FACULTAD DE DERECHO

ANÁLISIS DE LA BLOCKCHAIN Y DE LAS CRIPTOMONEDAS

Relación con el delito de blanqueo de capitales

Autor: Manuel Cereijo Comet
Director: Luis Garvía Vega

Madrid
Junio 2018

Manuel
Cereijo
Comet

ANÁLISIS DE LA BLOCKCHAIN Y DE LAS CRIPTOMONEDAS

Resumen

En el presente trabajo se lleva a cabo un estudio sobre el impacto que tienen nuevos avances tecnológicos que se emplean en el ámbito financiero, como el *blockchain* y las *criptomonedas*, en el delito de blanqueo de capitales. Comenzaremos estudiando el blanqueo de capitales desde un punto de vista jurídico e histórico, observando su evolución en base a los avances tecnológicos. Observaremos cómo funcionan estas innovaciones, analizando sus ventajas, riesgos y cómo pueden emplearse para ejecutar el delito mencionado. Para ser objetivos en su estudio también compararemos el impacto de las tecnologías objeto de estudio con otros métodos tradicionales de pago, como el dinero en efectivo, para ponderar la amenaza de esta tecnología. Tratando de ser lo más exhaustivo posible, también se analizará la regulación y el control que existe ya sobre este activo. Por último, plantearemos posibles modificaciones que se podrían integrar al sistema para un mejor funcionamiento del actual *criptomercado*. Tras el análisis se alcanzan conclusiones favorables al *blockchain* y a la mayoría de las *criptomonedas*. Es una tecnología que puede aportar ventajas en nuestro sistema económico y financiero actual, mientras que el uso delictivo de las mismas está concentrado y limitado a escasos ejemplares de estas divisas (ej: *Monero*). En cuanto a su regulación, ya se aplican las directrices establecidas en la Ley 10/2010 de prevención de blanqueo de capitales y financiación del terrorismo.

Abstract

In the present paper a study is carried out on the impact of new technological advances that are used in the financial field, such as *blockchain* and *cryptocurrencies*, in money laundering. We will start by studying money laundering from a legal and historical perspective, observing its evolution based on technological advances. Also, we will study how these innovations work, analyzing their advantages, risks and how they can be used to execute the aforementioned crime. To be objective in our study we compared the impact of the technologies under study with other traditional methods of payment, such as cash, to weigh the threat of this technology. Trying to be as exhaustive as possible, we also analyzed the regulation and control that exists over this asset. Finally, we will propose possible modifications that can be integrated into the system for a better functioning of the *cryptomarket*. After the analysis, favorable conclusions are reached to the *blockchain* and to the majority of the *cryptocurrencies*. It is a technology that can provide advantages in our current economic and financial system,

while the criminal use of these is concentrated and limited to few examples of these currencies (*Monero*). Regarding its regulation, the guidelines established in the Law 10/2010 on the prevention of money laundering and terrorist financing, are already being applied.

Palabras Clave

Blanqueo de capitales, *blockchain*, *Bitcoin*, *criptomonedas*, moneda digital, estado de bienestar, tecnología.

Key words

Money laundering, blockchain, Bitcoin, cryptocurrencies, digital money, welfare state, technology.

Índice

1. INTRODUCCIÓN

En el presente trabajo se estudiarán dos conceptos de indudable actualidad. Estos son el delito de blanqueo de capitales y la cadena de bloques o *blockchain*. Afirmamos que son actuales ya que aunque el origen del blanqueo de capitales se remonta a la imposición de los primeros impuestos en la Edad Media (Tondini, 2009), las técnicas de ejecución del mismo evolucionan constantemente. Esto es así porque los gobiernos y los órganos legislativos y reguladores internacionales tratan constantemente de erradicarlo. Consecuentemente, los criminales se ven obligados a inventar nuevas formas de introducción de capitales con origen ilegal en los cursos legales del dinero fiduciario. En estas innovaciones delictivas son especialmente útiles los avances tecnológicos, que son creados con mayor rapidez de los que la justicia es capaz de entenderlos y controlarlos. Por otro lado, la popularidad de la *blockchain* comienza a partir del año 2008, cuando el protocolo *Bitcoin* fue publicado. Desde entonces el número de inversores en *criptomonedas* ha crecido de forma exponencial, como se puede apreciar en base al aumento de capitalización del mercado (coinmarketcap.com).

En un primer momento puede parecer que no existe relación entre ambos conceptos ya que uno es una actividad delictiva y el otro una tecnología de reciente creación. Sin embargo, existe una gran relación debido a la utilización de la tecnología que emplean los delincuentes para blanquear capitales. Las *criptomonedas* tienen características muy atractivas para los delincuentes, puesto que permiten transacciones anónimas y difícilmente rastreables. Como mencionaba el Banco de España en un informe sobre estos activos, "*Bitcoin nace con ambiciones elevadas: proporcionar a los ciudadanos un medio de pago que posibilite la ejecución de transferencias de valor rápidas, a bajo coste y que, además, no pueda ser controlado ni manipulado por gobiernos, bancos centrales o entidades financieras*" (Gorjón, 2014). Esta es la relación.

La inspiración para la realización de este trabajo es precisamente el aumento de la popularidad de las *criptomonedas*, hasta el punto de que se ha convertido en habitual que diariamente aparezcan noticias en los periódicos y telediarios relativas a esta tecnología. Por otro lado, también se ha convertido en habitual que las noticias a las que nos hemos referido relaten delitos cometidos a través de las *criptomonedas*. Ante esta

situación surge la duda de cómo reaccionarán los gobiernos ante la amenaza de que su afán recaudador se vea mermado.

Teniendo en cuenta lo anterior, el objetivo general de la investigación es realizar un análisis exhaustivo del delito de blanqueo de capitales y de las monedas digitales para entender como las segundas pueden ser empleadas para cometer el delito mencionado. El objetivo final que perseguimos es ser capaces de emitir un juicio sobre si esta revolución tecnológica es positiva para el desarrollo del mercado financiero y de nuestra sociedad, o por el contrario si presenta una amenaza que debe ser regulada más estrictamente o, incluso, prohibida. Para ello, comenzaremos estudiando el tratamiento jurídico del blanqueo de capitales y su evolución histórica. Esto se realiza para detectar si existen patrones de comportamiento delictivos con todos los descubrimientos tecnológicos o si las *criptomonedas* son una mayor amenaza. Una vez conocemos cómo se ejecuta tradicionalmente este delito, analizaremos el contexto, funcionamiento y desarrollo de estos activos tecnológicos llamados *criptomonedas*. Tras esto entenderemos cómo se emplean para cometer el delito y su actual regulación y si esta es necesaria, suficiente y efectiva. También compararemos estos vehículos de inversión con otros medios de pago que son considerados seguros, como el dinero en efectivo.

Una vez el análisis haya sido realizado y se entienda el proceso de blanqueo a través de las *criptomonedas,* propondremos modificaciones al actual funcionamiento del mercado para que las desventajas o riesgos actuales sean menores. Aunque también nos preguntaremos si es estrictamente necesario tomar medidas o si se puede confiar en la sistematización del mercado actual y en su libre mejora con el paso del tiempo y la experiencia.

La metodología que emplearemos para ello se basará en un método inductivo. Se empleará este método para, habiendo analizado previamente el delito de blanqueo de capitales y estudiado el funcionamiento de las *criptomonedas*, poder aportar conclusiones respecto a la relación de ambos elementos.

La información necesaria para realizar el trabajo se ha empleado el método cualitativo. Concretamente se ha acudido a numerosas fuentes primarias de información, aunque también se ha obtenido información de fuentes secundarias.

Como decíamos, el grueso de las fuentes consultadas son primarias, principalmente artículos académicos. De esta forma se producirá la revisión de la literatura, entendiendo y estudiando las ideas que se han planteado ya sobre la cuestión que nos abarca.

Los artículos académicos a los que nos referíamos se han obtenido a través de plataformas como "Google Académico" y la biblioteca de la página web de la Universidad de Comillas. Aquí se encuentran una gran cantidad de artículos referidos al blanqueo de capitales, que además tratan aspectos diferentes como su prevención, su análisis jurídico o su relación con la criminalidad organizada. En el ámbito de los mercados de moneda digital también se encontraron numerosos artículos, puesto que es un tema muy innovador. Aunque es cierto que existe mucha menos literatura consultable que en otras materias, puesto que todavía estamos en una etapa prematura de esta tecnología. Para acotar la búsqueda se buscaron palabras clave como "blanqueo de capitales", "prevención de blanqueo de capitales", "narcotráfico","*criptomoneda*", "*blockchain*", "*Bitcoin*" o "*Monero*".

También, se observará la legislación actual española, entre la cual se encuentra el Código Penal español y la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. Existe también legislación europea y dictámenes emitidos por importantes instituciones, como el Banco de España, que también serán empleadas.

Se estudiarán noticias de prensa económica especializada. Hay periódicos como el "*Financial Times"* o "Expansión" que aportan un gran conocimiento en materias financieras.

En cuanto a las fuentes secundarias, se realizarán encuentros con profesores universitarios de asignaturas como "Derecho Fiscal", "Macroeconomía" o "Mercados Financieros", que puedan aportar una perspectiva diferente a las noticias de prensa.

También, debido a que es un tema novedoso, cuyas bases no están asentadas y con un futuro incierto no hay tantos documentos académicos a los que podemos acceder como en otras materias. Incluyendo, los artículos encontrados son muy cautelosos y no se pronuncian tanto sobre la materia puesto que es difícil prever que será de este

mercado en diez años. Por esto, también hemos consultado numerosos *blogs* y revistas especializadas en tecnología.

Con los resultados anteriores se obtendrá un resultado de la situación actual y de la utilidad y efectividad de nuestras leyes y organismos competentes de prevenir la comisión del delito de blanqueo. Pero, más importante, se obtendrá un resultado sobre la implicación que tienen las *criptomonedas* en la comisión del delito en cuestión.

2. REVISIÓN DE LA LITERATURA

Vamos a dividir el estudio del contenido académico ya publicado sobre el tema que nos ocupa en tres subapartados:

a) Análisis del delito de Blanqueo de Capitales.

b) Relación de este delito con las tecnologías: cómo se han empleado históricamente los avances tecnológicos para cometer el acto criminal.

c) Análisis del nuevo surgimiento tecnológico: las *criptomonedas* y el *blockchain*.

Comencemos el análisis:

Análisis del delito de Blanqueo de Capitales

El blanqueo de capitales es uno de los principales problemas en la actualidad para los estados, como afirma Galindo (2017). El motivo es simple, los gobiernos no funcionan si no existe la capacidad para financiar sus políticas, proyectos o pagar los sueldos de sus integrantes. Y la fuente de financiación por antonomasia es la recaudación de impuestos. Es decir, mediante las aportaciones al fisco de los ciudadanos integrantes de un país los gobiernos pueden realizar su actividad y salvaguardar el estado de bienestar. Si la recaudación es insuficiente, debido a que los ciudadanos no aportan las cantidades que debieran, es imposible mantener una educación, sanidad o pensiones públicas. Aquí reside la importancia del blanqueo de capitales como analizó Alemán (2013), si no se elimina, el estado social corre un grave peligro, y por ello los estados tratan de erradicarlo. Este problema es especialmente sensible en aquellos estados cuyo gasto público en políticas sociales es elevado.

Desde que existe un sistema fiscal que grava las actividades económicas de los individuos, existe un delito de blanqueo de capitales. El Dr. Bruno M. Tondini (2009), en "Blanqueo de capitales y lavado de dinero: Su concepto, historia y aspectos operativos" remonta el origen del delito a la Edad Media. Se trata de un delito ciertamente muy antiguo, pero que ha ido evolucionando en sus formas constantemente.

Consultamos la guía jurídica *online* Wolters Kluwer, donde se define el blanqueo de capitales como el proceso o conjunto de operaciones mediante el cual los bienes o el dinero resultantes de actividades delictivas, ocultando tal procedencia, se integran en el sistema económico y financiero. Es decir, desde un punto de vista más material, se entiende el blanqueo o lavado de capitales como la actividad destinada a dar apariencia de legitimidad a capitales que proceden de actividades ilegales.

Por otro lado, en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo se establece otra definición de lo que se entiende por blanqueo de capitales:

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.

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.

Existirá blanqueo de capitales aun cuando las conductas descritas en las letras precedentes sean realizadas por la persona o personas que cometieron la actividad delictiva que haya generado los bienes.

A los efectos de esta Ley se entenderá por bienes procedentes de una actividad delictiva todo tipo de activos cuya adquisición o posesión tenga su origen en un delito, tanto materiales como inmateriales, muebles o inmuebles, tangibles o

intangibles, así como los documentos o instrumentos jurídicos con independencia de su forma, incluidas la electrónica o la digital, que acrediten la propiedad de dichos activos o un derecho sobre los mismos, con inclusión de la cuota defraudada en el caso de los delitos contra la Hacienda Pública.

Se considerará que hay blanqueo de capitales aun cuando las actividades que hayan generado los bienes se hubieran desarrollado en el territorio de otro Estado.

El proceso delictivo se puede dividir en tres fases diferentes, que definiremos de acuerdo al conocimiento del registrador de la propiedad Juan María Díaz Fraile, plasmado en el Blog de Registradores de España:

I. Fase de sustitución. Esta fase también se puede denominar de colocación o de inserción. "*Consiste en introducir los activos, monetarios o no monetarios, procedentes de las actividades delictivas en instituciones financieras o no financieras. El objetivo es la simulación de licitud. En esta etapa es cuando se manejan las mayores cantidades de dinero en efectivo. Entra en el circuito financiero fraccionadamente, en pequeñas sumas que se depositan en efectivo, tratando de canjearse por otros instrumentos monetarios negociables. Suele haber desplazamiento físico de grandes cantidades fuera del lugar de obtención con destino a otros donde sea más fácil encubrir u ocultar su origen delictivo*".
II. Fase de ocultación. Esta segunda fase también se puede denominar de "ensombrecimiento". "*Consiste en realizar una serie de transacciones financieras más o menos complejas, en muchos casos internacionales, que separen el activo de su origen de modo suficiente como para borrar el rastro y complicar el seguimiento de las operaciones por parte de las autoridades*".
III. Fase de integración. También denominada de reinversión. En este momento se producirá el "*retorno de los activos blanqueados al sector de la economía del que procedían o a otro sector diferente, pero con apariencia de legitimidad*".

El delito de blanqueo de capitales se encuentra estrechamente ligado a la delincuencia organizada. Esto es así debido a que la satisfactoria ejecución de las fases necesita, normalmente, de cierta organización entre individuos y de actividades. Si el delito es ejecutado mediante una sola persona es mucho más probable que la policía detecte el delito. También es especialmente más sensible si el delito del que proviene el

capital también lo ha ejecutado la misma persona que ahora tratará de blanquearlo. Las pistas del delito que se dejan pueden permitir a la policía detectar al criminal. Existe una gran relación, especialmente, con el narcotráfico.

Pongamos un ejemplo, imaginemos que un sujeto "A" roba un coche en la calle valorado en 15.000€. Aquí nos encontramos ante un delito de robo, pero el delincuente tratará de convertir ese activo en liquidez, es decir efectivo, de forma que sea más difícil rastrearlo. El delincuente decide acudir a un taller de conocidos suyos, donde encarga que desmonten el coche para vender las piezas por separado, este servicio se pagará en dinero negro, es decir sin declararlo a Hacienda. "A" procederá a vender las piezas por separado, ya que es más difícil rastrear el delito que vendiendo el coche en una sola unidad, que también lo realizará en "negro" sin declararlo. Tras concluir todas las transacciones de venta, "A" tendrá en su posesión dinero en efectivo por un valor aproximado a 15.000€. Toda esta cantidad de efectivo se habrá obtenido de forma ilegal y ahora el delincuente tratará de introducir este dinero en el curso legal del dinero fiduciario del país en cuestión, para poder emplearlo con normalidad sin correr riesgos de ser detectado por la policía y que el delito inicial le sea imputado. Existen diferentes formas mediante las cuales se puede llevar a cabo este procedimiento, que veremos en el siguiente apartado.

Por casos como el del ejemplo anterior es necesario el delito de blanqueo de capitales, ya que si no es posible detectar a los delincuentes que obtienen dinero ilícitamente todavía se les puede imputar el delito de blanqueo, si se les detecta en la comisión del mismo. Básicamente podemos afirmar que otorga otra oportunidad a los cuerpos policiales de "atrapar" a los delincuentes.

En cuanto al impacto económico de este delito, un estudio sobre los paraísos fiscales (Braslavsky) estimó que los paraísos fiscales del mundo ocultaban "*un tercio de todos los fondos del sistema bancario mundial*", refiriéndose a riqueza de particulares. El autor se basa en un estudio del banco Merrill Lynch, en el que se llegaba al dato de que aproximadamente 6 billones de dólares se encontraban en estos sistemas bancarios ocultados de los Estados. Algunos de estos refugios financieros acaparan grandes cantidades de dinero, como las Islas Caimán donde se almacenan "*500.000 millones de dólares*" aproximadamente en 570 entidades bancarias diferentes.

Con estos datos nos hacemos una idea de la magnitud del delito y de como muchas entidades financieras aparentemente legales colaboran para que todo ese capital oculto sea luego blanqueado y regularizado para su uso normal.

Relación de este delito con las tecnologías: cómo se han empleado históricamente los avances tecnológicos para cometer el acto criminal

Las formas de comisión del delito evolucionan. Evolucionan porque los gobiernos y los órganos legislativos y reguladores internacionales tratan incesablemente de erradicarlo. Consecuentemente, los violadores de la legalidad se ven obligados a crear nuevas formas de introducción de capitales con origen ilícito en los cursos legales de transacciones económicas. En este aspecto, es esencial la tecnología. La tecnología e Internet avanzan a un ritmo vertiginoso. Este factor, usado incorrectamente, proporciona una alternativa a los medios tradicionales de blanqueo de capitales.

Observemos las principales formas a las que los delincuentes recurren para blanquear capitales. El diario La Información (2016) elaboró una lista basándose en el conocimiento de expertos como Juan Carlos Galindo, presidente nacional ejecutivo de la Asociación Española de Sujetos obligados en Prevención de Blanqueo de Capitales (ASEBLAC), veamos los principales ejemplos:

- Contrabando de efectivo. Este método consiste en transportar grandes cantidades de capital en efectivo a través de fronteras para depositarlas en entidades financieras de países extranjeros en los que existan menos controles, como paraísos fiscales (ejemplo: Panamá, las Islas Caimán, etc.). En este caso, avances tecnológicos como los aviones (los *jet* privados son todavía más útiles) o las grandes instituciones financieras, permiten esta posibilidad. Este es un método muy antiguo que ha ido evolucionando conforme ha avanzado el Derecho Internacional y las fronteras entre los países. Desde que existe el dinero en efectivo los grandes delincuentes han expatriado el capital obtenido ilícitamente. Antiguamente, sin las actuales contabilidades digitales, era todavía más complicado conocer el paradero de ese capital para las autoridades.

- Adquisición de activos inmuebles. Se suele producir con la "*compra de un inmueble y su escritura por debajo del precio pagado*" (noticia aparecida en

el diario La Información con fecha 15 Febrero 2016). Posteriormente se venderá el inmueble "*por su precio de mercado*", lo que "*permitirá justificar la diferencia*". En otros casos, los préstamos hipotecarios sobre una propiedad pueden servir también como alternativa. Este es un método también antiguo que se ha empleado frecuentemente en el pasado, aunque continúa siendo así.

- Compra de premios de lotería. Los delincuentes adquieren el resguardo del ganador del juego para simular que el capital proviene de esta actividad. Este método existe desde la creación de este tipo de concursos, como podemos observar es un delito que no es de reciente creación.

- Casinos. A través de este método el delincuente adquiere fichas para participar en los juegos que ofrece el casino con dinero ilegal. Tras realizar varias apuestas solicita al casino que emita un cheque que pruebe que el dinero final proviene de ganancias en el juego.

- Obras de arte. Esta es una buena opción para los delincuentes ya que el valor de los activos no es determinable objetivamente, tiene un alto componente subjetivo, por lo que permite justificar los precios fijados para compraventas.

- Testaferros. Para esta alternativa se emplearán empresas "pantalla", que será una compañía no tiene ninguna actividad mercantil y que será utilizada para "*ocultar movimientos ilícitos aprovechando la cobertura legal de confidencialidad u ocultando a sus verdaderos dueños por medio de una representación nominal*" (noticia aparecida en el diario La Información con fecha 15 Febrero 2016). Los avances tecnológicos que permiten la creación de entramados empresariales de este tipo es aprovechado por los delincuentes, que en numerosas ocasiones se sirven de la ayuda de importantes bufetes de abogados para que les asesoren en el establecimiento del entramado ilegal.

- Operaciones en el mercado de valores. Una de las formas más frecuentes es la "*adquisición de opciones de compra y venta sobre un mismo título a nombre de un mismo cliente que paga con dinero ilícito*". El intermediario pagará la operación que reporte beneficios "*con dinero lícito descontando la*

comisión" y destruye los justificantes de la operación *out of the money* para eliminar sospechas.

- Organizaciones no gubernamentales o sin ánimo de lucro. Estas entidades suelen tener acceso a importantes cantidades de dinero en efectivo, así como la confianza de la sociedad dado su supuesto fin. Estas características son ideales para el blanqueo de capitales, ya que el capital ilícito puede ser justificado como obtenido por medio de donaciones.

- *Initial Coin Offering* (ICO) (ESMA, 2017). Para finalizar, menciono esta forma de blanqueo que se basa en las *criptomonedas* (CNMV, 2018). Tras haber obtenido un capital en *criptomonedas*, como *Bitcoin*, procedente de transacciones ilegales (como, por ejemplo, la venta de cocaína en internet a través de la *deep web*) los delincuentes podrían crear un proyecto basado en *blockchain* para el que requiriesen capital on-line. Pongamos que este capital solo puede ser aportado a través de *Bitcoins*, por lo que introducirían todo el capital procedente de las actividades delictivas entre el capital conseguido de la ICO para la inversión en el proyecto. Así simularía dinero invertido legalmente. A través de los avances tecnológicos, esta vez con el *blockchain*, los delincuentes crean nuevas formas de comisión del delito de blanqueo de capitales.

Como podemos ver, existen numerosas formas que permiten a delincuentes blanquear capitales. Estas alternativas están en constante evolución, principalmente debido a los avances tecnológicos y también a los intentos del legislador de erradicar las formas de blanqueo de capitales más utilizadas de cada época.

Análisis del nuevo surgimiento tecnológico: las *criptomonedas* y el *blockchain*

Debemos destacar la última innovación: la tecnología *blockchain* y las *cryptocurrencies*. Antes de proceder al estudio de ambos, considero oportuno mencionar algunos datos que reflejen la magnitud y la importancia que han adquirido estas divisas (no sólo existe *Bitcoin*, hay cientos de ellas):

- La capitalización de mercado de *Bitcoin*, obtenida en la página "coinmarketcap.com", se sitúa por encima de los 285 mil millones de dólares americanos (con fecha 5/01/2018: $285.491.479.252), pero esta moneda sólo representa el 37% del mercado de *criptodivisas*. La segunda *criptomoneda* más expandida, *Ripple*, se sitúa por encima de los 120 mil millones de dólares americanos. El total del mercado se sitúa (con la misma fecha) en $776.760.044.158. Este dato se puede comparar con el Producto Interior Bruto de Portugal en 2016, 185.180.000.000 €, y es fácil llegar a percibir la magnitud y dimensión de este mercado en auge.
- El periódico inglés *The Telegraph* con fecha 30 de abril de 2017: "*Bank of England plots its own bitcoin-style digital currency*". Lo que significa que el banco de Inglaterra tiene un equipo de analistas estudiando la posibilidad de emitir su propia *criptomoneda* empleando el sistema *blockchain*.

Comencemos el análisis.

Como afirma IG Group Limited en su página web: "*Las criptomonedas son monedas virtuales. Pueden ser intercambiadas y operadas como cualquier otra divisa tradicional, pero están fuera del control de los gobiernos e instituciones financieras*". Existen centenas de monedas digitales, cada una con diferentes propósitos y características, pero todas tienen en común que operan empleando la tecnología *Blockchain*. Es muy importante entender que *Bitcoin* y *Blockchain* son elementos diferentes

¿Qué es y cómo funciona el *Blockchain*?

Para la explicación del funcionamiento de esta herramienta hemos utilizado el análisis de Preukschat et al. (2017), pero también los artículos publicados en el Blog "No creas nada" (Anónimo, 2018) y en Coindesk (Bauerle, 2018). La tecnología *blockchain*, o cadena de bloques, es un libro digital compartido, una base de datos pública, que registra todas las transacciones de una *criptomoneda* determinada entre partes. Funciona a través de una red de ordenadores que dan validez al sistema, ninguna autoridad ni ningún intermediario son necesarios, es una red descentralizada. Su función es muy similar a la que tendrían los libros contables de una empresa, es decir, identificar y almacenar la información de todos los movimientos que se produzcan. La cadena de

bloques está diseñada para que la información que se incluya en ella no pueda ser alterada.

Blockchain es el resultado de décadas de investigación. Esta tecnología no existiría sin el desarrollo de la criptografía (Molero, 2017, citado por BBVA, 2017), entendida como "*el arte de escribir con clave secreta o de modo enigmático*", según la Real Academia Española de la lengua. La criptografía fue inicialmente empleada en el ámbito militar, debido a la gran ventaja que supondría poder comunicarse entre aliados sin que los enemigos pudiesen descifrar los mensajes o, de otra forma, ser capaz de descifrar los mensajes encriptados del enemigo. Esto supondría una ventaja competitiva que podría decidir guerras.

Al hablar de criptografía, merece mención el matemático inglés Alan Turing, considerado el padre y creador de esta ciencia. Entre los méritos que se le atribuyen, destaca su hazaña de descifrar el lenguaje en clave de la máquina "Enigma", que empleaba Alemania en la Segunda Guerra Mundial y que supuso una gran ayuda al bando de *los aliados*.

En su inicio, los gobiernos mantuvieron la criptografía bajo secreto, como herramienta militar. Pero hacia la década de 1970, individuos comenzaron a utilizarla en sus proyectos particulares, tratando de obtener una mayor seguridad. Más concretamente en el año 1976, sale a la luz el Algoritmo Diffie-Hellman, inventado por Whitfield Diffie y Martin Hellman. Con él proponían romper las claves encriptadas en dos: una clave pública y otra privada. La pública se utilizará para encriptar los mensajes, que sólo podrán ser desencriptados mediante la clave privada. Complementaron el invento los americanos Ralf Merkle, con la creación de los Árboles de Merkle; y Ron Rivest, Adi Shamir y Leonard Adleman, creadores del Algoritmo RSA empleado para la generación de claves, el cifrado y el descifrado de mensajes. Así, se produjo el nacimiento de la criptografía de uso particular. Este sistema de encriptación de doble clave es el utilizado actualmente por *Bitcoin*.

En la década de 1990 estos avances no hicieron más que multiplicarse. En 1990 se crea la plataforma *Electronic Frontier Foundation* (www.eff.org), una organización sin ánimo de lucro para defender las libertades civiles en el mundo digital. Entre los valores que protegen se encuentran la libertad de expresión, la privacidad y anonimato o la innovación tecnológica y lo harán principalmente a través del activismo y del

desarrollo tecnológico. De esta plataforma surgirá el *manifiesto cripto-anarquista* de Tim May, que tendrá un importante papel en el tema que nos ocupa. En el texto explican cómo se utilizará la criptografía para desafiar y actuar al margen del Estado, y conseguir la privacidad y libertad necesaria en la Red que permitirá crear un mercado anarcocapitalista. En 1991 Phil Zimmermann lanza *Pretty Good Privacy* (PGP), el primer software de encriptación ampliamente utilizado. Se emplea el nombre de ciberpunk para estas corrientes antisistema que defienden libertad de expresión, de acceso a información y la privacidad *online*.

Estas son las semillas que germinaron en lo que hoy es el *criptomercado*. Aunque no cabe olvidar otros prototipos anteriores a *Bitcoin* como *Digicash* (1989), que no alcanzaron el éxito.

Aunque nos centraremos en el uso del *blockchain* para las *criptomonedas*, es un sistema que se puede emplear con inmensidad de fines, ya que es una plataforma digital en la que se pueden crear una gran cantidad de programas y donde se puede almacenar información de forma ilimitada (Retamal, Roig, & Tapia, (2017).

El elemento principal de la *blockchain* es su peculiar forma de almacenar la información. Las transacciones que hemos mencionado antes se unen en grupos que contienen la información, denominados "bloques". Estos bloques son codificados y vinculados o unidos a la red que forman el resto de bloques. Los bloques de información son emitidos cada cierto tiempo, dependiendo de la *criptomoneda*, por ejemplo *Bitcoin* emite un nuevo bloque cada diez minutos aproximadamente. Los bloques contienen toda la información histórica de las operaciones realizadas con una *criptomoneda*. Además, los bloques están interconectados entre sí. Al estar todos los bloques compartiendo la información, es muy difícil *hackear* el sistema, puesto que aunque se consiguiese alterar la información de un bloque, de forma fraudulenta, el resto de bloques detectarían que esa información ha sido modificada y apartarían ese bloque, sin verificarlo. Además, esto es posible porque la información de los bloques se almacena en miles de ordenadores, en vez de almacenarse solamente en uno. El resultado es un sistema de almacenamiento transparente y casi inmune a ataques cibernéticos, ya que las operaciones no son aceptadas si no son verificadas por la mayoría de la comunidad. Por otro lado, sí que es inmune a modificaciones o a errores humanos o informáticos.

Es muy importante dentro de esta tecnología mencionar lo que es el "minado". Minar es el término que se usa para los procesos de verificación de operaciones con *criptomonedas* y también para el proceso de creación de nuevas unidades de la moneda. Aunque parece algo muy complejo, cualquier persona con un ordenador lo sufrientemente potente y que pueda mantenerlo encendido sin cesar, puede ser un minero. Los ordenadores que realizan el minado se encargan de resolver complejos algoritmos matemáticos, ya que recordemos que las operaciones realizadas en la red están codificadas, para verificar la información de las operaciones con la *criptodivisa*. La solución de los algoritmos es un proceso continuado y que depende también de cómo se resolvieron los algoritmos anteriores y sus resultados para poder realizar el cálculo correctamente. Por otro lado, la complejidad de los algoritmos a resolver es ajustada regularmente para garantizar seguridad y para que el trabajo de los mineros sea constante. La similitud de este proceso de creación de bloques y de unidades de *criptodivisa* con el proceso de extracción de materiales como el oro de minas, hace que lo denominemos minado. Una vez verificada la información se creará un nuevo bloque, que contendrá las nuevas operaciones realizadas, y se introducirá en la cadena en conexión con el resto de bloques. El minado ofrece una recompensa a los individuos que empleen su ordenador para esta función, ya que las *criptomonedas* entregan unidades monetarias a cambio de realizar este proceso. Realizada correctamente, puede ser una actividad muy lucrativa.

El minado resulta una figura muy importante ya que es la manera mediante la cual la red emite nuevas unidades de la moneda. Cuando los mineros resuelven los problemas matemáticos y verifican un bloque, obtienen una recompensa: *Bitcoins*. Esos *Bitcoins* son de nueva creación. Aunque *Bitcoin* tiene un límite máximo de unidades en circulación, no así otras *criptomonedas*.

Se han creado empresas dedicadas exclusivamente al minado, ya que si por el minado de *Bitcoins* te entregan una cantidad de la *criptomoeda*, la cual llegó a tener un precio superior a los 20.000USD, puede llegar a ser un negocio muy rentable. El proceso que siguen estas empresas normalmente es adquirir una alta cantidad de ordenadores muy potentes e instalarse en un almacén en algún lugar del mundo donde la electricidad sea muy barata y donde se pueda hacer ruido. Por otro lado, también es importante que las condiciones climatológicas sean favorables, ya que las tarjetas gráficas de los ordenadores que minan se pueden recalentar al estar en funcionamiento

durante todo el día sin cesar. El principal inconveniente del minado es que el ordenador no puede apagarse, por eso se buscaban los factores mencionados anteriormente. Teniendo en cuenta lo anterior, la mayoría de las empresas o individuos dedicados a esta actividad se instalaron en China (debido al bajo precio de su electricidad y de los costes laborales), pero también otros países como Islandia han resultado interesantes, debido a que el frío ayuda a la refrigeración de los ordenadores.

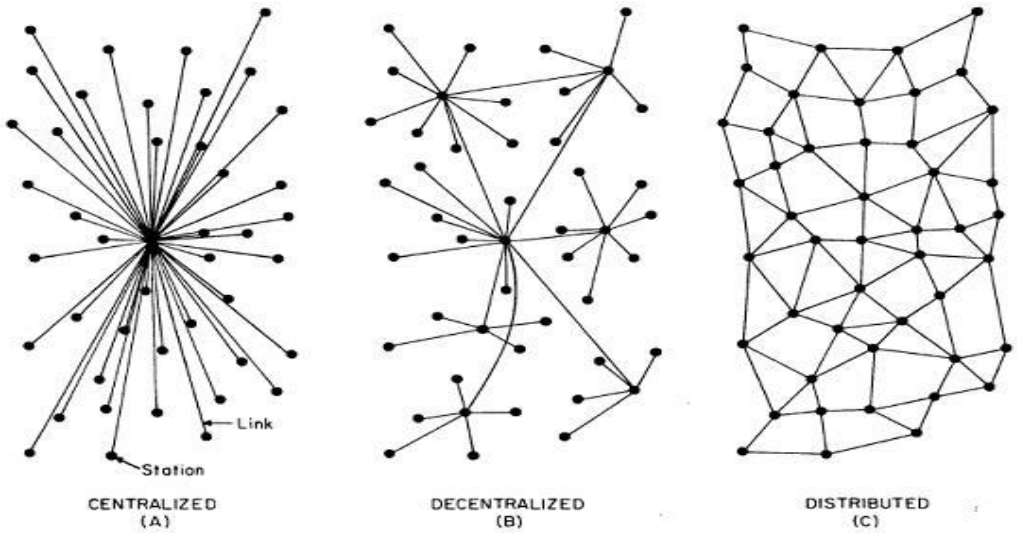
Por lo tanto, el proceso se resumiría de la siguiente forma:

1. El minero crea un nuevo bloque mediante la agrupación de transacciones realizadas con la *criptomoneda*.
2. El bloque es codificado y vinculado a la *blockchain*.
3. El minero obtiene la cantidad de *criptomoneda* establecida.

Es necesario entender quiénes participan en el sistema y cómo lo hacen. Un nodo es un usuario de la red que, básicamente, ha descargado en su ordenador el software necesario para ser partícipe en la red entre partes. En el caso de *Bitcoin*, el software necesario es el *Bitcoin-Qt* o *Bitcoin Core*. Mediante este software el dispositivo almacena y distribuye al resto de dispositivos una copia actualizada en tiempo real de la cadena de bloques al completo.

Una vez que los mineros han completado su función de verificar las transacciones de los bloques, el bloque se añade a la cadena y se comunica a los nodos para que realicen una copia, esto es explicado por Ramos (2014) y por el blog especializado "Oro y Finanzas" (Anónimo, 2017).

La red *Bitcoin* es una red *peer-to-peer* (P2P), lo que significa "de igual a igual". Esto se traduce en que todos los dispositivos integrantes de la red son iguales, no existe jerarquía entre los nodos. Tampoco existe un servidor o un servicio centralizado, pero esto no significa que la red esté descentralizada. La interconexión de todos los nodos por igual resulta en una red de malla de topología plana. La característica principal de este sistema es su resistencia a fallos, ataques informáticos y falsificaciones. En el caso de que un nodo fallase, por cualquier motivo, el resto de nodos perdurarían con la información verdadera y aislarían aquel con la información errónea (Villarreal, 2017).



Fuente: blog.bit2me.com

Aunque todos los nodos son iguales, estos pueden asumir diferentes funciones y tomar un rol más activo en la red, por ejemplo: minería o servicios de monedero.

Criptomonedas: Bitcoin

Estudiaremos la *criptomoneda Bitcoin* por ser la más popular, pero existen muchas otras, de las que mencionaremos datos importantes.

Acudimos a la página web de *Bitcoin* (https://bitcoin.org) a su apartado destinado a resolver dudas y explicar el funcionamiento y propósito de esta *criptomoneda* que ha revolucionado por completo el mercado financiero.

Se define de la siguiente forma: "*Bitcoin es una red consensuada que permite un nuevo sistema de pago y una moneda completamente digital. Es la primera red entre pares de pago descentralizado impulsado por sus usuarios sin una autoridad central o intermediarios. Desde un punto de vista de usuario, Bitcoin es como dinero para Internet. Bitcoin puede ser el único sistema de contabilidad triple existente*". Analizando su definición vemos claro su objetivo, crear un nuevo método de pago que no dependa de ninguna autoridad que pueda actuar de forma arbitraria. Es la creación de un tipo de dinero que sólo se regule por el mercado, por sus usuarios, por la oferta y la demanda.

También conviene citar a Fernández Burgueño (2012), el cual describió esta moneda como "*un bien patrimonial, privado, incorporal, digital, en forma de unidad de*

cuenta, creado mediante un sistema informático y utilizado como medida común de valor por acuerdo de los usuarios del sistema".

El concepto de "moneda criptográfica", denominada *criptomoneda* comúnmente, surge en el año 1998. Wei Dai (1998), un ingeniero informático es considerado el padre de la idea, la cual compartió en las plataformas creadas en la década de 1990 que hemos mencionado antes. La idea era un nuevo tipo de dinero que usase la criptografía y la informática para regularse, eliminando la necesidad de órganos centrales reguladores.

Pero el verdadero paso hacia el nacimiento de *Bitcoin*, y por lo tanto también de las *criptomonedas*, fue la publicación en el 2008 del protocolo *Bitcoin* (Nakamoto, 2008). Este artículo publicado sienta las bases y explica los conceptos iniciales, propone un sistema que se base en una moneda electrónica para realizar pagos electrónicos. Es un dato curioso que la identidad del Sr. Nakamoto es desconocida, se plantea incluso que es un alias bajo el que operan varias personas.

Tras su publicación, el día tres de enero de 2009 se produce el nacimiento de la red con el minado del primer bloque, denominado bloque "génesis", de la cadena. El minado de este bloque supuso una compensación de 50BTCs. Es muy conocida la primera transacción económica que se realizó a través de *Bitcoin*: el pago de dos pizzas a cambio de 10.000BTCs (cuyo valor alcanzó los 200.000.000USD aproximadamente).

¿Cómo funciona Bitcoin?

Bitcoin funciona a través de un sistema técnicamente muy complejo basado en la criptografía. Este sistema es explicado por Capellà, Isern y Mut (2014) en un curso sobre sistemas de pago electrónico en la Universidad Politécnica de Madrid. Los aspectos más importantes son:

- Función de *Hash* Criptográfica. Se trata de un algoritmo que transforma cualquier información que se introduzca en una cadena de bits de longitud fija. Es muy importante que la función sea:
    - Eficiente en la computación (rápida).
    - Resistente a preimagen (difícil generar el mensaje a partir del cual se ha derivado el hash).

    - Resistente a la segunda preimagen (difícil, dado un mensaje, conseguir un segundo mensaje que genere el mismo hash).
    - Resistente a colisión (difícil generar dos mensajes diferentes y que el hash de ellos sea el mismo).
- Firma digital. Se emplea la criptografía de clave pública para, mediante algoritmos, autenticar y verificar los datos de la transacción.
- Los Árboles de Merkle.
- Algoritmo *Hashcash*.

Los creadores de *Bitcoin* establecieron un límite máximo de unidades de la moneda que podían estar en circulación, recopilado por Dirkmaat (2017), este está fijado en 21.000.000 de *Bitcoins*. Pero la *criptomoneda* se puede dividir en una unidad inferior a la que se denomina "*satoshi*", cada *Bitcoin* se puede dividir en 100.000.000 de *satoshis*. La creación anual de unidades de la moneda está programada para que se ralentice con el paso del tiempo y no alcance el límite que hemos mencionado hasta el año 2140 aproximadamente.

Es realmente importante en el funcionamiento de esta moneda el sistema de doble cuenta encriptada para las direcciones (Capellà et al., 2014), pero también la función de los monederos o *wallets*. Estos instrumentos serían el sustituto de una cuenta corriente o de ahorro en un banco. Se trata de archivos protegidos por la criptografía, mediante una clave privada y una pública. La clave pública está compuesta de entre 27 y 34 caracteres y es la clave oficial del usuario, en la cual recibirá las transacciones de la *criptomoneda*. Por otro lado, la clave privada es empleada por el usuario para poder realizar transacciones desde su cuenta. Si no se posee la clave privada no se puede acceder a los fondos de una cuenta. Este mecanismo se conoce comúnmente como criptografía asimétrica.

Todas las transacciones realizadas en *Bitcoin* son públicas y no se pueden eliminar de la *blockchain*. Pero a las transacciones sólo se puede relacionar la clave pública, el propietario de la misma clave no se podrá identificar.

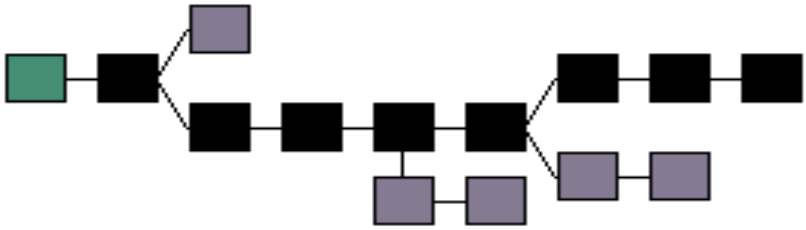
Las transacciones se reflejarán como una transmisión de *Bitcoins* de una dirección a otra. La información está firmada digitalmente y se empleará para adjudicar la nueva propiedad de la *criptomoneda* a la dirección de destino. Puesto que es una red *peer-to-peer* la transacción debe ser confirmada por la red que forman los demás

usuarios, una vez es confirmada se ejecuta. Confirmar la acción significa validarla e incluirla en un bloque de la cadena. Generalmente se necesitan varias confirmaciones de diferentes integrantes de la red, recordemos la minería.

Así es como surgirán los bloques para ser incluidos en la *blockchain*. Las transacciones validadas durante un periodo de tiempo concreto se incluirán en un nuevo bloque, creado por un minero, de transacciones confirmadas y validadas. Los bloques han ido continuamente uniéndose al bloque génesis. No existe un límite máximo de bloques que se vayan a crear, se minarán todos los bloques necesarios para recabar la información de las transacciones que se produzcan. La cadena es almacenada en todos los nodos de la red de forma continuada y en orden cronológico. De nuevo, destacamos que aquí reside la seguridad de *Bitcoin*.

El problema del *double-spending* se soluciona porque una vez que un bloque ha sido añadido a la cadena y todos los nodos tienen una copia almacenada no se puede reprogramar el bloque con una información errónea. Añadiendo a esto, si se va a atacar un bloque intermedio de la cadena será obligatorio para el atacante modificar instantáneamente cada bloque posterior de la misma cadena, ya que los siguientes bloques utilizarán la información que era correcta del anterior para enlazar las siguientes transacciones. Si la información del bloque intermedio ha sido modificada los nodos detectarán este problema. Además, regenerar el bloque intermedio que mencionábamos, más todos los posteriores es computacionalmente inviable en la actualidad.

En la generación de bloques se produce un fenómeno curioso: ¿qué ocurre cuando varios mineros están trabajando en validar un conjunto de transacciones y dos de ellos finalizan en el mismo intervalo de tiempo, con escasos segundos de diferencia generando un nuevo bloque cada uno de ellos? Cuando esto ocurre es porque ha habido muy poco tiempo de separación entre los bloques generados, por lo que los mineros no han detectado que el nuevo bloque ya se había generado. En estos casos, ambos bloques pueden ser válidos y contener la información apropiada, pero sólo uno de ellos integrará la cadena principal. El otro será descartado cuando los nodos comiencen a trabajar en el siguiente bloque de la red, puesto que el bloque que generen lo unirán al primer bloque que recibieron de los dos en disputa. Cuando la cadena continúe sobre uno de los bloques, se habrá producido el descarte del otro, que continuará en la red pero aislado. Este se denominará “bloque huérfano”.



Fuente: Blog “No creas nada”.

El proceso de minado ha sido explicado cuando hablábamos del *blockchain*, pero cabe mencionar algunas particularidades. El minado de *Bitcoins* es el proceso de añadir conjuntos de transacciones a la base de datos pública y compartida de transacciones usando el algoritmo *proof-of-work* a cambio de una recompensa en *Bitcoins*. Los mineros encargados de validar las transacciones e incluir bloques a la cadena reciben una compensación en *Bitcoin*, para compensar sus gastos e incentivar al mercado a realizar esta actividad, ya que si no se generan nuevos bloques *Bitcoin* no existiría. Inicialmente la recompensa por el minado de un bloque era de 50BTCs, pero se estableció que cada 210.000 bloques minados para la red el número de unidades de recompensa se reduciría a la mitad. La recompensa se otorga tras la unión de 100 nuevos bloques al generado, para evitar recompensas a bloques huérfanos. Transcurren unos 10 minutos entre cada bloque minado.

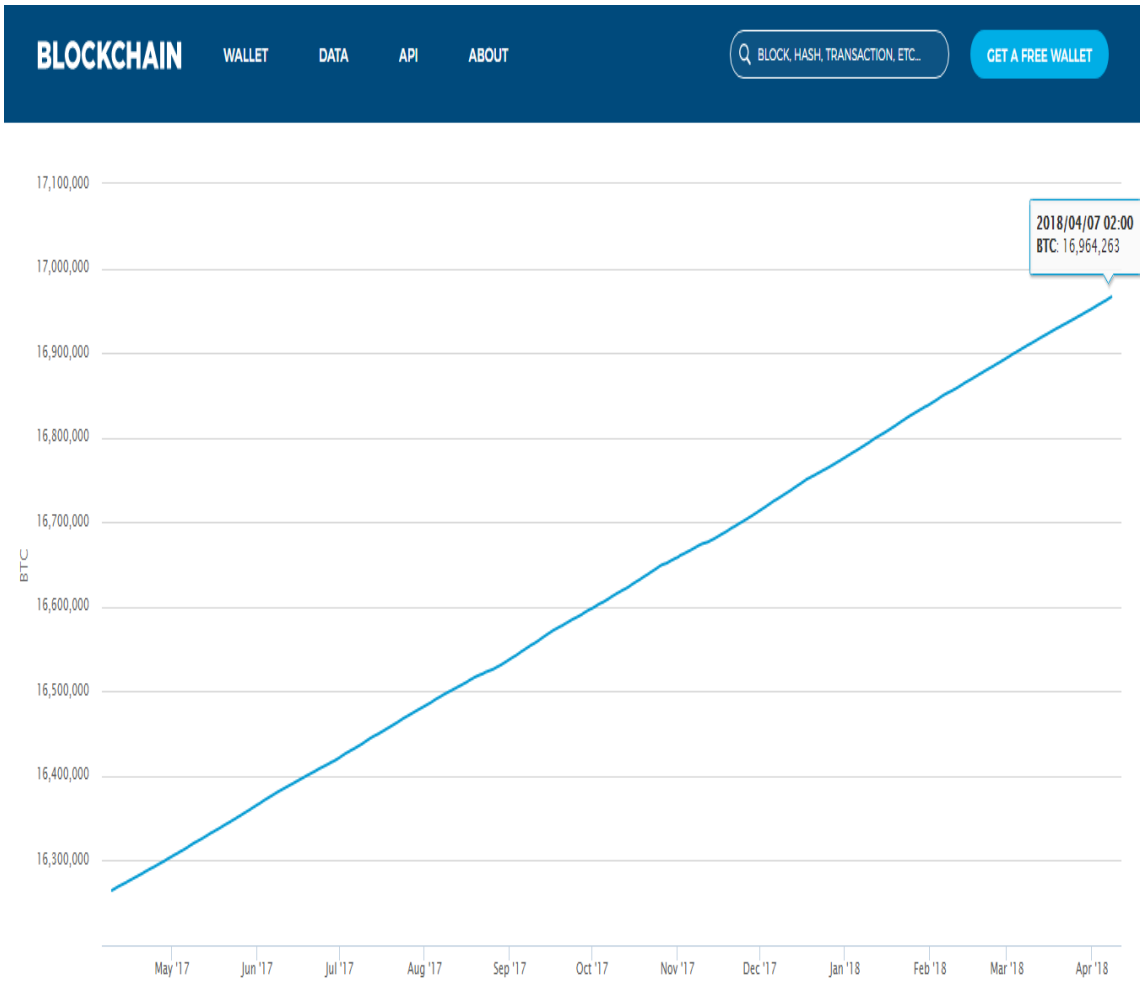
Existen diferentes formas de minar *Bitcoins* (Capellà et al., 2014) que resumimos a continuación:

- *Solo mining*. Un nodo hace minado de forma individual. Esta forma de minado es actualmente inviable debido a que no es competencia para las dos formas que describiremos a continuación.
- *Pool mining*. Los mineros se unen en grupos en los que todos los participantes colaboran aportando sus recursos para resolver un bloque de forma conjunta. Una vez que el pool consigue generar un bloque, las ganancias se reparten proporcionalmente entre todos los participantes del pool en función de los recursos proporcionados.
- *Rig mining*. Un minero o un grupo reducido de mineros operan un conjunto de dispositivos de minería. Generalmente se componen de un gran número de GPUs (*Graphics Processing Units* o Unidades de

Procesamiento Gráfico) o incluso de dispositivos mineros ASIC creados específicamente para la tarea de minado de *Bitcoins*.

Tanto *Bitcoin* como el resto de las *criptomonedas* están ofertadas en *exchanges*, que son intermediarios que prestan servicios de intercambio de monedas. En la mayoría de estos se pueden cambiar las principales divisas de curso legal por *Bitcoins*. Existen *exchangers* que solamente ofrecen servicios de transacción entre monedas digitales.

El 13 de enero de 2018 se completó el minado del 80% del total de *Bitcoins* queexistirán, es decir ya hay 16.800.000 unidades de *Bitcoin* en circulación. Los 4.200.000 *Bitcoins* que faltan por crearse se minarán entre 2018 y 2140.



Fuente: https://blockchain.info/es/charts/total-bitcoins

3. ANÁLISIS CRÍTICO

Ventajas

Vamos a mencionar brevemente las principales ventajas que la revolución tecnológica de la *blockchain* y de las *criptomonedas* aportan a los usuarios y también las ventajas que podrían aportar si se continúa investigando e invirtiendo en esta tecnología (Preukschat, 2017).

- Seguridad. El sistema aporta gran seguridad a las transferencias bancarias mediante el sistema de encriptación de las cuentas. Además la cadena de bloques asegura que las transferencias no sean modificadas.
- Descentralización y autorregulación. Estos atributos permiten a los usuarios e inversores ser los que elijan la dirección del mercado, sin ninguna autoridad superior a ellos que tome decisiones sobre el mercado. La libertad predomina.
- Revolución de monedas como *Rippel XRP* para transferencias bancarias. Es una revolución en cuanto a los costes que se eliminan, tanto monetarios (*fees*) como de conveniencia (tiempo). Transferir euros desde España a cualquier lugar del mundo es ahora mismo muy fácil, barato y rápido. Simplemente habría que realizar un intercambio de euros por *XRP* y transferir esta cantidad desde un *wallet* de *XRP* a otro. La operación se realizará en cuestión de segundos.
- *Smart Contracts.* Este es el proyecto que permite la *criptomoneda Ethereum.* A través de su tecnología se pueden crear contratos entre partes que son válidos y se autoejecutan.
- Almacenamiento y protección de patentes. Si la propiedad intelectual se almacena en *blockchain*, toda la información relativa a la misma, así como la cronología quedará estipulada y será irrefutable ya que los datos introducidos en la red no pueden ser alterados.

Usos para los que se está planteando y que podrían ser beneficiosos:

- Sanidad. El uso del *Blockchain* en ámbito sanitario para almacenar y compartir todos los documentos e historiales clínicos de los pacientes. Esto se haría de forma encriptada para proteger los datos. Pero si se implantase de forma mundial

permitiría una mayor seguridad sanitaria en el extranjero, ay que estos documentos podrían ser observados en caso de emergencia.

- Control Gubernamental. Si se obligase a los gobiernos a utilizar una *criptomoneda* (esta sería de ámbito nacional y su valor estaría igualado al euro, por ejemplo) para todos los pagos y cobros que realice, todos sus movimientos quedarían fijados en la *blockchain* y sería más sencillo controlar el fraude y la corrupción (Blanco, 2017).

Riesgos

Tras haber estudiado esta disruptiva tecnología que puede transformar completamente el mundo de las transacciones y de los contratos, cabe observar también los problemas o riesgos que puede conllevar. Existen ciertas características o aplicaciones, tanto de *Blockchain* como de las *criptomonedas*, para las que estos instrumentos son útiles que ponen en duda si su implementación es beneficiosa.

La CNMV en conjunto con el Banco de España (2018), han emitido una advertencia a todo el mercado alertando de los riesgos que conlleva invertir en activos como *Bitcoin*. Hemos listado los principales riesgos mencionados por la CNMV, pero también otros no especificados por esta entidad y que consideramos importantes. Posteriormente explicaremos aquellos riesgos que tienen relación directa con el delito de blanqueo de capitales.

1. El problema principal es el "anonimato" de los usuarios. Aunque los usuarios no son completamente anónimos, su información está encriptada y es prácticamente inaccesible. El sistema de doble encriptación explicado mantiene las transacciones realizadas por los usuarios accesibles solamente a quien posea la clave de acceso a la cuenta privada.
2. No existe una autoridad que controle el sistema, está descentralizado, provoca que sea ideal su uso para la realización de crímenes como el blanqueo de capitales.
3. Problemas con los operadores de servicios
    a. Robos de monederos.
    b. Pool mining

c. Cambio de divisas por *Bitcoin*
d. Las transacciones no se pueden cancelar.

4. Ordenadores cuánticos.
5. Actual uso puramente especulativo (volatilidad extrema) y problemas de liquidez.
6. Tratamiento por países, prohibición, etc.

Primer Problema: ANONIMATO

En la red *Bitcoin* es el inversor detrás del nodo es anónimo. Sólo se podrá obtener una dirección de muchos dígitos que estará encriptada y no permitirá conocer quién es el titular, ya sea una entidad jurídica o un individuo. Este desconocimiento implica que no se puede gravar una actividad económica y además que no se sabe cuál es el objeto de la transacción que se está realizando (Sasson, Chiesa, Garman, Green, Miers, Tromer, & Virza, 2014). Esto es algo realmente peligroso.

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014, May). Zerocash: Decentralized anonymous payments from bitcoin. In Security and Privacy (SP), 2014 IEEE Symposium on (pp. 459-474). IEEE.

El objetivo de la moneda fue estudiado por el Banco de España en su informe "Divisas o Monedas Virtual: El caso de Bitcoin" (Gorjón, 2012), que llegó la siguiente conclusión: "*Bitcoin nace con ambiciones elevadas: proporcionar a los ciudadanos un medio de pago que posibilite la ejecución de transferencias de valor rápidas, a bajo coste y que, además, no pueda ser controlado ni manipulado por gobiernos, bancos centrales o entidades financieras*". Como podemos observar, la idea de *Bitcoin* era facilitar el comercio y las transacciones financieras y monetarias entre individuos. El problema es que, debido a esa descentralización, es muy difícil controlar el objeto de las transacciones. Esto conlleva que su uso no siempre se haga con fines lícitos.

La agencia policial de la Unión Europea (Europol), estableció en su informe IOCTA (*Internet Organised Crime Threat Assessment,* 2017) que "*bitcoin continúa siendo una vía clave para facilitar el cibercrimen*", pero también añadió que "*otras criptomonedas tales como Monero, Ethereum, y Zcash también están adquiriendo popularidad en la clandestinidad digital*". Observamos un cambio de tendencia, puesto que *Bitcoin* se está utilizando en menor medida con estos fines.

La privacidad de la red *Bitcoin* supone un gran atractivo para personas que estén realizando transacciones y no deseen ser conocidos como autores de las mismas, este patrón es común en aquellos que pretenden realizar acciones delictivas. Es en este punto donde se produce la relación entre las *criptomonedas* y el delito de blanqueo de capitales.

Lo que vamos a tratar a continuación es lo que se conoce como *deep web*. Esto es la parte de la red *online* que contiene material, información y páginas web que no están indexadas en ninguno de los buscadores más populares existentes como pueden ser *Yahoo!* o *Google*.

Sobre todo en los inicios de *Bitcoin* la *criptomoneda* se utilizó en gran medida para fines delictivos (Barrera, 2018; Natour, 2017). Un claro ejemplo de esto fue el de *Silk Road*. Esta web, creada en 2011, actuaba a través de la red TOR (*The Onion Router*), que era un servidor de Internet que permitía a sus usuarios total privacidad y anonimato. Lo hacía a través de una red de comunicaciones distribuida de baja latencia por encima de la capa de internet y a través del cifrado de todos los datos que traficaban en la red. Podríamos establecer una semejanza con *Google*, con el agregado del anonimato y la imposibilidad de rastrear los datos y actividad de los usuarios. *Silk Road* utilizó esta red para crear un mercado en el que se pudiese comercializar todo tipo de productos, incluyendo productos ilegales como drogas (cocaína, cannabis, LSD, etc.), falsificaciones de carnés de identidad o armas (fusiles de asalto, escopetas, etc.). Además, existía la posibilidad de realizar contratos con expertos informáticos para piratear archivos electrónicos o incluso con sicarios y asesinos a sueldo. La plataforma facilitó transacciones por valor de USD1.200 millones. En cuanto a esta web podríamos afirmar que sería como *eBay* pero sin restricciones al comercio, ni siquiera los límites legales. Cabe destacar, que la web empleaba el medio de pago a través de *Bitcoin*, ya que las transacciones económicas corrientes a través de cuentas bancarias serían fácilmente rastreables. Pero además crearon un sistema para que la cuantía de las transacciones se transfiriese en cantidades irregulares y entre diferentes cuentas antes de llegar al destinatario pretendido, para que su rastreo por la red fuese muy complejo (existen operadores en la red que se dedican a ofrecer este servicio, denominados *mixers*). Estos operadores son fácilmente encontrarles en Internet. Observemos un ejemplo: si alguien adquiriese materiales ilegales por valor de USD5.000 en la web, a pagar en *Bitcoin*, no se haría una transferencia directa por esa cantidad exacta de la

dirección del comprador a la del vendedor. Los *mixers* realizarían previamente varias transferencias entre cuentas postizas y con cantidades diferentes antes de realizar la última transferencia con el importe especificado al destinatario. El prestador de este servicio obtendría una comisión del precio total por su servicio. Tras una larga y compleja investigación por parte de las mayores autoridades americanas como la Administración para el Control de Drogas (*Drug Enforcement Administration*) o el Buró Federal de Investigación (*Federal Bureau of Investigation*) consiguieron, supuestamente, averiguar quién era el creador de la web *Silk Road*: Ross William Ulbricht, un americano de Texas. El 2 de octubre de 2013 la web es cerrada por el FBI y Ross Ulbricht fue detenido y puesto ante la justicia norteamericana. El creador de la web fue acusado de hasta siete delitos (entre ellos: blanqueo de capitales, narcotráfico o violación informática) y ha sido sentenciado a cadena perpetua en prisión. Tras estos dramáticos sucesos la cotización de *Bitcoin* se desplomó un 30%, por lo que es fácil ver como de ligado estaba la *criptomoneda* a este tipo de mercado.

La historia de *Silk road* sirve en este trabajo para manifestar cuál era la utilidad que se le había dado a *Bitcoin* inicialmente. Pero este no es el único ejemplo, existen otros como el de *Sheep market*. Aunque no se puede culpar a la red *Bitcoin* del uso inadecuado que hagan sus usuarios, sí que la red actúa como una ventaja para que los delincuentes lleven a cabo su cometido.

Sin embargo, podemos decir que con el cierre de mercados como el de *Silk Road* y la aparición de otras *coins* más seguras y que permiten un mayor grado de anonimato a sus usuarios (*Monero*), el uso de *Bitcoin* con fines ilegales se ha reducido enormemente, o incluso ha desaparecido prácticamente. Hasta el año 2016, aproximadamente, *Bitcoin* continuaba teniendo un uso primordial en el tráfico de drogas (Sánchez, 2015). Esto queda reflejado en el informe IOCTA y en noticias como la publicada en El País sobre la facilidad del proceso de compra de drogas, en el que la mercancía era enviada en un sobre a través de la empresa Correos (Pareja, 2013). Pero actualmente no es así. Ante esto, ¿es necesario prohibir *blockchain* o *Bitcoin*?

Aun así, este problema podría solucionarse con los *tokens* de identidad. Aunque también cabe plantearse si esto es un problema realmente, ya que en caso de utilizarse con fines lícitos simplemente sería un extra de privacidad del que gozarían sus usuarios

y que no perjudicaría los intereses de ningún Estado ni de ninguna entidad ni persona física.

Segundo Problema: BLANQUEO DE CAPITALES

¿Cómo se blanquearía luego ese capital obtenido ilícitamente?

Sin duda está relacionado con el problema anterior, puesto que es el anonimato y la privacidad en la red de las *criptomonedas* lo que permite realizar con relativa facilidad el delito de blanqueo de capitales. También está muy relacionado con el delito los *mixers* que hemos mencionado.

El proceso comienza con la ejecución del hecho delictivo. Tras la realización del delito, mediante el cual el delincuente habrá obtenido unos beneficios económicos, el delincuente tratará de introducir los réditos en el curso legal del dinero, de forma que no levante sospecha para las autoridades que la cantidad monetaria podría proceder de una actividad ilegal. Para esta parte del proceso, los delincuentes se están sirviendo del protocolo *Bitcoin* y de las ventajas que este proporciona para ejecutar este delito. Empleando los denominados *mixers* introducirán el dinero en una cuenta *Bitcoin* y luego lo distribuirán entre numerosas cuentas que parecen de uso legal de forma repetida. Además las cantidades de las transferencias irán variando, simulando que pertenecen a transacciones diferentes. Así conseguirán que se pierda el rastro del dinero blanqueado entre diferentes cuentas, ya que las cuentas en las que se depositará finalmente el dinero serán difícilmente conectables con las que inicialmente introdujeron el dinero obtenido ilegalmente.

A pesar de lo anterior, no es tan sencillo como imaginamos. Inicialmente el mercado estaba libre de regulación y descontrolado, pero actualmente se ha avanzado mucho en la monitorización y fiscalización del mismo. Veamos el caso de España.

Acudiendo a la legislación española, observamos que cualquier persona, física o jurídica, que realice minado de *criptomonedas* está obligada a declarar esta actividad ante la Hacienda Pública. Según la Dirección General de Tributos (consulta V3625-16, de 31 de agosto) el minado de *Bitcoins* no puede someterse al Impuesto sobre el Valor añadido ya que "*no puede identificarse un destinatario o cliente efectivo de la misma, en la medida que los nuevos Bitcoins son automáticamente generados por la red*". Si

bien es cierto que la actividad está exenta del pago del Impuesto al Valor Añadido, aun así tiene que declarar la actividad como sujeta a este impuesto. Por otro lado, observando el modelo 347 de la Agencia Estatal de Administración Tributaria para declaraciones informativas de operaciones con terceros, se obliga a declarar la identidad de clientes o proveedores cuyas transacciones superen los 3.005,06 euros. También, las transacciones que se realicen con personas situadas en el exterior deben siempre declararse al Banco de España. Además, la Administración Tributaria ha declarado su intención de gravar las plusvalías que supuestamente obtengan los inversores por la simple tenencia de *criptomonedas*. Los usuarios deberían declarar como ganancia, al final del ejercicio fiscal, la diferencia entre el valor de mercado y el coste de adquisición de las monedas. Este último planteamiento muestra una posición muy agresiva con respecto a este mercado y puede agravar los problemas, incitando a los inversores en el mercado de *criptodivisas* a buscar soluciones alternativas fuera de la legalidad, donde no estén expuestos a una fiscalidad tan agresiva.

Observemos ahora la tributación en operaciones con *criptomonedas* pero que no sean resultado de minado (De la Cueva y Gómez, 2018), puesto que la legislación cambia en estos casos. Respecto al Impuesto sobre la Renta de las Personas Físicas, los beneficios obtenidos de realizar *trading* con *criptomonedas* tributarán en consideración de "*rentas del ahorro*", como se establece en el artículo 46. b. de la Ley del IRPF. Con respecto al IVA, la normativa cambia drásticamente en su tratamiento, puesto que las acciones de cambio de divisas por *criptomonedas* sí que estarán sujetas al impuesto mencionado (consulta V1029-15, de 30 de marzo).

A continuación estudiaremos los *exchanges*:

Las principales medidas de seguridad, que otorgan confianza a un *exchange* son las siguientes, según el blog especializado "Tecnobits" (Anónimo, 2018):

- Autenticación de dos factores
- Alertas por SMS o correo electrónico
- Correos electrónicos encriptados
- Monitorización de billetera

Se debe también, preferiblemente, utilizar un *exchange* donde haya un alto volumen de negociación entre los usuarios, es decir que haya un gran número de ellos y haya problemas de liquidez.

Los principales y más seguros *exchanges* para hacer *trading* de *criptodivisas*, según el blog especializado "Tecnobits" son:

- Binance. Se trata de una plataforma de reciente creación pero de las mayores del mundo, con sede en Hong Kong. El proyecto comenzó a través de una ICO (*Initial Coin Offering*, véase similar a una IPO), dónde recaudó USD15.000.000 aproximadamente. El CEO (*Chief Executive Officer*) es Changpeng Zhao, un experto en *Blockchain*. Fue Director de Desarrollo en *blockchain*, Cofundador y Director de Tecnología de *OKCoin*, y Fundador y CEO de BijieTech antes de trabajar en Binance.
- Bittrex. Este Exchange es muy interesante ya que está completamente regulado y tiene su base en Estados Unidos. Es imprescindible para las *criptomonedas* que quieren ofertarse en esta plataforma someterse a auditorías para verificar que cumplen los requisitos legales. Bittrex ha afirmado su compromiso de cumplir con todas las leyes y regulaciones requeridas por los organismos gubernamentales de los EE.UU.
- KuCoin. Es otro Exchange que ofrece gran seguridad a los usuarios y que fue fundado por expertos en esta tecnología.
- Cryptopia.
- Poloniex.
- Coinbase. Con sede en San Francisco, es un Exchange y *wallet* digital peculiar, ya que sólo oferta transacciones entre las monedas *fiat* principales y las principales *criptomonedas*. Ha adquirido gran popularidad por acciones como la inversión de €75Mill en 2015 del banco BBVA a través de BBVA Ventures o la reciente adquisición de la licencia *e-money* que emite la *Financial Conduct Authority* en el Reino Unido. Enviaron un comunicado interno a todos sus usuarios vía e-mail en el que mencionaban que "*la licencia permitirá a Coinbase emitir dinero electrónico y proporcionar servicios de pago en toda Europa*".

Vamos a observar el contexto legal de los *exchanges.* Es decir, si los *exchanges* cumplen con la normativa vigente en España. La ley 10 de 2010 de Prevención de Blanqueo de Capitales y de Financiación del Terrorismo es una normativa muy estricta que pretende combatir, siguiendo los principios comunitarios, estos graves problemas.

La Ley obliga a todos los operadores a conocer la identidad de sus clientes, además del origen de los fondos con los que estos están operando. Para comprobar que las entidades cumplen con esta obligación, la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC) exige la elaboración de un informe sobre el cumplimiento de esta normativa por parte de un experto independiente.

La Ley comienza estableciendo los sujetos que están obligados a cumplir con la normativa especificada. En esta lista se encuentran entidades de diferentes ámbitos, como las entidades de crédito, las aseguradoras o los fondos de pensiones.

Seguidamente destacamos algunas de las medidas de diligencia más relevantes que han de adoptar los sujetos obligados (Merino, 2010):

1.- Identificación formal.

- Los sujetos obligados identificarán ***a cuantas personas físicas o jurídicas pretendan establecer relaciones de negocio o intervenir en cualesquiera operaciones****. Sino, no pueden actuar.*

- La comprobación se hará ***previamente*** *y mediante* ***documentos fehacientes****. Provisionalmente, si no hay un especial riesgo, cabe admitir la firma electrónica o un primer ingreso procedente de una cuenta a nombre del mismo cliente, debiendo aportar físicamente el documento fehaciente en un mes.*

- Se determinará ***reglamentariamente*** *qué documentos deben de reputarse fehacientes a estos efectos.*

2.- Identificación del titular real.

- Al respecto, los sujetos obligados recabarán ***información de los clientes*** *para determinar si éstos actúan por cuenta propia o de terceros. Cuando existan indicios o certeza de que los clientes no actúan por cuenta propia, los sujetos obligados* ***recabarán la información precisa*** *a fin de conocer la identidad de las personas por cuenta de las cuales actúan aquéllos.*

- Adoptarán medidas adecuadas al efecto de determinar la ***estructura de propiedad o de control de las personas jurídicas****. Si no puede determinarla, no establecerán o mantendrán relaciones de negocio, especialmente si se*

trata de sociedades cuyas acciones estén representadas mediante ***títulos al portador****.*

- Se hará ***con carácter previo*** *al establecimiento de relaciones de negocio o a la ejecución de cualesquiera operaciones.*

- Se define quién debe de considerarse ***titular real****.*

3.- Propósito e índole de la relación de negocios.

- Los sujetos obligados ***obtendrán información*** *sobre esta materia. En particular, recabarán de sus clientes información sobre la naturaleza de su actividad profesional o empresarial e intentarán comprobar su veracidad.*

- Realizarán un ***seguimiento continuo*** *de la relación de negocios*".

Por otro lado, existen excepciones a estas diligencias, como por ejemplo las operaciones cuyo precio se cifre en menos de mil euros.

Los *brokers* de *criptomonedas* no están explícitamente citados entre los sujetos obligados a cumplir con la normativa de prevención de blanqueo de capitales, sin embargo dada su actividad podrían encajar en más de un tipo de la lista. También, por analogía se les podría incluir en las mismas obligaciones que los *brokers* tradicionales que operan con dinero fiduciario.

Sin embargo, acceder como inversor individual y no corporativo a un *exchange* como Coinbase, por ejemplo, es muy sencillo. El único documento que se solicita es una imagen del DNI o carnet de conducir y más adelante tendrás que indicar la cuenta bancaria desde la que estás haciendo el depósito para cambiar por *criptomonedas*. Si bien se podría decir que la plataforma está cumpliendo con su obligación al solicitar la identidad del inversor mediante un documento oficial, resulta un método no excesivamente seguro. Falsificar un documento de identidad es una acción muy sencilla y que el sistema del *exchange* podría no detectar. Binance, por otro lado, no solicita ningún tipo de documento para crear una cuenta en su plataforma de intercambio de *criptomonedas*. Aunque cabe mencionar que Binance sólo permite operaciones de *trade* entre *criptomonedas*, no acepta intercambios con dinero fiduciario. Esto significa que el capital que se introduzca en esta plataforma ha tenido que ser convertido a *criptomonedas* previamente en otro *exchange*, en el cual sí deberían haber solicitado la identidad del inversor y esto quedaría reflejado en la *blockchain*.

La normativa que hemos mencionado exige a los sujetos obligados realizar unas diligencias para conocer que el origen de los fondos que los clientes están utilizando es lícito y no proviene de ninguna actividad ilegal. Esto no es realizado por los *exchanges*.

Comprobemos todo lo anterior que hemos mencionado con el caso concreto de eToro.

Este bróker es empleado para invertir en acciones de los principales mercados del mundo, en ETFs (*Exchange-traded fund*) e incluso en *criptomonedas*. Aunque ellos se denominan como una "red social de *trading*" por el hecho de que las estrategias de inversión de los usuarios pueden ser copiadas a cambio de una comisión.

El bróker está regulado por las autoridades europeas, por lo que su actuación es plenamente legal y está sometido a la legislación vigente. También aparece regulado en la Comisión Nacional del Mercado de Valores como "*Empresas de Servicios de Inversión del Espacio Económico Europeo en Libre Prestación*". Además, en el apartado de regulación de su página web establece que "*Tanto el Reino Unido como Chipre han aprobado las leyes necesarias y han puesto en marcha una regulación efectiva y otras medidas para establecer los mecanismos adecuados con el objetivo de evitar y eliminar el blanqueo de capitales, actividades de financiación del terrorismo y los delitos financieros. Además, ambos países están comprometidos en la aplicación de todos los requisitos establecidos en los tratados y normas internacionales a este respecto y, de forma específica, los derivados de las Directivas de la Unión Europea. La legislación del Reino Unido y de Chipre se ha armonizado con la tercera Directiva de la Unión Europea para la prevención del uso del sistema financiero para el blanqueo de capitales y la financiación de actividades terroristas (Directiva 2005/60/CE). Como firmas reguladas, eToro Europa y eToro Reino Unido mantienen el compromiso de seguir todas las regulaciones relevantes y de garantizar que se toman todas las medidas adecuadas para combatir el blanqueo de capitales, las actividades de financiación del terrorismo y los delitos financieros*."

Por lo que podemos observar, esta plataforma cumple con la legalidad y opera en términos de cumplimiento con las normas nacionales e internacionales.

Nos surge la duda de cómo cumple un *exchange*, operando con *criptomonedas*, la exigencia de conocer la procedencia de los fondos con los que operan sus clientes.

Pero observamos que las transferencias a estos servidores se hacen con dinero fiduciario y a través de entidades bancarias europeas oficiales y perfectamente reguladas. Estas entidades ya han cumplido su deber de diligencia de estudio y control de los fondos de sus clientes, por lo que no cabría sospechar que el origen puede ser ilícito, de no ser así se habría llegado a esta conclusión con anterioridad. En caso de que las inversiones se produzcan desde terceros países, como China, la regulación que mencionamos no será aplicable.

Los *exchanges* cumplen con la regulación nacional, pero aun cumpliendo con ella presentan grandes déficits de seguridad para sus usuarios y son un riesgo en materia de prevención de blanqueo de capitales.

En este sentido, las plataformas de intercambio de *criptodivisas* establecen límites máximos sobre las cantidades de *criptomonedas* que se pueden extraer del exchange y convertir a dinero fiduciario. Veamos los principales ejemplos:

- Bittrex: 0.4 BTC / day

- Poloniex: $2k / day

- Binance: 2 BTC / day

- Coinbase: los límites varían dependiendo del tipo de cuenta que se tenga (modo de pago asociado, longevidad de la cuenta o transacciones realizadas). Para una cuenta estándar a la que hay asociada una tarjeta de crédito el límite rondaría los 100.000€.

Vemos como los límites son muy bajos, sobre todo para grandes inversores que han depositado cantidades de efectivo importantes. Ante un mercado tan volátil como el que estamos estudiando, no permitir a los inversores extraer en grandes sumas su capital puede resultar en grandes pérdidas. Sin embargo existen excepciones, ya que la mayoría de las plataformas permite la opción a sus inversores de aumentar el "*maximum withdrawal*" si el propietario de la cuenta verifica la misma aportando más información y documentos. En Bittrex el límite aumentaría hasta 100BTC diarios.

El motivo principal por el que los *exchanges* establecen estos límites, según la página web de Coinbase, es por "*security, regulatory compliance, and fraud prevention*". Así observamos como los *exchanges* realmente tratan de eliminar el

blanqueo de capitales de sus plataformas. Es seguro que no lo conseguirán de manera definitiva, al igual que los bancos y demás instituciones financieras, pero no se les puede acusar de no cumplir con la regulación y de ser una herramienta para los delincuentes que quieren introducir capital obtenido ilícitamente en el curso legal del dinero.

En un último punto a mencionar de la legalidad de los *exchanges*, queremos usar el conocimiento de Fernández Burgueño (2012), quien afirmó que los *exchangers* simplemente están prestando un servicio en el que ponen en contacto a sujetos con el deseo de vender un determinado activo y a sujetos con el deseo de comprar ese activo. Por lo tanto, como sujetos ofertantes de servicios la actividad de los mismos está sometida a la fiscalidad del Impuesto sobre el Valor Añadido (21%, en concreto) y su actividad es completamente legal. Este impuesto se aplicará sobre las comisiones que obtenga el prestador del servicio por el trabajo realizado.

Otro aspecto positivo en relación con estos operadores es su colaboración, cuando así son requeridos, con la justicia o las autoridades policiales para luchar contra el fraude y el blanqueo de capitales. Esto se refleja en la noticia emitida por El País, a la que nos referíamos con antelación, en la que se mencionaba la desarticulación una red de narcotraficantes que blanqueaban capitales a través de *Bitcoin* gracias, en parte, a la colaboración del *exchange* en el que realizaban las operaciones.

Si hablamos de blanqueo de capitales o delitos cometidos a través de *criptomonedas* es necesario hablar de *Monero* (*XMR*), una de las que se mencionaba en el informe IOCTA. Esta *criptomoneda* se lanzó en 2014, tras su bifurcación de la *criptomoneda Bytecoin*, que fue la primera en emplear el protocolo *CryptoNote*. Se lanzó sobre la base de ofrecer a los usuarios una posibilidad en el *blockchain* con un mayor grado de privacidad. *Monero* consigue ofrecer este servicio a través de la base del protocolo *CryptoNote*, en lugar del protocolo *Bitcoin*. La peculiaridad de este protocolo es que, aunque también emplea la *blockchain*, no se revela ni el emisor, ni el receptor, ni la cantidad real de la transferencia ejecutada. El único dato que se conoce es que el monto que se refleja de la transferencia será menor al real de la operación.

Los desarrolladores de *Monero* modificaron el código original, introduciendo el algoritmo *CryptoNight* al proceso de minado. Pero lo que permite a esta *criptomoneda* la privacidad absoluta es la tecnología *ring signatures*. Esta tecnología se basa en que a

los sujetos involucrados en una transacción se les adjudican varias firmas criptográficas (direcciones), de manera que para los sujetos ajenos a la transacción es imposible conocer la dirección IP del nodo o la identidad verdaderas de los involucrados. Sólo el emisor y receptor conocen las claves criptográficas verdaderas. Las transacciones de esta moneda son intrazables al completo, así es como se mantiene el anonimato. Como afirma la propia web de la *criptomoneda* (https://monero.org), "*Monero employs a specific protocol which generates multiple unique one-time addresses that can only be linked by the payment receiver and are unfeasable to be revealed through blockhain analysis*".

Monero ocupaba, con fecha de catorce de marzo de 2018, el puesto número doce como *criptomoneda* con mayor capitalización, concretamente USD3.695.525.781 con un precio de USD233,55 por unidad. No cabe duda de que el auge de esta *criptomoneda* está relacionado con su aceptación en diferentes plataformas de la *Deep web*, como *Alphabay* u *Oasis*.

Es preocupante que *criptomonedas* como *Monero* que representan proyectos que proporcionan una gran ayuda a delincuentes estén tan expandidos. Sin embargo, es erróneo afirmar que la generalidad de las *coins* tiene como objetivo ayudar o proporcionar herramientas para delinquir.

El uso de *Bitcoin*, la *criptomoneda* más expandida, con fines delictivos se ha reducido dramáticamente. Esto es debido a diferentes razones, entre ellas destacan que las autoridades son capaces de rastrear los movimientos de las cuentas en colaboración con los *exchanges* o que han aparecido nuevas *criptomonedas* como *Monero* que facilitan en una medida mucho mayor que *Bitcoin*. Como ejemplo tenemos la noticia publicada en el diario El País (Doncel, 2018), en la que se describe una operación de la Guardia Civil española, en colaboración con el Departamento de Seguridad Nacional de Estados Unidos (*Homeland Security Investigation HSI-ICE*) por la que han desarticulado una red de narcotraficantes que blanqueaban capitales a través de *Bitcoin*. Las autoridades han afirmado que "*se ha podido demostrar la bancarización de dinero procedente del narcotráfico por valor de 8.369.867 euros en efectivo, mediante el uso de 174 cuentas corrientes abiertas con la única finalidad de crear una gran estructura de blanqueo de capitales. Dentro de las múltiples metodologías de blanqueo detectadas por parte de los investigadores destacan principalmente el uso de tarjetas de crédito y*

la compra venta de criptomoneda". Pero lo más importante es que las autoridades han sido capaces de rastrear movimientos a través de *Bitcoin*, lo que significa que el delito en estas redes no queda impune. En la noticia también se menciona la importancia que han tenido en la investigación las autoridades de Finlandia, lugar donde el *exchange* estaba situado.

De este último acontecimiento se puede extraer la conclusión de que las *criptomonedas*, a pesar de que redes criminales tratan de emplearlas con fines delictivos, los delitos no pueden ser ocultados y las autoridades son capaces de rastrear los movimientos en el *blockchain*, con la colaboración de los *exchanges*. La delincuencia organizada trata siempre de encontrar nuevas formas de blanquear el capital obtenido de forma ilícita, especialmente mediante la tecnología. Pero, conforme esta se asienta y las autoridades empiezan a conocerla e investigarla son capaces de neutralizar actividades de este tipo. Eventualmente, las *criptomonedas* que realmente tienen proyectos definidos, como *Bitcoin*, *Ethereum*, *Neo* o *Ripple*, no serán empleadas con fines delictivos. Y sí serán utilizadas con este objetivo otras *criptomonedas* cuyo objetivo es prácticamente facilitar estas actividades, como *Monero*.

Tercer Problema: CONFIANZA EN LOS SERVIDORES

EXCHANGES

Hemos estudiado los *exchanges* en su relación con la Ley 10 de 2010, pero veámoslos ahora desde otro punto de vista. Existe un historial muy grande de malas prácticas que han provocado las pérdidas de las inversiones de muchos individuos que habían depositado su dinero en ellos. Algunas de estas son recopiladas por el blog tecnológico "Xataka" (2018) y son las siguientes:

- *Wash trades*. Se trata de operaciones de un operador consigo mismo para crear volumen de transacciones e influir en el precio, esto se denunció en Bitfinex.
- *Spoofing*. Órdenes de compra o venta enormes para simular un momento de optimismo o pesimismo que se cancelan según vaya afectando al precio. Esta práctica se ha denunciado en Coinbase y otros.

- *Painting the tape*. Similar al primero, pero con varios participantes. El inversor Mark Karpelès reconoció ante la justicia que usaba esta técnica en Mt. Gox.
- *Front-running*. Se produce cuando un operador es capaz de introducir su orden de transacción antes que la de los demás clientes en momentos oportunos.

A estos problemas se une una larga lista de robos en *wallets*.

Sin embargo, si acudimos al informe que emitió la *European Banking Authority* el 12 de diciembre de 2013 bajo el título de "*Aviso a los consumidores sobre las monedas virtuales*" (EBA, 2013), se destacan importantes riesgos respecto a los *exchanges*.

En primer lugar, al no estar regulado no es un sistema extremadamente seguro. Aunque podríamos pensar que las plataformas oficiales para realizar transacciones como las entidades financieras también sufren ataques y robos, garantizan los depósitos de sus clientes en caso de que algo como lo descrito pudiese llegar a ocurrir. El caso de las plataformas de intercambio de *criptomonedas* es diferente, ya que no garantizan los depósitos a los que introduzcan monedas tipo *fiat* para intercambiar por *criptomonedas*. Esto conlleva un riesgo alto, ya que el inversor podría perder grandes cantidades de dinero por problemas de seguridad de los que debía encargarse la plataforma digital, a pesar de esto el intermediario no se responsabilizaría de lo ocurrido.

Son múltiples los casos de robos en *exchanges* y monederos que han resultado en pérdidas para los usuarios. De hecho, es afirmado por expertos que los operadores digitales, como los *exchanges* y los *pools* de minado de *criptomonedas*, son el punto débil de esta tecnología y donde se producen los principales problemas. "*Son el punto de fricción entre las divisas de la economía tradicional y los bitcoins*" (Capellà et al., 2014):

- Coincheck. Se produjo un robo en esta plataforma de intercambio por valor de USD530.000.000 en un ataque informático contra su red en enero de 2018 (Shane, 2018). Era el mayor de Japón y uno de los mayores de Asia, se estima que 260.000 inversores, aproximadamente, han sido afectados. En este caso los *hackers* decidieron atacar los depósitos de los inversores de NEM (*New*

Economy Movement), otra moneda digital. Coincheck pidió disculpas a sus inversores y a la comunidad, ya que el robo supuso además un tremendo descenso en el valor de NEM. Un ejecutivo de la organización que sostiene la *criptomoneda* comunicó que estaban muy decepcionados de que los fallos de seguridad de los *exchanges* repercutieran negativamente en los precios de su producto, debido a la pérdida de confianza. Por todo esto, Coincheck anunció que destinarían USD423.000.000 a resarcir parcialmente a los usuarios afectados por el robo.

- Mt. Gox. En este Exchange también se produjo un robo, aquí el ataque concluyó con la extracción de USD400.000.000 en *Bitcoins*. El robo de los 744.408 *Bitcoins*, que eran el 6% de los *Bitcoins* que estaban en circulación en el momento, resultó en la quiebra de la empresa y la pérdida del dinero de los inversores.
- Los anteriores han sido de los robos más significativos que se han producido, sin embargo se han producido decenas de ataques de menor magnitud:
    - BIPS wallet: robo de 1.295 bitcoins.
    - Flexcoin: robo de 896 bitcoins.

Relación con el dinero en efectivo

Continuamos el análisis realizando una comparación de las monedas digitales con el dinero fiduciario en efectivo. Considero que esta comparación va a ser muy útil para entender la complejidad del problema, pero también para mostrar la parcialidad o falta de objetividad con que muchos individuos opinan y critican esta tecnología. No cabe duda de que existen diferencias en el trato que se les da a las *criptomonedas* en comparación con otros medios de pago que nadie considera peligrosos para el estado de bienestar.

El dinero en efectivo es una herramienta muy difícil de controlar ya que no existe ningún intermediario entre las partes involucradas, además no tiene porqué existir ninguna prueba del intercambio. Mientras en las *criptomonedas* todas las transacciones se almacenan en la *blockchain*, con el dinero en efectivo no existe ninguna forma de rastrear las transacciones, especialmente si se trata de pequeñas cantidades. Este hecho

sí que es conocido por el Gobierno de España, que en la página web del Tesoro Público, gestionado por el Ministerio de Economía, Industria y Competitividad, dedica un apartado entero a "Prevención del blanqueo y movimiento de efectivo".

Investigando en la web, el método mediante el cual se pretende controlar el uso del efectivo para la comisión de delitos (entre ellos el blanqueo de capitales, el narcotráfico, etc.) es el siguiente:

> *Todas las personas, por cuenta propia o de tercero, deberán presentar DECLARACIÓN PREVIA, cuando realicen los siguientes movimientos (artículo 34 de la Ley 10/2010):*
>
> *- Salida o entrada en territorio nacional, con medios de pago (billetes, moneda o cheques al portador), por importe igual o superior a 10.000 euros o su contravalor en moneda extranjera.*
>
> *- Movimientos internos, dentro del territorio nacional, con medios de pago (billetes, moneda o cheques al portador), por importe igual o superior a 100.000 euros o su contravalor en moneda extranjera.*
>
> *La omisión de la declaración, o la falta de veracidad de los datos declarados, determinará la intervención de la totalidad de los medios de pago, salvo el mínimo de supervivencia que se determine (hasta 1.000 €).*

Es especialmente interesante el segundo punto que controla los movimientos de efectivo dentro del territorio nacional ya que el límite de 100.000 euros se puede considerar muy elevado. Por ejemplo si se realiza una operación criminal de venta de sustancias estupefacientes ilegales hasta un valor de 50.000 euros el autor podría desplazarse por el territorio nacional transportando las cantidades legales de efectivo. Es cierto que el problema para el traficante vendría luego, a la hora de introducir el capital en el curso legal del dinero de manera que no levante sospecha. Pero el límite aun así se puede considerar que da margen a operaciones ilegales.

Respecto a esto, no podemos hablar de pasividad o permisividad del gobierno ni de la Unión Europea. Se continúa trabajando en esta materia sobre todo siguiendo las directrices del Grupo de Acción Financiera (GAFI), que es el órgano fruto de la cooperación internacional en materia de prevención de delitos a través de entidades

financieras. Recientemente se publicó la 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.

Pero, a pesar de todos los esfuerzos que se realizan, es prácticamente imposible asegurar el control sobre un medio de pago que es irrastreable. Puesto que está hecho de metal o de papel, no incluye ningún dispositivo tecnológico o chip que permita localizar su posición en un determinado momento o conocer su procedencia.

El mejor ejemplo que demuestra el funcionamiento de este tipo de pago es el narcotráfico. Esta actividad que ha estado muy expandida en España, principalmente en zonas como Galicia o Cádiz por su localización geográfica estratégica, cada vez se enfrenta a mayores problemas para continuar su actividad. Sin embargo es imposible acabar con el narcotráfico, a pesar de su prohibición, es categóricamente imposible. Mientras haya sustancias ilegales que un mercado desee consumir y la realización de la actividad reporte muy altos beneficios a sus ejecutores, la actividad no cesará, se encontrará otro camino para llevarla a cabo. Incluso hay Estados, como Singapur o Arabia Saudí, que han optado por penalizar la posesión de drogas con la pena de muerte, tratando de erradicar el problema, y aun así es imposible eliminarlo. Otros, tratando de evitar el blanqueo de capitales y la evasión fiscal, han tratado de eliminar el dinero fiduciario en efectivo de su circulación monetaria, pero este es un paso que solamente se podría tomar en países ricos y con bajas tasas de paro.

La única forma de controlar este problema es mediante la educación a la sociedad de los problemas y desventajas que acarrea el consumo de drogas, pero no mediante la prohibición.

Considero apropiado hacer una referencia a la reseña que realizó Dyanna María Ruíz Uzcátegui, sobre el libro "El mercado de la cocaína en España" de Olmedo Vargas. En este libro el autor analiza el mercado de la cocaína en España, ya que considera que es la sustancia más dinámica y representativa. El autor alcanza varias conclusiones en su trabajo, destaca la "*relación inelástica de la demanda de cocaína frente a los precios crecientes hasta el 2005*". Esto es así por la generalización en el consumo entre los diversos sectores sociales españoles dejando de ser un consumo elitista; que "*se facilitó por una alta capacidad de compra de los salarios de los profesionales y empleados, como por la incorporación masiva de la mujer a las actividades laborales y el auge de*

la economía". Aun así, el mercado de la cocaína en España ha estado reduciéndose paulatinamente desde su punto máximo en 1995, "*principalmente debido a la eficacia del control del Estado español*". También destaca "*una política sobre drogas muy equilibrada, tanto en programas de prevención del consumo como a la política de control a la oferta y la lucha contra el narcotráfico y el blanqueo de capitales*". El autor concluye, también, que "*el mercado español de cocaína es más importante por su naturaleza de puente de transacciones del narcotráfico hacia Europa Central y Oriental que por constituir un mercado de consumidores"* (Ruíz, (2009) citando a Vargas, (2008)).

Ante esto podemos concluir que aunque las autoridades y el Estado quieran velar por la seguridad y el bienestar de los ciudadanos que están bajo su tutela, hay barreras prácticamente intraspasables que el Estado nunca va a poder eliminar. Entre estas barreras está la libertad, la libertad de los ciudadanos para tomar decisiones sin ser observados por el Estado. Por esto, es imposible controlar en qué se gastan los ciudadanos el efectivo que poseen legalmente.

El narcotráfico no va a dejar de existir, y el efectivo o las *criptomonedas,* por la libertad que permiten a sus poseedores seguirán siendo las mejores opciones para realizar intercambios o para blanquear el capital obtenido de actividades ilegales.

Es en este momento cuando nos preguntamos ¿no es posible que estemos enfocando el problema erróneamente? ¿No es posible que el problema sea la prohibición? Es cierto que se ha reducido mucho el consumo de sustancias ilegales, pero ¿y si se legaliza? Así, al menos, se acabaría con el problema del blanqueo de capitales en su mayor parte. No olvidemos que el delito de blanqueo de capitales existe única y exclusivamente porque previamente se ha producido un hecho criminal del que unos individuos han obtenido un rédito económico. Si el delito inicial no se produjese, no se trataría de blanquear capitales.

Ante esta situación, la legalización de ciertas drogas (que se unirían a las ya legalizadas y muy perjudiciales drogas como el alcohol y el tabaco) y de la prostitución, siendo capaces de controlar el mercado para ofrecer seguridad tanto a los oferentes como a los consumidores, podría suponer una mejora radical en la reducción del delito de blanqueo de capitales. Por supuesto, esta no es una decisión sencilla, ya que implica

conflictos morales y de dignidad, además no debe tomarse teniendo en cuenta exclusivamente objetivos económicos.

4. POSIBLES MODIFICACIONES

En este apartado, tras haber analizado los riesgos que presentan las *criptomonedas*, queremos estudiar opciones que modificasen el sistema actual y lo hiciesen más transparente y seguro.

Se ha analizado un problema complejo de controlar, debido a su novedad y al uso que hace de la tecnología. Además, se ha explicado como la mayoría de los *exchanges* que operan en nuestro país cumplen con la normativa legal actual, por lo que el problema es de ese. Nos vamos a centrar en posibles soluciones para la prevención del blanqueo de capitales a través de este nuevo método de inversión. Aunque también se tratará de proponer alguna solución de mejora del sistema *blockchain* y de algunas *criptomonedas*.

Primera Opción: *Tokenización* del mercado

Esta solución está basada en la "*tokenización*" (Aru, 2017). La *tokenización* es "*una parte intrínseca de la tecnología blockchain que sirve al propósito de identificación y accesibilidad de la plataforma*". Todas las plataformas en *blockchain* emplean *tokens*, pero para *criptomonedas* que representan medios de pago como *Bitcoin* o *Litecoin* se suelen denominar *coins*, en vez de *tokens*. Pero los *tokens* tienen usos muy numerosos y diversos, diferentes de la mera representación monetaria. Uno de ellos es el almacenamiento, protección y presentación de información. Cualquier tipo de información puede incluirse en la cadena de bloques, ya sean datos personales, propiedad intelectual o *smart contracts*.

Con referencia a lo anterior, asistí a una conferencia en el Instituto de Empresa de Madrid sobre esta tecnología, donde uno de los ponentes era el Sr. Garrido, notario de profesión. Este mencionó el gran problema que suponía esta tecnología para el combate del blanqueo de capitales, por los motivos explicados previamente. Pero propuso una solución, que puede no ser definitiva, pero sí un avance. Afirmó que se podrían utilizar *tokens* en *blockchain* como herramientas para almacenar la información de los usuarios, a modo de identificación oficial, con sus datos personales, que permitan a las plataformas digitales de almacenamiento e intercambio de *criptodivisas* disponer de esa información. Es decir, en vez de *tokens* de contenido económico, *tokens* de

contenido informativo e identificativo. Cada usuario del sistema tendría un *token* que le representase únicamente a él, por lo que las operaciones económicas quedarían registradas y representarían a un usuario del sistema. A consecuencia de esto, se podrían adjudicar las operaciones a un individuo y exigirle la debida aportación mediante impuestos en caso de que sea necesaria.

El sistema funcionaría mediante el establecimiento de una exigencia por parte de los *exchanges* y los *wallets* a sus usuarios, esta exigencia no sería otra que el usuario deberá haber adquirido previamente un *token*. El *token* se crearía empleando *blockchain*, programando la información del usuario del *token* y adjudicándola al sistema de doble cuenta para las claves encriptadas. La información del *token* permanecerá encriptada, lo que hará que los datos de los usuarios sean secretos, cumpliendo además con la Ley de Protección de Datos. Sin embargo, al estar todos los usuarios correctamente identificados mediante los *tokens*, en casos donde fuese necesario, las autoridades podrían acudir a estos *tokens* y eliminar el problema del anonimato. Esta información sólo podría solicitarse por las autoridades en casos de alta sospecha delictiva. Por otro lado, al almacenarse la información de todos los usuarios en la *blockchain* esta permanece segura e inalterable.

El proceso comenzaría con la creación del *token* digital personal. Para este servicio se podrían definir una o varias empresas tecnológicas que se especialicen en *blockchain* y que se dediquen a la creación de *tokens* que almacenen información. El *token* de identidad contendría una serie de carpetas donde se incluirán los documentos requeridos para poder operar en transacciones financieras. Los documentos variarán dependiendo de quién sea el inversor, y es que el inversor puede ser una persona física o jurídica. En caso de ser una persona física se incluirían archivos con información como el Documento Nacional de Identidad, la cuenta bancaria, direcciones de correo electrónico y residencia. Por otro lado, en caso de ser una persona jurídica, incluiría los estatutos, las identidades de sus socios o dónde está basada la empresa. En cualquier caso, todos los documentos estarían encriptados y sólo serían accesibles para aquellos a los que el propietario de la cuenta concediese autorización.

La entidad o plataforma encargada de gestionar los obligatorios *tokens* de identificación podría ser de carácter público o privado. Si fuese de corte gubernamental el control sobre el proceso estaría asegurado y las autoridades podrían aumentar su

efectividad directa contra el blanqueo de capitales. Sin embargo, no debería ser estrictamente necesario, puesto que una entidad privada también podría realizar esta gestión mediante un algoritmo en el *blockchain*. Esto es así puesto que los documentos necesarios que se deberán incluir en el *token* tendrán confirmación notarial, y ante esta figura los gobiernos no tienen poder. Basándose en la personalidad semipública del notario el algoritmo podría comprobar si los documentos han sido verificados.

La única posibilidad de que este método llegue a aplicarse y resulte en efectos positivos para Hacienda es la regulación, la imposición de esta exigencia a los operadores de plataformas digitales de almacenamiento e intercambio de *criptomonedas* y monedas *fiat*. El legislador, mediante la creación de una norma que regule específicamente este sector podría obligar a esta tecnicidad a los sujetos implicados. La única forma de modificar el actual funcionamiento del *criptomercado* hacia una tendencia más controlable es mediante la regulación y la presión de los gobiernos, ya que precisamente esta tecnología se creó para huir del control y la vigilancia de entidades gubernamentales.

Esta posibilidad podría funcionar, pero no estaría libre de problemas. Por ejemplo, sería complicada la repartición de los *tokens*. Concretamente la supervisión de su adquisición presentaría ciertos problemas, ya que si se cometen errores en la misma el sistema fallaría. Debería tener la máxima transparencia para evitar corrupciones que otorgasen *tokens* falsos a delincuentes para operar en la red.

Segunda Opción: Prohibir las *criptomonedas*

Son numerosos los gobiernos, a nivel internacional, que han contemplado esta posibilidad o alternativas similares como la prohibición del minado en su país.

Esta posibilidad no es muy inteligente, por el simple hecho de que no va a funcionar. Por el mismo hecho que la prostitución o el tráfico de drogas, aun prohibidos, continúan operando en el mercado español sin “ningún” problema. Con las *criptomonedas* también ocurriría de esta forma ya que internet permite formas de movilidad en la red que no dejan huella y son irrastreables, como la red *TOR*.

A pesar de esto, cometemos un error si consideramos la prostitución o el tráfico de drogas como similares a un activo legítimo como las *criptomoendas*. No hay que

olvidar que *exchanges* que comercializan con estas monedas digitales han obtenido licencias para operar de países como el Reino Unido.

Tercera Opción: Observar la evolución

Esta opción sería equivalente a no realizar ningún tipo de actividad regulatoria o prohibitiva en el momento. Consistiría en una monitorización de la evolución del mercado para, en el futuro, actuar habiendo analizado la suficiente información.

Existen otras opciones que también se podrían estudiar, pero hemos decidido destacar estas por su claridad.

5. CONCLUSIONES

El análisis del delito de blanqueo de capitales y de las *criptomonedas* nos ha llevado a alcanzar las siguientes conclusiones:

- Las *criptomonedas* son indudablemente una respuesta del mercado a los excesos de los gobiernos en materias de regulación y de burocracia. También son una respuesta a los Bancos Centrales de todo el mundo que controlan el mercado económico a su gusto, lo que es considerado injusto y un abuso de poder que no es de agrado para muchos para muchos inversores. Puesto que surgen para combatir este problema ¿la solución es asfixiar esta tecnología con más regulación y prohibición? No. La regulación actual ya incluye y somete a las *criptomonedas* y a los *exchanges* que las ofertan. No podemos olvidar que hay excepciones a la norma general, como sería el caso que mencionamos de la moneda digital *Monero*. Pero esto no nos puede llevar a obviar el verdadero potencial del *blockchain* y de otras *criptomonedas* que verdaderamente presentan proyectos que podrían mejorar nuestra sociedad.
- En caso de que las autoridades consideren que sea absolutamente necesario continuar regulando, la posible imposición de la *tokenización* que favoreciese la identificación de los inversores podría permitir mayor seguridad. Los usuarios continuarían operando de forma anónima, pero todas las cuentas estarían verificadas y no existirían usuarios actuando de forma fraudulenta sabiendo que no van a poder ser identificados.
- Las *criptomonedas* no se emplean exclusivamente con el objetivo de blanquear capitales. Al igual que con la mayoría de avances tecnológicos, los delincuentes tratan de encontrar nuevas formas de delinquir, pero este no es el objetivo de *blockchain* o las *criptomonedas*. Es muy importante destacar el descenso o casi extinción del uso de *Bitcoin* tanto para blanquear capitales como para delinquir. Habiéndose producido esta tendencia no parece razonable la desconfianza generalizada por parte de las instituciones y de los medios de comunicación en su uso. La desconfianza y la futura regulación debe encaminarse frente a aquellos proyectos que empleen esta tecnología para deliberadamente desestabilizar nuestro sistema (*Monero, Silk Road*, etc.) y no frente aquellos que simplemente ofrecen otras alternativas al sistema actual.

- *Criptomonedas* como *Ripple XRP, Ethereum, Bitcoin* o *Neo* han demostrado que aportan valor y que pueden mejorar las condiciones del mundo financiero y contractual para aquellos que los usen. También existen muchos proyectos de contenido ajeno al mundo económico y que podrían ser revolucionarios en la facilidad y eficiencia del almacenamiento de información.
- No existe un vacío legal en el tratamiento jurídico de las *criptomonedas*. Tanto desde un punto de vista fiscal, así como preventivo en materia de blanqueo de capitales, la legislación actual somete este mercado.
- Los *exchanges* en los que se intercambian las *criptomonedas* cuentan con las licencias legales necesarias para poder operar en el mercado, como lo hacen los *exchanges* o *brokers* que ofertan acciones de empresas cotizadas. Y el único motivo por el que han sido otorgados las licencias requeridas es porque cumplen los requisitos necesarios para ser una plataforma comercializadora de este tipo de activos. Observando la Ley 10/2010 vemos que se deben ajustar a esta normativa.
- Los problemas y riesgos que hemos mencionado que esta nueva tecnología supone para nuestra sociedad y nuestro bienestar son solucionables, pero se necesita experiencia y que el *criptomercado* continúe evolucionando y mejorando. En este aspecto ha resultado muy útil comparar las monedas digitales con el dinero en efectivo, puesto que comparten características como la irrastreabilidad (además, esta característica es presunta, ya que todas las operaciones realizadas con *criptomonedas* se quedan almacenadas en la cadena de bloques y no se pueden borrar ni modificar).
- Resulta evidente que el mercado no se puede eliminar mediante la prohibición. Habiendo entendido como funciona la red *TOR* podemos concluir que los usuarios siempre van a poder acceder a plataformas de intercambio de *criptomonedas* sin que los gobiernos tengan conocimiento de ello. Por esto la solución no debe ser la prohibición, ya que esta no iba a solucionar nada.
- Es fácil comparar la situación actual del mercado de monedas digitales con el inicio de internet y de las empresas tecnológicas que se basaron en esta tecnología para prestar sus servicios. Al comienzo parecía una tecnología innovadora, una revolución que podría modificar nuestro modo de vida y también ser un peligro para la recaudación del Estado o por los contenidos a los

que todo el público podría acceder. Sin embargo, de todos los proyectos que surgieron, sólo los más fuertes y los que realmente aportaban valor a los consumidores e inversores son los que han sobrevivido (Facebook o Google).

- El blanqueo de capitales es el delito que penaliza al que trata de introducir un capital obtenido de forma ilegal en el curso legal del dinero. Podríamos pensar que es más importante tratar de eliminar los delitos previos para que no haya delitos de blanqueo. Con esto me refiero a las posibilidades de legalización de las drogas o de la prostitución, ya que son los mercados que más dinero "negro" generan. Aunque es un tema en efecto muy polémico y que no se limita a aspectos económicos, sino que también hay que valorarlo ponderándolo con la ética, la salud o la dignidad de las personas. Pero, las *criptomonedas* surgen como un ansia de libertad, como una necesidad de privacidad frente al control del Estado y puede que esto sea lo que ahora necesita la sociedad. La despenalización de las actividades mencionadas provocarían que el *criptomercado* no se emplease para blanquear o esconder el capital proveniente de esos crímenes.

BIBLIOGRAFÍA

Alemán Alonso, J. J. (2013). *De la sociedad del riesgo al desmantelamiento del estado de bienestar*, pp 145-147. Instituto de Filosofía del CCHS-CSIC.

Álvarez Pastor, M. (1997). *La prevención de blanqueo de capitales*. Madrid: Marcial Pons.

Aru, I. (2017). *Tokenización: la fuerza detrás de la tecnología Blockchain*. Consultado en https://es.cointelegraph.com/news/tokenization-the-force-behind-blockchain-technology por última vez el 11/04/2018.

Banco de España y CNMV. (2018). *Comunicado conjunto de la CNMV y del Banco de España sobre "criptomonedas" y "ofertas iniciales de criptomonedas" (ICOs)*. Consultado en https://www.cnmv.es/loultimo/NOTACONJUNTAriptoES%20final.pdf por última vez el 01/06/2018.

Barrera, S. (2016). *Así utilizan los cibercriminales el Bitcoin para blanquear el dinero procedente de un delito.* Consultado en http://www.tecnoxplora.com/internet/ciudad-con-ley/asi-utilizan-cibercriminales-bitcoin-blanquear-dinero-procedente-delito_2016040557fd332b0cf2fd8cc6b1fb55.html por última vez el 25/03/2018.

Bauerle, N. *How Does Blockchain Technology Work?* Consultado en https://www.coindesk.com por última vez el 09/04/2018.

BBVA. (2017). *De Alan Turing al 'ciberpunk': la historia de 'blockchain'*. Consultado en https://www.bbva.com/es/historia-origen-blockchain-bitcoin/ por última vez el 01/05/2018.

BBVA. (2015). *BBVA Ventures invierte en Coinbase, la plataforma líder de Bitcoin*. Consultado en https://www.bbva.com/es/bbva-ventures-invierte-en-coinbase-la-plataforma-lider-de-bitcoin/ por última vez el 11/04/2018.

Blanco, O. (2017). *Blockchain en la Administración Pública: La Internet de las Transacciones*. IBM. Consultado en https://www.ibm.com/blogs/think/es-es/2017/11/20/tecnologia-blockchain-administracion-publica/ por última en el 11/04/2018.

Blog de Registradores de España. *Las 3 fases del blanqueo de capitales: colocación, encubrimiento e integración.* Consultado en http://registradores.org/blog/fases-del-blanqueo-de-capitales/ por última vez el 01/04/2018.

Braslavsky, G. *Qué son los paraísos fiscales*. Disponible en http://www.forodeseguridad.com/artic/discipl/disc_4011.htm consultado por última vez el 16/04/2018.

Coinbase. Licencias legales. Consultado en https://coinbase.com/legal/licenses por última vez el 25/04/2018.

Comisión Nacional del Mercado de Valores. (2018). *Consideraciones de la CNMV sobre "criptomonedas" e "ICOs" dirigidas a los profesionales del sector financiero*. Consultado en https://www.cnmv.es/loultimo/comunicadoCNMV_ICO_ES%20final.pdf por última vez el 01/06/2018.

Comisión Nacional del Mercado de Valores. (2017). *ESMA alerta de los riesgos de las denominadas "ICO".* Consultado en https://www.cnmv.es/portal/verDoc.axd?t={d1d37c47-84fd-4a9b-8251-3186085e0c86} por última vez el 02/06/2018.

Dai, W. (1998). *B-money*. Consultado en http://www.weidai.com/bmoney.txt por última vez el 05/06/2018.

De la Cueva González-Cotera y Gómez Barrero. (2018). *La tributación del bitcoin y las criptomonedas en las personas físicas*. Consultado en http://www.elderecho.com/contenido_juridico/consultas_legales/bitcoins-tributacion-fiscalidad-criptomonedas-impuesto_11_1194430001.html por última vez 29/03/2018.

Dirección General de Tributos. (2015). *Sujeción al Impuesto sobre el Valor Añadido de la compra y venta de la moneda electrónica Bitcoin. Derecho a la deducción*. Consulta V1029-15, de 30 de marzo.

Dirección General de Tributos. (2016). *Sujeción al Impuesto sobre el Valor Añadido del minado de Bitcoin. Derecho a la deducción*. Consulta V3625-16, de 31 de agosto.

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.

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, así como sobre la supervisión prudencial de dichas entidades.

Directiva 2005/60/CE del Parlamento Europeo y del Consejo, de 26 de octubre de 2005, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo (Texto pertinente a efectos del EEE).

Dirkmaat, O. (2017). *Las limitaciones del bitcoin*. Consultado en https://www.libremercado.com por última vez el 09/04/2018.

EBA. (2013). *Aviso a los consumidores sobre las monedas virtuales*.

EFE. (2014). *Bankinter invierte en Coinffeine, una empresa española de tecnología bitcoin*. Expansión. Consultado en http://www.expansion.com/agencia/efe/2014/11/17/20125407.html por última vez el 01/04/2018.

España Alba, V. M. (2016). *Criptodivisas: Bitcoin y el blanqueo de capitales.* Consultado en http://www.elderecho.com/tribuna/penal/Criptodivisas-Bitcoin-blanqueo-capitales_11_935305002.html por última vez el 11/03/2018.

EToro. Licencias legales. Consultado en https://www.etoro.com/es/customer-service/regulation-license/ por última vez el 10/05/2018.

EUROPOL. (2017). *Internet Organised Crime Threat Assessment (IOCTA).* Consultado en https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017 por última vez el 01/06/2018.

Eyal, I., & Sirer, E. G. (2014). *Majority is not enough: Bitcoin mining is vulnerable*. In International conference on financial cryptography and data security (pp. 436-454). Springer, Berlín, Heidelberg.

Fernández Burgueño, P. (2012). *12 cosas que deberías saber antes de usar bitcoins (La Ley y el Bitcoin).* Consultado en https://angeldelsoto.com/blogs/noticias/16190463-12-cosas-que-deberias-saber-antes-de-usar-bitcoins-la-ley-y-el-bitcoin por última el 01/06/2018.

Ferruz, L., Rivas, F. J. (2017). *La burbuja de las criptomonedas: el caso del bitcoin.* Expansión. Consultado en www.expansion.com/opinion/2017/11/17/5a0f0f8b22601d1c268b45a9.html por última vez el 20/05/2018.

Franco, P. (2014). *Understanding Bitcoin: Cryptography, Engineering and Economics*. Wiley Finance Series.

Galindo, J. C. (2017). *La Corrupción dilapida el Estado de Bienestar*. Consultado en worldcomplianceassociation.com por última vez el 29/03/2018.

Gorjón, S. (2014). *Divisas o Monedas Virtual: El caso de Bitcoin.* Banco de España.

Hanke, S. (2014). *Friedman and Hanke on Bitcoin*. CATO Institute.

IG Group Limited. *Que son las criptomonedas*. Consultado en https://www.ig.com/es/invertir-en-criptomonedas/que-son-las-criptomonedas por última vez el 28/05/2018..

Jeffrey, S. (2015). *Bitcoin and modern alchemy: in code we trust*. Journal of Financial Crime, 22: 2, pp. 156-169.

Krugman, P. (2013). *Bitcoin is evil*. The New York Times. Consultado en https://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/ por última vez el 02/06/2018.

La Información. (2016). *25 formas de "cazar" a un blanqueador de capitales*. Consultado en https://www.lainformacion.com por última vez a 01/04/2018.

Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. Boletín Oficial del Estado.

Martínez, O. (2016). *Bitcoins y prevención de blanqueo de capitales*. Expansión. Consultado en http://www.expansion.com/juridico/opinion/2016/09/29/57ed56ff468aebfe2d8b4629.html por última vez el 25/03/2018.

Mendick, R. (2017). *Bank of England plots its own bitcoin-style digital currency.* The Telegraph. Consultado en https://www.telegraph.co.uk/news/2017/12/30/bank-england-plots-bitcoin-style-digital-currency/ por última vez el 30/03/2018.

Merino Escartín, J. F. (2010). *Resumen sobre la Ley de Blanqueo de Capitales y Financiación del Terrorismo*. Consultado en www.notariosyregistradores.com por última vez el 29/04/2018.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

Natour, L. (2017). *El bitcoin, ¿la moneda de los cibercriminales?* Consultado en http://www.abc.es/tecnologia/redes/abci-bitcoin-moneda-cibercriminales-201706021218_noticia.html por última vez el 05/04/2017.

No creas nada. *¿Cómo funciona Blockchain?* Consultado en https://www.nocreasnada.com por última vez a 09/04/2018.

Oro y Finanzas. (2017). *¿Qué es un nodo en Bitcoin?* Consultado en https://www.oroyfinanzas.com por última vez a 05/04/2018.

Pagliery, J. (2014). *Bitcoin and the future of money*. Vol. 1. Chicago, Illinois: Triumph Books LLC.

Pareja, P. (2017). *Se compra por Internet, llega en un sobre a casa*. Consultado en https://elpais.com/sociedad/2013/09/17/actualidad/1379450268_266579.html por última vez el 10/04/2018.

Pastor, D. Á., & Palacios, F. E. (2007). Manual de prevención del blanqueo de capitales. Marcial Pons.

Payeras Capellà, M. M., Isern Deyà, A. P., Mut Puigserver, M. (2014). *Introducción a Bitcoin*. Curso sobre Sistemas de Pago Electrónico. Lección 3. Universidad Politécnica de Madrid. Disponible en: http://www.criptored.upm.es/crypt4you/temas/sistemaspago/leccion3/leccion03.html.

Preukschat, P. (2017). *Blockchain: la revolución industrial de internet*. Barcelona: Ediciones Gestión 2000.

Preukschat, P. (2017). *Las ventajas del Blockchain para el comercio online, el método que ha cambiado la forma de comprar.* El Economista. Consultado en http://www.eleconomista.es/empresas-finanzas/noticias/8296264/04/17/Las-ventajas-del-Blockchain-para-el-comercio-online-el-metodo-que-ha-cambiado-la-forma-de-comprar.html por última vez el 10/04/2018.

PWC. *Making sense of bitcoin, cryptocurrency, and blockchain.* Consultado en https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html por última vez el 05/04/2018.

Ramos Taboada, F. (2014). *Bitcoinomics: ¿puede un sistema bancario de reservas fraccionarias funcionar dentro de la comunidad Bitcoin?*.a

Ruíz Uzcátegui, D. M. (2009). Reseña "El mercado de la cocaína en España" de Olmedo Vargas. *Aldea Mundo*, *14* (28), 133-133.

Real Academia Española. (2017). *Diccionario de la Lengua Española*. 23ª Edición. Madrid.

Retamal, C. D., Roig, J. B., & Tapia, J. L. M. (2017). *La blockchain: fundamentos, aplicaciones y relación con otras tecnologías disruptivas*. Economía industrial, (405), 33-40.

Sánchez Castrillo, Á. (2015). *Veinte gramos por un 'bitcoin'*. Consultado en https://www.infolibre.es/noticias/mundo/2015/07/17/veinte_gramos_por_bitcoin_35578_1022.html por última vez el 10/04/2018.

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014, May). *Zerocash: Decentralized anonymous payments from bitcoin*. In Security and Privacy (SP), 2014 IEEE Symposium on (pp. 459-474). IEEE.

SEPBLAC. Prevención del blanqueo de capitales y de la financiación del terrorismo (normativa nacional) Consultado en https://www.sepblac.es/es/normativa/prevencion-del-blanqueo-de-capitales-y-de-la-financiacion-del-terrorismo/.

Shane, D. (2018). *Un robo de criptomonedas por 530 millones de dólares puede ser el más grande de todos*. CNN Money. Consultado en http://cnnespanol.cnn.com/2018/01/29/robo-criptomonedas-coincheck-asia-japon/ por última vez el 11/04/2018.

Tesoro Público. Prevención del blanqueo y movimiento de efectivo. Consultado en http://www.tesoro.es/prevencion-del-blanqueo-y-movimiento-de-efectivo.

Tondini, B. M. (2009). *Blanqueo de capitales y lavado de dinero: Su concepto, historia y aspectos operativos*. Centro Argentino de Estudios Internacionales.

Vigna, P. y Casey, M. (2014). *The age of cryptocurrency: How bitcoin and digital money are challenging the global economic order*. New York: ST. Martins Press.

Villarreal, G. L. (2017). *Blockchain (no todo lo que brilla es Bitcoin)*.