FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES

El Bitcoin, ¿Presente y futuro del dinero?

Sus características e implicaciones

Autor: Pedro Gutiérrez Hernández
Director: Profª. Dra. María Josefa Peralta Astudillo

Pedro Gutiérrez
Hernández

Madrid
Marzo, 2015

El Bitcoin, ¿Presente y futuro del dinero?

Índice

Resumen

Este articulo analiza la moneda digital descentralizada, “peer to peer” descentralizada denominada Bitcoin con el fin de determinar su naturaleza e implicaciones. Como resultado un análisis teórico del dinero y del Bitcoin, así como las influencias sociales, podemos concluir que actualmente el Bitcoin no constituye una moneda operativa a pesar de reunir las condiciones potenciales para serlo. Esto es debido a la fluctuación de su valor y la concepción del mismo como un activo financiero por una gran parte de sus usuarios. Las potenciales consecuencias de su triunfo en un futuro son de carácter político y económico, principalmente la reducción del control sobre la política monetaria y una apertura del sistema financiero. El artículo concluye que el Bitcoin no constituye una moneda actualmente pero con la evolución de la regulación y desarrollo de un sistema financiero se convertirá en una moneda secundaria que desbanque a monedas débiles con valores de gran fluctuación. Por otra parte se concluye que no se convertirá en una alternativa viable a las principales monedas de la economía actual debido a las potenciales presiones gubernamentales.

Palabras clave: Bitcoin, Dinero, Moneda digital, Cadena Bloque, sistema monetario, economía descentralizada, peer to peer, Regulación sobre el Bitcoin, cyperpunks, Satoshi Nakamoto.

1. Introducción

Objetivos

El presente trabajo tiene como objetivo el estudio de una moneda digital, descentralizada y pseudoanónima conocida como Bitcoin que ha surgido en nuestra sociedad en el transcurso de los últimos años, desde 2009. En concreto se pretenderá dar respuesta a la cuestión de si realmente puede ser considerada como dinero. Además también se profundizará en el análisis de la regulación y de las influencias del Bitcoin en la sociedad tanto en la actualidad como en el futuro.

Metodología

Para realizar este análisis se ha recurrido en primer lugar a una exposición de las distintas teorías económicas sobre qué características reúne el dinero. Posteriormente se ha realizado una revisión y contrastación de estas características teóricas con la situación actual del Bitcoin.

Posteriormente, también se ha realizado un estudio de aplicación de las características del Bitcoin para concretar las potenciales implicaciones en la sociedad. Además se ha desarrollado en último lugar una investigación sobre las principales tendencias regulatorias alrededor del Bitcoin. Para ello se ha recurrido principalmente a actas del senado de EEUU, artículos periodísticos y fuentes bibliográficas provenientes de la biblioteca legal del congreso de EEUU.

Estado de la cuestión

A través del uso de un programa público Bitcoin permite la trasmisión de fondos de una moneda inexistente en un formato físico entre usuarios anónimos. Por primera vez en la historia contemporánea existe una forma de transmisión de valor monetario fuera del área de control de los gobiernos, bancos o autoridad central de cualquier clase. Por lo tanto un tema de gran

interés y relevancia es si realmente su comportamiento en la sociedad es el de una moneda.

Políticos, inversores y el resto de la sociedad están tratando de comprender la naturaleza de esta nueva forma de dinero y las implicaciones que tendrá en la sociedad. Debido a esto es importante analizar el concepto de Bitcoin y dar respuesta a los objetivos planteados en este trabajo.

Partes principales del TFG

El trabajo está dividido en seis partes. En la primera de ellas el trabajo se centra sobre la explicación del marco teórico del dinero con un recorrido por las definiciones otorgadas al mismo. Además también se profundiza, en esa primera parte, en la historia del dinero con un recurrido por todas las formas que ha adoptado y sus características. En la segunda parte se profundiza sobre el concepto de Bitcoin y su funcionamiento interno. De la misma forma que en la primera parte después se realiza una exposición de la historia del Bitcoin desde sus orígenes hasta el presente.

Habiendo finalizado el marco teórico en las dos primeras partes la tercera parte se centra en la complacencia del Bitcoin con la definición del dinero. En esta parte se trata de dar solución a uno de los principales objetivos del trabajo, la determinación del Bitcoin como una forma de dinero o no. En la cuarta parte se exponen las implicaciones, tanto actuales como potenciales, del Bitcoin en los diferentes sistemas sociales. La quinta parte se centra en la regulación legal del Bitcoin, sin centrarse en un área geográfica sino atendiendo a corrientes globales. Y por último se extraen las conclusiones del análisis para dar respuesta a las cuestiones planteadas en los objetivos.

2. Definición del concepto de moneda y principales características

¿Qué es el dinero?

El dinero es un producto cuyo origen, al igual que el del resto de productos, se encuentra en una demanda para satisfacer unas necesidades. Estas necesidades son las de facilitar los intercambios de los demás bienes y servicios en la economía. A lo largo de la historia del dinero, desde el uso de piedras hasta la forma actual del mismo, se puede observar es una constante evolución para aumentar esa satisfacción de la necesidad de realizar transacciones.

El primer objetivo de esta introducción teórica es comprender qué características hacen a un activo dinero. Y un segundo objetivo es observar su evolución a lo largo de la historia de la humanidad para llegar a una mayor comprensión del mismo y de sus distintas formas.

Alrededor del concepto del dinero hay un consenso general sobre su carácter como medio de cambio en una sociedad para la facilitación de las transacciones y medida de valor en el pago de bienes o servicios[1]. Por lo tanto lo que permitiría identificar si un activo es dinero es su habilidad para satisfacer esa necesidad de facilitador de transacciones. Para ello podemos identificar tres funciones principales que un activo necesitaría cumplir: Medida de valor, depósito de valor y medio de pago[1].

- Medida de valor:

Con medida de valor se entiende que los bienes y servicios comercializados en el mercado tienen un valor determinado en el activo considerado como dinero. Por ejemplo, en la Europa contemporánea todos los bienes y servicios tienen cuantificado su valor en Euros, siendo el Euro en último término otro activo que tiene carácter de dinero.

- Depósito de valor:

Para que un activo pueda ser considerado dinero tiene que tener la capacidad de mantener su valor en el tiempo de tal forma que si vendemos hoy unos activos a cambio de dinero tengamos la relativa seguridad de que podamos mantener ese valor en el tiempo. Esto es para garantizar su capacidad de, pasado un periodo de tiempo, utilizarlo en la compra de otros bienes sin que haya disminuido la capacidad de compra del usuario. Un ejemplo de un activo que falló en el cumplimiento de esta condición son los tulipanes. En Holanda en el siglo IX se utilizaban como medio de pago e incluso como medida de valor de los demás bienes. De todas formas presentaban un gran defecto y es que eran perecederos por lo que no representaban un depósito de valor seguro, con el tiempo esto llevo a una gran deflación y a su descarte como moneda[2].

Otro problema que afecta a esta capacidad de depósito de valor es la inflación. Cuando se produce un aumento en el nivel de precios de la economía, el dinero presente en la misma, pierde valor: resulta necesario entregar una mayor cantidad de dinero para obtener la misma cantidad de bienes o servicios. Por tanto, cuando hay inflación sostenida se reduce su función como depósito valor ya que con el paso del tiempo se devalúa pudiendo provocar su pérdida total de valor.

- Medio de pago:

Esta función es la que un principio propició el origen del dinero: su actuación como intermediario entre el intercambio de distintos bienes y servicios. En su ausencia los intercambios se realizan mediante el trueque, obligando a la existencia de una doble coincidencia de intereses, la del oferente que quiere vender un producto y la del demandante que quiere adquirirlo y a cambio le ofrece otro producto que el vendedor tiene que estar dispuesto a recibir a cambio del suyo. Por lo tanto lo que esta función permite es una gran eficiencia en los intercambios reduciendo los costes de transacción, favoreciendo de esta manera el comercio y la especialización, y en última instancia el desarrollo económico.

Para que pueda cumplir esta función de medio de cambio el activo tiene que contar con una serie de características. La más importante de ellas es que tiene que ser comúnmente aceptado por la sociedad de tal forma que sea universalmente aceptado como medio de pago. Además también es deseable que cumpla unas características que harían su uso más eficiente. Estas son la capacidad de transporte del activo, su divisibilidad y su resistencia a la falsificación. Pero como ya veremos más adelante no constituyen una característica excluyente a la hora de determinar a un activo como dinerario.

Resulta extremadamente complicado emplear una definición de dinero única y generalmente aceptada. De hecho, lo que se entiende por dinero ha ido variando a lo largo del tiempo. A continuación intentaré exponer de forma abreviada los distintos enfoques que se le ha dado a esta definición a lo largo del pensamiento económico para acotar el término "dinero". Se podrían distinguir dos tipos de definiciones que históricamente se han dado sobre el dinero: Definiciones a priori (basadas en sus funciones), y definiciones basadas en su sustitución cruzada con activos financieros, características temporales y capacidad representativa de la riqueza nacional.

Comenzaremos por ver las definiciones a priori ya que son las más intuitivas para el lector. De todas las definiciones emitidas encuentro relevante citar las definiciones emitidas por Newlyn y Lord Robins. La definición tradicional la tomamos de Lord Robbins quien menciona que "…el dinero es evidentemente un medio de compra final… es obvio que el dinero es en sí mismo es tan sólo un medio: un medio de cambio, un instrumento de cálculo."[4]. Esta definición dada por Robbins ha sido desafiada por las teorías que defienden que el dinero no es un mero instrumento de cambio sino que debe tener un valor intrínseco, como por ejemplo, el oro. Sin embargo en las corrientes contemporáneas se ha producido un alineamiento con esta concepción del dinero como únicamente un activo con valor en medida de su capacidad de intercambio.

En una época posterior podemos leer a Newlyn: "…la función primordial, cuyo desempeño nos permite identificar al dinero, es muy simple: la de fungir como medio de cambio."[5]. Como podemos ver de todas las funciones del dinero la de medio de cambio fue la que recibió una mayor atención de la teoría tradicional. En la actualidad, sin embargo, se considera que es la función del dinero como depósito de valor, esto es, como la forma de mantener riqueza, la que debe destacarse sobre el resto.

No obstante, una vez identificadas estas definiciones a priori del dinero la dificultad reside en identificar qué activos representan verdaderos medios de cambio, donde situar la línea que aportará "dineridad" al activo utilizado. Como respuesta a esta pregunta y un intento de limitar el rango de su definición del dinero Newlyn opina que "…sólo si el conjunto de transacciones que efectúa el pago es igual a una transferencia de dinero de unas manos a otras puede considerarse como dinero el activo al que se ha recurrido para financiar el pago"[5]. Esto hace referencia a una característica concreta que se le ha atribuido al dinero a lo largo de la historia y que ha ido ganando importancia. La liquidez del mismo, que está estrechamente relacionada con su función de medio de cambio y de depósito de valor.

Por liquidez se entiende comúnmente la habilidad que tiene un activo de convertirse en efectivo con una perdida pequeña de valor, un medio de cambio. Sin embargo esta concepción cuando se trata de discernir si algo constituye un medio de cambio puede ser demasiado generalista. Una definición más exacta la aporta Laidler quien concreta que la liquidez es el resultado de la conjunción de dos características: la primera, es que el dinero es aceptado como medio de cambio de bienes y servicios, y la segunda, es que se puede predecir su valor de mercado[6]. De aquí podemos deducir que para que un activo pueda ser considerado dinero, en primera instancia, tiene que ser medio de cambio y además albergar una capacidad previa de depósito de valor. El problema a resolver es donde situar el límite de esa liquidez de la que deben gozar los activos para poder considerarse dinero. En este punto es donde la definición de

dinero falla en su acotamiento ya que ese límite es sujeto de constante debate, más ahora que nunca con el surgimiento de nuevas formas de dinero.

Aquí nos topamos con un callejón sin salida ya que estas definiciones a priori que parten de una definición previa del dinero y después intentan encuadrar las características necesarias no pueden ser comprobadas empíricamente. Y es por esta imposibilidad de correlacionar la realidad con estas definiciones a priori por lo que se recurre a definiciones empíricas del dinero, basadas en la realidad observada.

Estas definiciones empíricas están basadas en la observación de los comportamientos de los agentes de mercado en el transcurso de sus actividades. Recurriendo una vez más a una cita de Lord Robbins "… una correcta comprensión de lo que debe considerarse como dinero, es una cuestión que sólo pueden descubrir los hechos." [7]. De la misma forma Friedman refiriéndose al dinero decía que "Considerado como un cuerpo de hipótesis sustantivas la teoría ha de juzgarse por su poder de predicción respecto de la clase de fenómenos que intenta explicar. Únicamente la evidencia empírica puede mostrar si es aceptada como válida o rechazada."[8]. De estos dos razonamientos podemos deducir que donde reside la consideración o no de un activo como dinero es en el trato que se le da por parte de sus poseedores y la aceptación que tiene por parte de los acreedores. Todo ello sin perder de vista que esta consideración vendrá determinada por la consecución o no de las funciones que teóricamente el dinero debería albergar.

Este acercamiento empírico ha llevado a una clasificación de los activos que son una representación de dinero situándolos en una escala. Estos activos, de mayor a menor "dineridad" serían los siguientes, según Milton Friedman en el siglo XX[9]:

M1: Incluye las monedas y billetes que representan un valor directo. También se incluirían en este grupo los cheques susceptibles de ser usados inmediatamente ya que representan un derecho equivalente al valor del dinero.

M2: Incluye el grupo M1 y además añade todo aquel depósito de dinero del grupo M1 que se ha realizado en bancos comerciales en forma de depósitos a la vista.

M3: Añade los depósitos de ahorro al grupo M2.

M4: Además de las anteriores incluye las participaciones en distintas entidades.

Con esta clasificación se consigue una identificación de aquellos activos en posesión de la población que debido a su utilización son considerados como dinero. Más recientemente esta clasificación ha sido cuestionada y se han propuesto nuevos índices agregados de medición de aquello que conforma dinero en la economía. De todas formas a estos nuevos índices a pesar de sus ventajas teóricas no han probado una mayor utilidad en términos empíricos.

Las definiciones empíricas encuentran una gran limitación y es que al centrarse en la evidencia empírica están condicionadas por el contexto macroeconómico en el que se produjo la investigación. Y este contexto económico no solo varía con la región y sociedad tratada sino que es susceptible de variar en el tiempo.

Después de haber intentado acercarnos a una delimitación del concepto del dinero desde distintos puntos podemos concluir que ninguna de las evidencias y razonamientos presentados pueden considerarse como definitivos. Como decíamos al inicio el dinero se encuentra en constante evolución en su forma. Estas concepciones de dinero están sujetas a posibles desarrollos y matizaciones así como excepciones. Para asentar más esta idea general de qué podemos determinar cómo dinero es necesario atender a la evolución de la moneda a lo largo de la historia. De esta forma veremos qué activos han sido considerados dinero, sus características generales y las excepciones que han existido.

La historia del dinero

Si tomamos un paso a atrás y se observa la trayectoria del dinero a lo largo de la historia podemos ver que ha ido evolucionando a lo largo del tiempo acordemente con la sociedad. En cada época el dinero tuvo ciertas características que cambiarían con el paso del tiempo.

Generalizando se puede considerar que el dinero ha pasado por cuatro distintas etapas a lo largo de la historia. Por orden cronológico estos tipos serian el dinero mercancía, el dinero metálico, el dinero signo y el dinero fiduciario[10]. Además actualmente hay autores que sostienes que nos estamos acercando a la época del dinero digital con la aparición de, entre otros, del Bitcoin[11].

La primera etapa que nos encontramos es el dinero mercancía el cual consistía en la utilización de un determinado bien con un claro valor intrínseco, como la sal o el cacao, para utilizarlo como medio general de pago. Esta época fue la que sucedió al trueque y la principal diferencia residía en que este bien intercambiado era generalmente aceptado, aún por aquellas personas que realmente no iban a hacer uso del mismo como bien. Otra característica que reunía este dinero mercancía es que representaba una medida de valor para los demás bienes y servicios. De todas formas a menudo representaba un depósito de valor inestable.

Algunos ejemplos históricos son la utilización de ganado en la antigua Roma o el cacao utilizado por los aborígenes de Sudamérica. Pero un ejemplo donde realmente se vislumbra el origen y la naturaleza de esta forma de dinero lo representa el sistema monetario que surgió en los campos de concentración nazis en la Segunda Guerra Mundial. En estos campos de concentración el servicio médico alemán repartía a todos los internos unas raciones de diversos bienes, incluidos comida, ropa, chocolate, cigarrillos y demás, que estaban estandarizadas para todos los prisioneros. Esto claramente no atendía a las preferencias y necesidades de cada uno de los internos. En estas circunstancias surgió la necesidad del trueque de esos bienes, lo cual siempre

resultaba difícil y laborioso ya que había que encontrar a alguien en posesión del bien deseado con la disposición de entregártelo a cambio de uno de los bienes de tu posesión. Con el paso del tiempo los prisioneros empezaron a usar los cigarrillos como bien general de intercambio y medida de valor para los demás. Esto se debió a su facilidad de transporte, conservación y valor intrínseco que tenían. Por ejemplo se sabe que una camisa costaba alrededor de unos ochenta cigarrillos y que algunos reclusos empezaron a ofrecer servicios de lavandería a cambio de dos cigarrillos por prenda. Incluso las personas que no fumaban aceptaban estos cigarrillos debido a la certeza que tenían de que serían capaces de intercambiarlos en el futuro por otros bienes. En definitiva, estos cigarrillos se convirtieron en la moneda del campo de concentración, representaban un depósito de valor, unidad de cuenta y un medio de cambio generalmente aceptado por la sociedad[12].

Un gran salto en la historia del dinero se produjo con la creación del dinero metálico. Este nacimiento según descubrimientos del historiador griego XXXXXX se sitúa en Lidia o Reino de Lidia, una región histórica situada en el oeste de la península de Anatolia, en lo que hoy son las provincias turcas de Esmirna y Manisa[13]. Fue reino e imperio desde la caída del Imperio hitita hasta su conquista por los persas. Este nuevo concepto le aportaba al dinero una practicidad y efectividad no conocida antes en términos de elaboración de la moneda, medición del valor de la misma, depósito de valor y capacidad de transporte. Debido a esto rápidamente se expandió hacia los cercanos Grecia y Persia. Los principales metales aceptados fueron el bronce, plata y oro. Los metales preciosos que han tenido un sentido de riqueza y de valor en sí mismos a lo largo de la historia humana. Además de por esta asociación con valor que han tenido históricamente estos metales la elección de los mismos se realizó por la facilidad de elaborar monedas con una cantidad y tamaño concreto del mismo.

En la Antigua Grecia se utilizaba la “stadia” como medida de longitud y el “dracmae” como medida de peso. Así mismo las monedas griegas recibieron el nombre de Dracmas. El monopolio de la creación de monedas residía en

aquellas polis con minas de plata. La de mayor extensión fue la moneda ateniense que exhibía en un dorso un rosto de Atenea y en el envés un búho[13]. Esto producía en las ciudades un efecto llamado de señoreaje. El término procede de seigneur, término francés empleado para designar al "señor feudal" que en la edad media tenía el derecho único de acuñar moneda. El señoreaje es el beneficio proveniente de la diferencia entre los costes de acuñamiento de esta moneda y valor de los bienes que puedes obtener con la misma[3].

Cuando este dinero metálico se vio insuficiente por la escasez de los propios metales y el rápido crecimiento del mercado se caminó hacia un nuevo tipo de dinero. Primero se llevó a cabo la creación de monedas con menor aleación de esos metales preciosos. Un ejemplo de esto se produjo en el Imperio Romano donde en tiempos de stress financiero o necesidad de financiación de guerras se llevaron a cabo estas estrategias para aumentar el dinero en circulación, este fue el caso de la guerra contra Hannibal[13]. Estas monedas circularon con el mismo valor que sus hermanas compuestas en un cien por cien por plata. Esto se mantuvo gracias a la fe de los habitantes en las promesas del gobierno de respaldar esas monedas a pesar de su diferente composición. En este proceso se puede ver cómo la moneda fue perdiendo ese énfasis en el valor intrínseco de la misma y se acercaba más a la definición que veíamos en un principio de Lord Robbins. Tal y como la ley de Gresham enuncia "La moneda mala sustituye a la buena."[14]. Esta ley enuncia que el valor de cambio de las monedas basadas en metales únicamente tenderá a acercarse a sus costes de producción, lo que con el tiempo produciría un alejamiento del concepto de moneda con únicamente valor intrínseco.

Este proceso terminó con la aparición de la moneda papel o el papel moneda que consiste en la expedición de documentos respaldados por cierta cantidad de metales preciosos normalmente custodiados por el estado. Por lo tanto estos documentos ya no contaban con ningún tipo de valor intrínseco propio. Su valor provenía de su utilidad y de su respaldo por parte del gobierno. El punto de inflexión se puede situar en Inglaterra cuando un extranjero holandés ocupo el trono en 1689. El destituido Carlos II había

entrado en banca rota debido a sus deudas y este nuevo rey, William of Orange. Es en este momento cuando a un grupo de burgueses y en especial a un comerciante escocés el rey propuso la idea de la creación de una nueva institución llamada Bank of England[3]. Este banco central se comprometía a la financiación de los asuntos reales siempre y cuando se le proporcionará el derecho único de emisión de moneda papel. Este concepto novedoso rápidamente se expandió por otras naciones que reconocieron un gran potencial en su instauración. En un principio se mantuvo la representación del dinero en un estándar bimetálico de plata y oro. Pero con el paso del tiempo se vio que este doble soporte del dinero papel llevaba a problemas monetarios entre ambas "monedas". Así es como en 1880 se instituyó el patrón oro que significaba que todas las unidades monetarias estarían unidas a un cierto peso de oro. El valor de la moneda por lo tanto pasaba a depender de los almacenes del país en oro.

Con el patrón oro se consiguió una estabilización de los precios y una explosión de la cantidad de transacciones realizadas mundialmente. Este patrón oro también limitaba la capacidad de emisión de dinero por parte de los estados ya que estos poseían una cantidad determinada de oro y cualquier devaluación de la moneda tendría consecuencias inmediatas. Debido a estos problemas la duración del patrón oro fue corta en el tiempo, hasta 1913**.** Estos problemas ligados al patrón oro son, a juicio de muchos autores, el origen de una alternativa a futuro como es el Bitcoin por lo que profundizaremos posteriormente en esta problemática.

En un intento por mantener la moneda unida a una reserva física de oro se convocó una convención en New Hampshire, durante la segunda guerra mundial. En ella se acordó ligar todas las monedas existentes en Europa con las reservas de oro en EEUU, por lo tanto con el dólar americano. Esto produjo un gran crecimiento descontrolado de la demanda de dólares americanos que llevo a Nixon a finalmente rechazar esta conexión con las reservas de oro de EEUU, incluida la relación del dólar americano con esas reservas. Esto acabó

por romper el vínculo con las reservas de oro y todas las moneras pasaron a carecer de ningún tipo de respaldo salvo la confianza en el gobierno.

Aparece así el llamado dinero fiduciario o moneda fiat, que se basa en la fe o confianza de la comunidad, es decir, que no se respalda por metales preciosos, únicamente en una promesa de pago por parte de la entidad emisora frente al derecho que representa. Es el modelo monetario que manejamos actualmente en el mundo.

Un curioso ejemplo de moneda fiduciaria lo podemos encontrar en una isla localizada en el medio del Pacifico al norte de Guinea. Esta es la solitaria isla de Yap, la cual recibió la visita en 1903 del antropólogo americano William Henry Furness III. Para su sorpresa descubrió que en la pequeña isla los aborígenes habían desarrollado un complejo sistema financiero. A falta de metales preciosos los aborígenes utilizaron como moneda fueron enormes "ruedas" de piedra que dependiendo de su tamaño y calidad tenían distinto valor. El nombre que recibió esta particular moneda era el de Fei. El obstáculo que tuvo que superar esta moneda fue, claramente, el de su inmovilidad física, lo que implicó que en los intercambios de grandes cantidades de feis el traspaso del dinero no se realizaba con los Fei sino que se realizaba un traspaso de derechos sobre el fei. Esto significo con el tiempo que tomo más importancia el derecho legal sobre los fei que la posesión física del mismo[4].

Este sistema financiero realmente resultaba complejo y avanzado cuando se producía una pérdida física de un Fei a causa de una marea o similar. En este caso la sociedad seguía reconociendo la existencia del derecho de esa familia sobre el Fei perdido. A medida que avanzaba el tiempo la población aceptaba sin ningún tipo de problema derechos sobre feis que nunca habían visto físicamente y que posiblemente ya no existieran debido a la confianza generada. Este particular caso histórico refuerza la idea de que el dinero puede ser cualquier cosa mientras se tenga un nivel de confianza en su uso y en los derechos que el mismo representa.

Otro tipo de dinero, según algunos autores, es el dinero electrónico. Este tipo de dinero es el surgido con las transacciones realizadas directamente con el banco sin necesidad de un intercambio físico de la moneda en sí. Un claro ejemplo de este tipo de dinero es el de las tarjetas de crédito y débito, las cuales capacitan para realizar transacciones remotamente utilizando el dinero "almacenado" en un banco. s Históricamente este tipo de dinero se situaría mucho atrás en el tiempo con el comienzo de la realización de transacciones por telégrafo en EEUU en el año 1840. El telégrafo ayudo a unir transacciones entre América y Europa con la creación del cable transatlántico en 1867. A partir de ese momento el crecimiento del uso de esta moneda electrónica, en vez de la moneda o el billete tradicional, creció exponencialmente. Con la introducción de la informática y finalmente con las bandas magnéticas y tarjetas de crédito su uso ya es ampliamente más extendido que su versión física. En la siguiente tabla podemos ver claramente esta utilización del dinero en Estados Unidos, en el año 2013:

Tipo de pago	Volumen	Porcentaje del volumen	Valor
Efectivo	107	25.54%	$ 1.800
Cheques	24.4	5.82%	$ 31.100
Tarjetas de crédito	65.5	15.64%	$34.400
Transferencias Bancarias	222	53%	$1.046.000

Fuente: Federal Reserve Payments Study, McKinsey payment map, 2013 ; Datos en miles de millones

Otras corrientes no considerarían este tipo de dinero electrónico como una nueva forma diferente del fiduciario. Sin embargo sería considerado como una evolución en el uso del mismo. Con esto quiero decir que en el dinero electrónico intrínsecamente la base del valor de la moneda sigue siendo el respaldo de una autoridad superior y la creación del mismo sigue teniendo la

misma fuente, es decir los bancos. La unidad de medida y de valor tampoco cambia ya que sigue siendo esa moneda fiat anteriormente creada. Por lo tanto es una adaptación de ese dinero fiduciario a la sociedad actual y los medios disponibles pero sin un cambio en la naturaleza del activo que representa el dinero.

La evolución real del dinero fiat se encuentra en la llamada moneda Digital. Con una introducción de la tecnología en nuestras vidas cada vez más profunda sería lógico que el dinero acabará adaptándose a esta nueva sociedad en la que vivimos. Siguiendo este proceso histórico ya existen varias formas de activos completamente digitales que aspiran a constituir en sí mismos una moneda. Este es el caso de Bitcoin y de otras muchas monedas basadas en datos y programación informática. Las mayores diferencias de este nuevo tipo de moneda están en su fuente de creación y en el hecho de que estas monedas no están controladas por ningún tipo de banco central o estado. Su emisión recae en la propia comunidad que mediante la resolución de problemas algorítmicos da soporte a las transacciones de la red al mismo tiempo que generan dinero de nueva creación. El valor de esta moneda, como los derechos sobre los Fei de la isla de Yap, se encuentra en la general aceptación del mismo. Y volviendo a la definición tradicional de dinero de Robbins, "…el dinero es evidentemente un medio de compra final… es obvio que el dinero es en sí mismo es tan sólo un medio: un medio de cambio, un instrumento de cálculo."[4], podemos comprender que la moneda digital no aspira a ser nada más que un medio de cambio.

En posteriores apartados analizamos las características y naturaleza del Bitcoin, a fin de concluir sobre el carácter de este tipo emergente de moneda y su posible futuro en la sociedad.

3. Presentación del concepto del BITCOIN

¿Qué es realmente el Bitcoin?

> Para comprender lo que es el Bitcoin hay que empezar por decir que se trata de una moneda digital. Esto dista conceptualmente de una moneda almacenada electrónicamente, como el dinero electrónico que hemos visto en el anterior apartado. Por ejemplo, el dinero que cada uno de nosotros tenemos almacenado en el banco es una moneda almacenada electrónicamente, Bitcoin es completamente distinto.

La moneda digital no es más que un código binario referente a las transacciones producidas, y que se conserva en una base de datos. De esto se deriva la primera gran característica de la moneda digital, no existe en ningún tipo de formato, no existe algo a lo que poder referirse y denominar como un bitcoin. Este concepto de no existencia es algo que no tiene comparación con lo conocido hasta hoy en día y que es crucial para entender la naturaleza de esta moneda.

Lo único que existe es un registro público de todas las transacciones producidas y las diferentes cuentas de los usuarios a las que refieren esas transacciones. Basándose en las transacciones procesadas en la red el sistema determinará cuántos bitcoin “tiene” cada cuenta de usuario. Esta base de datos donde se registran todos los movimientos producidos es la llamada Cadena de Bloque, de la que hablaremos más adelante.

Esto implica que la base de esta nueva forma de dinero digital se sitúa en la red, si esta red sufre cualquier fallo o deja de existir el Bitcoin dejaría de existir. Pero esto tiene grandes ventajas desde un punto de vista práctico. Un gran peligro de una moneda digital la cuál realmente esté representada por un código o programa es su fácil falsificación y reproducción. Bitcoin al existir solamente como una combinación de información de transacciones evita la amenaza de la falsificación. La única forma de realizar un ataque sería modificar las transacciones registradas en la Cadena Bloque, pero como veremos más adelante una serie de mecanismos evita este tipo de situaciones.

Un único Bitcoin es denotado como 1 BTC y dado su naturaleza digital puede ser dividido hasta alcanzar hasta 8 cifras decimales. Esto significa que la mínima cantidad de bitcoins que se puede poseer es 0.00000001 BTC, que como homenaje al creador se conoce como un Satoshi[15]. De esta forma las demás divisiones posibles también tienen su propia denominación:

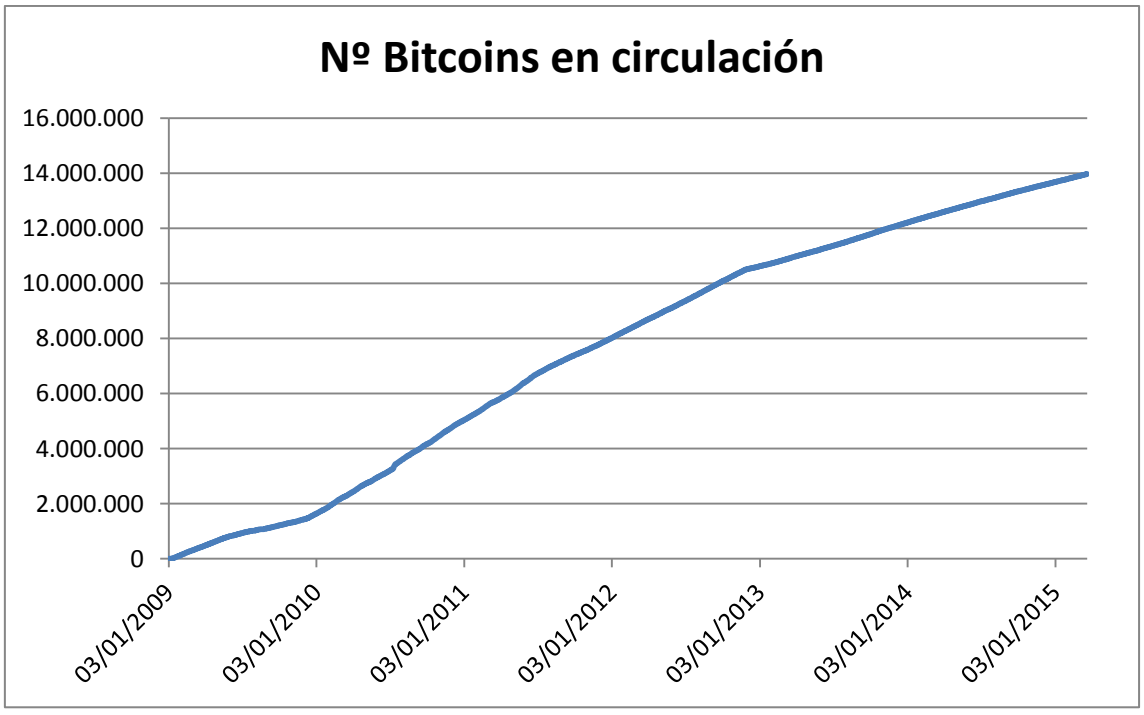
1 BTC	A bitcoin
0.01 BTC	A bitcent
0.001 BTC	An mbit
0.000001 BTC	A ubit
0.00000001 BTC	A satoshi

¿Cómo se crean los Bitcoin y como se regula su cantidad en el mercado?

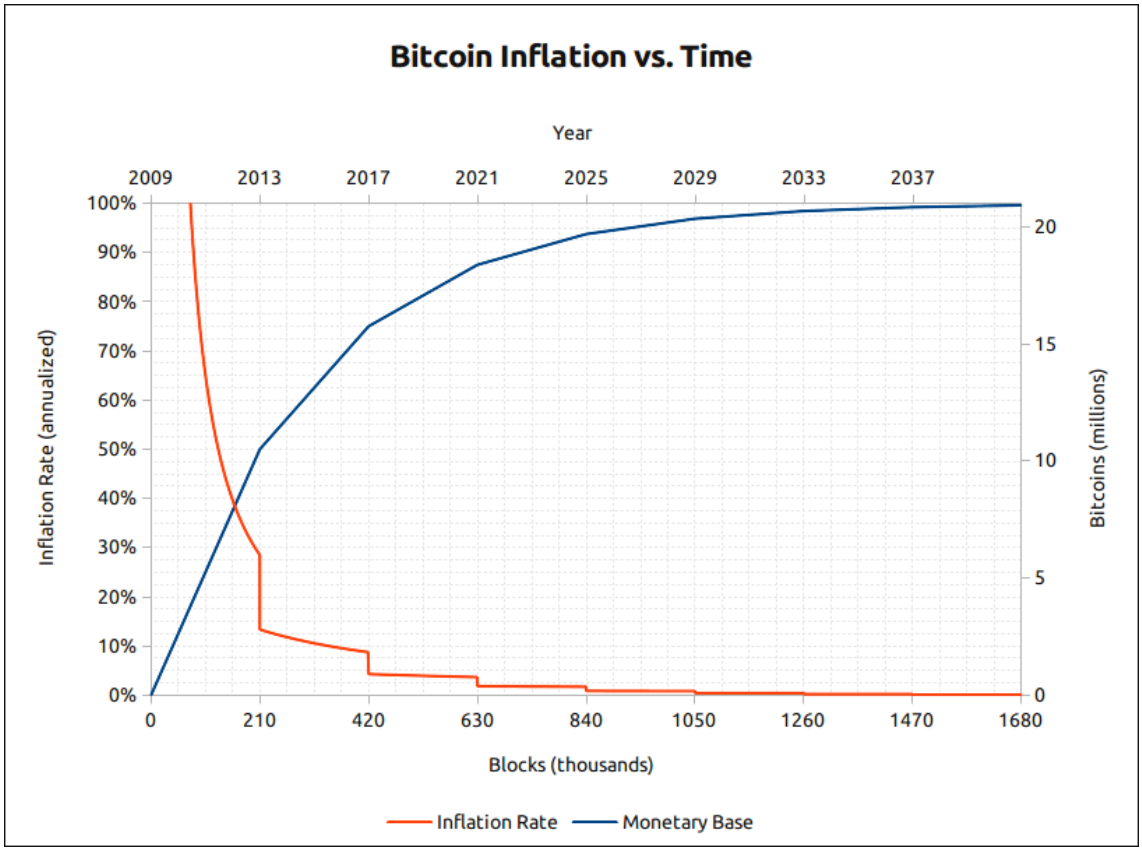
Técnicamente son creados de la nada. Son producidos por el software que controla el sistema basándose en unos algoritmos, para ser posteriormente distribuidos entre los usuarios que han posibilitado el procesamiento de información.

Un minero de Bitcoins es la persona que mediante un programa informático aporta la capacidad de procesamiento de su ordenador personal para el funcionamiento de la red a cambio de la posibilidad de obtener una cierta cantidad de Bitcoins de nueva creación. Lo único que se necesita para formar parte de este grupo es la descarga del programa informático "cliente Bitcoin completo"[16]. Este programa produce la unión de forma remota del ordenador a una red y lo convierte en un nodo de la misma. La capacidad de procesamiento de este ordenador será utilizado para la resolución de algoritmos relacionados con la verificación de transacciones producidas en la red. Basándose en la velocidad y número de algoritmos resueltos correctamente el sistema asignará unos Bitcoin de nueva creación a los diferentes mineros[16]. Este sistema además de estar diseñado como una forma de producir un flujo constante de Bitcoins en el sistema es además una forma de asegurar que toda la red es sostenible mediante sus propios usuarios.

De esta forma es como el Bitcoin realiza la inyección de dinero en el sistema, pero este sistema en un principio plantea un problema. A medida que el Bitcoin se volviera popular y la participación en el sistema aumentará, la cantidad de bitcoins creados crecería exponencialmente devaluando últimamente su valor. Sin embargo cuando se diseñó el software del Bitcoin se especificó que solo se podrían crear 25 millones de bitcoins y que los algoritmos necesarios para producirlos tienen una dificultad proporcional a la cantidad de bitcoins ya existente en el mercado[15]. La cantidad de 25 millones fue aleatoria y acorde con los cálculos de Satoshi Nakamoto, creador del Bitcoin, la creación se reduciría a la mitad cada cuatro años, con 10.5 millones en 2013, 5.25 millones en 2018, 2.625 millones en 2023 y así sucesivamente[11].

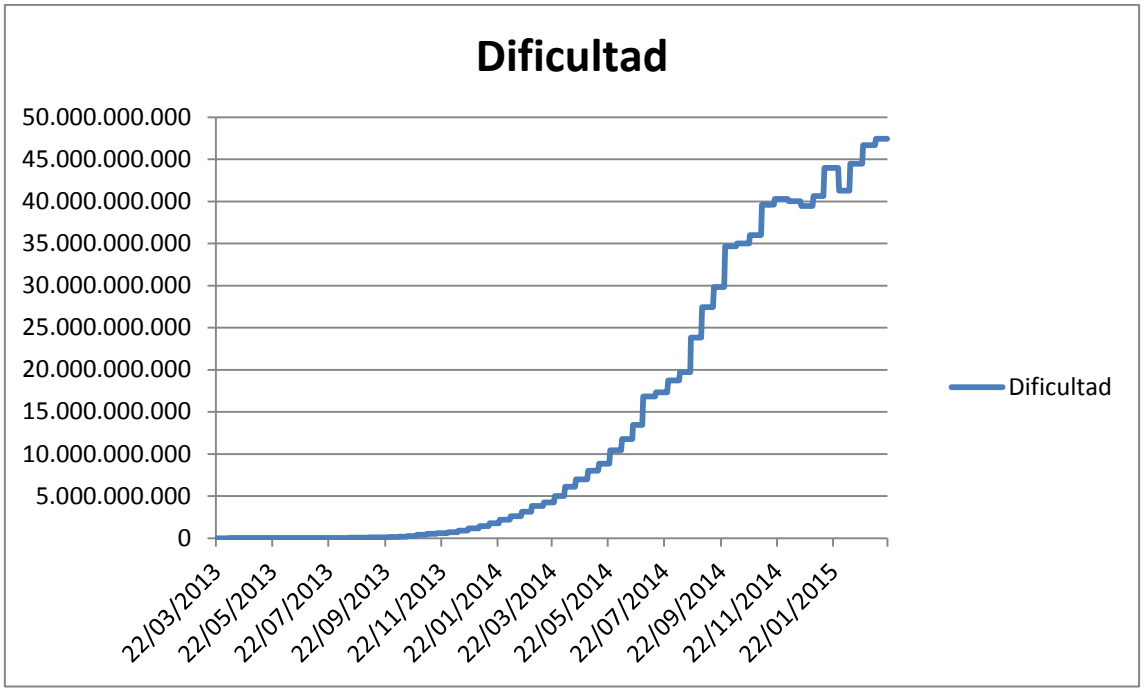


Nº de Bitcoins en circulación. 2009-2015 (con medias de 7 días). Fuente: Blockchain.info



La repercusión del alcance de este límite es de gran importancia en el Bitcoin. En el máximo los mineros ya no tendrían el incentivo para soportar al sistema y por lo tanto se paralizaría o necesitaría de una tercera entidad que lo soportará. Por lo tanto en el muy largo plazo se ha considerado posible una modificación del límite de bitcoins en circulación. Estas posibles ampliaciones tienen como objetivo asegurar la permanencia de este sistema.

Desde un punto de vista de unidad de cuenta, aunque el suministro de Bitcoins se reduzca drásticamente su habilidad para ser utilizado como moneda no se reduce. Al ser digital puede el Bitcoin puede llegar a ser dividido hasta nueve decimales facilitando su intercambio en cualquier cantidad. Esto le permite asumir apreciaciones, debidas a la escasez, recurriendo a la utilización de divisiones cada vez menores del Bitcoin.



Dificultad de la resolución del problema Hash. 2013-2015 (con medias de 7 días). Fuente: Blockchain.info

Como podemos ver en la gráfica la dificultad de conseguir un bitcoin con el tiempo aumentará y la aportación por parte de los mineros tendrá que ser proporcionalmente mayor. Es fácil caer en la concepción de que estos mineros al prestar sus procesadores no incurren en costes para la obtención de los bitcoins. El uso del procesador del dispositivo con la consecuente reducción de la vida útil y el coste de electricidad en la que se incurre son algunos de los costes asociados. Esto implica que los mineros solo aportarán su colaboración si el valor del Bitcoin es superior a los gastos en los que tienen que incurrir. En el largo plazo esto irá desplazando a los particulares en favor de las empresas que lo realicen a gran escala debido al decreciente margen obtenido con el tiempo.

Un ejemplo de este cambio hacia una dedicación industrial en la generación de Bitcoins lo tenemos en Changcheng, una pequeña ciudad en china donde se ubica el 3% de la capacidad de procesamiento de bitcoins mundial. Jin Xin, y tres personas más son propietarios de cuatro instalaciones completamente dedicadas a la obtención de bitcoins, las llamadas minas de Bitcoin. En el interior de una mina de bitcoins alojada en antigua fábrica se

puede encontrar una espectacular infraestructura de servidores, cientos de ventiladores y hasta camas para dormir. Estos servidores están funcionando 24 horas al día y siete días a la semana por lo que necesitan de supervisión constante por parte de los trabajadores que habitualmente viven en estas minas. Cada una de estas instalaciones es capaz de hacer unos 4.050 bitcoins al mes, valorados en unos 1,3 millones de euros, todo esto con un coste de electricidad mensual de 100.000 dólares y el deterioro de la gran infraestructura necesaria. Con el tiempo este ratio irá disminuyendo pero el aumento en sus economías de escala les permitirá asumir este crecimiento de la dificultad[17].

La realización de transacciones y el almacenamiento del Bitcoin

Como hemos visto anteriormente las transacciones producidas y documentadas en la Cadena Bloque son la base de todo el sistema del Bitcoin. Al no existir en ningún tipo de formato independiente toda transacción se tiene que realizar de una cuenta de cliente a otra, estas cuentas son denominadas carteras. En resumen, estas carteras actúan como cuentas bancarias desde las cuales se producen las transacciones.

Una cartera de Bitcoins es un archivo informático encriptado que contiene unas líneas de código representativas del mismo. Para comunicarte e identificar las carteras se utiliza una llave pública que es única para todas las carteras, está diseñada con una forma y longitud que garantiza su infinidad [16]. Esta llave publica es un análogo del IBAN de las cuentas bancarias actuales. Cada cartera además de tener esta llave pública también cuenta con una llave privada que actúa a forma de código de autorización para realizar transacciones desde tu cartera, de la misma forma que el PIN de una tarjeta de crédito.

Para la realización de una transacción se necesita de la llave pública de la cartera a la que se quiere enviar los bitcoins. Después se utiliza la llave privada para autorizar la transacción. En este momento se transmitiría la transacción a la Cadena Bloque donde sería verificada por los nodos de la red conformados por mineros. Todo este proceso puede llevarse a cabo sin la

necesidad de una tercera parte en la transacción, actualmente representada por los bancos. Este proceso de elaboración de las transacción y verificación de las mismas lo veremos en más detalle en el apartado dedicado a la Cadena Bloque.

Esta forma de procesar transacciones también proporciona al Bitcoin otra de sus características principales, la privacidad. El Bitcoin es considerado una forma de intercambio Pseudoanonima[11]. Esto significa que aunque la transacción es publicada en la Cadena Bloque no es posible unir las direcciones de las carteras con identidades personales ni con otras carteras de mismo propietario.

De lo expuesto anteriormente se puede deducir que el almacenamiento del Bitcoin se reduce al almacenamiento de las llaves que componen una cartera. La llave privada de la cartera es el elemento más importante de la misma ya que su pérdida inutiliza la cartera. La seguridad de cada usuario en el sistema del Bitcoin reside en gran medida en las formas utilizadas para el almacenamiento de las llaves.

Brevemente mencionaré dos formas de guardar estas claves. La primera se lleva a cabo utilizando una cartera caliente lo que significaría que las dos claves tendrían contacto directo o indirecto con internet. Un ejemplo de esto son las carteras gestionadas por empresas online que ofrecen estos servicios. Esta es la forma más cómoda de almacenar una cartera pero implica un gran riesgo de ataque informático. Frente a este tipo de almacenamiento existen las carteras frías donde se almacenan los datos de la cartera en dispositivos sin conexión con internet[18]. Este método es mucho más seguro, aunque también vulnerable ante robos físicos o simples pérdidas de las claves. Donde la mayor parte de la gente se sitúa es en una combinación de ambos métodos. Utilizan una cartera caliente con pocos fondos para realizar la mayoría de las transacciones y acumula su cantidad principal en una cartera fría con varios niveles de seguridad.

Como podemos ver, esta forma de gestión del almacenamiento del dinero, al igual que la gestión de las transacciones, deja fuera de lugar a la necesidad de un tercero. Aunque, como hemos mencionado brevemente, en la práctica se ha dado la proliferación de terceros que faciliten todos estos procesos (las carteras calientes). Este es el caso de los Patios de comercio.

Estos Patios de comercio de Bitcoin son empresas que actúan como plataformas de almacenamiento de llaves de carteras de Bitcoin y como mercado de compra y venta de bitcoins. Su surgimiento responde a la gran facilitación del proceso que suponen y por su interfaz atractiva de cara a un público menos formado en aspectos informáticos. Algunas de las principales firmas serían las siguientes: Mt.Gox, Bitstamp o MyBitcoin. Al mismo tiempo que han ofrecido grandes eficiencias al sistema también han proporcionado debilidades al mismo. La más relevante de ellas, como ya veremos posteriormente, es el riesgo de fraude por parte de estas terceras partes que no se encuentran reguladas por una entidad superior. Dos de las entidades mencionadas anteriormente ya se han declarado en bancarrota debido a sendos ataques informáticos a sus servidores, provocando cuantiosas pérdidas a todos sus usuarios. Estas entidades son: Mt. Gox con unas pérdidas de $500.000.000 y MyBitcoin [15].

¿Cómo funciona la cadena de bloques?

La cadena de bloques es la innovación más importante y el elemento clave del Bitcoin. La cadena de bloque mantiene una lista segura de todas las transacciones que se han producido en la historia del Bitcoin y basándose en ellas se determina la cantidad de bitcoins que atesoran las carteras.

Para una compresión más completa de la cadena de bloque es necesaria la exposición de tres conceptos técnicos clave, sin entrar en demasiado detalle. Estos son: Las funciones Hash, “time-stamp” y “proof-of-work”.

Una función hash es un algoritmo que recoge información de una determinada longitud y la procesa para generar un resultado de una longitud estandarizada, llamado el valor hash. Estas funciones hash son comúnmente

utilizadas en el mundo de la informática para manejar gran cantidad de información y poder buscar cierta información. Para una misma información recibida solo existe una posible información obtenida, el valor hash siempre será el mismo[16].

El Bitcoin utiliza estas funciones hash para la verificación de las transacciones así como para la identificación de las mismas. Si bien existen ciertas restricciones a estas funciones hash en su sistema. La función hash tiene que ser de una dirección lo que implicaría que teniendo el resultado no se puede obtener el origen, para garantizar el carácter pseudo-anónimo del Bitcoin. Y una misma información obtenida no puede tener el mismo valor hash que otra y además para garantizar la verificación de cada una de las transacciones no se puede permitir la entrada de dos informaciones coincidentes[16].

Un time-stamp digital es una prueba que identifique a un documento digital en un momento determinado del tiempo. Sus aplicaciones son muy numerosas, al igual que sus equivalentes físicos, desde documentar un contrato a certificar una transacción producida electrónicamente. La utilidad concreta en el Bitcoin es la de aumentar la seguridad de las transacciones. En el momento de la verificación, como veremos más adelante, se comprueba la fecha de la transacción como parte del proceso.

Por ultimo tenemos el proof-of-work, un protocolo de verificación de todas las comunicaciones de los clientes con el servidor. Primero el cliente se pone en contacto con el servidor para recibir el servicio, entonces el servidor propone un problema que debe resuelto por el cliente. Por último el servidor verifica que el problema ha sido resuelto correctamente por el cliente y autoriza el acceso al servidor[16]. Una de las ventajas de este método es su dificultad adaptable, habilidad que el Bitcoin utiliza para regular la producción de dinero en el tiempo, como hemos visto anteriormente.

Bitcoin combina todas estas ideas para conseguir una base de datos segura y pública, como es la cadena de bloques. Esta cadena de bloques está

compuesta por una sucesión de bloques que están conectados entre ellos. Las nuevas transacciones que se producen en el sistema se juntan en bloques que se añaden a partir del último bloque de la misma. La seguridad de esta cadena de bloque está garantizada por el protocolo de Proff-of-Work , que se aplica a toda la longitud de la cadena. Esto implica que para realizar un cambio en la cadena se tiene que aplicar un poder de procesamiento equivalente al todo el aplicado para verificar la cadena hasta el momento. Básicamente se trataría de tener que crear una cadena alternativa[16]. Esto es materialmente imposible ya que la cantidad de procesamiento necesario es demasiado costosa y materialmente muy difícil. Esto garantiza un sistema libre de manipulación y, por lo tanto, la seguridad del Bitcoin como sistema.

Volviendo al proceso de minería del Bitcoin podemos ver cómo funciona el proceso de la cadena de bloques. Primero la publicación en la red de una serie de transacciones de bitcoins que son captadas por los mineros y agrupadas en bloques sobre los que posteriormente se realizarán los trabajos de verificación. Una vez un bloque de transacciones ha sido verificado se añadire a la cadena de boque y el minero que haya realizado el proceso recibe la correspondiente recompensa en bitcoins de nueva creación.

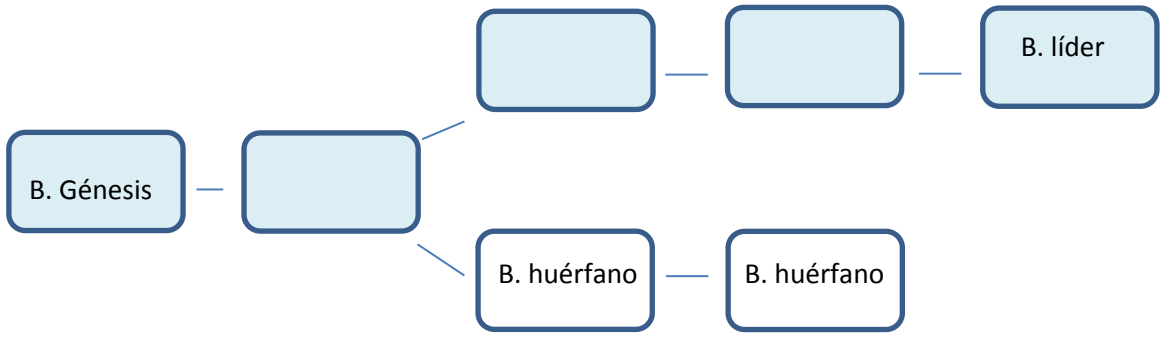
Cada bloque de la cadena está asegurado por el proceso llamado “Partial Hash Inversion Proof-of-Work”[16]. En el momento de creación del bloque se le asigna un número que lo identifique y se produce un time-stamp para el mismo. A continuación se recoge la información del último bloque de la cadena y se utiliza una función hash sobre la misma. Con todo lo anterior se crea una variable llamada “nodo”. Este nodo del bloque es el que resuelve la función hash parcial inversa. En la resolución de este problema son los mineros quienes aportan mayor valor a la red de Bitcoin. Cada bloque necesita de la obtención de un resultado determinado de la función hash para que el servidor garantice el acceso, el ordenador seguirá generando nodos hasta la consecución de la solución al problema del proof-of-work.

Cuando se obtiene el bloque con el hash adecuado se publica en la red de Bitcoin, en el servidor. En este momento el trabajo de un minero en

particular se transfiere para la revisión por parte de otros integrantes de la red. Se comprueba que consta con las principales partes necesarias. Esta son: Un time-stamp reciente, que el bloque propuesto realmente este basado sobre el último de la cadena y que todas las transacciones que componen el bloque son válidas en sí mismas[16].

Una vez que el bloque es comprobado se empieza a trabajar sobre los siguientes y ya formaría parte de la cadena como el último de la misma. El minero que haya utilizado su capacidad de procesamiento para obtener este bloque "correcto" recibirá la recompensa.

El bloque que es tomado como predecesor del procesado se llama "bloque padre". El primero de todos ellos es el llamado "bloque génesis" creado por Nakamoto, inventor del Bitcoin. Y el último de los bloques en la cadena se llama el "bloque líder". Pero esto no significa que la cadena bloque sea completamente lineal, en ciertos casos el procesamientos de bloques falla generando dos caminos a partir de el "bloque líder". Rápidamente el sistema condena uno de esos dos caminos dejando atrás los llamados "bloques huérfanos"[16].



Fuente: Elaboración propia

Esta situación es lo que se denomina un tenedor en la cadena y surge cuando dos mineros llegan a un mismo bloque a la vez. Ambos resolverían el problema hash pero solamente uno de los bloques generados podrá llegar a ser parte de la cadena. Este error puede conducir a dos caminos en la cadena durante un número de bloques antes de que condene uno de ambos. Sin embargo esto no significa que las transacciones que forman parte de los

bloques huérfanos caigan en el olvido sino que el sistema las añade de nuevo a la piscina de transacciones pendientes de resolución.

La red de Bitcoin actualmente procesa 110 mil transacciones diarias, 1.5 segundos por cada transacción de media[16]. Los críticos señalan que este método no sería capaz de manejar el volumen de transacciones que actualmente procesan MasterCard o Visa. Sin embargo, un aumento en las transacciones procesadas en el sistema del Bitcoin estaría emparejado con un aumento en la capacidad de procesamiento aportada por sus usuarios.

En el anexo se puede ver todo el proceso necesario desde que se reclama una transferencia por parte del cliente hasta que está realmente pasa a formar parte de la Cadena Bloque.

Incubación y nacimiento del BITCOIN

El Bitcoin surgió en un foro de internet donde por primera vez, el supuesto creador, Satoshi Nakamoto publicó un mensaje anunciando el nuevo avance en el que había estado trabajando años. El contenido del foro era científico conformado por una comunidad académica principalmente matemática e informática, metzdowd.com, el lugar perfecto para introducir este tipo de moneda revolucionaria basada en la informática y la matemática. El 31 de Octubre de 2008 fue el día elegido por Nakamoto para publicar el comentario titulado: “Bitcoin P2P e-cash paper”. El contenido del mensaje era el siguiente: “He estado trabajando en un nuevo medio de pago electrónico que es completamente PEER TO PEER, sin necesidad de contar con una tercera parte como intermediario. El ensayo está disponible en: http://www.bitcoin.org/bitcoin.pdf” [19].

Este documento de estilo académico describe todos los detalles de la nueva forma de moneda que Nakamoto había diseñado, el Bitcoin. No es un documento de fácil lectura ya que implica gran número de cuestiones técnicas como son: la forma de las transacciones, la seguridad, la generación del Bitcoin y la privacidad ofrecida por este sistema desde un punto de vista técnico. Además de estas cuestiones técnicas, Nakamoto también expone su

preocupación sobre cómo el desarrollo tecnológico había superado con creces al desarrollo financiero. Esta preocupación se centra en la figura de los bancos como entidades que ya no facilitan las transacciones en el mercado sino que se han convertido en un intermediario necesario que las ralentizaba. Así como una institución que representa un riesgo sistémico en la economía.

En palabras del propio 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 dispuestas realizar transacciones directamente sin necesidad de un intermediario.”[19.]

Esto representa el mayor avance propuesto por esta nueva forma de dinero digital, la eliminación de la confianza necesaria en una entidad emisora. Como ya hemos visto el Bitcoin es generado mediante la matemática y con la capacidad de ser totalmente operado por los usuarios. Esto implica que únicamente necesita de una aceptación general de su carácter como medio de cambio universal para poder operar.

Después de la publicación se supo que el trabajo de Nakamoto había comenzado un año atrás en 2007 en los principios de la crisis financiera[15]. Si vamos atrás en el tiempo y nos situamos en el 2007 podemos ver los primeros signos de que una parálisis del sistema financiero a nivel mundial. Las agencias de crédito ya empezaron a alertar sobre el riesgo presente en un gran número de hipotecas y se empezaron a producir los primeros rescates de bancos como el de Northern Rock en Inglaterra[15] y así una sucesión de acontecimientos que llevaron al público a un despertar amargo sobre la realidad financiera. En medio de esta tormenta es cuando Nakamoto se propuso crear esta nueva moneda”…basada en un sistema despojado de la necesidad de la confianza y de terceros agentes.”[19]. Con esto pretendía evitar en un futuro uno de los mayores problemas que represento la crisis financiera como son la quiebra y rescate de las entidades financieras.

Esta red estaría regulada últimamente por los distintos usuarios que participan en la misma. No contaría con un organismo regulador y por lo tanto

no se podría manipular mediante la política monetaria de los distintos países. Si vamos a las raíces de este razonamiento podemos unirlo con una forma de capitalismo liberal en la que el sistema no depende de un órgano regulador sino del interés personal de los usuarios. En uno de los intercambios de mensajes en los foros Nakamoto mencionaba el 14 de Noviembre de 2008: "Es un concepto muy atractivo desde el punto de vista liberal si se puede explicar adecuadamente, sin embargo soy mejor con el código que con las palabras."[19].

Además de este objetivo de superar las entidades financieras como intermediarios también había una motivación por la lucha de la libertad y privacidad. Esto es el anteriormente mencionado carácter pseudo-anónimo del Bitcoin. En uno de los comentarios de Nakamoto decía literalmente: "…podemos ganar una gran batalla en la carrera y ganar un nuevo territorio de libertad por muchos años"[19]. Estos ideales concuerdan con la escuela de pensamiento cypherpunk que defiende la privacidad y libertad como algo sagrado sobre cualquier otra cosa y utiliza como medio la tecnología.

Después de unos meses Nakamoto hizo honor a su promesa de sacar a la luz una versión en funcionamiento, pero aún con las características de un producto en desarrollo. De esta forma el 8 de Enero de 2009 se publicó en metzdowd.com una entrada titulada "Bitcoin v0.1 released"[15]. El mensaje que se podía leer en la web era el siguiente: "Anuncio el primer lanzamiento del Bitcoin, un nuevo sistema de moneda digital que utiliza un sistema completamente peer-to-peer…. Es un sistema completamente descentralizado sin ningún organismo o autoridad central…"[19].

Este programa se encontraba aún en fase experimental y permitía actualizaciones según fueran necesarias. Además de cuestiones técnicas este primer lanzamiento se topó con una cuestión crucial para el establecimiento y triunfo del Bitcoin. Dustin Trammel, un investigador de seguridad tecnológica en Austin, Tejas mencionaba: "El verdadero problema será conseguir individuos para realmente conseguir valor en el Bitcoin y pueda convertirse en moneda"[15]. Ya que el Bitcoin, al contrario que las primeras monedas como las metálicas de oro y plata, carece de un valor intrínseco y además no tiene una tercera entidad

sosteniéndolo, caso de la moneda fiduciaria. El mayor reto era conseguir un volumen suficiente de personas dispuestas a utilizarlo como para darle un valor en sí mismo como medio de cambio. A esta pregunta Nakamoto respondió: "Puede que simplemente tenga sentido conseguir unos cuantos Bitcoins en caso de que el concepto triunfe. Si suficiente gente piensa esto es posible que por sí mismo se convierta en un triunfo."[19]. Este concepto, como veremos más adelante, también acarreó uno de sus principales problemas, su equiparación con un activo de inversión en vez de una moneda de cambio.

La siguiente aparición del Bitcoin fue el 11 de Febrero de 2009 cuando alguien bajo el nombre de Satoshi Nakamoto se registró en la página P2Pfoundation.net, una comunidad esta vez dedicada concretamente a proyectos peer to peer y de un carácter más general[15]. El mismo día de registrarse publicó un link a una nueva versión del programa del Bitcoin. En este nuevo programa constaba de 31.000 líneas de código y ya contaba con los primeros Bitcoin generados en el llamado Bloque génesis, el primero de los bloques creados destinado a empezar la cadena de bloques. Además, este primer bloque contiene un mensaje oculto entre las numerosas líneas de código, este dice: "The Times 03/Jan/2009 Chancellor on brink of second bailout for Banks"[19]. Este mensaje hace referencia a una noticia de The Financial Times en la que se advertía de la necesidad de billones de dólares para el rescate bancario[20]. Con esto se intentaba revindicar el motivo por el cuál empezó el Bitcoin, la eliminación de los intermediarios financieros que suponen un riego a la economía.

En este nuevo lanzamiento del Bitcoin el discurso técnico del primer foro es sustituido por un discurso más retórico centrado en el idealismo detrás de la moneda. Particularmente se ataca a la moneda fiat y la banca de reserva fraccional para atraer a todos aquellos descontentos con la situación propiciada en la crisis financiera. Dicho discurso sostenía en primer lugar que con la moneda fiat los gobiernos ganaban un gran poder sobre el mundo financiero, ya que ellos eran los que tenían el control sobre la cantidad de dinero en circulación, y que esto era negativo para el valor de la moneda y el consumidor.

Además, la base del valor de la moneda fiat reside en la confianza depositada en el gobierno, lo que la hace vulnerable a pérdidas de confianza en el mismo. En segundo lugar atacaba a la banca de reserva fraccional que permite a los bancos prestar 10 veces la cantidad de dinero que realmente tienen en sus cuentas. Esto hace que la economía crezca a un ritmo acrecentado debido al apalancamiento pero es susceptible de quiebra si se produce una retirada de fondos de los bancos. Y si esta quiebra se produjese los bancos constituirían una figura de obligado rescate debido a su posición en el sistema de creación de dinero y ahorro.

En una serie de comentarios publicados por Nakamoto en la página de P2P foundations se puede leer: “El principal problema con la moneda tradicional es que la confianza es indispensable para hacerla funcionar….El banco central necesita ser depósito de confianza para no devaluar la moneda, pero en la historia se pueden ver varias ocasiones donde se han producido rupturas de esa confianza. Los bancos necesitan ser de confianza para custodiar nuestros ahorros y transferirlo electrónicamente, pero son capaces de prestar el dinero en forma de burbujas de crédito sin tener prácticamente una fracción en reserva. Tenemos que confiar en ellos para mantener nuestra privacidad, confiar en que ellos eviten que nuestras identidades sean robadas y nuestras cuentas vaciadas. “19.

Ante estos problemas expuestos Nakamoto situaba al Bitcoin como la solución. Este supondría la eliminación de terceros, una desconexión de la confianza necesaria con entidades reguladoras y una garantía de la privacidad e independencia de los usuarios. En estos primeros meses el éxito de la segunda versión de Bitcoin fue limitado, llegando solamente a unas 60 descargas semanales [11]. Sin embargo, una corriente de expertos en distintas áreas acudieron a Nakamoto con la intención de aportar su ayuda y colaborar en el proyecto con sus conocimientos. Entre estos se encontraban Mike Hearn, un ingeniero de Google en Zúrich, Suiza, Jon Matonis, director ejecutivo de una empresa consultora de pagos electrónicos, Lydia Group, y Hal Finney un programador con mucho renombre que participo en los primeros proyectos del

código PGP[15]. Estas adiciones al proyecto ayudaron a superar los fallos y agujeros que tenía el programa. Uno de los más valiosos contribuidores fue Gavin Andersen, un habilidoso programador crucial en la resolución de los problemas de código. En una entrevista reconoció que el código de Nakamoto es rudo y poco sutil [15].

Con estas adiciones al proyecto fueron numerosos los intentos por averiguar más cosas sobre el misterioso Satoshi Nakamoto del que aún no se conocía ningún tipo de detalle. Pero Nakamoto evadió todo intento por reconocerle o saber cualquier tipo de detalle sobre él, solo se comunicaba con sus colaboradores vía email o en foros públicos.

Con el tiempo Nakamoto pasó de ser el líder del movimiento a ocupar un segundo plano. El código del programa original había sido completamente rediseñado y estaba siendo constantemente controlado por un équido de desarrolladores altamente cualificados. En abril de 2011 Nakamoto en una nota a esos desarrolladores decía: “Me voy a ocupar de otras cosas”[19]. Después de este mensaje de despedida no se supo nunca nada más de él. De todas formas, el proyecto estaba vivo teniendo como cabeza visible a Andresen[15].

Un mes después de estos eventos se produjo una masiva explosión de popularidad del Bitcoin y las descargas experimentaron un crecimiento sin precedentes. En el Mayo de 2011 se produjeron 174.184 descargas y en el mes siguiente 329.229 [15]. El Bitcoin estaba viendo la luz.

Alrededor de esta explosión del Bitcoin surgieron plataformas online que facilitaban las transacciones para hacerlas accesibles a todo tipo de público. Estos serían los primeros patios de comercio de Bitcoin mencionados anteriormente. El primero en surgir fue BitcoinMarket.com en febrero de 2010[15], seguido de Mt.Gox. En estas primeras fases se percibía la novedad del concepto y su exposición limitada a ciertos círculos de la población.. Se producían reportes constantes de fallos en el sistema, transacciones fallidas, cuentas comprometidas entre otras dificultades que alejaban al público general del Bitcoin.

Con el tiempo la popularidad de esta nueva y novedosa forma de concebir la moneda capto la atención de otro tipo de público que vio gran potencial en su privacidad y se empezó a utilizar con fines de encubrimiento de fondos ilegales y transacciones de dudosa legalidad. En aquel momento Mt. Gox ya había procesado transacciones de Bitcoin por valor de un millón de dólares[15]. Una nueva página web llamada Silk Road empezó a operar aceptando únicamente Bitcoin como pago, esta página contaba todo tipo de drogas y demás productos ilegales a la venta. Debido a que las transacciones de Bitcoin son pseudo anómimas no se puede perseguir a quien hace o recibe el pago. Este lado oscuro del Bitcoin atrajo la atención de las entidades reguladoras de los distintos países y, como veremos en un apartado posterior, propició la regulación del mismo en distintos aspectos[21].

A pesar de estos problemas el Bitcoin siguió su camino de crecimiento llegando a la paridad con el dólar en Febrero de 2011[11]. La comunidad financiera empezó a verlo como una inversión con el potencial de grandes rentabilidades en el corto medio plazo. Un hecho que favoreció la imagen del Bitcoin como alternativa viable, y de inversión rentable, fue la utilización del Bitcoin para la financiación de WikiLeaks. Cuando se produjo el escándalo de Wikileaks todas las grandes empresas de pago electrónico como PayPal, Master Card o Visa negaron las donaciones realizadas hacia la organización[15]. En este momento el Bitcoin surgió como una opción alternativa de traspaso de dinero que no podía ser controlada y que era confiable, esto probó a la sociedad la funcionalidad del sistema. Un ejemplo de esta atención financiera es la entrada en el Bitcoin de los hermanos Winkelvos que han formado el primer trust basado en el Bitcoin. Este trust se encuentra en procesos legales de aprobación y supondría la cotización del Bitcoin en los patios de Wall Street[24].

Aunque se produjo crecimiento en su popularidad el mundo del Bitcoin seguía siendo peligroso sino se tomaban las precauciones necesarias o se carecía del conocimiento necesario para protegerte. Muchos vieron la

oportunidad de aprovecharse de la situación de gente entrante sin conocimientos para realizar todo tipo de trucos, engaños y estafas.

Una página llamada MyBitcoin llegó a tener una importante cuota de mercado de transacciones de Bitcoin en 2011, principalmente debido a que contaba con una interfaz atractiva y fácil de usar que atrajo a los curiosos y nuevos en el mundillo. En el verano de 2011 MyBitcoin anunció que había sido atacado por hacker y se había producido un robo de 154.406 bitcoins. Hechos que produjeron el cierre de la página[15]. El valor de estos bitcoins en el mercado eran de 2 millones de dólares y todos los usuarios que habían depositado sus bitcoins, la custodia de sus carteras, en esta plataforma habían perdido todo. Al no existir ningún tipo de entidad reguladora no existía ningún tipo de seguro frente a esas pérdidas ni vía legal de reclamación.

En este punto cabe preguntar si realmente se produjo un robo o fue la propia empresa la que surgió con el mismo fin de desaparecer. Muchos de los clientes denunciaron a los cuerpos judiciales pero debido al carácter opaco de la organización y del Bitcoin ninguno tubo éxito. La cabeza y fundador de MyBitcoin era Tom Williams, identidad electrónica que podía ser distinta a la real, y del cual no se volvió a saber [15]. En definitiva, la gente había confiado su dinero a un tercero totalmente desconocido y anónimo, todo ello pese a que el Bitcoin se creó con la idea de eliminar estos terceras intermediarios en las transacciones.

De esta forma el Bitcoin surgió de un foro de matemáticos e informáticos hasta llegar a captar la atención de muchos otros sectores y de una gran parte del público. Primero acudieron al programadores, cyperpunks y libertarios de distinta clase para ser seguidos por negocios ilícitos y buscadores de riqueza. Finalmente ha conseguido, y cada vez más, atraer a inversores y personas involucradas en el mundo de las finanzas. Este proyecto ha superado las barreras de su creador y ya ha pasado a ser de propiedad general. Ya no solo el Bitcoin en sí, sino también la ideología y tecnología que hay detrás representará un claro salto en el funcionamiento de la sociedad.

¿Quién es realmente Satoshi Nakamoto?

Actualmente aún no se ha esclarecido la identidad de Satoshi Nakamoto. Ni si quiera se puede precisar si es un nombre real o un alias utilizado para encubrir su identidad.

En los primeros días de Bitcoin cuando muy poca gente estaba involucrada Satoshi también actuó como minero generando alrededor de un millón de bitcoins [15]. Este millón está almacenado en ciertos números de carteras que son conocidos públicamente. Si se produjera algún movimiento en las mismas se podría intentar realizar un rastreo de las transacciones para encontrar a la persona. Pero para la decepción y sorpresa de la gente que intentaba seguir su pista estas carteras nunca recibieron o emitieron Bitcoins que pudieran revelar detalles de su identidad[15]. Este hecho resulta sorprendente ya que demuestra un gran interés por mantenerse oculto o un gran desinterés por el beneficio monetario que este número de Bitcoins le podrían aportar.

No existe una evidencia clara de quien podría estar detrás del Bitcoin. Sin embargo, el Bitcoin ya forma parte de la sociedad y la importancia de su creador ha quedado relevada a un hecho meramente histórico.

4. Definición de la verdadera naturaleza del BITCOIN

Una de los objetivos de este trabajo es concretar si el Bitcoin realmente representa una forma de dinero o si por el contrario ha de ser considerado como un activo intangible. Aunque esta discusión pueda parecer banal, ya que no afectaría a su funcionamiento, nada más lejos de la realidad. Esta clasificación del Bitcoin como una forma de dinero o no tiene un enorme impacto en los movimientos que se están produciendo por parte de los países en términos de regulación legal. La aplicación de impuestos, el control de su movimiento, la consideración de las transacciones, que carácter tienen en el patrimonio de una persona o la capacidad para utilizarlos como garantías de liquidez. Estos y otros muchos temas que determinarán en gran medida el futuro del Bitcoin están afectados por su consideración como dinero o como activo.

Como hemos visto la escuela moderna de economistas le atribuye al dinero tres funciones esenciales:

- Medio de cambio: El dinero debe de ser completamente intercambiable por bienes y servicios.
- Depósito de valor: El dinero tiene que ser capaz de transportar del presente al futuro la capacidad de compra.
- Unidad de medida: Los bienes y servicios tienen que poder ser medidos en términos de unidades monetarias.

Las principales críticas defienden que Bitcoin no cumple ninguna o alguna de estas tres condiciones que son necesarias para ser considerado dinero y por lo tanto debería considerarse como un activo intangible. En los siguientes puntos realizaremos una comparación del Bitcoin respecto a estas tres funciones fundamentales del dinero con el propósito de determinar su naturaleza.

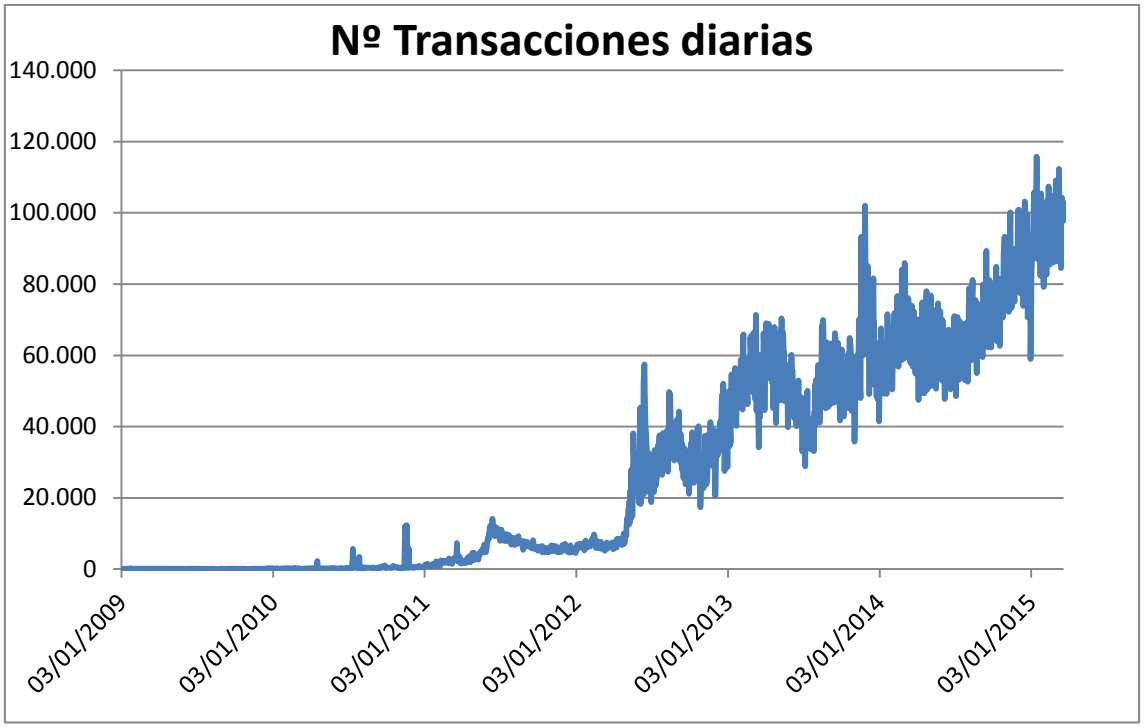
Medio de cambio

En relación con la capacidad del Bitcoin de actuar como medio de cambio existe un consenso en la comunidad económica sobre su total capacidad de cumplir esta función. Esto se ha probado a lo largo de la historia del Bitcoin a medida que su grado de aceptación se ha incrementado entre diversos negocios.

Es cierto que se ha visto un crecimiento en la aceptación del Bitcoin y se han aumentado las transacciones. De todas formas esta cifra está aún muy lejos de ser comparable con otros medios de pago como tarjetas de crédito.

	Volumen de transacciones diarias
VISA	19.000.000
MasterCard	11.000.000
PayPal	492.000
Western Union	225.000
Bitcoin	99

Número de transacciones diarias. 2014 (números en miles). Fuente: Grossman et al.



Número de transacciones diarias. 2009-2015 (con medias de 7 días). Fuente: Blockchain.info

Se puede considerar al Bitcoin como una start up. La base de clientes aún es muy pequeña y para conseguir convertirse en un medio universal necesitaría alcanzar una masa crítica. La masa crítica se conseguiría si el Bitcoin aportara un beneficio tal que logre superar las barreras que tiene la gente para cambiar su medio actual de pago. Cuando traducimos este beneficio a una moneda digital, el Bitcoin en este caso, el punto clave es la cantidad de usuarios que tiene la red antes de que un usuario entre a formar parte, es decir, la mayor posibilidad de realizar transacciones. De tal forma que el crecimiento del Bitcoin como forma de pago se prevé que sea cuadrático, debido al llamado efecto "network".

Parece existir consenso en que se puede alcanzar esta masa crítica debido a la tendencia de un crecimiento continuado en el número de transacciones de Bitcoin producidas, siendo estas actualmente ligeramente menores a 100.000 transacciones diarias. En el escenario en el que nos encontramos la tecnología tiene una gran influencia en la sociedad y el Bitcoin

aporta una evolución natural un la utilización de la tecnología a nuestra disposición para facilitar las transacciones de nuestro día a día.

De todas formas las críticas apuntan a que los grandes jugadores financieros también están apostando por formas de pago digital[22]. Esto llevaría a una confrontación directa con lo que el Bitcoin ofrece como ventaja competitiva al usuario sobre las formas de pago tradicionales. En la medida que estas acciones por parte de las entidades financieras provoquen un cierto inmovilismo hacia nuevas formas de dinero estarán afectando en gran medida la viabilidad de la expansión del Bitcoin.

Las principales ventajas que ofrecería el Bitcoin como medio de cambio serían las siguientes:

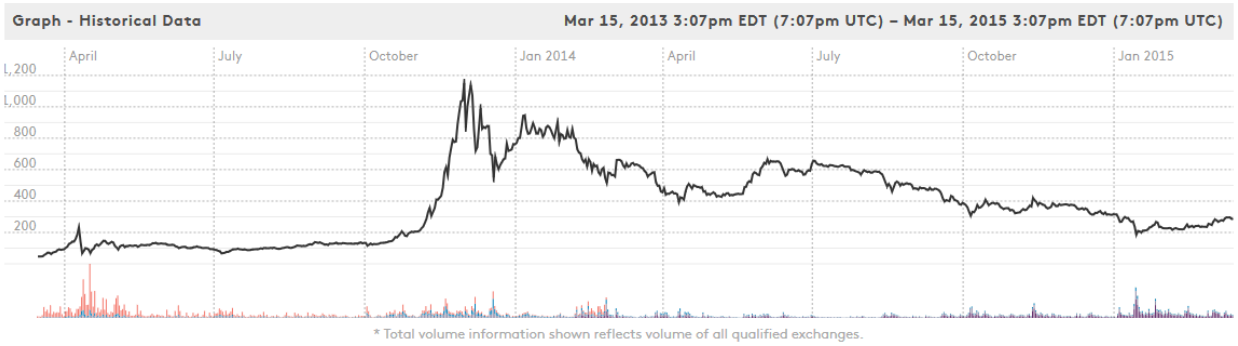
a) Costes de transacción menores a los que actualmente tienen las tarjetas de crédito. Esta condición está bajo sospecha de no ser viable en el largo plazo. El razonamiento detrás de esta afirmación reside en el coste de la minería de bitcoins y el beneficio obtenido por su realización. Según avanza el tiempo también aumenta la dificultad para realizar minería y de misma forma la cantidad beneficio obtenido se reduce (manteniendo el precio del Bitcoin como una constante). Esta reducción del beneficio por el número de transacciones procesadas llevará en última instancia a aumentar los costes de transacción para incentivar a los mineros.
b) Protección hacia los negocios del fraude de reclamación de fondos. Este fraude se produce cuando se paga un producto y posteriormente se reclama la anulación de la transacción a pesar de que el bien ha sido correctamente entregado. Con el Bitcoin este fraude no es posible ya que una vez la transacción se ha realizado no hay vuelta atrás. Esta ventaja también esconde un lado oscuro y es que disminuiría la protección de los clientes cuando el bien realmente no ha sido entregado.
c) Las transacciones serían completamente instantáneas no como las transferencias bancarias que suelen tener un retraso de dos días

hábiles. Aunque cercanas a los tiempos de ejecución de transacciones mediante tarjeta de crédito.

d) El Bitcoin no impondría comisiones base a las transacciones[23]. Esto es una gran ventaja ya que permitiría el funcionamiento de sistemas de micro pagos que facilitarían la prestación de numerosos servicios. Como por ejemplo el cobro del uso de internet en espacios públicos basado en los minutos utilizados o ancho de banda consumido.
e) Bitcoin es una forma de pago similar al efectivo donde el usuario es el que activamente tiene que generar la transacción y enviarla[23]. Sin embargo, las tarjetas de crédito funcionan de forma que el usuario entrega la autorización al vendedor para realizar la transacción. Esta sutil diferencia puede representar una gran protección ante el fraude y la realización de transacciones no deseadas por parte del vendedor.

De la misma forma los principales inconvenientes del Bitcoin como medio de cambio serían los siguientes:

a) Bitcoin actualmente no permite la función de crédito que si tienen las tarjetas de crédito. Muchos creen que esta función es fácilmente aplicable en las carteras de Bitcoin mantenidas por empresas dedicadas al soporte, como los patios de comercio, esto supondría emular la figura de un banco comercial.
b) El Bitcoin es actualmente una moneda poco liquida comparada con las monedas actuales. Y como hemos visto en el primer apartado, esta falta de liquidez, puede dañar enormemente su capacidad como medio de cambio y últimamente su carácter de dinero. La principal característica que lo haría un activo poco liquido es la volatilidad de su valor.

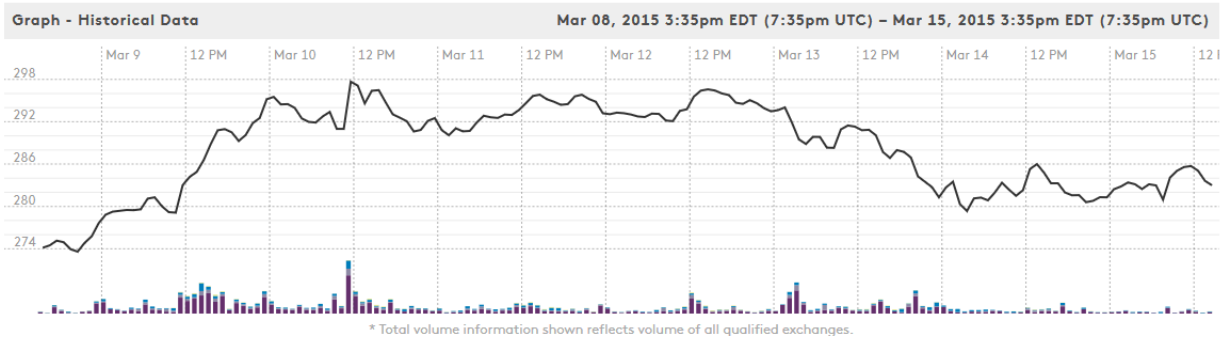


Pecio en dólares de un BTC. 2014-2015 (con medias de 7 días). Fuente: http://winkdex.com

Depósito de valor

En su capacidad de depósito de valor es donde el Bitcoin recibe el mayor número de críticas y donde más dudosa se puede ver su condición como dinero

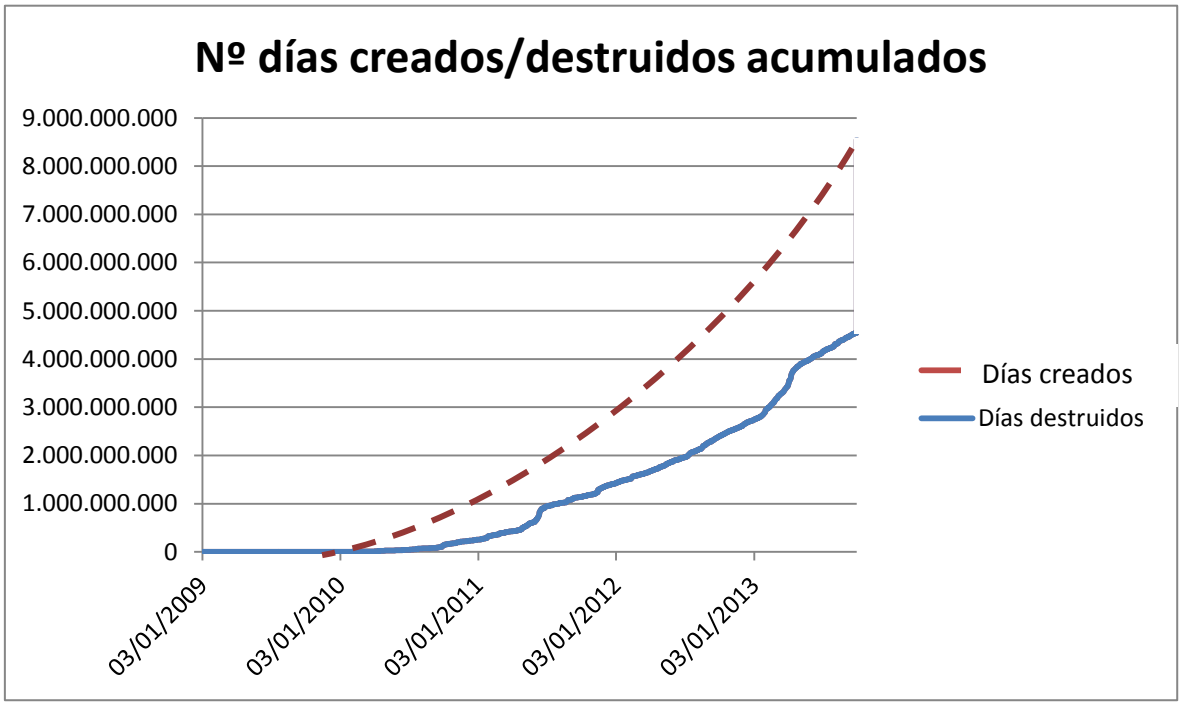
La principal causa de estos defectos como depósito de valor es la volatilidad en su precio que podemos apreciar en el gráfico anterior. Teniendo esta volatilidad su máxima expresión en Octubre de 2013 cuando el Bitcoin alcanzó los $1000 para posteriormente caer en Diciembre de 2013 a un precio de $600[23]. Es de notar que en los últimos meses el precio del Bitcoin se ha ido estabilizado en relación con sus orígenes pero la variación sigue siendo muy lejana a la deseable para una moneda. En el siguiente gráfico podemos apreciar una variación semanal del precio del Bitcoin (Marzo 2015). El precio se ha establecido en cerca de los $280, teniendo variaciones medias semanales de $50 [23].



Pecio en dólares de un BTC. 9/03/2015- 15/03/2015 (con medias de 7 días). Fuente: http://winkdex.com

Lo que produce esta gran variación de precios es una tensión entre su uso como moneda y su uso como inversión especulativa en la que se debe comprar bajo y vender alto. Un punto en el que hay que tener especial atención para determinar el carácter como inversión del Bitcoin es el nivel de acaparamiento del mismo. Este acaparamiento viene definido como la cantidad de bitcoins son retenidos por individuales como inversión frente al total de bitcoins en circulación.

Este efecto de acaparamiento puede ser medido en términos de "coin-days" destruidos[23]. Este término hace referencia en una transacción a la cantidad de tiempo que transcurre desde que se reciben unos bitcoin hasta que realmente son gastados. El cálculo de la destrucción de "coin-days" se obtiene multiplicando la cantidad gastada por el número de días desde que esos bitcoins fueron utilizados por última vez. Los "coin-days" son creados con el paso del tiempo y con la emisión de nuevos bitcoins.



Días destruidos acumulados. 2009- 2013 (con medias de 7 días). Fuente: http://blockchain.info

La diferencia entre ambas curvas muestra el nivel de acaparamiento presente en el Bitcoin. En la gráfica podemos ver como el acaparamiento crece con el tiempo, esto es debido a la caída de valor que ha sufrido el Bitcoin el último año unido al hecho de que una gran parte de los usuarios ve al Bitcoin como una inversión y no como medio de cambio. Debido a la caída de precio las transacciones se reducen a la espera de que los precios vuelvan a subir y poder cambiar esos Bitcoin por Dólares y no por Bienes o Servicios. Esta situación muestra una gran debilidad del Bitcoin como moneda ya que reduce drásticamente su liquidez.

La visión que se tiene del Bitcoin como inversión es el equivalente a la de una Start up. Se invierte en los inicios con un gran riesgo a cambio de una posibilidad de triunfo y crecimiento exponencial. El riesgo es que el valor del Bitcoin caiga a cero o sufra una gran caída. Hay ciertos escenarios bajo los cuales esto podría suceder y por lo tanto acabar con el Bitcoin también como moneda. Estos son: Un fallo en la seguridad del sistema, una pérdida de confianza por ataques de hackers que produzcan una migración masiva de usuarios y , entre otras, que surja otra moneda o cambio en las existentes que desbanque totalmente cualquier incorporación de nuevos usuarios en la red.

Si comparamos las características como depósito de valor del Bitcoin frente a otros activos nos encontramos con la siguiente situación:

Instrumentos bancarios	• Pago de intereses • Riesgo de contrapartida • Riesgo impositivo • Riesgo político (devaluaciones monetarias)
Efectivo	• Coste de oportunidad de intereses no recibidos • Anónima • Riesgo de robo • Difícil de trasladar en grandes cantidades • Riesgo político (devaluaciones monetarias)
Bitcoin	• Sin intereses • Pseudo-anónima • Riesgo de pérdida o robo • Transporte y almacenamiento fácil y poco costoso • Alta volatilidad de precio • Sin reconocimiento legal como moneda en curso

Las principales ventajas del Bitcoin son la ausencia de costes de almacenamiento y la protección frente a devaluaciones monetarias impuestas a nivel gubernamental. Como principales críticas y desventajas podemos observar la gran volatilidad de su valor, el riesgo de no recuperación en caso de pérdida y por ultimo su carencia de carácter de moneda de curso legal. Esta ausencia de legalidad y reconocimiento gubernamental hace probable su inutilidad para pagar, y crea incertidumbre sobre los riesgos impositivos y legales que recaen sobre la misma.

Unidad de cuenta

El Bitcoin tiene un gran potencial en términos de unidad de cuenta de los distintos bienes y servicios debido a su divisibilidad. Pero en la realidad la gran volatilidad del mismo no permite que los precios de una gran mayoría de los artículos se fijen basándose en el Bitcoin. Para un negocio marcar sus productos en unidades de bitcoin supone un gran riesgo de cambio de moneda, de la misma forma que las empresas que operan en distintas monedas. La diferencia es que el riesgo en el caso del Bitcoin es exponencialmente mayor debido a su gran volatilidad.

Lo que sucede en la realidad es que los bienes normalmente tienen una unidad de cuenta basada en dólares y dependiendo del valor del bitcoin respecto al dólar se le otorga a esos bienes un precio en bitcoins. En la actualidad ya han surgido una serie de procesadores de pago que facilitan estas transacciones entre divisas. Los comercios valoran sus bienes en una divisa de curso legal y el procesador de pago traduce este valor a bitcoin. Entonces permitiría al cliente pagar con Bitcoin, el procesador transformaría estos Bitcoin en Dolares utilizando un Patio de comercio y entregaría el valor en la primera divisa al comerciante. Cualquier fluctuación del precio durante el minuto que puede durar la transacción es asumida por el procesador de pago, pero al ser este intervalo temporal tan reducido el riesgo es asumible.

Desde un punto de vista puramente económico esto no representa una unidad de cuenta pura, sería una unidad de cuenta en potencia pero pobre en la práctica debido al riesgo que implica operar con ella.

Conclusión

Una vez visto como el Bitcoin se adapta a las tres funciones que son comúnmente aceptadas para denominar a un activo dinero podemos afirmar lo siguiente: El Bitcoin es un buen medio de cambio, un depósito de valor con un muy alto nivel de riesgo y una pobre unidad de medida.

Actualmente el Bitcoin no podría ser considerado como una moneda completamente funcional en todos los aspectos debido a los grandes inconvenientes que alberga. Su gran volatilidad le impide una funcionalidad completa e incita a una tendencia de usarlo como valor de inversión en vez de medio de cambio. La falta de respaldo por parte de terceras partes de confianza y seguros de valor también minan su capacidad para representar un verdadero depósito de valor seguro. Además, el mismo hecho de que no sea una divisa reconocida implica un riesgo.

Si el Bitcoin no llega a ser reconocido como una moneda de curso legal las presiones impositivas que se ejercerán sobre el mismo serán las equivalentes a las acciones u otros activos financieros. Este hecho sería una barrera a sus aspiraciones de convertirse en una moneda como explicaremos en un apartado posterior.

Esta valoración de la situación actual no es una negación de su potencial como moneda. Hay que recordar que "…el dinero es evidentemente un medio de compra final… es obvio que el dinero es en sí mismo es tan sólo un medio: un medio de cambio, un instrumento de cálculo."[4]. El futuro del Bitcoin como moneda depende de las presiones de la sociedad, concepción, aceptación y regulación del mismo. Sin embargo, actualmente no podría considerarse como dinero.

5. Implicaciones actuales y potenciales del Bitcoin

En este apartado se analizara de una forma general las implicaciones actuales y previsibles del Bitcoin. Estas influencias en la sociedad se podrían clasificar en torno a tres categorías: Económicas, políticas y legales.

Una de las principales implicaciones económicas es en qué medida el Bitcoin se integraría con el sistema financiero. Actualmente se opera con un sistema de reserva fraccionaria, lo que significa que los bancos retienen solo un porcentaje de los depósitos en reservas mientras distribuyen el resto del dinero en forma de crédito. Esto crea en la economía el llamada multiplicador monetario. De la misma forma que esto permite un crecimiento acelerado de la economía a través del aumento del flujo monetario también acarrea riesgos de quiebra para los bancos en situaciones de estrés financiero. En la reciente crisis financiera tenemos el ejemplo histórico claro de esta situación.

En un principio la ideología ligada al Bitcoin estaba encaminada a la eliminación de este sistema financiero para evitar los rescates bancarios[15]. Como hemos visto en anteriores apartados, el Bitcoin tiene la capacidad de operar sin la utilización de un intermediario ni un sistema financiero. Sin embargo nada impide que se desarrolle un sistema financiero alrededor del Bitcoin. Por lo tanto la creación de un sistema bancario por reservas basado en el Bitcoin similar al que existe actualmente es perfectamente posible y de hecho algunos patios de cambio ya lo pusieron en prueba, este es el caso de MT. Gox[15].

Pero en un sistema financiero que opere con Bitcoins el riesgo de contrapartida es muy superior al sistema bancario tradicional. Este riesgo de contrapartida es la posibilidad de pérdida de tus fondos por impago de la entidad financiera. En caso de quiebra de una entidad bancaria el seguro limita las pérdidas de los clientes, de la misma forma el banco cubre ciertos robos probados en tus cuentas bancarias. Sin embargo, en el Bitcoin estos sistemas de seguridad no existen actualmente. Las pérdidas son completamente

asumidas por los clientes de estas entidades sin posibilidad de reclamación o recurso legal. Este carácter del Bitcoin representa una barrera para su aceptación general en la sociedad.

Mt.Gox llevó a cabo este sistema bancario y aunque su desaparición no fue a causa de un colapso, realmente representa los peligros que implica un sistema financiero basado en el Bitcoin. La desaparición de Mt.Gox conllevó la pérdida de Bitcoins por valor de quinientos millones de dólares a todos sus usuarios, quienes no tenían forma legal de afrontar esta pérdida.

Estos riesgos están a su vez fomentados por el efecto que tiene el Bitcoin de rebajar las barreras de entrada al sector financiero. En el sistema tradicional para entrar en el sector financiero hace falta el cumplimiento de una regulación impuesta por las entidades guvernamentales. Por el contrario el Bitcoin ha permitido que distintas start up den sus primeros pasos en el mundo financiero, desde procesadores de pago, patios de cambio a sistemas de mantenimiento de carteras. Con la incorporación de estas nuevas entidades se espera que se incentive la innovación en el sector y que esto últimamente acabe siendo beneficioso para el consumidor. Sin embargo como hemos visto antes la introducción de estas entidades que no tienen que cumplir una cierta reglamentación representa un gran riesgo para el consumidor. Como veremos en el apartado siguiente esta apertura del sector financiero estará limitada en gran medida por la regulación emergente por parte de los países que han empezado a reaccionar al Bitcoin.

Otro efecto del Bitcoin en la economía es la facilitación de ciertos modelos de negocio en la sociedad. Una de las aplicaciones del sistema de Bitcoin es la posibilidad de realización de micro pagos. Ya que las transacciones de Bitcoin no tienen una comisión base es viable procesar una sucesión de ellas con importes muy reducidos. Al contrario de lo que sucede actualmente con los sistemas de pago por tarjeta de crédito o transferencia los cuales solo aceptarían pagos a partir de cierto importe. A primera vista puede resultar difícil ver utilidad en los micro pagos pero se puede concretar su potencial con los siguientes ejemplos de aplicación.

El primer ejemplo hace referencia a el modelo de negocio de la prensa online. Actualmente algunos periódicos de gran reputación como son The Financial Times o The New York Times cuentan con una versión electrónica. Pero a diferencia de otros esta versión electrónica es de pago. El modelo de negocio que actualmente tienen es el de suscripción, estableciendo precios diarios, semanales y mensuales. Estos rangos de precio tienen como objetivo fijar un pago mínimo y son debidos a las comisiones base a las que tienen que hacer frente los pagos por tarjeta electrónica.

El Bitcoin no cuenta con estas restricciones por lo que permite el desarrollo de un negocio en el que se cobre al usuario mediante transacciones automatizadas por cada artículo leído. Estas transacciones automatizadas no tendrían un precio mínimo. Esto constituiría un modelo de negocio alternativo al de suscripción o potencialmente complementario.

Otra aplicación potencial de micro pagos reside en el uso de internet en sitios públicos. Se podría llegar a cobrar basándose en los minutos utilizados e incluso en el ancho de banda consumida por muy baja que haya sido la cantidad. De la misma forma que con la prensa online esto ofrecería un modelo de negocio alternativo para mantener las redes de internet públicas.

También se pueden ver posibles influencias por parte del desarrollo tecnológico y la idea de la Cadena Bloque. La aplicación de este concepto puede ser muy conveniente para la gestión de ciertos mercados. En el fondo el Bitcoin es solamente un activo digital intangible, por lo tanto este sistema de regulación de las transacciones del Bitcoin se puede utilizar para otros activos digitales intangibles o derechos de uso.

Estos activos digitales estarían registrados en la Cadena de Bloques y asociados a una determinada cartera. Por lo tanto la propiedad de dichos activos le corresponde a aquel que este en posesión de la llave privada de esa cartera. Este sistema podría llegar a causar un impacto en la gestión de los activos financieros, este es el caso de bonos de deuda o acciones de una cierta empresa. Se facilitaría en gran medida el pago de los cupones a los

poseedores de bonos e incluso la realización del voto en el consejo de accionistas de una empresa. Para realizar el pago simplemente se tendría que realizar un pago distribuido a todas las carteras con el activo necesario y para los proceso de voto, en el caso de las acciones, se podría hacer online utilizando como acreditación la clave privada de tu cartera.

Esta gestión de activos financieros además puede abrir una gran puerta para la entrada de empresas en la utilización de financiación mediante acciones. Esto representaría un camino alternativo a la bolsa para empresas de pequeño tamaño, una forma, en definitiva, de crowdfunding.

Otra influencia de la tecnología utilizada por el Bitcoin se puede apreciar en la creación de la llamada propiedad inteligente[23]. Esto son propiedades, activos, que tengan acceso a la información almacenada en la Cadena de Bloque y tengan la capacidad de actuar en consecuencia de esa información. Un ejemplo de propiedad inteligente es el de un coche con acceso a internet, si se realiza una compraventa de este activo en la Cadena de Bloque, éste sería capaz de detectarlo y automáticamente actualizar sus códigos de acceso a, por ejemplo, la llave privada de la cartera receptora del activo.

En relación con el ámbito legal la implicación más directa que tiene el Bitcoin sobre la sociedad es su carácter pseudoanónimo lo que lo convierte una herramienta potencialmente útil para actividades ilícitas. Estas actividades van desde el blanqueo de dinero, la evasión de impuestos, utilización para la compra y venta de productos ilegales a la financiación de grupos terroristas. A lo largo de la historia del Bitcoin ya se han dado ejemplos notorios de un uso incorrecto del mismo. Uno de ellos es la página Silck road, ya mencionada anteriormente, dedicada a la compraventa de todo tipo de drogas. En un caso análogo en Francia se produjo la primera detención por blanqueo de dinero en Julio de 2014[25].

Para controlar este problema que supone para la sociedad el carácter pseudo-anónimo del Bitcoin se han intentado ciertas iniciativas denominadas “Green listing”[23]. Este proceso insta a los usuarios de las carteras de Bitcoin a

identificarse y registrarse en una plataforma que almacena estos datos. El modelo de negocio de esta base de datos reside en el cobro de una pequeña comisión a todos aquellos que quieran obtener la información de si una cartera ha sido registrada y validada. Cuando un cliente quiere pagar a un proveedor este primero podría comprobar si esa dirección de Bitcoin está registrada o no, y dependiendo de ello acometer o no la transacción.

Con este método se podría llegar a identificar en la red aquellos fondos considerados de origen dudoso y evitar que los negocios que acepten Bitcoins faciliten el blanqueo de dinero. Las principales críticas de este procedimiento se centran en la creación de una división entre los Bitcoin existentes en el mercado, los limpios y los sin identificar. Como actualmente no existe la imposición legal de comprobar el registro de las carteras algunos comercios más predispuestos a aceptar bitcoins sin identificar podrían cargar una diferencia de precio. Esto además de aumentar el coste del uso de bitcoins no reduciría en última instancia los crímenes de lavado de dinero.

En términos políticos el Bitcoin tiene principalmente dos implicaciones. La primera, y de un mayor calado si el Bitcoin llega a ser una moneda de gran volumen, es la imposibilidad de su manipulación por parte de los gobiernos. Las políticas monetarias expansivas y contractivas utilizadas por los gobiernos para controlar distintas situaciones económicas en la sociedad no se podrían llevar a cabo sobre una economía que principalmente use Bitcoins. Esta implicación es uno de los principales pilares para el rechazo gubernamental hacia el Bitcoin.

La otra gran implicación es la capacidad impositiva de los gobiernos sobre el Bitcoin. Esta problemática está compuesta a su vez por dos diferentes cuestiones. La primera es la capacidad del gobierno de registrar y aplicar impuestos sobre todas las transacciones realizadas con Bitcoins. Esto esta dificultado en gran medida por el carácter pseudoanónimo del Bitcoin. Y la segunda implicación viene dada por la elección del tipo de tasas impositivas aplicadas. Estas están principalmente divididas en las tasas impositivas aplicadas a operaciones realizadas con dinero y en las tasas aplicadas a los

activos financieros. En el siguiente apartado nos detendremos en la regulación vigente y su incidencia en este aspecto.

Finalmente, observamos que en un sistema que utilice el Bitcoin o, al menos, la tecnología de la cadena bloque habría una forma de medir las transacciones en la economía con un error menor al actual. Esto es principalmente causado por la economía sumergida, en un sistema operado por la cadena bloque esta no existiría ya que todas las transacciones estarían registradas públicamente. De esto se deduce que la posibilidad de medidas macroeconómicas sobre la economía es potencialmente mayor con la utilización del Bitcoin.

6. Análisis de la regulación emergente y sus implicaciones

En este apartado analizaremos la regulación actual o en proceso de implementación sobre el Bitcoin, así como los efectos que tendrá sobre la funcionalidad y concepción social del mismo. Como hemos visto el Bitcoin se ha trasladado de los círculos de libertarios y cyperpunks a otros círculos de la sociedad. Esto ha creado lo que se puede llamar una guerra civil en torno a la regulación entre "los primeros miembros más libertarios, y una facción más comercial que está buscando aceptar una regulación que garantice la legalidad de sus negocios"[26].

Por lo general se pueden apreciar dos tipos de regulación, o dos motivaciones de la misma, la primera es la regulación de las actividades ilegales asociadas al Bitcoin y la segunda es la relacionada con el aspecto económico e impositivo.

En primer lugar tenemos aquella regulación cuyo propósito reside en la erradicación de las actividades ilegales que han prosperado gracias al Bitcoin. En 1999 Milton Friedman ya afirmaba que "en un futuro cercano se desarrollará la posibilidad de intercambiar fondos por internet. Por supuesto tendrá un lado negativo. Esto significará que los mafiosos y personas ligadas a actividades ilegales tendrán un medio rápido de hacer prosperar su negocio"[27].

El primer hecho que llamó la atención de las entidades reguladoras de EEUU fue la creación de Silk Road, "la página ilegal en la que podías comprar todo tipo de drogas imaginables"[28]. Solo dos semanas después el Senador Chuck Schumer reclamó a las autoridades federales de EEUU el cierre de Silk Road y de la "moneda peer to peer anónima conocida como Bitcoin que alimenta a la página"[28]. De la misma forma la división de crimen digital del FBI decía en Enero del 2012 que el "Bitcoin seguirá atrayendo la atención de criminales con intención de robo de fondos o financiación de actividades ilegales… Ya que el Bitcoin no cuenta con una autoridad central la aplicación de la ley se encuentra con dificultades de detección de actividades ilícitas e

identificación de los usuarios."[28]. Además el FBI enfatizaba que el punto de presión donde se podría aplicar la regulación es en el nexo donde se transforman esos bitcoins en divisa de curso legal, todos los sitios que realicen esta actividad tendrían que estar registrados en la Red de Persecución de Crímenes Financieros (FinCEN) e implementar un programa de persecución del lavado de dinero.

En febrero de 2014 FinCEN se pronunció con dos fallos. El primero establecía que un minero de Bitcoin que solamente usará Bitcoin para beneficio propio no representaba una empresa de servicios monetarios ya que no entablaba una transmisión monetaria. Pero si se tiene intención de utilizar el Bitcoin para comprar bienes y servicios mediante transferencia de los mismos a la dirección del vendedor o acreedor se puede estar incurriendo en transmisión monetaria. En el segundo fallo se centró en las compañías con inversiones en la moneda digital, estas serían consideradas una entidad que incurre en transmisión de dinero y por lo tanto tienen que responder frente al "Bank Secrecy Act". Bajo esta ley estas compañías tienen que, además de estar registradas, conseguir una licencia de los 47 estados que forman los Estados Unidos, implementar programas contra el lavado de dinero y registrar todas sus transacciones. El coste de la obtención de dichas licencias es cercano a los veinte millones de dolares[28], gasto inalcanzable para la mayoría de las empresas relacionadas con el Bitcoin en la fecha.

Una segunda oleada de regulación llegó con la caída de Mt. Gox. En este caso se produjo un intento de prohibición total del Bitcoin en EEUU por parte del Senador Joe Manchin, miembro de la comisión bancaria del senado. Algunas de las razones eran "su inestabilidad y disrupción de la encomia" y "su papel en el desarrollo de actividades ilícitas"[29]. En otros países como Rusia o China si se llevó a cabo esta prohibición total del uso del Bitcoin en sus territorios[30]. Sin embargo hay indicadores de que Rusia retirará esta prohibición total en un futuro cercano [28]. Esta rama extrema de prohibición no se podría considerar una corriente a nivel global. En Europa aún no existe una regulación

determinada frente a estos intermediarios financieros relacionados con el Bitcoin.

En un segundo caso tenemos la problemática reguladora por el lado impositivo y de reconocimiento del patrimonio. Esta discusión se basa en el reconocimiento del Bitcoin como un activo financiero o como una moneda de curso legal. Dependiendo de esta denominación estará sujeto a diferentes aplicaciones impositivas las cuales limitarán o no su uso.

En EEUU debido a la gran variedad de regulaciones estatales las leyes relacionadas con el reconocimiento impositivo del Bitcoin son contradictorias. En el estado de Texas se reconoce al Bitcoin como una clara forma de dinero mientras que en el caso federal contra Silk Road se rehusó a reconocer al Bitcoin como dinero[28].

En Europa el gobierno alemán declaró en Junio del 2013 que el Bitcoin sería tratado como una actividad comercial y que estaría sujeto a impuestos relacionados con las plusvalías obtenidas, a menos que estos fueran mantenidos por un periodo superior a un año. En Agosto de 2013 el primer ministro alemán reconoció al Bitcoin como una unidad de cuenta equivalente a una "moneda privada" en la ley alemana. Lo que esto significa es que además de estar sujetos a impuestos sobre las plusvalías obtenidas tiene que tributar bajo los tipos de interés de ventas (IVA)[31]. De la misma forma la regulación en Reino Unido y España exigen el pago del IVA a las transacciones de Bitcoin, e incluso a la minería de Bitcoin[30].

Sin embargo Reino unido fue el primer país en reconocer un tratamiento legal al Bitcoin equivalente al aplicado a las monedas de curso legal, esto implicaba la retirada del impuesto de ventas aplicado sobre el Bitcoin. Esta actuación responde a un plan lanzado por el gobierno inglés en el que se pretende asegurar la protección de desarrollos positivos para la sociedad como el Bitcoin[32]. Sin embargo la tendencia global hasta el momento es la de negar el reconocimiento de dinero al Bitcoin. Las causas de esta negativa

normalmente son preocupaciones administrativas, incertidumbre legal o el simple afán de aplicar unos mayores impuestos sobre el mismo.

Los efectos de esta regulación sobre el Bitcoin son evidentes y vitales para su desarrollo futuro. La regulación relacionada con las actividades ligadas con el Bitcoin en su formato actual implicaría restricciones sobre la facilidad de acceso al mundo financiero que el Bitcoin supone, como hemos visto en el apartado anterior. Esta regulación aumentaría la seguridad a la hora de operar utilizando terceras partes por lo que resultaría beneficioso para el desarrollo, respecto al público general, del Bitcoin. Otro efecto potencial de esta regulación es la toma de posesión de las operaciones en Bitcoin por parte de los operadores financieros ya afianzados en nuestra sociedad. Un ejemplo lo encontramos en España donde Bankinter ha realizado la primera inversión en una startup de procesamiento de pagos de Bitcoin[33].

Pero, el mayor impacto sobre el funcionamiento del Bitcoin, lo presenta la regulación impositiva en función de su naturaleza. Adam j. Levit, profesor de derecho, escribió en un ensayo que la aplicación impositiva equivalente a un activo financiero destruiría en gran medida la capacidad del Bitcoin como dinero. Si se aplica impuestos a las plusvalías producidas en el momento de la venta haría que los Bitcoin no fueran equiparables entre sí mismos. Un Bitcoin obtenido a un precio muy bajo no tendría el mismo valor en origen que un Bitcoin obtenido a un precio mayor[34]. Este razonamiento también ha recibido críticas que lo categorizan de extremista. Tim Worstall, colaborador de Forbes, opinaba que estos impuestos afectan en su utilización pero que en última instancia los Bitcoins en el momento de la venta sí que siguen valiendo lo mismo en el sentido de que pueden ser intercambiados por la misma cantidad de bienes[35].

Al margen de esta discusión más teórica sobre su capacidad de operar como moneda se produce un efecto mucho más directo. Si el Bitcoin sufre una presión impositiva mayor de lo que otras monedas electrónicas de curso legal la ventaja competitiva del Bitcoin se reduce. Al resultar un medio de cambio

más caro no se conseguiría atraer a suficientes usuarios nuevos para llegar a su masa crítica y convertirse en un medio de cambio universal.

7. Conclusiones

Como hemos visto el Bitcoin tiene todos los elementos necesarios para convertirse en una moneda independiente de bancos centrales y entidades reguladoras.

Sin embargo actualmente consta de grandes obstáculos a su funcionalidad como moneda. La principal es la volatilidad de precios que sufre debido a los movimientos especulativos que ha sufrido. Esto le impide representar un depósito de valor seguro y formar una unidad de medida sin riesgo para los comercios. Con estos inconvenientes lo que se impide es una popularización del mismo entre círculos no formados de la sociedad que no están dispuestos a asumir tales riesgo de fluctuación. A su vez la volatilidad aumenta su concepción como un activo financiero, una forma especulativa que produce en su funcionalidad como moneda un efecto de deflación sistémica. Una bajada de precios en el Bitcoin produce entre los que lo toman como una inversión un efecto de acaparamiento que reducirá el nivel de transacciones en el mercado. Esta reducción de su utilidad por el acaparamiento produce a su vez sucesivas caídas de valor, transformando este proceso en una espiral que se autoalimenta.

Esto lo que denotaría es su condición actual como activo financiero, debido a su falta de funcionalidad como moneda. Pero también denota los grandes hitos que ha de cumplir para convertirse en una moneda. Estos son la eliminación de la volatilidad y la proliferación de usuarios que utilicen esta moneda como medio de cambio y no como medio de especulación. La volatilidad como hemos visto ya está en un proceso de reducción. De todas formas este estado es temporal ya que la formación de burbujas en un sistema como el Bitcoin, en el que no existe control gubernamental, depende completamente del estado anímico del mercado. El uso como moneda está amenazado por un mayor control impositivo sobre los beneficios producidos por la compra venta de Bitcoin. Esos tipos impositivos además de aumentar el coste de operar en Bitcoin aumentan la percepción del mismo en la sociedad como un activo financiero.

Por lo tanto para la superación de estos hitos el Bitcoin necesitará contar con el respaldo de un sistema financiero y regulación legal que actualmente está en un estado muy prematuro pero que muestra una tendencia de crecimiento.

Sin embargo, la consecución de estos hitos y la verdadera consolidación como moneda principal acarrearía unas grandes influencias en los sistemas políticos económicos y legales actuales. Estas influencias reducirían el poder estatal y dificultarían las acciones legales (debido a su carácter pseudoanónimo) por lo que surgirían numerosas presiones sobre el Bitcoin con el fin de evitar estas consecuencias. Para un cambio monetario total hacia el Bitcoin haría falta un apoyo económico, social y político del mismo, lo que debido a sus implicaciones se plantea imposible.

Por lo tanto, debido a las presiones ejercidas por parte de los grandes gobiernos no llegará a conformar una moneda que sustituya a las principales divisas mundiales como son el Dólar, Yen o el Euro entre otras. Sin embargo, el Bitcoin alberga el potencial para convertirse en una moneda alternativa a estas formas de dinero convencional. Esto produciría un desplazamiento de pequeñas monedas cuyo soporte gubernamental y aceptación es reducido, y por lo tanto sufren de fluctuaciones y riesgo de pérdida de valor. La característica de no necesitar un respaldo de confianza para mantener su valor permite al Bitcoin compensar esa falta de respaldo gubernamental de algunas monedas minoritarias.

Las iniciativas legales actuales y futuras están relacionadas con la eliminación de la condición totalmente privada el Bitcoin así como a la regulación de las entidades financieras que quieran operar con ellos. Esta eliminación de la condición privada del Bitcoin potencialmente se conseguirá mediante la aceptación del mismo como una forma monetaria y la realización de una presión legal sobre el registro de las carteras en bases de datos de “greenlisting”. También se implementará una dura normativa sobre las empresas que estén involucradas en la gestión financiera del Bitcoin, como las normativas actualmente ya existentes en EEUU. Esto producirá un movimiento

del soporte financiero hacia entidades ya establecidas en la sociedad que favorecerán a la seguridad del sistema y la entrada de nuevos usuarios.

Al margen de su posición como moneda el Bitcoin ha tenido un gran efecto en la sociedad debido a la tecnología que plantea para la gestión descentralizada y publica de activos mediante la informática. El sistema de gestión de la cadena de bloques será modificado y utilizado en futuras innovaciones, como, potencialmente, la gestión de las acciones de una empresa. Además es plausible la incorporación de parte de esta tecnología de pagos online en las actuales monedas electrónicas de curso legal.

Mi análisis está basado en la situación actual de la legislación y tendencias políticas sobre el Bitcoin. Por lo tanto el mismo es susceptible de ser perfeccionado en posteriores estudios con una mayor visibilidad de la aceptación social futura del Bitcoin.

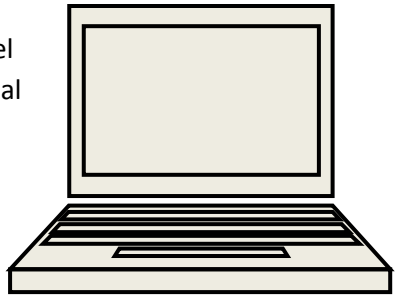
BIBLIOGRAFIA

1. Pagliery, Jose. 2014. Bitcoin and the future of money. Vol. 1. Chicago, Illinois: Triumph Books LLC.
2. Lord Robbins. 1935. An essay on the nature and significance of economic science.
3. Wood, John H. 1999. Money: Its origins, development, debasement, and prospects. In Money: Its origins, development, debasement, and prospects. Vol. XXXIX, 3-7. Great Barrington, Massachusetts: American Institute for Economic Research.
4. Martin, Felix. 2014. MONEY the unauthorised biography. Londres: Vintage.
5. Newlyn, N. T. 1962. The theory of money. Abstract. 11-20.
6. Laider, D. 1966. Some evidence on the demand for money. In . 3th ed., 544-45Journal of Political economy.
7. Lord Robbins. 1935. An essay on the nature and significance of economic science.
8. Friedman, M. 1959. The demand for money some theorical and empirical results. In , 67-69Journal of Political Economy.
9. Friedman, M. 1956. The quantity theory of money: A restatement. In . Chicago, Illinois: Chicago University press.
10. Mankiw, Gregory. 2005. Macroeconomía. Barcelona, España: Antoni Bosh Editor.
11. Vigna, Paul, and J. Michael Casey. 2014. The age of cryptocurrency: How bitcoin and digital money are challenging the global economic order. New York: ST. Martins Press.
12. Taylor, John. 2011. An essay on money, its origin and use.
13. Weatherford, Jack. 1998. La historia del dinero, de la piedra arenisca al cyberespacioAndres Bello publicaciones.
14. Roover. 1949. Gresham on foreing exchange. In , 91. Cambridge: Harvard University Press.
15. Pagliery, Jose. 2014. *Bitcoin and the future of money*. Vol. 1. Chicago, Illinois: Triumph Books LLC.
16. Franco, Pedro. 2015. Understanding bitcoin: The blockchain. In , 95-123. United Kingdom: Wiley Finance Series.
17. Waterfield, Alex, and Xavier Aaronson. 18/02/2015. **Así se fabrican bitcoins en china**. , http://www.expansion.com/multimedia/videos.html?media=HZ0Lywdqtml.
18. Halbert, Aaron J. 2014. *Bitcoin security: How to create a secure bitcoin wallet*. Great Britain: .

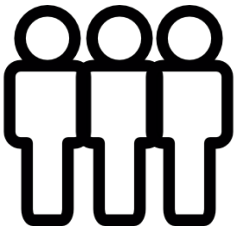
19. Champagne, Pkil. 2014. *The book of satoshi: The collected writititngs of bitcoin creator*. United States of America: E53 Publishing LLC.
20. Duncan, Gary. 2009. **Chancellor alistair darling on brink of second bailout for banks**. (January 3 2009), http://www.thetimes.co.uk/tto/business/industries/banking/article2160028.ece.
21. *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies,* First session (United States of America 2013).
22. Varian, H. 2003. *The economics of information technology*.
23. Franco, Pedro. 2015. Understanding bitcoin: Economics. In , 21-37. United Kingdom: Wiley Finance Series.
24. Popper, Nathaniel. February 19, 2014. Winklevoss brothers offer an index to track price of bitcoin. , http://dealbook.nytimes.com/2014/02/19/before-a-bitcoin-fund-comes-a-price-index/?_r=1.
25. Macheel, Tanaya. French officials seize $272.800 from illegal bitcoin exchange. *Coindesk*, http://www.coindesk.com/french-officials-seize-272800-illegal-bitcoin-exchange/.
26. Wile, Rob. 29/01/2014. **The emerging bitcoin civil war**. *Business Insider*, http://www.businessinsider.com/bitcoins-new-civil-war-2014-1.
27. Hanke, Steve. 2014. **Friedman and hanke on bitcoin**. Abstract. *CATO institute*.
28. Wenker, Nicolas. 2014. *Bitcoin pandemonium: The ongoing economic, public, and legal debate over the nature and impact of bitcoin*. Leipzig: Amazon uk.
29. **Manchin demands federal regulators ban bitcoin**. 2014. *Office of Sen. Joe Manchin*, http://www.manchin.senate.gov/public/index.cfm/press-releases?ID=237cbd66-6a26-4870-9bcb-20177ae902b0.
30. *Regulation of bitcoin in selected jurisdictions*2014. . Great Britain: Global Legal Research Directorate Staff.
31. Matt, Clinch. 2013. **Bitcoin recognized by germany as 'private money'**. *Cnbc*, http://www.cnbc.com/id/100971898.
32. Hern, Alex. 2014. **Bitcoin: UK plans to end tax on digital currency trades**. *The Guardian*, http://www.theguardian.com/technology/2014/mar/03/bitcoin-trades-uk-tax-digital-currency.
33. EFE. 2014. **Bankinter invierte en coinffeine, una empresa española de tecnología bitcoin**. *Expansion*, http://www.expansion.com/agencia/efe/2014/11/17/20125407.html.
34. Meyer, Robinson. 2014. **Why bitcoin can no longer work as a virtual currency, in 1 paragraph**. *The Atlantic*, http://www.theatlantic.com/technology/archive/2014/03/why-bitcoin-can-no-longer-work-as-a-virtual-currency-in-1-paragraph/359648/.
35. Worstall, Tim. 2014. **The taxation of bitcoin won't mean that bitcoin fails as A Currency**. *Forbes*, http://www.forbes.com/sites/timworstall/2014/03/28/the-taxation-of-bitcoin-wont-mean-that-bitcoin-fails-as-a-currency/.

ANEXO 1

El usuario envía el pago en bitcoins al mercader

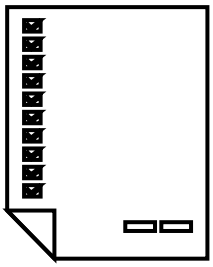


Esta transacción se publica en la red y los mineros empiezan a actuar sobre la misma

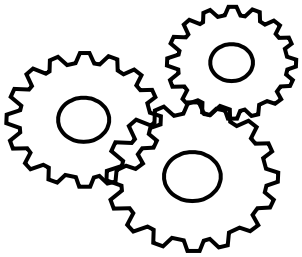


Se unifican una serie de transacciones en un bloque

Los mineros resuelven los problemas hash correspondientes al bloque



El minero que consiga primero resolver este problema retransmite de nuevo el bloque a la red para ser verificado por los demás mineros



Una vez hecha la comprobación por parte de la comunidad se añade este bloque a la cadena y se empieza a trabajar a partir de él