Bitcoin
¿Qué es eso?

1.- Qué es.

El Bitcoin es una entre muchas divisas digitales conocidas como criptomonedas. Sus dos principales características son que, diferencia de las monedas tradicionales, se puede realizar transacciones directamente entre particulares, sin intervención de terceros (como los bancos) y que su funcionamiento no depende de una institución central, sino de una base de datos distribuida.

En palabras de Félix Moreno de la Cova, abogado y economista referente en España del mundo Bitcoin, se puede definir como:

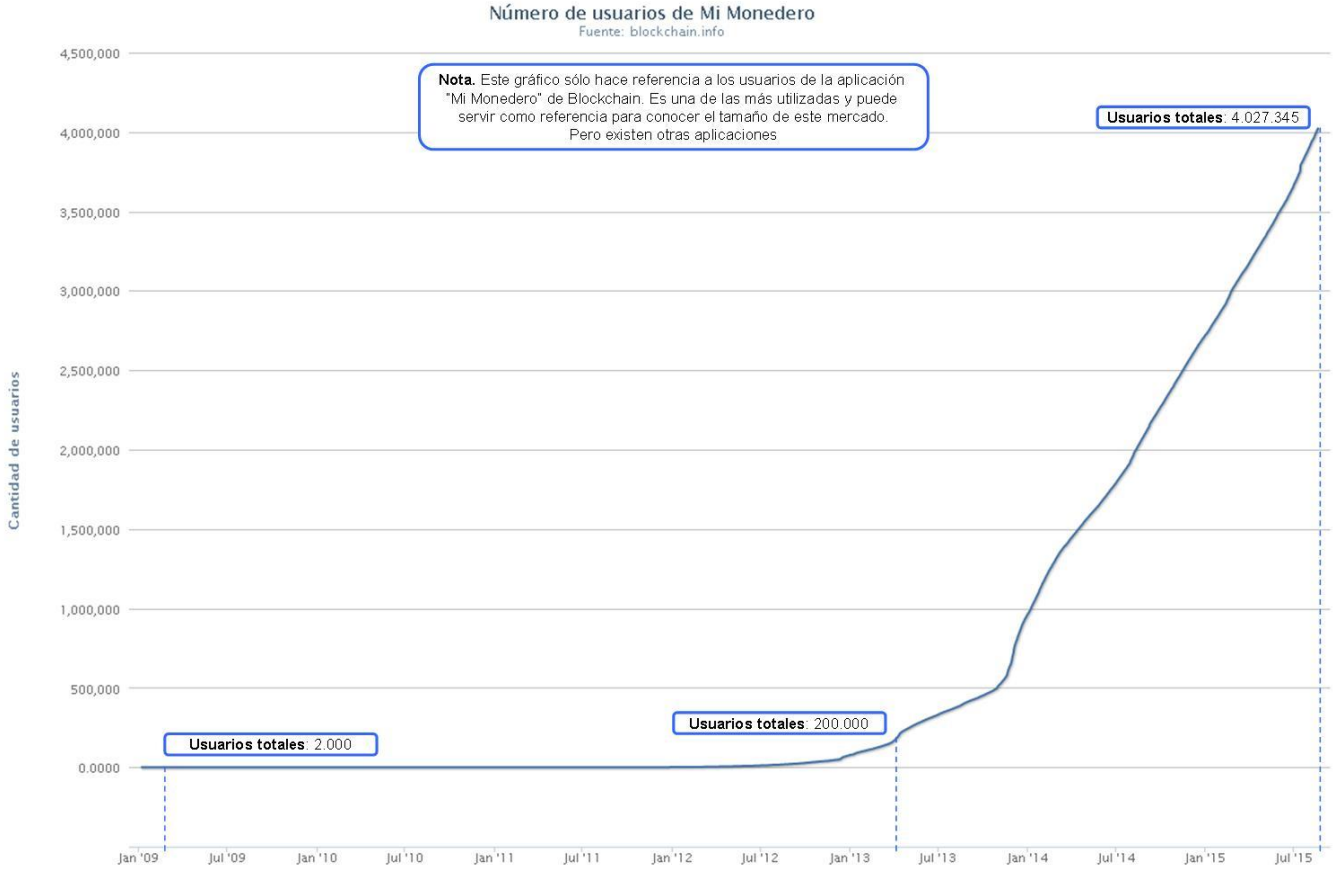
> "*Un acuerdo voluntario entre sus usuarios para utilizar 21 millones de fichas cifradas, y matemáticamente seguras, como moneda. Es decir: como unidad de cuenta, medio de pago y reserva de valor*".

Desde un punto de vista más jurídico, Pablo Fdez. Burgueño (abogado fundador de Abanlex, bufete especializado en Bitcoins) define así esta criptomoneda:

> "*Un Bitcoin es un bien patrimonial inmaterial, documento electrónico, objeto de derecho real, en forma de unidad de cuenta, definida mediante la tecnología informática y criptográfica denominada "Bitcoin", que permite ser utilizada como contraprestación en transacciones de todo tipo.*

Dichas unidades de cuenta son irrepetibles, no son susceptibles de copia y no necesitan intermediarios para su uso y disposición"

La conocida como "la moneda de Internet" es un proyecto relativamente nuevo que se encuentra en evolución. Por esta razón, sus desarrolladores recomiendan ser cautos y tratarlo como algo experimental por el momento. Sin embargo cada día son más los negocios y particulares que se suman al uso de esta moneda. Negocios tradicionales como restaurantes, tiendas, bufetes de abogados y servicios de Internet populares como Namecheap, Wordpress, Reddit y Flattr. En verano de 2012 el número total de usuarios no pasaba de 2.000, en julio de 2015 supera los 4 millones.



La palabra *Bitcoin* sirve para referirse tanto a la divisa digital como al sistema o protocolo que permite su existencia y funcionamiento. Este último también se conoce como *Blockchain*.

Bitcoin se podría considerar cómo la primera criptomoneda. Sin embargo no es la única, existen otras menos famosas que, aprovechando el protocolo abierto del *Blockchain,* han creado sus propias versiones del sistema pero compartiendo la misma base. Algunos ejemplos son las divisas *Ripple*, *Litecoin* o *Ethereum.*

2.- Origen.

La primera especificación del protocolo *Bitcoin* y la prueba del concepto la publicó Satoshi Nakamoto (seudónimo) en el 2009 en una lista de correo electrónico. Satoshi abandonó el proyecto a finales de 2010 sin revelar mucho sobre su persona. Desde entonces, la comunidad ha crecido de forma exponencial y cuenta con numerosos desarrolladores que trabajan en el protocolo Bitcoin.

Desde la década de 1970, la utilización de firmas digitales basadas en criptografía de clave pública ha proporcionado un fuerte control de propiedad. Sobre la base de la criptografía de clave pública, en 1998 Wei Dai describe b-Money, una solución descentralizada al problema de pagos electrónicos. Posteriormente, Nick Szabo y Hal Finney extienden y complementan el trabajo de Wei Dai.

En 2008, Satoshi Nakamoto publica un artículo en la lista de criptografía de metzdowd.com donde describe el protocolo Bitcoin.

El 3 de enero de 2009 la red P2P de Bitcoin entra en funcionamiento con la publicación del primer cliente, de código abierto, y la creación de los primeros Bitcoins.

3.- Características.

A) Open Software

El protocolo Bitcoin y su software se publican abiertamente y cualquier programador en cualquier lugar del mundo puede revisarlo o crear su propia versión modificada del software.

De la misma manera que nadie controla la tecnología detrás del correo electrónico, Bitcoin tampoco tiene propietarios. Bitcoin lo controlan todos los usuarios de Bitcoin del mundo. Aunque los programadores mejoran el software, no pueden forzar un cambio en el protocolo de Bitcoin porque todos los demás usuarios son libres de elegir el software y la versión que quieran. Para que sigan siendo compatibles entre sí, todos los usuarios necesitan utilizar software que cumpla con las mismas reglas. Bitcoin sólo puede funcionar correctamente si hay consenso entre todos los usuarios. Por lo tanto, todos los usuarios y programadores tienen un gran aliciente en proteger dicho consenso.

B) Cómo funciona:

- **Para el usuario normal**: desde su perspectiva Bitcoin no es más que una aplicación móvil o de escritorio más que provee un monedero Bitcoin personal y permite al usuario enviar y recibir Bitcoins con el. Así es como funciona Bitcoin para la mayoría de los usuarios.

- **Para el usuario avanzado**: Bitcoin utiliza el protocolo *Blockchain*, el cual genera una prueba infalsificable de cuatro elementos:
  - Existencia de la transacción
  - Contenido, integridad y no modificación

- Fecha y hora de registro
- Identidad (bajo seudónimo) del emisor y receptor.

Todo ello de forma automática sin la necesidad de la intervención de un tercero.

¿Cómo funciona el protocolo *Blockchain*? El proceso es sencillo, toda transacción en Bitcoins (junto a la que se puede anexar cualquier tipo de archivo) deja constancia de la existencia y contenido de dicha transacción en el día y hora en que se realizó.

Cuando los usuarios realizan transacciones éstas se almacenan públicamente y permanentemente en la red de forma encriptada, pero los *hash* (esto es, los algoritmos que representan los datos tanto de la transacción como su autor) pasan a la red de ordenadores de Bitcoin conocidos como "mineros", asegurando así su integridad e inmodificabilidad de modo que se refuerza la seguridad del sistema

Estos algoritmos son los que aportan a cada dato que se sube a la red *Blockchain* una prueba de existencia, integridad, etc. Permitiendo que terceros comprueben la legalidad de los mismos en caso de necesidad. Otra de las virtudes de la cadena de bloques es la de poder vincular unívocamente a cada usuario, y que el identificador de cada usuario esté vinculado a una persona real, como si fuera una cuenta bancaria

Gracias a esta tecnología se puede determinar de forma incontestable que esa transacción se realizó en un determinado bloque y saber la fecha exacta en que ocurrió, siendo esta información indestructible o imposible de modificar. Si se cambia el más mínimo dato del texto o archivo digital, el *hash* ya no coincidiría con el original.

C) Sistema anti-falsificación y anti-inflación

Quizás el mayor logro del creador del Bitcoin sea el de haber resuelto el problema del doble gasto en un sistema descentralizado, que tanto ha desvelado a economistas y programadores. Para evitar que un mismo Bitcoin sea gastado más de una vez por la misma persona (en otras palabras, para evitar la falsificación), la red se vale de un "servidor de tiempo distribuido", que identifica y ordena secuencialmente las transacciones e impide su modificación. Esto se logra por medio de pruebas de trabajo encadenadas también conocidas como POW por sus siglas en inglés (*Proof of work)* Dicho trabajo es realizado por los "mineros".

La oferta total de Bitcoin está limitada a 21 millones, cantidad a la que se pretende llegar, gradualmente a través del tiempo, en el año 2140. Esta autolimitación pone al Bitcoin a la par con el oro en el sentido de que la limitación funciona como un sistema antiinflacionista.

La moneda virtual usa la criptografía para controlar su creación. El sistema está programado para generar un número fijo de Bitcoins por unidad de tiempo a través de unos ordenadores llamados mineros. Actualmente, ese número está fijado en 25 Bitcoins cada diez minutos, aunque está programado de forma que se reduzca a la mitad cada 4 años. Así, a partir de 2017, se emitirán 12,55 Bitcoins cada diez minutos. La producción continuará hasta el año 2140, cuando se alcance el tope de 21 millones de unidades en circulación.

D) Seguridad contra piratas o hackers.

Mucho se ha hablado sobre la gran seguridad, en sentido informático y de software, que ofrece el protocolo *Blockchain*. Romper la seguridad del Bitcoin es matemáticamente posible, esto es debido a que el coste para lograrlo sería tan alto, que resultaría inasumible para muchas grandes multinacionales y gobiernos existentes hoy día.

Un atacante que intentase quebrar el sistema POW de Bitcoin necesitaría una potencia computacional mayor que el de todo el entramado (red-enjambre) de todos los mineros del sistema, y aun así, solo tendría una probabilidad de éxito del 50%. En otras palabras, romper la seguridad de Bitcoin exigiría una capacidad de computación y económica superior a la de empresas tecnológicas del tamaño de Google.

Pero esta moneda ha recibido múltiples ataques de hackers. El problema que todavía no ha resuelto el protocolo Bitcoin es su vulnerabilidad más común: el fallo del usuario. Los archivos de la cartera Bitcoin que almacenan las necesarias claves privadas pueden ser borradas, perdidas o robadas por los hackers. Para intentar paliar el problema se han creado algunas características que aportan mayor seguridad a ese punto, como la encriptación del monedero, monederos offline, monederos físicos y transacciones multi-firma.

D) Cómo se consiguen Bitcoins.

- Como pago por bienes o servicios.
- Mediante compra de Bitcoins en una casa de cambio de Bitcoin.
- Mediante intercambio de Bitcoins con particulares.
- A través de la actividad de Minero.

E) Los mineros

La “minería” es el sistema competitivo y descentralizado a través del cual se generan los Bitcoins, procesan transacciones, garantiza la seguridad de la red y consigue que todos los participantes estén sincronizados. Los individuos participantes son conocidos como “mineros” y están repartidos por todo el mundo.

Los servicios que ofrecen los mineros es el de procesar las transacciones y asegurar la red usando un hardware especializado. Ellos son los que llevan a cabo las pruebas de trabajo encadenadas (POW) que en su conjunto forman el conocido *Blockchain* asegurando la veracidad de las transacciones y el correcto funcionamiento de todo el protocolo Bitcoin.

Al contrario de lo que pueda parecer, ser minero no es fácil. No basta con tener un ordenador, es necesario tener un hardware especializado con un poder de computación fuera de lo normal. Ser minero conlleva una gran inversión además de que cuantos más mineros acceden a la red, más incrementa la dificultad para obtener

beneficios y los mineros deben buscar la mayor eficiencia para reducir sus costes operativos.

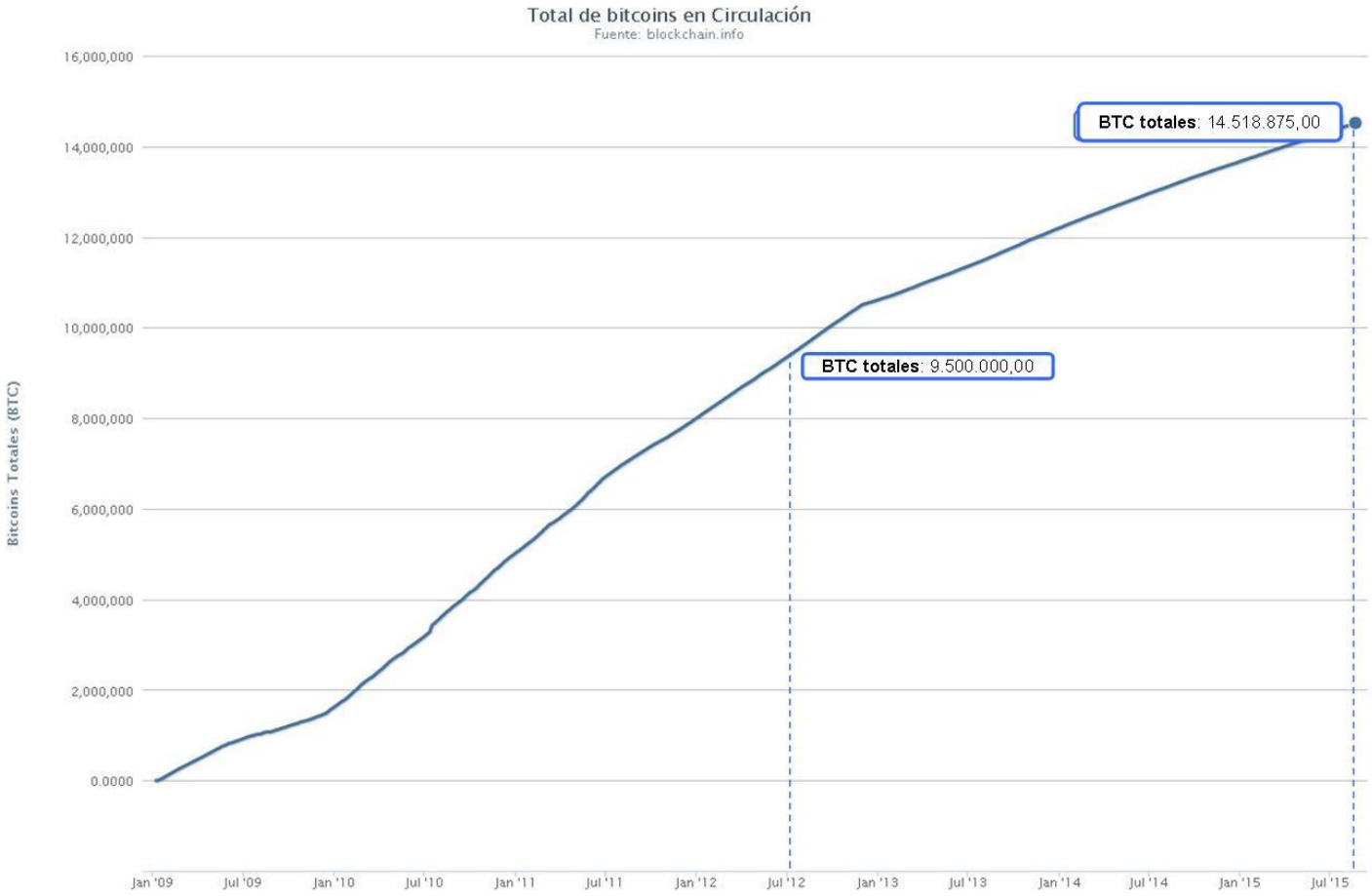
Estos mineros suelen agruparse formando asociaciones conocidas como *pools.* Gracias al trabajo conjunto consiguen mayor capacidad de computación y con ello mayor rendimiento y eficiencia.

Su actividad se recompensa por dos vías. Primero, con la entrega de los Bitcoins creados por ellos a partir de la solución de bloques; segundo, con las comisiones por acelerar las transacciones realizadas entre particulares. Estas dos vías de ingresos se complementan entre ellas de forma que con el paso del tiempo se crean menos Bitcoins pero habrá más en circulación y se harán más transacciones.

F) Creación de Bitcoins y su límite.

Como se comenta en el punto C) la creación de los Bitcoins está predefinida. El sistema está programado para generar un número fijo de Bitcoins por unidad de tiempo a través de los ordenadores de los mineros. Actualmente, ese número está fijado en 25 Bitcoins cada diez minutos, aunque está programado de forma que se reduzca a la mitad cada 4 años. Así, a partir de 2017, se emitirán 12,55 Bitcoins cada diez minutos. La producción continuará hasta el año 2140, cuando se alcance el tope de 21 millones de unidades en circulación.

Dicha limitación es una medida anti-inflacionista. Sin embargo, esto nunca será una limitación a su intercambio entre agentes de mercado pues los Bitcoin pueden dividirse hasta en 8 cifras decimales (0.000 000 01 BTC) e incluso unidades mas pequeñas si es que así se lo requiere en el futuro. Conforme el tamaño promedio de transacciones decrece, estas pueden ser denominadas como sub-unidades de Bitcoin, como por ejemplo el milliBitcoin (1 mBTC o 0.001 BTC).



4.- Ventajas y oportunidades.

- **Transferencias directas entre usuarios, sin bancos de por medio**: Con Bitcoin, podrá enviar y recibir cualquier cantidad de dinero instantáneamente desde y hacia cualquier lugar del mundo, en cualquier momento. Sin bancos con horarios. Sin fronteras. Sin límites impuestos. Los usuarios de Bitcoin siempre tienen un completo control sobre su dinero.

- **Comisiones casi inexistentes**: Al no existir intermediarios, las comisiones pueden ser muy bajas en comparación con otras monedas o medios de pago.

- **Su falsificación es prácticamente imposible**: gracias a su sistema criptográfico y a las medidas de protección que posee.

- **Anonimato y seguridad**: Cuando compramos con Bitcoin, no tenemos que revelar información sensible como el número de la tarjeta de crédito o cuenta bancaria. Eso hace imposible ser víctima del famoso phishing. Además, las transacciones con Bitcoin son seguras, irreversibles, y no contienen datos personales y privados de los clientes. Esto protege a comerciantes contra pérdidas ocasionadas por el fraude o devolución fraudulenta. Asimismo, los comerciantes pueden operar en nuevos mercados en los que las tarjetas de crédito no están disponibles o los niveles de fraude sean demasiado elevados.

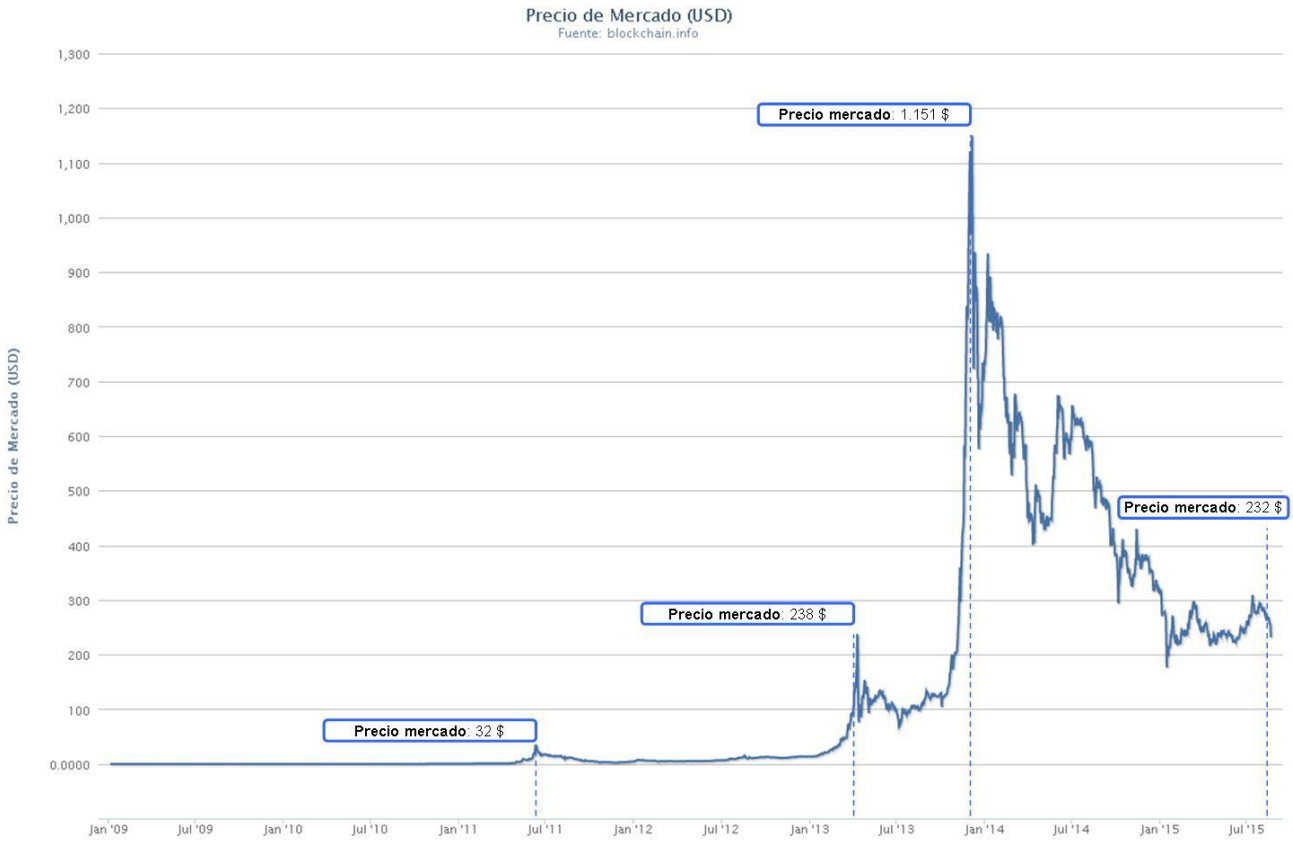
- **Neutral y Transparente**: Toda la información sobre el suministro de Bitcoin esta disponible en la cadena de bloques para cualquiera que quiera verificarlo y usarlo. Ningún individuo u organización puede controlar o manipular el protocolo Bitcoin porque es criptográficamente seguro. Se puede confiar en Bitcoin por ser completamente neutral, transparente y fiable

5.- Desventajas y riesgos.

- **Lavado de dinero:** Como consecuencia de la descentralización y el anonimato de Bitcoin, el origen o el destino de esos Bitcoin puede ser ilegal. Sobretodo preocupa la financiación del terrorismo a través de esta criptomoneda.

- **Seguridad**: Los hackers pueden robar Bitcoins accediendo a la cartera digital del usuario (se han dado muchos casos en “Plataformas de intercambio Bitcoin” alrededor del mundo). Además, Al no ver una autoridad central responsable de la divisa, los usuarios están desprotegidos ante los robos y estafas.

- **Volatilidad:** En el mercado el Bitcoin ha pasado de valer menos de 1 dólar a llegar en 5 años a 1.151 dólares el Bitcoin. En los últimos meses a caído a 232 dólares. Se trata de una divisa demasiado fluctuante, inestable y sobretodo impredecible, cosa que nunca gusta a los inversores.



- **Incertidumbre regulatoria**: Todos los riesgos anteriores hacen que la regulación sea difícil. Se quieren mitigar esos riesgos pero sin bloquear las virtudes de dicha divisa. Lo primero que se pretende regular es una obligación a las plataformas de intercambio y a los mineros de establecer un mayor control e información. Sobretodo del origen del dinero y para transacciones superiores a X cantidad. En USA se quiere regular a favor de la divisa. Pero hay otros países como china en los que se ha declarado ilegal para los bancos (los particulares pueden hacer lo que quieran).

6.- Legal.

A) Naturaleza Jurídica

Lo primero es dejar claro **qué no es el Bitcoin**.

No es dinero electrónico. Lo primero que se puede pensar sobre una divisa digital es acudir a la Ley 21/2011, de 26 de Junio, de Dinero Electrónico. Sin embargo, al leer la definición de dinero electrónico de su artículo 1.2 podemos ver que la naturaleza del Bitcoin no encaja con la misma:

> "*Todo valor monetario almacenado por medios electrónicos o magnéticos que represente un crédito sobre el emisor, que se emita al recibo de fondos con el propósito de efectuar operaciones de pago según se definen en el artículo 2.5 de la Ley 16/2009, de 13 de noviembre, de servicios de pago, y que sea aceptado por una persona física o jurídica distinta del emisor de dinero electrónico*".

Ante la falta en el Bitcoin del respaldo de un crédito contra el emisor, debemos considerar que el Bitcoin no es dinero electrónico por el simple hecho de que el emisor de dicho crédito no existe.

Una vez establecida esa premisa, hay que buscar la naturaleza jurídica del Bitcoin:

- **El Ministerio de Hacienda**, en su informe de la consulta Nº V1029-15 (30 marzo 2015), encaja el Bitcoin dentro de los "otros efectos comerciales" a los que se refiere el artículo 135.1.d) de la Directiva 2006/112/CE. Según la Secretaría General de Impuestos sobre el Consumo esos "otros efectos comerciales" se refiere a instrumentos de pago que permiten la transferencia de dinero. Es decir, se está equiparando el Bitcoin a un modo de pago similar al cheque, giro y operaciones con tarjeta de crédito. Las monedas virtuales Bitcoin actúan como un medio de pago.

- **Buscando Jurisprudencia** encontramos una única resolución al respecto, la sentencia 37/2015 del 6 de febrero 2015, de la Audiencia Provincial de Asturias. Dicha sentencia clasifica la compraventa de Bitcoin como un producto de riesgo para los bancos en relación con la Ley 10/2010 de Prevención de Blanqueo de Capitales y Financiación del Terrorismo (PBC/FT) puesto que se trata de contratación no presencial, propicia al anonimato y referente a una moneda virtual, sin autoridad central, difícilmente controlable. Por todo ello es susceptible de ser usada para el blanqueo de capitales y financiación del terrorismo.

- **En cuanto a la Doctrina,** destaca el abogado Pablo Fdez Burgueño que realiza una aproximación a la naturaleza jurídica del Bitcoin definiéndolo como "un bien patrimonial inmaterial, documento electrónico, objeto de derecho real, en forma de unidad de cuenta, definida mediante la tecnología informática y criptográfica denominada "Bitcoin", que permite ser utilizada como contraprestación en transacciones de todo tipo. Dichas unidades de cuenta son irrepetibles, no son susceptibles de copia y no necesitan intermediarios para su uso y disposición". Si bien es cierto que no se trata de una definición vinculante, también lo es que, a falta de una regulación específica, resulta bastante acertada y puede servir como referencia.

B) IVA

Por ahora es lo más claro que tenemos respecto a los efectos legales del Bitcoin. El Informe de la consulta Nº V1029-15 (30 marzo 2015) del Ministerio de Hacienda, mencionado anteriormente, no deja duda al respecto.

La decisión, basa en la interpretación de la directiva europea 2006/112/CE que regula el sistema común del impuesto sobre el valor añadido y es vinculante, concluye que **el Bitcoin está sujeto pero exento de IVA:**

> *"El concepto de «otros efectos comerciales» del artículo 135.1.d) de la Directiva 2006/112/CE está íntimamente ligado a instrumentos de pago que permiten la transferencia de dinero y que como tales operaciones financieras deben quedar exentas del Impuesto.*
>
> *Las monedas virtuales Bitcoin actúan como un medio de pago y por sus propias características deben entenderse incluidas dentro del concepto «otros efectos comerciales» por lo que su transmisión debe quedar sujeta y exenta del Impuesto."*

De esta forma la Dirección General de Tributos equipara el Bitcoin a un modo de pago similar al cheque, giro y operaciones con tarjeta de crédito, por lo que no puede tener un impuesto especial al usarse.

La consecuencia de esta decisión es que los ciudadanos residentes en España podrán comprar Bitcoins en toda Europa (incluso en los países en los que la criptomoneda está gravada con IVA como Estonia o Polonia) sin tener que desembolsar este porcentaje, ya que a ellos se les aplicará el IVA español, el cual es cero.

Esta decisión del gobierno español de calificar Bitcoin como un medio legal de pago, y por tanto no estar sujeto a IVA, coincide con la de países vecinos como Alemania, Reino Unido o Finlandia.

Pero esto **se refiere a la compraventa de Bitcoins, no al pago de productos o servicios a través de los mismos**. Hay que diferenciar la compraventa ***de*** Bitcoins y la compraventa ***con*** Bitcoins.

En el momento en el que compras un bien o servicio usando el Bitcoin como moneda sí que se debe pagar el IVA. La forma de hacerlo es sencilla: Pablo Fdez. Burgueño nos explica que la factura debe ser tradicional, pero el total a pagar deberá ser indicado también en Bitcoins.

Todas las cantidades deben mostrarse en una moneda de curso legal (euros o dólares, por ejemplo), y, al menos, el importe del Impuesto (IVA o IGIC) tiene que mostrarse en euros, según indica el RD 1619/2012 (art. 12.1). Las permutas en las que el Bitcoin es objeto de cambio, están sujetas al IVA y constituyen un gasto deducible, según indica la Ley 37/1992 (art. 79.1).

Imaginemos que queremos vender una mesa por 100€. La factura podría ser de la siguiente forma:

Concepto……100,00€ (0.6396BTC)
IVA (21%)……..21,00€ (0.1343BTC)
Total……..121,00€ (0.7739BTC)

C) Fiscalidad

Este campo es uno de los retos más difíciles que plantea el Bitcoin y su Protocolo *Blockchain*.

El Bitcoin se puede considerar un verdadero peligro para los Estados en la medida que su sistema, descentralizado y completamente anónimo, puede dejar sin sentido el sistema fiscal tal y como lo conocemos. Gracias a las propiedades ya explicadas de esta divisa digital, un usuario puede actuar de tal forma que sus operaciones sean completamente anónimas e irrastreables. De este modo es imposible calcular el IVA, IRPF, IS, etc. Estamos ante una autopista para la defraudación tributaria.

Es importante destacar que el Bitcoin juega un papel neutro. Es el usuario el que decide cómo usarlo. Si él quiere, se hará todo el registro de sus actividades de forma no anónima y rastreable, de modo podrá pagar impuestos de forma tradicional. Lo que es seguro, es la imposibilidad de Hacienda de conocer dichos datos si el usuario no lo desea. Estará por ver cómo regulan los estados para conseguir saltar este obstáculo.

Otro importante problema causado por las características del Bitcoin es que, en un hipotético caso en el que un sujeto haya sustituido su todo su dinero tradicional por unidades Bitcoin, hace más tedioso y complicado ejecutar las sentencias condenatorias de pago o cobrar las multas de toda clase.

D) Obligaciones de prevención de Blanqueo de Capitales y Financiación del Terrorismo.

La comentada sentencia de la AP Asturias junto con el informe del Ministerio de Hacienda tiene como consecuencia la obligación para todas las empresas que compran y venden Bitcoins en España del cumplimiento de la Ley PBC/FT.

Como ya se ha explicado, la AP de Asturias clasifica la compraventa de Bitcoin como un producto de **riesgo** para los bancos en relación con la Ley PBC/FT puesto que se trata de contratación no presencial, propicia al anonimato y referente a una moneda virtual, sin autoridad central, difícilmente controlable. Por todo ello es susceptible de ser usada para el blanqueo de capitales y financiación del terrorismo.

Al entrar en la categoría de **riesgo**, los bancos se ven obligados a realizar una comprobación de la identidad de los intervinientes a través de lo documentos fehacientes reforzados del art. 11 y ss.

"*El art. 7.r de dicha ley es tajante cuando dice que si los bancos no pueden llevar a cabo de forma diligente esa comprobación, no establecerán relaciones de negocio ni ejecutarán operaciones o podrán fin a las mismas. Se trata de un mandato legal imperativo que se impone a la voluntad de las partes*"

Dadas las características del Bitcoin, resultará muy difícil que las empresas dedicadas a la compraventa de esta criptomoneda cumplan al pie de la letra las disposiciones legales a las que se refiere, por lo que no es descartable la necesidad de actualización de la Ley PBC/FT.

E) Regulación Internacional.

Las reacciones en el mundo ante esta innegable revolución son variadas:

- En **Alemania**, **Reino Unido** y **Finlandia** se está regulando de la misma forma que en España.

- En el **Estado de Nueva York** ya han entrado en vigor las polémicas "*bitlicencias*", una regulación recientemente promulgada relativa a obligaciones específicas de PBC/FT.

- **Japón**, **EEUU** y **China** planean promulgar conjuntamente la que sería la primera regulación internacional sobre Bitcoin relativa la Prevención de Blanqueo.

- En **Argentina, Zimbabwe** y **Venezuela** se ha declarado ilegal y se ha prohibido su uso.

- En **Australia** se ha declarado oficialmente que el Bitcoin y todas las criptomonedas tienen estatus jurídico de moneda a efectos fiscales.

El *Homeland Security and Governmental Affairs Committee* de USA ha redactado un informe sobre la regulación del Bitcoin en 40 países. Acceso al informe