura especulación.

En la actualidad, es extremadamente común leer diariamente noticias relacionadas con estos nuevos métodos de pago y transferencia, por lo que es de gran importancia entender que podrían suponer un cambio global en cuanto al nivel de control de la política monetaria, y dar lugar a enfrentamientos entre grandes empresas y países. Es por esto que los objetivos de este trabajo son: determinar si es factible el reemplazo del dinero fiat por las stablecoins, y, hasta qué punto las criptomonedas y sus derivaciones son usadas con fines ilegales, ya sea para lavado de dinero o evasión de impuestos, entre otros.

CAPÍTULO 1: JUSTIFICACIÓN, OBJETIVO, METODOLOGÍA, Y ESTRUCTURA

La integridad de este Trabajo de Fin de Grado está justificada y respaldada por los artículos, revistas, bases de datos, y otras fuentes citadas en el texto, referenciadas en la bibliografía.

El objetivo principal hacia el que está enfocado este trabajo, es la conclusión de si las criptomonedas son activos que desplazarán al dinero fiat en cuanto a uso, extensión y seguridad, o son una herramienta destinada a ser usada de forma especulativa o ilegal. Para lograr este objetivo, se plantearán otros más concretos: definición de las criptomonedas en general y el Bitcoin en particular, el blockchain, la situación actual del mercado y regulaciones, la moderna variación de estas monedas, apodadas stablecoins, y la presentación de las posibles afecciones ilegales que son inherentes a este tipo de activos y que presentan riesgos y dificultades a la hora de gestionar su regulación.

La metodología utilizada para la realización de este Trabajo de Fin de Grado será a partir del empleo de datos publicados en páginas web como Investing.com, Blockchain.com y TradingView.com, entre otras, así como el uso continuo de artículos académicos, libros, y trabajos que estén relacionados con las criptomonedas, su funcionamiento y las posibles implicaciones legales en cuanto a la regulación y otros aspectos de importancia. En este trabajo se expondrán gráficos y datos de fabricación propia en la plataforma Google Sheets, otros provenientes de Statista.com, o con origen en Google Analytics, complementando la información y proporcionando herramientas para la correcta comprensión de las afirmaciones y cuestiones planteadas. Las referencias aquí expuestas y orígenes de datos utilizados serán referenciados en la bibliografía en formato APA (7.ª edición).

Para realizar de una forma estructurada la ordenación de este Trabajo de Fin de Grado, el estudio se ha dividido en tres capítulos, conclusión, y bibliografía.

Después de este primer capítulo de Metodología y Estructura, el segundo se centra en la exposición del funcionamiento de las criptomonedas, el blockchain, y su posible validez como alternativa al dinero fiat. Para ello, este capítulo se ha dividido en cuatro apartados: Situación de Mercado, Funcionamiento, Tercera generación, y Alternativa al Dinero Fiat. Este capítulo será indispensable para entender con profundidad las implicaciones que conlleva esta nueva tecnología en lo referente a la fiscalidad.

En el tercer capítulo se exploran las criptomonedas aplicadas a usos ilegales, a través de tres apartados: Facilidades Para el Uso Ilícito, Control Sobre las Criptomonedas, y Estimaciones del Fraude Fiscal.

Como último apartado se encuentra la Conclusión, donde se valorará si las criptomonedas representan un riesgo para los gobiernos, los bancos centrales, y el control del orden monetario internacional.

CAPÍTULO 2: CRIPTOMONEDAS

Las criptomonedas son monedas virtuales que actúan como medio para facilitar las transacciones digitales. Estas operaciones están aseguradas mediante encriptación (la técnica más utilizada es el hash). A diferencia de las monedas fiduciarias, las criptodivisas suelen estar descentralizadas, y no cuentan con el respaldo de una autoridad central o un gobierno, haciendo uso de la tecnología blockchain para su funcionamiento, que permite las transacciones entre pares, eliminando así la necesidad de una cámara de compensación central. Al estar descentralizada, una copia de las transacciones estará disponible para todos los usuarios y participantes de la red.

Actualmente hay más de 5200 criptodivisas en circulación, algunas de las criptodivisas más comunes son Bitcoin, Ethereum, Ripple, Litecoin e IOTA. Bitcoin fue la primera criptodivisa y sigue siendo líder en términos de popularidad, uso y capitalización de mercado. La mayoría de las criptodivisas se crean mediante un proceso llamado minería, donde un “minero” recoge las transacciones de criptodivisas pendientes, verifica su legitimidad, y las reúne en bloques que forman parte de una cadena de bloques (blockchain). Una vez que un bloque se escribe con éxito en la cadena, el minero es recompensado con una criptomoneda recién emitida, a modo de comisión por el servicio.

Las monedas digitales ofrecen muchas ventajas potenciales, entre ellas una mayor velocidad y un menor coste a la hora de realizar pagos y transferencias, sobre todo a nivel transfronterizo. Más allá de los sistemas de pago, es probable que la tecnología blockchain afecte y altere sectores que van desde los servicios financieros, la manufactura, la sanidad y los servicios públicos, entre otros.

Al mismo tiempo, las criptomonedas plantean riesgos considerables como instrumentos potencialmente utilizados para el blanqueo de capitales, la financiación del terrorismo, la evasión fiscal y el fraude. Los organismos reguladores de todo el mundo tratan de establecer un marco legal para su uso y disfrute.

Las medidas de emergencia anunciadas por la Reserva Federal de EE.UU. (recorte de los tipos de interés a cero), y las compras ilimitadas de activos, han impulsado cierto optimismo hacia las criptodivisas.

Las criptomonedas son difíciles de regular debido a su estructura descentralizada y a sus operaciones a escala mundial, lo que convierte su mejor virtud en su mayor riesgo. Muchas son opacas y operan fuera del sistema financiero convencional, lo que dificulta el control de sus movimientos. Las medidas reguladoras efectivas para las criptodivisas están todavía en una fase inicial en la mayoría de los países. En Estados Unidos, los legisladores no ven con buenos ojos la idea de que las grandes empresas tecnológicas introduzcan su propia moneda, ya que les podría proporcionar un poder mayor que el del propio Estado, y ya se ha presentado un proyecto de ley que pide que se prohíba a las grandes empresas

tecnológicas actuar como instituciones financieras o lanzar su propia criptodivisa, en el mismo momento en el que Facebook intenta emitir su propia moneda.

2.1 SITUACIÓN DE MERCADO

La capitalización de mercado de todas las criptomonedas juntas ascendía a 1,61 billones de dólares en mayo de 2021. Bitcoin es la mayor criptodivisa por capitalización de mercado, con un 42,69% del mercado total. Le siguen Ethereum, Theter y Cardano. Hay más de 5200 criptodivisas en circulación actualmente (CoinMarketCap, 2021).

Ya que el Bitcoin acapara cerca del 50% del mercado de criptomonedas, nos centraremos en el mismo para estudiar detenidamente la variación histórica de precios. Desglosaremos la variación en cuatro grandes movimientos:

1. -83,82% entre el 11 de diciembre de 2017 y el 10 de diciembre de 2018 (371 días).
2. +346,31% entre el 17 de diciembre de 2018 y el 24 de junio de 2019 (189 días).
3. -72,25% entre el 24 de junio de 2019 y el 24 de marzo de 2020 (259 días).
4. +1.585,59% entre el 9 de marzo de 2020 y el 12 de abril de 2021 (339 días).

Gráfico 1. Evolución BTC/USD

Fuente: elaboración propia a partir de los datos de investing.com

La inestable variación que realiza el Bitcoin y, por extensión, del mercado global de criptomonedas, se ha convertido en un atrayente del inversor inexperto, que trata de ganar grandes sumas de dinero de forma rápida y fácil, lo que supone una desvinculación total de

la idea que originó este tipo de activos: la sustitución del dinero fiat. Para conseguir este objetivo, deberían de cumplir uno de los requisitos básicos; el mantenimiento del valor en el tiempo. Esta variabilidad tan agresiva mostrada por las criptomonedas los últimos años, crean al inversor o al poseedor de estos medios de pago una gran incertidumbre, por lo que podríamos suponer que, a simple vista, las monedas virtuales no son más que activos muy arriesgados a los cuales es difícil atribuir un valor concreto.

2.1.2 ICOs

Las Initial Coin Offerings (ICOs) o ventas de tokens, son *smart contracts* basados en la tecnología del blockchain, diseñados para obtener financiación externa mediante la emisión de monedas o tokens. Los *smart contracts* son protocolos informáticos que automatizan las transacciones de intercambio de valor entre el emprendedor y los inversores, creando potencialmente una perfecta desintermediación. Desde la perspectiva de un emprendedor, las ICOs son atractivas ya que ofrecen financiación en todas las etapas de la empresa con un alcance global, con unos costes de transacción cercanos a cero. Desde el punto de vista del inversor, las ICOs ofrecen potencialmente una gran liquidez, en el caso de que se trate de tokens líquidos, donde podrían deshacerse de su posición de forma rápida. Sin embargo, existe una distinción entre tokens de utilidad, de seguridad y de criptomoneda (Momtaz, 2019, 7). Mientras que los dos últimos tipos de tokens se rigen por las leyes de valores o activos, los tokens de utilidad operan en una zona gris de terminología legal dudosa. Los tokens de utilidad ofrecen la promesa de que el token puede ser canjeado por los productos o servicios del proyecto de la ICO una vez que se hayan desarrollado, tomando la idea del Crowdfunding. La diferencia principal es, que los inversores en tokens de utilidad no tienen actualmente derechos en muchas jurisdicciones, lo que convierte este tipo de tokens en una posible estafa.

2.1.2.1 CÓMO FUNCIONAN LAS ICOs

En primer lugar, un grupo de reputados programadores o expertos de la comunidad, comienzan a trabajar en una idea de forma conjunta. Antes de la venta de tokens, suelen publicarse prototipos de la plataforma o versiones alfa y un sitio web oficial que presenta el proyecto, incluyendo calendarios y detalles técnicos.

A continuación, los programadores anunciarán el proyecto en línea y publicarán toda la información relacionada. Las plataformas usadas suelen incluir foros como Reddit, Bitcointalk y los sitios web oficiales. Algunos proyectos tienen un sitio web o una sección de ICO que se utiliza específicamente para dar a conocer los tokens y los eventos relacionados con la ICO de la empresa. Independientemente de las formas, el sitio web indicará el calendario de la ICO, incluyendo el número, las fechas y la duración de las fases, el precio y la oferta de los tokens, y la cantidad de fondos que se recaudarán. Habrá medios sociales y grupos de chat oficiales y no oficiales en WeChat, Telegram, Facebook, Slack y WhatsApp,

entre otros, para mantener informados a los inversores y permitir que los interesados interactúen entre sí. Se realizan regularmente sesiones AMA (Ask Me Anything) y se publican actualizaciones en vídeo en YouTube y Tencent Media para informar a los inversores del progreso de las ICO y del software. Debido al entorno no regulado, los estafadores participan activamente en estos entornos para robar tokens e información sensible a los inversores que forman parte de estos foros.

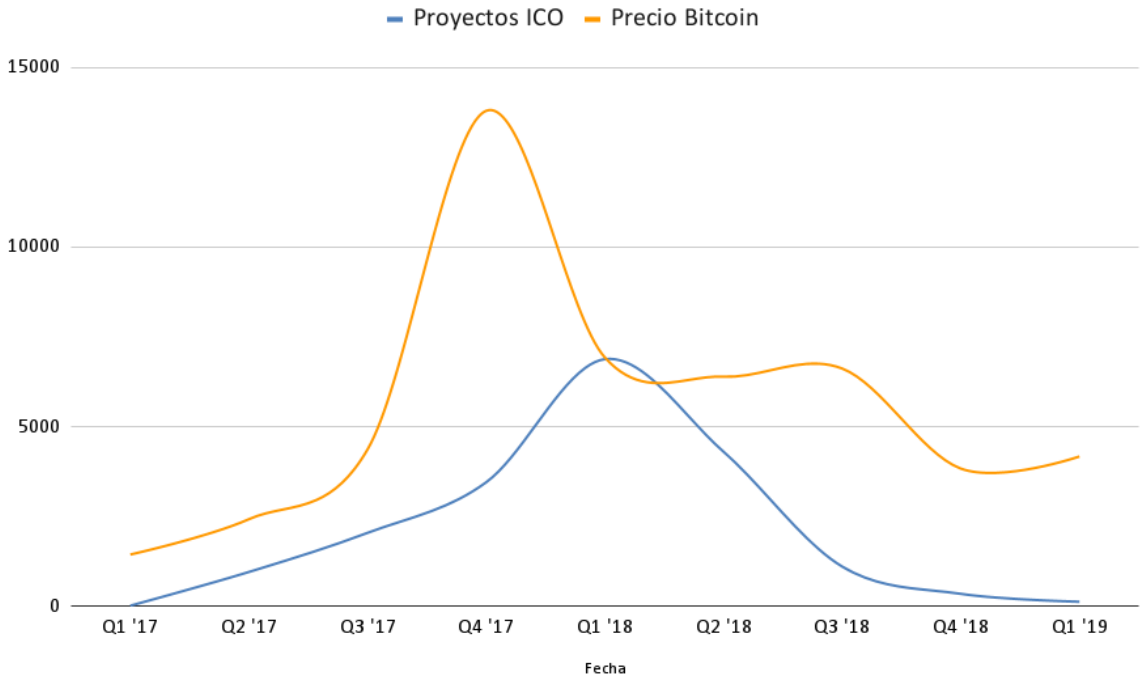
Antes del lanzamiento de la ICO, se proporcionará información a los inversores en el sitio web o a través de artículos en línea que detallen cómo y dónde comprar los tokens. El registro en las bolsas de criptomonedas o en un sitio web permitirá a la empresa obtener una lista blanca (whitelist), formada por todos los inversores que hayan cumplido con sus procesos de conocimiento del cliente. Los inversores tendrían que comprar las criptomonedas designadas para poder canjearlas por los nuevos tokens cuando comience la ICO. Después de acreditar sus carteras electrónicas con las criptodivisas aceptadas para la ICO, normalmente Bitcoin o Ethereum, los inversores están listos para participar en la ICO enviando las monedas a sus direcciones. Por ejemplo; el creador de la ICO solicita a los inversores que envíen Bitcoin, Ethereum o Litecoin a la dirección de su monedero de criptomonedas, tras lo que hará entrega de los tokens a aquellas personas que hayan cumplido el acuerdo. En la mayoría de los proyectos, los inversores recibirán los tokens una vez finalizada la ICO y los almacenarán en sus respectivos monederos. Inmediatamente después del lanzamiento oficial del proyecto, es probable que el nuevo token pueda negociarse en aquellas bolsas que acepten la cotización de tokens. En el caso de que alguno de los inversores quiera intercambiar los tokens a dinero fiduciario, deberá primero realizar el cambio a una criptomoneda como Bitcoin, tras lo que realizará el cambio a la moneda que requiera. Para intercambiar los nuevos tokens por dinero en efectivo, es necesario realizar un proceso inverso.

2.1.2.1 SITUACIÓN ACTUAL

Las ICOs son un gran avance tecnológico que nos acerca aún más a un mundo más globalizado, en el cual las comisiones y los intermediarios desaparecen para lograr un mercado más eficiente. Si bien la idea es sumamente novedosa y ofrece una gran expectación, al realizar un estudio más exhaustivo sobre las ICOs, podemos ver que, por ahora, se encuentran en una fase parecida a la de las criptomonedas, puesto que los números y datos que reflejan parecen indicar que su compra, venta, y movilización están atados a las propias criptomonedas, lo que hace que se difumina aún más la línea que separa la tecnología blockchain y las monedas en sí.

En el siguiente gráfico se puede ver la comparación entre la cantidad de dinero invertido a nivel global en ICOs y el precio del Bitcoin, que usaremos como referencia de la variación del mercado total de criptomonedas, dada su gran importancia y peso dentro del mismo.

Gráfico 2. Relación entre la financiación de ICOs y el precio del Bitcoin



Fuente: elaboración propia a partir de los datos de CB Insights e Investing.com

Podemos apreciar que, a mayor subida del precio de las criptomonedas, mayor financiación reciben los proyectos de ICOs, de los cuales, la mayoría, únicamente ofrecen un *paper* escueto, en el que no se detallan datos, previsiones, o funcionamiento empresarial, y son víctimas de la pura especulación. Este gráfico demuestra que la inversión en ICOs es originada por la popularidad de la tecnología blockchain y sus aplicaciones, no por ser un tipo de financiación novedoso que conlleva muchas ventajas tanto para el inversor como para el empresario, siendo un caso similar al de las monedas virtuales.

2.1.2.2 ESTADO DE LA REGULACIÓN DE LAS ICOs

Hay algunos factores que contribuyen a la dificultad de regular las ICOs, como que sigue siendo polémico el hecho de si la emisión de los tokens digitales equivale a la creación de un nuevo valor y, por lo tanto, debe someterse a la supervisión y regulación del gobierno o de las bolsas (Skinner, 2017). De hecho, los tokens digitales comparten instrumentos comunes con todas las monedas digitales, los valores, y los activos, ya que pueden utilizarse para intercambiar ciertos bienes o servicios como las monedas, se consideran métodos de inversión puros como los valores, y pueden realizar algunas funciones especiales como los activos. Por ejemplo, las criptodivisas son activos y no instrumentos de financiación o pago según los reguladores de Suiza y Singapur, pero todavía no se exige a las criptodivisas que obtengan una aprobación o licencia, ni se regulan las transacciones.

Otro de los aspectos que hace que las líneas jurisdiccionales sean indistintas, es la naturaleza pública y distribuida del blockchain, que involucra a los desarrolladores o nodos de todo el mundo bajo diferentes jurisdicciones en la red, aunque el proyecto en sí esté ubicado en una determinada geografía.

Por estos motivos, se están comenzando a crear nuevas entidades que dediquen sus esfuerzos al entendimiento, regulación, y promulgación de esta nueva tecnología llamada blockchain, lo que hará que se incluya por definición a las ICOs. Los proyectos más avanzados son los de Suiza y Singapur.

2.2 FUNCIONAMIENTO DE LAS CRIPTOMONEDAS

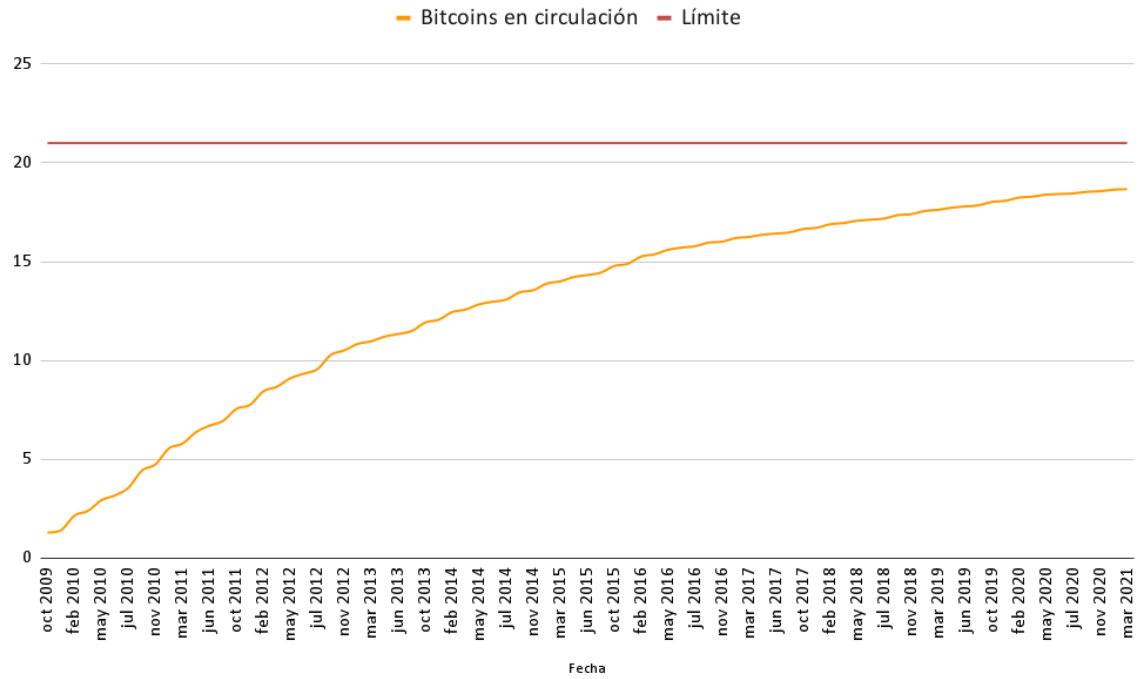
Las criptomonedas ofrecen una forma segura y eficiente de transferir activos digitales a través de una red de blockchain, donde las transacciones se aseguran mediante criptografía o una técnica de encriptación denominada función hash, y todas las transacciones se registran en un libro de registros distribuido públicamente conocido como blockchain.

Cuando se produce una nueva transacción, se transmite a través de la red a los usuarios (conocidos como mineros) para que verifiquen la legitimidad de la transacción. Los mineros compiten entre sí para resolver un problema criptográfico (hash), que es necesario para escribir la nueva transacción en la cadena de bloques. Un bloque está formado por todas las transacciones que se producen durante un determinado periodo de tiempo. Cuando se realiza una transacción nueva, se verifica, se escribe dentro de su bloque correspondiente, y este a su vez pasa a formar parte de una cadena de bloques más grande (blockchain).

Los mineros que tienen éxito resolviendo la función hash, son recompensados con criptodivisas recién emitidas. Así, el proceso de minería controla la creación de nuevas monedas, a través de la utilización de un hardware muy potente.

En el mayor de los casos, las criptomonedas son productos con un número limitado de unidades, por lo que una vez sea emitida esta última moneda, no podrá emitirse más. Por ejemplo, el número máximo de Bitcoin es de 21 millones.

Gráfico 3. Número de Bitcoins en circulación

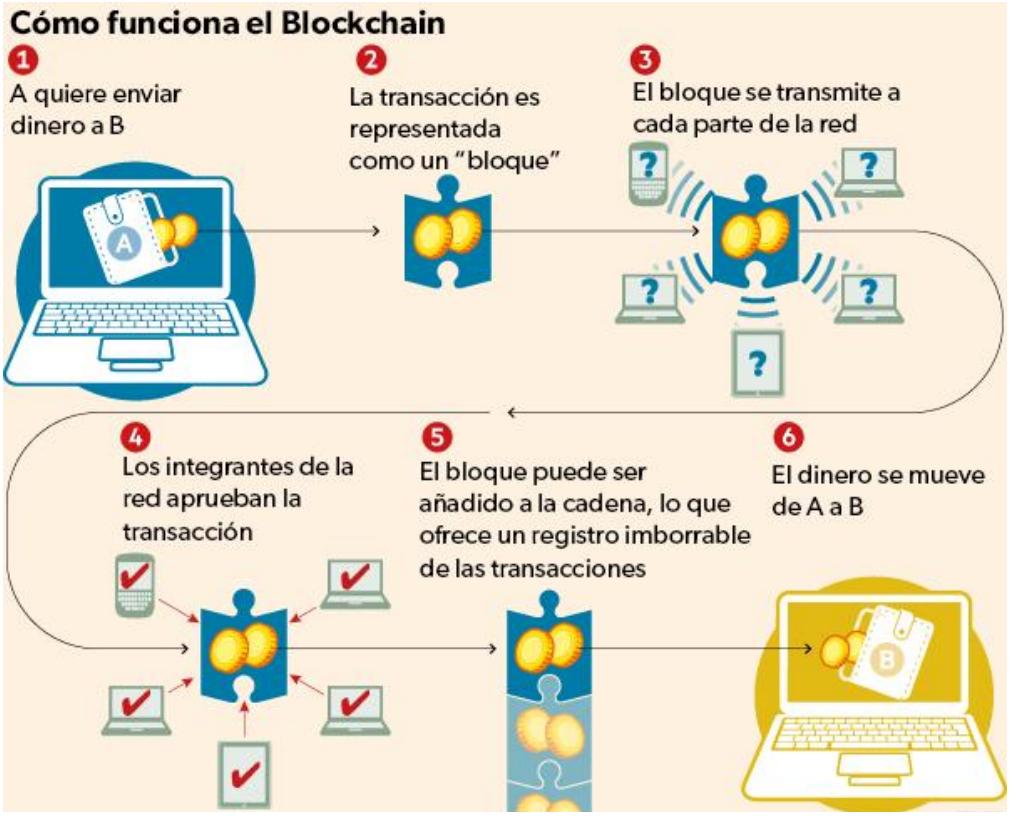


Fuente: elaboración propia a partir de los datos de Blockchain.com

2.2.1 BLOCKCHAIN

Blockchain, como se ha mencionado anteriormente en diversas ocasiones, es la tecnología principal que está detrás de la mayoría de las criptomonedas, ICOs, y stablecoins, en particular el Bitcoin. Se trata de un libro de registros descentralizado compuesto por una serie de bloques que contiene los historiales de todas las transacciones que han tenido lugar en una red determinada. La cadena de bloques crece a medida que se añaden nuevos bloques.

Gráfico 4. Funcionamiento del Blockchain



Fuente: World Economic Forum

Cada bloque que se añade a la cadena de bloques tiene su propia identidad cifrada (hash) y es visible para cada usuario de la red. La función hash es única para cada bloque, y empezará siempre por cuatro ceros. El hecho de que se intente manipular el valor de uno de los bloques, hasta el cambio más ínfimo cambiaría totalmente el hash resultante de la encriptación de los datos, por lo que dejaría de empezar por 0000, y ésta variación sería claramente visible, además de que, para conseguir la función hash de un bloque, se debe usar el hash del bloque anterior, por lo que si un bloque cambia, cambiará todo el resto de la cadena de bloques, y será evidente que un dato ha sido variado. La búsqueda de una función hash que empiece por cuatro ceros a partir de unos datos determinados que contienen la información de la transacción es el acto de minar. Sin embargo, se podría realizar un cambio en un bloque, y volver a minar de nuevo ese bloque y los siguientes, para obtener funciones hash que comiencen por cuatro ceros para todos los bloques con los nuevos datos. Para solucionar este problema, existen copias exactas de cada blockchain, por lo que, si una de estas variaciones es distinta, se realiza una comparación de todas ellas, para lo que se realiza una especie de concurso, y se eliminan y sustituyen las que tengan menor probabilidad de ser correctas.

Gráfico 5. Cifrado SHA 256 usado para obtener las funciones hash

Fuente: academy.bit2me.com

La naturaleza descentralizada del blockchain elimina la necesidad de autoridades centrales como bancos, cámaras de compensación, u otros intermediarios. Ofrece mayor eficiencia, más seguridad y un mayor nivel de confianza para todos los integrantes de la red y partícipes de su uso. Además de ser la tecnología central detrás de las criptomonedas, tiene grandes aplicaciones potenciales en muchas otras áreas: Cisco espera que el mercado de la cadena de bloques (en términos de ingresos) alcance los 10.000 millones de dólares en 2021 y estima que la cadena de bloques tiene el potencial de representar hasta el 10% del PIB mundial (Incisive Business Media, 2019).

2.2.1.1 CASOS DE APLICACIÓN DEL BLOCKCHAIN

Louis Vuitton y Dior planean lanzar la tecnología blockchain basada en Ethereum para la moda de lujo llamada Aurora. La cadena de bloques le permitirá al cliente hacer un seguimiento de la mercancía y verificar la autenticidad de los productos (Simms, 2019).

El Gobierno de Corea del Sur está estudiando planes para dedicar un fondo de 400 millones de dólares a la investigación y el desarrollo de la cadena de bloques. Este fondo se utilizará probablemente en los próximos años hasta 2025.

Singapur está siguiendo un camino similar al de Corea del Sur, ya que el país se ha asociado con el Centro de Innovación de Blockchain de IBM para cultivar el talento local y fomentar la innovación e investigación de esta nueva plataforma. La plataforma permitirá pagos transfronterizos más rápidos y con menores comisiones en múltiples monedas, el cambio de divisas, y la liquidación de valores denominados en moneda.

Dubai planea utilizar la tecnología blockchain para verificar las sentencias judiciales transfronterizas. Esta iniciativa podría dar lugar a la creación de un sistema judicial basado en el blockchain, que sería el primero del mundo.

El Gobierno Metropolitano de Seúl ha puesto en marcha el Equipo de Gobernanza de Blockchain de Seúl para explorar los beneficios de blockchain en los servicios administrativos, entre los que se plantea la posibilidad de realizar un sistema de votación en línea.

2.3 TERCERA GENERACIÓN

Las generaciones de la tecnología blockchain se dividen en tres, y cada una de ellas está representada por la moneda más importante: primera generación (Bitcoin), segunda generación (Ethereum) y tercera generación (Cardano), que es en la que nos encontramos actualmente, e impulsa aún más la popularidad y la facilidad de uso del blockchain y las criptomonedas.

Las plataformas de tercera generación están experimentando una gran atracción, ya que mejoran los problemas que afectan a las plataformas de segunda generación. Las plataformas de tercera generación pretenden abordar el problema de la escalabilidad y la congestión de la red asociados a Ethereum. La tercera generación de blockchain pretende sustituir a la segunda, ofreciendo un procesamiento de datos y tiempos de transacción más rápidos, y tarifas aún más baratas.

En cuanto a los servicios financieros, el blockchain puede suponer un enorme ahorro en costes de infraestructura, transacciones y administración. Según un informe del Banco Santander, para 2022 blockchain puede reducir los costes de infraestructura de los bancos atribuibles a la negociación de valores, los pagos transfronterizos y el cumplimiento de la normativa, en aproximadamente 20.000 millones de euros al año.

Además de simplificar los pagos fronterizos y ofrecer comisiones mínimas, la compraventa de acciones es otra área potencial que podría verse afectada por esta tecnología, ya que podría permitir una mayor precisión en las operaciones, y un proceso de liquidación más corto. NASDAQ y la Bolsa de Valores de Australia ya están explorando soluciones para reducir costes y mejorar la eficiencia de sus sistemas.

Relacionando el uso del blockchain con el transporte, tiene un inmenso potencial en el sector del transporte de mercancías al simplificar el proceso de pago, la gestión de la flota y aportar más eficiencia a la cadena de suministro. Una de las implicaciones más básicas es la creación de un sistema de pago racionalizado, en el que los contratos inteligentes escritos en la cadena de bloques pueden desencadenar la transferencia de fondos a un conductor de forma instantánea una vez que se ha completado una entrega. Esto aumenta la eficiencia no solo al omitir la documentación física, sino también al eliminar por completo la participación manual al automatizar la ejecución del contrato. Además, podría hacer que el mantenimiento de registros sea más fácil, seguro y transparente para las empresas de transporte. Las empresas podrán mantener registros de cada camión de su flota, con información detallada sobre el mantenimiento o los daños sufridos a lo largo de la vida del camión, lo que ayudaría a las empresas a comprar y vender vehículos de una forma más informada.

Aplicando esta tecnología a los bienes inmuebles, el blockchain ofrece un potencial significativo en la forma de agilizar la compra y venta de terrenos y edificios, ya que elimina el error humano y evita la pérdida de datos. Con una red de blockchain, se puede lograr que los datos de los bienes raíces sean fácilmente descubribles, comparables, y verificados, ayudando a eliminar la asimetría de la información, además de proporcionar una mayor

transparencia en torno a los títulos de propiedad, las transferencias de títulos y los precios de los activos.

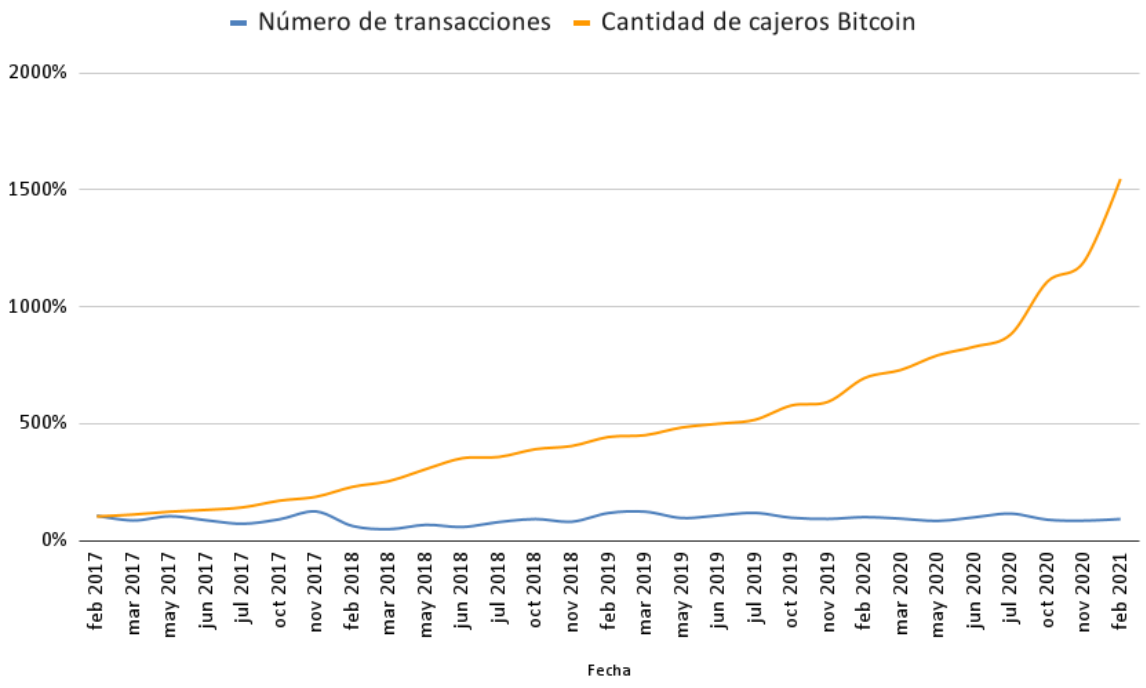
Estos cambios que se implantará a medio plazo en la economía, no tardarán en llegar al consumidor habitual, consiguiendo que todas estas ventajas sean usadas diariamente por cualquier persona en su día a día, desde hacer la compra hasta comprar una casa, gestión de alquileres e hipotecas, voto electoral electrónico, e incluso emisión de títulos universitarios o certificaciones académicas, entre otros.

2.4 ALTERNATIVA AL DINERO FIAT

Debido a las grandes fluctuaciones del precio de las criptomonedas, se hace imposible que cumpla la función de depósito de valor, indispensable para cualquier método de pago verdaderamente útil, ya que las fluctuaciones generan una gran inseguridad para los usuarios y además hacen imposible predecir el valor que tendrá su dinero en un futuro.

Existe mucha especulación en cuanto a si el Bitcoin sucederá, o no, al dinero fiat, y de las posibles implicaciones que tendrá este cambio. Observando los datos recogidos entre 2017 y 2021 y ajustándolos, obtendremos la variación de la cantidad de transacciones mensuales de Bitcoin, así como la variación de la cantidad de cajeros Bitcoin (Bitcoin ATM), y podemos llegar a varias conclusiones:

Gráfico 6. Relación entre el número de transacciones y la cantidad de Bitcoin ATMs



Fuente: elaboración propia a partir de los datos de coinatmradar.com

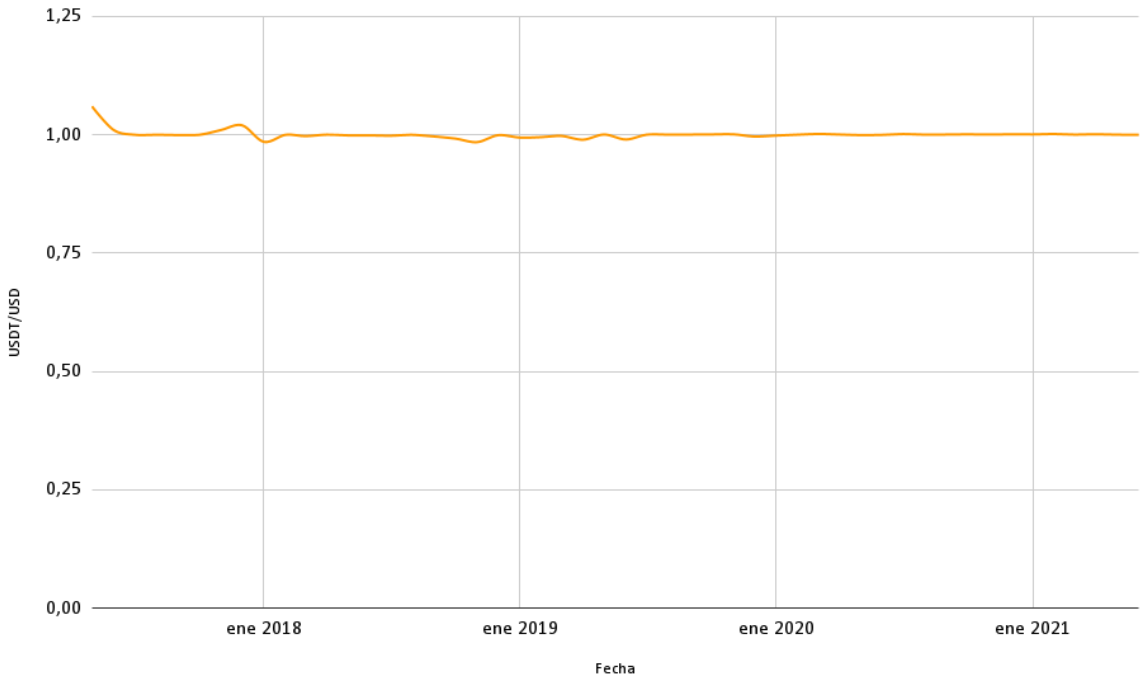
Se aprecia que se realizan un número constante de transacciones mensuales, pero debido a las fluctuaciones tan agresivas de estos activos, no podemos diferenciar entre su uso como método de pago y la especulación. Es por esto que se han comparado los datos con la cantidad de cajeros a nivel global, pudiéndose ver que, a pesar de haber un número exponencialmente creciente de cajeros, no aumenta la cantidad de transacciones, o ésta se mantiene constante. Podríamos concluir en que no se ha extendido su uso de forma masiva a nivel global, y, por ahora, no constituye una alternativa viable al dinero fiat, a pesar de las grandes ventajas que presenta. Esto puede ser debido a regulaciones de distintos países, o el desapego que existe por parte del público general, reticente a la hora de adquirir activos tan volátiles.

2.4.1 STABLECOINS

Las monedas estables o *stablecoins* intentan resolver el problema de la gran volatilidad de los precios denominados en dólares que caracteriza a la mayoría de las criptomonedas, vinculando su valor a cantidades fijas de instrumentos monetarios tradicionales.

Una stablecoin como Tether (también conocida como USDT) está respaldada 1:1 por el dólar estadounidense. Por cada unidad de USDT que está en circulación, los proveedores de servicios financieros apartan 1 dólar y lo mantienen en reserva.

Gráfico 7. Valor de Tether frente al dólar (USDT/USD)



Fuente: elaboración propia a partir de los datos de investing.com

El número de stablecoins que existen se ha disparado en los últimos años, así como su cantidad. También es posible encontrar criptoactivos vinculados a otras monedas fiduciarias, como el euro, e incluso otros criptoactivos o bolsa de ellos.

Algunos proyectos de stablecoins han vinculado sus activos digitales a metales preciosos o a otras criptodivisas. Proyectos como Libra (ahora Diem), de Facebook, pretenden que las stablecoins se utilicen como medio de intercambio, respaldadas por una cesta de diferentes monedas nacionales.

Tether Stablecoin (USDT)

Tether es emitida por una empresa con sede en Hong Kong, también llamada Tether. La empresa afirmó originalmente que cada USDT estaba respaldado por un dólar, pero desde entonces ha mencionado en varias ocasiones que realmente hay un sistema de reserva fraccionaria.

Ya que es muy popular, el uso de Tether está ampliamente extendido, a pesar de que la empresa Tether ha estado en el centro de varias demandas por supuesta manipulación del mercado de su propia moneda (Atkins, 2021).

Binance Stablecoin (BUSD)

Binance USD es una stablecoin respaldada por USD 1:1 y emitida por el principal bróker de criptomonedas Binance, en asociación con Paxos. El precio de la stablecoin es siempre de 1 dólar, y BUSD está regulada por el Departamento de Servicios Financieros del Estado de Nueva York.

Gemini Stablecoin (GUSD)

El Gemini dólar GUSD es la stablecoin emitida por Gemini, una bolsa de criptomonedas fundada por los gemelos Winklevoss. Está destinada a proporcionar tokens en la red Ethereum, con el estándar ERC-20, que ofrecen estabilidad de precios para los mercados de criptomonedas.

La fijación de precios 1:1 de la stablecoin Gemini es auditada mensualmente por una empresa de contabilidad pública registrada de forma independiente.

Coinbase Stablecoin (CUSD)

La stablecoin, cuyo precio es de 1 dólar, fue lanzada por Coinbase y la empresa de pagos Circle como parte del Centre Consortium.

USDC se lanzó en septiembre de 2018 con el objetivo de proporcionar un refugio seguro a los inversores en tiempos de volatilidad, así como permitir a las empresas aceptar pagos en criptodivisas gracias a la estabilidad de su precio.

Tanto Circle como Coinbase cumplen con la normativa, y una importante empresa de contabilidad verifica la vinculación 1:1 de USDC a USD.

2.4.1.1 DESVENTAJAS DE LAS STABLECOINS

Mientras que criptomonedas como el Bitcoin están totalmente descentralizadas, no puede decirse lo mismo de las stablecoins, ya que los activos subyacentes deben mantenerse en reservas. Uno de los grandes retos que presentan estas monedas, es garantizar que están debidamente garantizadas, proporcionando información y siendo sujetas a auditorías y agencias reguladoras continuamente.

Por último, está la complicada cuestión de la regulación, y el constante enfrentamiento entre los bancos centrales y las grandes empresas multinacionales que desean emitir su propia moneda, temiendo que este cripto activo pudiera acabar con la soberanía de las monedas fiduciarias e incluso desencadenar una crisis económica.

2.5 COMPRAVENTA DE CRIPTOMONEDAS

Para analizar la situación actual de compraventa desde la perspectiva de un inversor minorista o retail, se expondrán dos de las mayores redes de intercambio a nivel global: Coinbase y Binance.

Como en cualquier bróker o red de intercambio, el primer paso es la verificación de la identidad a través del envío de una fotografía o escaneo de un documento identificativo, tras lo que se realizará una verificación de la cuenta bancaria del usuario, así como un test de conocimientos, para cumplir con la normativa europea que trata de subsanar la pérdida incontrolada de capital sufrida por cada vez más habitantes de la región, debida a la poca comprensión y entendimiento que existe acerca de los mercados financieros y su terminología. Tras la fase de verificación, se ha de realizar un ingreso de dinero, generalmente a través de tarjeta, transferencia bancaria, o PayPal, lo que suele estar condicionado a una comisión de tasa fija o variable, que impone la empresa.

Una vez se realiza el ingreso, tendremos a nuestra disposición todos los activos que oferte la red de intercambio, y con un simple clic podremos entrar en largo (comprar) o en corto (vender), una cantidad de unidades o fracciones de ellas, pudiendo realizar una transacción con un número entero, o no, de cualquier criptomoneda.

2.5.1 COMISIONES

Las comisiones en las redes de intercambio de criptomonedas son elevadas, aún tratándose de servicios enfocados principalmente a inversores minoristas, quienes, sin leer detenidamente los términos y condiciones, encuentran sus beneficios consumidos por éstas.

Tabla 1. Comparación de las comisiones de Coinbase y Binance

Concepto	Coinbase	Binance
Compraventa (spread)	0,50%	0,02% - 0,1%
Compras con tarjeta	3,99%	3% - 4,5%
Transferencia bancaria	10€ ingreso, 25€ retirada	15€

Fuente: elaboración propia a partir de los datos de Coinbase.com y Binance.com

2.5.2 EJEMPLO PRÁCTICO

Poniéndonos en situación de un inversor minorista con 1.000€ que desea obtener rendimientos de la totalidad de su capital invirtiendo en criptomonedas a través de Coinbase, realizaremos una compra con tarjeta de crédito puesto que la disponibilidad del dinero es inmediata. Tras esta compra, sufriremos una comisión por ingreso a través de tarjeta de crédito de 3,99%, además de la comisión de compraventa de 0,5%, lo que se traduce en 39,9€ y 4,8€, obteniendo un poder de compra real de 955,3€.

Una vez queramos retirar esta cantidad, suponiendo una variación del 0% en el precio del activo contratado, existen comisiones que no se detallan de la misma forma que las expuestas anteriormente, como son las de retiro de dinero en una moneda fiat. Coinbase y Binance publicitan que la retirada del dinero es totalmente gratuita, sin embargo, esto sólo es así para los casos en los que esa transacción se realice en alguna criptomoneda ofertada por la empresa, y sea una retirada a una cartera externa en posesión del usuario. Para los casos en los que se desee realizar un retiro del dinero en euros, dólares, libras u otra moneda fiat, la comisión será del 1% sobre el montante retirado, quedando 945,747€, un 5,4% menos que al inicio.

CAPÍTULO 3: USO ILÍCITO DE CRIPTOMONEDAS

Aunque se puede decir que el objetivo principal del Bitcoin y otras criptomonedas descentralizadas es prevenir la "tiranía monetaria" evitando a la banca centralizada, algunos defensores reconocen la necesidad de estandarizar su uso y proteger su seguridad para popularizar la moneda y demostrar su legitimidad. Bitcoin no ofrece ningún tipo de autoridad oficial de resolución de disputas, dejando a los usuarios de que sus transacciones se mantengan seguras gracias a los procedimientos de autorregulación del programa, a través del blockchain.

Las cuentas de los usuarios en las plataformas de intercambio no están vinculadas a cuentas bancarias ordinarias ni a otros datos de identificación personal, haciendo más difícil la protección de los derechos de propiedad, y creando casos de inversores defraudados más difíciles de resolver que los de fraude en transacciones financieras convencionales.

La raíz del sistema Bitcoin es que la confianza en la moneda se basa en sus propiedades de autorregulación, sin requerir el control de ninguna autoridad. Sin embargo, los usuarios que son hackeados, robados, o que tienen disputas derivadas de transacciones en Bitcoin, recurren cada vez más a las autoridades legales tradicionales para obtener una solución.

El principal problema que se presenta, es el de las implicaciones del aumento previsto de las transacciones transfronterizas similares al dinero en efectivo. Bitcoin, la primera moneda digital diseñada para tener un alcance real y global, amplía el campo de uso de las transacciones similares al efectivo, creando nuevos problemas en la administración de las leyes fiscales transfronterizas. Bitcoin permite el intercambio de bienes, servicios e información a una escala nunca antes vista: un bazar mundial en el que las empresas multinacionales y los vendedores individuales tienen el mismo acceso a los posibles compradores, aunque las transacciones entre ellos son tan difíciles de investigar como los intercambios de dinero en efectivo.

Bitcoin amplía el horizonte de las transacciones, desde los intercambios tradicionales cara a cara o por correo, hasta el mundo sin fronteras de Internet. Esto incluye las compras legales rutinarias, la evasión de impuestos, el blanqueo de dinero y las compras ilegales de drogas y armas. Entre las principales críticas al Bitcoin está su supuesto uso para actividades delictivas y como conducto para la evasión de impuestos.

El blanqueo de capitales a través de las fronteras nacionales implicaba tradicionalmente a grandes bancos multinacionales especializadas en transacciones financieras transfronterizas. Como tal, los esfuerzos de lucha contra el blanqueo de dinero han utilizado tradicionalmente a los bancos multinacionales como puntos de contacto centralizados para informar de las transacciones sospechosas de blanqueo de fondos ilícitos. Sin embargo, las transacciones de criptomonedas se realizan entre redes descentralizadas de usuarios repartidos por todo el mundo.

Tabla 2. Explotación de las vulnerabilidades en cada etapa

Factores de riesgo	Fase inicial	Fase intermedia	Fase final
Anonimato	Pueden ser utilizadas por delincuentes y asociaciones	Nombres sospechosos, especialmente si hay mulas de dinero involucradas que no pueden ser identificadas	Permitir el canje del dinero del delito de forma anónima a personas que no pueden ser rastreadas
Transacciones en tiempo real	El dinero del fraude puede ser ser transferido a otra criptomoneda en otro país	Las transacciones se producen en tiempo real, por lo que hay poco tiempo para detenerlas si se sospecha de blanqueo de capitales	Los beneficios del crimen pueden ser movidos rápidamente a través del sistema sistema financiero mundial y retirarse en otro país

Fuente: elaboración propia (Cambell-Verduyn, 2018, 5)

3.1 LÍMITES DE LA AUTORREGULACIÓN

Las empresas del ecosistema de las criptomonedas, como Coinbase o Binance, han desarrollado diversos servicios que cumplen con la legislación antiblanqueo. BitInstant, una de las principales empresas emisoras de tarjetas de débito con criptomonedas, con sede en Nueva York, promovió el registro voluntario y el cumplimiento de las leyes contra el blanqueo de capitales. Los intercambios de monedas virtuales por dinero fiat, como BitFinex, con sede en Hong Kong, exigen a los clientes una aplicación más exhaustiva y minuciosa del cumplimiento de las normas, que implica la presentación de documentos de identificación certificados y una prueba válida de domicilio (BitFinex, 2021). BTC China, con sede en Hong Kong, así como las bolsas británicas Bitstamp y CEX.IO, aplican unas normas mínimas de lucha contra el blanqueo de capitales exigiendo a los clientes que proporcionen copias de sus pasaportes para verificar su identidad.

Sin embargo, estos esfuerzos de las empresas en materia de lucha contra el blanqueo de capitales varían considerablemente, ya que las bolsas de criptomonedas como HitBTC sólo exigen la identificación de los titulares de cuentas que consideran "sospechosas" (HitBTC, 2021). Las diferencias entre los esfuerzos de cada empresa en materia de lucha contra el blanqueo de capitales han llevado a desarrollar un conjunto de directrices comunes. En un intento de desarrollar normas comunes de gestión de riesgos y de cumplimiento, el organismo con sede en Delaware llamado Digital Asset Transfer Authority (DATA) publicó un borrador de directrices globales de lucha contra el blanqueo de capitales en 2015, haciendo hincapié en la necesidad de equilibrar los esfuerzos de lucha contra el blanqueo de capitales con los derechos y valores fundamentales, incluidas las libertades civiles, la privacidad y la inclusión financiera, la transparencia y la responsabilidad. Su proyecto de directrices instaba a las empresas criptomonedas a aplicar un programa básico de cumplimiento de la lucha contra el blanqueo de capitales, independientemente de que la ley lo exija o no. Los datos especifican que el cumplimiento de la legislación contra el blanqueo de capitales implica procedimientos internos escritos y formación anual de los empleados

sobre evaluaciones de diligencia debida basadas en el riesgo, supervisadas por directores de cumplimiento independientes. Este proyecto de directrices sugería que las empresas recopilaran los nombres y las direcciones de los clientes, así como que consideraran la posibilidad de aplicar procedimientos más profundos de identificación y verificación de los clientes, especialmente a los evaluados de alto riesgo. Estos procedimientos incluyen desde la simple búsqueda en Google de la persona o la empresa en cuestión o la comprobación del registro de la empresa en el organismo gubernamental correspondiente, hasta la solicitud de referencias bancarias y de otro tipo, la obtención de informes crediticios o comerciales, e incluso la comprobación de los antecedentes penales (DATA, 2015).

3.2 BLANQUEO DE CAPITALES

El blanqueo es el acto de hacer que las ganancias obtenidas ilegalmente o el “dinero sucio” parezcan limpios colocándolas dentro de un sistema financiero legítimo junto a otras transacciones legales. Entre el tres y el cuatro por ciento de todas las ganancias delictivas en Europa se blanquean a través de criptomonedas, lo que se estima en 4.000 a 5.000 millones de dólares de Bitcoins blanqueados en 2016.

Como se ha expuesto anteriormente, el blockchain puede considerarse un libro de contabilidad visible y verificable públicamente. Todas las transacciones se registran en el blockchain y pueden verificarse a través de sitios web públicos, como blockchain.info y otros de código abierto. Cualquier persona, en cualquier lugar, puede ver todas las transacciones de bitcoin de una dirección a otra en tiempo real. El saldo total actualizado de la cantidad de bitcoins en una dirección también es visible públicamente, pero esa dirección está cifrada por la tecnología SHA-256, al igual que el resto de información sensible. Esto quiere decir que no hay nombres conectados a la dirección y al monedero de Bitcoin. Sin embargo, debido a este concepto de lo que es el blockchain, toda la información histórica sobre cualquier dirección de bitcoin y la información sobre las transacciones está a un solo clic de distancia.

El blanqueo de capitales es un fenómeno delictivo en constante cambio, con modus operandi actualizados y modelos de negocio en evolución. Para la empresa delictiva, no es fácil conseguir una estrategia de blanqueo decente dada la alta regulación que existe en la mayoría de países. El beneficio final del delito, sin los medios para blanquearlo, haría que el negocio delictivo no fuera rentable. Tradicionalmente, el blanqueo del dinero del delito se facilita mediante mulas de dinero, cuentas en el extranjero, o productos de lujo: arte, casas, barcos, o una combinación de ellos. Según evolucionan las metodologías, aparecen nuevas alternativas como Western Union o Perfect Money, que ocupan un lugar destacado en las tramas de blanqueo de capitales, o las tarjetas de crédito de prepago, los vales de regalo u otros artículos de valor no tradicional fácilmente canjeables.

En la actualidad, los denominados nuevos métodos de pago se están convirtiendo en uno de los factores más importantes en las tramas de blanqueo de capitales, categoría donde cabría destacar las criptomonedas. El Bitcoin es una forma de pago cada vez más popular

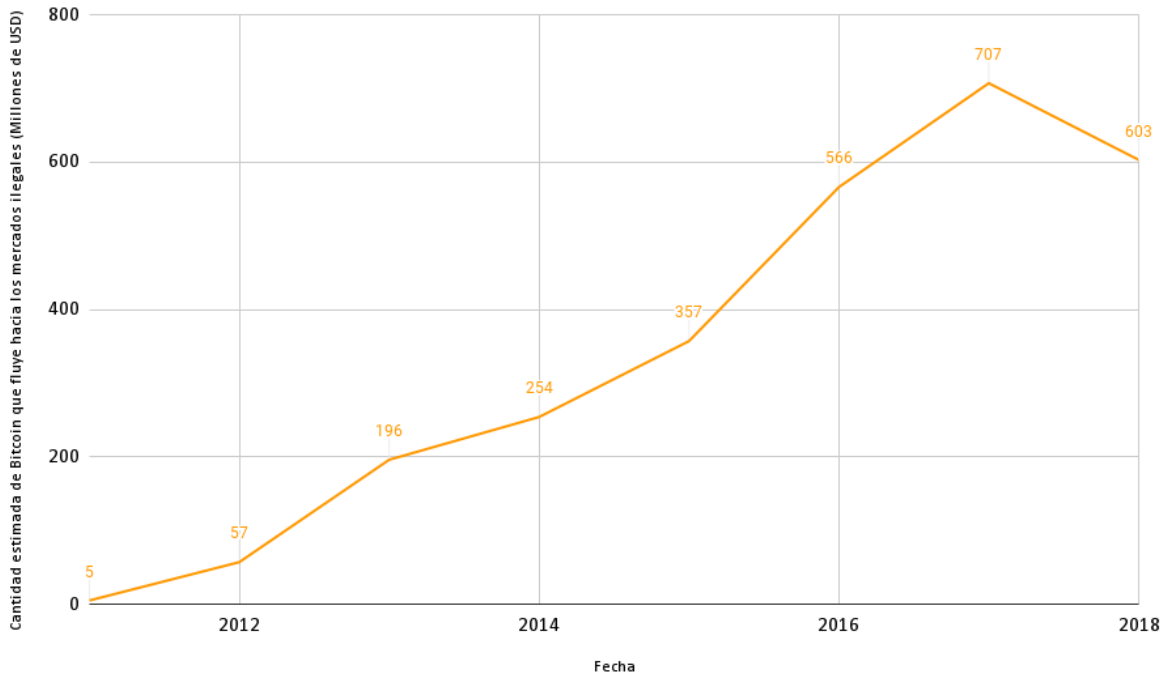
entre delincuentes; la Europol ha informado de que el Bitcoin representa más del 40% de todos los pagos identificados entre delincuentes en las investigaciones sobre ciberdelincuencia (EUROPOL, 2015). Queda por ver hasta qué punto esto puede considerarse una prueba de que existe una afluencia en el uso del Bitcoin como método de pago delictivo destacado entre otras opciones.

3.3 MERCADOS CLANDESTINOS

Los mercados clandestinos pueden considerarse como un facilitador del uso de criptomonedas en los esquemas de blanqueo de dinero actuales y futuros. Estos mercados sumergidos son fácilmente accesibles y están ganando popularidad entre los delincuentes para desplegar actividades delictivas, dada la creciente facilidad de uso.

Gracias a la popularización de la navegación anónima usando la red Tor, se abrió a un público general la posibilidad de navegar a través de internet sin desvelar datos personales o información sensible acerca del dispositivo que se usa, localización, o dirección IP. De este modo surgió la llamada Dark Web (o Deep Web), que atrae a un número creciente de curiosos. Las investigaciones cuantitativas sobre la Dark Web indican que más del 50% de todo el contenido de la misma es ilegal (Moore & Rid, 2016).

Gráfico 8. Cantidad estimada de Bitcoin que fluye hacia los mercados ilegales (Millones de USD)



Fuente: elaboración propia a partir de los datos de statista.com

3.3 ESTAFAS

Las estafas se crean con anuncios que promueven el uso del Bitcoin, como precio de oferta, intercambio de bitcoin, carteras, etcétera. Cada vez más, el Bitcoin se convierte en una utilidad básica entre los ciberdelincuentes; dos de los principales atractivos de la moneda digital son sus disposiciones para el pseudo anonimato y su protocolo de transacción irreversible. Este tipo de disposiciones engendran los intereses contrapuestos entre los usuarios legítimos, que realmente quieren transferir dinero de forma eficiente y segura, y los ciberdelincuentes que aprovechan estas propiedades para realizar transacciones irrevocables y supuestamente imposibles de rastrear.

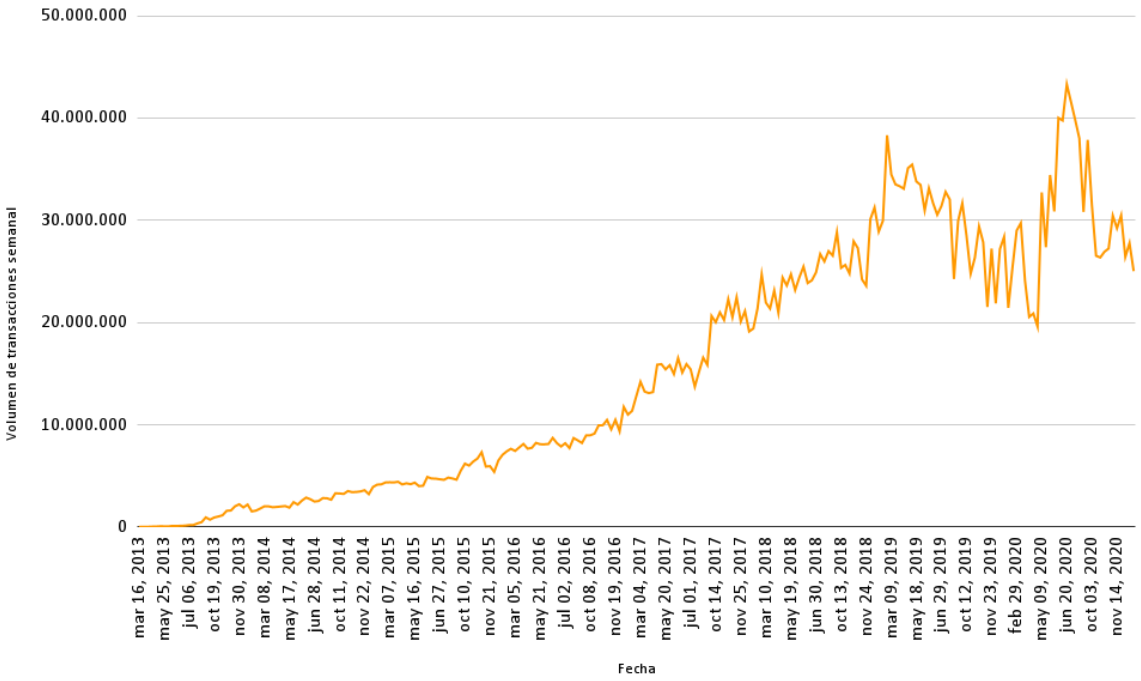
3.3 EVASIÓN DE IMPUESTOS

La evasión de impuestos está ocurriendo hoy en día en todo el mundo, pero, en la mayoría de casos, puede ser identificada por el gobierno para tomar las medidas necesarias. Las criptomonedas proporcionan una nueva forma de evadir impuestos, ya puede ser intercambiable y transferible instantáneamente de forma anónima.

Dado que esta tecnología es muy novedosa nos encontramos aún en la fase de adaptación al cambio, y se requiere una investigación para comprobar la red blockchain y su transacción para fijar los impuestos pertinentes. Si el seguimiento de un usuario sospechoso fuera posible, las autoridades tendrán el poder de gestionar los problemas en la evasión de impuestos.

En las redes de intercambio de Bitcoin y otras monedas, se mueven miles de millones de dólares de transacciones. Como se ha mencionado en el de los límites de la autorregulación, aumentar la cantidad de información existente de cada usuario en los monederos y redes de intercambio de criptomonedas, es un paso esencial para lograr la correcta identificación de los usuarios.

Gráfico 9. Número de transacciones semanales de Bitcoin en Estados Unidos



Fuente: elaboración propia a partir de los datos de coin.dance.com

En 2015 se estimó que cerca de 2,8 millones de personas en Estados Unidos poseían criptodivisas, pero solo 807 personas declararon Bitcoins en sus impuestos. En EEUU, las criptodivisas están definidas como una propiedad, no como una moneda, lo que significa que las ganancias y las pérdidas deben ser declaradas por los contribuyentes al igual que cualquier otro activo. El 36% de los inversores de Bitcoin afirmaron que, a sabiendas, no declararían las ganancias o pérdidas de capital de la criptodivisa en sus impuestos de 2017 (Connell, 2017).

3.4 REGULACIÓN

La regulación de la red Bitcoin y el blockchain en general, será difícil debido a su naturaleza compleja y descentralizada, que la hace esencialmente impermeable a un único punto de regulación. En lugar de intentar controlar todos los aspectos de la red Bitcoin, es más eficaz analizar cada entidad de transacción de Bitcoin individualmente y determinar en un análisis abreviado de coste-beneficio cuáles serán los mejores aspectos a regular.

3.4.1 REGULAR AL EMISOR

La regulación del emisor inicial de Bitcoin probablemente resulte inviable debido a la naturaleza en gran medida pseudo anónima y dispersa de las identidades de los remitentes en la red blockchain. Cuando un remitente envía bitcoins a otro usuario de Bitcoin o a un servicio de blanqueo de dinero, no se intercambia ninguna información personal identificable. A menos que haya algún resultado físico o rastreable de la transacción (por ejemplo, que el remitente haya facilitado su dirección de envío), la probabilidad de identificar al propietario de una dirección Bitcoin de un solo uso es extremadamente baja. Además, atacar a la base de usuarios de una comunidad probablemente dará lugar a una mayor desconfianza y desaprobación hacia el gobierno, y podría conducir a un aumento del anonimato. Por lo tanto, la aportación de recursos para intentar rastrear a los usuarios que no han proporcionado ninguna información de identificación personal, supera en gran medida el beneficio de regular lo que probablemente sean transacciones menores y puede dar lugar a una ocultación aún mayor del blanqueo de dinero.

3.4.2 REGULAR AL RECEPTOR

Del mismo modo, regular a los receptores o, para este caso concreto, blanqueadores de Bitcoin, será inviable. Aunque esto podría permitir la aplicación de la ley y la regulación a aquellos que actúan con una clara intención criminal, como, por ejemplo, los blanqueadores de dinero que ya hayan sido identificados con anterioridad, y así evitar la reacción de la comunidad que podría resultar de intentar regular todos los remitentes de Bitcoin, la regulación de los blanqueadores se enfrenta a los mismos problemas de anonimato que la de los emisores: si no hay una salida física que rastrear, se dedicarán importantes recursos para obtener recompensas relativamente pequeñas.

Por otro lado, los infractores pueden ampararse tras leyes internacionales menos rigurosas. Por tanto, perseguir a los receptores de Bitcoin en general, y a los blanqueadores de dinero en particular, resultará ineficaz.

3.4.3 REGULAR A LOS MINEROS

Los mineros, como se mencionó en el segundo capítulo, son los encargados de verificar las transacciones dentro de una red blockchain, recibiendo a cambio una comisión emitida en la misma criptomoneda que supervisan.

Existe una cierta falta de culpabilidad al realizar el acto de procesar la transacción, ya que el software de minería procesa las transacciones para el blockchain sin intervención alguna por parte del usuario. Aunque algunos usuarios de Bitcoin pueden entender cómo la red Bitcoin y cómo su actividad de minería puede completar un bloque de transacciones, la mayoría de los usuarios están incentivados por la posibilidad de recompensas, y no tienen

conocimientos del funcionamiento real del blockchain. Además, al igual que los emisores y receptores, su identidad es prácticamente anónima.

3.4.4 REGULAR A LAS REDES DE INTERCAMBIO

Por último, y lo más prometedor, es la regulación de las casas de cambio de Bitcoin y otras criptomonedas. Dado que los intercambios de Bitcoin suelen tratar con monedas fiduciarias, será más fácil que entren en las leyes de intercambio de dinero que definen el dinero como moneda respaldada por un gobierno.. Además, las bolsas ganan credibilidad gracias a la confianza de los usuarios y al volumen de transacciones. Si la bolsa tiene pocos usuarios dispuestos a comerciar o si no es digna de confianza, no permitirá fácilmente que se produzcan las fases de blanqueo de dinero sin llamar la atención. Debido a esta contrapartida, es probable que las bolsas estén menos descentralizadas y, por lo tanto, serán más fáciles de regular. Una red de intercambio que facilite cientos o miles de transacciones, y que posiblemente reciba comisiones por el procesamiento de las mismas, no podrá demostrar un desconocimiento acerca de lo que ocurre en la empresa. Por lo tanto, de las entidades principales de una transacción de Bitcoin, o de blockchain en general, la regulación de las redes de intercambio parece la más probable.

3.4.5 ESTADO ACTUAL DEL MARCO LEGAL Y LOS IMPUESTOS

Hasta ahora, lejos de la creación de una regulación específica y de ser consideradas como monedas que realmente podrían suplantar al dinero fiat, las criptomonedas se incluyen dentro de otros activos que generan rentas, y su imposición varía dependiendo del país en cuestión:

Tabla 3. Tributación del Bitcoin en varios países

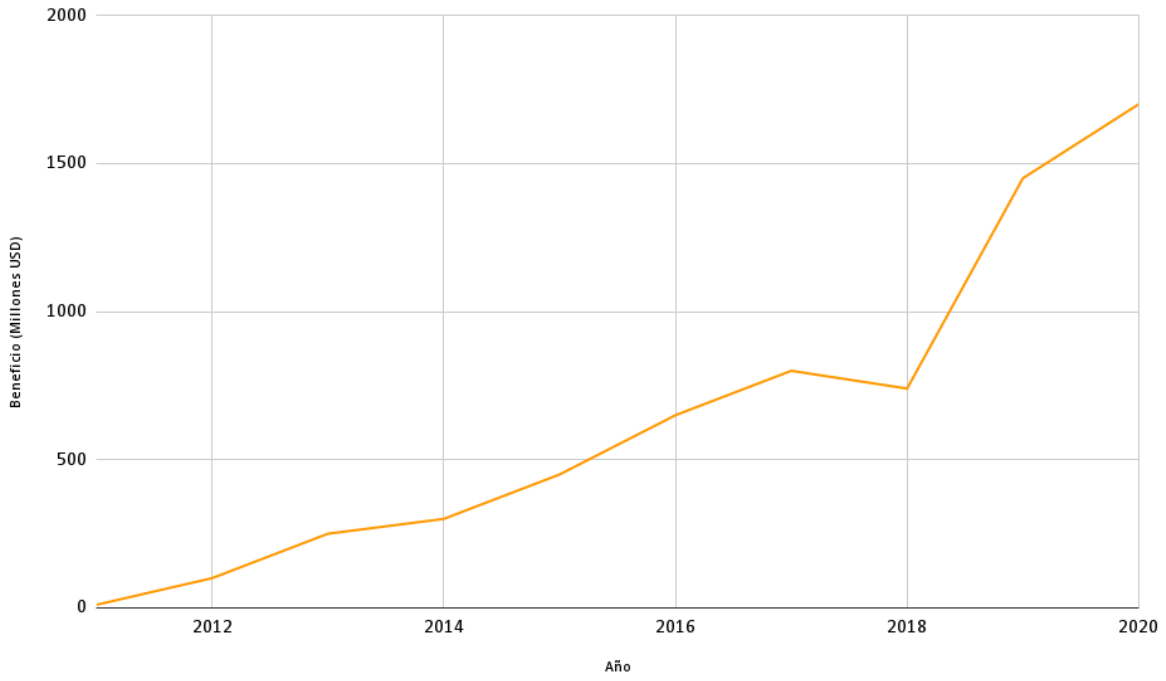
País	Marco legal	Impuestos
España	Tiene marco legal	Renta por ganancias, IVA y renta por patrimonio
Estados Unidos	Tiene marco legal	Renta propiedades
Alemania	Tiene marco legal	Renta por ventas ganancias si se tiene Tiempo menor a un año, grava al 25%
Reino Unido	Tiene marco legal	Renta por ganancias, se mira cada caso para aplicar pago
Australia	Tiene marco legal	Renta por ganancias, si es menor de 10.000 dólares australianos exenta
Japón	Tiene marco legal	Renta por ganancias, renta por patrimonio.

Fuente: elaboración propia (Autoras, 2018)

3.5 RETOS

La naturaleza anónima y descentralizada de las criptodivisas ha dado oportunidades a los delincuentes para llevar a cabo actividades ilícitas. Las criptomonedas se han utilizado ampliamente en los mercados ilegales para recibir pagos por servicios ilícitos como la denegación de servicio distribuida, los distribución de malware, redes de bots y la compra de productos ilegales como armas, drogas y documentos falsificados o robados. Los mercados de la deep web, como Silkroad, AlphaBay y Hansa, son recurrentes, por lo que, por mucho que se logre llegar a cerrar estos puntos de venta, aparecen nuevos con mayor seguridad. Este tipo de webs facilitan el comercio de productos ilícitos como antigüedades robadas, drogas y armas de fuego, remitiendo dinero a zonas que están sometidas a un gran escrutinio financiero o a un embargo, y financiando públicamente sus operaciones.

Gráfico 10. Beneficio de los mercados ilegales de la Deep Web (millones de USD)



Fuente: elaboración propia a partir de los datos de bankinfosecurity.com

Un número importante de delincuentes anuncian bolsas de criptomonedas o Initial Coin Offerings (ICOs) con el objetivo de blanquear dinero para obtener beneficios ilícitos. Existen redes de Intercambio de Bitcoin como OKCoin con cientos de miles de dólares estadounidenses blanqueados (Gautham, 2016), así como el caso de BitInstant, en el que se blanquearon más de 1.000.000 de dólares para los clientes de Silk Road (Revilla, 2014). Las criptodivisas han hecho avanzar con creces las operaciones de diferentes familias de malware como el ransomware, con CryptoLocker y CryptoWall recibiendo 133.045,9961 BTC y 87.897,8510 BTC respectivamente (Emerging Technology From The Arxiv, 2018); el crypto jacking, con JenkinsMiner que hizo ganar a su operador más de 3.000.000 dólares en Monero (Muy Seguridad, 2018); y los troyanos de robo de criptomonedas, como

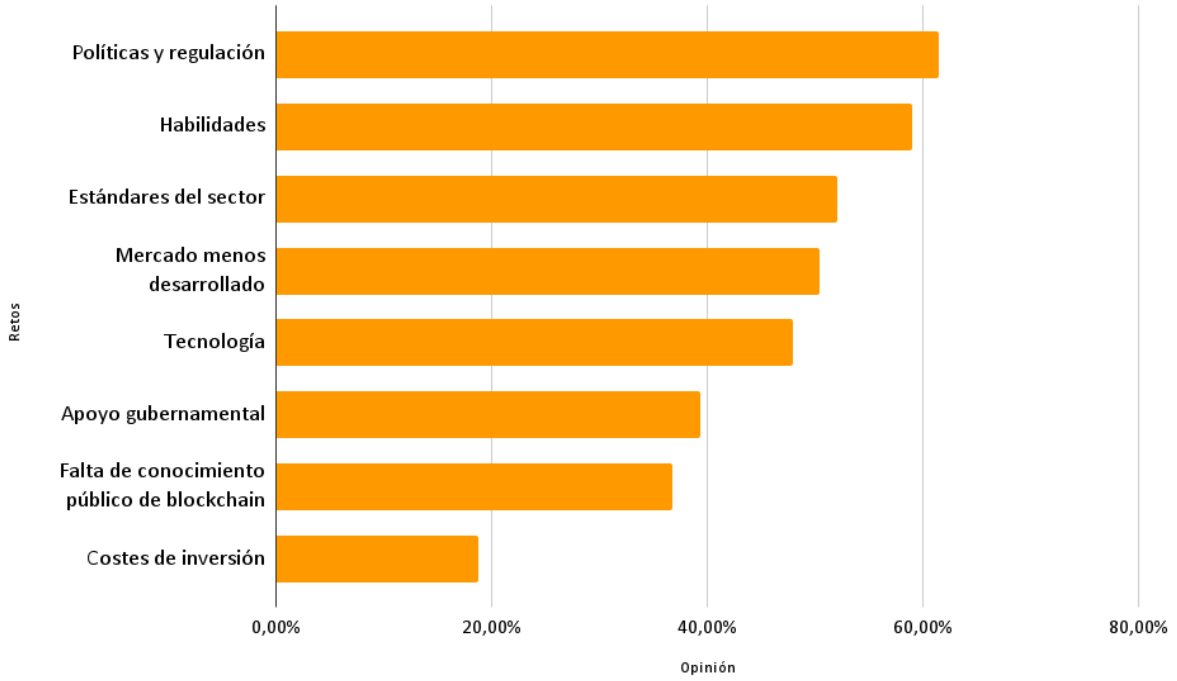
CryptoShuffler, que robó cientos de miles de dólares estadounidenses apuntando al contenido de la memoria volátil, es decir, el contenido del portapapeles de los dispositivos, al tener direcciones de monedas copiadas por los usuarios (Crespo, 2017).

Los Bitcoins están asociados a una plétora de tipos de delitos como los estupefacientes, las armas de fuego, el blanqueo de dinero, el terrorismo y la explotación infantil, es por esto que la comunidad internacional, incluida la INTERPOL, han comenzado a centrarse en el dominio y la creación de departamentos específicos de blockchain. Para ello, se ha destinado una cantidad importante de recursos a la exploración del uso de Bitcoins por parte de las personas que realizan prácticas ilegales con el mismo, así como al desarrollo de herramientas analíticas propias para rastrear las transacciones dentro del blockchain.

Se podrían dividir en dos los grupos de pensamiento de las autoridades en cuanto al uso del Bitcoin y otras criptomonedas: el primer grupo considera que los Bitcoins son una solución que permite a los delincuentes facilitar sus actividades ilegales en ausencia de vigilancia, y por ello pide su prohibición. El segundo grupo considera a las criptomonedas como una oportunidad de investigación en la que la información asociada a la delincuencia está ahora indexada de forma pública y permanente en el blockchain, pudiendo ser analizada con el fin de extraer datos forenses que puedan conducir a la atribución y el enjuiciamiento del delito.

La gran atención prestada al análisis de las transacciones de Bitcoin puede atribuirse al importante número de casos penales relacionados con ellas, a pesar de la existencia de criptodivisas más anónimas y más tecnológicamente avanzadas. El valor del Bitcoin y su amplia adopción por parte de los mercados han desempeñado un papel catalizador en el impulso de la magnitud de los casos delictivos. A pesar de la amplia adopción de Bitcoins por parte de los delincuentes, los recientes éxitos de las herramientas analíticas contemporáneas que permitieron a los investigadores policiales desanonimizar parcialmente la red Bitcoin y revelar las identidades de los criminales, han provocado un cambio en el uso de las criptodivisas.

Gráfico 11. Opinión de principales retos para el desarrollo de la industria del blockchain (China)



Fuente: elaboración propia (PwC, 2018)

3.5.1 MÁS ALLÁ DEL BITCOIN

Otras monedas, como Dash y Zcash permiten a los usuarios mantener su historial de actividad y saldo en privado, lo que impide a los investigadores identificar y rastrear las transacciones sospechosas. Del mismo modo, Monero utiliza "firmas de anillo", "transacciones de anillo" y "direcciones furtivas", desarrolladas por Ronald Rivest, Adi Shamri y Yael Tauman, para ofuscar los orígenes, los importes y los destinos de las transacciones (Monero, 2021).

Verge es otra criptomoneda anónima que aprovecha el protocolo *Wraith* para permitir a sus usuarios cambiar entre libros de blockchain públicos y privados. Cuando el protocolo *Wraith* está activado, los datos de las transacciones quedan ocultos (Kolupaev, 2017).

Por último, Namecoin no tiene las mismas características de anonimato ni los mismos objetivos que las criptodivisas anteriores, pero sigue considerándose una amenaza potencial, debido a que permite a los usuarios registrar de forma anónima sitios web ilegales sin proporcionar ninguna información personal, lo que impide a los investigadores identificar a los administradores que están detrás de estas páginas (Namecoin, 2011).
Además del trabajo actual de las fuerzas del orden a nivel nacional, INTERPOL actúa como un centro de información a nivel internacional al reunir a investigadores policiales de varias

naciones, investigadores y desarrolladores de blockchain para compartir las mejores prácticas de investigación y las herramientas forenses para las criptomonedas.

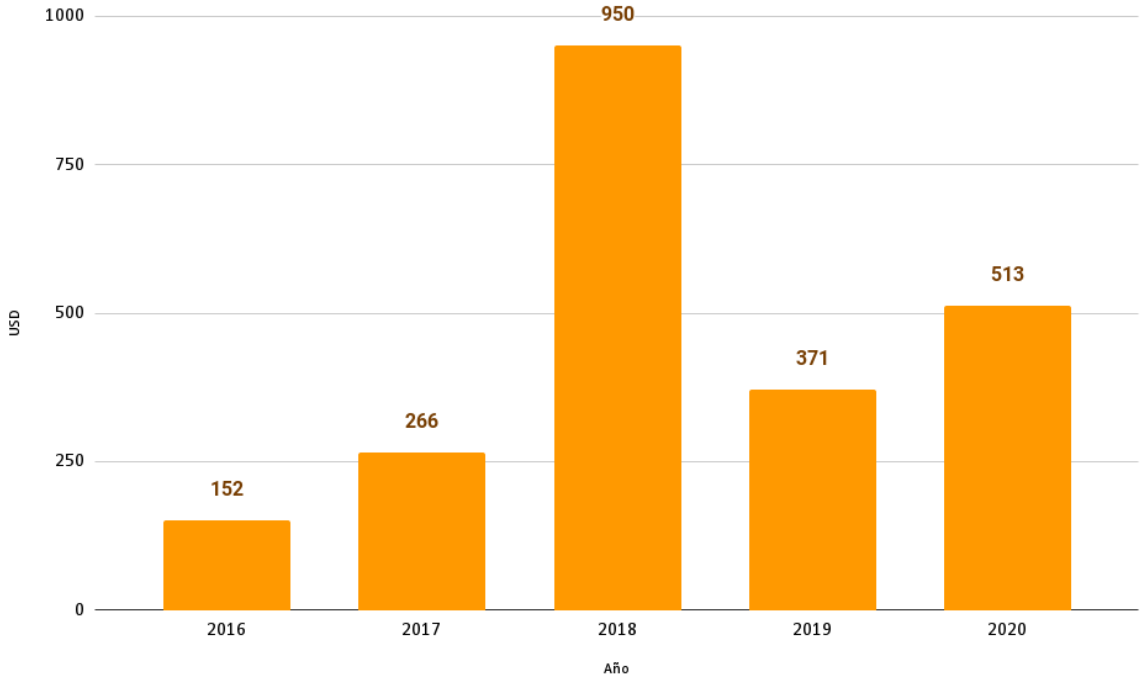
3.5.2 REFLEXIONES ACERCA DE LA REGULACIÓN

Los proveedores de servicios de Bitcoin, especialmente las redes de intercambio y los monederos electrónicos, están sujetos a la regulación del país pertinente, por lo que las únicas preguntas reales que quedan son: si los proveedores de servicios de Bitcoin y los usuarios de los mismos cumplirán con estas leyes o las desobedecerán abiertamente, utilizando Internet como un velo además de definir con exactitud a cuál de las diversas leyes aplicables se someterán los proveedores de servicios de criptomonedas; y si las leyes son suficientes para prevenir la actividad delictiva expuesta anteriormente. Además, quedaría por resolver la problemática de la supresión del atractivo de estos activos a la hora de regularlos, puesto que los usuarios podrían ser más propensos a buscar otros métodos alternativos para conservar su anonimato y privilegios.

Una de las principales motivaciones que originaron la creación del Bitcoin y otras criptomonedas, es la desconfianza de las instituciones financieras, tras lo que los defensores de esta nueva tecnología se sometieron a las redes de intercambio, a los monederos electrónicos y a otros servicios relacionados, lo que ha dado lugar a que ocurran los mismos acontecimientos de robo, que crean una vez más la desconfianza que ya existía hacia las instituciones financieras más estables y fiables. Por otro lado, es irónico que los mismos usuarios que huían de las entidades reguladas, estén cómodos siendo partícipes de otras nuevas entidades que también están reguladas, o están en proceso de estarlo.

Flexcoin, el primer banco de Bitcoin del mundo, advirtió en diversas ocasiones a sus clientes que por el mero hecho de ser una entidad que opera con Bitcoins, sufren una mayor cantidad de ciberataques en comparación con otras entidades financieras. Flexcoin cierra sus puertas de forma indefinida en 2014, tras el revuelo de haber sufrido un robo de 1.000 Bitcoins, de los cuales se conocen las dos direcciones a las que fueron enviados, pero dado el anonimato, es imposible revertir la operación o encontrar al culpable (RPP Noticias, 2014).

Gráfico 12. Volumen de robo de criptomonedas a nivel global (millones de USD)



Fuente: elaboración propia a partir de los datos de ciphertrace.com

Si el gobierno expresa una intención más clara de regular los intercambios de criptomonedas y los monederos electrónicos, la línea divisoria entre los intercambios de Bitcoin fiables y los intercambios ilegítimos será aún más clara de lo que es ahora. Sin embargo, si el gobierno no ha determinado que los Bitcoins representan una amenaza suficiente, la incertidumbre continuará como resultado de la falta de regulación.

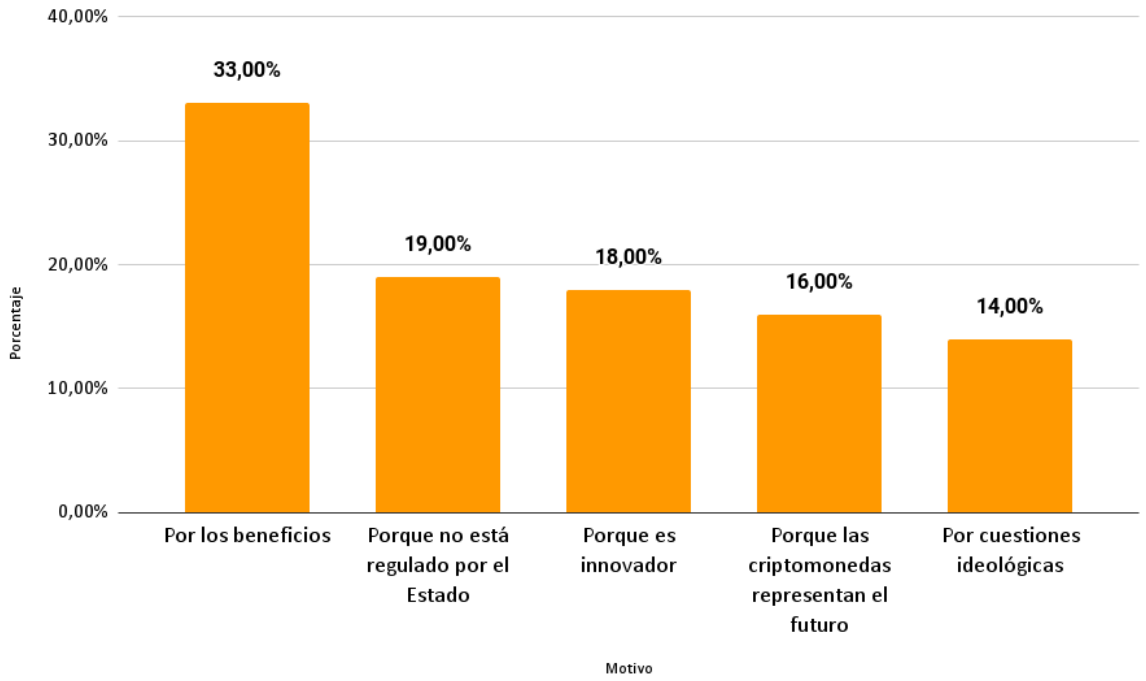
El actual esquema de regulación es insuficiente para proteger contra las amenazas de blanqueo de dinero, evasión fiscal y otras actividades delictivas. Las tecnologías que proporcionan herramientas para que los delincuentes mantengan su anonimato (como la red Tor), para llevar a cabo actividades delictivas y de blanqueo de dinero, se encuentran completamente al margen del hecho de que una determinada red de intercambio cumpla, o no, con la normativa regulatoria, puesto que estas herramientas funcionan a nivel usuario, de forma totalmente independiente de la entidad.

Hasta que los gobiernos aclaren su posición sobre la regulación del uso de las criptomonedas, los usuarios legítimos e ilegítimos seguirán confiando en los proveedores de servicios que puedan demostrar los indicios de fiabilidad, como la verificación de la identidad.

CONCLUSIÓN

Aún no se realiza un uso continuado real como moneda de cambio y depósito de valor por el usuario medio de las criptomonedas. La especulación, desinformación, falta de regularización y de leyes internacionales, hacen que estos activos sean usados de forma casi exclusiva por los especuladores.

Gráfico 13. Razones por las que comprar criptomonedas (Francia)



Fuente: elaboración propia a partir de los datos de odoxa.fr

La popularidad de las criptomonedas ayuda a la creación y el desarrollo de nuevas tecnologías de blockchain, lo que es beneficioso para la mayoría de sectores de la industria, e incluso para el usuario medio, estimándose que en pocos años esta nueva tecnología sea de uso diario en múltiples trámites y gestiones.

Se crean constantemente nuevos tipos de activos basados en la misma tecnología que las criptomonedas, como lo son las stablecoins y las ICOs. Sin embargo, actualmente, gracias a la falta de regulación y a su carácter global, existen numerosas contrapartidas en términos de seguridad a la hora de contratar estos activos, puesto que es fácil el no cumplimiento del contrato por cualquiera de las partes interesadas, y, ya expuestas las dificultades que ofrecen las criptomonedas a la hora de realizar su trazabilidad, es común la estafa.

Por otro lado, en el caso específico de las stablecoins, estas solucionan gran parte de los problemas que presentan las criptomonedas comunes, sin embargo, pierde el incentivo

principal: la descentralización. Al ser monedas centralizadas, esto hace que exista una menor privacidad y que su precio pueda variar en torno a otros activos, los cuales pueden ser gestionados por el Estado (como es el caso del dólar y la Reserva Federal en Estados Unidos), lo que hace que, a fin de cuentas, estas criptodivisas sigan teniendo su valor controlado por terceras partes.

Además de su uso especulativo, el uso en mercados ilegales y en la evasión de impuestos es muy elevado. El anonimato y la encriptación que ofrece la tecnología blockchain es uno de los pilares básicos sobre los que se sustentan las preocupaciones de los gobiernos a un nivel internacional, dado que es extremadamente compleja la regulación de estos activos.

No sólo existe preocupación gubernamental sino empresarial y a nivel usuario, puesto que las entidades que operan con criptomonedas y, sobre todo, con Bitcoin, están sujetas a un alto nivel de ataques informáticos, así como los usuarios de estas plataformas, lo que crea un gran nivel de desconfianza.

Los riesgos principales de las criptomonedas se pueden desglosar en:

- Monederos virtuales sin un nombre de persona física adjunto.
- La mezcla de claves (de encriptación SHA-256) públicas y privadas dificulta el seguimiento de las transacciones ilegales.
- El sistema descentralizado que define a la mayoría de criptomonedas permite pagos transfronterizos de forma rápida, eficaz y anónima.
- El porcentaje de actividad ilegal financiada por criptomonedas es muy alto.
- La escasa información requerida por empresas gestoras de redes de intercambio.

Aún queda por resolver el paradigma de la regulación, y encontrar la resolución a la tesitura de eliminar las ventajas de estas monedas a cambio de un uso más seguro, lo que haría que los usuarios dejen de usarlas y se creen otras nuevas, con mayores dificultades para la regulación y la trazabilidad.

Las criptomonedas y, en especial, la tecnología blockchain, constituyen el futuro de una sociedad con mayor privacidad y facilidad a la hora de la gestión de datos personales y procedimientos gubernamentales, como el voto electrónico, escrituras de viviendas, información personal, etcétera, pero, sin embargo, posiblemente estas monedas basadas en el blockchain descentralizado clásico, no lleguen nunca a sustituir de forma consistente el uso de una moneda fiat, puesto que los gobiernos no lo permitirían, además de requerir un nivel de entendimiento tecnológico mucho mayor que el medio, y no ofrecer el mismo nivel seguridad y respaldo estatal que su contrapartida fiduciaria.

BIBLIOGRAFÍA

Atkins, J. (2021, Enero 15). *Crypto Crime Cartel: The end is nigh for Tether*. CoinGeek. https://coingeek.com/crypto-crime-cartel-the-end-is-nigh-for-tether/

Bit2Me. (2018, Febrero 12). *¿Qué es SHA-256?* Bit2Me Academy. https://academy.bit2me.com/sha256-algoritmo-bitcoin/

BitFinex. (2021). *Legal y Privacidad*. BitFinex. https://www.bitfinex.com/legal/exchange/terms

Blockchain.com. (2021, Mayo 31). *Bitcoin circulante total*. Blockchain.com. https://www.blockchain.com/charts/total-bitcoins

Cambell-Verduyn, M. (2018, Marzo). Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law and Social Change*, *69*(2), 5. https://www.proquest.com/abicomplete/docview/1993215873/401F6992E43845FAPQ/1?accountid=14744

CB Insights. (n.d.). Blockchain Trends In Review. *Research Report*, *1*(1), 15.

Cipher Trace. (2021). *Cryptocurrency Crime and Anti-Money Laundering Report*. https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/

Coin ATM Radar. (2021, Marzo 1). *Bitcoin ATM Installations Growth*. Coin ATM Radar. https://coinatmradar.com/charts/growth/

Coin Dance. (2021). *itcoin trading volume on online exchanges in the United States*. Coin Dance. https://coin.dance/

CoinMarketCap. (2021, Mayo 29). *Cryptocurrency Prices*. CoinMarketCap. https://coinmarketcap.com/

Coin Metrics. (2021, Abril 13). *Number of daily Bitcoin transactions worldwide from January 2017 to April 13, 2021*. Coin Metrics. https://coinmetrics.io/

Connell, J. (2017). *Only 807 People Have Declared Bitcoin for Tax Purposes According to IRS*. https://news.bitcoin.com/807-people-declared-bitcoin-tax-purposes-according-irs/

Crespo, A. (2017). *CryptoShuffler, un troyano que roba Bitcoins de usuarios utilizando el portapapeles de Windows*. https://www.redeszone.net/2017/11/01/cryptoshuffler-troyano-roba-bitcoins-usuarios-utilizando-portapapeles-windows/

DATA. (2015, Julio 1). *Global AML / KYC Draft Guidelines from DATA*. DATAAuthority. https://datauthority.org/blog/2015/07/01/global-aml-kyc-guidelines-data/

Emerging Technology From The Arxiv. (2018). *El lucrativo alcance de los ataques 'ransomware' en Bitcoin*. https://www.technologyreview.es//s/10173/el-lucrativo-alcance-de-los-ataques-ransomware-en-bitcoin

EUROPOL. (2015). The Evolution of Criminal Markets. *Exploring Tomorrow's Organised Crime*. http://www.europol.europa.eu/sites/default/files/Europol_OrgCrimeReport_web-final.pdf

Feldman, S. (2019, Febrero 22). *Darknet Bitcoin Use Is Persistent Despite Busts*. Statista. https://www.statista.com/chart/17128/darknet-use-of-bitcoin/

Gautham. (2016). *Bitcoin Exchange OKCoin Fined in Money Laundering Case*. https://www.newsbtc.com/all/china-okcoin-exchange-fined/

HitBTC. (2021, Mayo 27). *Condiciones de Servicio*. HitBTC. https://hitbtc.com/es/terms-of-use

Incisive Business Media. (2019, Abril 11). *10% of the world's wealth set to be stored on blockchain by 2027*. International Investment. https://www.internationalinvestment.net/news/4001800/world-wealth-set-stored-blockchain-2027-cisco

InDiem. (2021, Mayo 27). *About InDiem*. InDiem Blockchain explorer. https://indiem.info/

Investing. (2021, Mayo 30). *BTC/USD - Bitcoin Dólar*. Investing.com. https://es.investing.com/crypto/bitcoin/btc-usd

Kolupaev, S. (2017). *What is Wraith Protocol?* https://medium.com/@sashakolupaev/what-is-the-wraith-protocol-bd1dfb289cda

Momtaz, P. P. (2019). Token Sales and Initial Coin Offerings: Introduction. *The Journal of Alternative Investments*, *21*(4), 7. https://jai.pm-research.com/content/21/4/7/tab-article-info

Monero. (2021). *Firma de anillo*. https://web.getmonero.org/es/resources/moneropedia/ringsignatures.html

Moore, D., & Rid, T. (2016, Febrero 1). Cryptopolitik and the Darknet. *Survival, Global Politics and Strategy*, *58*(1), 7-38. https://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085

Muy Seguridad. (2018). *El malware de criptominado apunta ahora contra los servidores Jenkins*. https://www.muyseguridad.net/2018/02/21/malware-criptominado-contra-servidores-jenkins/

Namecoin. (2011). *Namecoin*. https://www.namecoin.org/

Odoxa. (2018, Enero 19). *Le Bitcoin, connu mais mal-compris et mal-aimé, attire tout particulièrement les jeunes*. Odoxa. http://www.odoxa.fr/sondage/bitcoin-connu-mal-compris-mal-aime-attire-particulierement-jeunes/

PwC. (n.d.). A quick snapshot of CBDC maturity globally. *PwC Global CBDC Index*, *1*(1), 17.

PwC. (2018). China blockchain survey report. https://www.pwccn.com/zh/risk-assurance/2018-china-blockchain-survery-report.pdf

Revilla, J. M. (2014). *El CEO de BitInstant, condenado en el 'caso Silk Road'*. https://www.itespresso.es/ceo-bitinstant-condenado-caso-silk-road-132455.html

RPP Noticias. (2014, Marzo 5). *Banco canadiense digital Flexcoin cierra tras el robo de casi 1.000 bitcoins*. RPP Noticias. https://rpp.pe/tecnologia/mas-tecnologia/banco-canadiense-digital-flexcoin-cierra-tras-el-robo-de-casi-1000-bitcoins-noticia-674416

Schwartz, M. J. (2021, Febrero 5). *Led by Hydra, Darknet Markets Logged Record Revenue*. Bank Info Security. https://www.bankinfosecurity.com/blogs/led-by-hydra-darknet-markets-logged-their-best-year-ever-p-2990

Simms, T. (2019, Mayo 16). *Louis Vuitton y Christian Dior revelan una plataforma blockchain para verificar los productos de lujo*. CoinTelegraph. https://es.cointelegraph.com/news/louis-vuitton-and-christian-dior-owner-unveils-blockchain-platform-to-verify-luxury-goods

Skinner, C. (2017). *The Crazy World of Crypto Currencies and ICOs*. https://thefinanser.com/2017/06/crazy-world-crypto-currencies-icos.html/

TradingView. (2021, Mayo 29). *Cryptocurrency Market*. TradingView. https://www.tradingview.com/