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

2018-2019

Trabajo Fin de Máster

"Informe: atribución de responsabilidades en los mercados de monedas virtuales"

Jorge Somolinos Calvo

Tutor: Fernando Mª Ramos Suárez

Facultad de Puerta de Toledo, 27 de septiembre de 2019

DETECCIÓN DEL PLAGIO

La Universidad utiliza el programa **Turnitin Feedback Studio** *para* comparar la originalidad del trabajo entregado por cada estudiante con millones de recursos electrónicos y detecta aquellas partes del texto copiadas y pegadas. Copiar o plagiar en un TFM es considerado una **Falta Grave**, y puede conllevar la expulsión definitiva de la Universidad.

ÍNDICE

ÍNDICE 1

ANTECEDENTES 2

NORMATIVA ANALIZADA 3

INFORME 4

1. INTRODUCCIÓN 4

1.1. Monedas virtuales y *tokens* 4

1.2. Blockchain 9

1.3. Smart contracts 14

2. ANÁLISIS DE LA NORMATIVA 17

2.1. Régimen general 17

2.2. Ley de Servicios de la Sociedad de la Información 20

2.3. Ley de Prevención de Blanqueo de Capitales y Financiación del Terrorismo 22

2.4. PROTECCIÓN DE DATOS 26

2.5. MiFID II Y MIFIR 31

2.6. Ley de Servicios de Pago 34

CONCLUSIONES 37

1. El futuro inmediato. 38

BIBLIOGRAFÍA, NORMAS Y DOCUMENTOS UTILIZADOS 42

1. BIBLIOGRAFÍA 42

2. DOCUMENTOS 43

3. NORMAS 44

ANTECEDENTES

La empresa Crypto Assets, S.L. (en adelante, "Crypto Assets"), es una *start-up* de reciente creación especializada en la *tokenización* de activos inmuebles. Es decir, digitalizan activos reales, asignándoles un determinado número de fichas, que después podrán ser adquiridas por los clientes con fines de inversión. El valor del inmueble, en este caso, tendrá un valor fijo reflejado en *tokens* o fichas, lo que permitirá que, ante aumentos de precio del bien, aumente el valor de cada uno de ellos.

Además, la empresa se empleará la plataforma ya existente de Ethereum como base para crear sus propios *tokens*, empleando el estándar ERC-20 de la misma, y por tanto no prestará servicios de intercambio de dinero ni similar. Cada *token* se intercambiará directamente por los Ethers de la plataforma.

El presente informe tiene por objeto analizar si Crypto Assets deberá cumplir con los siguientes marcos normativos, a fin de establecer posibles contingencias por responsabilidad en caso de incumplimiento:

- Régimen General
- Servicios de la Sociedad de la Información.
- Prevención del Blanqueo de Capitales y Financiación del Terrorismo.
- MiFID II y MIFIR.
- Protección de Datos
- Medios de Pago.

NORMATIVA ANALIZADA

- Código Civil de24 de julio de 1889.
- Directiva (UE) 2014/65, relativa a los mercados de instrumentos financieros, de 15 de mayo.
- Directiva (UE) 2015/849, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, de 20 de mayo.
- Directiva (UE) 2015/849, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, de 20 de mayo.
- Directiva (UE) 2018/843, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE.
- Directiva (UE) 2019/713, sobre la lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo, de 17 de abril.
- Directiva (UE) 2019/713, sobre la lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo, de 17 de abril.
- Ley 34/2002, de Servicios de la Sociedad de la Información
- Real Decreto 1464/2018, de 21 de diciembre, por el que se desarrollan el texto refundido de la Ley del Mercado de Valores
- Reglamento (UE) 600/2014, relativa a los mercados de instrumentos financieros, de 15 de mayo.

INFORME

1. INTRODUCCIÓN

Dada la importancia de comprender los fundamentos que subyacen en el modelo de negocio de Crypto Assets, debemos iniciar el presente informe con una introducción sobre los elementos tecnológicos.

1.1. Monedas virtuales y *tokens*

Actualmente se estima que existen cerca de 2.300 monedas virtuales diferentes[1], y creciendo (a principios de 2019, por ejemplo, se estimaba que había en torno a 1200[2]). Pero esto no impide que pueda existir una definición que englobe, con más o menos precisión, todas estas variantes. En efecto, una moneda virtual se puede definir de forma muy sencilla como una unidad abstracta con valor económico propio y que, a priori, permite llevar a cabo transacciones únicamente entre los usuarios de una misma plataforma. Ahora bien, ¿qué implica esta definición?

Al denominarla como una "unidad abstracta" se pone de relieve que no tiene representación física; existe únicamente en la Red. Esto, pese a lo innovador del concepto de "moneda virtual", no es algo nuevo para los que llevamos ya muchos años usando tarjetas de crédito o débito, o incluso el *smartphone* para llevar a cabo transacciones.

Lo verdaderamente revolucionario que acompaña a este hecho es su estrecha relación con la descentralización, ese "valor propio". Esto se debe a que no existe ningún Estado detrás de monedas virtuales como el Bitcoin, no hay vinculación directa a moneda *fiat* de ninguna clase. La comunidad internacional, hasta hace relativamente poco, apenas ha prestado atención a este tipo de activos, en gran parte debido a que su valor real no suponía un foco de peligro para la economía de los Estados (en 2018 se estimó que, en el momento de mayor cotización del Bitcoin, su peso en el PIB mundial rondaba el 1%[3]). Sin embargo, recientemente se han visto avances en este sentido, como las posturas defensivas que han adoptado países como China o Corea del Norte, o la reticencia con la que muchos países han acogido la nueva moneda virtual proyectada por Facebook y otros socios (Libra) que

[1] Dato extraído de https://coinmarketcap.com, que contiene una de las listas más exhaustivas en materia de moneda virtuals (consultado el 30/07/2019).
[2] LEGERÉN MOLINA, A., *Retos jurídicos que plantea la tecnología de la cadena de bloques. Aspectos legales de blockchain*, Revista de Derecho Civil, vol. VI, núm. 1 (enero-marzo), Estudios, A Coruña, 2019, página 209.
[3] CARRERAS BAQUER, O., *¿Qué podemos esperar de las Moneda virtuals?*, "Dossier: el dinero: pasado, presente y futuro", Caixabank Research, 2018, 2018.

sugieren que los gobiernos están empezando a prepararse ante el potencial disruptor que tiene una nueva clase de moneda que, por su propia naturaleza, es internacional y ajena a todo tipo de intervención externa.

Esta situación de ajenidad al sistema monetario y financiero suponen tanto ventajas como inconvenientes, sobre todo en un contexto como el actual, postcrisis, en el que arrastramos una enorme desconfianza en la capacidad de bancos y gobiernos para gestionar el dinero de los ciudadanos (se considera que existen unos 1.700 millones de personas que se encuentran fuera del sistema financiero a día de hoy[4]). Por una parte, su uso es totalmente digital y globalizado, lo que favorece su uso para operaciones instantáneas entre distintos países, y la falta de regulación permite que se desarrollen adaptándose a las necesidades de sus usuarios. La otra cara de la moneda es que esta misma falta de control limita mucho la seguridad jurídica, que muchas veces crea inseguridades que no se ven del todo paliadas aunque el código sea férreo y sin fisuras: a fin de cuentas, éste podrá controlar lo que ocurre cuando se llevan a cabo transacciones, pero no es habitual que lo haga con lo que ocurre "alrededor" -estableciendo, por ejemplo, un régimen de responsabilidades o garantías contra el blanqueo de capitales y la financiación del terrorismo-.

Por último, está el hecho de que es un tipo de moneda que sólo puede ser empleada a través de una determinada plataforma. Como se menciona anteriormente, esa era la idea inicial, ya que cuando nació este "movimiento" la interseccionalidad era muy limitada. No obstante, hoy en día ya existen *exchanges* que facilitan un servicio de intercambio de monedas virtuales, pero sin estos intermediarios privados, Bitcoins y Ethers, por ejemplo, no podrían intercambiarse; es decir, si X tuviera, en este caso, 10 bitcoins y quisiera hacer una transacción en Ethers, tendría que adquirir Ethers con dinero "real", pero no podría hacerlo con los Bitcoins que ya tiene. Esto supondría un límite enorme a la capacidad transaccional de estos activos y, por tanto, su valor se vería seriamente afectado. En cualquier caso, como digo este es un problema que está más que superado.

Y es en este punto que resulta interesante hablar de los *tokens* propios. En el caso de CRYPTO ASSETS, la idea se fundamenta en la creación de unas fichas propias que sirven única y exclusivamente para llevar a cabo transacciones dentro de la parcela propia de esta empresa. Por ello, no se puede decir que estos *tokens* sean monedas virtuales

[4] Galán, J., *Blockchain y la nueva moneda virtual Libra, concepto a concepto*, El País Economía, 2019 (consultado en https://retina.elpais.com/retina/2019/07/12/innovacion/1562924481_828592.html el 26/06/2019).

realmente, ya que carecen del carácter de activo intercambiable por otros similares o de medio de pago que se les atribuye a las divisas. Así, podemos decir que el proyecto de CRYPTO ASSETS no supone la creación de una moneda virtual: emplea la que ya ha creado Ethereum (Ether) para crear unas fichas que tienen un valor determinado en relación con ésta, que sí lo es.

Un último punto a tener en cuenta es que las monedas virtuales adolecen, a día de hoy, de una elevada volatilidad. No tener un Banco Central detrás que las regule y les otorgue solidez hace que su cotización se sustente principalmente sobre la ley de la oferta y la demanda y la eficacia de los algoritmos que las "ordenan" y, a un nivel aún más esencial, en el valor que les otorgue el mercado, en la confianza y la credibilidad que son capaces de generar, lo que, a principios de 2018, situaba su tasa de volatilidad diaria en un 7%, un 125% anual[5].

Debemos recordar en todo momento que España no tiene una regulación específica en materia monedas virtuales y Europa las contempló en la suya hace apenas dos años (aunque hace algo más que tienen un ojo puesto sobre este tipo de tecnologías[6]), por lo que, en un informe como este, relativo a la responsabilidad en los mercados de moneda virtual, nos interesará más saber *qué no son*. Este análisis se llevará a cabo más adelante, pero podemos adelantar que su importancia reside en el hecho de que pocas normas sectoriales que actualmente puedan aplicarse a un modelo de negocio como el que proyecta CRYPTO ASSETS.

Una vez definido el concepto de moneda virtual, pasaré a describirlas un poco más en profundidad, diferenciando sus clases para establecer unas nociones más específicas que ayuden a entender las características del modelo concreto de negocio que plantea CRYPTO ASSETS.

Se han definido cuatro tipos de monedas virtuales, basados en el uso que se les dé a sus *tokens*[7]:

---

[5] MATUTE, M., *Las 'Moneda virtuals': alarma mundial*, Escritura pública, 2018 (consultado en https://www.notariado.org/liferay/c/document_library/get_file?folderId=12092&name=DLFE-320372.pdft el 17/08/2019).

[6] Dictamen 2017/C-246/02, de 26 de abril, del Comité Económico y Social Europeo sobre «Digitalización y modelos económicos innovadores en el sector financiero europeo, consecuencias para el empleo y para la clientela».

[7] GÓMEZ DE LA CRUZ ALCAÑIZ, A., *Análisis sobre la regulación de criptoactivos en Europa*, ICOFUNDING, Madrid, 2019, páginas 5 y 6.

- *Payment / Exchange / Currency tokens*: son las conocidas como "monedas virtuales" en sentido estricto. Están destinadas principalmente a la realización de pagos. Los dos ejemplos más conocidos son el Bitcoin y el Litecoin.

  Existe una subdivisión dentro de este tipo que merece la pena mencionar aparte: las *Stablecoins*. El fin de estas monedas virtuales es también el intercambio, pero a diferencia de las anteriores cuentan con un soporte físico -aunque también se puede conseguir este efecto recurriendo a algoritmos- que limitaría su volatilidad. Un ejemplo de esto podría ser la nueva moneda virtual que tienen proyectada Facebook y otros asociados, la Libra.

- *Utility tokens*: en general, son *tokens* que garantizan el acceso a determinados servicios que ofrece la plataforma que los emite, sin que puedan ser utilizados fuera de ella. Como ejemplo de esto tenemos el BAT, *token* propio del navegador Brave, y que sólo se puede utilizar en esta plataforma y con un fin concreto.

- *Security / Asset tokens*: como su propio nombre indica, son principalmente un soporte que garantiza un derecho. Este tipo de *tokens* son los que están destinados básicamente a la inversión, por lo que son los que se suelen emitir al lanzar una ICO. Son, concretamente, el tipo de ficha que crea CRYPTO ASSETS en su actividad.

- *Hybrid tokens*: una vez conocidos los demás, baste decir que es un tipo de *token* que tiene las características de más de uno de los anteriores. El ejemplo más claro de este caso es el Ether, que tiene aplicaciones dentro de los tres tipos anteriores.

Además, cabe decir que un *token*, tal y como está configurado hoy en día este sector, podría empezar siendo de un tipo y que su utilidad cambiase, haciéndolo también su clase. De todas formas, esta distinción es más doctrinal que otra cosa; en realidad lo que se suele tener más en cuenta a la hora de establecer diferencias entre monedas virtuales -al menos desde un punto de vista legal- es si un *token* se ve afectado por normas financieras como el MIFID II o no. En cualquier caso, de esto se hablará más en profundidad en el siguiente Capítulo del informe.

1.1.1. ¿Qué es la tokenización de activos?

Tokenizar o digitalizar un activo supone establecer una equivalencia en *tokens* o fichas para un determinado bien o derecho. El número de éstas dependerá tanto del valor del

activo como de las fichas, siendo este último una decisión libre, y la evolución de ambos a lo largo del tiempo dependerá generalmente del *smart contract* que se haya ideado.

Dicho de otro modo, se denomina "tokenización" al acto de "transformar" un bien o derecho en *tokens* o fichas digitales transaccionables. Esta nueva herramienta tecnológica, a la que tenemos acceso en gran medida gracias a la disrupción causada por el *blockchain*[8] supone realmente la asignación a cada bien un determinado número de *tokens* que serán un reflejo de su valor. Esto puede abarcar prácticamente cualquier activo, de forma que, por ejemplo, puede tokenizarse incluso el dinero *fiat*[9] o los derechos de propiedad intelectual, mediante la asignación a cada *token* de un valor determinado en dólares o en otra divisa. En resumen, éstos son "referencias criptográficas registradas en una base de datos distribuida"[10], representaciones digitales de los activos.

Al principio del párrafo anterior he entrecomillado la palabra "transformar" porque, naturalmente, no podemos convertirlo en datos en sentido estricto: el activo sigue siendo el activo, y mediante la tokenización lo que se hace es imponerle cargas basadas en el modo en que se haya hecho aquélla. En nuestro caso, la propiedad del bien tokenizado se encontraría dividida entre los usuarios inversores que tuvieran en su poder todas las fichas que la componen.

Hay, así, una pregunta principal que responder: qué ¿garantiza que el valor de estos *tokens* no se va a ver alterado artificialmente por los distintos operadores de la *blockchain*? Pues bien, la diferencia principal con el Bitcoin es que los *tokens* de CRYPTO ASSETS sí que poseen un valor "real", por lo que sus fluctuaciones no dependen del mercado de moneda virtual, sino de las variaciones en el valor del propio bien. Así, si un activo que vale 1.000 € está dividido en 100 fichas, cada una valdrá 10€, y si dos años después su valor ha subido a 1.200 €, cada una valdrá 12. Naturalmente, podrían redactarse cláusulas que establezcan nuevas formas de gestionar las variaciones de valor del bien en el futuro (por ejemplo, emitiendo nuevos *tokens* o retirando los que ya posean los *tokenholders* cuando aumenta o cae dicho valor, respectivamente, o atribuyendo un porcentaje de los aumentos a la plataforma para crear algún tipo de fondo de garantía; las opciones son variadísimas).

[8] GONZÁLEZ-MENESES, M., *Entender el blockchain, una introducción a la tecnología de registro distribuido*, Thomson-Reuters Aranzadi, Madrid, 2017, pág. 96.
[9] Ibid, pág. 26.
[10] Ídem.

Una vez establecido esto, avanzamos un paso más: la plataforma de tokenización de activos de CRYPTO ASSETS no funciona sobre Bitcoin -ya que, aunque increíblemente innovadora en su momento, tiene sus limitaciones- sino en Ethereum. A diferencia del Bitcoin, el sistema Ethereum permite la creación de *smartcontracts*, de los que se hablará más adelante, y de *tokens* (a través del estándar ERC-20, que es básicamente un tipo de *smartcontract* que existe en esta plataforma y con el que se pueden registrar y transmitir estas "fichas" a través de la propia Ethereum[11]). Gracias a este mecanismo, cualquiera puede generar *tokens* digitales, "cuyo tráfico es controlable por la propia *blockchain* de Ethereum y susceptible de programación mediante Smart Contracts desplegados y ejecutados sobre ésta"[12].

Nada impediría, además, que se estableciesen mecanismos retributivos como dividendos, ni la emisión de más fichas al estilo de un aumento de capital. Sin embargo, a la hora de poner en práctica todas estas ideas debe tenerse en cuenta que se estaría entrando en el pantanoso terreno de la normativa financiera, que puede ser suficiente para lastrar a una empresa pequeña como una *start-up.* En este sentido, en el Capítulo 2 de este informe hablaré sobre estas normas concretas y cómo y cuándo son de aplicación.

1.2. Blockchain

La tecnología *blockchain*, que ha sido mencionada por encima hasta el momento, ha sido uno de los principales catalizadores de este auge de las monedas virtuales. Sin embargo, como ya se ha expuesto, no debe entenderse como algo indisoluble del mundo de las monedas virtuales: es una tecnología que, esencialmente, garantiza la integridad de los datos que se incorporan a ella, y que por tanto les dota de garantías. Dicho de otro modo, aporta un método de registro que es público, descentralizado, desintermediado y deslocalizado.

En cuanto a qué es el *blockchain*, uno de los aspectos principales lo describe Manuel González-Meneses de forma bastante sencilla: "una *blockchain* es un registro que no se lleva por una sola persona o entidad individualmente responsable de esta llevanza, sino por un número indeterminado de personas o agentes, que podrían ser incluso todos los usuarios del sistema"[13]. Así, se puede decir que es básicamente una tecnología que ofrece

[11] Ibid, página 96.
[12] Ibid, página 106.
[13] Ibid, página 31.

un modo de registro descentralizado (que es, de hecho, lo que significan las siglas DLT en inglés), que basa sus garantías en la multiplicidad de los datos que se conservan en ella y que se cotejan en muchos lugares (nodos) en tiempo real, por lo que si éstos no coincidiesen se tendría constancia inmediata de que han sido alterados en algún punto; como es muy complicado que tantas personas se pongan de acuerdo para modificar los datos y lo hagan exactamente del mismo modo, esta garantía parece bastante consistente. Bien es cierto que en el caso del Bitcoin no se requiere que la totalidad de los registros coincidan (se toma por válida la posición mayoritaria) pero nada impide que en otras configuraciones se exijan porcentajes más altos o incluso que la totalidad de ellos sean idénticos.

La idea nace de la desconfianza creciente que existe en los registros centralizados, a los que un ataque podría, potencialmente y por mucho que las medidas de seguridad sean de última generación, inhabilitar temporal o incluso definitivamente. En un mundo cada vez más rápido -casi instantáneo para gran cantidad de actividades en la Red-, las consecuencias de una parálisis de los sistemas suponen un riesgo creciente que empresas y autoridades públicas se esfuerzan por reducir. Este es el motivo por el que hay muchas iniciativas desarrolladas sobre esta tecnología que no tienen nada que ver con las monedas virtuales, y que van desde la creación de un registro único de historiales clínicos a los que se pueda acceder desde cualquier lugar del país a ideas para reducir costes en transacciones financieras. Y el tema de los costes es precisamente otra de las ventajas que tiene el *blockchain*: deslocalizar los registros supone, a fin de cuentas, ahorrarse servidores centrales y otros costes relacionados con el uso de terceros de confianza y certificaciones, mientras que la carga para los usuarios que participan en la cadena de bloques es casi imperceptible.

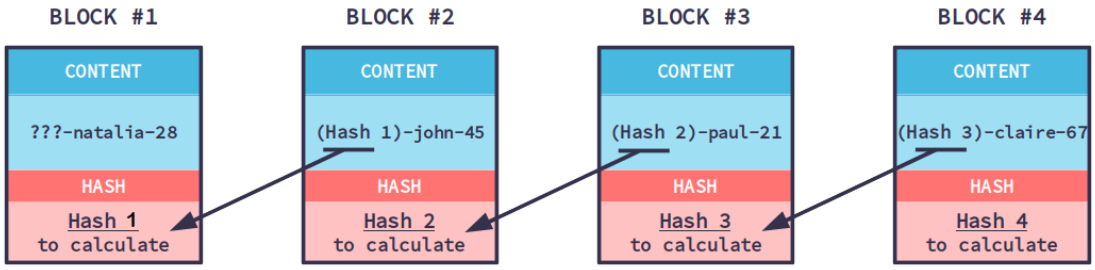
La principal causa que menciona García-Meneses para el auge del *blockchain*[14] es la creciente tendencia a la economía colaborativa, que en este caso habría alcanzado a los registros de información. Esto, unido a la desconfianza en las instituciones -principalmente financieras- que trajo consigo la Crisis económica de 2007, crearon el hábitat perfecto para el nacimiento del Bitcoin (Satoshi Nakamoto publicó su primer artículo hablando de esta moneda virtual en 2008[15]). Aunque los orígenes de esta

[14] Ídem.
[15] NAKAMOTO, S. (seudónimo), *Bitcoin: a peer-to-peer Electronic Cash System*, blog Bitcoin.org, 2008.

tecnología se remontan hasta 1991, año en que fue ideada por Stuart Haber y W. Scott Stornetta[16], es el ejemplo más conocido del uso de la cadena de bloques.

Su fortaleza se basa, en realidad, en el especial uso que se les da a los *hashes*. Un *hash* es una serie de letras y números que se corresponden, de forma unívoca, con unos determinados datos. Por tanto, no es otra cosa que una función resumen que asegura la integridad (inalterabilidad) de la información resumida, por lo que cuando coinciden dos *hashes* se tiene la seguridad de que ambas informaciones son exactamente la misma. Tanto en el caso del Bitcoin como en el que nos ocupa, cada uno de ellos representa una transacción (por ejemplo, A compra a B x *tokens*, por lo que A pasa a tener $(x_1 + x)$ y B pasa a tener $(x_2 – x)$).

La novedad viene de crear bloques que vinculan cada transacción nueva a la inmediatamente anterior que se ha registrado, añadiéndole el *hash* de ésta última, y creando así, al vincular unos bloques a otros de forma sucesiva, lo que se llama "cadena de bloques".



Pero no se trata sólo de esto, ya que si este registro estuviera en un único lugar sería perfectamente alterable: sería posible modificar ambos *hashes* y nadie se enteraría. Por tanto, el otro aspecto que le dota de garantías es esa "distribución" de los registros de que hablábamos antes en los llamados "nodos". Así, en aplicación del problema de los generales bizantinos[17] se coteja cada nueva acción que se pretende registrar con otras muchísimas cadenas que se conservan alrededor del mundo, de modo que, en caso de que

[16] BEYER, S., *Blockchain before Bitcoin: a history*, BlockTelegraph.io, 2018 (consultado en https://blocktelegraph.io/*blockchain*-before-bitcoin-history/ el 12/06/2019).
[17] GONZÁLEZ-MENESES, M., *Entender el blockchain, una introducción a la tecnología de registro distribuido*, Thomson-Reuters Aranzadi, Madrid, 2017, páginas 33-36.

alguno de los *hashes* no coincida con los que se le suponen idénticos, la operación no será válida. Dado que, como he mencionado antes, se presupone un cierto grado de alteración de los datos contenidos en las cadenas de bloques (que no tiene por qué ser malintencionada, podría ocurrir que se hubieran corrompido los datos, por ejemplo), lo que se lleva a cabo es un cotejo a nivel mundial en el que basta con que haya una mayoría de coincidencias; a este punto, clave en el registro de cualquier operación en este tipo de sistemas, se le denomina "proceso de consenso". Y todo esto en el marco de un sistema totalmente automatizado, diseñado para que no sea posible "meterle mano". Naturalmente, es totalmente imposible alcanzar el 100% de fiabilidad, pero la dificultad de crear una *fork* (que supone básicamente el establecimiento de una suerte de "universo paralelo", de una nueva cadena de bloques dentro del sistema con información distinta de la original) que además prevalezca sobre la principal es tan alta que se considera improbable.

Finalmente, el hecho de que la *blockchain* sea pública (cuando lo sea) garantiza que toda la información contenida en ella es accesible por cualquiera, lo que le dota de una gran transparencia. Como se mencionó anteriormente, no es obligatorio que una *blockchain* tenga exactamente las mismas condiciones que la que usa el Bitcoin, pero esta es una opción que puede ser útil o no dependiendo del proyecto. En el caso CRYPTO ASSETS, por ejemplo, el hecho de que la cadena de bloques fuese pública haría las veces de una especie de Registro de la Propiedad paralelo, en el que se pudiera ver quién posee cuántos *tokens* y sobre qué activos. Supone, en fin, y como ya se ha dicho, un extra de transparencia si es bien empleada, lo cual es positivo para cualquier participante que no albergue intenciones aviesas.

No obstante, esto no significa que la tecnología *blockchain* sea siempre pública. Como explicó Buterin en un conocido artículo[18], existen tres tipos de cadenas de bloques:

- *Blockchain* públicas, en las que cualquiera puede llevar a cabo una transacción, leer y/o participar en el proceso de consenso, como ya he explicado.
- *Blockchain* en consorcio, posiblemente las menos conocidas. Éstas consisten en el establecimiento de unos nodos concretos que son los que se encargan del proceso de consenso. Así, en vez de tener una cantidad indeterminada de nodos

[18] BUTERIN, V., *DAOs, DACs, DAs and More: An Incomplete Terminology Guide*, blog Ethereum.org, 2014 (consultado en https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/?source=post_page---------- el 30/07/2019).

que participan en él, tenemos una cantidad preestablecida que actúan en consorcio (de ahí el nombre). Buterin pone como ejemplo una *blockchain* en la que los nodos consorciados son 15 entidades financieras, y en el que la verificación de cada nuevo bloque pudiera requerir la connivencia de 10 de ellas. Más allá de esto, podrá tener más o menos publicidad y el acceso podrá ser libre o condicionado; la característica distintiva es este control de los nodos.

- *Blockchain* totalmente privadas, que son aquellas para las que los permisos están centralizados y no permiten la consulta externa, ya que están ideadas para servir a un propósito específico interno para una empresa o grupo. Se distinguen de las consorciadas en este carácter puramente privado, aunque en la práctica la distinción doctrinal suele estar en la dicotomía entre la pública y la privada, por entender que el control sobre el proceso de consenso implica la "privatización" de la cadena de bloques. Un ejemplo del uso que se le podría dar a una *blockchain* privada es el mantenimiento y organización de bases de datos de una empresa.

En el artículo, Buterin enumera los pros y contras de las *blockchain* tanto públicas como privadas, pero no se va a ahondar más en este punto. A fin de cuentas, el proyecto de CRYPTO ASSETS se llevará a cabo sobre la plataforma Ethereum, empleando también su *blockchain*, que en este caso es pública.

En fin, la aplicación de la *blockchain* a la idea de la tokenización de activos que propone CRYPTO ASSETS es una opción muy viable, dadas las garantías que ofrece sin requerir una gran inversión en servidores por parte de la plataforma. La cuestión, una vez se ha decidido emplear esta tecnología, radica en el modo en que quiere hacerse.

CRYPTO ASSETS, al proponer el empleo de la cadena de bloques de Ethereum, que ya está en funcionamiento, tiene acceso a varias ventajas. Por ejemplo, ésta permite el establecimiento de *smartcontracts* (de los que se habla más adelante en este informe) y la emisión de *tokens*, por lo que supone una herramienta de gran utilidad para la empresa. Así, una vez establecido el contrato inteligente y el funcionamiento del sistema de fichas para inversión y financiación, la empresa estaría lista para funcionar (al menos desde el punto de vista tecnológico).

En definitiva y a modo de sumarísimo resumen, se puede decir que las ventajas de esta tecnología son dos básicas y una tercera es opcional[19]:

1. Gran Seguridad.
2. Eficiencia económica.
3. Transparencia.

1.3. Smart contracts

Se conoce por *smartcontracts* al proceso automatizado digitalmente de realización de negocios jurídicos. Dicho de forma algo arcaica, permite "programar" los movimientos de los activos que se intercambian en la red. Y si nos tomamos un segundo para desgranar el término, podemos ver que se habla de "contratos" porque se están estableciendo y regulando derechos y obligaciones entre particulares, y de "inteligentes" porque son el resultado de la aplicación de la tecnología al funcionamiento de los contratos tradicionales. La Ley de Servicios de la Sociedad de la Información (en adelante "LSSI") establece en su Anexo una definición de contrato electrónico: "*todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones".* Más allá de esta definición, que se centra principalmente en el medio físico en el que se formaliza el contrato, encontramos pocas referencias más a los tipos de contratos en la Red. Esta indefinición, no obstante, no supone la alegalidad de estos contratos, ya que en la práctica se les sigue aplicando la normativa existente en esta materia; empezando por el Código Civil, los contratos inteligentes deberán cumplir con las reglas habituales de contratación, empezando por que "*el contrato existe desde que una o varias personas consienten en obligarse, respecto de otra u otras, a dar alguna cosa o prestar algún servicio"*[20]. Es decir, el contrato inteligente será tan válido como cualquier otro cuando exista un acuerdo de voluntades y se reúnan los requisitos habituales.

Esto puede parecer extraño, ya que en la esencia de los *smartcontracts* está la falta de presencia humana. Pero creemos que el hecho de que un contrato inteligente sea esencialmente código que trabaja automática o incluso autónomamente no debe hacernos

[19] GONZÁLEZ-MENESES, M., *Entender el blockchain, una introducción a la tecnología de registro distribuido*, Thomson-Reuters Aranzadi, Madrid, 2017, página 93.
[20] Art. 1254, Código Civil de 1889.

perder de vista la realidad: pese a su nombre, estos contratos no piensan por su cuenta, "piensan" lo que sus desarrolladores les han dicho. Por ello, en cualquier caso existe un acuerdo de voluntades entre dos personas, físicas o jurídicas, cuando se llevan a cabo transacciones a través de este medio.

Como mencionan varios autores en el blog del Consejo General de la Abogacía Española[21] para desarrollar este tipo de contratos con garantías en nuestro país debemos fijarnos en los artículos 27 y siguientes de la LSSI. Aunque, como se ha visto, esta norma se encuentra desfasada en lo concerniente a contratos inteligentes -y a otras cuestiones-, estos preceptos establecen obligaciones para el prestador de servicios de la sociedad de la información. En cualquier caso, hablaremos de lo que esto supone para CRYPTO ASSETS en el apartado correspondiente.

En este punto debemos hacer una rápida mención también a las ICOs (*Initial Coin Offering*, por sus siglas en inglés), ya que su concepto nace de los *smartcontracts* de Ethereum. Consisten, básicamente, en la emisión masiva de *tokens* que tienen como fin la financiación de una empresa o proyecto, habitualmente una *start up*. A diferencia de la tokenización de la que hemos venido hablando anteriormente, en este caso no hay "nada real" tras estos *tokens*, tan solo una idea que se quiere llevar a cabo. Ahora bien, por la propia naturaleza de este tipo de contratos inteligentes, es muy difícil que se pueda reclamar algo al sujeto emisor, careciendo éste, en la práctica, de cualquier grado de responsabilidad en la mayoría de los casos[22]. Esto se debe a que, pese a su parecido con las OPV, precisamente se suele tratar de huir del régimen jurídico que éstas tienen. Esto, sumado al hecho de que la mayoría de *start-ups* carecen de un equipo con experiencia en desarrollo empresarial y que suelen adolecer de escasez de medios, supone un gigantesco problema de seguridad jurídica y las convierte en inversiones de muy alto riesgo. Podemos añadir también el hecho de que un elevado porcentaje de ICOs tienen una probabilidad bajísima de devolver las rentabilidades prometidas o son estafas sin ambages, lo que ha hecho que los reguladores y gobiernos nacionales "se pongan las pilas" para intentar imponer un cierto orden o, directamente, prohibirlas (como en China

[21] BLANCO PÉREZ, M.A., LÓPEZ-ROMÁN, E. *et alia, Contratos Inteligentes: los "Smart Contract",* blog CGAE, 2017 (consultado en https://www.abogacia.es/2017/03/06/contratos-inteligentes-los-smart-contract/ el 01/08/2019).

[22] GONZÁLEZ-MENESES, M., *Entender el blockchain, una introducción a la tecnología de registro distribuido*, Thomson-Reuters Aranzadi, Madrid, 2017, página 106.

o Bangladesh). De nuevo, se desarrollará más esta problemática a la hora de hablar del régimen de responsabilidades, aunque a priori no afecta a CYPTO ASSETS.

El principal problema al que nos enfrentamos cuando buscamos encontrar un régimen apropiado para los *smart contracts* es el hecho de compaginar la propia definición de éstos con la realidad del mundo *off-line* u *off-chain*. Este tipo de contratos son puro código, y llevan la autorregulación en su esencia; y esta autorregulación, como hemos visto, supone además su principal garantía, ya que lo que está codificado, en teoría, no se puede modificar con intenciones aviesas. Pero en el mundo real la libertad de contratación tiene sus límites, del mismo modo que existen normas que regulan los incumplimientos o la responsabilidad de las partes. ¿Deberíamos entender que lo que esté o no contemplado en el *smart contract* es lo único que importa? Aunque este es el punto de vista de ciertas corrientes afines al criptoanarquismo (que lo resumen en el famoso "*code is law*"[23], o "el código es ley"), lo cierto es que tanto el carácter no negocial de estos contratos como sus efectos sobre la vida y la economía de las personas parecen crear una puerta de acceso para que el Derecho tradicional "haga lo suyo", aunque sea de la forma menos invasiva posible.

Como demostró el famoso caso de The DAO[24], las garantías que ofrecen este tipo de sistemas descentralizados son buenas pero relativas, y cuando estas fallan el usuario no debería quedar desprotegido. El presente informe tampoco busca ser un artículo doctrinal, por lo que se va a extender demasiado en la exposición de un caso que no tiene mayor relevancia para el tema que aquí se trata pero, dada la importancia que éste tiene, merece la pena que nos detengamos un instante en ello.

A lo largo del primer semestre de 2016, el proyecto de "The DAO" se puso en funcionamiento, y formó parte de la primera generación de DAOs (o "decentralized autonomous organization", por sus siglas en inglés) que se creaban tras su conceptualización en el White Paper de Ethereum. La idea era que el usuario-inversor adquiría *tokens* de The DAO con Ethers, lo que suponía tener derecho de voto sobre las actividades que ésta llevaba, así como a recibir ciertas "recompensas", de forma parecida a la adquisición de acciones de una empresa. El caso es que, en el código del *smart contract* del proyecto -que fue publicado en su White Paper-, resultó que se dejaba al

[23] LESSIG, L., *Code and Other Laws of Cyberspace, 1999*.
[24] GONZÁLEZ-MENESES, M., *Entender el blockchain, una introducción a la tecnología de registro distribuido*, Thomson-Reuters Aranzadi, Madrid, 2017, página 114.

descubierto un *exploit*, un fallo de diseño que podía ser usado para hackear o crackear el sistema; desvió un tercio de los Ethers que estaban en poder de The DAO sin que sus curadores o comisarios del sistema pudieran evitarlo.

Esto causó que se promoviese un *hard fork*, de los ya mencionados, que tenía como fin devolver los *tokens* robados a una cuenta desde la que sus los inversores pudiesen volver a cambiarlos por Ethers. Se creó así un cisma en la propia plataforma de Ethereum, dividiendo a los que abogaban por un mínimo control para ofrecer un nivel básico de garantías a los usuarios y los que consideraban que tanto las monedas virtuales como los contratos diseñados con ellas debían quedar al margen de toda intervención que no contemplase su propio código. Pese a la cantidad de dinero en juego -unos 3.6 millones de Ethers, valorados por aquél entonces en unos 50 millones de USD-, las autoridades decidieron no actuar por considerar que no tenían competencias para ello, y por eso tuvo que ser la propia comunidad de Ethereum quien lo hiciera[25]. Es el mayor ejemplo (pero no el único) de los principales peligros asociados a los contratos inteligentes: si el código presenta vulnerabilidades y alguien se aprovecha de ellas, no hay más garantías que las que específicamente se recojan en la plataforma o acuerdo entre las partes, e incluso en este último caso no siempre existe la posibilidad de obligar a que se cumplan; aunque en teoría los *smart contracts* están sometidos al Derecho como cualquier otro contrato, nos topamos con la problemática común a todos los que se elaboran en Internet: conocer, a ciencia cierta, qué jurisdicción es la aplicable en cada momento.

2. ANÁLISIS DE LA NORMATIVA

En este punto analizamos la normativa que Crypto Assets nos solicitó, a efectos de determinar su aplicabilidad al modelo de negocio de la empresa.

2.1. Régimen general

El primer paso es analizar la literalidad del Código Civil español de 1889 y, a partir de las características esenciales de la responsabilidad que se extraigan, analizar los otros campos, más específicos, en los que ésta puede exigirse en los mercados de moneda virtual. La responsabilidad civil, tanto contractual como extracontractual, se puede definir esencialmente como aquélla que busca resarcir un daño causado a otra parte como

[25] Securities and Exchange Commission, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, Release Nº 81207, 2017.

consecuencia una acción u omisión propias. El artículo 1089 del Código Civil determina que "las obligaciones nacen de la Ley, de los contratos y cuasicontratos, y de los actos y omisiones ilícitos o en los que intervenga cualquier género de culpa o negligencia". Conforme a esta definición, que es la base de todo el sistema de responsabilidades, vemos que una empresa puede ser considerada responsable más allá de lo que haya establecido en un contrato bilateral con otra parte como, en este caso, el que se pueda establecer entre la plataforma y un usuario de la misma, y deja la puerta abierta a que se le puedan atribuir, tanto a una como a otro, en función de los actos de unos y otros.

Dado que la parte de responsabilidad que tiene que ver con el incumplimiento contractual tiene causas bastante evidentes -al menos en cuanto a conceptos generales se refiere- pasaremos de ello de forma muy ligera. Baste decir que, como ordena el artículo 1101 del Código, tanto quien incumpla sus obligaciones contractuales como quien, incluso cumpliendo con ellas, incurriera "en dolo, negligencia o morosidad" deberá asumir los daños y perjuicios que haya causado a la otra parte. Esta segunda opción se puede relacionar directamente, por ejemplo, con la hipotética existencia de cláusulas abusivas en los contratos entre la plataforma y los usuarios conforme a la Ley de Defensa de los Consumidores y Usuarios.

Otra cosa es la responsabilidad extracontractual. En ella, la base no es la quiebra de las obligaciones contractuales, sino la producción de un daño. La norma de referencia en este punto es el artículo 1902 del mismo Código Civil, que establece que "[e]l que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado".

Por otra parte, nos encontramos ante la complicada tesitura de decidir cuál es el régimen jurídico aplicable. La norma habitual es que se considere que la jurisdicción se determinará en función del lugar en el que sucede el hecho que da lugar a la responsabilidad no contractual[26], pero al hablar de Internet esta seguridad se difumina. Pese a que la norma es clara, ¿cómo se establece el lugar en el que ocurren los hechos? La problemática deriva del hecho de que la normativa actual se sustenta sobre la condición de la territorialidad, más o menos innegable, de todo lo que ocurre. Sin embargo, Internet es distinta; es una suerte de tierra de nadie en el que, si todos los

[26] Artículo 10.9, Código Civil: "las obligaciones no contractuales se regirán por la ley del lugar donde hubiere ocurrido el hecho del que deriven. La gestión de negocios se regulará por la ley del lugar donde el gestor realice la principal actividad."

interesados en un conflicto se encuentran en distintos Estados (y eso cuando se puede determinar), es muy complicado atribuir responsabilidades. Esto es especialmente patente cuando hablamos de monedas virtuales y, más aún, en el caso de algunas en particular, como el Bitcoin. Ésta última, además de hacer de la deslocalización total su punto fuerte, no identifica ni a sus usuarios ni a la persona o personas que tiene detrás y que desarrollaron su código, ya que Satoshi Nakamoto no es su nombre real. Al contrario que Ethereum, plataforma cuyo creador -Vitalik Buterin- es más que conocido e interviene activamente en ella, todo en el ecosistema del Bitcoin parece haber sido desarrollado para preservar el anonimato de quienes participan en ella. Todo esto hace virtualmente imposible atribuir responsabilidades en este punto, ya que, como sabemos, la identificación del sujeto obligado es necesaria para poder hacerlo.

No obstante, ya se pueden ver cláusulas de exclusividad jurisdiccional y arbitraje en las fundaciones asociadas a las plataformas[27] (cláusulas que habitualmente remiten a los lugares que les son más favorables, dada la gran libertad que otorga Internet), entre otras cosas porque establecerse en un lugar físico es necesario para operar en la mayoría de Estados de forma legal[28].

Así pues, vemos que el régimen general tiene una aplicabilidad bastante escasa en este nuevo entorno por la imposibilidad de aplicar sus presupuestos. Dicho esto, queda claro que este es algo de lo que adolecen la mayoría de normas que pueden suponer la eventual responsabilidad en el mundo de las monedas virtuales, pues se sustentan precisamente en estos mismos presupuestos del Derecho tradicional; es por eso que, como se mencionó anteriormente, a día de hoy sólo son de aplicación, en general, unas pocas normas en el mundo de las monedas virtuales. A ellas dedicaremos los siguientes apartados.

En fin, en contraposición a lo anterior debe tenerse en cuenta que CRYPTO ASSETS es una empresa que, dada su domiciliación en España, sus actividades están sujetas al régimen aplicable aquí, incluida la necesidad de que sus socios sean personas, físicas o jurídicas, identificables y susceptibles de ser responsables conforme al régimen general Es suficiente con estas consideraciones para lo que interesa en este informe, ya que sólo con esto se entiende que **la plataforma debería hacerse cargo de los daños producidos**

[27] T&C de Ethereum ("*Governing Law and Jurisdiction*"). Consultado en http://ethereum.org/terms-of-use/ el 11/09/2019; T&C de Bitcoin ("9.*Arbitration*"), consultados en https://bitcoin.org/es/legal#english-noliability el 11/09/2019.

[28] Directiva 2000/31/CE, de Comercio electrónico; Ley 34/2002, de Servicios de la Sociedad de la Información.

por las acciones u omisiones, negligentes o culpables, que hubiera llevado a cabo -así como el resto de participantes en el mercado-.

2.2. Ley de Servicios de la Sociedad de la Información

La Ley 34/2002, de Servicios de la Sociedad de la Información (en adelante LSSI) es resultado de la transposición de la Directiva 2000/31/CE, relativa al comercio electrónico. Como es habitual, la primera cuestión a analizar es si esta Ley es de aplicación a CRYPTO ASSETS. Pues bien, primero hay que determinar si ésta es un prestador de servicios de la sociedad de la información; la Ley determina que lo serán todos aquéllos que presten, valga la redundancia, servicios de la sociedad de la información, que a su vez vienen definidos como "todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario"[29]. La definición es más larga y menciona específicamente algunos casos (como la contratación de bienes y servicios por vía electrónica), a la vez que establece claramente algunas excepciones, que no aplican a CRYPTO ASSETS; pero lo que viene a decir, en cualquier caso, es que no hay una lista cerrada en cuanto a qué servicios son considerados como tal. Por otro lado, hay otra condición que hay que tener en cuenta para saber si es obligatorio cumplir con la LSSI, relativa a la nacionalidad o al público objetivo al que va dirigida la actividad económica. Baste saber que, ya que la plataforma está afincada en España, la Ley le es de aplicación.[30]

Por tanto, una vez establecido que CRYPTO ASSETS es un prestador de servicios de la sociedad de la información, toca conocer cuáles son sus obligaciones en este campo. Conforme al artículo 10 de la Ley, los deberes del prestador son bastante simples, y se limitan esencialmente a tener a disposición del público, "de manera fácil, directa y gratuita", cierta información en el Aviso Legal. En la página web o aplicación de CRYPTO ASSETS, en su caso, deberá constar:

- El nombre y denominación social, CIF, domicilio y dirección de correo electrónico, teléfono, fax o cualesquiera otros medios de contacto.
- Los datos de inscripción registral.
- Información relativa a los precios de sus productos y servicios, en los que deberá estar incluido el IVA, conforme a la normativa tributaria.

[29] Anexo, Definiciones, Ley 34/2002, de Servicios de la Sociedad de la Información.
[30] Artículo 2, LSSI.

- Los códigos de conducta a los que esté adherido, en su caso.

Son especialmente importantes, también, los artículos 27 y siguientes de la Ley, en tanto que establecen expresamente determinadas obligaciones en los distintos momentos de la contratación[31].

Así, antes de contratar deberá darse la siguiente información, de forma clara y accesible (especialmente en dispositivos móviles o de "pantallas con formato reducido")[32]:

- Los trámites que, en su caso, deban seguirse. Un ejemplo en este caso podría ser la necesidad de establecer un *wallet* que sirva para guardar, con clave privada, las monedas virtuales o *tokens*.
- Si el documento electrónico en el que se formalice el contrato se va a archivar y/o va a ser accesible para el usuario.
- Los medios técnicos con los que cuente CRYPTO ASSETS para "identificar y corregir errores en la introducción de los datos".
- El idioma de contratación.

Y finalmente, en las 24 horas siguientes a la formalización del contrato, se deberá enviar un acuse de recibo y la confirmación de la aceptación por parte del usuario, por e-mail u otro medio válido.

Por otro lado, será necesario recabar el consentimiento del usuario antes de llevar a cabo comunicaciones comerciales, salvo que se haya una relación contractual previa[33]. Es decir, sí que se podrán enviar comunicaciones comerciales sin consentimiento o petición expresa cuando el usuario ya sea cliente de la plataforma, pero no antes. No obstante, será obligatorio en cualquier caso que el usuario tenga la opción de negarse a recibir estas comunicaciones, para lo que habrá que habilitar un medio sencillo (a través de un link en los correos publicitarios, por ejemplo) para que éste pueda hacerlo. Por otro lado, cuando se utilicen *cookies* -que será casi siempre en estos ámbitos-, deberá redactarse una Política de Cookies, de modo que se pueda cumplir con el deber de información que establece la normativa de Protección de Datos, tratada más adelante.

[31] BLANCO PÉREZ, M.A., LÓPEZ-ROMÁN, E. *et alia, Contratos Inteligentes: los "Smart Contract",* blog CGAE, 2017 (consultado en https://www.abogacia.es/2017/03/06/contratos-inteligentes-los-smart-contract/ el 01/08/2019).
[32] Artículo 27, LSSI.
[33] Artículo 21, LSSI.

La última obligación general que establece la Ley es el deber de conservar documentos (en soporte digital o papel) que supongan medio de prueba suficiente de los negocios jurídicos que se lleven a cabo. Por ello, será recomendable tener siempre hechos *back-ups* de seguridad.

Finalmente, en cuanto a lo que supondría conforme a la LSSI el incumplimiento de las mencionadas obligaciones, la doctrina ha venido alzando un dedo acusador hacia esta Ley, debido a la falta de un régimen sancionador específico. Si se atiende a los artículos 14 y siguientes ("Responsabilidad de los prestadores de servicios de la sociedad de la información"), lo que figura es, en esencia, una remisión al régimen civil, penal y administrativo, tras lo que se enumeran una serie de exclusiones a esta regla básica. No existe, pues, un régimen de responsabilidad propio en esta Ley, sino que, más bien, establece excepciones al régimen general. Visto el modelo de negocio de CRYPTO ASSETS, parece que ninguna de éstas le es aplicable, ya que pretenden limitar la responsabilidad de aquellos prestadores que sirvan como medio para que los particulares participen en la Red, de distintas formas (compartiendo archivos, comentarios, etcétera). Sí le serían aplicables algunas de estas exclusiones, por ejemplo, en cuanto a los contenidos que haya en otras páginas web a las que haya vínculos en la suya, o en cuanto a los comentarios de los usuarios en caso de contar con un foro, pero sólo si desconocía dichos contenidos; si se demuestra que podían ser conocidos por CRYPTO ASSETS y que ésta no hizo nada para bloquearlos o suprimirlos, se le podría considerar responsable.

Por tanto, la Ley 34/2002, de Servicios de la Sociedad de la Información, será de obligado cumplimiento para CRYPTO ASSETS.

2.3. Ley de Prevención de Blanqueo de Capitales y Financiación del Terrorismo

La normativa contra el blanqueo de capitales y la financiación del Terrorismo está cobrando en los últimos tiempos una gran importancia en relación con las monedas virtuales.

En mayo del año pasado se promulgó la Directiva (UE) 2018/843, que pretende limitar, en la medida de lo posible, el empleo de las monedas virtuales con fines de blanqueo de

capitales o de financiación del terrorismo. Y para ello, nace con la intención expresa[34] de abarcar todos los usos posibles de las monedas virtuales. Aunque el plazo de transposición termina en enero de 2020, es recomendable tratar directamente lo que supondrá la entrada en vigor de esta norma.

El punto estrella de la Directiva es la asignación de responsabilidad en este ámbito a los *exchanges* y a las entidades que presten servicios de custodia de claves criptográficas privadas (*wallets*) dentro de la Unión Europea[35]. Hasta esta fecha, ninguno de los dos sujetos estaba obligados a cumplir con la normativa de PBC, pero, dado que se detectó que las monedas virtuales se empleaban habitualmente para infringir la normativa internacional en este ámbito, y que éstos son los únicos que, por el momento, pueden llevar a cabo un cierto control sobre las transacciones realizadas, el legislador europeo consideró "esencial ampliar el ámbito de aplicación de la Directiva (UE) 2015/849"[36] para incluirles como sujetos obligados. Así, deberán implantar medidas de *due diligence* enfocadas a detectar actividades sospechosas, si bien esta misma norma entiende que el anonimato característico de las monedas virtuales hace que tener a los *exchanges* y a los proveedores de servicios de *wallet* controlando posibles transacciones ilícitas no resolverá totalmente el problema, ya que no es obligatorio hacer uso de estos servicios para participar en los ecosistemas de monedas virtuales.

En este aspecto se pronunció también el Grupo de Acción Financiera Internacional (GAFI) a principios de este verano. Bajo la supuesta presión de países como Japón para regular las monedas virtuales desde la óptica del blanqueo de capitales, el día 21 de junio se emitió una recomendación[37] destinada a todos aquellos sujetos que operasen con este tipo de activos. En ella se animaba a los operadores, en concreto los *exchanges*[38], a que implantasen medidas para cumplir con la normativa de blanqueo de capitales a partir de transacciones que superasen los 1.000USD. Como dijo el Secretario del Tesoro de EEUU,

[34] Considerando 10, Directiva (UE) 2018/843, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE.
[35] NIETO GIMÉNEZ-MONTESINOS, M.A. y HERNÁEZ MOLERA, J., *Monedas virtuales y locales: las paramonedas, ¿nuevas formas de dinero?,* Revista de Estabilidad Financiera, Banco de España, Núm. 35, páginas 105-122, Madrid, 2018.
[36] Considerando 8, Directiva (UE) 2018/843, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE.
[37] GAFI (o FATF, por sus siglas en inglés), *Guidance for a risk-based approach to Virtual Assets and Virtual Asset Service Providers*, 21 de junio de 2019.
[38] Directiva (UE) 2019/713, sobre la lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo, de 17 de abril.

Steven Mnuchin, se les requerirá que apliquen estas normas del mismo modo que las instituciones tradicionales[39].

Todo esto implica, en definitiva, que aquellos de estos sujetos que estén domiciliados en España deberán cumplir con las medidas de *due diligence* que contempla el Capítulo II de la Ley 10/2010, y que se pueden resumir en:

- La identificación formal de las personas físicas y jurídicas con las que se entablen relaciones de negocio y, concretamente, del titular real que está detrás de las segundas.
- El conocimiento de la relación de negocio que se lleva a cabo y la llevanza de un seguimiento continuo de la misma.
- La aplicación de las medidas de diligencia debida, entre las que se encuentran las anteriores. Además, el sujeto obligado deberá estar en condiciones de demostrar que las medidas por las que se ha optado son adecuadas para lograr los fines propuestos.

Ahora queda considerar si estas medidas afectan también a CRYPTO ASSETS. Pues bien, el GAFI publicó en 2019 una Guía[40] en la que se establece, precisamente, que los "proveedores de servicios de activos virtuales" serán considerados sujetos obligados, y deberán cumplir con las obligaciones de *due diligence* que se han mencionado previamente. Así pues, ¿es CRYPTO ASSETS un proveedor de servicios de activos virtuales? Según la Guía, este tipo de proveedores se definen como aquella persona física o jurídica que, sin encontrarse enmarcada en ninguna otra recomendación (del GAFI) lleva a cabo actividades de: **i) intercambio entre activos virtuales y dinero *fiat***; ii) intercambio entre una o más formas de activos virtuales; iii) transferencia de activos virtuales; **iv) guarda y/o administración de activos virtuales o instrumentos que permitan el control sobre los mismos**; o v) participación y provisión de servicios financieros relacionados con el emisor de la oferta o venta de un activo virtual.

[39]ALEXANDRE, A., *El GAFI fortalecerá el control sobre los exchanges de moneda virtuals para prevenir el lavado de dinero*, CoinTelegraph, 21 de junio de 2019 (consultado en https://es.cointelegraph.com/news/fatf-to-strengthen-control-over-crypto-exchanges-to-prevent-money-laundering, el 19/08/2019)

[40] GAFI, *Guidance for a risk-based approach to Virtual Assets and Virtual Asset Service Providers*, junio de 2019.

Como vemos, CRYPTO ASSETS entra, de lleno, en al menos dos de estas categorías, y conforme a esto **le corresponderán las mismas obligaciones** que a las entidades financieras en materia de Prevención de Blanqueo de Capitales:

- Para empezar, deberá estar licenciada o registrada, como mínimo, en el España;
- Deberá cumplir con las obligaciones de *due diligence* antes mencionadas en transacciones ocasionales en activos virtuales que sobrepasen el umbral de 1000€;
- "Obtener, retener y transmitir la información requerida sobre el originador y el beneficiario, de manera inmediata y segura" cuando se realicen transferencias de activos virtuales[41].

Otra cuestión que es interesante mencionar, aunque no resulta relevante para el caso de CRYPTO ASSETS, es que la Directiva de 2018 renombra a las monedas virtuales como "monedas virtuales"[42] siguiendo la tendencia del GAFI[43], lo que las aleja de la *alegalidad* en la que estaban inmersas y deja claro que la Comisión les presta, al fin, suficiente atención como para ponerle nombre oficialmente (en Directivas anteriores, como en la 2015/849 o la 2009/110/CE, sólo existía el concepto de "dinero electrónico", inaplicable en la práctica a estas tecnologías).

En fin, el acercamiento a las monedas virtuales desde el punto de vista de la prevención del blanqueo y la financiación del terrorismo está siendo muy lento, y generalmente se circunscribe -como es natural- a ámbitos que los Gobiernos pueden controlar, pero pese a todo es el ámbito en el que más se está avanzando a nivel internacional.

Para finalizar, es interesante saber que el régimen sancionador en caso de incumplimiento de la normativa de PBC es bastante duro. Entre otras sanciones, podrán retirarse las licencias, cuando las haya, o imponerse multas de hasta 1.000.000€ o, alternativamente,

[41] GAFI, Recomendación (16).

[42] Art. 1.2.d), Directiva (UE) 2018/843: *"monedas virtuales": representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos".* Esta será la redacción del artículo 3.18 de la Directiva (UE) 2015/849 cuando entre en vigor plenamente, en 2020.

[43] GAFI, *Directrices para un enfoque basado en riesgo: Monedas Virtuales*, de junio de 2015. En ella, se introdujo el concepto de "moneda virtual" y se modificaron los requisitos para que se aplique la normativa de PBC a las empresas del mundo de las moneda virtuals.

de hasta el 10% del volumen de negocios anual para las personas jurídicas, por lo que se encuentra entre los regímenes sancionadores más severos.

2.4. PROTECCIÓN DE DATOS

La normativa de Protección de datos afecta de un modo muy particular al mundo de las monedas virtuales, ya que la propia esencia de la tecnología *blockchain* parece atentar directamente contra los estándares europeos en esta materia. Por ejemplo, es imposible borrar o modificar los datos una vez están en la cadena de bloques, dejando sin efecto no sólo los derechos de los interesados, sino también contraviniendo varios de los principios básicos de la protección de datos personales, como son el de minimización limitación del plazo de conservación o el de exactitud.

Este hecho ha motivado que, en julio de este mismo año, el Servicio de Investigación del Parlamento Europeo emitiese un estudio analizando si los registros distribuidos podían enmarcarse dentro del ámbito de la normativa europea de protección de datos[44]. Este estudio detectó dos presunciones que son las principales causas de colisión entre el RGPD y esta tecnología: a) la presunción que el RGPD hace de que, detrás de cada tratamiento de datos personales, existe (y es identificable) una persona física o jurídica que actúa como Responsable; b) la de que los datos pueden ser modificados o borrados cuando sea necesario para cumplir con los requisitos legales o la voluntad de los interesados.

Más allá de las propuestas que el EPRS hace para solucionar este problema, resumibles en alternativas a la modificación del RGPD, como puede ser el fomento de los códigos de conducta y certificación o la colaboración entre las distintas autoridades de protección de datos, realmente la solución es complicada. El Reglamento se ideó como una norma basada en principios básicos, neutrales tecnológicamente, y es esta amplitud en su diseño lo que da lugar al problema.

De modo que, para no hacer de este punto un análisis de lo que podría mejorarse en un sentido o en otro, es mejor que nos centremos en lo que la normativa de protección de

[44] EPRS, Study on: *and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?*, julio de 2019.

datos afecta a las plataformas y operadores en los mercados de moneda virtual como CRYPTO ASSETS.

Para empezar, debemos ser conscientes de que CRYPTO ASSETS actúa como Responsable de los datos que recoge de los interesados, ya que lo hace con el fin de destinarlos a sus propios fines de tratamiento. Vemos, por tanto, que CRYPTO ASSETS deberá cumplir con las obligaciones que las normas de protección de datos atribuyen a tales figuras, a saber:

- Cumplir con los principios del tratamiento de datos (artículo 5.1, RGPD):
    - Licitud, lealtad y transparencia del tratamiento.
    - Limitación de la finalidad.
    - Minimización de datos tratados.
    - Exactitud de los datos tratados.
    - Limitación del plazo de conservación de los datos.
    - Integridad y confidencialidad de los datos.

- En cuanto a la licitud del tratamiento, que éste se circunscriba en alguno de los que se admiten en el artículo 6 del RGPD:
    - Que se cuente con el consentimiento del interesado.
    - Que el tratamiento sea necesario para la ejecución de un contrato.
    - Que el tratamiento sea necesario para cumplir una obligación legal.
    - Que el tratamiento sea necesario para proteger los intereses vitales del interesado u otra persona física.
    - Que el tratamiento sea necesario para el cumplimiento de una misión de interés público.
    - Que el tratamiento sea necesario para la satisfacción del interés legítimo del Responsable.

- Deberán llevarse a cabo las preceptivas evaluaciones de riesgo, así como las Evaluaciones de Impacto cuando fuera necesario -tanto por imperativo legal como por considerarse oportuno-.
- Se deberá informar de forma clara y efectiva a los interesados sobre[45]:

[45] Artículos 13 y siguientes, RGPD.

- La identidad y los datos de contacto del Responsable.
- Los datos de contacto del Delegado de Protección de Datos, en su caso.
- Los fines del tratamiento y su base jurídica. Cuando ésta sea el consentimiento, deberá informársele de que puede retirarlo en cualquier momento, y en caso de que sea el interés legítimo, especificar cuál es exactamente.
- Los destinatarios de los datos que existan, en su caso.
- La existencia de situaciones de transferencia internacional de los datos.
- El plazo de conservación de los datos o el criterio usado para establecerlo.
- Los derechos de acceso, rectificación, supresión, limitación, oposición y portabilidad de los datos que amparan al interesado, y el modo previsto para que lo puedan ejercitar. También habrá que informarles de que tienen el derecho a acudir directamente ante la autoridad de control (la AEPD en España[46]) para presentar las reclamaciones que consideren oportuno.
- La existencia de decisiones automatizadas y las consecuencias que éstas puedan tener para el interesado.

No obstante, aunque todo esto deberá ser accesible por el titular de los datos, tanto como la normativa como la práctica habitual del sector ha venido admitiendo la "dosificación" de esta información en capas, siendo la primera la que primero ve el interesado, con los datos mínimos imprescindibles para que pueda considerarse informado, e incluyendo en la segunda y posteriores (a las que el usuario accederá si así lo desea) el resto de información.

En este sentido, el artículo 11 de la LOPDGDD admite que la primera capa sólo contenga tres conceptos: i) la identidad del Responsable y su representante (si lo tiene), ii) la finalidad del tratamiento y iii) la posibilidad de ejercer los derechos del interesado.

[46] Aunque los artículos 57 y siguientes de la LOPDGDD admiten la posibilidad de que aparezcan Agencias Autonómicas de Protección de Datos, en principio las competencias de estas se limitarían al sector público y a aquellos tratamientos "que se encuentren expresamente previstos […] en los Estatutos de Autonomía. Por ello, salvo que en futuras versiones de algún ET se considere que las autoridades autonómicas puedan tener competencias en materia de moneda virtuals, no será necesario mencionarlas.

- Habrá de implantar las medidas técnicas, organizativas y de seguridad que sean apropiadas para proteger los datos de los interesados y, en caso de que el tratamiento en cuestión lo exija, deberá designar un Delegado de Protección de Datos (DPO). Especialmente importantes serán las que estén relacionadas con la Seguridad desde el Diseño y la Seguridad por Defecto.

Una vez dicho todo esto, ya conocemos cuáles son las obligaciones de empresas como CRYPTO ASSETS en este marco jurídico, en tanto que serán consideradas Responsables por los datos que recojan y traten para sus propios fines. Pero ¿qué se le puede exigir en relación con los datos de sus clientes que vayan a ser integrados en una *blockchain?* Como ya se ha dicho, estos datos permanecerán en ella, inalterables, por un período de tiempo sobre el que CRYPTO ASSETS no tiene ningún control, lo que supone, inevitablemente, la quiebra de varios principios y la pérdida efectiva de derechos por parte de los interesados. En el caso de las personas jurídicas no sería un problema, ya que sus datos de identificación no son considerados datos de carácter personal y, por tanto, tampoco su clave pública. El problema viene cuando hablamos de personas físicas.

Partiendo de la base de que, como se ha dicho, CRYPTO ASSETS es el Responsable de los datos, ¿qué deberá tener en cuenta a la hora de "imprimir" las transacciones que se realicen a través de ella en una *blockchain?* Pues bien, el hecho de que los datos inscritos en ella estarán cifrados (*hasheados*) ya implica que se está implantando una primera medida de seudonimización. Pero para garantizar, en cierta medida, el cumplimiento de asegurar la efectividad de los derechos de los interesados, una posible medida sería hacer que el usuario emplease, para dar las órdenes a la plataforma, una clave segura, pero que ésta inscribiese las transacciones con una clave pública *ad hoc*. Dicho de otro modo, la plataforma usaría una clave pública específica para cada cliente, asignada en el momento de crear la cuenta en la plataforma, para inscribir cada transacción en la cadena de bloques.

Esta es una opción que ya se ha venido manejando desde hace un tiempo[47] (solución que impulsó la autoridad francesa, el CNIL[48]), ya que tiene la inestimable ventaja de servir

[47] EPRS, *Study on: and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?*, julio de 2019, página 88.
[48] Commission Nationale de l'Informatique et des Libertés (CNIL), *Blockchain, Solutions for a responsable use of the blockchain in the context of personal data*, París, 2018.

como medio de "borrado" de los datos que se hayan incluido en la *blockchain*. En efecto, si el usuario decidiera solicitar su eliminación, bastaría con suprimir los datos que le vinculasen a la clave pública que se le asignó en su momento y crearle otra nueva, lo que, como vimos en el apartado 2.2., imposibilitaría el acceso a esos datos. Naturalmente, habría que conservar registros de los movimientos fuera de la *blockchain* para poder cumplir con las obligaciones legales, conforme a los principios de legalidad, limitación de la conservación y de responsabilidad proactiva.

Otra posible opción sería la anonimización de los datos, conforme a criterios basados en el riesgo, de forma previa a su inclusión en la cadena de bloques. Sin embargo, los requisitos para considerar que un dato es anónimo (recordemos que ésta deberá ser irreversible) son tan elevados que, en la práctica, incluso grandes entidades con muchos recursos tienen problemas para cumplir. Y una *start-up* lo tendría aún más complicado.

También se ha planteado la opción de considerar a la *blockchain* en la que se inscriben los movimientos como un Encargado o Corresponsable de tratamiento[49]. Esto, a mi parecer, sería inútil en el contexto actual, ya que, precisamente, las cadenas de bloques públicas son sistemas de registro descentralizados y no existe nadie detrás que las controle directamente ni, por tanto, pueda firmar contratos. Por supuesto, esto no quita que las entidades que creen *blockchains* privadas deban cumplir con requerimientos de la normativa de protección de datos.

En este caso también existe un régimen sancionador, y bastante estricto, además. Las multas por incumplimiento de las obligaciones en materia de protección de datos pueden alcanzar los 20.000.000 de Euros o hasta el 4% del volumen de negocio anual global en los casos más graves, por lo que es una normativa que merece la pena cumplir. Si bien es cierto que el RGPD se empezó a aplicar hace apenas año y medio, las cifras que publicó la AEPD no dejan lugar a dudas: las reclamaciones ante la autoridad española crecieron "casi un 33%" de 2017 a 2018, y las resoluciones sancionadoras fueron 907, frente a las 852 de 2018 (de las cuales 434 supusieron una sanción económica)[50]. Las autoridades nacionales todavía tantean un terreno que es nuevo, pero algunas como la francesa[51] (la

[49] Commission Nationale de l'Informatique et des Libertés (CNIL), *Blockchain, Solutions for a responsable use of the blockchain in the context of personal data*, París, 2018, punto 4.
[50] Infografía "La Agencia Española de Protección de Datos en cifras (2018)", mayo de 2019 (consultado en https://www.aepd.es/media/infografias/memoria-AEPD-2018.jpg el 05/09/2019).
[51] Sancionó a Google con 50 millones de Euros tras las denuncias por incumplimientos de varias organizaciones, al considerar que existió por parte de la plataforma una grave "falta de transparencia, la

CNIL) o la italiana[52] (la AGCM) ya han impuesto multas de gran calado y la sociedad cada vez presta más atención a la protección de los datos personales. La importancia del cumplimiento normativo en este ámbito es creciente, y no hacerlo puede, como ya hemos visto, suponer sanciones capaces de hacer peligrar la supervivencia de muchas empresas.

En fin, y a modo de síntesis, queda claro que CRYPTO ASSETS **deberá cumplir con esta normativa**, adaptando sus Políticas de Privacidad y de uso de *cookies* (si las hay) a los estándares mencionados y asegurando la privacidad de las personas físicas que participen de su plataforma.

2.5. MiFID II Y MIFIR

Ambas normas fueron promulgadas el mismo día 15 de mayo, con la experiencia de la Crisis de 2007 a sus espaldas y los objetivos principales de unificar criterios entre Estados miembros y mejorar la transparencia en los mercados y la seguridad de quienes inviertan en productos financieros, con especial énfasis en los minoristas, por lo general más desprotegidos[53]. Aunque fuera *in extremis* -como lo definieron algunos periódicos en su momento- España transpuso parcialmente la Directiva a principios del 2018, culminando la misma en diciembre del mismo año, en el Real Decreto Ley 1464/2018, por el que se desarrolla el Texto Refundido de la Ley de Mercado de Valores (TRLMV).

Pero ¿dónde está la dificultad para establecer la relación que CRYPTO ASSETS tiene con esta normativa? Pues el principal problema se centra en la falta de consenso normativo acerca de qué es una moneda virtual. El ESMA (*European Securities and Markets Authority*), recordaba en su informe de enero de este año que actualmente no existe ninguna definición de "criptoactivo" en la normativa financiera de la Unión (desde la quinta Directiva de PBC ya tenemos una en ese ámbito, como hemos visto), pese a que es un elemento clave para saber si son "calificables como instrumentos financieros dentro

información insatisfactoria proporcionada y la falta de consentimiento válido para la personalización de publicidad". Fuente: http://www.mundolopd.com/privacidad/denuncias-google-sancioni-50-millones/, consultada el 18/09/2019.

[52] Sancionó a Facebook con 10 millones de Euros por "suministrar los datos de sus usuarios para fines comerciales sin informarles" previamente. Fuente: http://www.mundolopd.com/privacidad/denuncias-google-sancioni-50-millones/, consultada el 18/09/2019.

[53] RUIZ DOTRAS, E., *Poscrisis: tipos de interés cero, devaluaciones sincrónicas y moneda virtuals*, Oikonomics, Revista de economía, empresa y sociedad de la UOC, ISSN 2339-2546, Barcelona, 2018, página 47.

de la MIFID II"[54]. Esto ha venido obligando a los reguladores nacionales a aplicar por analogía muchas normas que no prevén este uso, sin contar con que su labor interpretativa puede ser invalidada tanto por el legislador como por los tribunales, con la consiguiente inseguridad jurídica.

De hecho, nuestra CNMV, en su comunicado conjunto con el Banco Central[55], muestra un gran escepticismo en relación con las monedas virtuales. El texto está dedicado a advertir al potencial inversor en este tipo de activos de los riesgos que llevan asociados, como la elevada volatilidad o que no existen en un entorno regulado o controlado.

Ante esta tesitura, el ESMA solicitó la opinión de dichas autoridades nacionales competentes que, de forma mayoritaria, consideraron que algunos tipos de cripto activos (entre el 10 y el 30% de los que existían en ese momento) podrían ser considerados valores negociables según la MiFID II[56]; es decir, un tipo de instrumento financiero[57].

Esta Directiva enumera las actividades que pueden ser consideradas como "servicios y actividades de inversión"; en lo que a CRYPTO ASSETS interesa, lo serían

- Las de recepción, transmisión y ejecución de órdenes de clientes relativas a instrumentos financieros.
- Asesoramiento en materia de inversión.

Aunque CRYPTO ASSETS no tiene la necesidad de lanzar (al menos por el momento), una ICO para financiarse, en el mundo de las monedas virtuales es algo tan habitual que nunca está de más tener unas nociones básicas sobre las consecuencias que puede tener elegir bien el modo de elaborar el proyecto; además (y más importante) en otro comunicado la CNMV y el BCE establecen, *de* facto, el tipo de *tokens* que van a ser considerados como "instrumento financiero". Para ambos organismos, los factores relevantes "para valorar si a través de una ICO se están ofreciendo valores negociables" son:

> "*i) Que los tokens atribuyan derechos o expectativas de participación en la potencial revalorización o rentabilidad de negocios o proyectos o, en*

[54] European Securities and Markets Authority (ESMA), *Advice on Initial Coin Offerings and Crypto-Assets*, de 9 de enero de 2019, punto 77.
[55] CNMV y Banco de España, *Comunicado conjunto de la CNMV y del Banco de España sobre "moneda virtuals" y "ofertas iniciales de moneda virtuals" (ICOs)*, de 8 de febrero de 2018, Madrid.
[56] Ídem, punto 82.
[57] Anexo I, Sección C, Directiva 2014/65/UE, relativa a los mercados de instrumentos financieros, de 15 de mayo.

general, que presenten u otorguen derechos equivalentes o parecidos a los propios de las acciones, obligaciones u otros instrumentos financieros incluidos en el artículo 2 del TRLMV (instrumentos financieros sometidos a la ley (texto refundido de la ley del mercado de valores)).

ii) En el caso de tokens que den derecho a acceder a servicios o a recibir bienes o productos, que se ofrezcan haciendo referencia, explícita o implícitamente, a la expectativa de obtención por el comprador o inversor de un beneficio como consecuencia de su revalorización o de alguna remuneración asociada al instrumento o mencionando su liquidez o posibilidad de negociación en mercados equivalentes o pretendidamente similares a los mercados de valores sujetos a la regulación."[58]

En lo que afecta a CRYPTO ASSETS, de hecho, su proyecto de tokenización de activos para la inversión les asimilaría mucho a la definición i). Sin embargo, el hecho de que este comunicado conjunto se enfoque únicamente en las ICOs, hace que la empresa **no sea considerada sujeto obligado** bajo esta normativa. Sin embargo, dada la cercanía de ambos proyectos, sería recomendable adoptar medidas que redunden en una mayor seguridad de sus usuarios-inversores.

En este sentido conviene recordar que la consideración de alguno de estos tipos de *token* como un activo financiero podría conllevar la obligación de cumplir, entre otras, con las siguientes normas europeas y la que las desarrollen, de modo que una buena medida proactiva sería aplicar alguna de sus obligaciones[59]:

- Directiva de Folletos.
- Directiva de Transparencia.
- Directiva sobre la Firmeza en la Liquidación de Valores.
- Etc.

[58]CNMV, *Consideraciones de la CNMV sobre "moneda virtuals" e "ICOs" dirigidas a los profesionales del sector financiero*, de 8 de febrero de 2018, Madrid.
[59]GÓMEZ DE LA CRUZ ALCAÑIZ, A., *Análisis sobre la regulación de criptoactivos en Europa*, ICOFUNDING, Madrid, 2019, página 8.

Y también merece la pena recordar, aunque no le sea aplicable a CRYPTO ASSETS, que el incumplimiento de la normativa relativa a instrumentos financieros (MIFIR, MIFID II y el Real Decreto 1464/2018) expondrá a quien lo cause a su régimen sancionador, siendo las más graves la prohibición temporal o permanente para ejercer y la imposición de multas administrativas de hasta 5.000.000 de € y/o del doble de los beneficios derivados de la infracción, en su caso.

2.6. Ley de Servicios de Pago

La Directiva 2015/2366, sobre servicios de pago en el mercado interior es una norma que tampoco va a aplicarse a las plataformas que utilicen monedas virtuales. Sin embargo, considero que es muy interesante hacer un pequeño comentario sobre ella en aras de aclarar el motivo. Hoy por hoy la PSD2 funciona sólo en el ámbito de los servicios bancarios[60] y lo que motivó que fuera promulgada en 2015 fue la enorme expansión que han tenido los pagos a través de medios digitales, desde tarjetas de crédito a pagos desde teléfonos móviles[61]. Resulta imposible enmarcar a las monedas virtuales en las definiciones de "servicios de pago" que contiene el ANEXO I de la Directiva, y además, para aclarar todas las dudas que pudieran existir, el considerando 8, en su última línea, establece que sólo se aplicará "a las operaciones en todas las monedas oficiales"

En cualquier caso, el legislador no consideró apropiado tratar las monedas virtuales como medio de pago. Esto puede deberse a varios factores, de los cuales los más importantes, probablemente -no es más que una impresión personal-, sean el desconocimiento que había por aquel entonces acerca del mundo de las monedas virtuales (precisamente fue en 2015 cuando el GAFI incluyó por primera vez previsiones relativas a ellas[62]), la urgencia existente por regular los medios electrónicos de pago y que, sencillamente, se quiso elaborar una norma específica que afectase directamente a las entidades de crédito.

[60] Artículo 1.1, Directiva 2015/2366, sobre servicios de pago en el mercado interior, de 25 de noviembre. En el considerando 28 también menciona que esta norma va dirigida especialmente a entidades de crédito, y la remisión que se hace al artículo 2.1 de la Directiva 2009/110/CE para identificar a las "entidades de dinero electrónico", como ya se ha visto en el apartado de Blanqueo de Capitales, es inaplicable a las monedas virtuales.

[61] Considerando 4, Directiva 2015/2366, sobre servicios de pago en el mercado interior, de 25 de noviembre.

[62] GAFI (o FATF, por sus siglas en inglés), *Guidance for a risk-based approach to virtual currencies*, junio de 2015.

En cuanto a la Directiva de Dinero Electrónico, sólo podría considerarse aplicable cuando la moneda virtual sea definible como un "valor monetario almacenado por medios electrónicos o magnéticos que representa un crédito sobre el emisor", y además se emita al recibo de fondos con el propósito de efectuar operaciones de pago, y sea aceptado por la persona física o jurídica que vaya a recibir el pago[63]. Como vemos, son muchas condiciones, y el mero hecho de que deba "representar un crédito sobre el emisor" va a dejar fuera a la mayoría de monedas virtuales y, en concreto, a los *tokens* de CRYPTO ASSETS.

Aunque no se solicitó su tratamiento, también es recomendable hacer una pequeña mención a la Directiva (UE) 2019/713, sobre la lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo, de 17 de abril, ya que en ella se establecen varias consideraciones relativas a las "monedas virtuales", algo que resulta de gran interés.

La definición básica de esta norma es la de 'instrumentos de pago distintos del efectivo', que se define como:

"un dispositivo, objeto o registro protegido, material o inmaterial, o una combinación de estos, exceptuada la moneda de curso legal, que, por sí solo o en combinación con un procedimiento o conjunto de procedimientos, permite al titular o usuario transferir dinero o valor monetario incluso a través de medios digitales de intercambio"[64]

Pues bien, aunque menciona, con claridad meridiana, a las monedas virtuales al decir que serán 'instrumentos de pago distintos del efectivo' los registros protegidos (principalmente *hashes* y firmas electrónicas) que por sí solos o en combinación con un conjunto de procedimientos permita transferir dinero o valor monetario, se establece una especialidad para ellas que va a determinar los sujetos obligados por esta norma. Así, el considerando 10 de esta norma indica que deberá aplicarse "a las monedas virtuales sólo en la medida en que puedan usarse de manera habitual para efectuar pagos"; es decir, que, siguiendo con la tendencia habitual hasta el momento en este sector, sólo serán sujetos obligados aquellos que conviertan (*exchange*) las monedas virtuales en dinero real o

[63] GÓMEZ DE LA CRUZ ALCAÑIZ, A., *Análisis sobre la regulación de criptoactivos en Europa*, ICOFUNDING, Madrid, 2019, página 15.
[64] Artículo 2.a), Directiva (UE) 2019/713, sobre la lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo, de 17 de abril.

funcionen como un vehículo que permita el intercambio de monedas virtuales por bienes y servicios (*wallets*).

Para acabar, quedaría simplemente mencionar que la Directiva (UE) 2019/713 contiene también un mandato a los Estados miembros para que, antes del 31 de mayo de 2021, establezcan régimen propio de responsabilidad para personas físicas y jurídicas, así como sanciones que incluyan, además de multas de carácter penal, otras como la exclusión para el disfrute de ayudas públicas, inhabilitación temporal o permanente para el ejercicio de sus actividades comerciales o incluso la disolución judicial de la entidad.

CONCLUSIONES

Este informe estaba destinado a establecer si los marcos normativos estudiados eran aplicables al modelo de CRYPTO ASSETS.

La tokenización de activos que propone CRYPTO ASSETS es un proyecto con repercusiones muy interesantes en el mercado, ya que podría servir a muchos propósitos: desde otra óptica, podría ser una fuente de financiación alternativa a las tradicionales, como el préstamo hipotecario, a una forma de organizar propiedades colectivas.

Es de esperar que gran parte de la nueva legislación que está por venir vaya por el camino de integrar las monedas y activos virtuales en el tráfico económico general. Y esto, desde el punto de vista de las empresas que se hayan constituido aprovechando la falta de regulación actual, puede ser un problema. Por ello se ha propuesto establecer unas medidas internas de cumplimiento mínimas que vayan dirigidas a ofrecer garantías a los clientes, especialmente las relativas a la seguridad de la información.

El grueso del informe está destinado al análisis de las normas. En él, se han tratado cinco ámbitos en los que las plataformas que operan en el entorno de las monedas virtuales pueden tener una afectación más especial y, además, cómo el régimen general del Código Civil será el que pueda suponer, de forma residual, la **responsabilidad civil** de la empresa, en su caso.

Cumplir con la Ley 34/2002, de Servicios de la Sociedad de la Información es relativamente sencillo. Bastaría con estar al día con los deberes de información que constan en el artículo 10 y con las obligaciones relativas a la contratación por Internet que desarrollan los artículos 27 y siguientes. Dado que cualquier prestador de servicios de la sociedad de la información debe cumplir con esta norma, y tener una plataforma que opera en Internet, aceptando y facilitando transacciones cae, sin lugar a dudas, en la definición de este concepto, es seguro que CRYPTO ASSETS **deberá cumplir con sus deberes en este ámbito**.

La normativa de PBC, por su parte, será de **cumplimiento obligatorio**, ya que, si bien su aplicación a las empresas que se dedican a la prestación de servicios de activos virtuales es muy reciente, se trata de obligaciones cuya implantación debe hacerse desde el primer momento, antes incluso (si no se ha hecho ya) de empezar la actividad. Por ello se recomienda la implantación de medidas de *due diligence* cuando sea pertinente, que se registre ante la autoridad competente (el SEPBLAC en el caso de España) y se asegure

de “obtener, retener y transmitir la información requerida sobre el originador y el beneficiario, de manera inmediata y segura” cuando se realicen transferencias de activos virtuales.

También **deberá cumplir**, desde luego, con la normativa de protección de datos personales, ya que la seguridad de todos los datos de sus clientes que sean personas físicas habrá de estar garantizada. Como sabemos, CRYPTO ASSETS será Responsable de estos datos, y deberá cumplir con todas las obligaciones relacionadas con este estatus. Además, dada la problemática que la inclusión de los datos de estas personas en una *blockchain* tiene en cuanto al cumplimiento de las obligaciones relacionadas con sus derechos y con los principios básicos del tratamiento, se recomienda establecer las medidas mencionadas en el informe y que avalan autoridades nacionales como el CNIL francés.

En cuanto a la normativa financiera, como se ha visto, **no resulta de aplicación**. Sin embargo, aunque se modifique el modelo de negocio para que no se le aplique la normativa financiera, sería recomendable ofrecer a los consumidores algún tipo de garantías de las que se prevén en estas normas, a través de normas corporativas vinculantes o la adhesión a un Código de Conducta.

Por último, queda recordar que CRYPTO ASSETS **no resultará afectada** por la normativa relativa a los medios de pago, ni la vigente actualmente ni la que entra en vigor en 2021, aunque dado el mandato que la Directiva (UE) 2019/713 impone a los Estados, se recomienda estar al tanto de la posible evolución legislativa en este ámbito.

1. El futuro inmediato.

A lo largo de todo el informe ha habido una constante: la regulación de las monedas y los activos virtuales está todavía muy joven, pero las autoridades, tanto nacionales como internacionales, han puesto ya sus ojos sobre esta nueva forma de entender el dinero. Son conscientes de que es un ámbito que escapa al control que es capaz de ejercer un Estado sobre su moneda -o el Banco Central Europeo en el caso de la Unión-, por lo que es de esperar que en los próximos años veamos avances significativos en su regulación. La Quinta Directiva de Prevención del Blanqueo de Capitales y la Financiación del Terrorismo ya sentó un primer precedente legislativo que entrará en vigor plenamente en el año 2020, y el GAFI, por su lado, sigue adaptando sus Recomendaciones para tratar de ordenar el sector en el marco de la lucha contra el blanqueo de capitales. Así pues, ¿Qué

debe tener en cuenta una *start-up* (o cualquier otra empresa que emplee monedas virtuales en su modelo de negocio, realmente) para estar preparada para estos cambios normativos que se avecinan?

Por todo lo dicho, hay que esperar el establecimiento de normas eminentemente internacionales, ya que las políticas nacionales que intentasen combatirlo sin coordinarse con el resto de actores internacionales "tendrían efectos muy limitados"[65]. Si bien es cierto que algunos Estados ya han empezado a tomar medidas por su cuenta, las tendencias son más bien variadas.

Por una parte, está el grupo de países que han optado por prohibir el uso de monedas virtuales en el comercio interior, como China, Bangladesh, Rusia o Ecuador[66]. Se trata, como vemos, de naciones eminentemente intervencionistas, que, como se suele decir, si me permiten la expresión, "tratan de ponerle puertas al campo", ya que un ciudadano de cualquiera de ellos que se interesase por las monedas virtuales podría usar una VPN para evitar el control estatal (en caso de que la prohibición llegase tan lejos, como en el caso de China).

Por otra parte, Estados como Japón, que fue el primero en autorizar "el uso del Bitcoin como medio de pago legal"[67], en 2016, o Malta, que las reconoce también como medio de intercambio. Este es el grupo de países más escaso, ya que, si bien se suelen enmarcar en otro más amplio (los conocidos como "*crypto friendly"*) lo cierto es que la mayoría se limitan a establecer normas de tributación favorables para quien las use, ya sea en su actividad económica o en su vida privada, en el caso de personas físicas. Algunos de estos segundos podrían ser Suiza, tan conocido por sus normas favorables a las *start-ups* de este tipo que hay una región, Zug, que es conocida como "*crypto valley*", o Eslovenia, que consideró al Bitcoin como "moneda virtual" en 2017, antes de que lo hiciera la Quinta Directiva de Prevención del Blanqueo de Capitales y la Financiación del Terrorismo.

Por último, tenemos el grupo más amplio de países, entre los que se encuentra España, que están tratando de encuadrar las monedas virtuales en las normas ya existentes, especialmente en materia de productos financieros, con las carencias e incompatibilidades

[65]Considerando 4, Directiva (UE) 2015/849, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo.
[66] MATUTE, M., *Las 'Moneda virtuals': alarma mundial*, Escritura PÚBLICA, 2018 (consultado en https://www.notariado.org/liferay/c/document_library/get_file?folderId=12092&name=DLFE-320372.pdft el 17/08/2019).
[67] Ídem.

que esto conlleva. Incluso así, las posturas son diversas, y se dan casos en los que la postura es favorable a las monedas virtuales (en Holanda le han dado al Bitcoin la consideración de objeto de trueque) y, en otros, se emiten señales de alarma. Aquí, la CNMV ha emitido diversas consideraciones en este sentido, pero sin una adaptación legislativa específica, la capacidad adaptativa del Derecho a una nueva realidad de estas características es muy limitada.

Teniendo esto en cuenta, sería recomendable una adaptación proactiva de los participantes en el mundo de las monedas y activos virtuales, ya sea a través de códigos de conducta específicos o de normas corporativas vinculantes que se adelanten, en la medida de lo posible, a las modificaciones legislativas que están por venir y ofrezcan garantías específicas a los usuarios -considerándoles, incluso, (dependiendo del caso) como consumidores conforme a la normativa específica en este ámbito-. Dado que muchas de las plataformas (como CRYPTO ASSETS) realmente operan desde la óptica de la economía colaborativa, la autorregulación será, en general, esencial para prepararse ante lo que está por venir.

Por ejemplo, una de las cuestiones a las que apunta la doctrina especializada es a la aparente intención que subyace detrás del artículo 4.c) de la Directiva 713/2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo de implantar un nuevo delito de "lavado de monedas virtuales"[68]. El mandato que este precepto impone a los Estados es el de incluir en sus ordenamientos jurídicos la conducta delictiva de "*posesión, para su utilización fraudulenta, de un instrumento de pago inmaterial distinto del efectivo que haya sido objeto de obtención ilícita, falsificación o alteración, al menos si el origen ilícito del instrumento se conocía en el momento de su posesión*". Sin embargo, la premisa de que quien realizase este acto delictivo debería conocer el origen ilícito de las monedas virtuales que obrasen en su posesión es, a día de hoy, prácticamente inviable. Si bien es cierto que una de las ventajas del *blockchain* es que todo queda registrado y que esos registros son públicos, el anonimato que impera en estos ecosistemas es una gran traba para el cumplimiento de esta obligación. Por otra parte, aunque ahora los *exchanges* y empresas como CRYPTO ASSETS estarán obligados a identificar a quienes utilicen sus plataformas, debe recordarse que no es obligatorio hacerlo para usar y adquirir monedas virtuales; ¿significa eso que se podría

[68] ZÁRATE, C., *Este es el futuro delito de blanqueo de moneda virtuals*, Revista Byte, 2019, Madrid (consultado en https://revistabyte.es/actualidad-byte/blanqueo-de-moneda virtuals/ el 19/09/2019).

llegar a presumir, en un futuro, que toda moneda virtual no adquirida a través de un "sujeto obligado legalmente" tiene un origen ilícito? A día de hoy no parece muy probable, pero todo dependerá de la eficacia de las medidas que se vayan adoptando. Con todo, esta medida parece algo vacua.

Por otro lado, es de esperar un "estrechamiento del cerco" del Derecho Financiero entorno a las ICOs, Los Gobiernos y la mayoría de entidades intergubernamentales competentes ya han mostrado su preocupación por este tema, y es que, en 2018, ya se estimó que el 80% de las ofertas iniciales de moneda virtual que se emitían eran un fraude[69]. Por desgracia no hay datos más actuales, aunque se entiende que la proliferación del uso de las monedas virtuales debería ir aportando más luz a estos ámbitos, moderando el porcentaje de abusos que se llevan a cabo. El principal objeto de preocupación es, de nuevo, lo difícil que resulta identificar verdaderamente a los sujetos que están detrás de las ICOs. Por ello, una de las medidas estrella que podemos esperar en un plazo no muy largo es el establecimiento de requisitos de identificación por parte de sus promotores, la obligación de que éstas se lancen en plataformas con una certificación especial, etcétera; de forma similar a lo que ocurre en los mercados financieros tradicionales.

En cualquier caso, el elevado margen para la especulación que reina en este ámbito debe apelar a la cautela a la hora de internarnos en este mundo, y la regulación que está por venir, más que acabar con los activos y monedas virtuales, puede revitalizarlos. Si se hace bien, dotar a este sector de normas y garantías legales hará muchas personas que optan por no acercarse a ellos por inseguridad y desconfianza decidan hacerlo. Ahora está en manos de los Estados decidir si combaten esta nueva forma de entender el dinero o si lo acogen como un modelo compatible (o incluso sustitutivo, eventualmente) con el tradicional.

[69] Informe *CryptoAsset Market Coverage Initiation: Network Creation*, de SATIS GROUP para BLOOMBERG, 11 de julio de 2018, página 1.

BIBLIOGRAFÍA, NORMAS Y DOCUMENTOS UTILIZADOS

1. BIBLIOGRAFÍA

ALEXANDRE, A., *El GAFI fortalecerá el control sobre los exchanges de monedas virtuales para prevenir el lavado de dinero*, CoinTelegraph, junio de 2019 (consultado en https://es.cointelegraph.com/news/fatf-to-strengthen-control-over-crypto-exchanges-to-prevent-money-laundering, el 19/08/2019)

BEYER, S., *before Bitcoin: a history*, BlockTelegraph.io, 2018 (consulted en https://blocktelegraph.io/*blockchain*-before-bitcoin-history/ el 12/06/2019).

BLANCO PÉREZ, M.A., LÓPEZ-ROMÁN, E. *et alia, Contratos Inteligentes: los "Smart Contract",* blog CGAE, 2017 (consultado en https://www.abogacia.es/2017/03/06/contratos-inteligentes-los-smart-contract/ el 01/08/2019).

BUTERIN, V., *DAOs, DACs, DAs and More: An Incomplete Terminology Guide*, blog Ethereum.org, 2014 (consultado en https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/?source=post_page---------- el 30/07/2019).

BUTERIN, V., *On Public and Private s*, blog Ethereum.org, 2015 (consultado en https://blog.ethereum.org/2015/08/07/on-public-and-private-*blockchains*/ el 10/08/2019).

CARRERAS BAQUER, O., *¿Qué podemos esperar de las Monedas virtuales?,* "Dossier: el dinero: pasado, presente y futuro", Caixabank Research, 2018.

GALÁN, J., *y la nueva moneda virtual Libra, concepto a concepto*, "El País Economía", 2019 (consultado en https://retina.elpais.com/retina/2019/07/12/innovacion/1562924481_828592.html el 26/06/2019).

GÓMEZ DE LA CRUZ ALCAÑIZ, A., *Análisis sobre la regulación de criptoactivos en Europa*, ICOFUNDING, Madrid, 2019.

GONZÁLEZ-MENESES, M., *Entender el blockchain, una introducción a la tecnología de registro distribuido*, Thomson-Reuters Aranzadi, Madrid, 2017.

GUILLERMO JIMÉNEZ, W. y SOLER PEDROZA, I., *¿Cómo establecer la jurisdicción y competencia en casos de internet? Tendencias internacionales y nacionales*, Revista Diálogos de Saberes, nº 41, páginas 15-32, Bogotá, 2014.

LEGERÉN MOLINA, A., *Retos jurídicos que plantea la tecnología de la cadena de bloques. Aspectos legales de Blockchain,* Revista de Derecho Civil, vol. VI, núm. 1 (enero-marzo), Estudios, A Coruña, 2019.

LESSIG, L., *Code and Other Laws of Cyberspace*, 1999.

MATUTE, M., *Las 'Monedas virtuales': alarma mundial*, Escritura PÚBLICA, 2018 (consultado en https://www.notariado.org/liferay/c/document_library/get_file?folderId=12092&name=DLFE-320372.pdft el 17/08/2019).

NAKAMOTO, S. (seudónimo), *Bitcoin: a peer-to-peer Electronic Cash System,* blog Bitcoin.org, 2008.

NIETO GIMÉNEZ-MONTESINOS, M.A. y HERNÁEZ MOLERA, J., *Monedas virtuales y locales: las paramonedas, ¿nuevas formas de dinero?*, Revista de Estabilidad Financiera, Banco de España, Núm. 35, páginas 105-122, Madrid, 2018.

PÉREZ LÓPEZ, X., *Blanqueo de Capitales y TIC: marco jurídico nacional y europeo, modus operandi y monedas virtuales [Ciberlaundry. Informe de situación],* Thomson-Reuters Aranzadi, Madrid, 2019.

RUIZ DOTRAS, E., *Poscrisis: tipos de interés cero, devaluaciones sincrónicas y monedas virtuales*, Oikonomics, Revista de economía, empresa y sociedad de la UOC, páginas 45-57, ISSN 2339-2546, Barcelona, 2018.

RUIZ-GALLARDÓN, M., *Fe Pública y "tokenización" de activos en blockchain, en Criptoderecho. La regulación de blockchain*, Wolters Kluwer, Madrid, 2018.

ZÁRATE, C., *Este es el futuro delito de blanqueo de monedas virtuales*, Revista Byte, 2019, Madrid (consultado en https://revistabyte.es/actualidad-byte/blanqueo-de-monedas virtuales/ el 19/09/2019).

2. DOCUMENTOS

CNMV y Banco de España, *Comunicado conjunto de la CNMV y del Banco de España sobre "monedas virtuales" y "ofertas iniciales de monedas virtuales" (ICOs)*, de 8 de febrero de 2018, Madrid.

CNMV, *Consideraciones de la CNMV sobre "monedas virtuales" e "ICOs" dirigidas a los profesionales del sector financiero,* de 8 de febrero de 2018, Madrid.

Commission Nationale de l'Informatique et des Libertés (CNIL), *Solutions for a responsable use of the blockchain in the context of personal data*, París, 2018.

Dictamen 2017/C-246/02, de 26 de abril, del Comité Económico y Social Europeo sobre «*Digitalización y modelos económicos innovadores en el sector financiero europeo, consecuencias para el empleo y para la clientela*».

EPRS, *Study on: and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?*, julio de 2019.

European Securities and Markets Authority (ESMA), *Advice on Initial Coin Offerings and Crypto-Assets*, de 9 de enero de 2019.

GAFI (o FATF, por sus siglas en inglés), *Recomendaciones GAFI.*

GAFI, *Directrices para un enfoque basado en riesgo: Monedas Virtuales*, de junio de 2015.

GAFI, *Guidance for a risk-based approach to Virtual Assets and Virtual Asset Service Providers*, junio de 2019.

Infografía "*a Agencia Española de Protección de Datos en cifras (2018)*, mayo de 2019 (consultado en https://www.aepd.es/media/infografias/memoria-AEPD-2018.jpg el 05/09/2019).

Informe *CryptoAsset Market Coverage Initiation: Network Creation*, de SATIS GROUP para BLOOMBERG, 11 de julio de 2018, página 1.

Lista de coinmarketcap.com sobre monedas virtuales.

Securities and Exchange Commission, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, Release Nº 81207, 2017.

T&C de Bitcoin ("9. *Arbitration*"), consultados en https://bitcoin.org/es/legal#english-noliability el 11/09/2019.

T&C de Ethereum ("*Governing Law and Jurisdiction*"). Consultado en http://ethereum.org/terms-of-use/ el 11/09/2019;

White paper de Libra, https://libra.org/es-LA/white-paper/#introduction (consultado el 23/06/2019).

3. NORMAS

Código Civil de24 de julio de 1889.

Directiva (UE) 2014/65, relativa a los mercados de instrumentos financieros, de 15 de mayo.

Directiva (UE) 2015/849, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, de 20 de mayo.

Directiva (UE) 2015/849, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, de 20 de mayo.

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

Directiva (UE) 2019/713, sobre la lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo, de 17 de abril.

Directiva (UE) 2019/713, sobre la lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo, de 17 de abril.

Ley 34/2002, de Servicios de la Sociedad de la Información

Real Decreto 1464/2018, de 21 de diciembre, por el que se desarrollan el texto refundido de la Ley del Mercado de Valores

Reglamento (UE) 600/2014, relativa a los mercados de instrumentos financieros, de 15 de mayo.