FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES

Bitcoin y el cambio de divisa

Autor: Alfredo Iglesias Colino

Director: Fernando Hernández Sobrino

Madrid
Julio 2016

Alfredo
Iglesias
Colino

Bitcoin y el cambio de divisa

ABSTRACT

Bitcoin ha venido para quedarse y para revolucionar la industria financiera, entre otras, aunque no cumpliera su utópica misión. Si el propósito de crear la criptomoneda era prescindir de los intermediarios en las transacciones financiera, precisamente son ahora estos intermediarios e instituciones financieras quienes más contribuyen a su desarrollo, y posiblemente uno de los sectores que más se beneficiará de ello. A pesar de que al principio las miradas iban a la moneda, al tiempo se ha conocido que el verdadero valor para las empresas se encuentra en Blockchain, y no sólo por los nuevos productos y modelos de negocio que puedan surgir, sino por la potencialidad para reducir costes operativos de forma considerable. A lo largo de este trabajo se hará un recorrido por el desarrollo de esta tecnología, se explicará qué es, y cómo afectará a distintas industrias. Se hará especial hincapié en su incidencia en el sector financiero, y cómo va a permitir la transformación de las organizaciones hacia modelos mucho más eficientes.

ÍNDICE

INDICE FIGURAS

INDICE TABLAS

1. INTRODUCCIÓN

Una divisa es la moneda de curso legal en una región o estado, con un cierto valor y que se utiliza como medio de pago, a cambio de bienes y servicios.
Según el BCE, el dinero en cualquiera de sus formas tiene tres funciones: "es un medio de intercambio, es decir, un medio de pago con un valor en el que todo el mundo confía. Es una unidad de cuenta que permite expresar el precio de los bienes y servicios. Y es un depósito de valor. [https://www.ecb.europa.eu/explainers/tell-me-more/html/what_is_money.es.html].

1.1.- La era del dinero físico

Sin embargo, el camino hasta llegar a lo que hoy en día entendemos por dinero fue largo. Previo a la aparición de cualquier moneda, la economía se basaba en el trueque, que consistía en un intercambio directo de bienes o servicios por otros. Las limitaciones del trueque son evidentes, y pronto se manifestó la necesidad de un bien intermedio.

"En toda comunidad humana acaban apareciendo ciertos bienes que son más fácilmente intercambiables que otros, de forma que los individuos los demandan, no por su utilidad, sino por su especial capacidad para circular por el mercado, para servir de moneda de cambio" [Uran, 2012]

El dinero surge para sustituir el viejo sistema de trueque, con el fin de facilitar las transacciones. Pero no cualquier cosa vale como moneda de intercambio. El bien tiene que ser escaso, para que pueda tener valor, y además debe ser aceptado por los partícipes de la población o sociedad que lo usa.

Así, a lo largo de la historia, según las épocas y civilizaciones, se ha utilizado como dinero desde metales preciosos como el oro, la plata o el cobre, que tenían un valor y además eran escasos, hasta piedras preciosas, pasando por la sal y otras especias. Si primero se usaron metales en bruto, viruta o polvo, con el tiempo se acuñaron las primeras monedas. Las monedas tenían la importante virtud de tener igual forma, con lo que una moneda tenía una cantidad determinada de oro o plata, y con ello un valor fijo fácilmente intercambiable en el comercio.

Aquellas monedas de metales nobles tenían un valor intrínseco otorgado o respaldado por el peso del material del que estaban constituidas y su valor era proporcional a la cantidad de metal noble que contenían. Se acuñaron más tarde monedas de metales no nobles, cuyo valor estaba respaldado por cierta cantidad de oro y plata depositados en los bancos.

Surgen así los primeros billetes o papel moneda, que no eran sino vales de monedas reales (dinero real) depositadas en las entidades o bancos que emitían dichos vales. Estos billetes eran certificados que prometían la entrega de un valor en monedas de oro y plata al portador.

Con la quiebra del patrón oro en 1971, sistema que fijaba el valor de una unidad monetaria en términos de una cantidad de oro, la moneda pasa a no tener un respaldo en oro y por tanto un valor intrínseco, aunque conservó un valor legal, otorgado por las autoridades de gobierno. Así, en la economía moderna aparece la figura del dinero

fiduciario o dinero *fiat*, que no está respaldado por oro ni por un bien preciado almacenado en ningún sitio, y la escasez del mismo no proviene de su naturaleza sino que viene dada por el poder de las autoridades de gobierno. Este dinero existe por decreto e imposición de una ley de curso legal, y a día de hoy son los Bancos Centrales quienes llevan a cabo la labor de emitirlo y fijan la cantidad de dinero en circulación, de manera que tenga un valor estable. El único respaldo a la moneda es la confianza en la economía del país o grupo de países que empleen la moneda.

En palabras del propio BCE, "las economías modernas, incluida la zona del euro, se basan en el dinero fiduciario, que es la moneda declarada de curso legal y emitida por un banco central, pero que, a diferencia del dinero representativo, no puede convertirse, por ejemplo, en un peso fijo de oro. No tiene valor intrínseco —en principio, el papel utilizado para fabricar billetes carece de valor— y, sin embargo, se acepta a cambio de bienes y servicios porque los ciudadanos confían en que el banco central mantenga estable el valor de la moneda a lo largo del tiempo"`[https://www.ecb.europa.eu/explainers/tell-me-more/html/what_is_money.es.html].

1.2.- La era del dinero electrónico

Además, hoy en día la moneda actual también existe sin su representación física. Se trata del dinero digital, que no es más que un apunte electrónico que representa un valor monetario almacenado. Durante mucho tiempo, las tarjetas de débito y crédito han sido los actores dominantes en el entorno de los medios de pago en Internet. Tarjetas de crédito como VISA, American Express, MasterCard posibilitan el mayor grueso de las transacciones, y aunque a día de hoy siguen gozando de buena salud, el auge del comercio electrónico y las compras por internet ha hecho que les hayan surgido una serie de competidores (Figura 1). [Baur, 2015]

Competidores como PayPal, que es un medio de pago digital que originariamente surgió como facilitador de transacciones para el portal de comercio electrónico eBay, y que a día de hoy es uno de los principales agentes de pago para el *e-commerce*. [Baur, 2015] PayPal es un intermediario online de pagos en Internet, que a día de hoy cuenta casi con 290 millones de usuarios. En el ciberespacio, no siempre se puede confiar en el vendedor y PayPal se convirtió en un intermediario ideal, con un proceso de resolución de disputas. El comprador da su dinero a PayPal que luego lo transmite, por una tarifa, al proveedor para completar la transacción [Simser, 2015]

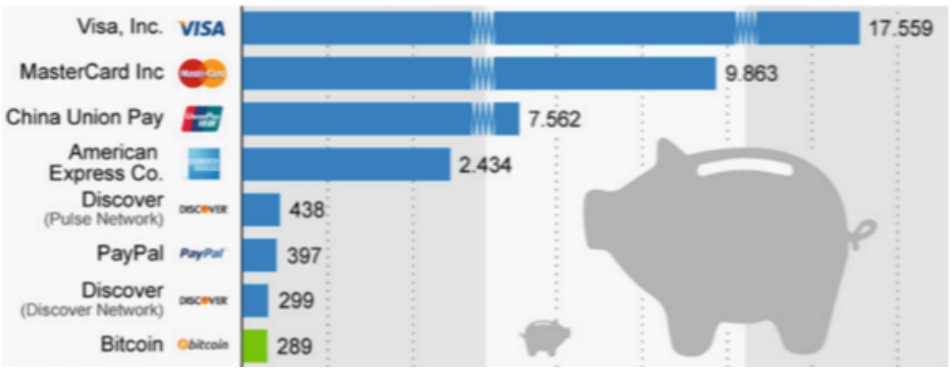

Figura 1.- Volumen diario de transacciones en millones de USD, a finales de 2013. Fuente [Baur, 2015]

1.3.- La irrupción del dinero digital

Y es que el comercio en Internet se basa casi exclusivamente en pagos realizados por medio de instituciones financieras que actúan como intermediario de confianza entre las partes que intervienen en la transacción. El establecimiento de esta confianza implica que el intermediario debe tener información relevante y suficiente sobre las partes. Otro inconveniente de este sistema es que no es posible realizar transacciones completamente irreversibles ya que las instituciones financieras no pueden evitar intermediar en las posibles disputas entre las partes. Además, la necesidad de un mediador en la transacción eleva el coste de la misma, lo que implica la necesidad de transferir una cantidad mínima para poder rentabilizar el proceso. [Nakamoto, 2008]

Llegados a este punto, parece evidente que el hecho de que las transacciones necesariamente tengan que pasar por las entidades financieras que actúan de intermediarias ya no las convierte en facilitadores del flujo de capital, sino más bien en un estorbo que lo ralentiza. En palabras de Nakamoto: "Lo que se necesita es una forma de pago electrónica basada en pruebas criptográficas y no en confianza, permitiendo de esta manera a dos partes que estén dispuestas a realizar transacciones entre ellos, que lo hagan directamente sin necesidad de un intermediario." [Nakamoto, 2008]

Sobre esta base, en el año 2009, un nuevo agente monetario irrumpe en la sociedad moderna: Bitcoin, una moneda criptográfica puramente virtual. La diferencia que presenta esta nueva moneda tiene que ver con su creación, que está basada en algoritmos criptográficos y recae en los usuarios del sistema, así como que no tiene ningún tipo de respaldo físico ni legal. Su principal característica es que es totalmente descentralizada pues no hay ninguna institución ni banco central detrás de ella.

Bitcoin comparte una serie de características propias del dinero *fiat* electrónico, que son condicionantes importantes para la validez del mismo. En primer lugar, la escasez, que permite mantener el nivel de la inflación. En segundo lugar, la seguridad; Bitcoin sigue los máximos patrones de seguridad utilizando claves privadas. Cuando una persona se registra en Bitcoin, recibe una clave privada asociada a un monedero, y cada transacción en la que intervenga quedará registrada en una base de datos pública, que se mantendrá siempre actualizada. Por último, la usabilidad y sencillez. Para un usuario o cliente, transferir Bitcoins es muy sencillo, sólo necesita un monedero, y realizar la transacción. Las transacciones se llevarán a cabo en breves minutos, independientemente de la distancia geográfica. [Baur, 2015]

La creación y desarrollo de bitcoin se basa en el sistema descentralizado blockchain, que ha supuesto una revolución en el modus operandi de las transacciones financieras a través de Internet. Además, este protocolo puede aplicarse a otros muchos ámbitos por lo que ha despertado el interés de bancos y entidades financieras así como de otras empresas de distintos sectores. Por ello, se están desarrollando sobre la base de blockchain nuevos protocolos que tratan de cubrir estas nuevas aplicaciones tecnológicas.
Por ello, los objetivos que se han planteado en el presente trabajo son:

- Realizar una revisión de la situación actual y aplicaciones del bitcoin y blockchain.
- Discutir la posible aplicación de este método al cambio de divisa entre particulares

2. METODOLOGÍA

Para la realización del trabajo se realizó una búsqueda bibliográfica. Puesto que blockchain se ha utilizado primordialmente para la moneda digital bitcoin, los términos principales de búsqueda fueron “bitcoin" y "blockchain+bitcoin.
Las bases de datos consultadas fueron Web of Science, EBSCO Business Source Complete, Accounting, Tax and Banking Collection (PROQUEST), Science Direct, Asian and European Business Collection y Google Scholar. Dado que el trabajo inicial de Bitcoin por Satoshi Nakamoto (Muy probablemente el pseudónimo de un grupo) se publicó en 2008, no se han limitado los años de búsqueda. Los resultados obtenidos se muestran en la tabla 1.
De hecho, hasta 2011 no comenzaron a publicarse trabajos de investigación en revistas sobre criptomonedas, en especial bitcoin. A partir de 2013, las revistas especializadas han comenzado a recibir y aceptar trabajos sobre estos temas más frecuentemente.
No obstante, en la búsqueda con las palabras clave blockchain y bitcoin en la base de datos Scopus desde el año 2013 al 2016, el tipo de documento más frecuente son las ponencias de conferencias. El número de publicaciones ha crecido desde el año 2013 y habrá que esperar hasta finales del presente año 2016 para confirmar la tendencia al alza. (Figura 2)

Base de datos	**Palabra Clave**	**Número de resultados**	**Año de la primera publicación**
Asian and European Business Collection (PROQUEST)	Bitcoin	712	2011
	Blockchain+Bitcoin	172	2013
Accounting, Tax and banking Collection (PROQUEST)	Bitcoin	3976	2011
	Blockchain+Bitcoin	481	2013
Ebsco Business Source Complete	Bitcoin	1873	2011
	Blockchain+Bitcoin	77	2014
Google Scholar	Bitcoin	678	2015
	Blockchain+Bitcoin	154	2015
Science Direct	Bitcoin	343	2011
	Blockchain+Bitcoin	49	2013
Scopus	Bitcoin	408	2012
	Blockchain+Bitcoin	50	2013
Web of Science	Bitcoin	215	2012
	Blockchain+Bitcoin	20	2013

Tabla 1.- Número de resultados obtenidos en las distintas bases de datos y año del primer documento reseñado.

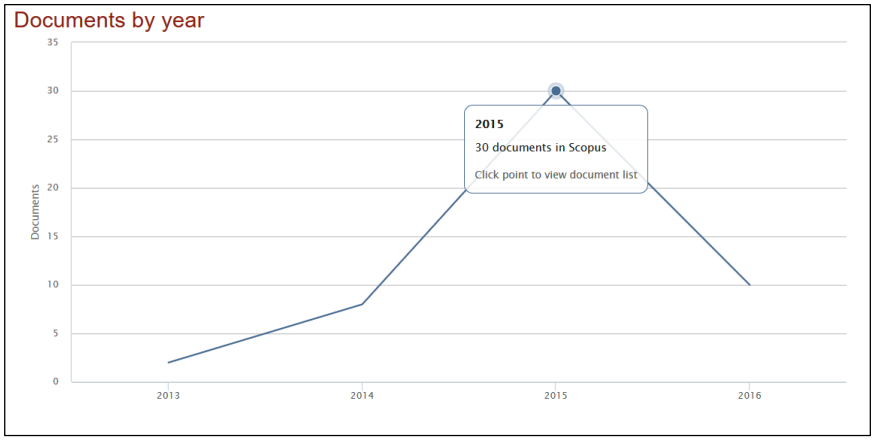

Figura 2.1- Número de documentos que incluyen las palabras clave "blockchain+bitcoin" en la base de datos SCOPUS desde 2013 a 2016

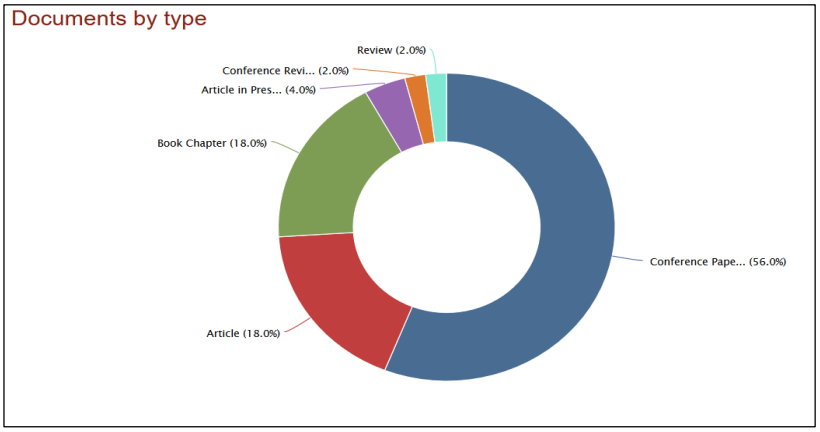

Figura 2.2- Tipo de documentos que incluyen las palabras clave "blockchain+bitcoin" en la base de datos SCOPUS desde 2013 a 2016.

3. DESARROLLO DE BITCOIN

3.1.- ¿Qué es Bitcoin?

Bitcoin es una moneda virtual o cripto-moneda, que en definitiva es una cadena de firmas digitales. En sí mismo, bitcoin no es nada. A diferencia del dinero electrónico almacenado en una cuenta corriente como lo que es, dinero, bitcoin no es atribuible a ningún tipo de activo almacenable o tangible. Simplemente es un código binario registrado en una base de datos de la que se hablará más adelante. Ésta base de datos es blockchain, y es un registro público de todas las transacciones que se llevan a cabo dentro de la propia red entre los distintos clientes de la misma. Cada vez que se procesa una transacción, el propio sistema actualiza todos los monederos con la cantidad de bitcoins que "hay" en cada uno.

Técnicamente, una criptomoneda es un activo intangible, una propiedad digital cuyo poseedor puede ser probado criptográficamente. [Back, 2014]

Para un usuario o cliente, podemos considerar que bitcoin no es más que una aplicación digital que le provee de un monedero bitcoin personal con un a clave, con el cual puede enviar y recibir monedas. Estas transferencias de monedas se hacen a través de un servicio descentralizado, pues no hay ningún agente que lo regule, y de forma anónima, ya que cada usuario tiene una clave, o varias claves si tiene varios monederos. Y no hay forma de relacionar un monedero a una persona física o persona jurídica. A pesar de ser anónimo es completamente transparente, pues blockchain funciona como una base de datos gigante donde quedan registrados los detalles de cada transacción, y que se actualiza a medida que las transacciones se suceden.

3.2.- Cómo se emiten los Bitcoins: Minería

Detrás de este sistema cuyo funcionamiento a priori parece sencillo, se encuentran los mineros, o clientes completos, quienes no sólo son los encargados de hacer posibles las transacciones y mantener la red usando hardware especializado, sino que además son ellos quienes introducen nuevos bitcoins a la red mediante el complejo y competitivo proceso de minería. [Hayes, 2016] Cualquiera puede ser cliente completo, solo tiene que descargarse el código de Blockchain.

Los mineros se encargan de realizar las pruebas de trabajo necesarias para prolongar la cadena de bloques hasta realizar la transacción. Para realizar esta actividad los mineros cuentan con dos incentivos, que es la manera en que la red les premia por sus servicios: bitcoins y comisiones.

Por un lado, los mineros recogen bitcoins procesando transacciones. En un principio cualquiera puede ser minero, aunque la realidad demuestra que son empresas que, como si de minas de oro se tratara, invierten gran cantidad de trabajo, esfuerzo y dinero en desenterrar los bitcoins. Se necesita un gran poder computacional para ello, proporcionado por hardware especializado, de manera que los mineros con más poder o mayor eficiencia, serán los que tengan más posibilidades de desenterrar las nuevas monedas. A este poder computacional a menudo la literatura se refiere como *hashpower, hashing power, mining effort* o simplemente *hashrate.* El poder

computacional se mide en *hashes* por segundo, donde un *hash* es una sola iteración del algoritmo criptográfico conocido como función *hash* [Hayes, 2016].

El protocolo está diseñado desde el momento de su implementación, de tal forma que:

- Los nuevos bitcoins (BTC) se desentierran a un ritmo fijo y conocido, desenterrándose los nuevos bloques en intervalos de aproximadamente 10 minutos.

- Además ese ritmo preestablecido lleva una velocidad decreciente; el número de bitcoins minados se reduce a la mitad cada cuatro años, a lo largo del tiempo. Los primeros bloques desenterraban 50BTC. A día de hoy 25BTC, y esta cifra seguirá reduciéndose a la mitad cada cuatro años aproximadamente. [Hayes, 2016]

- Y esto lo hará hasta alcanzar los 21 millones de bitcoins, máximo que habrá en circulación y momento en el que la emisión se detendrá. [Hayes, 2016; https://bitcoin.org/es/faq]

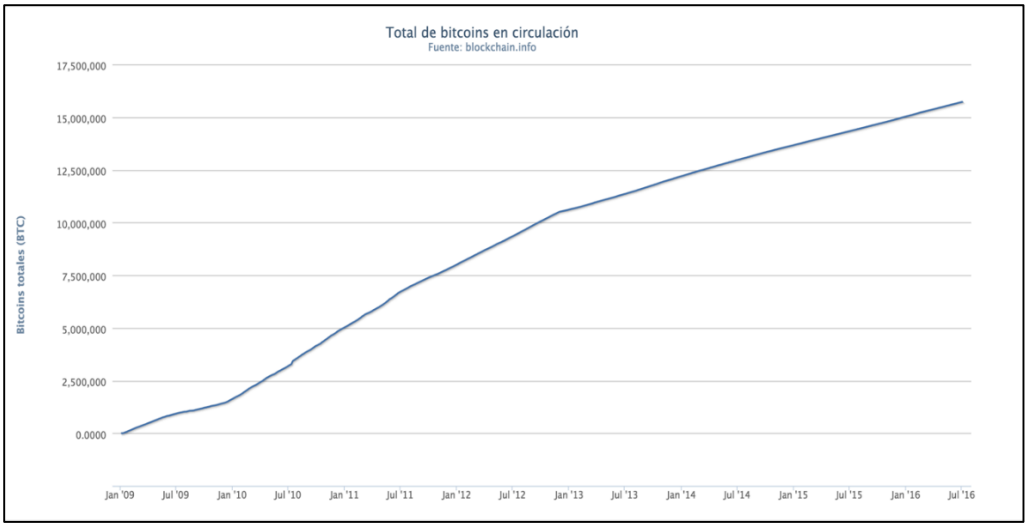

Figura 3.- Nº de bitcoins en circulación. 2009-Actualidad. Fuente: blockchain.info

Esto es así desde el momento en el que se implementó la moneda, y lo es siempre por consenso, ya que la única manera de cambiarlo sería consensuando una modificación en el protocolo con la cooperación de casi todos los usuarios, para lo cual habría que contar con un poder como mínimo mayor del 50% de las CPUs. [Nakamoto, 2008] Una organización poderosa podría invertir en hardware especializado de minado para así controlar la mitad del poder computacional de la red, y de esta manera poder bloquear o revertir transacciones. Sin embargo, no hay garantías de que pudieran mantener ese poder en el tiempo ya que requeriría invertir tanto o más que todos los mineros del mundo juntos. [http://www.coindesk.com/information/what-is-bitcoin/]

A pesar de que el límite establecido en la creación de la criptomoneda sea de 21 millones de BTC (bitcoins), debido a su naturaleza digital la moneda es divisible hasta las ocho cifras decimales. La cantidad divisible más pequeña es el 'satoshi' en honor al creador de bitcoin, que es 0,00000001 BTC, es decir, la cienmillonésima parte de un bitcoin. [http://www.coindesk.com/information/what-is-bitcoin/]

Por lo tanto, las unidades de bitcoin son: [https://en.bitcoin.it/wiki/Units]

Bitcoin	1 BTC
Deci-bitcoin	0.1 BTC
Centi-bitcoin	0.01 BTC
Milli-bitcoin	0.001 BTC
Micro-bitcoin	0.000001 BTC
Finney*	0.0000001 BTC
Satoshi	0.00000001 BTC

*El finney recibe su nombre en honor a Hal Finney, uno de los pioneros de bitcoin.

El hecho de que los bitcoins se desentierren a un ritmo preestablecido hace que la minería sea un negocio muy competitivo. Cuantos más mineros accedan a la red, más difícil será obtener beneficios desenterrando bitcoins de manera que los pools mineros deben buscar la eficiencia para reducir costes operativos.

De hecho, a medida que más bitcoins sean desenterrados, mayor será la dificultad de los problemas que tengan que resolver para facilitar las transacciones y desenterrar monedas. De manera que conforme aumenta la dificultad, más energía *hash* y esfuerzo deben invertir los mineros. Además el propio sistema auto-ajusta el grado de dificultad dependiendo de la capacidad computacional agregada a la red de manera que se mantengan estables en el tiempo los intervalos de 10 minutos de tiempo de confirmación que ya han sido mencionados y explicados con anterioridad. Así, cuanto mayor sea la capacidad computacional agregada a la red, mayor será la dificultad para desenterrar bitcoins y viceversa (Figura 4) [Hayes, 2016].

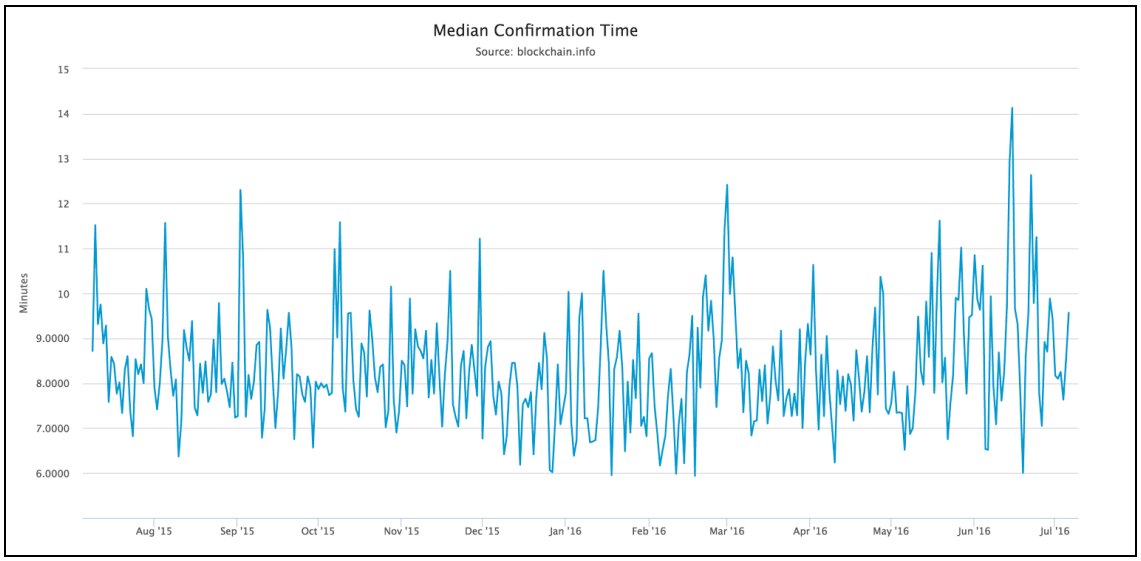

Figura 4.- Tiempo medio de confirmación. Fuente: https://blockchain.info/es/charts

Las gráficas que se muestran a continuación, miden la dificultad relativa de encontrar un nuevo bloque. Dificultad que se ha ajustado periódicamente en función de la energía hash desplegada mediante la red de mineros para desenterrar monedas. Es decir, a medida que se ha ido agregando (o quitando) capacidad computacional a la red, la dificultad ha aumentado (o disminuido).

La gráfica (Figura 5) muestra la evolución de la dificultad desde la primera emisión de bitcoins.

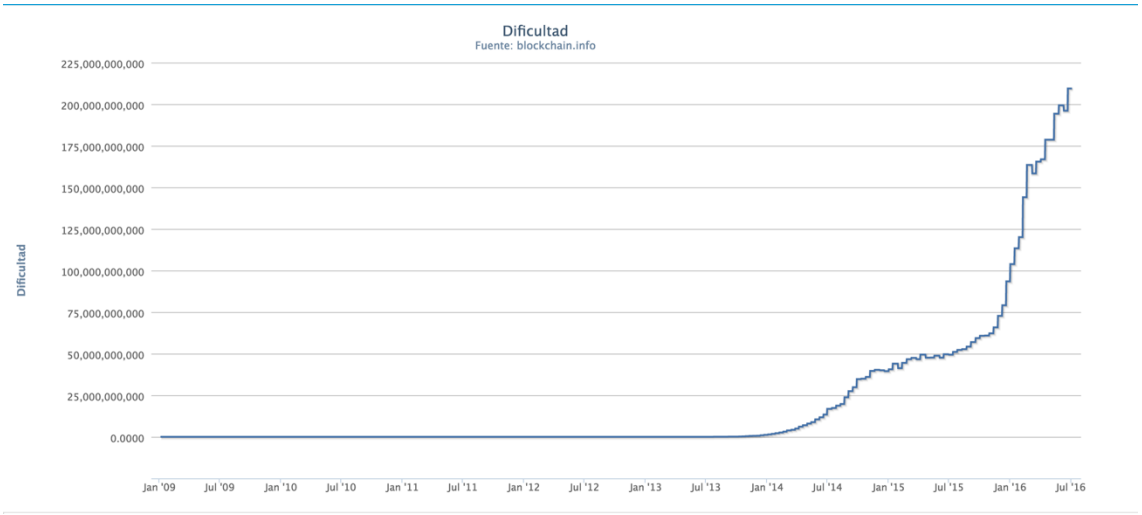

Figura 5.- Dificultad desde inicio bitcoin. Fuente: blockchain.info

Los mineros en su empresa de procesamiento de transacciones y obtención de monedas incurren en una serie de costes. La amortización del propio hardware especializado utilizado para procesar hasta la electricidad, son algunos de los costes asociados. Por eso es importante que el valor de los bitcoins obtenidos sean mayor que los costes [Houy, 2014] El valor de los BTC es el precio de cambio de los bitcoins con sus *trading pairs* fijado en las plataformas de cambio. Ejemplos de estas plataformas de cambio son: Coindesk [http://www.coindesk.com/price/], Bitstamp [https://www.bitstamp.net].

Así con todo, la minería parece ser un negocio rentable. Además de los bitcoins, los mineros también pueden ganar con las comisiones. De manera que el día que se alcancen los 21 millones de bitcoins, a pesar de no poder desenterrar más, el incentivo de las comisiones debe ser suficiente para que los mineros sigan asegurando el funcionamiento de la red blockchain. Para entonces, bitcoin contará con una cantidad de usuarios tal que las comisiones serán un negocio suficientemente atractivo. Y debe serlo. Debe ser rentable para que los mineros sigan invirtiendo dinero, tiempo y esfuerzo en mejorar su hardware y optimizar sus procesos, ya que cuanto mayor sea el poder computacional de estos, más seguro y robusto será el propio sistema [Houy, 2014]

De momento muchos mineros no cobran comisión, y se pueden hacer transacciones con coste cero. Algo que sin duda irá a menos a medida que sea menor la recompensa por minar bitcoins. [http://www.coindesk.com/information/how-do-bitcoin-transactions-work/]

4.- ¿CÓMO SURJE BITCOIN?

4.1.- La antesala a la creación de bitcoin: b-money

Bitcoin es la implementación del concepto de *'b-money'* o 'moneda criptográfica' descrito y propuesto por primera vez por Wei Dai, ingeniero computacional y *cypherpunk*, en una cadena de mails que se intercambiaba por aquel entonces con

colegas informáticos, allá por 1998. Este concepto de cripto-moneda sugería la creación de un sistema anónimo y distribuido de dinero electrónico *('anonymous, distributed electronic cash system')* que prescindiera de los agentes centrales del sistema financiero y de los tradicionales intermediarios en las transacciones.
Wie Dai declaró lo siguiente: "En una cripto – anarquía, el gobierno no se destruye de forma temporal sino que permanentemente esta prohibido y es innecesario" "Hasta ahora no está claro, incluso teóricamente, cómo podría funcionar tal comunidad . Una comunidad se define por la cooperación de sus participantes, y la cooperación eficiente requiere un medio de cambio (dinero) y una forma de hacer cumplir los contratos. Tradicionalmente, estos servicios han sido prestados por el gobierno o las instituciones patrocinadas por el gobierno, y sólo a entidades legales. En este artículo describo un protocolo por el que estos servicios pueden ser prestados a entidades no rastreables "[Wei Dai, "b-money" http://www.weidai.com/bmoney.txt, 1998].

Tradicionalmente, los gobiernos y autoridades centrales han sido las encargadas, o mejor dicho, han tenido el poder de crear el dinero. Y más desde que el dinero dejó de estar respaldado por oro. Así, la creación del dinero está supeditada a los intereses de unos organismos centrales. Frente a esto, lo que esta declaración viene a sugerir es un sistema en el que ningún ente central pueda tener el control, sino que dicho control resida en el conjunto de partícipes del sistema. De ahí que sea distribuido.

Además, el sistema es anónimo pues cada usuario tiene una clave de manera que las transacciones siempre se asocien a un monedero pero sin que exista de manera necesaria una forma de relacionar cada monedero con una persona física o jurídica.

Wei Dai en su mail propone dos protocolos para llevar a cabo la creación de esta moneda virtual. El primero el mismo autor lo da por imposible por impráctico, sin embargo, será el que impulse el segundo protocolo propuesto.

En el primer protocolo cada participante del sistema mantiene en una base de datos cuánto dinero pertenece a cada participante bajo su seudónimo, y cada vez que se realiza una transferencia se actualiza la base de datos. Cómo se actualiza es el tema de este protocolo.[Wei Dai "b-money]. Para esto debe existir acuerdo entre las partes. Y en este protocolo cualquier persona puede crear dinero resolviendo una serie de problemas computacionales.
El segundo protocolo difiere del primero en que en lugar de ser todos los usuarios los que intervienen en la actualización de la base de datos, sólo es un subconjunto de la población, a los que se refiere como servidores, los que tienen la tarea de aceptar las transacciones. Transacciones que deben después comunicar a todos los usuarios.

De alguna manera el sistema tiene que ser capaz de generar confianza, por lo que se requiere algún mecanismo que haga a los servidores comportarse de manera honesta, en beneficio de la red. Wei Dai propone una serie de posibles soluciones a estos requerimientos que pasaban por hacer depositar a cada usuario una cierta cantidad de dinero en una cuenta especial para ser utilizado como posibles multas o recompensas por conducta maliciosa. Además, cada servidor debería comprometerse a publicar periódicamente sus bases de datos actuales de creación de dinero y la propiedad del mismo. Cada participante debería verificar que sus propios saldos de cuentas son correctas y que la suma de los saldos de las cuentas no es mayor que la cantidad total de dinero creado. [Wei Dai, 1998]

Como primera toma de contacto con lo que será la moneda virtual está bien, sin embargo, el modelo dista mucho de ser perfecto. En cualquier caso, la intención del mail de Wei Dai no era otra que la de plantar la primera semilla, y que supusiera el punto de partida para el desarrollo del idealizado sistema. Según las propias palabras de su creador, "El protocolo propuesto en este artículo permite a entidades con seudónimos imposibles de rastrear cooperar entre ellas de manera más eficiente, proporcionándoles un medio de intercambio y una manera de hacer cumplir los contratos. El protocolo probablemente se pueda hacer mas eficiente y seguro, pero espero que esto sea un paso para hacer de la cripto-anarquía una posibilidad tanto práctica como teórica." [Wei Dai, "b-money", 1998]

Esta teoría es la base de la creación de bitcoin en los años posteriores. Para terminar de comprender la esencia del concepto tan rompedor que supone bitcoin me parecía relevante mencionar la figura del *cypherpunk* Wei Dai, y la historia de cómo aspiraba a un sistema monetario en que no fuera necesario el papel de un regulador central, sino que el propio conjunto de los usuarios lo regularan de acuerdo a sus intereses comunes.

4.2.- Protocolo Bitcoin

Siguiendo la línea marcada por la teoría cripto-anarquista y partiendo de la idea del 'b-money', Sathosi Nakamoto, propone crear el sistema Bitcoin, un sistema distribuido de pago, o lo que es lo mismo, un sistema consensuado y descentralizado, basado en el uso de monedas criptográficas, y que prescinde completamente de cualquier autoridad central tanto para la facilitación de las transacciones, como para la regulación del propio sistema y para la propia emisión de la moneda.

El artículo de Nakamoto en que publica por primera vez la idea de Bitcoin, resuelve los problemas que Wei Dai sugería, desde cómo abordar la creación de las moneda criptográfica, a cómo garantizar la confianza en el sistema. Por un lado resuelve cómo hacer las transacciones que generen confianza. La confianza la genera por un lado el propio sistema pues todas las transacciones se harán de forma pública, y quedarán registradas en una base de datos a la que todos los usuarios tengan acceso, y por otro lado la generan los propios usuarios que facilitan las transacciones al actuar de buena fe. Consigue que aquellos actúen de buena fe, al dotar al protocolo de un sistema de incentivo o compensación, a los usuarios encargados de posibilitar las transacciones, por operar de manera correcta. Estos incentivos precisamente son en forma de monedas que reciben al facilitar las transacciones. Con lo que queda así resuelto también el problema de la creación del dinero.

Las monedas se transfieren de un propietario a otro firmando digitalmente un *hash.* El problema de este método es que el beneficiario de la transacción no puede verificar que el propietario no haya gastado dos veces la misma moneda. "La única manera de confirmar la ausencia de una transacción es tener conocimiento de todas las transacciones" [Nakamoto, 2008] Por lo tanto, la solución posible para controlar el doble gasto pasa por que todas las transacciones sean públicas, y los participantes del sistema estén de acuerdo en el orden en que se han acontecido las distintas transacciones.

El primer paso de la transacción comienza por el sellado en el tiempo o *timestamp*, que registra públicamente todas las operaciones, probando y verificando su existencia en el tiempo antes de introducirla en el *hash.* Cada *timestamp* incluye el anterior en su *hash* formando una cadena, con cada sellado temporal reforzando los anteriores. [Nakamoto, 2008]

Para implementar un sistema distribuido con sellado temporal basado en el P2P, se necesita un sistema de pruebas de trabajo. Las pruebas de trabajo son los problemas que deben resolver los nodos, resolviendo los *hash.* Esta prueba de valor consiste en lo siguiente: para cada bloque se añade un *nonce*, que no es otra cosa que un número aleatorio utilizado en protocolo de autentificación, y que sólo se puede usar una vez. Este proceso se iterara hasta que se da con el *nonce* en satisfaga el valor hash buscado y que verifique el bloque. Es precisamente a este proceso iterativo hasta dar con el valor requerido para verificar un bloque al que nos referimos como prueba de trabajo.

Una vez que el esfuerzo computacional de la CPU consigue satisfacer una prueba de trabajo, el bloque ya no se puede modificar sin rehacer el trabajo. En cuanto nuevos bloques se unan en cadena a este, para modificar un bloque pasado habría que rehacer todos los bloques que le sigan. [Nakamoto, 2008] Esto dificulta sobremanera los ataques, haciendo casi imposible los ataques, hasta el punto de que cada bloque que se añade a la cadena disminuye de manera exponencial la probabilidad de que un ataque suceda. [Nakamoto, 2008]

La prueba de trabajo también resuelve el problema de la toma de decisiones basada en el acuerdo de la mayoría. Lo que tiene las pruebas de trabajo es que permiten por cada CPU un voto, y la decisión de la mayoría viene representada por la cadena más larga, que es la que tiene en la que se ha invertido más esfuerzo para resolver las pruebas de trabajo.

4.3.- ¿Qué es realmente Blockchain?

Quizá el verdadero valor del desarrollo de bitcoin no sea la moneda en sí misma, sino la cadena de bloques o *blockchain,* la red pública y distribuida que guarda los registros de cada transacción.

Una cadena de bloques, en inglés y comúnmente conocida por *blockchain,* es una serie ordenada de bloques, aceptada en consenso por todos los usuarios como veraz, de manera que determina computacionalmente la posesión de un activo y el cambio de manos del mismo, así como el orden cronológico en que suceden las transacciones. [Friedenbach, 2013]

Blockchain es "un libro contable descentralizado de transacciones a través de una red *peer-to-peer*". [http://www.pwc.com/us/en/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html)] Es "una base de datos distribuida que mantiene una lista cada vez mayor de registros de datos protegidos contra la manipulación y revisión de los propios operadores o nodos de la propia base de datos. De alguna manera es un libro de contabilidad pública de todas las transacciones que han sido ejecutadas" [Fanning, 2016] "Blockchain crece constantemente a medida que se añaden bloques

completos a los anteriores formando una cadena. Estos bloques se añaden en un orden lineal, cronológico" [Fanning, 2016].

Otra definición que dan Schatsky y Muraskin, es "un libro digital de contabilidad, de transacciones distribuidas, con copias idénticas que se mantienen en varios sistemas informáticos controlados por entidades diferentes. Cualquier persona participante en un blockchain puede revisar las entradas en el mismo; los usuarios pueden actualizar el blockchain únicamente por consenso de la mayoría de los participantes. Una vez que ha entrado en una blockchain, la información nunca puede ser borrada; idealmente, un blockchain contiene un registro preciso y capaz de verificación de cada transacción que se ha hecho." [Schatsky, 2016]

4.4.- ¿Cómo funciona la cadena de bloques?

Las nuevas transacciones se muestran a todos los nodos, de ahí, cada nodo registra distintas transacciones en un bloque. Después cada nodo trabaja para resolver la prueba de trabajo de su bloque. Cuando por fin un nodo resuelve una prueba de trabajo y encuentra el valor hash para dicho bloque, comparte el bloque con el resto de los nodos. [Nakamoto, 2008]

Ahora todos los nodos deben aceptar el bloque como válido, cosa que ocurrirá si todas las transacciones del bloque son válidas y no hay doble gasto. Una vez un nodo ha aceptado un bloque, se pone manos a la obra en crear el siguiente bloque de la cadena, usando el hash del bloque aceptado como el hash previo del nuevo bloque (Figura 6). [Nakamoto, 2008]

Además blockchain propone un sistema de incentivos con el que da respuesta por partida doble al tema de la creación del dinero y la generación de confianza en el sistema.

Por un lado, la primera transacción de cada bloque tiene de especial que desentierra una serie de monedas, que pasan a ser propiedad del creador del bloque. Este es un gran incentivo para que los nodos, den soporte a la red y faciliten las transacciones, y es la manera de poner nuevas monedas en circulación [Nakamoto, 2008]. El incentivo también puede ser en forma de comisiones transaccionales.

Por otro lado, para la generación de confianza y que los nodos actúen de forma honesta, confía en los incentivos. Tiene sentido pensar que los nodos actuarán de buena fe, ya que les es más rentable actuar de acuerdo a unas normas que precisamente les hacen ganar dinero a ellos. Lo que no sería comprensible es que los nodos atacaran al sistema, pues estarían destruyendo el valor de la moneda, y con ello su propia riqueza.

Si en un primer momento es Nakamoto el primer impulsor de bitcoin, en 2008 con la publicación de su mítico trabajo, y en el año 2009 con la primera emisión de Bitcoins (BTC), al cabo de poco tiempo Satoshi, cuya identidad a día de hoy sigue siendo desconocida[1], decide desvincularse por completo del proyecto; concretamente en 2011.

[1] La identidad de Satoshi Nakamoto permanece desconocida día de hoy. No se sabe si Satoshi Nakamoto es el alias de una persona física, de un grupo de personas, o incluso

[BBVA Innovation Center, FinTech Serie por Innovation Edge, 2016] Para entonces bitcoin ya era una realidad que había atraído la atención de diversas personalidades, desde programadores a ingenieros, pasando por expertos en métodos de pago. Un elenco de talentos que impulsaron el carro del sistema de pago *peer-to-peer* y lo desarrollaron, optimizando las distintas limitaciones de la propuesta inicial de Satoshi Nakamoto, hasta el sistema abierto que es hoy en día. Además, se han desarrollado otros usos para Blockchain aprovechando las muchas posibilidades que ofrece y que más adelante se mencionaran.

---

de una empresa. La única manera en que se comunicaba con el mundo era por medio de emails. Mucho se ha investigado acerca de su identidad, para no llegar a nada. La primera semana de mayo de 2016, un australiano de nombre Craig Steven Wright aseguraba que él era Satoshi Nakamoto. Y sus argumentos parecieron convencer a dos voces autorizadas dentro del mundo de Bitcoin. Gavin Andersen, uno de los principales desarrolladores del software que da soporte a Bitcoin se mostraba bastante convencido de que era cierto, mientras que Jon Matonis, uno de los fundadores de la Bitcoin Foundation afirmaba que las pruebas eran concluyentes, después de que ambos conocieran al Sr Wright en persona [Cookson, FInantial Times, 2 mayo 2016. Aseguró que tenía pruebas que haría públicas y que convencerían al mundo de que es el creador de Bitcoin. Sin embargo, finalmente se retractaba de su decisión de hacer públicas sus claves [Bitcoin backtrack, Fast Financial Times, 5 mayo 2016]. No confirmaba su identidad, pero tampoco la desmentía, dejando así la duda en el aire, y el debate sobre la mesa.

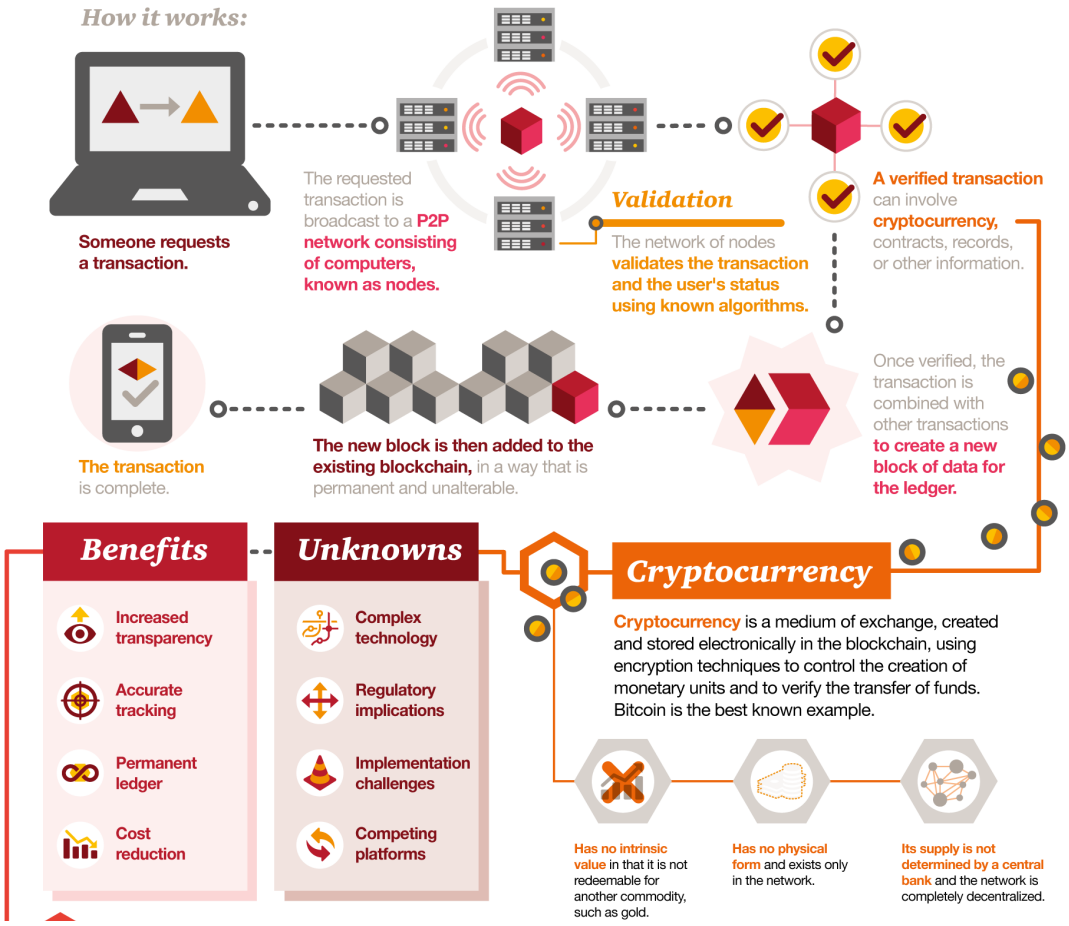

Figura 6.- Esquema de funcionamiento de blochain. Fuente: http://www.pwc.com/us/en/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html

5.- BITCOIN 2.0

Desde la disrupción de Bitcoin en el mercado, el interés suscitado por las criptomonedas ha sido cada vez mayor. Este interés se traduce en cada vez más expertos volcados en el desarrollo de la tecnología y su aplicación a múltiples propósitos, financiados tanto por bancos, instituciones financieras e incluso inversores privados, lo que que está llevando a importantes avances.

Si en un principio blockchain se pensó para hacer transferencias (en bitcoins), al poco tiempo se vería que esto era insuficiente, pues la cadena de bloques invitaba a aumentar el espectro de productos y datos que podía almacenar y transferir. Uno de los avances más significativos, y que guarda relación con el objetivo de este trabajo, son la aparición de estructuras financieras complejas no monetarias.

Así, han surgido un abanico de productos transferibles o mejor dicho, registrables en blockchain que no son monedas. Algunos de estos son dividend-yield bonds, los tokens o fichas de propiedad de un activo o archivo, una gran variedad de contratos inteligentes, y por supuesto, plataformas y mercados distribuidos donde poder intercambiar todo lo anteriormente citado. [Friedenbach, 2013]

Si bien es cierto que cada vez se va entendiendo más el funcionamiento del sistema descentralizado, y las muchas posibilidades que ofrece, el complejo sistema de consenso hace que no sea precisamente fácil adaptar el protocolo a las nuevas necesidades que van surgiendo,. Esto se debe a que las normas que rigen el sistema se definen en su creación, y la única manera de cambiarlas es con el consenso de todos los participantes. Además no sólo es difícil por eso; en caso de ponerse de acuerdo, todos los participantes deberían implementar los cambios exactamente de la misma forma. [Friedenbach, 2013]

El objetivo de Bitcoin era relativamente simple: una cadena de bloques que permitiera la transferencia de un solo activo digital, que era el bitcoin, y que en cualquier caso la finalidad no era que fuera canjeable por cualquier cosa. [Friedenbach, 2013] Limitar su aplicación a un uso tan especifico permitió en su momento simplificaciones en la aplicación. Pero las nuevas demandas que surgían del mundo real desafiaban continuamente esas simplificaciones.

De ahí que la innovación haya centrado en aspectos determinados, y corregir ciertas limitaciones del propio sistema de cara a la expansión de su uso para otros fines.

Algunas de estas limitaciones y problemas que han surgido son, entre otros:

1. El conflicto de la descentralización y la escalabilidad. Un mayor tamaño de los bloques haría posible que la red aumentara la tasa de transacciones. Pero redes más grandes implicarían más trabajo para los mineros que hacen posible las transacciones, lo cual supone un riesgo de centralizar el poder pues se aumentaría la dependencia en los actuales pools mineros. Algo que como ya sabemos va contra la propia naturaleza de bitcoin. [Back, 2014]

2. Han surgido otro tipo de activos financieros además de divisas, que se pueden intercambiar a través de blockchain, como los IOUs, contratos a futuros, SWAPS, y otros tipos de contratos. [Friedenbach, 2013]

3. Y no sólo eso, además el desarrollo de nuevas tecnología constantemente sugiere, propone y permite el uso de las propiedades de Blockchain para nuevas aplicaciones, de diversos tipos de industrias, ni imaginadas en el momento inicial en que se desarrolló Bitcoin. [Friedenbach, 2013]

5.1.- *Pegged Sidechains* o Cadenas Laterales Vinculadas

De acuerdo con los anteriores puntos mencionados, la primera solución a estas limitaciones fue la creación de cadenas de bloques alternativas, o *altchains*, que comparten los principios del mismo código con Bitcoin, del cual difieren en modificaciones de partes puntuales, de manera que esas variaciones parciales iban a permitir la correción de limitaciones concretas del Blockchain original para dar distintas respuestas a las nuevas necesidades o funcionalidades requeridas del sistema.

Cabe y es preciso mencionar que cualquiera puede crear una criptomoneda. Obviamente, cualquiera con los suficientes conocimientos informáticos, puede crear una criptomoneda. Bitcoin es un código libre al que todos tenemos acceso, por lo que sería

relativamente fácil crear una moneda alternativa basándose en el código de la original. De hecho así ha sucedido; desde la aparición de Bitcoin se han sucedido la aparición de distintas monedas virtuales alternativas.

Casi todas ellas se desarrollan a partir de la cadena de bloques de Bitcoin, y tratan de abordar algunas de las deficiencias de la propia Bitcoin o, por el contrario, aprovechar las virtudes de la cadena de bloque para otros fines. Por ejemplo, Namecoin lo que permite es la posibilidad de almacenar datos dentro de la Blockchain de Bitcoin con el fin de realizar un registro de información de dominio público descentralizado. Otras como Litecoin se diferencian de Bitcoin principalmente en tener un tiempo de generación de bloques más pequeño, además de tener más *coinbases,* que son plataformas de compra-venta de criptomonedas. [Schwartz, 2014]

Sin embargo, esta solución de crear cadenas de bloques alternativas con sus propias criptomonedas tiene dos inconvenientes. El primero es obvio y es la fragmentación de la infraestructura del propio sistema. "El segundo problema es que dichas *altchains* o cadenas alternativas normalmente tienen su propia criptomoneda o *altcoin*, con un precio flotante. Para acceder a dichas *altchains* los usuarios deben utilizar esta moneda, la cual deben conseguir en mercados como los mencionados en el anterior capitulo, y de alguna manera quedan expuestos a un alto riesgo debido a la volatilidad asociada a las nuevas monedas." [Friedenbach, 2013]

Una propuesta que considero merecedora de mención es la de las *Pegged Sidechains* o cadenas laretales vinculadas. Una nueva tecnología, que da otro paso en el desarrollo de Blockchain, basada en la vinculación de distintas cadenas, que básicamente permite transferir bitcoins y otros activos entre múltiples blockchains. Este avance ofrece a los usuarios el acceso a nuevos e innovadores sistemas de criptomoneda utilizando los activos que ya poseen. Usando y aprovechando la propia tecnología de Bitcoin, estos sistemas permiten interactuar más fácilmente con los demás y con Bitcoin, evitando los problemas de liquidez y las fluctuaciones del mercado asociados a las nuevas monedas. [Friedenbach, 2013]

Ya se ha mencionado con anterioridad en este trabajo la separación de "Bitcoin" la cadena de bloque (Blockchain) de "Bitcoin" la moneda. De la misma manera aplicable a las distintas *altchains* y sus respectivas *altcoins*. Pues bien, el desarrollo de las cadenas laterales vinculadas es precisamente lo que permite es el movimiento de los distintos activos entre las distintas cadenas. "El concepto de *cadena lateral (sidechain)* no es otra cosa que una cadena de bloque que valida datos de otras cadenas de bloques." [Friedenbach, 2013]

A continuación se muestra una tabla con las principales criptomonedas (tabla 2). En dicha tabla sólo he querido mostrar un Top 20 de monedas por *market cap* pero en el siguiente enlace se accede a la lista completa de las muchísimas alternativas a Bitcoin: http://coinmarketcap.com/currencies/views/all/

#	Name	Symbol	Market Cap	Price	Available Supply	Volume (24h)
1	Bitcoin	BTC	$ 10,693,843,884	$ 679.94	15,727,675	$ 122,762,000
2	Ethereum	ETH	$ 975,931,566	$ 11.96	81,620,785	$ 10,396,700
3	Ripple	XRP	$ 234,948,210	$ 0.006647	35,345,971,933 *	$ 466,404
4	Litecoin	LTC	$ 203,838,585	$ 4.38	46,495,179	$ 8,699,550
5	NEM	XEM	$ 94,390,200	$ 0.010488	8,999,999,999 *	$ 939,532
6	Dash	DASH	$ 47,302,765	$ 7.21	6,561,299	$ 302,341
7	Lisk	LSK	$ 30,908,000	$ 0.309080	100,000,000 *	$ 462,198
8	Dogecoin	DOGE	$ 29,774,352	$ 0.000284	105,016,389,699	$ 379,049
9	Monero	XMR	$ 21,423,871	$ 1.74	12,305,497	$ 240,223
10	Nxt	NXT	$ 21,007,072	$ 0.021028	998,999,999 *	$ 869,873
11	Waves	WAVES	$ 17,368,300	$ 0.173683	100,000,000 *	$ 293,976
12	Steem	STEEM	$ 14,659,388	$ 0.204864	71,556,680	$ 9,718
13	Factom	FCT	$ 12,855,152	$ 1.47	8,753,219 *	$ 695,634
14	Emercoin	EMC	$ 12,645,704	$ 0.332282	38,057,145	$ 83,070
15	Siacoin	SC	$ 12,558,014	$ 0.000794	15,807,259,104	$ 320,828
16	BitShares	BTS	$ 11,710,464	$ 0.004566	2,564,940,000 *	$ 297,218
17	Stellar	XLM	$ 10,761,258	$ 0.001962	5,485,679,598 *	$ 49,514
18	Peercoin	PPC	$ 9,624,236	$ 0.413352	23,283,392	$ 53,280
19	Bytecoin	BCN	$ 7,305,455	$ 0.000040	180,717,599,092	$ 2,097
20	Counterparty	XCP	$ 6,945,755	$ 2.64	2,626,302 *	$ 34,211

Tabla 2. Top 20 criptomonedas en el mercado de US en $. Fuente: http://coinmarketcap.com/currencies/views/all/ (15 Junio de 2016)

Se observa que Bitcoin se mantiene como la principal moneda pues es con diferencia la que más valor de mercado tiene, con una capitalización de 10 billones de dólares.

Es interesante conocer las distintas alternativas pues cada una tiene una fortaleza concreta. Algunos de los algoritmos de las *altcoins* tienen más robustez que otros, otros sin embargo son mucho más rápidos a la hora de validar transacciones. Por ejemplo, como ya se ha mencionado antes, Litecoin es más rápido, concretamente hasta cuatro veces más rápido que las transacciones con Bitcoin, lo que le hace la alternativa idónea para aplicaciones donde la velocidad sea fundamental, como en el trading. [Baur, 2015]

En cualquier caso, cualquier protocolo alternativo debe cumplir una serie de características, y en Ripple Labs definen una serie de axiomas a propósito de los cuales se evaluará la fortaleza del algoritmo de consenso de los distintos protocolos de cadenas de bloques. Estas tres características o axiomas son los siguientes [Schwartz, 2014]:

1. En primer lugar, tiene que ser **correcto**: esto significa que tiene que ser capaz de diferenciar las transacciones correctas de las fraudulentas.

   Cualquier protocolo tiene que ser capaz de sobreponerse al 'Problema de los Generales Bizantinos'. Este problema consiste en que un grupo de generales, cada uno a cargo de una armada, deben coordinar un ataque comunicándose entre ellos a través de mensajeros. Debido a que las armadas se encuentran en un territorio hostil, que además no conocen bien, es posible que algunos mensajeros no lleguen. Aparte de esto, algunos generales pueden ser traidores y estar conspirando o bien de manera individual o bien de manera conjunta. En cualquier caso los mensajes que lleguen de estos generales traidores estarán corrompidos y tratarán de sugerir un plan que condene al fracaso la intención de los generales honestos. De igual manera, en la cadena de bloque puede pasar que nodos fallen, o que manden mensajes erróneos, así como que haya nodos maliciosos que traten de convencer al sistema para que acepten transacciones fraudulentas. [Schwartz, 2014]

   La robustez de un algoritmo se mide por la cantidad de procesos erróneos que puede tolerar en una red con un numero determinada de nodos, y aun así alcanzar consenso.

2. En segundo lugar, ha de haber **acuerdo**: Tiene que haber un acuerdo entre los nodos o las partes en que una transacción es válida y no fraudulenta. Esto debe ser así para evitar que pueda producirse el doble gasto: utilizar una misma moneda para dos transacciones.

   El doble gasto consiste en que un usuario malicioso de la red puede crear dos transacciones correctas separadas la una de la otra, de manera que realice simultáneamente dos compras para las cuales tiene fondos para cubrir individualmente, pero no para las dos juntas. A este problema la literatura se refiere como "problema del doble gasto" y el algoritmo de consenso debe ser capaz de identificarlo.

3. Finalmente, está la **utilidad**, lo que básicamente se traduce en que el proceso realmente sea practicable, sencillo y ágil. De nada sirve un algoritmo que garantice los primeros dos, si para ello va a necesitar un año para realizar la transacción, o en su defecto que consuma excesiva capacidad computacional.

Estas tres propiedades o axiomas, cuando se dan a la vez y así han de hacerlo, ratifican el concepto de **consenso**; que es el estado alcanzado por los nodos de la red en el cual aceptan una transacción. [Schwartz, 2014]

Generalidades aparte, hay otra moneda que merece una mención especial a la que más adelante dedicaré un epígrafe, y es el XPR de Ripple.

5.2.- Ripple: Una alternativa seria a Bitcoin

Como ya se ha comentado en el anterior punto, la creación de Bitcoin da el pistoletazo de salida para que surjan multitud de criptomonedas. Si hasta ahora nos hemos referido a Bitcoin exclusivamente, además de por ser la primera en surgir, la más importante por uso, capitalización y ser la mas conocida, también lo es porque entendiendo el principio que rige Bitcoin se entiende el del casi todas las criptomonedas restantes.

Sin embargo, en este apartado haré un breve inciso para presentar otra criptomoneda que está cobrando un papel muy relevante y que se ha desarrollado más bien de forma paralela a Bitcoin. Además, considero oportuna la mención a ésta precisamente por ser la empresa detrás de ella una de las que más inversiones está recibiendo del sistema bancario.

Concretamente me refiero al Ripple, de símbolo XRP. Esta moneda ha sido creada por la empresa privada Ripple Lab Inc, que desde hace unos años se dedica a desarrollar software y tecnología basada en el concepto de blockchain, aunque dista de ser el mismo modelo. El Ripple difiere de Bitcoin en dos aspectos fundamentales que a continuación expongo.

-. Así como Bitcoin se basaba en un código abierto y una cadena de bloques a la que todos los usuarios de internet tienen acceso y en la que todos participan y comparten el poder. Ripple también es de código abierto, sin embargo es un sistema de cadenas de bloque "privado" pues su despliegue depende únicamente de Ripple Labs. [Schwartz, 2014]

-. En segundo lugar, la forma en que se emite la moneda es completamente distinta. Recordemos que las monedas Bitcoins se desenterraban en un proceso de minería que dependía del trabajo de los mineros, que con sus capacidad computacional para posibilitaban las transacciones y con ello desenterraban nuevas monedas, las cuales se emitían a un ritmo preestablecido y fijo. Pues bien, los XRP o Ripples se crearon todos de una vez, y fueron concretamente 100 billones de unidades de XRP, de los cuales los fundadores de Ripple conservan un 20%, la empresa Ripple Lab Inc un 25%, y el otro 55% están en el mercado. [Schwartz, 2014]

Frente al sistema de aceptación de transacciones mediante pruebas de trabajo en el que se basa el proceso de Blockchain, Ripple propone un nuevo protocolo de consenso, basado en un algoritmo de consenso del protocolo de Ripple, RPCA por sus siglas en inglés.

Además, en Ripple los usuarios que facilitan las transacciones son principalmente los usuarios de Ripple Labs [Armsknecht, 2015], por lo que estamos hablando de un sistema ciertamente centralizado. El hecho de que ellos controlen casi la mitad de las monedas existentes, les permite no sólo controlar la liquidez del mercado, sino que posibilita el funcionamiento de la cadena de Ripple y la última implementación, Ripple Interledger. [Schwartz, 2014]

La idea de Ripple Interledger es básicamente la misma de las cadenas laterales vinculadas, con las salvedad de que en este caso son los propios miembros de Ripple

Lab los que actúan de intermediarios y facilitan las transacciones en esa cadena lateral que hace de puente entre distintas cadenas.

Si hay una tecnología que ha tomado la delantera en la carrera por ser adoptada por los grandes bancos para las transacciones transfronterizas esa es sin lugar a dudas Ripple, [Fanning, 2016] con su tecnología Interledger.

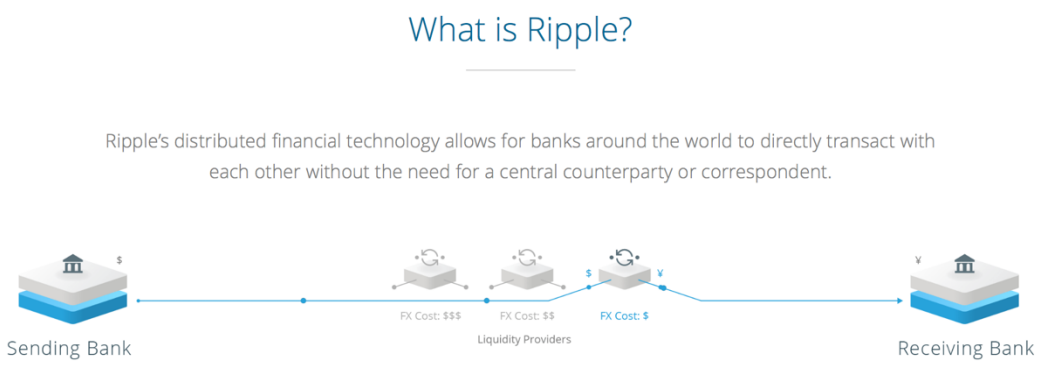

Figura 7. Esquema transferencia Ripple. Fuente: https://ripple.com

Las transferencias transfronterizas a través de este sistema son tan fáciles para el usuario como que uno emite la orden de transferencia en una moneda, y Ripple se encarga de realizar el cambio de divisa. Una de las particularidades de Ripple es que la empresa que lo impulsa es propietaria del 25% de las monedas, y los fundadores de otro 20%. Con esto son capaces de proveer de liquidez al sistema.

No sólo ha visto cómo grandes bancos como el Santander, a través de su fondo de VC Santander InnoVentures, ha invertido de 4 millones de euros, sino que además cuenta con algunos de los principales bancos en su cartera de clientes deseosos de beneficiarse de la gran fortaleza de este sistema, que son las transferencias transfronterizas.

5.2.a.- Principales diferencias entre Bitcoin y Ripple

La principal diferencia entre estos dos modelos, como ya se ha expuesto, es que mientras Bitcoin es un sistema completamente descentralizado en el que las transacciones se aprueban entre todos los bloques mediante las pruebas de trabajo, en el caso de Ripple se puede hablar de un sistema de cierta manera centralizado, en el que los trabajadores de Ripple Labs serían los que validan las transacciones.

Sin embargo, las diferencias no quedan ahí. A continuación un breve recorrido por las dos opciones a propósito de:

- Seguridad:

Para empezar, el protocolo de Bitcoin se ha estudiado hasta la fecha mucho más que Ripple, y por tanto hay mucho más entendimiento sobre el mismo.

Si en Bitcoin la seguridad de las transacciones que son aceptadas se consigue en base a pruebas de trabajo donde cada voto estaba ligado con la CPU de cada minero y el poder computacional, en Ripple el voto depende de los servidores validadores. [Armknecht, 2015]

Estos servidores validadores aparecen en una lista, entre los cuales el usuario puede elegir quienes quiere que sean por defecto sus validadores de confianza. Y la inmensa mayoría de ellos, son miembros de la empresa Ripple Labs.

En Bitcoin una vez que una transacción ha sido aprobada es imposible modificarla. No así en Ripple, donde, si en un momento dado la mayoría de los servidores se convierten en maliciosos, pueden reescribir completamente el historial de transacciones. Afortunadamente, prácticamente todos los servidores de Ripple, como ya se ha dicho, son de la propia Ripple Labs.

- Pagos

En Bitcoin los pagos se confirman de media cada 10 minutos, como se vio en el epígrafe que explica el proceso de minería, por medio de las pruebas de trabajo que desenterraban los nuevos bloques.

Ripple permite pagos mucho más rápidos, verificando las transacciones en cuestión de segundos.

- Privacidad y anonimato

Ambos son sistemas de pago donde los registros de todas las transacciones que se llevan a cabo son públicos. El anonimato se mantiene con seudónimos, de manera que si se quiere no se relacionen los monederos con la identidad del propietario.

Por supuesto los usuarios pueden tener diversos monederos, con distintas claves o seudónimos, para que no se sepa el total de su balance personal. En el caso de Bitcoin, una transferencia puede tener distintos inputs, es decir, lo transferido puede provenir de distintas cuentas. En Ripple, generalmente, los pagos tienen una sola cuenta como input. [Armknecht, 2015]

- Gestión de los clientes, actualización del protocolo y mantenimiento

Tanto Ripple como Bitcoin son códigos abiertos, lo que permite a cualquier ente o entidad descargarlo y desarrollar sus propios softwares, que puedan interrelacionarse con el original. Los clientes oficiales de Bitcoin los mantiene y actualiza regularmente la Bitcoin Foundation. En el caso de Tipple, quien haría esto es Ripple Labs. [Armknecht, 2015]

Todos los cambios en el protocolo de Bitcoin se discuten de forma pública en foros online, donde todos los usuarios desarrolladores argumentan y votan. En otras palabras, los cambios se consensuan entre toda la comunidad. Este proceso es mucho menos transparente en el caso de Ripple. [Armknecht, 2015]

- Descentralización

Mientras que sendos sistemas son descentralizados y ese es el propósito de las criptomonedas, la realidad de cierta manera dista de ser así. Puesto que en Bitcoin no son tantos las entidades o pool mineros que llevan a cabo la verificación de las transacciones y controlan la seguridad del sistema. De la misma manera Ripple es un sistema centralizado de cierta manera, y con más razón que Bitcoin, ya que la mayoría de los servidores de verificación dependen de Ripple Labs. Y además, en el caso de Ripple tanto la empresa como los fundadores de la misma mantienen la propiedad de una gran parte de los XRPs, la moneda de Ripple. Con lo cual, verdaderamente Ripple Labs puede controlar la economía de Ripple. [Armknecht, 2015]

6.- APLICACIONES DE BLOCKCHAIN

Blockchain, la tecnología detrás de Bitcoin, se ha convertido en uno de los mayores focos de interés de la industria financiera, y de otros tantos sectores. Blockchain ofrece una nueva forma de registrar tanto transacciones como otras interacciones digitales de manera segura y transparente, resistente a caídas del sistema, auditable y eficiente [Schatsky, 2015]. Como tal, su potencial transformador para revolucionar industrias como la financiera, mejorar practicas como la contabilidad y auditoría, y desde luego posibilitando nuevos productos, servicios y modelos de negocio. La innovación tan disruptiva que supone esta tecnología cambiará para siempre la sociedad, desde la forma de operar en múltiples sectores, como el financiero, hasta la manera de hacer cosas tan triviales como votar en unas elecciones. Y es que las ya conocidas virtudes, son aplicables a otras muchas industrias.

Recordemos que Blockchain, es una gran base de datos, un libro de registros, donde se guarda un registro público y actualizado del contenido de los distintos monederos de los usuarios. Que en verdad Bitcoin la moneda no es nada que se almacene, sino que es un activo intangible que se reduce a un código binario, y muestra el estado de un determinado monedero de la cadena de bloque.

Las grandes ventajas de utilizar Blockchain se podrían resumir en las siguientes: [Schatsky, 2016]

- Es global, y fácilmente accesible para todo el aquel que tenga acceso a un dispositivo móvil con internet. De hecho va a permitir llevar la banca a mucha gente sin acceso a los bancos.
- Confianza y transparencia; pues todos los registros de la base de datos distribuida al ser de dominio público y estar en constante actualización, lo que posibilita la creación de libros de cuentas fácilmente auditables.
- Las transacciones son irreversibles. Con lo que se evitan las posibles disputas entre contrapartidas.
- El sistema es totalmente descentralizado, y no son necesarias las labores de intermediación entre partes, lo que simplifica los procesos de validación de middle y back-office. Y por consiguiente, reduciendo costes. Además, las transacciones son más rápidas.
- Es un sistema robusto, con un sistema de incentivos para que los usuarios que lo hacen posible, lo sigan haciendo. Además, por ser descentralizado si un servidor

falla, el sistema se apoya en los otros muchos servidores que se mantienen operativos.

- La seguridad del sistema es máxima, basada en algoritmos capaces de detectar las transacciones fraudulentas.

Por blockchain se transfieren bitcoins, que no dejan de ser datos. Si se entiende que la funcionalidad de Blockchain es la guarda un registro de datos público, ésta misma funcionalidad es aplicable a cualquier dato del que se quiera guardar un registro público con un código, quiera ser públicamente rastreable, auditable y conocido en cualquier momento.

Por lo tanto el futuro de Blockchain pasa por traspasar las fronteras de los métodos de pago y lo meramente financiero, para aplicarse en distintos sectores e industrias. Cada vez surgen nuevas líneas de investigación, y parece que sólo la imaginación podrá decir dónde está el límite.

En este apartado haremos una pequeña mención al estado del arte del uso de blockchain en distintos sectores.

Para empezar, si los primeros años posteriores a la creación de bitcoin el mundo lo recibió con bastante recelo, en los últimos años, la inversión en dicha tecnología ha aumentado de forma extraordinaria. En ésta página web, http://www.coindesk.com/bitcoin-venture-capital/, hay un desglose de las rondas de inversión recibidas por las distintas *fintechs* dedicadas al desarrollo de la tecnología blockchain, así como de aplicaciones de soporte a dicha tecnología a lo largo de estos años. [http://www.coindesk.com/bitcoin-venture-capital/]

La inversión queda resumida en la siguiente gráfica (Figura 7), donde se observa el importantísimo crecimiento del volumen de las mismas.

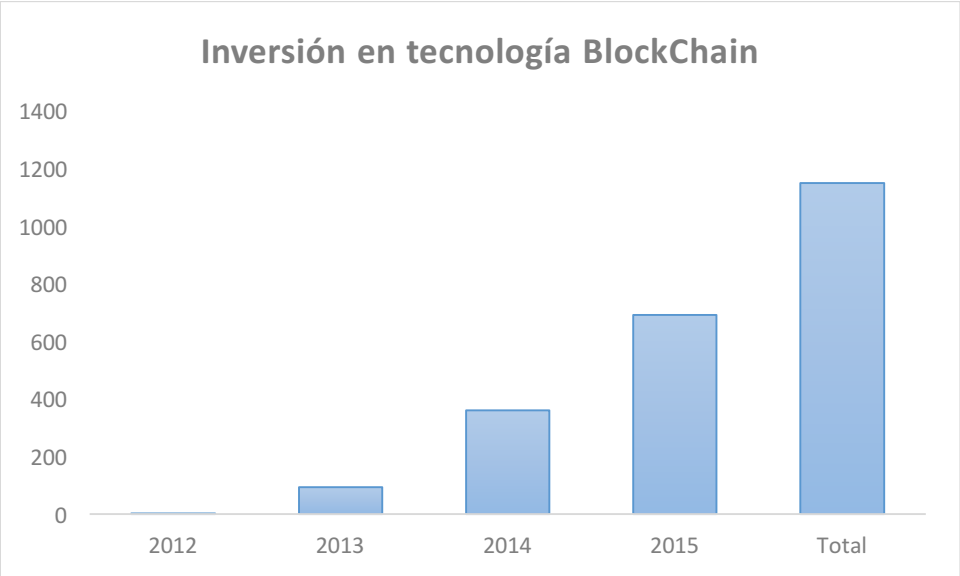

Figura 8. Inversión en tecnología Blockchain. Fuente: http://www.coindesk.com/bitcoin-venture-capital/

En 2012 la inversión en esta tecnología apenas supera los USD 2 millones. El siguiente año la inversión es de USD 95 millones, para pasar a una inversión de 360 millones en

2014. La inversión no para de crecer, alcanzando cifras de alrededor de 690 millones en 2015. En total la inversión acumulada durante estos años roza los USD 1,15 billones en más de 120 empresas relacionadas con esta tecnologías [Schatsky, 2016]. Según las previsiones de Morgan Stanley, sólo durante el año 2017 se invertirán USD 1 billón [Steenis, 2016].

6.1.- Futuras líneas de investigación y desarrollo

Como todas las nuevas tecnologías, las posibilidades que ofrece Blockchain son muchas. Desde optimizar procesos a nuevos modelos de negocio.

Hemos visto como hasta el año 2015 incluido, se ha invertido USD 1 billón, y esa cantidad es la que previsiblemente se invertirá sólo en el próximo año.

Algunos hitos que se han acontecido, y que de alguna manera hablan de la importancia que se le está dando por la relevancia de los protagonistas son por ejemplo la creación de R3, un consorcio formado por 30 de los bancos más importantes del mundo para diseñar y construir soluciones a partir de la tecnología Blockchain. Nasdaq está invirtiendo en la creación de un *market exchange* privado [Schatsky, 2016]. Microsoft ha lanzado un software de blockchain como servicio para empresas y redes de negocios, basado en el concepto de la nube. Y además, esta última ha firmado una alianza estratégica con el consorcio R3 antes mencionado. [Johnson, 2016].

En definitiva, en estos momentos están surgiendo cantidad de nuevos conceptos y prototipos, y las inversiones se suceden en diversas industrias.

Sin duda muchos sectores se verán afectados, y beneficiarán de la tecnología Blockchain. Entre ellos, los sectores de la tecnología, medios y telecomunicaciones, consumo, salud. También el sector público, y, por supuesto, el sector financiero al que a continuación dedicaré un capítulo aparte.

La tecnología blockchain aplicada a los medios de comunicación, como puedan ser periódicos o revistas digitales, dará soporte a los micro-pagos, de esta manera posibilitará que los medios cambien su modelo a uno en que se pueda cobrar al lector por artículos o publicaciones leídas concretas frente al modelo actual de las suscripciones mensuales.

Otros ven en Blockchain una forma de asegurar y proteger la propiedad intelectual, así como trabajos de creatividad digital como imágenes y música.” [Schatsky, 2015]

El el sector del consumo, la aplicación más obvia será la utilización de esta tecnología como plataforma o medio de pago, compitiendo con los ya existentes. Otras aplicaciones requieren de más imaginación, como la empresa DocuSign, un proveedor de firmas electrónicas y gestor de transacciones digitales, que ha integrado la tecnología blockchain y los contratos para automóviles, y que pretende simplificar los procesos y trámites de compra-venta de coches, leasing,… [Schatsky, 2015] Otro uso sería en la venta de tickets de eventos, donde esta tecnología ayudaría a prevenir el fraude. [Fanning, 2016]

Otro sector en el que ha suscitado gran interés es en el de la salud. Blockchain posibilita el registro del historial médico, de manera que el paciente pueda compartirlo con distintos médicos de manera sencilla. Además puede ser también interesante el registro otros datos como facturas, pruebas, seguros, reclamaciones, de forma que el carácter irrevocable facilite la gestión de reclamaciones y resolución de disputas [Schatsky, 2015]. Esto principalmente interesante para instituciones privadas y compañías de seguros. Empresas como Philips Healthcare han confirmado que se encuentran actualmente explorando el potencial uso de esta tecnología, aunque no ha revelado que aplicaciones está evaluando [Schatsky, 2015]

Otro sector que sin duda se beneficiará de la gran red de registros públicos que es Blockchain es precisamente el sector público. Como resulta obvio pensar, la aplicación de esta tecnología es idónea para los registros públicos, como por ejemplo el registro de la propiedad. El registro de automóviles. Una gran base de datos nacional que interconectara los distintos registros a nivel local. La información sería pública y de fácil acceso. Incluso revolucionaria algo tan trivial como la forma de votar en un proceso de elecciones.

El sector del lujo es otro que parece haber encontrado en Blockchain una forma efectiva de verificar la originalidad de los productos [Fanning, 2016]. La originalidad se refiere a procedencia, y sin duda una de las ideas más laureadas del pasado año, ganadora del concurso de innovación BBVA Open Talent 2015, es Everledger que pretende verificar los diamantes desde su procedencia, a lo largo del proceso de compra venta. Evitando de esta forma el fraude y la comercialización de diamantes falsos, así como por otro lado evitar la entrada al mercado de los diamantes de sangre, posibilitando el rastreo de diamantes robados, entre otros.

La realidad en cualquier caso, es que a día de hoy es imposible saber cómo reaccionarán las distintas empresas de los sectores anteriormente mencionados y cómo se adaptarán los pero lo que parece claro es que los tiros empiezan a apuntar en una dirección común: blockchain.

De todas formas, y a pesar de la cantidad ya invertida y que el desarrollo de esta tecnología avanza a pasos agigantados, aún es pronto para poder hablar de una implementación a nivel global. Pasarán unos años todavía para que empecemos a ver los frutos de muchas de estas inversiones e iniciativas.

Entre otras cosas, ahora mismo no hay capacidad computacional suficiente para explotar todo el potencial de Blockchain. Es cierto que hay muchas entidades privadas desarrollando sus propias blockchains, y sistemas de blockchains privados para unos pocos participantes. Aun así, la capacidad dista mucho de permitir un uso genérico para las operaciones que se pretenden llevar a cabo.

Por eso mismo, la principal línea de desarrollo ahora mismo, dejando a un lado el estudio de las posibles aplicaciones, es la optimización del proceso de verificación, de manera que se consigan procesos mucho más eficientes que no requieran de toda la capacidad que requiere la validación de todos los usuarios de cada transacción. Buscar mecanismos de verificación que no requieran de la aprobación de todos los miembros sino de sólo unos pocos, sin perder por ello robustez, es decir, que las verificaciones sigan siendo correctas y no se apruebe ninguna que no deba ser aprobada.

Otra línea que se sigue investigando, es la de los *smart contracts*, o contratos inteligentes. Que son los que posibilitarán la gran mayoría de las funciones anteriormente expuestas.

7.- BLOCKCHAIN

Si la primera respuesta de la gran banca a la nueva moneda no fue otra que la indiferencia, pronto se entendió como una amenaza para el sistema y el rechazo del sistema financiero a la cripto-moneda Bitcoin o similares fue en aumento.

Sin embargo, con el tiempo se ha visto que son muchas las virtudes del sistema Blockchain como para que la banca no volviera sus ojos hacia ello, hasta el punto de haber alcanzado el estado actual de embelesamiento y admiración por la tecnología Blockchain. Nivel de admiración que se traduce en las numerosas y millonarias inversiones que los grandes bancos han realizado, y siguen realizando a día de hoy, para desarrollar esta tecnología y poder adaptarla a sus necesidades. Morgan Stanley prevé que la inversión en esta tecnología en 2017 alcance el billón de dólares. [www.the-blockchain.com/docs/Morgan-Stanley-blockchain-report.pdf]. La intención de las instituciones financieras es clara; adaptar la tecnología blockchain a sus necesidades operativas internas, apartando todo lo lejos posible bitcoin. Existe una clara voluntad en el sector por canalizar el potencial transformador de Blockchain.

Este cambio de actitud lo evidencian hechos tan representativos como lo es la creación del R3, un consorcio formado por 30 de los principales bancos del mundo. R3 pretende ofrecer un servicio de Blockchain, comúnmente referido en la literatura como BaaS *(Blockchain as a Service)*, para los miembros del grupo. Algunos de sus miembros son el Barclays, Credit Suisse, Commonwealth Bank of Australia, HSBC, Natixis, RBS, UBS, UniCredit, Wells Fargo, etc. El principal objetivo es poder realizar transacciones instantáneas a través de una red global y privada. [Fanning, 2016]

Otros como Goldman Sachs están invirtiendo en crear su propia Blockchain, con su correspondiente moneda, para las necesidades de la misma compañía. También está invirtiendo en Circle Internet Financial, una empresa que pretende dar un mejor sistema de back-end basado en Blockchain.

El hecho de que ningún ente estuviera detrás de la moneda, así como que no existiera ningún tipo de activo físico que pudiera respaldarla eran algunos de las principales, y comprensibles, preocupaciones de sus detractores. Si el uso de esta moneda alcanzara una cierta notoriedad o relevancia en la sociedad, podría poner en jaque las estructuras político-financieras del mundo, ya que los estados y sus bancos centrales perderían el control sobre la moneda, una de las principales herramientas con las que cuentan los organismos de gobierno para influenciar en la economía. Y de ninguna manera estaban dispuestos a perder este poder.

Además otros factores como la volatilidad y la estabilidad de la moneda, la fortaleza, la seguridad, las malas prácticas que podrían encubrir su anonimato, la regulación… Eran muchas las dudas y pocas las respuestas.

7.1.- Nuevo marco competitivo

La gran cuestión de la banca con blockchain es que, si bien la tecnología puede hacerles ahorrar grandes costes en estructuras internas e intermediarios necesarios, es un arma de doble filo pues el desarrollo de las tecnología puede hacer que aparezcan nuevos agentes que cambien por completo el entorno competitivo tal y como lo conocemos hoy día. [Van Steenis, 2016]

El miedo no es infundado y de hecho, se percibe en el sector tiempos de cambios. La consultora estratégica strategy& del grupo pwc, resalta en un informe[2] que el sector financiero teme que el fenómeno fintech vaya a arrebatar hasta un 25% del negocio en los próximos 5 años. [http://www.pwc.es/es/sala-prensa/notas-prensa/2016/entidades-financieras-temen-auge-fintech.html] Sin embargo, las FinTech consideran que ese bocado puede ser todavía mayor y alcanzar hasta un 33%. Las fintech, además de estar ganando mercado a costa de los pertenecientes al sistema financiero tradicional (bancos, compañías de seguros, brokers, gestores de activos, …), están presionando los márgenes a la baja y con ello la rentabilidad de las entidades financieras. Además, el estudio llevado a cabo por strategy& incluye cuales son las áreas más amenazadas, que como se podía intuir, son la banca retail, los medios de pago, y los servicios de gestión de activos y patrimonios. [http://www.pwc.es/es/sala-prensa/notas-prensa/2016/entidades-financieras-temen-auge-fintech.html]

Sin embargo, la aparición de estas start-ups supone una oportunidad que los bancos no pueden dejar pasar ya que, por mucho riesgo que exista de que pierdan negocio a favor de las fintechs que no paran de surgir, el potencial de los beneficios fruto de las posibles sinergias, es abrumadoramente atractivo para ambas partes.

La realidad es que ya han surgido empresas que tendrán gran impacto en los servicios financieros. Un ejemplo es Coinbase, que ya se ha presentado con anterioridad en este trabajo como una plataforma de intercambio, y que además a creado una tarjeta de débito basada en bitcoin. Usando los protocolos de Blockchain, será la primera tarjeta que de el paso a registrar cada transacción directamente en una cadena de bloques, ahorrándose la mayoría de los costes de back-end [Fanning, 2016]. Otra de la que ya hemos hablado, y que es reconocida por ser "probablemente la que ofrece la función más desarrollada hasta el momento como servicio financiero basado en Blockchain" [Fanning, 2016], es Ripple. Ésta ofrece la posibilidad de hacer transacciones transfronterizas de manera rápida y sencilla, con los costes mínimos. Gracias a esta aplicación las instituciones financieras pueden hacer este tipo de transacciones a tiempo real, con certeza, y con los mínimos costes.

[2] El informe 'Blurred lines' acerca de Cómo FinTech está redefiniendo el sector financiero, elaborado por PwC a partir de 544 entrevistas con directivos del sector – consejeros delegados, responsables de Innovación y responsables de Tecnología y Sistemas (CIOs) – en todo el mundo, analiza cómo las nuevas tecnologías digitales van a cambiar el sector financiero, tal y como lo conocemos ahora. [http://www.pwc.es/es/publicaciones/financiero-seguros/assets/pwc-fintech-global-report-2016.pdf]. Según este informe el 57% de los directivos bancarios encuestados no saben cómo enfrentarse a blockchain.

7.2.- Aplicaciones al sector financiero

Desde luego, si hay dos ámbitos en los que el sector financiero se puede beneficiar claramente de las ventajas del sistema blockchain, esas son las transacciones transfronterizas y los mercados de capitales. [Van Steenis, 2016]

Los beneficios no vendrán en nuevos productos o servicios, ni desarrollo de nuevos modelos de negocio, sino por una importantísima reducción de los costes operativos.

Por el lado de los mercados de capitales, la transformación del sistema financiero a unas estructuras de mercado construidas sobre la tecnología blockchain será una gran tarea que requerirá de una enorme inversión, sin embargo, los ahorros serán considerables.

Según el informe[3] "BlockChain In Capital Markets" [Van de Velde, 2016] el desarrollo de la tecnología blockchain aplicada al sector financiero reducirá los costes de manera importante atacando dos puntos claves:

1. Las comisiones de los servicios externos.

2. Los costes de las operaciones , así como de los sistemas de IT.

Sólo en el área de mercados de capitales, la banca gasta cerca de USD 100-150 billones en operaciones y IT, así como otros USD 100 billones en servicios asociados. El uso de Blockchain, permitiría llevar libros de contabilidad digitales mucho más eficientes, que podrían reducir los costes en el sector bancario hasta en USD 20 billones al año [Van Steenis, 2016]

Les va a permitir ahorrarse los tremendos costes de intermediación en sus operaciones, empezando por ahorrar en sus procesos internos de en middle y back office. Además de que van a eliminar muchas duplicidades propias de los sistemas de verificación bancarios.

En cuanto a las transacciones transfronterizas, sin duda, si un agente está tomando la delantera en ofrecer una solución a esta cuestión es Ripple, que simplificará tanto el proceso. Veamos un ejemplo:

> Una persona en España quiere enviar dinero en USD a su hijo que estudia en EEUU. Concretamente quiere transferirle EUR 1000. Para ello, da a su banco, el Santander, una orden de transferencia de EUR 1000 a la cuenta de su hijo en el Bank of America que recibirá USD. El Santander enviará el dinero al Banco Central Europeo. El BCE, lo hará a la Reserva Federal. Y ésta, lo transferirá al Bank of America. Este proceso puede llevar desde 3 días a una semana hasta que el dinero realmente llega al banco de destino. Y en el proceso de intermediación habrá quedado en comisiones un 10% de lo que inicialmente se quería mandar.

[3] Informe "BlockChain In Capital Markets" redactado y publicado por consultores Oliver Wyman de manera conjunta con miembros de Clearnet, disponible en: http://diyhpl.us/~bryan/papers2/bitcoin/BlockChain-In-Capital-Markets.pdf],

Con Ripple, esta transacción se confirmaría y depositaría en cuestión de segundos. Hablamos de transferencias a tiempo real, con certeza casi absoluta de entrega.

7.3.- Contratiempos y regulación

Quedan claros los beneficios de Blokchain, y la banca parece decidida a aprovecharlos. Eso sí, las instituciones financieras tienen que cumplir una serie de requerimientos para con los reguladores. Para empezar dar acceso a revisar todas sus transacciones. Además, deben asegurarse de que cualquier cliente en su plataforma debe ser revisado bajo los parámetros de las políticas de KYC (know your costumer) y AML (Anti-Money Laundering) [Van Steenis, 2016]. Es decir, conoce a tu cliente y de dónde proviene su dinero. Esto último choca de frente con características intrínsecas de Blockchain como lo son el anonimato. Por lo que tendrán que ingeniárselas para ser capaces de incluir sistemas para controlar el lavado de dinero, entre otras cosas.

Y además, el carácter público y global de los libros contables distribuidos, que son Blockchains interconectadas, que traspasan fronteras y jurisdicciones, requerirá desde luego los esfuerzos de los organismos reguladores para coordinarse en este nuevo entorno global.

En este aspecto los organismos reguladores tendrán que hacer especial hincapié. El poder de blockchain es inmenso, y su carácter lo hace especialmente vulnerable a que utilizado con fines no lícitos. A ojos a algunos, este sistema es altamente propicio para el lavado de dinero y para la aparición de plataformas de mercado negro.

El FSOC *(Financial Stability Oversight Council)*, según recoge el periodista Berney Jopson en el Finantial Times, asegura que Blockchain, "como casi todas las nuevas tecnologías, posee ciertos riesgos e incertidumbres que los reguladores financieros deberán controlar." Además añade que "los participantes del mercado tienen limitada experiencia trabajando con sistemas de libros contables distribuidos, y es probable que las vulnerabilidades operacionales asociadas a dicho sistema no se muestren hasta que sean implementados a escala." [Jopson, *Finantial Times*, 22 junio 2016]

A medida que las criptomonedas continúan ganando terreno como medio de pago, el carácter volátil y la oportunidad de invertir especulativamente, empuja a los usuarios a no utilizarlo como medio de pago. [http://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/qa-what-is-blockchain.pdf] Aun así, tiene el potencial de convertirse en un medio de pago global, donde el único requisito para participar es tener acceso a la tecnología, y no requiera de historial bancario y cuenta bancario. De alguna manera, Blockchain llegará a las personas allí donde no llegan los bancos.

7.4.- Por qué deberían los bancos utilizar Blockchain?

1.- Por seguridad; la criptografía utilizada para proporcionar irreversibilidad a las transacciones hace que no puedan ser modificadas. Además las claves privadas para cada usuario y producto, unido a la encriptación de los registros de las transferencias de datos, lo hace aun mas seguro.

2.- Reducción de costes. Una base de datos pública, abierta y compartida posibilita una simplificación y reducción considerable de los procesos y equipos para validar las transacciones de un banco. Los datos son irrevocables pues las transacciones son irreversibles. Además es público y perfectamente auditable. Y por último los usuarios pueden compartir los costes de desarrollo y mantenimiento de la infraestructura. [Van Steenis, 2016]

Según un informe llevado a cabo por Morgan Stanley [http://www.the-blockchain.com/docs/Morgan-Stanley-blockchain-report.pdf], una infraestructura común, como la que posibilita blockchain, compartida y mantenida entre diversos participantes del mercado podría suponer un ahorro de costes de hasta el 30/40/50%.

3.- Blockchain aumenta considerablemente la velocidad de las transacciones. Tanto como que el monedero de el vendedor y comprador se actualizan simultáneamente en cuanto la transacción es verificada. Además hay muchos menos errores.

En definitiva, Blockchain es una gran oportunidad para transformar el sector en uno mucho más eficiente lo que permitirá mejorar los márgenes operativos, lo que a su vez supondrá mejores condiciones que ofrecer a los clientes. Un sector más transparente, que no sólo genere más confianza en el consumidor, sino que sea más eficientemente auditado y controlado.

Además, Blockchain tiene el potencial de convertirse en un medio de pago global, donde el único requisito para participar es tener acceso a la tecnología, y no requiera de historial bancario y cuenta bancario. De alguna manera, esta tecnología llegará a las personas allí donde no llegan los banqueros, y llevará los servicios financieros allá donde no llegan los bancos.

8.- DISCUSIÓN

El primer objetivo del trabajo, además de entender bitcoin y la blockchain, era hacer una revisión del estado del arte de la tecnología. Considero importante entender la separación de Blockchain como plataforma de Bitcoin, la moneda. Y de cierta manera, para quien no esté puesto en el tema y haya oído hablar de Bitcoin de pasada, quizá le sorprenda que la verdadera innovación, que la tecnología que realmente tiene ese inmenso potencial transformador de operaciones y sectores, es Blockchain. La red inicialmente pensada para dar soporte a la criptomoneda.

Es esta separación de conceptos la que permite aplicar dicha tecnología a diversos usos que van mucho más allá de la transferencia de dinero digital. El carácter público del libro de registros que es Blockchain lo hace idóneo para aplicaciones que manejen gran cantidad de datos, donde la verificación y el acceso a los mismos de manera sencilla y global sean sencillo, transparente y ágil.

Si bien Blockchain por el carácter anónimo que tiene puede dar lugar a usos indebidos, como medio para lavar dinero o que posibilite el mercado negro, son muchas las cosas buenas que puede aportar.

Mi opinión personal es que esta gran base de datos pública puede contribuir como nada que se haya inventado hasta la fecha al desarrollo de los países, especialmente aquellos menos desarrollados, que generalmente coinciden con ser países con los regímenes menos transparentes, con más corrupción en sus gobiernos y con más inestabilidad política y jurídica. Empezando por algo tan básico como la celebración de unas elecciones, en estos países donde se producen amaños en el recuento de votos, una votación a través de Blockchain sería imposible de amañar, pues cada voto quedaría públicamente registrado, de forma irrevocable, y fácilmente auditable o comprobable, donde además el carácter anónimo mantendría el secreto del voto. No sólo eso, un registro público de la propiedad en Blockchain de la misma manera aportaría seguridad a los propietarios de inmuebles, fincas y un largo etcétera. Por tanto, Blockchain arrojaría transparencia y seguridad a la gestión de estos países, permitiéndoles desarrollarse.

Por otro lado, se pretendía estudiar el uso de la aplicación para el cambio de divisas *peer-to-peer*, lo que viene a ser entre dos personas sin necesidad de intermediarios.

Bitcoin surge de una corriente anarquista que nace con el firme propósito de prescindir de los intermediarios en las transacciones financieras. Y aunque en su ADN figure la idea, para decepción de los utópicos que creían que el desarrollo de Bitcoin y Blockchain permitiría prescindir de los bancos, la realidad parece indicar que no será así. Y que precisamente son los bancos los que más se beneficiarán de esta tecnología diseñada para acabar con ellos. En este sentido, conviene reconocer el mérito del sector financiero, que ha estado ágil reconociendo el inmenso potencial, y apostando por el desarrollo del mismo, con la firme intención de aprovecharse de ello.

Si hay una industria en la que los avances están siendo rápidos es en la financiera, al ser la primera en apostar claramente por el desarrollo de Blockchain.

Los bancos están decididos a beneficiarse de esta tecnología, que les va a permitir ahorrarse los tremendos costes de intermediación en sus operaciones, empezando por ahorrar en sus procesos internos de en middle y back office. Además de que van a eliminar muchas duplicidades propias de los sistemas de verificación bancarios. Por supuesto, también está la posibilidad de hacer transacciones transfronterizas prácticamente en tiempo real por medio de Ripple.

A lo largo de estos últimos años hemos visto la aparición de nuevas, muchas y variadas empresas innovadoras, que han cambiado las reglas de juego. Empresas basadas en la economía colaborativa como Airbnb, o BlaBlaCar, que han supuesto una revolución importante en su sector, tienen en común dos cosas: la primera, la meteórica captación de nuevos clientes o usuarios que utilizaran su plataforma, y la segunda, que primero vino la innovación disruptiva, el nuevo modelo de negocio, y a posteriori las autoridades reguladoras hicieron lo propio, que es regular la actividad.

El uso de bitcoin y/o blockchain, y donde digo bitcoin me refiero a cualquier criptomoneda o activo intangible, no parece que vaya a correr la misma suerte.

Por un lado el uso masivo parece que va a tener que esperar. Primero porque no hay capacidad computacional suficiente como para un uso global y en masa. Además, "la percepción del usuario acerca de esta tecnología es que es compleja, y por el momento no parece dispuesto a utilizarlo como medio de pago" [Baur, 2015].

Además, el sector financiero es quizá uno de los más regulados y supervisados, y más desde que estallara la crisis de 2008. En este sector las innovaciones disruptivas no pueden ser a priori de la regulación y aprobación de los organismos reguladores. En este sentido, el esfuerzo por regularlo debe ser el máximo por parte de las autoridades competentes.

Con blockchain, cualquier persona con acceso a un dispositivo móvil con internet podría tener crearse un monedero en la red. Por ser un sistema anónimo, o pseudoanónimo, no se requiere ningún tipo de documento para acceder a él. No es necesario contar con ningún tipo de historial bancario, ni realizar un perfil de riesgo, ni nada por el estilo. Esto hará que mucha gente que no tiene acceso a los bancos, vayan a tener acceso a un sistema bancario.

En resumidas cuentas, a día de hoy hay tecnología disponible para hacer transacciones transfronterizas y en distintas divisas. Y todo ello sin necesidad de comprar la moneda intermedia que sería la criptomoneda. La cosa va aún más lejos ya que por un lado, las transacciones serán mucho más rápidas que con los actuales mecanismos, tan rápidas como que Bitcoin tarda de media 10 minutos, Litecoin 4 veces menos, y Ripple cuestión de segundos. Y por otro lado, realizar las transacciones por medio de blockchain va a reducir los costes de las mismas considerablemente, pues se elimina la necesidad de intermediarios.

9.- CONCLUSIONES

-. Bitcoin, y particularmente blockchain, son una realidad que está llamada a revolucionar distintas industrias. Esencialmente en los procesos de registro y gestión de datos.

-. Si bien es cierto que Blockchain, y Bitcoin, permitirán el desarrollo de nuevos productos, servicios y modelos de negocio, el verdadero potencial transformador para muchas empresas viene de la capacidad de simplificar las estructuras operativas y reducir costes.

-. En el sector financiero, esa revolución vendrá principalmente en dos vertientes: la primera son medios de pagos y las transacciones, especialmente las transfronterizas donde la divisa del emisor sea distinta que la del receptor, que podrán hacerse prácticamente a tiempo real con conocimiento exacto en cada momento de dónde está el dinero; y la segunda viene en el área de los mercados de capitales, donde se podrá tanto prescindir de intermediarios como simplificar los procesos de middle y back office, reduciendo de manera importante la estructura de costes. Aunque debido a la vasta y minuciosa regulación del sector, la adopción e implementación de estos sistemas se hará de manera paulatina.

-. El uso de bitcoin como medio de pago esta lejos de ser adoptado por las masas. Primero, debido a su carácter volátil, es percibido más como una oportunidad de inversión especulativa y los usuarios lo utilizan para trading más que como medio de pago. Por otro lado, aún es una tecnología desconocida para muchos, y es percibida como un complejo mecanismo de pago. Por último, la propia red global de cadenas de bloque aún no tiene capacidad computacional suficiente para asumir ser utilizada como un medio de pago de uso global.

Apéndice: definiciones

Una *moneda (coin)* o cualquier activo[4], es una propiedad digital cuyo poseedor puede ser probado criptográficamente.

Un *bloque* es una colección de transacciones que demuestran cambios en el control o posesión de un activo.

Una *cadena de bloques (blockchain)* es una serie ordenada de bloques, aceptada en consenso por todos los usuarios como veraz, de manera que determina computacionalmente la posesión de un activo y el cambio de manos del mismo, así como el orden cronológico en que suceden las transacciones.

La *reorganización* o simplemente *reorg* ocurre a nivel local en clientes o usuarios cuando una cadena competidora más larga sobrepasa a una cadena previamente aceptada. Al ser más larga, es aceptada por más usuarios, lo cual conlleva más pruebas de trabajo, y por tanto a partir de este momento pasa a ser la cadena de bloques aceptada. La nueva cadena de bloque sustituye a la cadena sobrepasada, que desaparece del historial de consenso.

El concepto de *cadena lateral (sidechain)* no es otra cosa que una cadena de bloque que valida datos de otras cadenas de bloques.

[4] Entiéndase por activo cualquier dato u objeto transferible por *Blockchain*

BIBLIOGRAFÍA

1. Banco Central Europeo. "¿Qué es el dinero?" 24 de noviembre de 2015. Web del Banco Central Europeo. Disponible en: https://www.ecb.europa.eu/explainers/tell-me-more/html/what_is_money.es.html] Acceso: Junio 2016

2. Durán C.G. 2012, "Evolución de los métodos de pago: del trueque al microchip". Repositorio institucional de la universidad de Oriente Venezuela. Disponible en: http://ri.biblioteca.udo.edu.ve/bitstream/123456789/4585/1/TESIS%20CARLOS%20DURAN.pdf

3. Coin Desk. "What is bitcoin?" 20 Marzo 2015. Disponible en http://www.coindesk.com/information/what-is-bitcoin/. Acceso Junio 2016

4. Coin Desk 20 Marzo 2015. Disponible en: http://www.coindesk.com/information/how-do-bitcoin-transactions-work/ Acceso Mayo 2016

5. Dai Wei. 9/11/2014 "b-money". 1998. Disponible en http://www.weidai.com/bmoney.txt Acceso Junio 2016.

6. Baur A. W., Bühler J., Bick M., Bonorden C.S. 2015. "Cryptocurrencies as a Disruption? Empirical Findings on User Adoption and Future Potential of Bitcoin and Co," en: *Open and Big Data Management and Innovation*, ed. Springer International Publishing , pp.63-80.

7. Armknecht, F., Karame, G.O., Mandal, A., Youssef, F., Zenner E. 2015, "Ripple: Overview and Outlook" , en: *Trust and Trustworthy Computing* Página 163-180, Proceedings 8th International Conference, TRUST 2015, Heraklion, Greece, August 24-26, eds Mauro Conti, Matthias Schunter, Ioannis Askoxylakis, Springer International Publishing pp. 163-180. DOI: 10.1007/978-3-319-22846-4.

8. Hayes, A.S. 2016, "Cryptocurrency Value Formation: An empirical study leading to a cost of production model for valuing Bitcoin", *Telematics and Informatics*. DOI: http://dx.doi.org/10.1016/j.tele.2016.05.005

9. Nakamoto S. "Bitcoin: A Peer-to-Peer Electronic Cash System", disponible en: https://bitcoin.org/bitcoin.pdf . Mayo 2016

10. Back, A., Corallo, M., Dashir L., Friedenbach M., Maxwell,G.,Miller, A., Poelstra A., Timón,J. y Wuille P.† 2014, "Enabling Blockchain Innovations with Pegged Sidechains", disponible en: https://blockstream.com/sidechains.pdf

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

12. Schwartz, D., Youngs, N., Britto, A. 2014, "The Ripple Protocol Consensus Algorithm". Ripple Labs Inc., disponible en: https://ripple.com/files/ripple_consensus_whitepaper.pdf.

13. Houy, N. 2014, "The Economics of Bitcoin Transaction Fees" ,GATE WP 1407, disponible en: http://ssrn.com/abstract=2400519 o http://dx.doi.org/10.2139/ssrn.2400519

14. Plansky, J., O'Donnell, T., y Richards, K. 2016, "A strategist's Guide to Blockchain", disponible en: http://www.strategy-business.com/article/A-Strategists-Guide-to-Blockchain. January 11, 82, 2016.

15. Friedenbach, M., Timón J., 2013, "Freimarkets: extending bitcoin protocol with user-specified bearer instruments, peer-to-peer exchange, off-chain accounting, auctions, derivatives and transitive transactions", disponible en: http://freico.in/docs/freimarkets-v0.0.1.pdf.

16. Fanning, K. and Centers, D. P. ,2016, "Blockchain and Its Coming Impact on Financial Services", J. Corp. Acct. Fin., 27: 53–57. doi: 10.1002/jcaf.22179.

17. Glick B., 27 octubre 2015, "Why blockchain heralds a rethink of the entire banking industry", Computer Weekly, disponible en http://www.computerweekly.com/ezine/ComputerWeekly/Blockchain-sparks-change-in-banking-industry.

18. @PwCFinTech, Q&A ,"What is blockchain?", 2016, disponible en: http://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/qa-what-is-blockchain.pdf.

19. Schatsky, D., 2016, "Beyond Bitcoin—Blockchain Is Coming to Disrupt Your Industry: Weekend Reading", CFO Journal from the Wall Street Journal, disponible en: http://deloitte.wsj.com/cfo/2016/02/26/beyond-bitcoin-blockchain-is-coming-to-disrupt-your-industry-weekend-reading/tab/print/.

20. Schatsky, D. y Muraskin C., 2015, "Beyond bitcoin. Blockchain is coming to disrupt your industry", Deloitte University Press, disponible en:

http://d27n205l7rookf.cloudfront.net/wp-content/uploads/2015/12/DUP_1381_Beyond-bitcoin_SFS_vFINAL.pdf

21. PWC, 2015-16, "Making sense of bitcoin, cryptocurrency, and blockchain", disponible en: http://www.pwc.com/us/en/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html.

22. Coin market, 9 julio 2016, Crypto-currency market capitalizations, disponible en: http://coinmarketcap.com/currencies/views/all/

23. Coin Desk, 19 junio 2016,"Bitcoin Venture Capital", disponible en: http://www.coindesk.com/bitcoin-venture-capital/.

24. Van Steenis, H., Graseck, B. L., Simpson, F., Faucette, J. E.,Global Insight, FinTech April 20, 2016 "Global Insight: Blockchain in Banking: Disruptive Threat or Tool?", disponible en: http://www.the-blockchain.com/docs/Morgan-Stanley-blockchain-report.pdf.

25. Jopson, B. 22 Junio 2016, "Regulators say bitcoin poses Finantial stability risks", disponible en: http://www.ft.com/cms/s/0/a1fc3522-314b-11e6-bda0-04585c31b153.html#axzz4DKIb39hA

26. Van Steenis H., 13 Junio 2016, Handled right, blockchain could help Banks and thir customers, disponible en: http://www.ft.com/cms/s/0/e0880cf6-3800-11e6-9a05-82a9b15a8ee7.html#axzz4DKIb39hA.

27. Van de Velde J., Scott A., Sartorius K., Dalton, I., Shepherd B., Allchin C., Dougherty M., Ryan P., Rennick E., febrero, 2016, "Blockchain in Capital Markets The Prize and the Journey", disponible en: http://diyhpl.us/~bryan/papers2/bitcoin/BlockChain-In-Capital-Markets.pdf.

28. Cookson, R., "Has the creator of bitcoin been revealed?", 2 Mayo, 2016, *Finantial Times*, disponible en: http://www.ft.com/cms/s/0/e729c740-106c-11e6-839f-2922947098f0.html#axzz4DvhL1Zad

29. Bitcoin backtrack; "Wright pull Satoshi proof", 5 mayo 2016, *Fast Finantial Times*, Disponible en: http://www.ft.com/fastft/2016/05/05/bitcoin-backtrack-wright-pulls-satoshi-proof/

30. Johnson, P., "Impulsando los servicios financieros en la revolución del blockchain", 4 abril 2016, Disponible en: https://news.microsoft.com/es-xl/impulsando-los-servicios-financieros-en-la-revolucion-del-blockchain/#sm.0001g4usrcn18eifwys2gcm10pa9i

31. BBVA Innovation Center, "Tecnología Blockchain, el avance de Bitcoin y de los pagos virtuales", FinTech Serie por Innovation Edge, enero 2016, Disponible en: http://www.centrodeinnovacionbbva.com/sites/default/files/ebook-cibbv-tecnologia_blockchain-es.pdf

32. Jopson, B., "Regulators say bitcoin poses 'financial stability risks'", 22 junio 2016, *Financial Times,* Disponible en: http://www.ft.com/cms/s/0/e0880cf6-3800-11e6-9a05-82a9b15a8ee7.html#axzz4DKIb39hA