

Máster Universitario en Derecho de las
Telecomunicaciones, Protección de Datos, Sociedad de la
Información y Audiovisual
2017-2018

Trabajo Fin de Máster

“Informe a Asociación de Consumidores Sobre la Protección de Inversores en Criptomonedas”

Orlando Marcelo Valverde Ganoza

Tutor

Fernando Ramos Suarez.

Madrid, 05 de julio de 2018.



Esta obra se encuentra sujeta a la licencia Creative Commons **Reconocimiento – No Comercial – Sin Obra Derivada**

RESUMEN

En la actualidad, gracias a los avances tecnológicos que se han desarrollado en el área de la ingeniería informática, ha sido posible crear una herramienta tecnológica para almacenar información que está considerada virtualmente incorruptible y que permite compartir dicha información con todos sus usuarios; esta herramienta es conocida como cadena de bloques o *“Blockchain”*.

A partir de la creación del *“Blockchain”* se ha generado una plataforma para la creación de activos digitales a los que sus usuarios han decidido otorgarles un valor monetario, para así poder utilizarlos como medio de pago entre ellos o para representar una acción dentro de una compañía o una promesa de acceso a bienes o servicios que se encuentran en desarrollo; aplicando tecnología de *“Blockchain”* a estos activos con el propósito de otorgarles mayor seguridad. Es en este contexto, que las inversiones en criptodivisas han alcanzado cifras récord, superiores a cualquier proyecto en moneda fiduciaria; por lo que se está volviendo necesaria su regulación.

No obstante, el derecho, por lo general, regula situaciones jurídicas luego de que estas se han presentado en el mundo real, en consecuencia, se ve tardía la regulación de la inversión en criptodivisas en muchos países del mundo. Dicho esto, la falta de regulación no es impedimento para que usuarios de todo el globo se conviertan en inversionistas a partir de una ICO; en ese sentido, es necesario establecer parámetros y lineamientos mediante los cuales, los inversionistas puedan sentirse seguros al momento de invertir en esta clase de activos.

Finalmente, se ha propuesto una especie de guía para el inversionista, con el propósito de que se conozcan las alternativas de inversión y los medios por los cuales, un usuario pueda hacer inversiones en ICO, de forma tal que no sienta sus derechos vulnerados o amenazados durante el proceso.

Palabras Clave: Criptoactivos, criptomonedas, ICO, blockchain, mineros, tokens, criptodivisas, wallets.

ABSTRACT

Nowadays, thanks to the technological advances that have been developed in the area of computer engineering, it has been possible to create a technological tool to store information that is considered virtually incorruptible and that allows to share this information with all its users; the mentioned tool is known as "Blockchain".

The creation of the "Blockchain" has generated a platform for the development of digital assets to which their users have decided to give them a monetary value, in order to use them as a means of payment between them or to represent an action within a company or a promise of access to developing goods or services; while applying "Blockchain" technology to these assets for the purpose of giving them greater security. It is in this context that the investments in cryptocurrency have reached record figures, superior to any project in fiduciary currency; so it is becoming necessary to regulate it.

However, law, in general, regulates legal situations after these have been presented in the real world, as a result, the regulation of investment in cryptocurrency in many countries of the world is belatedly seen. That said, the lack of regulation is not an impediment for users around the globe to become investors in an ICO; In this sense, it is necessary to establish parameters and guidelines whereby investors can feel safe when investing in this kind of assets.

Finally, a type of guide for the investor has been proposed, with the purpose of knowing the investment alternatives and the means by which a user can make investments in ICO, so that he does not feel his rights violated or threatened during the process.

Key Words: Cryptoassets, cryptocurrencies, ICO, blockchain, mining, tokens, cryptocurrency, wallets.

AGRADECIMIENTOS

Deseo expresar mi total agradecimiento a todos los que me han acompañado y ayudado durante la elaboración de este trabajo, en especial a mis padres Orlando Valverde y Marcela Ganoza, sin cuyo apoyo nada de esto hubiese sido posible, y a quienes dedico esta obra. Asimismo, deseo hacer extensivo mi agradecimiento a los compañeros de clase con quienes se ha generado una amistad que va más allá de las aulas y; así también a mis profesores de la Universidad Carlos III de Madrid por los conocimientos impartidos y orientaciones recibidas.

ÍNDICE

- I. INTRODUCCIÓN.
 - 1.1. Introducción.
 - 1.2. Objetivos.
- II. CRIPTOACTIVOS
 - 2.1. Aspectos claves del Bitcoin.
 - 2.1.1. La Criptografía de Clave Pública.
 - 2.1.2. El Protocolo de Comunicación
 - 2.1.3. Los Monederos
 - 2.1.4. Las Transacciones
 - 2.1.5. Los Mineros
 - 2.1.6. Los Mercados de Compra y Venta de Monedas
 - 2.2. Aspectos Jurídicos de los Criptoactivos
 - 2.2.1. Naturaleza Jurídica
 - 2.2.2. Configuración como Dinero Electrónico o Medio de Pago
 - 2.3. La Propuesta de Modificación de la Cuarta Directiva de Prevención de Blanqueo de Capitales
 - 2.4. Clases:
 - 2.4.1. Criptomonedas:
 - Bitcoin.
 - Ethereum
 - Ripple.
 - 2.4.2. Tokens:
 - 2.4.3. Smart Contracts:
- III. ICO's
 - 3.1. Breve Historia de las ICOs
 - 3.2. Naturaleza Jurídica de las ICOs,
 - 3.2.1. El Crowdfunding
 - 3.2.2. Securities Versus Utilities.
 - 3.2.3. Posicionamiento de la CNMV y el Banco de España
 - 3.3. Las Fases de una ICO.
 - 3.4. El Fraude en las ICO.
 - 3.5. El trading en las ICOs.
 - 3.5.1. DAICO el modelo de Vitalik Buterin.
 - 3.6. Régimen Jurídico Aplicable:
 - 3.6.1. Europa:
 - 3.6.2. Asia:
 - 3.6.3. Estados Unidos
- IV. INFORME A ASOCIACIÓN DE CONSUMIDORES SOBRE INVERSIÓN EN CRIPTOACTIVOS.
 - 4.1. Mecanismos para Adquirir Criptoactivos:
 - 4.2. Funcionamiento del Mercado de Criptoactivos:
 - 4.3. Brokers:
 - 4.4. Wallets:
 - 4.5. Casos de Fraude en las ICOs
 - 4.6. Implicaciones jurídicas de las ICOs

- 4.6.1. Cumplimiento en materia de Prevención de Blanqueo de Capitales
- 4.6.2. Las implicaciones del Reglamento General de Protección de Datos.
- 4.6.3. La contratación electrónica a distancia: la Ley de Servicios de la Sociedad de la Información y la Ley
- 4.6.4. General de Defensa de Consumidores y Usuarios.
- 4.7. Legislación Aplicable en la Unión Europea y en España
- 4.8. Recomendaciones.

V. CONCLUSIONES

VI. BIBLIOGRAFÍA

VII. ANEXOS

I. INTRODUCCIÓN

1.1. Introducción:

En el presente trabajo se ha realizado una investigación académica acerca de la inversión en criptoactivos, estableciendo una línea de partida desde la definición de criptoactivos hasta las recomendaciones necesarias para poder llevar a cabo una inversión inteligente y en un espacio seguro.

Es importante señalar la relevancia de la presente investigación debido a que, si bien es cierto, en la Unión Europea no se consideran a las criptodivisas como monedas o dinero en sí, su uso ya se está volviendo algo común en las transacciones del día a día; y cada vez existen más personas interesadas en aprender sobre estos nuevos conceptos. En ese sentido, no es erróneo afirmar que, en los próximos años, la sociedad reciba con brazos abiertos a las criptomonedas en el mercado fiduciario común y corriente.

Sin embargo, no se puede dejar de advertir que existe información sobre el aspecto jurídico de las criptomonedas, pero lamentablemente de forma muy limitada, así que uno de los objetivos planteados en esta investigación es poder ayudar a futuros investigadores a establecer la naturaleza jurídica de estos nuevos fenómenos sociales, para así poder legislarlos adecuadamente.

Finalmente, se han establecido lineamientos para futuros inversionistas en criptoactivos, en donde se explica de forma simple y amigable, cómo se debe invertir en las Initial Coin Offerings de forma inteligente, segura y siempre obedeciendo lo dispuesto por la normativa para los casos en concreto.

1.2. Objetivos:

- Elaborar un informe para consumidores sobre inversión en criptodivisas.
- Establecer la conceptualización de criptodivisa para la Unión Europea.
- Conceptualizar la tecnología blockchain.
- Conceptualizar la tecnología wallet.
- Establecer las distintas clases de criptoactivos y sus características.
- Conceptualizar las ICO.
- Establecer la naturaleza jurídica de las ICO.

II. CRIPTOACTIVOS

Todas las divisas necesitan alguna manera de controlar su demanda y por lo tanto establecer distintos mecanismos para evitar las falsificaciones; por ese motivo los bancos centrales de todos los países que emiten algún tipo de divisa, les colocan ciertas características y mecanismos para evitar la emisión fraudulenta de las divisas.

En el caso de los criptoactivos, es necesario mantener un sistema que pueda prevenir que usuarios inescrupulosos traten de manipular los protocolos de uso del sistema, haciendo cuentas inconsistentes para los demás usuarios; en ese sentido, esta tecnología se soporta en el uso y aplicación de herramientas criptográficas. (Naryanan, Bonneau, Felten, Miller, & Goldfeder, 2016).

Los criptoactivos ya forman parte de nuestra sociedad, como un movimiento entre los más jóvenes dedicados a la informática o en artículos de prensa sobre temerarias inversiones en una moneda basada sobre una tecnología de la que se conoce poco; no obstante, es innegable que estos activos digitales cada vez se están mezclando con la realidad de la sociedad.

De acuerdo con la Financial Action Task Force, las criptomonedas son unidades digitales que pueden ser usadas como medio de pago en el intercambio de bienes y servicios, como depósito de valor y unidad de cuenta. (Financial Action Task Force, 2015).

En primer lugar, es necesario establecer que la definición exacta de criptoactivos aún se encuentra en evolución; no obstante, es posible brindar una aproximación a su correcta conceptualización gracias a sus características; en primer lugar, es necesario establecer que son activos digitales que se crean dentro de redes distribuidas y permiten registrar el flujo de información en cada sistema (Giupponi, 2018).

La Directiva (UE) 2015/849 relativa a la Prevención de la Utilización del Sistema Financiero para el Blanqueo de Capitales o la Financiación del Terrorismo, define al término “moneda virtual” como: *“la representación digital de valor no emitida por un Banco Central ni por una autoridad pública, ni necesariamente asociada a una moneda fiduciaria, pero aceptada por personas físicas o jurídicas como medio de pago y que puede almacenarse, transferirse o negociarse por medios electrónicos”*.

En segundo lugar, cabe destacar que los criptoactivos se construyen o crean cimentándose en redes abiertas con verificación descentralizada; en ese sentido, cualquier usuario puede ingresar a la red y actuar como verificador de la información existente que se encuentra en tráfico dentro de dicha red, por ese motivo, los sistemas de criptoactivos no tienen una autoridad central que regula su funcionamiento (Giupponi, 2018).

Finalmente, los criptoactivos son *criptográficos*, porque usan técnicas basadas en la tecnología criptográfica para verificar el flujo de la información, asegurándose que el

mensaje sólo pueda ser decodificado por el receptor indicado en el envío (Giupponi, 2018).

2.1. Aspectos claves del Bitcoin.

2.1.1. La criptografía de Clave Pública.

La capacidad de autenticar un documento electrónico o un activo electrónico se basa en la tecnología de cifrado asimétrico o también conocido como el sistema de clave pública o criptografía de clave pública, generando confianza a través de las firmas digitales y funciones asociadas.

García e Ivars señalan que, *“la firma electrónica funciona mediante la encriptación o cifrado de los datos que la componen, de forma que, si no se tiene la clave, el documento se convierte en ilegible. Para ello es necesario contar con dos tipos de claves: clave privada y clave pública que se corresponden de forma matemática.”* (García García & Ivars Bañuls, 2004).

De acuerdo con Pertíñez, Bercovitz y Gonzales de Alaiza: *“En los sistemas criptográficos de clave asimétrica o pública, se emplean dos claves asociadas. Por una parte, una clave privada, conocida únicamente por su titular, la cual debe mantenerse en secreto; y por otra parte, una clave pública, relacionada matemáticamente con la anterior y que debe ser accesible para cualquiera.”* (Pertíñez Vílchez, Bercovits Rodríguez-Cano, & González de Alaiza Cardona, 2010).

Tal y como señala la Fábrica Nacional de la Moneda y Timbre: *“La clave pública está asociada con la clave privada usada por el firmante, de forma que puede ser utilizada para verificar, pero no para generar la firma recibida. Si el algoritmo de verificación comprueba la coherencia de la firma con el contenido del documento y con la clave pública, se establece la mencionada vinculación subjetiva y objetiva.”* (Real Casa de la Moneda - Fábrica Nacional de la Moneda y Timbre, 2009).

2.1.2. El Protocolo de Comunicación

Un protocolo es un medio estándar de comunicación que permite la interrelación entre procesos, que posiblemente se ejecutan en equipos diferentes, es decir, un conjunto de reglas y lineamientos que deben respetarse para el envío y la recepción de datos a través de una red. (CCM, 2018).

También se puede conceptualizar a un protocolo como, el conjunto de reglas normalizadas o estandarizadas para la

representación, señalización, autenticación y detección de errores, necesarios para enviar información a través de un canal de comunicación. (Redes Informáticas 4to, 2018).

Simplificando este concepto, los protocolos de comunicación sirven para intercambiar todos los datos en la red a nivel mundial, debido a que es el Border Gateway Protocol el que les dice a los routers cómo enviar este tráfico de un punto a otro valiéndose de los Internet Service Providers. (Pérez, 2018).

En el caso de los criptoactivos, se utilizan protocolos de criptografía y alta seguridad, así como protocolos descentralizados para la validación de saldos y transacciones, los que, junto con el sistema de claves públicas y privadas, los usuarios puedan firmar digitalmente sus transacciones. (Arango - Arango & Bernal Ramírez, 2017).

2.1.3. Los Monederos

Los monederos o billeteras de criptomonedas son “cuentas” digitales que se usan para almacenar, enviar y recibir este tipo de divisa entre usuarios de la misma.

De acuerdo con Eles Serrano: *“es un software que hace de billetera o cartera virtual encriptada otorgando seguridad total para guardar, enviar o recibir cualquier criptomoneda o dato.”* (Serrano, 2017).

En teoría, los criptoactivos no están almacenados en ningún lado, porque se encuentran registrados en forma de transacciones dentro del blockchain; en ese sentido, la cadena de bloques registra las criptomonedas que se han recibido o enviado desde una dirección pública en concreto, utilizando determinada clave pública para su encriptación y, por lo tanto, poder conocer a cada momento cual es el saldo del monedero de criptoactivos. (Steemit, 2017).

En realidad, lo que se almacena en el sistema, es la clave privada, que es el código únicamente conocido por el usuario para poder descifrar la información que se le ha sido enviada, y que muestra la propiedad de una clave pública (Criptonetwork, 2018); en consecuencia, el monedero virtual, no solo actúa como una especie de libro personal de cuentas del usuario, sino también como un sistema de almacenamiento de claves asimétricas.

2.1.4. Las Transacciones:

En este aspecto, es necesario definir a un criptoactivo como una cadena de señales digitales; cada propietario de estos activos digitales realiza una transferencia al siguiente al firmar digitalmente un hash de la transacción anterior y la clave pública del siguiente propietario, y añadiéndolas al final de la cadena de bloques. (Nakamoto, 2018).

Uno de los principales problemas se centra en que el propietario que recibe el criptoactivo, no puede verificar que uno de los propietarios que le antecede no haya realizado un “doble gasto” de la misma moneda; por esta razón al sistema de cadena de bloques, solo le interesa lo que se encuentra en el último eslabón de la cadena, para evitar que existan intentos de realizar dobles gastos.

Para poder lograr este objetivo sin tener que recurrir a un tercero verificador, las transacciones tienen que ser anunciadas públicamente, bajo un sistema mediante el cual todos los usuarios puedan acoger como verdadero a un solo hilo de eslabones que conforman la cadena de bloques, a razón de conocer en cuál etapa de la cadena quien recibió qué moneda; si el propietario que recibe el criptoactivo necesita tener pruebas de la transacción, la aceptación unánime del historial existente, es información suficiente para este fin. (Nakamoto, 2018).

2.1.5. Los Mineros

Para crear una divisa digital que pueda adquirir valor real, necesita diseñarse de forma tal que sea escasa, tal y como el oro y los diamantes fueron considerados escasos en el mercado para que funcionen como un soporte a las divisas.

En el mundo digital, una forma de lograr la escasez de la “divisa” es diseñar el sistema de forma tal que, para generar dinero, sea necesario resolver un “acertijo” computacional que toma cierto tiempo develar. Esto es lo que se conoce como minado. (Naryanan, Bonneau, Felten, Miller, & Goldfeder, 2016).

Se escucha mucho hablar del término “minado” en el mundo de los criptoactivos; sin embargo, no muchas personas saben cómo poder conceptualizar este término, que en realidad es uno de los cimientos en la tecnología de los criptoactivos más populares, como Bitcoin, Ethereum o Bitlite.

Según Anthony Idalion, cuando se realizan transacciones de criptomonedas, se envían solicitudes de transacción a todos los

ordenadores en la red de Blockchain para que esta transacción sea validada y añadida a dicha red. Para poder alcanzar esta finalidad, el ordenador debe efectuar una función hash en todas estas operaciones, es decir, resolver una especie de rompecabezas conectado al último bloque que ha sido añadido al Blockchain. El ordenador que resuelva este rompecabezas puede añadir estas transacciones en un bloque, y este bloque a la cadena de bloques; como resultado de este proceso, el ordenador que resuelva primero la función hash será premiado con un pago en el criptoactivo utilizado en dicha red. (Idalion, 2017).

El proceso relatado anteriormente, se conoce como minado de criptomonedas.

En palabras más sencillas, cada vez que una persona realiza una transacción con criptoactivos o criptomonedas, se genera un problema matemático, y para resolverlo es necesario una potencia computacional de cálculo superior al que poseen muchas entidades; lo que hacen los mineros es resolver este problema definido en un algoritmo, para que la solución de este pueda ser añadida al Blockchain. Con miles de transacciones ocurriendo a cada minuto, el poder minar criptoactivos genera una oportunidad de negocio muy atractiva para cierto sector, por lo que esta actividad se vuelve cada vez más competitiva. (Llovera Aguirre, 2017).

Con respecto al pago de impuestos por el desarrollo de la actividad de minado, Hacienda ha determinado que dicha actividad no conduce a una situación en la que exista una relación entre el proveedor del servicio (minero) y el destinatario del mismo (usuarios) y en los que una retribución abonada al prestador del servicio, sea el contravalor del servicio prestado; en consecuencia, la falta de una relación directa entre el servicio prestado y la contraprestación recibida por los servicios de minado, no estarían sujetos al Impuesto sobre el Valor Añadido. (Secretaría de Estado de Hacienda - Dirección General de Tributos, 2017).

En este sistema, los mineros de criptomonedas tienen que dedicarse a seis tareas principalmente (Naryanan, Bonneau, Felten, Miller, & Goldfeder, 2016):

- *Validar transacciones*: En primer lugar, los mineros tienen que revisar las transacciones y validarlas, verificando que las firmas digitales que contienen son correctas y que los activos que se consignan en ellas han sido usados previamente.

- *Mantener la cadena de bloques y validar nuevos bloques:* Esto se debe hacer indagando y solicitando a todos los usuarios información sobre nodos pasados e históricos que ya forman parte de la cadena de bloques antes de que el minero se una al sistema; luego debe revisar a los nuevos bloques que están siendo transmitidos mediante el sistema y validarlos en el proceso.
- *Ensamblar un bloque “candidato”:* Una vez que el minero tenga una copia actualizada de la cadena de bloques, es hora de iniciar la construcción de bloques nuevos. Para realizar esto, el minero debe agrupar todas las nuevas transacciones de las que pueda tener noticia y añadirlas a un bloque que sea la extensión del último bloque del cual tuvo conocimiento, recalando la necesidad de verificar que cada transacción incluida sea válida para el sistema.
- *Encontrar un nonce¹ que valide el bloque creado:* Este paso requiere mucho trabajo para el minero, debido que para emitir este número es necesario un elevado nivel computacional.
- *Esperar a que el bloque sea aceptado:* Cuando se crea un bloque, no existe la garantía de que este sea añadido a la cadena si es que no existe consenso de parte de todos los mineros.
- *Obtener ganancias:* Una vez que todos los mineros hayan aceptado la creación del bloque, ellos empezarán a minar encima de este bloque creado. En el primer cuarto del 2015, la recompensa por crear un bloque de bitcoins era otorgar alrededor de 25 unidades de este activo digital, lo que a finales de 2017, equivaldría a \$425.000 Dólares Americanos²

2.1.6. Los Mercados de Compra y Venta de Monedas:

Como todo mercado, el mercado de compra y venta de criptoactivos acerca a vendedores que desean deshacerse de cierta cantidad de “monedas” y de compradores que están dispuestos a pagar un precio por ellas.

En la mayoría de redes de blockchain, un mecanismo de conversión de tokens vinculado a una criptomoneda siempre está

¹ Nonce: En la criptografía un nonce es un número arbitrario que puede ser usado una sola vez. Frecuentemente es un número aleatorio utilizado en protocolos de autenticación para asegurar que las comunicaciones antiguas no puedan ser utilizadas en ataques de respuesta. Asimismo, pueden ser utilizados como vectores de inicialización y en funciones Hash criptográficas. (Rogaway, P. (2005). *Nonce-based Symmetric Encryption*. Davis: University of California).

² Información obtenida desde <https://www.buybitcoinworldwide.com/es/precio>

presente. No obstante, es necesario recalcar que la creación y el desarrollo de un mercado de compra y venta fluido no es un requerimiento necesario para la creación de un criptoactivo; sin embargo, es la señal de que esta blockchain es exitosa. (Idalion, 2017).

El mercado de criptoactivos es un sistema en constante movimiento y evolución, con más de 700 esquemas existentes de criptomonedas que compiten entre sí³, creando una extensa oferta de este tipo de medio de intercambio.

En primer lugar, es necesario establecer que el mercado de intercambio de criptodivisas actúa de forma similar a los mercados regulares de dólares o euros, por ejemplo. El precio oscilará dependiendo cuantas personas deseen adquirir dichos activos. (Naryanan, Bonneau, Felten, Miller, & Goldfeder, 2016).

2.2. Aspectos Jurídicos de los Criptoactivos:

Es necesario precisar que la regla 2° de la Instrucción para la aplicación de las Tarifas de Impuesto sobre Actividades Económicas, aprobadas por el Real Decreto Legislativo 1175/1990 de 28 de setiembre indica que: *“El mero ejercicio de cualquier actividad económica especificada en las Tarifas, así como el mero ejercicio de cualquier otra actividad de carácter empresarial, profesional o artístico no especificada en aquellas, dará lugar a la obligación de presentar la correspondiente declaración de alta y contribuir por este impuesto, salvo que en la presente instrucción se disponga otra cosa.”*

No obstante, la compra-venta de criptoactivos a través del desarrollo y explotación de una web propia, es una actividad que no se encuentra especificada en las citadas Tarifas del Impuesto; en ese sentido, en la regla 8° de la Instrucción se regula un procedimiento mediante el cual se permite clasificar, provisionalmente, aquellas actividades que no se hallan especificadas en el grupo o epígrafe dedicado a las actividades no clasificadas en otras partes, a las que por su naturaleza se asemejen tributando a otro grupo o epígrafe. (Secretaría de Estado de Hacienda - Dirección General de Tributos, 2017).

2.2.1. Naturaleza jurídica:

Existe un gran debate sobre la naturaleza jurídica de los criptoactivos; muchos juristas los llegan a declarar como:

³ Arango-Arango, C. y Bernal-Ramírez, J. (2017). *Criptomonedas*. Bogotá: Banco de la República de Colombia.

- Título valor: En la definición más acorde con la definición clásica, se trataría de una anotación electrónica que incorpora el derecho a una cantidad de dinero (Islas, 2017). No obstante, debido a que no cuenta con el respaldo de ningún Banco Central, el propietario del activo digital no tendría derecho per se a una cantidad de dinero, lo que convertiría a los criptoactivos en títulos valores impropios.

Según Paulina Islas (Islas, 2017): *“los titulares de criptomonedas no incorporan derecho alguno y solo pueden cambiar la criptomoneda por una de curso legal, si alguien acepta su oferta y se la compra por dinero”*.

No obstante, es evidente que el propietario de cierta cantidad de criptomonedas va a ser capaz de cambiarlas por cualquier divisa, debido a que ese derecho es otorgado por la ley de la oferta y la demanda, y actualmente parece que la demanda es imposible que llegue a cero.

- Bien mueble digital: De acuerdo con Paulina Islas, citando a Pablo Fernández Burgueño (Islas, 2017), señala que se trataría de un bien mueble digital, no fungible y de propiedad privada. El hecho que sea no fungible significa que no se consume con el uso, lo que coincide con la idea de utilizar metales preciosos para la acuñación de monedas.
- Divisa simple o medio de pago: De acuerdo con la sentencia del Tribunal de Justicia de la Unión Europea del 22 de octubre de 2015, se considera al bitcoin, así como a las demás criptomonedas, un medio de pago contractual y directo entre los operadores que la aceptan. (Sentencia , 2015).

2.2.2. Configuración como dinero electrónico o medio de pago:

En primer lugar, es necesario precisar que el Banco Central Europeo reconoce que los avances tecnológicos que presentan las herramientas tales como el Blockchain, tienen el potencial de incrementar la eficiencia, el alcance y la variedad de los métodos de pago y transferencias; sin embargo, los órganos legislativos de la Unión Europea buscan evitar aparecer como impulsores del uso de “monedas” digitales creadas por privados, debido a que estos medios de pago no se encuentran legalmente establecidos como monedas de curso legal emitidas por bancos centrales de los países. (Banco Central Europeo, 2016).

No obstante, para las entidades de la Unión Europea se entiende que los criptoactivos no son monedas; debido a que según lo dispuesto en el Reglamento (CE) N° 974/98 del Consejo, el euro

es la moneda única de la unión económica y monetaria. En ese sentido, los criptoactivos no deberían ser considerados monedas, más bien un medio de cambio, no de pago; debido a que estas pueden ser utilizadas para fines distintos del de pago. (Banco Central Europeo, 2016).

En este acápite, es importante resaltar lo mencionado por la consulta parlamentaria 184/47663 que realizó el Gobierno Español el 03 de marzo de 2017:

“en el caso de que las autoridades monetarias y financieras consideren que el bitc in es un medio electr nico concebido para ser utilizado como medio de pago al portador, le resultar an de aplicaci n las limitaciones al pago efectivo”.

2.3. La propuesta de modificaci n de la Cuarta directiva de Prevenci n de Blanqueo de Capitales:

La mencionada propuesta contiene medidas, pol ticas y lineamientos destinados a combatir contra la financiaci n del terrorismo y a aumentar la transparencia de las transacciones financieras y de las entidades societarias dentro del marco jur dico de los pa ses que conforman la Uni n Europea.

El objetivo de esta propuesta es contrarrestar y disminuir la existencia de lagunas, evitando generar obst culos innecesarios al intercambio de bienes y a las transacciones financieras que dan movimiento a la econom a de los pa ses europeos. (Comisi n Europea, 2016).

El motivo de la propuesta se da por la creciente amenaza terrorista de los  ltimos tiempos, y que gracias a los avances tecnol gicos se ha facilitado la ocultaci n y el traslado de fondos en todo el mundo, dificultando el rastreo del dinero y facilitando que cualquier clase de delincuentes puedan borrar su rastro del sistema.

En esta propuesta, se busca designar como entidades obligadas de informar a las administraciones p blicas, a los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias, con el prop sito de permitir a las autoridades competentes vigilar las transacciones sospechosas con monedas virtuales sin desaprovechar o alejar las ventajas e avances innovadores de estas tecnolog as (Comisi n Europea, 2016).

En ese sentido, la propuesta define como entidades obligadas a todos los que controlen el acceso a las monedas virtuales, tales como plataformas de cambio y a los proveedores de monederos electr nicos; teni ndose en cuenta la fragmentaci n de la informaci n financiera, y por otro lado, la falta de acceso directo y r pido a esa informaci n de parte de las

Unidades de Investigación Financiera y las autoridades competentes en la lucha contra la financiación del terrorismo (Comisión Europea, 2016).

Los recientes análisis realizados a escala de la Unión han puesto de relieve algunos de sus riesgos, especialmente en lo que respecta a los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias debido a que, las transacciones con monedas virtuales gozan de un mayor grado de anonimato que las transferencias financieras clásicas de fondos y, por lo tanto, entrañan el riesgo de que la moneda virtual pueda ser utilizada por organizaciones terroristas para ocultar transferencias financieras. (Comisión Europea, 2016)

Según la Unión Europea, la medida propuesta carece de efectos negativos sobre las ventajas y los avances tecnológicos que presenta la tecnología de registros distribuidos subyacente a las monedas virtuales, pero esto estaría por confirmarse de acuerdo con la aplicación de la propuesta.

2.4. Clases:

Es importante distinguir entre criptodivisas y token. Una criptodivisa o criptomoneda es una moneda que se utiliza dentro de cada blockchain distinta para pagar, como su nombre indica, una divisa. Un token es una representación de un activo real o, incluso, un activo digital por sí mismo, como una acción o una propiedad, y quien tenga el token en propiedad es quien estaría en posesión del activo real. Es decir, una blockchain suele tener una única criptodivisa y puede tener múltiples tokens (García, 2017).

2.4.1. Criptomonedas:

Una criptomoneda, puede definirse como un activo digital que ha sido diseñado y construido como un medio de intercambio, cuyos cimientos descansan en la criptografía para asegurar la fluidez transaccional, así como para controlar la creación de dicho activo. (Chohan, 2017).

Una criptomoneda se define por tres características principales: la seguridad, la descentralización y el anonimato. La seguridad es una característica muy importante, el uso de criptografía en las transacciones de valor que se insertan en el blockchain soluciona dos posibles problemas, el doble gasto y la falsificación de la divisa. (Bravo, 2017).

La descentralización, es otra de las características por las que las criptomonedas gozan de seguridad, debido a que todos los

usuarios poseen la misma información, mayor es la dificultad para adulterar la información contenida en dichos nodos. (Bravo, 2017).

Y, por último, el anonimato, esta característica se centra en que los usuarios no tienen que identificarse para realizar transferencias en wallets de criptoactivos, sin embargo, las características del wallet hacen que las transacciones sean transparentes y gracias a los avances de la tecnología, las vuelven rastreables. (Bravo, 2017).

- Bitcoin:

El Bitcoin es la primera divisa digital descentralizada, cuyo funcionamiento no depende de un Banco Central o administrador (Nakamoto, 2018). Este sistema se basa en la tecnología Peer-to-Peer, en donde las transacciones son realizadas directamente entre los usuarios sin un intermediario. (Matonis, 2015).

Estas transacciones son verificadas por nodos de redes a través de sistemas criptográficos y almacenados en un registro público digital llamado blockchain (Bambara & Allen, 2018).

Bitcoin fue inventada por una persona o un grupo de personas que usa el alias de Satoshi Nakamoto en el año 2009, y fue lanzado al público como un software open source; no obstante el dominio web *bitcoin.com* fue registrado en agosto de 2008 y en noviembre de ese mismo año, "Satoshi Nakamoto" publicó "*Bitcoin: a Peer-to-Peer Electronic Cash System*" (Nakamoto, 2018).

El Bitcoin fue diseñado alrededor de la idea de usar criptografía para controlar la creación y el flujo de la moneda en lugar de confiar en una autoridad o un administrador para la realización de esta tarea (Matonis, 2015).

El Bitcoin funciona en un sistema de Blockchain, interpretado como una larga cadena de datos que representa todas y cada una de las transacciones realizadas con Bitcoins a lo largo de la historia de esta moneda, confirmando la identidad de los propietarios de Bitcoin y la cantidad de esta divisa que manejan. Cuando un usuario descarga un monedero de Bitcoin, descarga toda la blockchain; en consecuencia, todos los usuarios de este activo tienen una copia de todo el sistema. (Matonis, 2015).

Una vez descargado el wallet, el programa genera automáticamente una dirección para recibir y enviar Bitcoins; de forma seguida, el usuario ya puede empezar a navegar en la web para obtener Bitcoins o productos que puedan ser intercambiados por este activo. (Matonis, 2015).

En este sistema la anonimidad del usuario está garantizada, debido a que solo es necesario descargar un programa para utilizar Bitcoins, y no es requerido añadir información personal que pueda identificar al usuario. Además, los monederos no están ligados a ninguna cuenta bancaria, lo que significa que pueden realizarse transacciones entre usuarios o entidades sin que se enteren terceros (Nakamoto, 2018) (Matonis, 2015).

- Ethereum:

En términos simples, Ethereum es una plataforma de software abierto basado en Blockchain, que permite a los desarrolladores crear y desplegar aplicaciones descentralizadas (Davies, 2016).

Como Bitcoin, Ethereum está distribuida en una blockchain pública. No obstante, existen distinciones entre una y otra plataforma, la más importante es la diferencia que existe entre el propósito y la capacidad de cada una.

Como ya se ha explicado, Bitcoin es un sistema intercambio basado en tecnología de Peer-to-Peer que permite la transferencia de Bitcoins, y la blockchain de Bitcoin es utilizada para rastrear la propiedad de este activo digital; en cambio, la blockchain de Ethereum se centra en correr el código de programación de cualquier aplicación descentralizada. (Davies, 2016)

En la blockchain de Ethereum, se realiza minado para obtener Ether, una especie de token que sirve para alimentar a la red; más que una especie de criptoactivo de cambio, el Ether es utilizado para desarrolladores de aplicaciones que desean pagar por comisiones y servicios en la red de Ethereum. (Buterin, 2016).

Este criptoactivo puede ser utilizado para construir Organizaciones Descentralizadas Autónomas (DAO por sus siglas en inglés), estas son organizaciones descentralizadas que no cuentan con un líder en concreto, gestionadas por un código de programación que se basa en una serie de Smart

Contracts redactados en la blockchain de Ethereum. (Swan, 2015)

Este código está diseñado para reemplazar las reglas y estructuras de una organización en sentido clásico, eliminando la necesidad de una regulación centralizada; este DAO es propiedad de todos aquellos que hayan adquirido Ethers, pero en lugar de brindar a cada propietario acciones equitativas en esta organización, los Ethers actúan dándole a las personas derecho a voto en la DAO (Davies, 2016).

- Ripple:

Ripple también es una red de pagos que funciona a través de redes Peer-to-Peer, similar al Bitcoin en muchas formas, pero con distintas aplicaciones. En primer lugar, Ripple permite a los usuarios realizar transacciones firmadas a través de criptografía en donde se puede transferir virtualmente todo, desde dólares hasta acciones en compañías que cotizan en bolsa (Buterin, 2016).

La manera en que Ripple administra esta información es almacenando todos los activos como si fueran deuda entre sujetos que confían entre ellos; si alguien quisiera transferir cierta cantidad de un activo a alguien en quien no confía, la red de Ripple busca el camino entre estos dos sujetos para enlazarlos a través de usuarios que confían entre ellos. (Buterin, 2016).

No obstante, Ripple también sufre de críticas, debido a que su divisa (llamada XRP) existe sólo como deuda, tiene ventajas y desventajas; una de las ventajas es que permite que sus valores solo sean representados en formas criptográficas, sin embargo, esta también es una gran desventaja en sí misma, debido a que como sólo copia en la blockchain ciertos aspectos de la divisa, y deja la información a medias entre los usuarios. (Bradbury, 2013).

Además, los XRP no necesitan la cadena de confianza para ser transferidos entre un usuario a otro, teniendo como mecanismo de seguridad el cobro de una tasa de transacción para poder delimitar el camino que ha tomado la divisa entre un usuario y otro (Buterin, 2016).

2.4.2. Tokens:

En el idioma inglés, la palabra Token define a objetos similares a monedas que pueden servir como instrumentos de intercambio y

que dan derecho a disfrutar de una cantidad determinada de bienes y servicios, estos tokens son creados por el proveedor de los bienes y servicios. (Bambara & Allen, 2018).

Con la creación de Ethereum, se gestó la posibilidad de utilizar tokens que representasen derechos sobre bienes fungibles o servicios fungibles y que puedan ser objeto de comercio (Bravo, 2017). Estos tokens pueden intercambiarse entre wallets, subdividirse en decimales, e incluso comprarse y venderse en mercados destinados a este tipo de comercio.

El token es un activo fungible o ficha de valor comerciable, que se asemeja a una *utility* y se intercambia a través de blockchain, para poder servir como medio de intercambio por bienes y servicios de todo tipo (Carbó Valverde & Rodríguez Fernández, 2017).

Los usos y características de los tokens varían, siendo la clasificación más habitual la que segrega a estos criptoactivos en dos categorías:

- Security Tokens: Esta clase de tokens, generalmente otorga participación en los futuros ingresos o el aumento del valor de la entidad emisora o del negocio. (Banco de España - CNMV, 2018).
- Utility Tokens: Estos tokens otorgan derechos para acceder a un servicio o recibir un producto, sin perjuicio de hacer mención a expectativas de revalorización y de liquidez o a la posibilidad de negociarlos en mercados específicos. (Banco de España - CNMV, 2018).
- Payment Tokens: Estos tokens sirven a sus titulares como medios de pago (Gurrea Martínez, 2018). El GAFI⁴ en su Informe de junio de 2014 y junio de 2015, considera que las Monedas Virtuales no tienen la condición de divisa de curso legal en ninguna jurisdicción. No obstante, al tratarse de un activo digital que utilizan los usuarios para transmitir valor, podríamos llegar a la conclusión de que se trata de dinero electrónico (Ramos, 2018).

2.4.3. Smart Contracts:

Un Smart Contract es un protocolo con características especiales destinado a contribuir, verificar o implementar la negociación o desarrollo de un contrato, conteniendo toda la información sobre el contrato y que ejecuta las condiciones de este

⁴ Grupo de Acción Financiera Internacional.

automáticamente; este tipo de contratos inteligentes permiten realizar transacciones basadas en confianza con terceras partes, que pueden ser rastreables e irreversibles (Tar, 2017).

Este concepto fue creado por Nick Szabo en 1995 (Al Khalil, Ceci, O'Brien, & Butler, 2017) cuya aplicación se perdió en el olvido hasta hace pocos años, en donde la aparición de redes Peer-to-Peer y la creación de sistemas comunitarios de intercambio virtual de activos favoreció el resurgimiento de este término y la especialización de la tecnología.

Los Smart contracts son, en puridad, programas de ordenador que pueden ser ejecutados a petición del usuario, en este caso una de las partes de la relación contractual, enviando transacciones verificadas a través de los nodos de una red de Peer-to-Peer. Estos nodos contienen colectivamente toda la información en una red de Blockchain. (Atzei, Bartoletti, Cimoli, Lande, & Zunino, 2017).

Un elemento crucial de los Smart contracts es su correcta ejecución al cumplirse ciertas condiciones que dan origen al contrato, sin la necesidad de una autoridad o un tercero que verifique la ejecución contractual. La resolución de potenciales problemas generados en la ejecución contractual, se realizan mediante un protocolo de consenso entre los usuarios de la plataforma, debido a que todos ellos tienen la misma información contenida en el blockchain (Atzei, Bartoletti, Cimoli, Lande, & Zunino, 2017).

III. ICO's

La ICO (Initial Coin Offering), puede hacer referencia tanto a la emisión de criptomonedas, como a la emisión de activos digitales de diversa naturaleza conocidos como Tokens (Banco de España - CNMV, 2018), que se encuentran asociados a proyectos empresariales que están en etapas de desarrollo o a proyectos que, por su naturaleza, no encuentran un financiamiento constante a través de los medios regulares.

Las ICO, también llamadas Token Sale o Crowdsale, es un mecanismo por el cual se recolecta capital a través de la emisión de criptoactivos como porcentaje de una serie de monedas totalmente nueva, a cambio de capital que puede ser dinero real o algún otro tipo de criptoactivo. Las ICO venden criptoactivos o pueden vender derechos y participación en un proyecto, y se diferencian de las Initial Public Offerings (IPO), que vende una parte de la compañía al inversionista (Chohan, 2017).

3.1. Breve Historia de las ICOs⁵:

- En julio de 2013, Mastercoin presenta la primera crowdsale y recauda \$500.000.00 dólares.
- En abril de 2014, la empresa escocesa de crowdfunding Madsafe recauda \$ 7 Millones de dólares en 5 horas.
- En julio de 2014, Ethereum realiza su primera ICO recaudando \$18.4 Millones de dólares.
- En julio de 2015, las ICO afrontan un crecimiento lento, desanimando a nuevas inversiones y proyectos en blockchain.
- En octubre de ese mismo año, Augur una plataforma open source que se dedica a predicción del mercado recauda tokens de Bitcoins y Ethereum por un valor de \$5.3 Millones de dólares.
- En noviembre de 2015, el mercado de criptoactivos alcanza una capitalización de \$7,915'780,000.00 dólares.
- En abril de 2016, el DAO recauda \$150 Millones en una ICO.
- En junio de 2016, Waves recauda 30.000 Bitcoins (alrededor de \$16 Millones de dólares en la fecha), convirtiéndose en la mayor crowdsale de criptoactivos.
- En noviembre de 2016, Golem, una empresa informática de Polonia recauda \$8.6 Millones de dólares en 29 minutos.

⁵ Coinlist. (diciembre, 2017). EL Ascenso de las ICO. Recuperado de <https://coinlist.me/es/icos/historia-icos>.

- En abril de 2017, Gnosis, aplicación de predicción de mercado basada en Ethereum, recauda \$12.5 Millones de dólares en tokens en 12 minutos, convirtiéndose en la recaudación de crowdfunding más rápida de la historia, hasta el momento.
- En mayo de 2017, Brave, un navegador web de opensource, recauda \$35 Millones de dólares en 30 segundos.
- En junio de 2017, Dentacoin se convirtió en la primera compañía en ser comprada con criptoactivos, por el valor ascendente a 31.5 Millones de Dentacoins.
- En ese mismo mes, los inversores de la ICO de Ethereum obtuvieron una rentabilidad de 131,089%.
- Asimismo, la plataforma israelí Bancor recoge \$153 Millones de dólares en menos de 3 horas.
- En julio de 2017, el proyecto de Blockchain Tezos, reúnen alrededor de \$232 Millones de dólares, representados en bitcoins y Ether, en 13 días.
- En ese mes, las recaudaciones alcanzan un valor histórico de \$798'251,174 dólares.
- En agosto de 2017, el boxeador norteamericano Floyd "Money" Mayweather, recauda \$30 Millones de dólares en una ICO.
- Asimismo, los montos recogidos por las ICO superan las fases iniciales de las financiaciones de capital de riesgo para compañías de internet.
- En setiembre de 2017, China prohíbe las ICO, luego de que el Banco Central las declarara ilegales por "perturbar el mercado financiero", haciendo que la valoración de Bitcoin, Ethereum y demás criptoactivos se desplome.
- Finalmente, en octubre de ese mismo año, se advirtió que las ICO habían recaudado más de \$2 Billones de dólares.

3.2. Naturaleza Jurídica de las ICOs

Para poder analizar la naturaleza jurídica de las ICO, es necesario establecer que estos mecanismos de colecta de activos no pueden generalizarse, debido a que debe identificarse el tipo de token que está siendo ofrecido, dada la naturaleza maleable de este activo.

En ese sentido, Aurelio Gurrea y Nydia Remolina (Gurrea Martínez & Remolina León, Problemática Jurídica y Financiera de las ICO, 2018), señalan que, para determinar la naturaleza jurídica de las ICO, deben implantarse dos sistemas regulatorios; sistema de control ex-ante y ex-post.

En el sistema de control ex-ante, se debería establecer al menos, un enfoque basado en establecer criterios para definir concretamente y lograr clasificar a los criptoactivos con carácter "*numerus clausus*" y que los organizadores de la ICO sepan a ciencia cierta qué tipo de criptoactivos van a emitir y cuál es el régimen jurídico que se les aplicará a los mismos.

Mientras que en el control ex-post, se debe establecer un enfoque basado en principios generales que establezcan una clasificación abierta de los criptoactivos, para que los organizadores clasifiquen sus activos y solo requiera aprobación ex- ante del organizador en ciertos casos; y finalmente, la fijación de principios generales acompañados de un control ex-ante (Gurrea Martínez & Remolina León, Problemática Jurídica y Financiera de las ICO, 2018).

3.2.1. El Crowdfunding:

El crowdfunding es un método de colecta a través de pequeñas contribuciones realizadas por usuarios de una plataforma que fue creada con esta finalidad (Freeman & Nutting, 2015).

También puede considerarse al crowdfunding como una iniciativa propuesta por alguien orientada a recolectar dinero para un nuevo proyecto, a través de pequeñas donaciones de otras personas (Atzei, Bartoletti, Cimoli, Lande, & Zunino, 2017).

El crowdfunding apareció por primera vez en Estados Unidos cuando Brian Camelio, lanzó en internet la plataforma ArtistShare en 2003, siendo esta una página web en donde los fans podían financiar los proyectos de sus artistas favoritos; esto evolucionó a una plataforma de crowdfunding en donde los propios artistas podían solicitar ayuda para financiar sus grabaciones y vídeos (Freeman & Nutting, 2015).

Existen tres marcados tipos distintos de crowdfunding: El crowdfunding basado en recompensas, el crowdfunding basado en deuda y el crowdfunding basado en donaciones.

En el crowdfunding basado en recompensas, el organizador de esta iniciativa sigue siendo el titular de la propiedad intelectual, patentes, derechos de marca y derechos de autor, sobre lo que desea financiamiento, prometiendo una participación o la entrega

del bien que está produciendo; no obstante, el usuario de la plataforma que brinda dinero para este proyecto asume el riesgo de su inversión, sin que exista garantía alguna de que el proyecto tenga éxito. Un estudio demuestra que en el 70% de este tipo de crowdfunding, no se cumple con la fecha establecida para otorgar las recompensas esperadas por los financistas (Freeman & Nutting, 2015).

Mediante el crowdfunding basado en deuda, el organizador del proyecto se compromete a devolver al inversionista, el monto otorgado para realizar el financiamiento, más un porcentaje adicional por la deuda generada, tiene la misma lógica que un préstamo regular; esta clase de crowdfunding ha ganado mucha popularidad entre las startups y los proyectos de negocio basados en redes Peer-To-Peer (Freeman & Nutting, 2015).

Finalmente, el crowdfunding basado en donaciones, es más utilizado en campañas humanitarias colectivas y de ayuda social o interés ambiental; mediante este tipo de colecta, el inversionista otorga capital para que se realicen proyectos de índole humanitaria y no se espera un retorno en especie o capital hacia este (Freeman & Nutting, 2015).

3.2.2. Securities Versus Utilities:

En primer lugar, es necesario establecer la correcta definición entre Securities Tokens y Utilities Tokens. Los primeros tienen que demostrar los siguientes atributos: ¿Ofrece una oportunidad para contribuir financieramente y obtener beneficios de una compañía propiedad de quienes organizan la ICO?; y, ¿Este esquema involucra una inversión monetaria en una empresa para obtener beneficios solo de esa inversión? (Pollock, 2018).

Asimismo, se pueden diferenciar a los Security tokens como acciones en un negocio, inversiones para desarrollar un proyecto comercial y ofrecer dividendos y beneficios a los inversionistas (Benoliel, 2017); así como también, pueden otorgar participación en los futuros ingresos o el aumento del valor de la entidad emisora o del negocio (Banco de España - CNMV, 2018).

Por otro lado, los utility tokens pueden ser definidos como: *“la representación de un acceso futuro a los servicios o productos ofrecidos por una compañía. La característica que define a los utility tokens es que estos no están diseñados como inversiones...”* (Pollock, 2018).

Este tipo de criptoactivos también pueden ser considerados como una especie de cupones para que la compañía le provea al

inversionista del producto o servicio que se encuentra desarrollando.

Asimismo, otorgan derecho a acceder a un servicio o a un bien en desarrollo, sin perjuicio de existir expectativas de revalorización y de liquidez o la posibilidad de negociarlos en mercados específicos (Banco de España - CNMV, 2018).

Benoliel define a las utility tokens como servicios o unidades de servicios que pueden ser adquiridos; comparables a claves API, usadas para acceder a algún sistema (Benoliel, 2017).

3.2.3. Posicionamiento de la CNMV y el Banco de España:

La CNMV y el Banco de España, han precisado que las criptomonedas o criptoactivos, no se encuentran respaldados por ningún banco central de ningún país, aunque son aceptadas como alternativas a las divisas de uso legal; sin embargo, estas entidades han otorgado ciertas características a estos activos digitales (Banco de España - CNMV, 2018):

- No es obligatorio aceptarlas como medio de pago de deudas u otras obligaciones.
- Circulación limitada.
- Su valor es oscilante, por lo que no pueden considerarse un buen depósito de valor ni una cuenta de unidad estable.

Según la Comisión Nacional del Mercado de Valores, conjuntamente con el Banco de España, los criptoactivos así como los distintos actores implicados en su comercialización directa o indirecta, no se encuentran regulados por la Unión Europea (Banco de España - CNMV, 2018); esto quiere decir que las personas que compran o comercializan este tipo de activos digitales, no gozan de las garantías, salvaguardas y beneficios otorgados a los productos financieros correctamente regulados.

En ese sentido, de acuerdo con lo señalado por estas entidades, los inversores no cuentan con la protección otorgada por la legislación española y europea, siendo inversiones sumamente expuestas al fraude, estafas, manipulación de precios o cualquier otra actividad ilícita.

La CNMV y el Banco de España, han hecho la advertencia de que ninguna ICO ha sido registrada, autorizada o verificada por ningún organismo supervisor en España (Banco de España - CNMV, 2018).

La carencia de mercados organizados, comparables con los mercados de valores a nivel mundial, dificulta la venta de activos mediante ICO para obtener efectivo convencional que pueda ser usado por todos; sus propietarios pueden no disponer de opciones en el momento deseado para recuperar la inversión o convertir a los activos en divisas regulares. Este contexto, convierte a las ICO en mercados especulativos de alta volatilidad (Banco de España - CNMV, 2018).

El fenómeno de las ICO es un fenómeno de alcance global, debido a que la plataforma de desarrollo de estos mecanismos de financiación es el internet; es por este motivo que la CNMV y el Banco de España indican que es conveniente la regulación a nivel internacional, para alcanzar posiciones conjuntas de los reguladores del mercado de divisas en el mayor número posible de jurisdicciones.

3.3. Las Fases de una ICO.

De acuerdo con los manuales encontrados en las distintas plataformas online (ICO4YOU, 2018), regularmente las ICO cuentan con un promedio de 11 fases, las cuales son:

1) Creación de la idea:

Esta fase se concreta mediante el anuncio en webs o comunidades web orientadas al negocio de los criptoactivos, tales como Bitcoin talk o Reddit. Los creadores de la idea de negocio preparan una especie de presentación para inversores, en donde se explica el propósito del proyecto ICO.

Luego de esta presentación, los “organizadores” reciben múltiples comentarios, en los que se explica de forma individual ciertos puntos de la ICO, esto ayuda a determinar si los inversionistas se encuentran interesados o no, de acuerdo con la cantidad de comentarios recibidos (ICO4YOU, 2018).

La naturaleza de las ICO se centra en que el proyecto resulte atractivo para los inversionistas, por ese motivo los organizadores del proyecto tienen que realizar los ajustes necesarios a la idea de negocio, en función de las respuestas recibidas de parte de los usuarios de las plataformas de crowdfunding.

2) Elegir un Equipo:

De acuerdo con la investigación realizada, en un equipo que organiza un ICO, existen aproximadamente entre 20 a 30 participantes (Cazorla, 2018); desde especialistas en el contenido del proyecto

hasta community managers para administrar las páginas de las redes sociales.

3) Estudio del Mercado:

Es necesario estudiar los ICO de empresas anteriores y con finalidades similares, de ser posible, debido a que estas experiencias le brindan al organizador, y también al inversionista, una perspectiva más amplia e informada del posible futuro de la ICO (ICO4YOU, 2018).

4) Registro de la Compañía:

Para brindarle legalidad a las futuras inversiones, es necesario registrar la compañía en un país amigable con las ICO; en este aspecto, los creadores de criptoactivos prefieren a Estados Unidos, Belice, Estonia, Chipre, Gran Bretaña, Singapur, Suiza, entre otros. (Arango - Arango & Bernal Ramírez, 2017)

5) Preparación de la Oferta:

El llamado whitepaper es el documento principal en este esquema y, por lo tanto, el más difícil de elaborar. En este documento tiene que establecerse la oferta final que será puesta en exhibición para que los inversionistas decidan finalmente si apoyar económicamente o no, el mencionado proyecto.

6) Lanzamiento del Sitio Web y Suscripción por Email.

Actualmente, si una organización cuenta con una página web bien estructurada y con publicidad a gran escala, genera confianza en los inversionistas, por lo que es una medida estratégica que garantiza la existencia de la compañía; no obstante, cuando se inicie la ICO, es probable que el dominio web se sature, la página sufra ataques DDoS o spam, por lo que nunca está de más proteger el sitio web de la compañía (ICO4YOU, 2018).

7) Términos y Condiciones para Inversionistas:

En este punto es necesario determinar si existirán ventas preliminares o pre ICO's; es recomendable realizar ambas, dando la oportunidad a los usuarios de detectar posibles fallos en el sistema; asimismo, la compañía debe informar al inversionista sobre el mecanismo de colecta utilizado por la empresa y cuáles son las condiciones de uso de la plataforma.

8) Creación de Canales de Comunicación:

Ahora bien, el paso siguiente en este esquema es proveer comunicación a los inversionistas interesados y al público en general, acerca de la existencia de este proyecto de inversión, por lo que es determinante la creación de plataformas de comunicación tales como redes sociales, correos electrónicos, grupos en whatsapp o telegram, así como también utilizar nuevos medios como Reddit, WeChat, VKontakte; creando foros de interacción para mantener informados a todos los inversionistas acerca de las novedades y fecha de inicio de la ICO (ICO4YOU, 2018).

9) Diseño y Publicación de la Campaña de Recompensas:

Las recompensas en el mundo de los criptoactivos es la posibilidad de recibir criptomonedas o tokens gratis durante el desarrollo de una ICO (ICO4YOU, 2018); como ya ha sido establecido, estos criptoactivos pueden ser cambiados por divisas de uso común, o si es que este criptoactivo se vuelve lo suficientemente popular, puede generar una inversión seria.

10) Actividad en Redes Sociales:

En este punto, ya solo es necesario mantener el interés de los inversionistas para que no se pierda la emoción de la compra del criptoactivo ofrecido.

11) Añadir el Proyecto de Inversión a ICO Trackers:

Los ICO Trackers ofrecen el servicio de recolectar información acerca de la plataforma de crowdfunding, realizando un análisis sobre el modelo de negocio, el nicho de mercado, la calidad del equipo de trabajo, el nivel de competitividad, el historial técnico del equipo y el análisis de comentarios de la comunidad de usuarios y noticias existentes sobre el proyecto (ICO4YOU, 2018).

3.4. El Fraude en las ICO.

El auge de las Initial Coin Offerings, como esquema de recopilación de fondos, gracias a la poca regulación de los países se ha convertido en un ambiente ideal para el desarrollo de prácticas ilegales como el fraude o la estafa, en donde supuestos “empresarios” organizan ICO's con el único propósito de obtener transferencias de dinero de parte de inversionistas que caen en el engaño orquestado por estos empresarios.

En ese sentido, es necesario poder advertir los signos de cualquier intento de estafa en estas plataformas; al respecto es necesario precisar

lo que indican los especialistas en este tema para evitar caer en este tipo de fraudes.

Como aspecto principal al momento de determinar la existencia de un intento de fraude o estafa en una ICO, es necesario que el inversionista preste especial atención a las características del mercado del criptoactivo, la forma en la que se utilizará la plataforma, entre otros elementos (Bastardo, 2017); debido a que si no queda bien definido el papel del activo luego de la ICO, es un signo claro de potencial estafa.

Otra característica a tener en cuenta, son las alianzas con casas de cambio de importancia en el mundo de los criptoactivos, debido a que los empresarios prometen muchas veces, que el dinero de los inversionistas se revalorizará; es comprensible que cuando se oferten proyectos nuevos que recién se encuentran naciendo en el mundo de las ICO, no tengan estas alianzas, pero al menos debe de tenerse como objetivo claro, para que el inversionista tenga una plataforma adecuada con el propósito de administrar adecuadamente su dinero (Bastardo, 2017).

De igual manera, es recomendable examinar los antecedentes de los miembros del equipo que están organizando la recaudación; debido a que muchas veces es posible determinar si es que alguno de ellos ha participado anteriormente en ICO's exitosas o si es que tienen antecedentes de manejos irregulares de fondos (Criptonetwork, 2018).

Afortunadamente, dado el volumen de inversión que representan las ICO a nivel mundial, distintos entes reguladores en el mundo han empezado a interesarse en este tipo de plataformas de recaudación, como por ejemplo Estados Unidos, China, Canadá, Corea del Sur, Singapur, entre otros (Benoliel, 2017).

3.5. El Trading en las ICO's:

En palabras sencillas, el trading consiste en comprar y vender activos en los mercados financieros con el objetivo de obtener un beneficio. La idea es comprar barato y vender caro, para de esta forma obtener una ganancia (Jimenez, 2016).

El trading es parte de los movimientos financieros, ejercido por los "traders", mejor conocidos como comerciantes. El trading consiste en negociar y/o especular en algún mercado bursátil, con la finalidad de obtener ganancias rentables. Los traders requieren de los brokers online, o convencionales, para así ejercer sus actividades financieras. (Bravo, 2017).

En el trading es necesario que el mercado que acoja ofertas y demandas de compras y ventas guarde o administre las claves privadas de los usuarios o clientes. Es decir, el usuario debe de crearse una wallet en la

web y enviar las monedas para intercambiarlas como si un mercado financiero o Bolsa se tratara.

Para acceder a los Mercados de trading no se necesita más que cumplir con procedimientos de KYC o Blanqueo a efectos de identificación, sin embargo; en definitiva, no están controlados (Ramos, 2018).

La quinta directiva de Blanqueo de Capitales define a los traders como (Comisión Europea, 2016): “proveedor de servicios de custodia de monederos electrónicos”: una entidad que presta servicios de salvaguardia de claves criptográficas privadas en nombre de sus clientes, para la tenencia, el almacenamiento y la transferencia de monedas virtuales.”

Esta parte del mercado de comercialización de criptoactivos es fundamental para el ciclo de vida de los Tokens y las ICO, ya que estas se ofrecen en estos mercados y de acuerdo a la oferta y la demanda es que se valorizan; por lo tanto, un proyecto de ICO debe estar referenciado en estos traders o exchangers para lograr otorgar un revestimiento de legalidad y confianza a las transacciones.

Para realizar actividades de trading, lo principal que se necesitará será un broker, que es un intermediario que permite introducir órdenes de compraventa en el mercado, a cambio de comisiones por cada operación (Jimenez, 2016); luego de haber obtenido un bróker, y como paso final indispensable, es instalar una plataforma de trading, el cual se define como un software especializado en servicios financieros, que permite visualizar gráficamente la evaluación de la inversión futura o de la inversión realizada.

3.5.1. DAICO el Modelo de Vitalik Buterin.

En enero de 2018, Vitalik Buterin⁶ anunció al mundo un nuevo y mejorado modelo de ICO, el cual mezclaría las ventajas y características de las DAO con las ICO, formato denominado DAICO.

De acuerdo con mismo Vitalik Buterin (Buterin, Explanation of DAICO, 2018), la idea del DAICO se centra en que este es un solo Smart contract publicado por un solo equipo desarrollador que desea recaudar fondos para un proyecto; nada fuera del otro mundo hasta el momento, no obstante, el contrato DAICO inicia en modo contribución, especificando un mecanismo a través del cual todos pueden contribuir con ETH al contrato y obtener tokens por esta acción.

⁶ Vitalik Buterin es un programador de nacionalidad rusa, creador y co-fundador de Ethereum.

Una vez que el periodo de contribución ha terminado, la posibilidad de contribuir con ETH se detiene, y se establecen los balances iniciales de tokens; en ese sentido, a partir de este punto los tokens pueden ser utilizados en mecanismos de trading (Buterin, Explanation of DAICO, 2018).

Finalmente, también existe un mecanismo a través del cual, los poseedores de tokens pueden votar en resoluciones, las cuales pueden ser aprobadas con una mayoría del quórum; en este aspecto, la finalidad es restringir el uso de tokens a los desarrolladores, y establecer un presupuesto mensual para llevar a cabo el proyecto, aumentándolo cada vez que el equipo desarrollador demuestre avances positivos.

No obstante, si no se llegan a apreciar avances en el desarrollo del proyecto, los inversionistas pueden cancelar totalmente el DAICO y obtener un reembolso completo del importe invertido en el proyecto (Buterin, Explanation of DAICO, 2018).

Como es apreciable, la principal diferencia entre las ICO y el DAICO, se centra en el manejo de los fondos recaudados; en la primera, cuando se recolectan los fondos, el equipo desarrollador también participa como administrador de los activos, muchas veces sin rendir cuentas de los avances del proyecto, llegando a provocar demoras en la entrega de los bienes o servicios.

Mientras que, en el DAICO, los desarrolladores se encuentran a merced de la administración de los inversionistas, gracias a la aplicación de un algoritmo de Smart contracts.

3.6. Régimen Jurídico Aplicable:

3.6.1. Europa:

Como se ha establecido anteriormente, la Unión Europea no tiene vigente una legislación uniforme sobre criptoactivos o Initial Coin Offerings, debido a que la Unión no reconoce a este tipo de activos digitales como divisas propiamente dichas, a razón de reconocer al Euro como la única moneda legalmente establecida en la comunidad económica europea.

Sin embargo, el vicepresidente de la Comisión Europea para el Euro y el Diálogo Social, Valdis Drombovskis, ha señalado que la Unión Europea se encuentra lista para regular a las criptomonedas y a las ICO (Drombovskis, 2018).

No obstante, debido a la creciente demanda de criptoactivos y a la creciente oferta de ICO a nivel mundial, distintas naciones europeas han visto emergente la posibilidad de regular estas actividades económicas, para poder darles un revestimiento de legalidad a la recaudación de fondos por estos medios.

En ese sentido, países como Suiza, a través de la Autoridad Supervisora del Mercado Financiero (FINMA), ha publicado las directrices que regirán a las ICO dentro de dicho país, partiendo de las bases de la regulación vigente para el mercado financiero (Rivero, 2018).

Ahora bien, la FINMA reconoce que no todo lo regulado en el mercado financiero suizo es aplicable a las ICO; no obstante, es necesario evaluar cada caso dependiendo de la ICO. Esto demuestra que no se está promulgando una regulación específica para las ICO en Suiza, pero el órgano regulador ha determinado que, para evaluar a los tokens ofrecidos en estas plataformas, se reconocerán tres categorías que dependen de las características y transferibilidad de los mismos (Rivero, 2018).

En este contexto, las categorías de tokens contempladas por el regulador suizo son los tokens que están diseñados como medios de pago, los tokens destinados a proveer o proporcionar acceso a un bien o servicio; y finalmente, los tokens que representan activos con respaldo físico real.

Adoptando una postura similar a la suiza, encontramos a España, en donde no se ha regulado aún este tipo de plataformas, no obstante, Víctor Rodríguez, Director General de Política Estratégica y Asuntos Internacionales de la CNMV (Europa Press, 2018), ha informado que el organismo supervisor del mercado de valores, aplicará por analogía la normativa del mercado financiero hacia las ICO hasta que exista legislación europea especializada en la materia.

3.6.2. Asia:

En el continente asiático se han establecido tres países en donde las ICO están creciendo y desarrollándose como un mecanismo de inversión confiable y que brinda beneficios de acuerdo con los tokens ofrecidos, estos países son Singapur, Corea del Sur y Hongkong.

Sorprendentemente, en Corea del Sur, país que estaba considerado como la meca de las criptomonedas, se está elaborando un proyecto de ley para prohibir plataformas de negociación, debido a que muchos ciudadanos aprovechaban la

falta de regulación de estos activos financieros, evadiendo impuestos y realizando actividades ilícitas como la prostitución y la comercialización de drogas (EFE, 2018).

Ahora bien, las criptomonedas se han convertido en medios de intercambio muy populares en Corea del Sur y Japón, así como también se han vuelto una forma de proteger los ahorros o como fondo de pensiones ante los bajos rendimientos de las aseguradoras en estos países asiáticos (EFE, 2018); por este motivo, existen muchos detractores del mencionado proyecto de ley, debido a que si bien es cierto, muchas veces se utilizan mal a los cryptoactivos, estos significan una forma adicional de ingreso para los ciudadanos promedios en estos países asiáticos.

Mientras tanto, en Singapur, el regulador del mercado financiero en este país, ha establecido que los tokens se encontrarán bajo su jurisdicción, si es que constituyen productos regulados al amparo de la “ley de valores y futuros” (Suberg, 2017); afirmando la aplicación del método caso por caso, analizando cada token puesto a disposición de los inversionistas, y determinando su naturaleza jurídica.

En Honkong, las ofertas públicas de tokens han alcanzado niveles exorbitantes, debido a que las compañías están buscando métodos alternativos para recolectar capital fuera de sus países de origen (Crypto Economy, 2018); no obstante, en este país asiático se está tomando la posición de China, buscando declarar la ilegalidad de este tipo de activos digitales.

3.6.3. Estados Unidos:

En Estados Unidos, la SEC determinó que las ICO no se consideraban mecanismos legales de financiamiento, debido a que en ninguna oportunidad habían actuado como regularmente lo haría una empresa que cumple con lo regulado por las leyes federales de ese país (Clayton, 2017).

Sin embargo, esto no quiere decir que sean terminantemente ilegales, puesto que, en el Estado de California, se admite la inversión de particulares y empresas en ICO si es que se cumple con lo prescrito por las leyes creadas para regular el mercado financiero (Subramanya, 2018).

IV. INFORME A ASOCIACIÓN DE CONSUMIDORES SOBRE INVERSIÓN EN CRIPTOACTIVOS:

4.1. Mecanismos para Adquirir Criptoactivos:

En la actualidad cohabitan diversas plataformas web que permiten negociar estos activos, hay exchanges que funcionan con los principios de mercado y hay plataforma que ofrecen un precio de compra y una venta para quien desee comprar estos activos y tenerlos en un wallet (García, 2017).

Existen muchos mecanismos para adquirir criptoactivos que se encuentran en circulación gracias a las plataformas de internet; dicho esto, es necesario centrarse en las cuatro alternativas principales: aceptándolas como medio de pago, minando bitcoins, visitando páginas de internet o resolviendo captcha y por medio del mercado de criptomonedas.

- Aceptar criptoactivos como medio de pago: es la forma más sencilla de obtener este tipo de divisas digitales; sólo es necesario que el establecimiento brinde un código QR vinculado al monedero o la dirección web del monedero, para que el comprador realice la transacción (Dinero, 2017). Para que esto se realice, es necesario que ambas partes acuerden realizar la compraventa con este tipo de medio de intercambio.
- Minado de criptoactivos: Como ya ha sido establecido, a través del minado de criptoactivos, un equipo de programadores resuelve una ecuación, con el propósito de realizar un hash a todas las operaciones realizadas en la cadena de bloques utilizada, y así poder añadir un bloque adicional que represente todas las transacciones realizadas hasta la fecha. El inconveniente con este tipo de mecanismo de obtención de criptoactivos; es que exige una alta inversión por los equipos de cómputo, electricidad y personal, para desempeñar distintas labores.
- Visitando páginas de internet o resolviendo captcha: en esta alternativa, el usuario obtendrá criptoactivos como medio de pago por haber realizado una labor; como por ejemplo ver publicidad en internet y resolver captchas de seguridad (Dinero, 2017); la desventaja de esta actividad es que la remuneración por las labores realizadas se percibe en la milésima parte de la unidad de un criptoactivo, como por ejemplo, milibitcoins (mBTC) o satoshis (μ BTC)⁷.

⁷ 1 satoshi es la millonésima parte de un Bitcoin.

- A través del mercado de compraventa de criptoactivos: esta actividad consiste en comprar criptoactivos por un precio “económico” para el mercado y cuando estas, por acción de la oferta y la demanda, suban de precio y aumenten de valor, venderlas (Dinero, 2017); luego de esto hay que esperar a que las criptomonedas bajen de precio, para continuar el ciclo económico. La desventaja de este método para conseguir criptodivisas es que se requiere un amplio conocimiento sobre la fluctuación del mercado de activos digitales y manejar un aproximado del comportamiento del mercado sobre la compra y venta.

4.2. Funcionamiento del Mercado de Criptoactivos:

Antes de hablar sobre el funcionamiento del mercado de criptoactivos, primero es necesario establecer cómo estos activos digitales obedecen a la ley de la oferta y la demanda⁸. Cuando una criptodivisa tiene un valor elevado, suele ser porque los traders, colocan un precio elevado teniendo en cuenta lo solicitado que puede estar dicho activo (Criptotendencia, 2017).

Mientras la ley de la oferta y la demanda se cumpla, la cotización de los distintos criptoactivos se mantendrá en constante crecimiento (Criptotendencia, 2017); esto quiere decir que mientras más usuarios se encuentren interesados en adquirir una criptodivisa o token en específico, el precio aumentará debido a lo escaso que resulta este bien deseado.

La forma más sencilla de comprender el funcionamiento del mercado de criptoactivos, es estableciendo que, para llevar a cabo una transacción en criptomonedas, se necesita un monedero para gestionar los movimientos.

Cuando se realiza una transferencia de criptoactivos, se envía la cantidad deseada a la dirección electrónica del destinatario; luego las diferentes transacciones se agrupan en bloques gracias a la labor de los mineros, quienes validan estas transferencias gracias a la resolución de ecuaciones matemáticas. Finalmente, los bloques se añaden a la blockchain, cerrando el círculo de transacciones e iniciándose uno nuevo (Escribano, 2018).

Existen diversas plataformas web que permiten negociar estos activos, hay exchanges que funcionan con los principios de mercado y hay plataforma que ofrecen un precio de compra y una venta para

⁸ La ley de la oferta y la demanda señala lo siguiente: *“El punto que existe entre la demanda y la oferta de algún bien material, siempre se va a encontrar con algún equilibrio en el mercado”*.

quien desee comprar estos activos y tenerlos en un wallet (García, 2017).

Ahora bien, si es que se desea adquirir criptomonedas, es necesario advertir que cierto tipo de criptoactivos, como el Bitcoin, Ethereum o el Litecoin, pueden ser adquiridos de forma sencilla con una tarjeta de crédito o una transferencia bancaria; no obstante, si es que el usuario desea adquirir monedas de menor importancia en el mercado, es necesario recurrir a la figura del Exchange.

Para adquirir BTC, ETH o LTC, es recomendable entrar en una plataforma de Exchange en donde es necesario registrarse como usuario y añadir un método de pago para poder realizar la adquisición del activo digital; en donde también se pueden administrar los contenidos de los monederos que se encuentran en posesión del usuario; es menester resaltar que en este tipo de plataformas se pueden ofrecer en venta criptomonedas y así contribuir a la fluctuación de la divisa.

Por otro lado, para adquirir criptoactivos de menor importancia, como Ripple, Tron, NEO o IOTA, es necesario tener previamente adquiridos criptoactivos que sean aceptados por los usuarios de estas plataformas de Exchange, como Bitcoins, Ethereum o Litecoin; con el propósito de utilizar este tipo de criptodivisas como mecanismos de cambio.

La liquidez de estos activos está limitada a la plataforma en la que se operan y su cotización es fruto de la oferta y la demanda en los distintos exchanges y plataformas, y como ya ha sido mencionado, no existe un agente central, por la propia naturaleza de la tecnología, que regule el precio de los activos (García, 2017).

De acuerdo con Iñigo García, entrevistado por Ismael Vargas, el análisis más adecuado de aplicar para determinar cuándo comprar o vender algún criptoactivo, es el análisis del potencial de utilidad de la blockchain concreta, debido que, al final, el valor de cualquier divisa está muy influenciado por cuanta gente lo utiliza para sus negocios. Esto, añadido a que además de pagos, con esta tecnología se pueden realizar multitud de operaciones, gestión de activos, gobernanza de empresas, y muchos casos de uso más que aún no se hayan ideado (García, 2017).

4.3. Brokers:

En el mundo de los criptoactivos, un bróker es el intermediario de las operaciones realizadas entre los vendedores y compradores de criptomonedas, debido a que estas operaciones frecuentemente

necesitan asesoría por los cambios, descensos, aumentos y la misma mecánica de las mencionadas operaciones (Criptotendencia, 2018).

En este contexto, los brokers son los sujetos encargados de realizar las ventas a los inversionistas, y por dicha labor, cobran comisiones por cada venta; ahora bien, estas comisiones pueden variar de acuerdo con la compañía. La más grande distinción entre los brokers regulares y los brokers de criptoactivos, es que la única forma de contactar con los segundos es vía online.

Ahora bien, es necesario poder elegir a un bróker que pueda cubrir las necesidades del inversionista y que tenga dentro de su cartera de clientes e inversiones, a los criptoactivos deseados por el usuario. Existen diversos factores que se debe tener en cuenta al momento de escoger un bróker: la fiabilidad del bróker, las condiciones para mantener una cuenta, el apalancamiento⁹ disponible, los instrumentos financieros que aplica, las comisiones que cobra, entre otros.

4.4. Wallets:

Tal y como ya ha sido establecido, tener un monedero virtual o wallet es el primer paso para poder utilizar criptodivisas; sin esta herramienta no se podrán recibir, almacenar o invertir criptomonedas (Pastor, 2018).

Una wallet es una interfaz que da acceso al usuario a la red de bloques en donde se encuentra la criptomoneda deseada; como ocurre con las cuentas bancarias, las wallet tienen un sistema de seguridad basado en criptografía asimétrica, en concreto, en el sistema de claves pública y privada (Pastor, 2018).

Cuando el ordenador envía un paquete de datos utilizando este sistema de claves, es posible determinar la identidad del usuario, también demostrando la existencia de claves privadas para su descriptación.

En concreto, la wallet no almacena los criptoactivos de los usuarios, debido a que estos se encuentran grabados en la cadena de bloques; lo que permite esta interfaz es guardar nuestras claves privadas que nos otorgan acceso a estas criptodivisas.

Existen distintos tipos de monederos para criptoactivos, los cuales ofrecen tanto ventajas como inconvenientes que tendrán que ser

⁹ Apalancamiento es la cualidad de las inversiones por contratos con diferencia (acuerdo por el que se intercambia la diferencia del valor de un activo en el momento de apertura del contrato y de su cierre); a través del apalancamiento se busca ajustar el costo que se requiere para invertir en algún activo.

analizados por los usuarios al momento de decidirse por uno de ellos; todo dependerá del estilo de administración deseado para dichas criptomonedas.

- Wallets de escritorio: Estos monederos se instalan en el ordenador del usuario; es un software que permite crear direcciones para enviar y recibir criptomonedas, además de almacenar las claves de los monederos con los que ya se han realizado transacciones (Pastor, 2018).
- Wallets móviles: Si el usuario necesita acceder a sus criptomonedas estando lejos de su ordenador, es indispensable que cuente a este tipo de monederos como una de sus herramientas. Estas wallets móviles almacenan las claves privadas de las distintas direcciones de criptoactivos y le brindan al usuario operabilidad desde su teléfono móvil a través de conexiones a internet o NFC (Pastor, 2018); es necesario precisar que los monederos que utilizan NFC no descargan muchas veces la cadena de bloques completa, porque es demasiado pesada y la transferencia por medio de esa tecnología no permite la comunicación de ese volumen de información.
- Wallets en la web: Este tipo de monederos funcionan en cualquier navegador web, lo que los vuelve sumamente accesibles; sin embargo, su principal desventaja es que el usuario no tiene control sobre los servicios ofrecidos, estos están controlados por una empresa que utiliza sus servidores para prestar este servicio (Pastor, 2018). También se consideran como sitios web que permiten a los usuarios movilizar su dinero de forma independiente, teniendo control exclusivo de sus llaves privadas y sin tener que instalar ningún software (Criptotendencia, 2018).
- Wallets Físicos: Estos monederos son dispositivos físicos que cuentan con un chip seguro que hace que no se puedan usar a menos que se identifiquen con la clave privada del usuario. Si se rompen o se pierden es posible restaurarlos con un mecanismo instalado por el fabricante; la ventaja fundamental es ese control total sobre esa clave privada y, por tanto, sobre las criptodivisas que se almacenan en ella. Este tipo de monederos son los que proporcionan mayor seguridad, y son ideales para almacenar criptodivisas a medio y largo plazo. (Pastor, 2018).

Los monederos de criptoactivos tienen las siguientes características:

- Control sobre la divisa: Las wallets permiten el manejo individual o conjunto de las criptodivisas, e incluso por parte de un tercero autorizado.

- Validación: Todos los wallets pueden utilizar validación completa, simplificada o centralizada, para validar las transacciones realizadas, dependiendo si se descarga completamente la cadena de bloques, solo los hash del bloque o el nodo completo de un tercero, respectivamente.
- Transparencia: El grado de transparencia del wallet y de las transacciones dependerán únicamente de los usuarios.
- Entorno: los usuarios pueden instalar los monederos de criptoactivos en entornos seguros o no seguros, dependiendo de sus necesidades y de sus conocimientos técnicos a aplicar para otorgar seguridad a sus transacciones.
- Privacidad: Finalmente, los usuarios pueden revelar o no su identidad a los demás, y permitir o no si es que desean que las empresas encargadas de crear criptoactivos asocien las transacciones a la IP del usuario.

4.5. Casos de Fraude en las ICOs:

Debido al riesgo existente, al invertir con fondos representados en divisas reales, es necesario señalar que han existido casos de fraude en el mundo de las ICO y de esa forma advertir a los usuarios y posibles inversionistas sobre este tipo de hechos; los más resaltantes son los siguientes.

- PlexCoin: esta ICO fue suspendida en diciembre de 2017 por la SEC de Estados Unidos como respuesta a una denuncia contra el creador de esta ICO, Dominic Lacroix. La denuncia alegaba que en esta ICO se estaba ofreciendo un falso retorno de la inversión de aproximadamente 1,354%; determinándose que no podía existir un retorno tan alto. La SEC congeló los \$15 millones de dólares recaudados por esta ICO desde agosto de 2017 y encarceló a su organizador (Kean, 2018).
- Benebit: Esta ICO afirmaba que utilizaba tokens en una plataforma de blockchain para unificar los programas de fidelización de clientes, tales como las millas de viajero frecuente; este proyecto contaba con todas las características de legalidad plasmadas en puntos anteriores del presente trabajo. No obstante, los usuarios empezaron a sospechar cuando las fotos mostradas en la página web provenían de la página de una escuela británica. Luego de que se descubriera esta irregularidad, el equipo de Benebit empezó a eliminar cualquier rastro de la ICO, haciéndose de forma ilegal de un aproximado de \$4 millones de dólares (Kean, 2018).

- Opair & Ebitz: Opair promovió un sistema basado en blockchain de tarjetas de débito utilizando su propio token el XPO; mientras que Ebitz se hacía pasar por un clon de otro criptoactivo. La comunidad de usuarios advirtió que los perfiles de LinkedIn del equipo de Opair eran falsos y que los correos de Ebitz se enviaban desde el servidor de Opair. Cuando se descubre la estafa, ambas ICO son desmanteladas, logrando reunir y hacer desaparecer alrededor de 400 BTC (Kean, 2018).
- REcoin y RDC: Estas dos empresas deseaban crear una criptomoneda respaldada por activos existentes en el mundo real, tales como bienes raíces y diamantes; no obstante, la SEC advirtió que ninguna de estas dos empresas había iniciado los proyectos por los cuales recolectó el dinero, tergiversando así la inversión. Según la SEC, el organizador de estas ICO, Maksim Zaslavsky, logró recaudar \$2 millones de dólares (Kean, 2018).
- PonziCoin: esta ICO se ofertaba como una moneda legítima y afirmaba ser el primer esquema Pozi legal del mundo; siendo esta una estafa a simple vista, el organizador de esta ICO logró obtener \$250,000.00 dólares y escapó con todo el dinero recaudado (Kean, 2018).

4.6. Implicaciones jurídicas de las ICOs

4.6.1. Cumplimiento en materia de Prevención de Blanqueo de Capitales

En la propuesta de Directiva Europea sobre la lucha contra el Blanqueo de Capitales COM (2016) 450 se señala como sujetos obligados al cumplimiento de la Directiva a los “Exchangers” distinguiendo dos tipos de Agentes de Cambio:

- 1) Agentes de Cambio que únicamente prestan servicios de cambio de monedas por monedas fiduciarias.
- 2) Agentes de Cambio que prestan servicios de monederos electrónicos, es decir que custodien las credenciales necesarias para acceder a monedas virtuales.

De acuerdo con Fernando Ramos (Ramos, 2018), se puede considerar que las obligaciones contenidas en la Directiva Europea sobre la lucha de Blanqueo de Capitales aplican a los Exchangers, pero no a las ICO por sí mismas, siempre y cuando estas actividades no se dediquen a cambiar criptoactivos por monedas fiduciarias.

No obstante, no se puede considerar a las cantidades superiores a 15,000€ dentro de lo dispuesto por la Ley 10/2010 de Prevención de Blanqueo de Capitales, debido a que los criptoactivos no son considerados como moneda fiduciaria, por el momento.

Ahora bien, dado a que los exchangers en el mundo real, si se dedican a cambiar criptoactivos o criptomonedas por divisas reales, si se encuentran sujetos a la normativa extranjera sobre blanqueo de capitales (Estados Unidos, Alemania, entre otras); por ese motivo, es recomendable que los participantes de una ICO se identifiquen plenamente con su DNI o Pasaporte, y que las transacciones por montos superiores a los 10,000€ cuenten con mayores diligencias de seguridad de parte de los usuarios.

En este punto, es necesario hacer mención de las acciones tomadas en otras legislaciones; por ejemplo, en Estados Unidos, las leyes de Know-Your-Customer son un medio esencial para poder realizar actividades económicas en donde se encuentren inmersas las criptodivisas (IBC Group, 2018).

Por otro lado, Singapur está buscando seguir los pasos de China y Corea del Sur, debatiendo sobre la posibilidad de prohibir las ICO en su territorio, debido a la alta posibilidad de servir como herramienta para el blanqueo de capitales proveniente del triángulo de oro asiático¹⁰ (IBC Group, 2018).

El cofundador de Ethereum, Vitalik Buterin, comentó que “es un hecho confirmado que el noventa por ciento de las nuevas empresas fracasan. Y también debería ser un hecho confirmado que el 90 por ciento de estos ERC20 en CoinMarket Cap acabarán en cero “ (Ramos, 2018).

4.6.2. Las implicaciones del Reglamento General de Protección de Datos.

De acuerdo con Fernando Ramos (Ramos, 2018), dejando de un lado las implicaciones en materia de protección de datos de las ICO al momento de recabar los datos de los usuarios que deseen realizar inversiones en estas plataformas; si no hay que tener en consideración acerca de los datos personales que se quedan almacenados en la blockchain,

¹⁰ El Triángulo de Oro Asiático es la zona comprendida entre las fronteras de Myanmar, Laos y Tailandia, por donde transcurre una larga parte del río Mekong, el 8vo río más largo del mundo; en esta zona existe una gran producción de opio y heroína.

debido a que estos permanecerán ahí y serán de conocimiento público de todo aquel que la haya almacenado, incumpléndose con el artículo 17 del RGPD:

“El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales”.

Asimismo, tomando en cuenta al punto 1 del artículo 4 del RGPD, las claves públicas de los wallets utilizadas en las transacciones con criptoactivos podrían ser consideradas como datos de carácter personal, en la medida que sirvan como medio para identificar al individuo portador de dicha clave (Ramos, 2018).

En ese sentido, en los supuestos donde no exista posibilidad alguna de identificar al titular de dichas claves, esto no será materia de protección de datos de carácter personal; siendo necesaria la seudonimización de los datos, con el propósito de otorgar mayores medidas de seguridad al tratamiento.

4.6.3. La contratación electrónica a distancia: la Ley de Servicios de la Sociedad de la Información y la Ley General de Defensa de Consumidores y Usuarios.

El proceso de contratación de la ICO, al ser electrónico y a distancia, deberá cumplir la Directiva 2000/31/CE relativa a los Servicios de la Sociedad de la Información y Comercio electrónico, así como la Directiva 2011/83/UE sobre derechos de los consumidores, en todos aquellos aspectos relativos a las condiciones generales de la contratación, deber de información, lenguaje claro, poner a disposición los T&C, pasos técnicos, entre otros (Ramos, 2018).

De acuerdo con el considerando II de la Ley 34/2002 Ley de los Servicios de la Sociedad de la Información y del Comercio Electrónico, se acogen los conceptos amplios de “servicios de la sociedad de la información”, incluyendo, pero no limitados a la contratación de bienes o servicios por vía electrónica, siempre que esto represente una actividad económica para el prestador.

En consecuencia, gracias a lo advertido anteriormente, las plataformas que ofrezcan servicios de Exchange, los creadores de criptodivisas y los que organizadores de ICO deben adoptar las medidas prescritas en la Ley 34/2002 si es que quieren iniciar labores económicas en el territorio español.

Asimismo, si es que los prestadores de servicios de la sociedad de la información no se encuentran en territorio español, la ley es aplicable a todo negocio que surta efectos en España.

Además, debido a la naturaleza del servicio brindado y a las implicaciones tanto financieras como sobre los datos personales de los usuarios, es necesario que se informe a los inversionistas sobre las medidas de seguridad tomadas por los prestadores de los servicios de la sociedad de la información, en este caso las plataformas de Exchange, los brokers, entre otros.

Un punto aparte es la importancia de contemplar lo dispuesto por el artículo 92 del Decreto Legislativo 1/2007, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios, en donde se prescribe que se regirán por todo lo dispuesto en el Título III los contratos celebrados a distancia con los consumidores y usuarios en el marco de un sistema organizado de venta o prestación de servicios a distancia; donde no se debe olvidar que de acuerdo al artículo 3 de la mencionada norma, los ciudadanos españoles que contratan con empresas que prestan servicios en una ICO.

4.7. Legislación Aplicable en la Unión Europea y en España

En la legislación española el hecho más relevante que determina el tratamiento de las ICO se encuentra en la definición de valor negociable de la Ley del Mercado de Valores. Específicamente, en el art. 2.1 de la mencionada ley donde se establece que: *“Tendrá la consideración de valor negociable cualquier derecho de contenido patrimonial, cualquiera que sea su denominación, que por su configuración jurídica propia y régimen de transmisión, sea susceptible de tráfico generalizado e impersonal en un mercado financiero.”* (Redacción, 2018)

Si bien, las ICO no cuentan con una regulación expresa en España, tampoco el Blockchain, según para qué se use una ICO, ésta puede ser incluida en el ámbito de aplicación de la Ley del Mercado de Valores (LMV) y, por lo tanto, estar sujeta a dicha regulación y al control de la CNMV (Plana, 2018).

Ya se ha mencionado en acápites anteriores que la CNMV, ha determinado dos condiciones importantes a tener en cuenta para clasificar a una ICO como valor negociable:

- El criptoactivo debe otorgar derechos o expectativas de participación en la potencial rentabilidad del proyecto, o se otorguen derechos similares a las acciones.

- Que el criptoactivo otorgue derechos para acceder a bienes o servicios desarrollados por la empresa que organiza la ICO.

En consecuencia, los valores emitidos a través de ICOs que puedan considerarse valores negociables, quedan sujetos a la Ley del Mercado de Valores y demás normas, como las MiFID II y demás (Plana Paluzie, 2018).

4.8. Recomendaciones.

- Descargar una wallet con buenas recomendaciones de parte de la comunidad on line; y aprender cómo utilizar correctamente todas las opciones brindadas en ella, para conocer el funcionamiento de la cadena de bloques que se encuentra contenida en ella.
- Estar al tanto del movimiento de la oferta y la demanda, para saber en qué ICO participar y si es que la inversión realizada podrá mantenerse en el tiempo, de acuerdo a la naturaleza del token adquirido.
- Revisar la identificación de los organizadores del ICO, puesto que si tienen experiencia deben tener algún tipo de comentarios en los foros especializados en el tema.
- Corroborar que lo afirmado en la página web de la ICO sea cierta, y verificar que esta página web y el servicio ofrecido cumpla con toda la normativa europea y española aplicable al caso en concreto.

V. CONCLUSIONES

- 1) Para la Unión Europea, el término moneda virtual se define como: *“la representación digital de valor no emitida por un Banco Central ni por una autoridad pública, ni necesariamente asociada a una moneda fiduciaria, pero aceptada por personas físicas o jurídicas como medio de pago y que puede almacenarse, transferirse o negociarse por medios electrónicos.”*
- 2) Los criptoactivos basan sus operaciones en la tecnología blockchain; esta tecnología funciona convirtiendo en un “bloque” a todas las transacciones realizadas en un período de tiempo determinado a través de la labor de los mineros, a este bloque se le aplicará un código hash que será aceptado por todos los mineros que trabajan con la mencionada blockchain para luego agregarla a la cadena de bloques.
- 3) Las wallets son programas que contienen en si misma a toda la blockchain de un determinado criptoactivo; estas almacenan toda la información necesaria para poder gestionar las criptodivisas de los usuarios.
- 4) Existen diversos tipos de criptoactivos, pero los más populares son las criptodivisas, los tokens y los Smart contracts. Los primeros son un medio de intercambio, los tokens pueden otorgar distintos valores a su propietario, mientras que los Smart contracts son algoritmos de ejecución automática.
- 5) Dependiendo de sus características, la naturaleza jurídica de un criptoactivo puede definirse como un título valor, un bien mueble o una moneda simple.
- 6) La ICO, puede hacer referencia tanto a la emisión de criptomonedas, como a la emisión de activos digitales de diversa naturaleza conocidos como Tokens (Banco de España - CNMV, 2018), que se encuentran asociados a proyectos empresariales que están en etapas de desarrollo o a proyectos que, por su naturaleza, no encuentran un financiamiento constante a través de los medios regulares.
- 7) Es necesario que los inversionistas en una ICO estén al tanto de los antecedentes del equipo organizador, de las características del token al cual se va a invertir, de cómo funciona una ICO, de las medidas de seguridad necesarias en las wallets a instalar y por último, conocer la rentabilidad de la inversión para que esta sea segura y se pueda mantener en el tiempo.

VI. BIBLIOGRAFÍA

- Al Khalil, F., Ceci, M., O'Brien, L., & Butler, T. (2017). *A Solution for the Problems of Translation and Transparency in Smart Contracts*. Dublin: Governance, Risk & Compliance Technology Centre.
- Arango - Arango, C., & Bernal Ramírez, J. (2017). *Criptomonedas*. Bogotá: Banco de la República - Colombia.
- Atzei, N., Bartoletti, M., Cimoli, T., Lande, S., & Zunino, R. (2017). SoK: Unraveling Bitcoin Smart Contracts. *7th International Conference on Principles of Security and Trust*. Thessaloniki: ETAPS.
- Bambara, J., & Allen, P. (2018). *Blockchain: A Practical Guide to Developing Business, Law and Technology Solutions*. Nueva York: McGraw Hill Education.
- Banco Central Europeo. (2016). *Dictamen del Banco Central Europeo de 12 de Octubre de 2016*. Fráncfort del Meno: Banco Central Europeo.
- Banco de España - CNMV. (2018). *Comunicado Conjunto de la CNMV y del Banco de España Sobre Criptomonedas y ICO*. Barcelona: Banco de España.
- Bastardo, J. (2 de setiembre de 2017). *Cómo Identificar una Estafa Encubierta en una ICO*. Obtenido de Criptonoticias: <https://www.criptonoticias.com>
- Benoiel, M. (4 de Agosto de 2017). *Startupgrind*. Obtenido de Understanding the Difference Between Coins, Utility Tokens and Tokenized Securities: <https://medium.com>
- Bradbury, D. (27 de mayo de 2013). *Chris Larsen: Ripple is HTTP for Money*. Obtenido de Coindesk: <https://www.coindesk.com>
- Bravo, J. A. (6 de noviembre de 2017). Criptomonedas y Tokens no son el mismo criptoactivo. (A. Preuskchat, Entrevistador)
- Buterin, V. (2016). *Smart Contracts: The Blockchain Technology That Will Replace Lawyers*. Obtenido de Blockgeeks: <https://blockgeeks.com>
- Buterin, V. (6 de enero de 2018). *Explanation of DAICO*. Obtenido de Research: <https://www.ethresearch.ch>
- Carbó Valverde, S., & Rodríguez Fernández, F. (2017). Economía de los Criptoactivos: Mitos, Realidades y Oportunidades. *Economía y Finanzas Españolas*, 1 - 13.
- Cazorla, L. (8 de junio de 2018). *El Blog de Luis Cazorla*. Obtenido de Tokens y Criptomonedas: Algunas Reflexiones Sobre su Naturaleza Jurídica: <http://www.luiscazorla.com>
- CCM. (04 de junio de 2018). *Internet (protocolos)*. Obtenido de CCM Web Site: <https://es.ccm.net>
- Chohan, U. M. (2017). *Cryptocurrencies: A Brief Thematic Review*. Canberra: School of Business and Economics, University of New South Wales.
- Clayton, J. (2017). *Statement on Cryptocurrencies and Initial Coin Offerings*. Washington D.C.: U.S. Securities and Exchanges Comission.

- Comisión Europea. (2016). *Directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo*. Estrasburgo: Parlamento Europeo.
- Criptonetwork. (02 de Mayo de 2018). *Wallets de Bitcoin y Criptomonedas*. Obtenido de Investing: <https://es.investing.com>
- Criptotendencia. (16 de diciembre de 2017). *¿Qué es y como funciona la oferta y la demanda en las criptomonedas?* Obtenido de Cripto Tendencia: <https://www.criptotendencia.com>
- Criptotendencia. (1 de enero de 2018). *¿Qué son los Brokers Online?* Obtenido de Criptotendencia: <https://www.criptotendencia.com>
- Crypto Economy. (12 de mayo de 2018). *Las mecas de las ICO en Asia: Honkong y Singapur*. Obtenido de Cryptoeconomy: <https://www.crypto-economy.net>
- Davies, S. (2016). *What is Ethereum? A Step-by-Step Begginers Guide*. Obtenido de Blockgeeks: <https://blockgeeks.com>
- Dinero. (23 de febrero de 2017). *Cuatro Formas de Conseguir Bitcoins*. Obtenido de Dinero: <https://www.dinero.com>
- Drombovskis, V. (26 de febrero de 2018). EU says stands ready to regulate crypto-currencies. (H. Jones, Entrevistador)
- EFE. (12 de enero de 2018). Corea del Sur estudia prohibir la negociación en criptomonedas. *Expansión*. Seúl, Area Capital de Seúl, Corea del Sur.
- Escribano, G. (23 de febrero de 2018). *Diccionario para entender qué son y cómo funcionan las criptodivisas*. Obtenido de La Fiebre del Bitcoin: <https://cincodias.elpais.com>
- Europa Press. (10 de mayo de 2018). Mercado Financiero. *La CNMV aplicará la normativa de valores a las criptomonedas hasta que haya regulación europea*. Madrid, Madrid, España.
- Financial Action Task Force. (2015). *Guidance for a Risk-Based Approach: Virtual Currencies*. París: FATF/OECD.
- Freeman, D. B., & Nutting, M. R. (2015). *A Brief History of Crowdfunding*. Chicago: Freedman .
- García García, E., & Ivars Bañuls, J. A. (2004). *La Firma Electrónica al Servicio del Ciudadano*. Madrid: Tirant Lo Blanc.
- García, Í. (21 de setiembre de 2017). *¿Cómo operar en criptodivisas? Plataformas, mercados, liquidez...* Entrevista a Íñigo García. (I. Vargas, Entrevistador)
- Giupponi, E. (12 de Abril de 2018). *Criptoactivos: ¿son una fuente de riesgo financiero?* Obtenido de El Cronista: <https://www.cronista.com>
- Gurrea Martínez, A. (23 de marzo de 2018). *Centro de Estudios Garrigues*. Obtenido de Problemática Jurídica y Financiera de las ICO'S: <http://blog.centrogarrigues.com>

- Gurrea Martínez, A., & Remolina León, N. (11 de abril de 2018). *Problemática Jurídica y Financiera de las ICO*. Obtenido de Hay Derecho: <https://hayderecho.com>
- IBC Group. (21 de febrero de 2018). *Como evitar el blanqueo de capitales en una ICO*. Obtenido de IBC Group: <https://ibcgroup.io>
- ICO4YOU. (15 de junio de 2018). *ICO Manual*. Obtenido de Trusted Initial Coin Offerings: <https://ico4you.com>
- Idalion, A. (2017). *Blockchain: The complete guide to understanding Blockchain Technology for beginners in record time*. Auto publicado.
- Islas, P. (22 de diciembre de 2017). *IDC Online*. Obtenido de Bitcoin: su naturaleza jurídica: <https://idconline.mx>
- Jimenez, A. (12 de diciembre de 2016). *¿Qué es el Trading?* Obtenido de Microdinero: <https://www.vivus.es>
- Kean, B. (20 de febrero de 2018). *No creas en el "hype". Las cinco mayores "estafas de salida de las ICOs": Opinión de Expertos*. Obtenido de Cointelegraph: <https://es.cointelegraph.com>
- Llovera Aguirre, M. (04 de Diciembre de 2017). *Criptoactivos en Palabras Sencillas*. Obtenido de LinkedIn: <https://es.www.linkedin.com>
- Matonis, J. (2015). *Bitcoin 101*. Londres: Thomson Reuters.
- Nakamoto, S. (06 de junio de 2018). *Bitcoin: a Peer to Peer Electronic Cash System*. Obtenido de Bitcoin: <https://www.bitcoin.org>
- Naryanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrencies Technologies*. Princeton: Princeton University Press.
- Pastor, J. (28 de enero de 2018). *Monederos físicos de bitcoin: qué son y cómo funcionan a la hora de proteger tus inversiones*. Obtenido de Xataka: <https://www.xataka.com>
- Pérez, I. (04 de junio de 2018). *Protocolo de Comunicación de Internet Hace Vulnerables las Transacciones Bitcoin*. Obtenido de Criptonoticias: <https://www.criptonoticias.com>
- Pertínez Vílchez, F., Bercovits Rodríguez-Cano, R., & González de Alaiza Cardona, J. J. (2010). *Los Contratos de Adhesión y La Contratación Electrónica*. Madrid: Tirant Lo Blanc.
- Plana Paluzie, A. (02 de mayo de 2018). *Marco jurídico de las initial coin offering – ICO en España*. Obtenido de Law & Trends: <https://www.lawandtrends.com>
- Plana, A. (11 de mayo de 2018). Regulación de las Initial Coin Offering – ICO en España. *Diario Jurídico*. Madrid, Madrid, España.
- Pollock, D. (14 de marzo de 2018). *Cointelegraph*. Obtenido de Utility or Security Token: <https://cointelegraph.com>
- Ramos, F. (12 de marzo de 2018). *La Digitalización Del Sector Financiero Tokens e ICOs: Consideraciones Previas (2ª parte de 3)*. Obtenido de DPO&IT Law: www.dpoitlaw.com

- Real Casa de la Moneda - Fábrica Nacional de la Moneda y Timbre. (2009). *La Administración Electrónica y el Servicio a los Ciudadanos*. Madrid: Gobierno de España - Ministerio de Economía y Hacienda.
- Redacción. (11 de mayo de 2018). *Regulación de las Initial Coin Offering – ICO en España*. Obtenido de Diario Jurídico: <https://www.diariojuridico.com>
- Redes Informaticas 4to. (04 de junio de 2018). *Protocolos de Comunicación*. Obtenido de Redes Informaticas web site: <http://www.redesinformaticas4to.blogspot.com>
- Rivero, J. (16 de Febrero de 2018). *Autoridad Financiera de Suiza Regula las ICO y Clasifica Tres Tipos de Tokens*. Obtenido de Criptonoticias: <https://www.criptonoticias.com>
- Secretaría de Estado de Hacienda - Dirección General de Tributos. (2017). *Compraventa de Criptomonedas a través del desarrollo y explotación de una web propia*. Madrid: Hacienda.
- Sentencia , C-264/14 (Tribunal de Justicia de la Unión Europea 22 de octubre de 2015).
- Serrano, E. (15 de Diciembre de 2017). *¿Qué es un Wallet?* Obtenido de Guia Bitcoin: <https://guiabitcoin.com>
- Steemit. (17 de Julio de 2017). *Tipos de Monederos para Criptomonedas*. Obtenido de Steemit Beta: <https://steemit.com>
- Suberg, W. (02 de agosto de 2017). Singapur aclara regulación de los token de las ICO, sigue a EE.UU. *Cointelegraph*.
- Subramanya, A. (23 de febrero de 2018). *Initial Coin Offering (ICO)- Legal Status under the laws of the United States of America and India*. Obtenido de Medium: <https://www.medium.com>
- Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. Sebastopol, California: O'Reilly Media, Inc.
- Tar, A. (31 de octubre de 2017). *Smart Contract, Explained*. Obtenido de Cointelegraph: <https://cointelegraph.com>

VII. ANEXOS

Anexo A: Dictamen del Banco Central Europeo

BANCO CENTRAL EUROPEO

DICTAMEN DEL BANCO CENTRAL EUROPEO de 12 de octubre de 2016 sobre una propuesta de directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica la Directiva 2009/101/CE (CON/2016/49) (2016/C 459/05)

Introducción y fundamento jurídico El 19 de agosto de 2016 y el 23 de septiembre de 2016, el Banco Central Europeo (BCE) recibió del Consejo y del Parlamento Europeo sendas solicitudes de dictamen sobre una propuesta de directiva por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica la Directiva 2009/101/CE (1) (en lo sucesivo, «directiva propuesta»).

La competencia consultiva del BCE se basa en el artículo 127, apartado 4, y el artículo 282, apartado 5, del Tratado de Funcionamiento de la Unión Europea, pues la directiva propuesta contiene disposiciones que afectan a las competencias del BCE. En particular, la competencia consultiva del BCE se basa en el artículo 127, apartados 2 y 5, y el artículo 128, apartado 1, del Tratado, pues la directiva propuesta contiene disposiciones que afectan a ciertas funciones del Sistema Europeo de Bancos Centrales (SEBC), incluidas las de promover el buen funcionamiento de los sistemas de pago, contribuir a la buena gestión de las políticas que lleven a cabo las autoridades competentes con respecto a la estabilidad del sistema financiero, y autorizar la emisión de billetes de banco en euros en la Unión. De conformidad con la primera frase del artículo 17.5 del Reglamento interno del Banco Central Europeo, el presente dictamen ha sido adoptado por el Consejo de Gobierno.

1. Observaciones 1.1. Regulación de los proveedores de servicios de cambio de monedas virtuales y custodia de monederos electrónicos 1.1.1. La directiva propuesta amplía la lista de entidades a las que obliga la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo (2) para incluir en ella a los proveedores que presten principal y profesionalmente servicios de cambio de monedas virtuales por monedas fiduciarias [entendidas en la directiva propuesta como las monedas declaradas de curso legal (3)] y a los proveedores de servicios de custodia de monederos electrónicos que ofrezcan servicios de custodia de las credenciales necesarias para acceder a monedas virtuales (en lo sucesivo, los «proveedores de servicios de custodia de monederos electrónicos») (4). La directiva propuesta exige además a los Estados miembros que se aseguren de que los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias y los proveedores de servicios de custodia de monederos electrónicos estén autorizados o registrados (5). El BCE apoya resueltamente estas normas, que son conformes con las recomendaciones del Grupo de Acción Financiera (GAFI) (6), ya que los terroristas y otros grupos de delincuentes son actualmente capaces de

(1) COM(2016) 450 final. (2) Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) n.º 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión (DO L 141 de 5.6.2015, p. 73). (3) Véase el considerando 6 de la directiva propuesta. (4) Véanse el considerando 6 y el artículo 1, punto 1, de la directiva propuesta. (5) Véase el artículo 1, punto 16, de la directiva propuesta. (6) Véanse en la dirección del GAFI en internet (www.fatf-gafi.org) los documentos siguientes: «International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations» (febrero de 2012); «Virtual Currencies Key Definitions and Potential AML/CFT Risks» (junio de 2014), y «Guidance for a Risk-Based Approach-Virtual Currencies» (junio de 2015).

transferir fondos en redes de monedas virtuales ocultando las transferencias o aprovechando cierto grado de anonimato en esas plataformas de cambio. El uso de monedas virtuales supone además mayores riesgos que los medios tradicionales de pago en el sentido de que la transferibilidad de las monedas virtuales se basa en la internet y no tiene otro límite que la capacidad de la red subyacente de ordenadores e infraestructura de tecnología informática de la moneda virtual de que se trate.

En este contexto, el BCE entiende además que las monedas digitales no tienen que cambiarse necesariamente por monedas legalmente establecidas, sino que pueden también utilizarse para adquirir bienes y servicios sin necesidad de cambiarse por monedas legalmente establecidas o recurrir a un proveedor de servicios de custodia de monederos electrónicos. Esas operaciones no estarían comprendidas en ninguna de las medidas de control establecidas en la directiva propuesta y podrían ser un medio de financiación de actividades ilícitas.

1.1.2. El BCE reconoce que los avances tecnológicos que presenta la tecnología de registros distribuidos subyacente a medios de pago alternativos como las monedas virtuales tienen el potencial de incrementar la eficiencia, el alcance y la variedad de los métodos de pago y transferencia. Sin embargo, los órganos legislativos de la Unión deben evitar aparecer como impulsores del uso de monedas digitales establecidas con carácter privado, pues estos medios de pago alternativos ni están legalmente establecidos como monedas ni son monedas de curso legal emitidas por bancos centrales y otros poderes públicos (1). Preocupan al BCE varias de las diferencias entre lo que la directiva propuesta llama «monedas fiduciarias» y las «monedas virtuales». Una de estas diferencias es la volatilidad vinculada a las monedas virtuales, que es normalmente mayor que la de las monedas emitidas por bancos centrales o cuya emisión autorizan estos, pues esta volatilidad no siempre parece relacionada con factores económicos o financieros. Además: a) a diferencia de los tenedores de monedas legalmente establecidas, los tenedores de unidades monetarias virtuales carecen normalmente de la garantía de poder cambiar dichas unidades por bienes y servicios o monedas legalmente establecidas en el futuro, y b) la confianza de los actores económicos en las monedas virtuales, de aumentar sustancialmente en el futuro, podría, en principio, afectar al control de los bancos centrales sobre la oferta monetaria, lo que podría suponer un riesgo para la estabilidad de precios, si bien en la práctica actual dicho riesgo es limitado. Por lo tanto, aunque conviene que los órganos legislativos de la Unión, de acuerdo con las recomendaciones del GAFI, regulen las monedas virtuales desde el punto de vista de la lucha contra el blanqueo de capitales y la financiación del terrorismo, su objetivo en este ámbito no debe ser fomentar una mayor utilización de las monedas virtuales.

1.1.3. La directiva propuesta define el término «monedas virtuales» como la «representación digital de valor no emitida por un banco central ni por una autoridad pública, ni necesariamente asociada a una moneda fiduciaria, pero aceptada por personas físicas o jurídicas como medio de pago y que puede transferirse, almacenarse o negociarse por medios electrónicos» (2).

(1) Véase la página 13 de la exposición de motivos que acompaña a la directiva propuesta, así como sus considerandos 6 y 7. Véase también el proyecto de informe sobre monedas virtuales de la Comisión de Asuntos Económicos y Monetarios del Parlamento Europeo [2016/2007(INI)], de 23 de febrero de 2016. (2) Artículo 1, punto 2, letra c), de la directiva propuesta. La definición parece basarse en la propuesta en el apartado 19 del Dictamen de la Autoridad Bancaria Europea (ABE) sobre las monedas virtuales (EBA/Op/2014/08), de 4 de julio de 2014, disponible en inglés en la dirección de la ABE en internet: www.eba.europa.eu. (3) Véase la definición de «moneda» en el artículo 2, letra a), de la Directiva 2014/62/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a la protección penal del euro y otras monedas frente a la falsificación, y por la que se sustituye la Decisión marco 2000/383/JAI del Consejo (DO L 151 de 21.5.2014, p. 1). Véase también la página 16 de la «Staff Discussion Note» del Fondo Monetario Internacional (FMI) titulada «Virtual Currencies and Beyond: Initial Considerations» (enero de 2016), disponible en la dirección del FMI en internet: www.imf.org. (4) Véanse el preámbulo y el artículo 3, apartado 4, del Tratado de la Unión Europea; el artículo 119, apartado 2, del Tratado de Funcionamiento de la Unión Europea, y el artículo 2 del Reglamento (CE) n.º 974/98 del Consejo, de 3 de mayo de 1998, sobre la introducción del euro (DO L 139 de 11.5.1998, p. 1).

El BCE tiene varias observaciones particulares que formular sobre esta definición.

En primer lugar, las «monedas virtuales» no son monedas desde el punto de vista de la Unión (3). Conforme a los Tratados y lo dispuesto en el Reglamento (CE) n.º 974/98 del Consejo, el euro es la moneda única de la unión económica y monetaria, es decir, de los Estados miembros que han adoptado el euro como su moneda (4).

En coherencia con el planteamiento ya adoptado o en estudio en otros países que regulan los servicios de cambio de monedas virtuales, como Canadá, Japón y Estados Unidos, el BCE recomienda definir con mayor detalle las monedas virtuales aclarando expresamente que no son monedas o dinero legalmente establecido (1).

En segundo lugar, puesto que las monedas virtuales no son en realidad monedas, sería más exacto considerarlas como medio de cambio, no de pago. Además, la definición por la directiva propuesta de las monedas virtuales como medio de pago olvida que en ciertas circunstancias dichas monedas pueden utilizarse para fines distintos del de medio de pago (2). Como observa el Banco de Pagos Internacionales (BPI), la tecnología de registros distribuidos subyacente a muchos sistemas de monedas digitales podría tener aplicaciones mucho más amplias que las de pago (3). El GAFI observa al respecto que, entre los usos de las monedas virtuales distintos de los de pago, puede citarse el de depósito de valor para ahorro o inversión, como los derivados, los productos básicos y los valores (4). Las monedas digitales más recientes, basadas en una tecnología más compleja de registros distribuidos y cadenas de bloques, tienen una serie de aplicaciones que van más allá del pago (5), inclusive, por ejemplo, la de casino en línea. En vista de lo expuesto, el BCE sugiere que la directiva propuesta, al definir las monedas virtuales, se refiera también a otros posibles usos de estas.

El BCE propone que la definición de monedas virtuales de la directiva propuesta se adapte de manera que tenga en cuenta los aspectos a los que se ha hecho referencia.

1.2. Registros centrales de cuentas bancarias y de pago 1.2.1. La directiva propuesta dispone que los Estados miembros implanten mecanismos centralizados automatizados, como registros centrales o sistemas centrales electrónicos de consulta de datos, que permitan identificar en tiempo oportuno a cualquier persona física o jurídica que posea o controle cuentas de pago y cuentas bancarias en una entidad de crédito en su territorio (6). La exposición de motivos que acompaña a la directiva propuesta aclara al respecto que los Estados miembros son libres de establecer sea un registro central de entidades bancarias, sea un sistema de consulta de datos, según lo que mejor se adapte a su marco existente (7). Por lo tanto, los Estados miembros tienen libertad para designar a su banco central nacional (BCN) como administrador del registro central de cuentas bancarias (y de pago). Además, conforme a la directiva propuesta, tendrían acceso al registro central las unidades de información financiera y otras autoridades competentes.

1.2.2. El BCE ya ha manifestado con anterioridad su opinión de que, a efectos de determinar si se ha infringido la prohibición de financiación monetaria establecida en el Tratado, las tareas encomendadas a un BCN en el Sistema Europeo de Bancos Centrales (SEBC) relacionadas con la creación de un registro central de cuentas bancarias no deben considerarse funciones de banca central ni facilitan el cumplimiento de funciones de esta clase (8).

(1) Véanse, por ejemplo, los artículos 2 a 5 de la Ley japonesa de servicios de pago, que definen las cibermonedas de manera que se excluye el yen y las monedas extranjeras, y el artículo 103, apartado 8, de la «Draft Regulation of Virtual Currency Businesses Act» de la Conferencia nacional de comisarios de Estados Unidos para unas leyes estatales uniformes, de 2 de febrero de 2016, que define la moneda virtual de manera que se excluye el dinero. Puede verse un amplio análisis del tratamiento regulador de Bitcoin en 41 países en el informe de la Biblioteca jurídica del Congreso de Estados Unidos titulado «Regulation of Bitcoin in Selected Jurisdictions», (enero de

El BCE considera que la tarea de crear un registro central conforme al artículo 30 de la Directiva (UE) 2015/849 es claramente una tarea gubernativa, pues su finalidad es luchar contra el blanqueo de capitales y la financiación del terrorismo. A fin de salvaguardar la independencia financiera de los miembros del SEBC y disipar las dudas sobre financiación monetaria vinculadas al desempeño de una tarea gubernativa, el BCE subraya que, en relación con la asunción de la función de gestión de un registro central de cuentas, la legislación nacional que incorpore al derecho interno la directiva propuesta debe incluir un mecanismo de recuperación de costes con procedimientos expresos de seguimiento, asignación y facturación de todos los gastos efectuados por el BCN respecto de la gestión del registro central y el acceso a este.

2. Observaciones técnicas y propuestas de redacción En un documento técnico de trabajo separado figuran las propuestas de redacción específicas, acompañadas de explicaciones, correspondientes a las recomendaciones del BCE encaminadas a modificar la directiva propuesta. El documento técnico de trabajo está disponible en inglés en la dirección del BCE en internet.

Hecho en Fráncfort del Meno, el 12 de octubre de 2016.

El Presidente del BCE Mario DRAGHI

2014). Véanse también las actas de la Comisión permanente del Senado de Canadá sobre banca, intercambio y comercio, de 26 de marzo de 2014, en las que el Departamento de Finanzas de Canadá declara que la moneda virtual no es la moneda oficial del país; no es el dólar canadiense. (2) Véase la página 24 del informe del BCE «Virtual Currency Schemes — a further analysis» (febrero de 2015), disponible en la dirección del BCE en internet: www.ecb.europa.eu. (3) Véase la página 15 del informe del Comité de Pagos e Infraestructuras del Mercado del BPI titulado «Digital currencies» (noviembre de 2015), disponible en www.bis.org. (4) Por ejemplo, criptomonedas como el «ether», unidad monetaria de la cadena de bloques «ethereum», se negocian en bolsas con fines de inversión y especulativos, pero no siempre se usan como medio de pago. Véase también la página 4 del documento del GAFI «Guidance for a risk based approach-Virtual Currencies» (junio de 2015), disponible en la dirección del GAFI en internet: www.fatf-gafi.org. (5) Véase la página 7 de la «Staff Discussion Note» del FMI titulada «Virtual Currencies and Beyond: Initial Considerations» (enero de 2016), disponible en la dirección del FMI en internet: www.imf.org. (6) Véase el artículo 1, punto 12, de la directiva propuesta. (7) Véase la página 7 de la exposición de motivos que acompaña a la directiva propuesta. (8) Véanse, por ejemplo, el apartado 2.1 del Dictamen CON/2011/30; el apartado 2 del Dictamen CON/2011/98; los apartados 3.1 y 3.2 del Dictamen CON/2015/46, y los apartados 3.1 a 3.8 del Dictamen CON/2016/35. Todos los dictámenes del BCE están disponibles en la dirección del BCE en internet: www.ecb.europa.eu.