Bitcoin, Blockchain y DAOs

Francesc Roca Campmany
Ingeniero de Telecomunicaciones
ETSETB (Universidad Politécnica de Catalunya)
Francescr@gmail.com

Resumen - El propósito de esta exposición es acercarnos a la revolución tecnológica más disruptiva de todas las que están en marcha en la actualidad. El avance es fruto de la aparición, en 2009, de la primera moneda digital (bitcoin) que fue capaz de operar, a través de una red pública y abierta como Internet, sin intermediarios ni instituciones centrales, es decir, de manera descentralizada (o persona a persona, P2P) pero garantizando una confianza total en la seguridad de las transferencias realizadas entre los usuarios de la misma red.

Se pretende el uso de un lenguaje de bajo contenido técnico y accesible a todos los públicos que no requiera conocimientos informáticos y/o de telecomunicaciones para su comprensión. Se prestará especial atención a algo que va más allá de la propia moneda digital ya que, como veremos, Bitcoin sólo es la punta del iceberg de un gran cambio que está a punto de llegar.

Nos sumergiremos en la tecnología que se encuentra detrás de Bitcoin, la cadena de Bloques (Blockchain) y explicaremos el mecanismo (Proof of Work) que permite generar los incentivos necesarios para que emerga una comunidad que se encargue de mantener la propia red y que, al mismo tiempo, evite ser manipulada por intereses particulares.

Bitcoin es solo la primera fase y embrión de un movimiento muy potente y cuya clave es que atrae, año tras año, a gente de mucho talento. Actualmente, existen otras Blockchains nuevas y distintas a la precursora Bitcoin. Concretamente, en la Blockchain Ethereum ya es posible no solo realizar pagos sino también establecer contratos persona a persona y crear organizaciones descentralizadas prácticamente autónomas. La magnitud del cambio sobre nuestras vidas puede llegar fácilmente al nivel de impacto en la sociedad que tuvo la Imprenta en el s. XV o la reciente Internet en relación a la capacidad para romper barreras de acceso que habían estado presentes hasta el mismo día de su aparición.

Esta exposición se divide en los siguientes apartados:

Palabras clave - Bitcoin, Criptomoneda, mineria, Cadena de Bloques (Blockchain), Ethereum, Descentralización, Contratos Inteligentes (Smarts Contracts), DAO (*Decentralized Autonomous Organization*)

1. Introducción

Es increíble cómo Internet ha cambiado nuestras vidas. Hoy es posible hacer cosas que hasta hace poco nos parecían de ciencia ficción. Podemos conectarnos con cualquier parte del planeta o acceder a toda la información del mundo desde nuestro teléfono móvil; cosas que hace 10 o 20 años nos parecían inimaginables.

De todas maneras, aunque Internet ha sido desde sus inicios una red bastante descentralizada, nunca se había podido enviar dinero sin intermediarios, es decir, sin pasar por puntos centralizados como las redes de los bancos, los bancos centrales, de las tarjetas de crédito, de la red SWIFT, etc. Cuando hacemos compras en Internet o hacemos transferencias bancarias o con Paypal, el dinero y la información de las transferencias circulan primero por estas redes privadas antes de llegar al destinatario, actuando de esta manera como intermediarios. Además, la información queda almacenada en sus servidores sin tener claro si hacen un uso adicional ilícito (en el caso de la información personal que viaja por internet y queda almacenada en los servidores de una empresa nos viene a la cabeza rápidamente una red social como Facebook y el comercio que hace con nuestra información). Los pagos o transferencias nunca habían viajado por Internet directamente entre compradores y vendedores o entre personas y/o entidades.

En la antigüedad, cuando queríamos comerciar con alguien, nos citábamos físicamente con la persona y era indispensable disponer de algo de valor para dárselo a cambio (se hacía un "trueque"). Con el tiempo, para evitar cargar con objetos de valor, para poder intercambiar o para evitar el riesgo de quedarnos sin compra porque el vendedor no quería lo que se le ofrecía a cambio, apareció el dinero. A partir de ese momento el comercio comenzó a fluir y se incrementó vertiginosamente.

Pero el comercio a distancia seguía siendo muy difícil porque teníamos que enviar la mercancía y confiar en que el otro nos la pagaría. El camino fue despejándose cuando surgieron los intermediarios, instituciones o personas que construían confianza y que se encargaban de transportar los productos y el dinero por nosotros. Así, le pagábamos a Marco Polo con nuestro oro en Venecia y él podía ir Pekín y pagar con aquella cantidad de oro la seda correspondiente. Esta intermediación fue fundamental en la construcción de nuestra sociedad porque no sólo habilitó el comercio global, sino que, por ejemplo, también es la base de muchas otras instituciones de confianza como, por ejemplo, las democracias que hoy conocemos, ya que los políticos no dejan de ser los representantes, es decir, los intermediarios entre la sociedad y la gobernanza de un país.

Pero toda intermediación tiene sus problemas. La confianza es algo frágil y, cuando cambia cualquier elemento, entran las dudas. De hecho, uno de los pueblos que más éxito cosecharon en el arte de la intermediación fueron los judíos precisamente por el elevado grado de confianza que siempre ha habido entre los miembros de su comunidad. Un ejemplo claro pasa en el Mediterráneo de los siglos X al XV. Cuando un comerciante, por ejemplo de Génova o Venecia, quería algún producto que sólo podía encontrar en Constantinopla, Alejandría o El Cairo, normalmente terminaba encargando el transporte de la mercancía a un judío porque eran ellos los que podían asumir mejor el riesgo de transportar en barco la mercancía y que después no les pagaran lo acordado. En esos tiempos, los judíos tenían una muy buena reputación como intermediarios de transporte marítimo de mercancías o directamente como mercaderes porque

minimizaban muy bien el riesgo ya que el grado de confianza entre su comunidad era casi tan elevado como el que podría haber entre los miembros de una misma familia. Por lo tanto, como mercaderes, podían estar bastante seguros de que no serían traicionados cuando llegaran al puerto de destino y quisieran intercambiar la mercancía por el dinero acordado antes de ser enviada. Además, dadas las múltiples emigraciones forzadas de su historia, los judíos tenían siempre pequeñas comunidades en la mayoría de ciudades portuarias del Mediterráneo. Esto les permitía tejer una red conectada de intermediarios a partir de la cual organizar todo el transporte de las mercancías.

Pero, como en cualquier servicio que da garantías ante un riesgo, existe un coste asociado y esto es lo que ocurre hoy en día cuando utilizamos las redes de los bancos o de las tarjetas de crédito para hacer nuestras compras, que cobran a los usuarios cuantiosas comisiones por las transferencias o a los vendedores por las ventas que aceptan con tarjetas. Y esta es la razón, o una de las razones principales, por las que hoy la mitad de la población mundial no accede a los servicios financieros básicos (la barrera de entrada).

Entonces, si Internet nos cambió la vida de maneras increíbles, nos dio acceso a la comunicación con todo el mundo, eliminó las barreras de entrada para el acceso al conocimiento y nos permitió compartir de manera ilimitada, ¿por qué, hasta hace bien poco, todavía no se podían eliminar los intermediarios de la ecuación? ¿Por qué no se podían eliminar los intermediarios en los servicios que operan a través de Internet? Las razones principales eran 2:

1) La incapacidad para desplegar una red que operara de manera descentralizada, es decir, sin intermediarios
2) La dificultad que siempre ha habido para encontrar soluciones al problema de la replicación de la información digital y los riesgos que se derivan (ejemplo: la posibilidad que alguien malintencionado se dedique a duplicar activos digitales de valor y a sacar rendimiento ilegal o ilícito).

Respecto a la primera razón, el objetivo era encontrar un protocolo que permitiera que una red que no tiene entidad central que la gestione pudiese gestionarse a sí misma con la colaboración de todos por igual (la única alternativa posible puesto que el caos no es una opción). La única manera de lograrlo era encontrar un mecanismo que permita agilizar el establecimiento de consensos entre todos sus miembros porque esta la única manera de asegurar que las decisiones se toman entre todos.

En referencia a la segunda razón, el problema en una red descentralizada, hasta hace poco, era que no se podía asegurar que la persona que hacía un pago con dinero electrónico después no haría un duplicado (copy-paste) de ese dinero y volvería a hacer otro pago a otra persona creando así dinero de la nada. De hecho, en cierto modo, este fue un problema similar al que se enfrentaron las discográficas cuando la música se digitalizó, cuando la música pasó del vinilo a un simple archivo en el ordenador. Y aún peor fue para estas discográficas cuando la gente, viendo que se podían replicar los ficheros de manera infinita y sin coste, empezó a compartir la música que tenía y, a cambio, los demás también compartían la suya. La realidad es que las discográficas, por muy poderosas que fueran y por muy controlado y cautivo que tuvieran su mercado, no encontraron la solución para evitarlo. Finalmente no tuvieron más remedio que cambiar su modelo de negocio. De hecho, hoy en día, quien más negocio hace actualmente en la industria de la música, no son las discográficas sino empresas tecnológicas como Apple

(Itunes) o Spotify (música en streaming) que precisamente se adaptaron a la nueva realidad y cambiaron el modelo de negocio.

Técnicamente, estos 2 retos (conseguir una red descentralizada que actúe por consenso y evitar el problema de la replicación de información digital) ya estaban sobre la mesa desde los años 60 e informáticos y matemáticos de todo el mundo habían estado intentando encontrar la solución sin éxito. La comunidad matemática llamó a ese reto el "problema de los generales bizantinos".

Se le llamó así porque en su formulación típica planteaba el caso de un grupo de generales del antiguo imperio bizantino con batallones a su cargo, que estaban dispersos alrededor del enemigo y que debían ponerse de acuerdo en la hora de un ataque coordinado. El plan solo tenía éxito si la mayoría de generales se sincronizaban y atacaban todos al mismo tiempo. El problema es que solo se podían comunicar entre ellos mediante mensajes y que no había ninguna autoridad que los coordinase. Incluso podía darse el caso que entre ellos hubiese un traidor que intentase sabotear el consenso pasando información incorrecta.

El creador de Bitcoin consiguió resolver este problema matemático definitivamente en 2008 cuando hizo público el whitepaper donde detallaba el mecanismo de la Cadena de Bloques o Blockchain y el mecanismo de incentivos que evita la manipulación (el Proof of Work). Veremos más adelante como técnicamente funcionan estos 2 mecanismos.

2. Bitcoin

Así, en 2008 ocurrió algo increíble; alguien tuvo una de las ideas más brillantes desde que se inició el milenio. Digo alguien porque la identidad real de la persona o grupo de personas que tuvieron la idea es, a día de hoy, desconocida. Lo único que sabemos es el seudónimo que utilizó o utilizaron: Satoshi Nakamoto.

En octubre de 2008, casualmente unos días después del inicio de la peor crisis financiera de este siglo (crash de Lehman Brothers), Satoshi Nakamoto hizo público, en una serie de foros del mundo hacker y la cultura cyberpunk, la definición de un nuevo protocolo que permitía eliminar de golpe uno de los problemas no resueltos más famosos en los campos de la computación teórica y de la matemática de los últimos 50 años. Evidentemente, la magnitud de la idea era de proporciones incalculables si tenemos en cuenta que muchas mentes brillantes de la segunda mitad del siglo XX lo habían intentado sin éxito y si tenemos en cuenta que parte de la comunidad académica especializada piensa, hoy en día, que el autor de aquella idea debería haber recibido el premio Nobel si no fuera porque es anónimo y el reglamento de los Nobel no permite premiar autores anónimos o difuntos.

Satoshi, no sólo tenía los conocimientos de teoría económica y matemática suficientes para definir de manera impecable aquel nuevo protocolo sino que, además, fue capaz de codificarlo, implementarlo en forma de software y ponerlo en funcionamiento sin errores ni vulnerabilidades. No se conformó con ello y consiguió convencer a un grupo de gente mínimo inicial para que se involucrara, lo difundiera y lo utilizara lo suficiente como para acabar alcanzando la masa crítica necesaria al cabo de unos años.

Satoshi llamó "Bitcoin" a aquel sistema. Le puso este nombre porque esa plataforma no era más que una red de nodos o computadoras que se intercambiaban dinero puramente electrónico (bits, 0s y 1s) de manera segura y confiable y el nombre de la moneda digital que circulaba por aquella red privada la había llamado precisamente bitcoin.

Pero, el protocolo que él definió ha ido mucho más allá de inventar una criptomoneda o moneda digital de valor (el bitcoin como dinero) o una plataforma distribuida de Software que permita el envío confiable de esas criptomonedas entre sus usuarios (Bitcoin como sistema). De hecho, en mi opinión, la mejor aportación que hizo Satoshi es un detalle al que ni siquiera él le dio nombre: la invención de un protocolo que permitía desplegar una base de datos distribuida que se actualizaba por consenso cada 10 min y que permitía el intercambio de información entre personas de manera confidencial y confiable (es importante notar que en esta definición no he indicado en ningún momento el concepto de moneda digital o criptomoneda. Veremos la importancia de esto más adelante)

La propia comunidad de programadores y usuarios acabó bautizando este protocolo con el nombre de Blockchain porque el mismo Satoshi, en su whitepaper inicial, ya hacía referencia a las cadenas de bloques que iban creando los clientes de software Bitcoin a medida que pasaba el tiempo y a medida que las transferencias de bitcoins que se producían en esa red tenían que ir quedando registradas. Así, en el protocolo que él definió, cada 10 min se generaba un archivo (él lo llamaba "bloque") donde quedaban registradas todas las transferencias válidas que habían sucedido en todo el mundo durante los 10 min previos a la generación del propio bloque, es decir, las transferencias que se habían hecho en el mundo mientras se estaba cociendo el bloque anterior.

La clave de todo era que estos bloques estaban perfectamente encadenados de manera cronológica, había una conexión temporal inmutable entre ellos. Era imposible manipular o alterar el orden temporal en el que habían quedado registrados. Por eso se le llama CADENA de bloques y no lista de bloques, grupo de bloques o agregación de bloques. Los bloques están encadenados por una marca temporal incorruptible. Cada nuevo bloque hace referencia al bloque anterior. La razón es que, matemáticamente, se puede demostrar que esta referencia temporal entre bloques no se puede romper ni piratear de ninguna manera, como mínimo, con la tecnología de computación disponible en la actualidad (veremos que sucede cuando la computación cuántica sea un hecho).

Por tanto, si lo miramos desde una perspectiva histórica, lo que tenemos actualmente es lo que comúnmente se denomina como Blockchain, es decir, una cadena de bloques que se encuentra en todos los discos duros de los PCs que forman la red y que pulula indefinidamente y de un lado a otro por el espacio público de Internet. Esta Blockchain empezó en Enero de 2009 cuando Satoshi Nakamoto la puso en marcha ejecutando el primer software de la plataforma Bitcoin. Esta Blockchain la forman actualmente varios centenares de miles de bloques (conectados en estricto orden temporal) que contienen todas las transferencias hechas desde el minuto cero. Así, el software Bitcoin ocupa unos 20 Gb en la memoria de los ordenadores y gran parte de estos 20 Gb están ocupados por esta cadena bloques (el resto lo forman las líneas de código que dan forma al protocolo y permiten la comunicación segura y confiable entre los nodos).

3. Propiedades de Bitcoin

Es de admirar la personalidad que tuvo la persona o grupo de personas detrás del seudónimo Satoshi Nakamoto porque fue capaz de mantener el anonimato simplemente por fidelidad a las convicciones ideológicas del colectivo al que pertenecía (movimiento cyberpunk). Además, habría que recordar que, con ello, se le cerraron las puertas a recibir el reconocimiento público - y quizás económico - que seguramente se merecía y merece (como decíamos, incluso un premio Nobel no sería descartable).

También es de admirar su generosidad pues hizo un gran regalo a la humanidad haciendo de Bitcoin un sistema público, gratuito y libre (Open Source), es decir, permitiendo que cualquier persona pudiese obtenerlo, leerlo, analizarlo, hacer una copia, cambiarle algún parámetro o alguna parte del código y poner en marcha uno de nuevo. Y lo mejor de todo, aprender de él. Si además, quien haga una copia similar, consigue que un mínimo número de personas se lo instale y lo ponga en funcionamiento para establecer una red alternativa, ya tenemos una réplica de Bitcoin (que, evidentemente, ya no sería no se podría llamar Bitcoin). Y de hecho, desde que Bitcoin nació, eso mismo es lo que ha pasado unos cientos de veces con la aparición de un sinfín de criptomonedas alternativas.

Bitcoin representa la sustitución de la confianza en las instituciones por la confianza a través de las redes y las matemáticas. Durante siglos, la sociedad humana se ha basado en la confianza en las instituciones cuando el fin era coordinar una actividad entre un gran número de personas. Estas instituciones estaban dirigidas por grupos reducidos de personas que se regían por reglas y políticas determinadas que eran supuestamente transparentes que permitían garantizar, de ese modo, la correcta supervisión y rendición de cuentas. La confianza se establecía a través de la tradición, a través de la reputación, a través de la longevidad.

En la actualidad, esas instituciones de confianza están fallando. Están fallando en todo el mundo. Están fallando, por ejemplo, en el caso de los periódicos tradicionales. Están fallando las instituciones políticas y muchos tipos de instituciones más. Y una de las razones principales es que representan los sistemas de escala propios de las sociedades industriales. Pero el problema es que cada vez vivimos menos en sociedades de este tipo, sociedades del tipo Estado-nación industrial. Actualmente nos adentramos en la época de las sociedades de la información a escala global y que colaboran a través de las fronteras y a escalas masivas. Ahora hay que resolver problemas que afectan no solo a 30 millones de personas en un país, sino a siete mil millones y medio de personas en todo el planeta. Y para problemas de tal magnitud y colaboraciones a ese nivel o a esa escala, las instituciones tradicionales ya no funcionan. No son capaces de escalar. El modelo en sí no es erróneo, no tienen por qué ser corruptas (aunque lo son cada vez más), pero simplemente no permiten resolver los problemas de una sociedad global. Un claro ejemplo de esta lucha desigual es la que mantienen los gobiernos nacionales contra los mercados financieros (que operan masivamente a escala global y a una velocidad de cambio o adaptación mucho más elevada que la que muestran las instituciones nacionales tradicionales).

Y hoy en día, que ya vemos como esas instituciones no funcionan, también vemos la aparición de nuevos sistemas de gobierno, sistemas que nos permiten colaborar, comunicar y resolver problemas en esa escala global que comentamos. El primero de ellos fue Internet y con ella fuimos testigos de la aparición del primer sistema de comunicación que trasciende a las

naciones, que trasciende fronteras y que permitió que cualquier persona, en cualquier lugar del mundo, tuviera la oportunidad de participar en una economía global sin barreras de acceso, sin identificaciones, sin credenciales, simplemente con la simple acción de ejecutar un software. Y esto, efectivamente, cambia el mundo, cambia los modelos de confianza tradicionales.

Por otra parte, en lo que hace referencia al dinero, Bitcoin no es más que el último estadio de la evolución del mismo. Esta evolución ha seguido, a lo largo de la historia, una clara tendencia a la abstracción.

A un nivel muy básico, la primera forma de comunicar el valor de las cosas fue el trueque, intercambio de cosas que considerábamos de igual valor. Así, las formas de valor iniciales eran muy tangibles: materias primas, una cabra, un plátano, una piña. Eran formas muy pobres de dinero ya que se podían comer, podían morir o podían perderse fácilmente. No eran formas de dinero muy buenas simplemente porque tenían valor por sí mismas.

A partir de ahí se empezaron a ver las primeras formas abstractas de dinero. La primera gran evolución tecnológica fue comenzar a intercambiar algo que, simplemente, no se pudiese comer - una pluma, una perla, una cadena con nudos, algo colorido que se pudiese utilizar con fines estéticos, etc. Es en ese preciso momento cuando el dinero empieza a adoptar una forma abstracta. Fue primer gran momento de transformación tecnológica en el dinero, cuando el mismo dejó de ser un bien de consumo tangible con valor intrínseco y se convirtió en algo que simplemente hacía referencia a su valor. Fue el primer paso hacia la abstracción.

Nos llevó cientos de miles de años antes que pudiésemos ver la introducción de los metales preciosos. Fue la segunda transformación importante en la tecnología de dinero. Históricamente, los metales preciosos se encuentran, por primera vez, en el comienzo de las civilizaciones agrarias avanzadas (entre el 2500 y 1500 aC) que se encontraban en la zona de la Media Luna Fértil en el Medio Oriente como los babilonios, los egipcios y los griegos. En los metales preciosos se combinaban algunas de las características más importantes del dinero: difícil de encontrar (escaso); fácilmente transportable, fácil de dividir (se puede cortar una moneda de oro en pedazos y subdividir las piezas); y universalmente valioso para fines estéticos.

Dos evoluciones tecnológicas y luego nada en unos pocos miles de años. Pero entonces a alguien se le ocurrió una brillante idea: si entrego mi oro a alguien de confianza, que me pueda dar un pedazo de papel que diga que tengo una cantidad oro determinada en una bóveda segura y cuando quiera lo puedo volver a cambiar, entonces las cosas cambian porque, a partir de ese momento, uno puede operar con el papel en vez de con el oro. Y el papel es más fácil de llevar. Mientras se confíe en que el dinero está a buen recaudo en la bóveda de alguien de confianza, el papel se erige como una nueva forma de dinero.

Y así llegamos hasta el siglo XX, hace unos 60 años, cuando fuimos testigos de otra nueva forma de dinero, las tarjetas de plástico y las operaciones con las cuentas bancarias a través de cajeros.

Finalmente, en 2008 aparece Bitcoin. Bitcoin es, en mi opinión, una transformación muy radical. Es tan radical como el cambio de metales preciosos al papel moneda. Tal vez aún más radical. Y entonces, qué aporta de nuevo Bitcoin? La cuestión fundamental en la descripción de Bitcoin es que si se utilizan referencias a nuestra experiencia existente, esa experiencia se basa en miles de años de entender el dinero como algo asociado a un formato muy físico y entonces nos

equivocamos. Con Bitcoin estamos tratando de explicar una forma de dinero que es totalmente abstracta. Por ejemplo, la descripción más elemental sería definirlo como un token (testigo como el que pasa de una mano a la otra en las carreras de relevos) pero en versión digital y que representa el hecho de haber sido aceptado como participante de una red. Pero eso ni tan siquiera permite empezar a describir lo que es Bitcoin.

Uno de los malentendidos más comunes, cuando se intenta describir Bitcoin, es que la gente piensa que es simplemente un sistema de pago o una nueva forma de digitalización del dinero. Pero esta visión es pobre porque el dinero digital ya lo utilizamos desde hace años con la aparición de las cuentas bancarias y las transferencias electrónicas. Bitcoin no se queda ahí. Lo que lo hace diferente es que no es una forma de dinero que se registra en una base de datos. No es una forma digital de dinero que representa una deuda contraída con un banco central o con algún gobierno. Tampoco es una forma digital de dinero que haya sido emitida por el banco central soberano de un Estado o de un rey. Es una forma de dinero digital que ha sido emitida a través de la computación compleja y, por tanto, fruto de un alto consumo energético en Internet. Se registra simultáneamente en cada equipo que participa en la red Bitcoin y está validado de forma independiente por cada equipo que participa en la red Bitcoin. No puede ser falsificado. No puede ser censurado. No puede ser bloqueado ni requisado. Puede ser transmitido a cualquier parte del mundo como información. Puede ser verificado de forma independiente por cualquier persona que lo reciba. Y no es controlado por nadie, su valor no se controla, su emisión no se controla, su propiedad no está controlada. Es dinero que viaja directamente de una persona a otra persona sin intermediarios.

Cuando se realiza una transacción en el sistema Bitcoin no hay nada que obligue a relacionarla con una identidad. No es necesario crear una cuenta con los datos personales. No es necesario registrarse en ningún sitio. No es necesario identificarse o dar el nombre o la ubicación o la dirección o la edad o el sexo o la raza o la religión o la nacionalidad. Nada.

Ni siquiera es necesario ser humano! Bitcoin permite por primera vez en la historia que entidades no humanas puedan controlar y poseer valor lo cual es algo muy extraño porque nunca hemos tenido nada similar en ningún sistema legal del mundo. Existe algo parecido, la ficción legal de que empresas y corporaciones puedan poseer valor, pero las empresas sólo pueden existir como asociaciones entre seres humanos vivos, que acaban tomando decisiones y que, al final, son los propietarios de ese valor.

En Bitcoin un agente de software que no es propiedad de ninguna persona, mediante el uso de la criptografía, puede poseer y realizar transacciones en la red Bitcoin. Esto crea algunas posibilidades muy interesantes pero también algo inquietante de cara al futuro. Los sistemas de inteligencia artificial podrán poseer y controlar dinero sin que ningún humano vivo esté involucrado. Aparecerán corporaciones que no tendrán ejecutivos o directores, que no tendrán seres humanos que tendrán a la corporación bajo su control o que tomaran decisiones en nombre de ella. Estas corporaciones serán totalmente controladas por software.

En resumen, las características principales que definen a Bitcoin serían:

1) Utiliza la tecnología y protocolo Blockchain, es decir, un libro contable, distribuido de manera global, que contiene información inmutable sobre transacciones y que se presenta ordenado de manera totalmente cronológica.

2) Establece consensos de manera continua y descentralizada a través de un mecanismo llamado Proof of Work que, al mismo tiempo, asegura la red y nos permite confiar en ella.
3) El sistema de acceso es abierto, pues permite que cualquiera pueda participar sin barreras ni filtros.
4) Es neutral, porque no hace diferencias de clase entre sus usuarios (lo único que importa es si una transacción es válida y no quién es el emisor o el receptor)

Las principales ventajas como medio de pago serían:

Mayor privacidad ya que consigue eliminar la interferencia de terceros en las transacciones.

Aumento decreciente y predecible de la masa monetaria (la masa monetaria aumenta año tras año pero cada año aumenta una cantidad más pequeña hasta llegar al año 2130 en el que dicho aumento será despreciable y se considerará terminada la emisión total de bitcoins). Este comportamiento de la emisión de nueva moneda, a diferencia de las monedas o divisas actuales, ayuda a preservar - y probablemente a mejorar - el poder adquisitivo de los usuarios.

Muy menores - e incluso nulas - comisiones por transferencias comparadas con las que son cobradas por los bancos o por servicios de pago en la red (PayPal). Estas comisiones pequeñas no son para un intermediario propiamente dicho pues se las queda el minero que consigue validar un bloque y su función es aportar incentivos para que siga habiendo mineros que mantengan la red. Además, estas comisiones son voluntarias si lo que pretendemos es que se valide nuestra transacción lo más rápidamente posible pero nadie está obligado a pagarlas si acepta con ello el tiempo medio de 1 día para estar totalmente seguro que la validación es definitiva.

Simplifica y acelera el pago persona a persona, prescindiendo de intermediarios no deseados.

Tal y como lo ha sido el dinero efectivo en toda su historia, los bitcoins o las dirección Bitcoin asociadas a monederos de usuarios puede ser anónimas, si así lo desean los propios usuarios.

Permite realizar transferencias a cualquier parte del mundo al mismo coste

Es transparente: aunque nadie está forzado a revelar su identidad, todas las transacciones quedan grabadas para la eternidad en un registro de libre acceso (Blockchain) y que está a disposición de todos (se puede consultar online en internet y todos los mineros lo tienen localmente en su disco duro). Es importante no mezclar los conceptos de transparencia y anonimato. En el sistema Bitcoin, se puede llegar a esconder nuestra identidad pero lo que nunca podremos esconder son los movimientos que hace nuestra cuenta, es decir, cuánto dinero recibimos, de qué cuenta, cuánto dinero enviamos y a qué cuenta (sistema totalmente transparente)

Admite transacciones complejas (depósitos en custodia; seguros de depósitos; garantías; mediación, etc.) con un firme apoyo criptográfico para todo tipo de reglas y condiciones libremente acordadas por las partes.

Nunca se detiene: no hay festivos ni fines de semana para las operaciones en bitcoins.

Hace viables los micropagos a gran escala.

Impide la congelación de fondos (ningún gobierno, banco o institución puede embargarnos o bloquear nuestros fondos)

Impide la reversión involuntaria de pagos.

Impide la restricción arbitraria de bienes y servicios que pueden adquirirse (no importa quién eres, que raza, clase social, sexo, edad o nacionalidad tengas) No es necesario apelar a terceros para su custodia o traslado.

Se puede guardar en múltiples localizaciones simultáneamente.

No requiere confianza en un tercero ni en un determinado sistema legal para preservar su valor. Ni tan siquiera hay que confiar en la comunidad, que podría ser un tipo de tercero. De hecho Bitcoin es un sistema que permite la desconfianza en la comunidad o en la posibilidad que haya alguien malintencionado en la comunidad. La confianza es en las matemáticas que se encuentran detrás de la criptografía y la Teoría de Juegos que nos protegen de la existencia de miembros malintencionados en la comunidad.

Facilita la protección contra el robo en todas sus formas

La tecnología de encriptación en que se basa el protocolo de Bitcoin es varias veces más segura que la empleada por los bancos y las compañías que gestionan los pagos con tarjetas de crédito (VISA, Mastercard).

No puede ser eliminado por ataques legales / informáticos, dada su naturaleza descentralizada.

No se puede falsificar.

Es fácil e instantáneamente reconocible.

Es, a efectos prácticos, infinitamente divisible.

Hay toda una serie de ejemplos reales de cosas que se pueden hacer hoy en día con bitcoins u otras criptomonedas que con los otros medios de pago tradicionales es prácticamente imposible llevar a cabo:

Dar 10 céntimos a tu blogger favorito con un coste de transacción menor a un centavo.

Escribir un libro, crear una obra de arte, tocar y / o cantar una canción; subirlas a Internet y venderlos sin demoras y, además, minimizar la piratería porque al ser posible pagar cantidades muy pequeñas y directamente al autor aumentan las posibilidades de concienciación de la gente por el pago de contenidos.

Enviar 1euro a una persona con un coste de transacción menor a un centavo, sin importar la distancia a la que ésta se encuentre.

Enviar diez mil dólares a una persona con un coste de transacción menor a un centavo, sin importar la distancia a la que ésta se encuentre.

Tener una cuenta de ahorro sin necesidad de pagar a un tercero por el servicio.

Abrir una tienda en línea en minutos sin tener que utilizar carros de compras ni proceso de pagos, y sin costes adicionales.

Cobrar por un bien o servicio sin tener que preocuparse por si PayPal o las empresas de tarjetas de crédito te pedirán que les devuelvas el dinero (por ejemplo, en el caso que se demuestre que a la otra persona le han robado la tarjeta y alguien ha hecho un pago ilícito con ella)

Dar dinero a una organización que tu gobierno (o Pay Pal) desaprueba; poder hacerlo anónimamente. Muy interesante en casos donde se quiere financiar organizaciones vetadas por intereses económicos de un país (ejemplos claros son las donaciones a Greenpeace, a Wikileaks, etc)

Proteger tus ahorros de la inestabilidad económica y las políticas financieras absurdas de tu país

Viajar a otro país y poder costear los gastos sin necesidad de pasar por una casa de cambio (en un futuro próximo cuando la mayoría de servicios básicos se puedan conseguir en bitcoins u otros criptomonedas)

Por otro lado hay una serie de falsos mitos o dudas que genera el uso del Bitcoin y que habría que puntualizar:

1. Los gobiernos podrían acabar con Bitcoin cuando lo perciban como una amenaza?

Si Bitcoin funciona en el país más intervencionista y censurador del mundo, China, es que puede funcionar en cualquier país del mundo. Y no pensemos que China no se ha esforzado en censurarlo porque Bitcoin aún no le ha representado una amenaza real ya que los eventos sucedidos en China en Agosto de 2016 demuestran todo lo contrario: la fuga de capitales a través de Bitcoin de muchos ahorradores para protegerse de las continuas manipulaciones del Banco Central con su moneda (devaluación forzada del yuan) hicieron tomar al gobierno chino medidas severas contra la criptomoneda para intentar evitarlo. Por otro lado, en el hipotético caso de que pudiera ser censurado de alguna manera, sólo sería necesario un usuario que actuara de bridge (puente) con el exterior – con una comunicación telefónica, radiofónica o hasta por satélite – y los esfuerzos de censura en ese territorios quedarían totalmente desactivados.

Volviendo al ejemplo chino de las compras de bitcoins para evitar pérdidas en ahorros o para evitar la inseguridad o incertidumbre en las inversiones, como decíamos, estas compras provocaron la furia del gobierno chino y un control muy duro sobre las casas de cambios (que son a los únicos puntos de la red Bitcoin que, en cierta medida, aún pueden ser controlados por la administración de un Estado porque es el Estado quien da la licencia a las empresas que operan con la moneda nacional ofreciendo cambios con otras divisas o commodities, en este caso, por otras criptomonedas). Este control llegó hasta el punto de suspender temporalmente las licencias de operación de las casas de cambio de China. Pero lo único que han conseguido es un desplazamiento de los cambios de divisas de las casas de cambio chinas a las japonesas, es decir, una disminución del negocio de sus empresas nacionales. Y todo ello sin tener en cuenta que estas compraventas de bitcoins también se pueden hacer por fuera del circuito (en los mercados Over the Counter, OTC) donde se pueden comprar y vender grandes cantidades de bitcoins de persona a persona o de entidad (eso sí, sin ninguna empresa que opere como intermediaria dando garantías a nivel contable y a nivel de marco regulatorio con su licencia).

Por otra parte, técnicamente sería muy difícil que, en el caso de que los Gobiernos presionaran a las operadoras de telecomunicaciones para que prohibieran el tráfico específico de Bitcoin, realmente obtuvieran algún resultado efectivo ya que es bastante fácil enmascarar el tráfico de Bitcoin. Además, sólo que hubiera un solo país donde no estuviera prohibido, el problema desaparecería ya que sólo haría falta contratar una VPN que tengas salida en ese país o instalarse algún proxy de aquel país (de la misma manera que hace la gente que quiere ver partidos de fútbol o series que sólo se pueden ver en otros países). Y todo ello sin tener en cuenta que, por ejemplo en las ciudades, en un caso extremo, se podrían llegar a desplegar redes WIFI privadas

con cobertura en toda la ciudad que fueran totalmente independientes de las grandes operadores de telecomunicaciones.

2. Podría haber un multimillonario que comprara la mayoría de los bitcoins y luego se dedicara a manipular el mercado?

En primer lugar, como el número de bitcoins es limitado, su precio aumentaría bruscamente. Esto enriquecería los poseedores actuales de bitcoins. Entonces, las expectativas y las órdenes de venta cambiarían inmediatamente y entre la gente que aún no tendría bitcoins se desencadenaría una masiva “fiebre por el bitcoin”. Con unos cuantos millones de euros alguien podría comprar muchos bitcoins, pero NO una elevada proporción de los bitcoins disponibles. Primero, porque la mayoría de los bitcoins ni siquiera están a la venta (los que se negocian son una fracción mínima del total), y segundo porque si, por ejemplo, Warren Buffett decidiera invertir buena parte de su fortuna en bitcoins, el primer Bitcoin le costaría unos 1.100 eur (al precio actual), pero el último le costaría probablemente millones de euros si es que, en esos momentos, tuviera la suerte de encontrar a alguien dispuesto a vendérselos.

Por otra parte, supongamos que un magnate – o un gobierno – de algún modo consigue adquirir un porcentaje significativo de todos los bitcoins que hay a día de hoy… ¿Qué poder le otorgaría esto? el de venderlos en un instante para deprimir el precio transitoriamente, después de haber pagado millones o billones de euros para adquirirlos? ¿Cuántas veces podría hacer algo así antes de perder todo su "poder de fuego" en manos de cada vez más compradores de oportunidad? ¿Y todo esto para qué?

Lo único que conseguiría el autor de un "ataque de fuerza bruta monetaria" es despertar el interés de todo tipo de inversores, que pasarían a competir con él por un activo en rápida apreciación...

3. Se podría destruir la red Bitcoin por culpa de una espiral deflacionista de los precios?

El número de bitcoins que se generarán ya está predefinido y tiene un límite: 21 millones. No me pregunten por qué la cifra de 21 millones pero el hecho es que es así como lo definió Satoshi Nakamoto (quizás lo escogió para dar alguna pista sobre su identidad, por ejemplo haciendo referencia a la película "21" que se estrenó casualmente pocos meses antes, en marzo del mismo año 2008, y que hablaba de un grupo de matemáticos del MIT que deciden utilizar su talento e inteligencia para ganar cantidades ingentes de dinero utilizando técnicas matemáticas jugando en los casinos de Las Vegas. Además, al final de la película hay un guiño al tema en cuestión donde el botín final resulta que ha estado substituido por unas monedas doradas de chocolate muy parecidas a las que se utilizan gráficamente para representar a los bitcoins. También, en una versión más "espiritual ", bien podría ser que Satoshi hubiera elegido el 21 porque, en la Biblia, este número es el símbolo de la perfección y la madurez).
Todo esto son simples especulaciones pero el hecho real es que los bitcoins se van generando cada vez que hay un proceso de minado (un proceso de minado se da cada vez que se genera un nuevo bloque, cada 10 min se crean unos bitcoins y es el "minero" o la persona que tiene el

ordenador que ha conseguido generar el nuevo bloque, quien se los queda. Es su premio como ganador de la "carrera" por ser el primero que genera un bloque). Además, el número de bitcoins que se van creando (los premios o recompensas para los mineros que se dan en cada nuevo bloque) van disminuyendo con el tiempo: cada 4 años, la cantidad disminuye a la mitad, por ejemplo, ahora mismo, cada vez que un minero genera un bloque, la persona que tiene el ordenador que lo ha generado gana 12,5 bitcoins pero en 4 años pasará a ganar solo 6,25 bitcoins. Esto implica que, a medida que pasan los años, cada vez se generan menos bitcoins y que, si como máximo se pueden generar 21 millones, en Marzo de 2140 se terminará de generar el último Bitcoin. De este modo, nos encontramos con un sistema monetario en el que, a medida que avanza el tiempo, el número de monedas nuevas que entran en circulación es cada vez más escaso y, como consecuencia, su valor aumenta. Si el valor del Bitcoin aumenta, el coste de los productos en relación al Bitcoin irá disminuyendo progresivamente. ¿Quiere decir esto que vamos a entrar en lo que los economistas llaman una espiral deflacionista (caída inesperada y sistémica de precios)?

No, porque en realidad este fenómeno sólo se produce durante la reubicación de los recursos que suele pasar una economía después de un colapso financiero y, sobre todo, después de un colapso financiero que viene como consecuencia de años de inflación crediticia y de ir hinchando la burbuja inyectando más deuda. Y está claro que esta no es la situación porque en el sistema Bitcoin no hay inflación crediticia sino todo lo contrario.
Por otro lado, hay gente que dice que si la moneda es deflacionaria, entonces ¿quién se gastaría unos bitcoins si el valor se incrementa con el paso del tiempo, en lugar de guardarlos indefinidamente?
Respuesta: ¡quien en un determinado momento valore lo que puede adquirir con ese dinero... más que al dinero en sí mismo! Un buen ejemplo de esto es el de la tecnología informática: la gente sigue comprando ordenadores, aun sabiendo que, en un futuro cercano, los ordenadores tendrán más memoria, mejores baterías, serán más rápidos, más portátiles, más amigables... y, sobre todo, más económicos. Por lo tanto, si lo compran, es porque realmente, en ese momento, para el comprador tiene más valor el producto que el dinero. Es verdad que este ejemplo de los ordenadores parte de la idea de un escenario inflacionista (que es el que ha habido siempre) pero, incluso teniendo en cuenta esto, el comprador siempre puede terminar comprando porque el valor que le otorga al producto es superior al que él le da a las monedas en ese momento. Lo único que cambia en este caso, es que cuando piensa con el valor de las monedas piensa con el valor actual más el incremento que tendrá en un futuro. Pero el resultado es el mismo, termina haciendo un juicio entre el valor del producto y el valor del dinero más su incremento futuro y se queda con el primero.

Renunciar a gastar bitcoins adquiridos no es un problema para el sistema; por el contrario, es una prueba de la confianza en su valor futuro y de sus excelentes cualidades monetarias (la gente tiene la costumbre de desprenderse de la mala moneda).

Por tanto, en el fondo, lo que hace una moneda deflacionaria es, indirectamente, forzar la apuesta por proyectos a largo plazo. Y proyectos a largo plazo es precisamente lo que le falta a nuestra sociedad (las compañías que cotizan en bolsa actúan por resultados anuales, sus directivos obtienen primas por resultados a corto plazo, los políticos aplican políticas que

afectan sólo a sus mandatos de 4 años, etc.). En cambio, Bitcoin incentiva el ahorro y la inversión a largo plazo, al tiempo que desincentiva el consumo irracional y el endeudamiento insostenible.

4. ¿Es cierto que Bitcoin ha sido hackeado o pirateado? ¿Bitcoin es seguro?

Una transferencia entre direcciones Bitcoin es varias veces más segura que una transferencia entre cuentas de diferentes bancos (sin contar el riesgo que implica la forzosa intromisión de terceros en el sistema bancario). El código de Bitcoin es auditable para quien lo desee, es decir, está abierto al examen de todos los interesados para encontrar vulnerabilidades y agujeros de seguridad gracias a que es público.

Además, el diseño de Bitcoin y su arquitectura criptográfica admite actualizaciones futuras para hacer frente a potenciales ataques. Los ataques que ha habido hasta el momento, y que han aparecido en los medios de comunicación, presentan a Bitcoin como un sistema inseguro y vulnerable y, en realidad, no han sido ataques al sistema Bitcoin sino a las bases de datos de las webs de casas de cambio de bitcoins porque estas empresas no tenían sus redes privadas correctamente securizadas. Así pues, afirmar lo contrario es tanto absurdo como decir que un hackeo a las bases de datos de un banco sería un hackeo al dólar o al euro.

Además, insisto, la red Bitcoin nunca ha podido ser hackeada hasta el momento y podemos estar seguros de que grandes intereses (sobre todo de la banca), mentes brillantes (informáticos y matemáticos) y hackers de todo tipo lo han estado intentado durante los últimos años y, para su desgracia, no han cosechado éxito alguno en su aventura.

5. Como puede generar confianza un sistema monetario utilizado por sujetos anónimos? Puede el anonimato significar un agujero para la evasión de impuestos?

El anonimato no es algo que Bitcoin impone; es una elección que Bitcoin admite. Además, llevamos toda la historia conviviendo con un sistema anónimo: el dinero en efectivo. Por otra parte, es cierto que Bitcoin puede ser utilizado con fines ilícitos pero también es cierto que lo pueden ser el dólar, el rublo, el euro, etc. Además, también los cuchillos pueden ser utilizados con fines ilícitos y nunca se han prohibido simplemente porque son de gran utilidad para la sociedad y no nos podemos privar de los mismos.

Además, mi intuición, me dice que es perfectamente plausible un escenario en el que, la única manera de acabar con la evasión de impuestos e, incluso, la elusión fiscal injusta socialmente, es la contraria a la utilizada en la actualidad: la supuesta persecución "implacable" de Hacienda. Cuando todos sabemos que Hacienda no tiene los recursos ni los medios para serlo y, especialmente, con quien se puede permitir gabinetes de juristas profesionales para hacer "ingeniería" fiscal. Por tanto, una manera de conseguir terminar con ello podría ser justamente la contraria, es decir, provocar que lo pueda hacer todo el mundo! Si lo puede hacer todo el mundo, entonces ya nadie puede obtener una ventaja competitiva sobre nadie y nos pone a todos por igual. Es en este momento, cuando el Estado o las mismas elites se pondrían las pilas para evitar la sangría masiva. Es en ese momento cuando el sistema de por sí puede actuar de manera natural (no manipulada) y terminar emergiendo una solución real y efectiva (un sistema contable de gestión de impuestos basado en Blockchain?)

4. Estatus legal de Bitcoin

Uno de los aspectos más importantes de la definición legal del dinero es que éste debe tener una identidad nacional. Bitcoin nunca ha sido utilizado como moneda nacional, pero no hay que descartar esta posibilidad: bajo ciertas circunstancias, un país podría abolir su propia moneda y adoptar a Bitcoin u otra criptomoneda como moneda nacional. ¿Qué país escandinavo será el primero? Dinamarca, Estonia, Suecia? Precisamente Suecia fue el país que puso en circulación un billete por primera vez en la Historia... será el primero en suprimirlos totalmente? Recordemos que los países nórdicos ya no fabrican moneda ni billetes (lo tienen contratado a empresas extranjeras) y, por ejemplo en Dinamarca, más del 80% de los pagos ya se hacen por internet o con tarjetas.
Una razón por la que podría considerarse a Bitcoin como una forma de dinero es que hay mercados de intercambio, y por tanto, de facto, los bitcoins se tratan como dinero. A diferencia de la mayoría de las commodities tangibles, los bitcoins son electrónicos, tienen un coste de transacción prácticamente nulo, son fungibles (aunque se podría debatir sobre esta propiedad), son extremadamente divisibles y pueden intercambiarse rápidamente por una gran cantidad de divisas.

Hay muchas categorías en las que Bitcoin podría encajar, y no son todas mutuamente excluyentes. Podría caracterizarse como un título o valor. Aunque no sería acertado que los títulos o valores tengan un emisor institucional. Tal vez se parecería más a una commodity; poseer bitcoins es algo así como ser el dueño de una cantidad de carbón almacenado en un contenedor. Esta posesión es transferible. Si uno es dueño de acciones de, por ejemplo, Apple, el valor de lo que uno tiene dependerá de las ganancias futuras de la compañía, es decir, de las decisiones que tomen sus directores, de las condiciones del mercado, etc. En cambio, los bitcoins no generan ganancias de por sí que deban ser repartidos entre los dueños de los bitcoins (1 Bitcoin hoy seguirá siendo un Bitcoin dentro de 10 años, es decir, nadie te dará mas bitcoins en el futuro si las cosas van bien sólo porque tú ahora tengas un Bitcoin. Lo máximo a lo que puedes aspirar es que ese 1 bitcoin se cambié por mas euros 10 años después de haberlo adquirido pero no que tengas 1 bitcoin y pico).

Respecto a definir Bitcoin como reserva de valor (según la típica definición legal) parece una definición atractiva, pero Bitcoin no involucra un contrato en base al cual uno puede, en el futuro, reclamar un valor. Tener bitcoins no implica una relación con un emisor.

Si vamos a lo que es oficialmente considerado por las autoridades a día de hoy, vemos que es considerado como una commodity electrónica por el ente de regulación de commodities americano (la CFTC o Commodity Futures Trading Commission) pero también fue considerado como una digital currency por el Tesoro de los EEUU en la resolución del 19 de Noviembre de 2013. En Europa incluso es considerado como una moneda convencional, tal y como resolvió el Tribunal de Justicia de la Unión Europea el 22 de octubre de 2015.

Así, en la UE, esta sentencia significó que la compra-venta de bitcoins estuviera libre de impuestos (IVA) en todos los países que forman parte de la jurisdicción del Tribunal. También en la compra de cualquier producto se dejó de calcular el IVA sobre el valor en bitcoins de la propia compra (el IVA ahora ya sólo aplica sobre el valor del propio producto como ocurre en cualquier compra hecha con cualquier otra moneda nacional).

Es curioso señalar cómo, antes de esta sentencia, diferentes países se habían mostrado individualmente con visiones contrarias: mientras que la autoridad fiscal del Reino Unido había adoptado la posición que bitcoin es una moneda, en algunos países, como Suecia y Alemania, habían argumentado que debería ser tratado más como una mercancía o commodity, por lo que una simple transferencia de la misma debían estar sujeta a impuestos en (IVA). De todos modos, con la sentencia del Tribunal de Justicia de la UE, ahora todos los países se han acabado alineando con la sentencia.

Esta decisión a nivel europeo ha significado un impulso muy significativo para Bitcoin en una de las zonas comerciales más grandes del mundo. Hasta entonces el doble impuesto (al producto que comprabas y a la cantidad de bitcoins utilizada) había elevado el coste de la compra o el uso de la moneda virtual en toda la Unión Europea.

Por otra parte, el año pasado, el ministro de Finanzas de Luxemburgo otorgó a la empresa Bitstamp la licencia para operar libremente como una entidad de pago en su país lo que le dio acceso a prestar servicio a los 28 estados que conforman la Unión Europea a partir del 1 de julio de2016. Así Bitstamp ha convertido en la primera casa de cambio de Bitcoin en obtener esta aprobación.

Esta licencia, entre otros beneficios, ofrece a Bitstamp la posibilidad de asociarse con cualquier entidad bancaria europea. La empresa también permitirá a sus clientes cambiar bitcoins por euros y viceversa, contando con la confianza proporcionada por una casa de cambio con licencia. Además, según las propias declaraciones del ministro de Finanzas de Luxemburgo, este suceso marcará un antes y un después para Bitcoin y la tecnología financiera en Europa, cuestión que podría hacer surgir una nueva industria estandarizada al menos en los países europeos.

En paralelo, después de una espera de casi cuatro años, en EEUU, se fijó la fecha límite del 11 de marzo de 2017 para que la SEC (organismo regulador estadounidense de seguros y productos financieros) aprobase o no una regulación que permitiría al ETF Bitcoin de los hermanos Winklevoss entrar en el Mercado Global Bates (los hermanos Winklevoss son los que invirtieron en Facebook antes que saliera y que perdieron su litigio con Mark Zuckerberg) .También hay otros dos fondos que han completado peticiones similares para entrar en la lista de la Bolsa de Acciones de Nueva York. No hay ninguna garantía de que cualquiera de estas solicitudes tenga éxito. Pero la mayoría de los expertos afirma que un ETF Bitcoin es eventualmente inevitable (recordemos que un ETF es un producto financiero que se negocia en la Bolsa pero que hace referencia a las pérdidas o beneficios que se dan en un fondo de inversión concreto, Por ejemplo , un ETF del Litio es un producto financiero que está asociado a una cartera o fondo de inversión que invierte todo lo que la gente ha "depositado" en el ETF en empresas o actividades relacionadas con el Litio: acciones en empresas de minería de litio, compra directa de litio, acciones en empresas de baterías, acciones en empresas proveedoras de centrales nucleares de fusión experimentales, acciones en empresas de coches eléctricos, de móviles, etc.)

La SEC se mostró muy reticente a la aprobación por temas de seguridad pero los hermanos Winklevoss siguen intentando avanzar en los problemas que hicieron a la SEC denegar el acceso al mercado: por ejemplo, proponen mantener las claves privadas cerradas en ordenadores sin conexión y que estas, a su vez, estén bloqueadas en localizaciones seguras. Por tanto, para que hubiera un robo, múltiples individuos en múltiples sitios deberían otorgar simultáneamente acceso a un actor malintencionado que quisiera las llaves.

Aun así, la SEC, de momento, rechaza su aprobación por razones de conflicto de intereses porque los Winklevoss se han quedado simultáneamente con varias funciones importantes en un fondo ETF: ser la promotora del ETF, la proveedora del precio de referencia para a la acción subyacente y poseer la custodia de esta acción, todo al mismo tiempo.

Ciertamente, lo que algunos ven como una oportunidad para que los inversores medios participen en una de las grandes innovaciones financieras de estos años podría detonar en una gran subida de la cotización del Bitcoin y una locura de intercambios en un mercado bastante salvaje de por sí.

Para acabar de complicar la situación, el reducido tamaño del mercado de intercambio de bitcoins por divisas que hay hoy en día, podría ser un impedimento para el comercio apropiado del fondo. Además, en Estados Unidos, sumando todos los intercambios, el volumen medio diario de bitcoins que se compran o venden es de unos 30 millones de dólares. Pero si se aprueba el ETF estamos hablando de, como mínimo, 300 millones de dólares que seguramente entrarían durante la primera semana (300 millones es la media que entra durante la primera semana en cualquier ETF que es aprobado). Además, se trata de una extraordinaria oportunidad para inversores en Bitcoin que ahora mismo no tienen posibilidades de hacerlo en el sistema financiero tradicional. Por ejemplo, Inversores institucionales como fondos de pensión no han podido nunca tomar parte de Bitcoin ya que muchas de sus directrices exigen que los valores de su cartera estén registrados oficialmente por las autoridades estatales.

Además, si empezara a entrar mucho capital nos podríamos encontrar con otro problema porque por ejemplo, ahora mismo, es imposible comprar 2 millones de dólares en bitcoins cualquier día en una casa de cambio de EEUU sin mover el mercado. Y por cada acción de la ETF que se comprara, un "participante autorizado" –el propio creador del mercado de fondos – tendría que comprar una cantidad equivalente en bitcoins. Esto, de rebote haría aumentar la actividad de los mercados extrabursátiles Over The Counter (OTC) que son mercados secundarios no regulados donde se pueden conseguir grandes cantidades de bitcoins directamente de privados (obviamente con un sobreprecio). Estos mercados OTC (que fueron uno de los grandes causantes de la crisis financiera internacional de 2008 por su opacidad y falta de control) permiten la compra directa, de persona a persona, sin pasar por una casa de cambios y son muy utilizados cuando se quieren hacer compras masivas de activos sin que la propia compra haga subir el precio y el que la hace acabe saliendo perjudicado como pasa en los mercados de compra-venta regulados (donde, el simple hecho de comprar 1 bitcoin hace aumentar el valor del mismo y la compra del siguiente bitcoin ya resulta más cara)

Así, la posibilidad de lanzamiento del primer ETF asociado a Bitcoin podría conducir a una exuberancia irracional si el precio del bitcoin aumenta dramáticamente. Si es así, se podrían ver comportamientos hasta ahora nunca vistos. Estamos hablando de las chispas que podrían saltar en poner en contacto por primera vez la red de pagos descentralizada Bitcoin y el sistema financiero internacional. Y todavía no sabemos muy bien cuál será la reacción de ambos mundos el día que finalmente se produzca este choque.

5. Blockchain

Como decíamos, Blockchain es la base que ha dejado Bitcoin para experimentar y sobre la que se puede producir la verdadera disrupción. ¿Será Blockchain la base de un nuevo sistema diferente a todo lo que hemos visto hasta ahora (feudalismo, comunismo o el actual, el capitalismo)?

Veamos qué es exactamente Blockchain:

Recordemos que Blockchain significa Cadena de Bloques. Cada Bloque no es más que un archivo donde se encuentran todas las transacciones de bitcoins que se han hecho durante los 10 min previos al comienzo del minado o creación de ese bloque. Todos los bloques están matemáticamente ligados unos a otros siguiendo un orden cronológico. Por tanto, ahora mismo tenemos una cadena de aproximadamente 475.000 bloques que va pululando por Internet. Esta cadena, actualmente, ocupa 20 Gb en el disco duro de cualquier minero que se instale el software cliente de Bitcoin.

En el fondo, lo que se crea con el protocolo Blockchain no es más que un Libro mayor o Libro maestro que actúa como registro único común y que está localizado en todas las máquinas que son miembros de la red, es decir, en todos los ordenadores, servidores, tablets o móviles repartidos por el mundo que tienen instalado el software de Bitcoin. Podríamos decir que en esta red, y en cualquier Blockchain, todos somos notarios de la información, todos damos fe de que la información que hay registrada es válida, es decir, todos escuchamos o leemos la información, la comprobamos, la cotejamos y la verificamos.

Por lo tanto, Blockchain no es más que un protocolo que permite disponer de una base de datos distribuida entre los miembros de la red que la componen y que, cada vez que se registra nueva información (las últimas transferencias en el caso de Bitcoin), se hace por consenso.

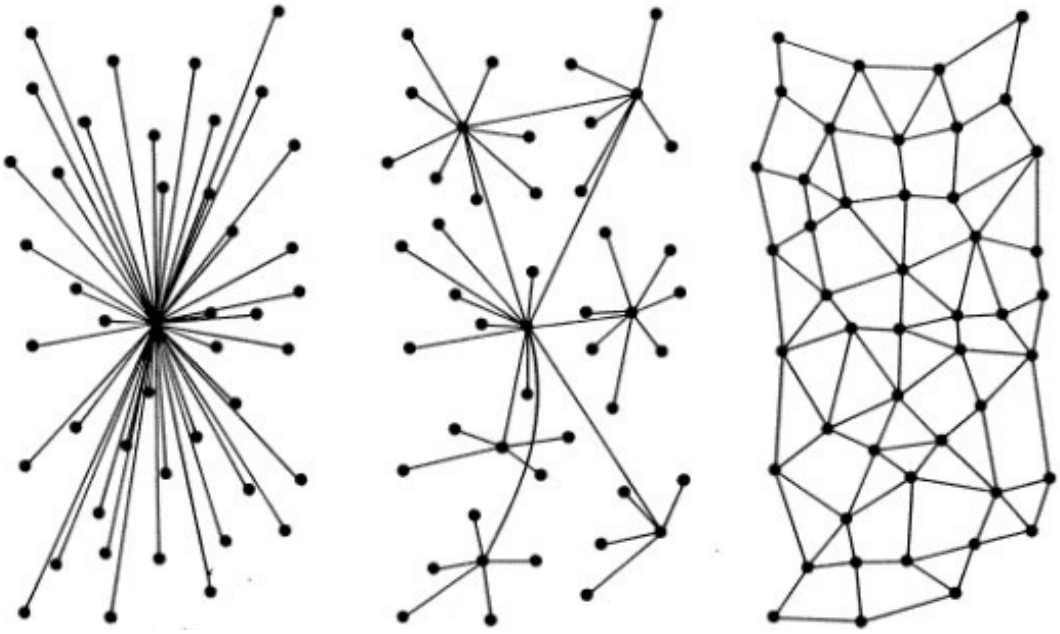
Es decir, se trata de un protocolo que permite establecer consensos automáticamente y de manera descentralizada (lo valida la mayoría de los miembros, no una entidad central). Por ejemplo, en el caso de la Blockchain Bitcoin (más adelante veremos que puede haber otras Blockchains que no sean de Bitcoin), si se pretende que en la próxima actualización del registro o Libro mayor (en 10 min) figuren una serie de transferencias pero que unas concretas no estén, entonces, la única manera de hacerlo es conseguir que más del 50% del poder de decisión de los miembros de esta red piense igual que tú y tampoco quiera incorporarlas al libro mayor. Tiene sentido, no es más que el poder democrático de la mayoría.

La idea que hay detrás de este "consenso" que se establece cada 10 min de manera automática y descentralizada es precisamente la idea feliz que tuvo Satoshi para poder superar el 2º obstáculo que se indicó en la Introducción : la posibilidad de replicar infinitamente y sin coste la información digital.

En una red centralizada donde hay intermediarios (por ejemplo, los bancos), este problema puede quedar solucionado con el control y la garantía que da el propio intermediario. Pero, para solucionar este problema en una red descentralizada, donde no hay ninguna entidad central que pueda validar que una persona no esté gastando su dinero dos veces, se debe conseguir definir un sistema que establezca, de manera automática, un consenso sobre esta decisión entre todos sus miembros. El sistema debe ser descentralizado y de confianza.

Este consenso debe ser tal que al menos el 50% de los miembros se pongan de acuerdo en que un dinero que se ha gastado o transferido no se pueda volver a gastar o transferir una segunda vez. Y además, hay que ir rápido en establecer este consenso porque 10 min después ya hay que empezar a trabajar para la validación de las siguientes transferencias y la generación del siguiente bloque.

Para entender cómo se establece este consenso de manera automática y segura primero se debe visualizar esquemáticamente cómo está organizada la red que forman todos los miembros de una Blockchain. Lo primero que hay que tener presente, como se ha insistido varias veces, es que se trata de una red descentralizada, es decir, una red donde para ir de un punto a otro no se debe pasar siempre por una zona central ya que todos los miembros se comunican entre ellos a través de otros miembros vecinos que hay por el camino. Además, esta red también es distribuida porque siempre hay diferentes caminos o rutas para ir de un punto a otro y no hay ninguna entidad central que gestione las comunicaciones que sea indispensable para las relaciones entre sus miembros.



(I) Red centralizada (II) Red descentralizada
(III) Red distribuida

Figura 1. Tipos de redes

Por otra parte, en esta red hay básicamente 2 tipos de miembros. Podríamos decir que unos tienen un rol más activo y los otros un rol más pasivo.

Los que tienen un rol más activo se les llama "mineros" y, en el caso de la Blockchain Bitcoin, son todos aquellos que tienen instalado el propio software de Bitcoin y cuyos ordenadores o servidores se dedican automáticamente (sin ninguna acción de las personas) a hacer unos servicios indispensables para la comunidad:

1) validar que las transacciones que realizan los usuarios de Bitcoin sean correctas (por ejemplo, que nadie intente enviar más dinero del que realmente tiene en su cuenta o gastarlos más de una vez)

   y

2) trabajar para que todas las transacciones válidas queden incluidas por la eternidad en la Blockchain (en el registro común, en el Libro Mayor), es decir, "trabajar de manera consensuada con todas las demás mineros" para la generación de un bloque cada 10 min

El gasto de energía que dedican los ordenadores de los mineros para llevar a cabo estas dos funciones (que es bastante elevado), lo compensan con unos bitcoins que pueden ganar si son los primeros que consiguen generar un bloque en una ronda. Esta recompensa es bastante cuantiosa y, de hecho, los mineros hacen negocio porque el coste de la electricidad y los ordenadores es menor que las ganancias medias que se obtienen a partir de las recompensas. En realidad, lo que hace la mayoría de mineros es asociarse en grupos grandes, que se llaman pools (similar a lo que vendrían a hacer las peñas quinielísticas) y así obtienen unas ganancias mínimamente asegurados repartiéndose los premios)

Es importante señalar que cualquiera que lo desee puede ser minero. No hay ninguna barrera de entrada ni ninguna licencia a pagar. Lo único que hay que hacer es instalar el software gratuito de Bitcoin y asumir el consumo continuo y el coste de la electricidad de tener el procesador del ordenador o servidor funcionando las 24 horas del día, 365 días al año. Cabe decir que si no se tiene un ordenador dedicado a ello, el propio irá más lento.

Por otra parte, los miembros que tienen un rol más pasivo vendrían a ser los usuarios normales que lo único que quieren es poder hacer compras o transferencias con bitcoins.

Los 2 tipos de usuarios se han de instalar el software o aplicación Bitcoin pero la versión que utilizan los usuarios normales es una versión más reducida y simplificada que la que utilizan los mineros (y ocupa sólo unos pocos Mb). La diferencia es que el software Bitcoin de los mineros debe incorporar la información de todos los bloques que se han generado desde el min 0 (Enero 2009), es decir, un archivo de 20 Gb porque lo tienen que utilizar para comprobar que los usuarios que quieran hacer transferencias no hayan hecho algunas en el pasado que hayan dejado su saldo a 0 o que no estén utilizando el mismo dinero más de una vez.

En cambio, los usuarios normales que solo quieren operar con bitcoins, lo único que deben hacer es instalar una pequeña aplicación o app en su ordenador y, como esta versión ocupa tan poco, también se puede instalar en el móvil o la tablet. Entonces, desde la aplicación correspondiente, ya se pueden enviar o recibir bitcoins y saber el saldo en cada momento (esta aplicación se la suele llamar "monedero")

La arquitectura de una red descentralizada como Bitcoin puede representarse gráficamente de la siguiente manera:

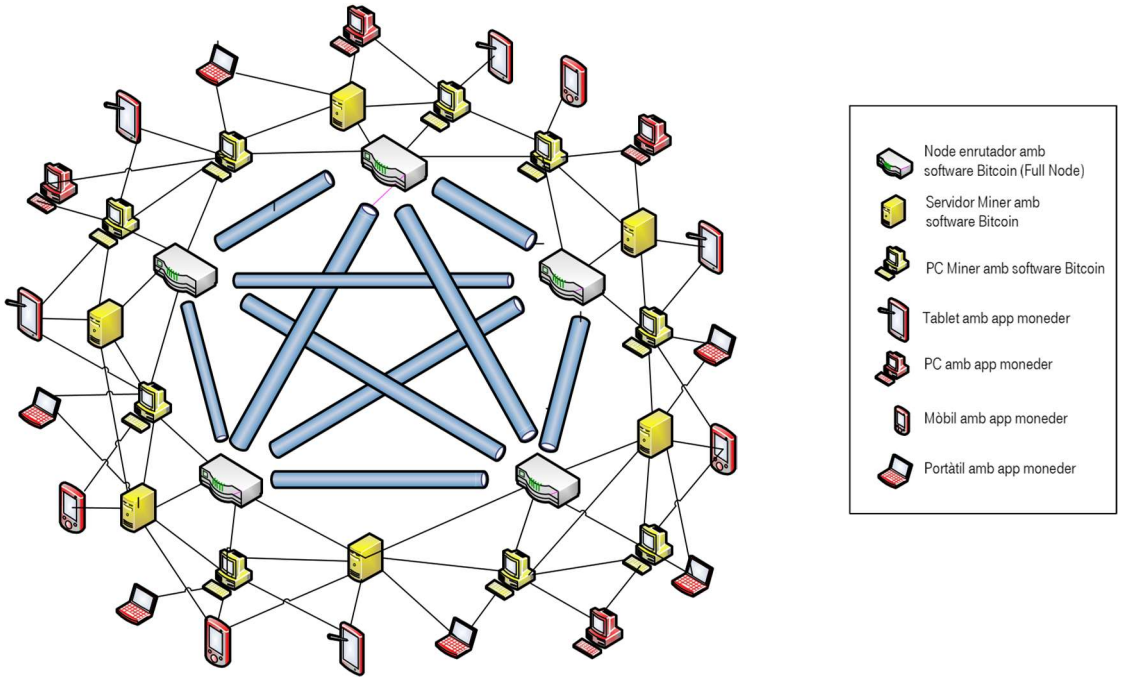


Figura 2. Red descentralizada Bitcoin

A tener en cuenta que los dispositivos, portátiles o PCs de color rojo serían los de los usuarios pasivos (los que solo quieren hacer compras, ventas o transferencias) y los que son de color amarillo vienen a ser los usuarios activos (los que hacen un servicio indispensable para la comunidad, los mineros).

6. Blockchain. Modelo operacional

Ahora que ya sabemos cuáles son los nodos o miembros de esta red y qué estructura presenta, vamos a ver cómo se consigue a nivel técnico y matemático el consenso automático para que cada transacción válida quede registrada por la eternidad en el Libro Mayor de la Blockchain:

Cuando un usuario quiere enviar unos bitcoins a otro usuario lo primero que hace es:

1) Pedir la dirección destino a la persona o entidad a la que quiere enviar el dinero
2) Después, desde, por ejemplo su móvil, abre la app de Bitcoin (el "monedero")
3) La propia app, lo primero que hace de manera automática es intentar contactar con los ordenadores de los mineros que tiene más cerca
4) El Usuario introduce manualmente la dirección del destinatario e introduce la cantidad de bitcoins que quiere enviarle
5) La app envía entonces un mensaje a los mineros más próximos pidiendo que por favor validen que aquella transacción es correcta y que la incluyan lo antes posible en la Blockchain
6) El destinatario sólo podrá estar seguro que ha recibido los bitcoins cuando vea que esa transacción ha sido incluida en un bloque de la Blockchain y, si puede ser, esperar a que se generen unos bloques más encima del bloque donde se encuentra su transacción (esto es importante para las compras de productos porque un vendedor no debería enviar nunca el producto al comprador hasta que no vea que la transacción ha quedado registrada en la Blockchain y espere un tiempo prudencial de aproximadamente una hora)
7) Al mismo tiempo que el primer minero recibe la petición de incluir la transacción en el siguiente bloque que pretende generar, también reenvía esta transacción a sus mineros vecinos.
8) Los mineros vecinos hacen lo mismo: intentan incluir aquella transacción en un bloque y también reenvían la transacción a sus vecinos
9) Aunque parezca mentira, como la información viaja a la velocidad de la luz, en pocos segundos aquella transacción ya ha llegado a todos los ordenadores de los mineros que hay repartidos por todo el mundo
10) Una vez todos los mineros disponen de aquella nueva transacción y la validan, se dedicarán a trabajar de "forma consensuada" para que quede incluida de "manera segura y confiable" en el siguiente bloque que se genere en la Blockchain

Y este último es el paso clave de todo, es decir, cómo conseguir que:

a) Los mineros trabajen de manera "consensuada" (recordemos que el consenso es obligatorio en cualquier organización o red descentralizada)
b) Las transacciones queden incluidas de "manera segura y confiable" (recordemos que podría haber algún minero deshonesto que, por ejemplo, se dedicara a trabajar por la generación de un nuevo bloque y que este nuevo bloque no incluyera una transacción concreta que hubiera hecho, por ejemplo, un amigo suyo. Si esto sucediera, su amigo podría volver a hacer otra transacción con el mismo importe aunque su saldo ya estuviera agotado porque la primera transacción, a efectos reales, no estaría registrada)

La manera de conseguir que todos los mineros trabajen de manera "consensuada" es, de alguna manera, conseguir que todos los mineros trabajen en paralelo por el mismo objetivo (generar bloques con las transacciones válidas cada 10 min) y que sólo un minero, de manera aleatoria, sea el que consiga este objetivo. Además, tan pronto aparece el primer minero que ha conseguido generar el bloque, éste lo distribuye inmediatamente a todos los otros mineros y éstos, automáticamente, revisan todas las transacciones de ese nuevo bloque para comprobar que sean válidas. Si son válidas entonces los mineros comenzarán el trabajo de volver a generar un nuevo bloque y, el hecho de que este nuevo bloque que empiezan a intentar generar lo liguen (de manera incorruptible) al bloque anterior que el minero les acababa de enviar, significará que aprueban este bloque anterior que habían recibido, que están de acuerdo, y por tanto, que establece el consenso deseado.

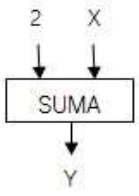
Es importante remarcar que es gracias al carácter aleatorio que tiene el hecho de que sea un minero u otro el que consiga generar un nuevo bloque, que podemos decir que todos los mineros están trabajando en "paralelo" y de manera descentralizada. Porque si no querría decir que alguno de los mineros tiene alguna técnica secreta para conseguir generar bloques que iría me allá de la suerte o la aleatoriedad. Y eso, en el fondo, implicaría que hay algunos mineros que la mayoría de las veces lograrían generar el Bloque ganador y, por tanto, que la red ya no sería tanto descentralizada sino centralizada en aquellos mineros que tienen la técnica secreta.

Por otra parte, la manera de conseguir que la generación del siguiente bloque se produzca de manera aleatoria o por azar en vez de una técnica concreta es forzar que los ordenadores de los mineros realicen un tipo concreto de operaciones que tienen 2 propiedades muy especiales:

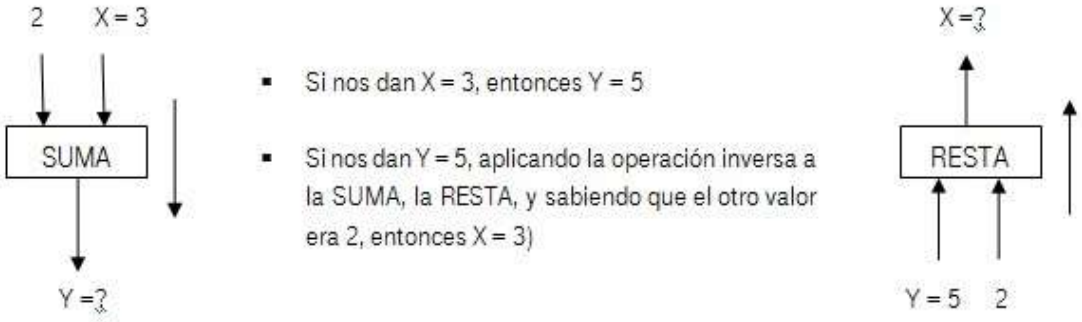
1) Son operaciones que hacen un cálculo que sólo va en un solo sentido
2) Son operaciones que introducen un carácter de aleatoriedad al resultado

Este tipo de operaciones o funciones con estas características tan peculiares se las llama HASH. Calcular el HASH de 2 valores es algo diferente a calcular, por ejemplo, la SUMA de 2 valores. La diferencia principal es precisamente lo que comentábamos antes: que el HASH sólo opera en un sentido y la SUMA opera en los 2 sentidos. Qué quiere decir que opere en un sentido o en 2 sentidos? Pues que si tenemos una SUMA genérica, por ejemplo, en el caso de la SUMA, si tenemos la siguiente expresión genérica:

$$2 + X = Y$$



Siempre podremos encontrar el resultado (Y) si nos dicen la X pero también podremos siempre encontrar cuál es la X que hace que el resultado sea Y. Es decir, si nos dicen que X = 3 siempre podremos saber el resultado: 5 (2 + 3 = 5) pero si nos dicen el resultado (5) y nos piden averiguar cuál era la posible X si el otro valor de entrada era 2, lo podemos encontrar usando el camino inverso o aplicando la operación o función inversa: la RESTA (5 – 2 = 3). Esto quiere decir que la función SUMA opera en los 2 sentidos.



En cambio, cuando calculamos el HASH de 2 valores nunca podremos hacer el camino inverso. Así como la SUMA tiene un camino inverso que es hacer la RESTA, el HASH no tiene camino inverso, no existe una operación inversa al HASH!

De este modo, lo que se pide a los mineros cuando deben trabajar para la generación de un bloque es que encuentren un valor que inicialmente ninguno de los mineros no sabe (X) y que, al hacer la operación HASH de este valor con un segundo valor (Y) que sí saben todos los mineros, el resultado sea un valor concreto que también saben todos los mineros (Z). Si el HASH operara en 2 sentidos (como la SUMA) esto sería muy fácil de conseguir, sólo deberían conseguir calcular la operación inversa del HASH con el resultado que todo el mundo sabe (Z) y uno de los 2 valores que todo el mundo también sabe (Y) y ya obtendrían el valor que nadie sabe (X =?)

La gran ventaja, como hemos dicho, es que la operación HASH es tan especial y peculiar que no permite encontrar una función espejo que haga la operación en el sentido inverso. Por tanto, la única manera de lograr obtener ese valor de la entrada que nadie sabe (X =?) Es lo que se llama "prueba y error". Es decir, pedirle a los ordenadores de los mineros que vayan probando aleatoriamente muchos valores de X y seguidamente calculando el HASH de este valor X con la Y hasta que, por suerte, tropiecen con el valor concreto que hace que el resultado sea lo que todo el mundo buscaba (Z).

Ahora que ya hemos visto cual es la actividad principal que mantiene ocupado las 24 horas del dia al PC o servidor del minero (el procesador o la CPU está calculando millones de operaciones HASH por segundo hasta que el resultado sea el que todos buscan) nos queda entender cómo Satoshi logró encontrar un método para que las transacciones quedaran incluidas en la Blockchain de forma "segura y confiable", es decir, encontró un método que le permitió evitar

al máximo la presencia de mineros deshonestos que hicieran trampas. Lo que hizo Satoshi es inspirarse en una idea que ya había propuesto Adam Back en 1997 para evitar el SPAM en los correos electrónicos, es decir, para evitar que emisores deshonestos enviaran correos electrónicos de forma indiscriminada y masivamente, sin el consentimiento de los que recibían los correos.

La estrategia que definió Adam Back era muy simple: establecer un mecanismo rápido para verificar que quien envía un mensaje tiene un mínimo interés por enviarlo. Para evitar que se envíen correos de forma masiva (como los comerciales o los que pretenden engañar con la intención de sacar provecho económico de la víctima) la idea que tuvo era que quien lo enviaba debía estar dispuesto a " pagar "con el tiempo de procesamiento de su ordenador. Así conseguía evitar que un emisor deshonesto enviase miles de correos simplemente porque no tenían ningún coste asociado. Con el método de Adam Back, si alguien quería enviar SPAM, se arriesgaba a que su ordenador se colgara o le acabara saliendo humo.

Por tanto, la solución de Adam fue inventarse un mecanismo donde fuera relativamente costoso para el emisor generar cada correo que quisiera enviar y donde fuera rápido de verificar por el receptor que el emisor había dedicado un esfuerzo considerable al enviar ese correo. Este mecanismo lo llamó hashcash (porque también utiliza la función HASH para conseguir el objetivo... alguien debería hacer un monumento de una vez al inventor del HASH!). Y HASCASH es con el que se inspiró Satoshi Nakamoto para definir un mecanismo similar para Bitcoin: el "Proof of Work"

El "Proof of Work" en la red Bitcoin se basa precisamente en las mismas acciones y operaciones que hemos explicado que tenían que hacer todos los mineros para asegurar que la generación de cada bloque se hicíese de manera descentralizada, es decir, ir probando valores diferentes y calcular el HASH de cada valor con otro (que es conocido por todos) y esperar a que, en una combinación de éstas, el resultado sea un concreto que todo el mundo también sabe.

Insistimos: que se haga de manera descentralizada es equivalente a decir:

1) Que todos los mineros se ponen a trabajar en paralelo para conseguir ser el primero que consigue generar el siguiente bloque (recordemos que sólo el primero es quien gana la recompensa)

2) Que el proceso para obtener un ganador sea una lotería, es decir, que sea totalmente aleatorio quién es el primer minero que logra generar el bloque.

En el caso concreto del "Proof of Work", la idea es que el número de veces que cada minero prueba un valor y calcula su HASH sea muy muy grande. Es decir, la idea es garantizar que los ordenadores de los mineros han llegado a probar millones de valores y después han hecho los respectivos millones de cálculos HASH para lograr encontrar el resultado esperado. Se pide una "prueba de esfuerzo" a los ordenadores. Con ello se evita que cualquier minero pueda generar bloques de forma deshonesta y sin coste alguno. Hay un "esfuerzo" a "pagar" para generar bloques.

En resumen, en la generación de un nuevo bloque (minar un bloque), hay una "sorteo" entre todos los mineros que trabajan en paralelo. Este “sorteo” terminará dando premio al primer minero que, después de haber demostrado su esfuerzo ("Proof of Work") calculado millones de operaciones HASH sobre millones de valores diferentes que habrá ido probando, por casualidad, obtenga un valor resultado o de salida concreto y que todo el mundo conocía antes de empezar.

Este minero, además de tener el honor de generar un bloque que quedará registrado para la eternidad, también ganará un dinero como recompensa por haber dado con el clavo.

Lo bello del diseño de Satoshi es que consigue que cada bloque se generé a una media de 1 bloque cada 10 min. Evidentemente los bloques no se generaran justo a los 10 min, lo harán en el minuto 9, en el minuto 11 y medio, en el 8, etc pero de media, si tomamos una muestra suficientemente grande de bloques, veremos que en promedio se generan aproximadamente cada 10 min.

Esto lo consigue utilizando fórmulas matemáticas de la teoría de la probabilidad y monitorizando constantemente la capacidad de procesamiento agregada de todos los mineros o, lo que es lo mismo, midiendo permanentemente el poder de cómputo global de la red (que lo medirá en número de operaciones HASH/seg). Hay que tener en cuenta que cuanto mejor sean las tarjetas procesadoras de los mineros, más rápido irán y más HASH/seg podrán calcular. Pero si aumenta el número total de operaciones que es capaz de realizar la red en su conjunto, entonces debería disminuir los tiempos medios para la generación de bloques. Pero Satoshi programó el software Bitcoin de manera que conseguía anular los efectos secundarios de este incremento inevitable de la capacidad de cómputo porque, para él, era prioritario que la generación de bloques se realizará a un ritmo constante.

A medida que va creciendo el poder de cómputo de la red Bitcoin (mas mineros van entrando o mejor hardware va siendo utilizado) el código de Satoshi es suficientemente hábil y dinámico como para, cada aproximadamente 2 semanas, actualizar el valor que todos tienen que buscar. Lo modifica de manera que hace que sea más difícil encontrarlo, es decir, que en uno de esos millones de operaciones HASH que hace cada ordenador, la probabilidad que salga el valor propuesto por el código sea cada vez más baja. Así, compensa el incremento de la capacidad de procesamiento global con el incremento de la dificultad para encontrar el resultado y, de esta manera, consigue mantener siempre constante el mismo valor de "1 bloque cada 10 min". ¿Cómo calcula la capacidad de procesamiento global? Muy fácil, Satoshi la calculó directamente en el inicio de todo cuando solo era él el único que realizaba minería (tenía varios ordenadores con el software instalado y trabajando para la red) y le fue muy fácil sumar la potencia de sus CPUs para saber el total. Luego, a partir de ahí, incluyó un algoritmo en su software de Bitcoin que permitía actualizar ese valor real calculado inicialmente midiendo como iba mejorando la velocidad de procesamiento del sistema en un periodo suficientemente largo (él lo estableció en 2 semanas). La idea era la siguiente: durante esas 2 semanas el software iba contando el número de bloques realmente generados y, si salían 2016 (número de bloques generados en 2 semanas si cada bloque se genera cada 10 min) quería decir que la capacidad de computo se mantenía igual que en el periodo de 2 semanas anterior. Por el contrario, si se generaban más de 2016 bloques, quería decir que más ordenadores se habían incorporado a la red o que algunos de los existentes habían incrementado su CPU. En este caso, lo que hacía el algoritmo es incrementar la dificultad en un grado proporcional de manera que, en vez de generarse a una media de 8 o 9 minutos volvieran a generarse a una media de 10 min.

Finalmente, es importante darse cuenta de que, la única manera de conseguir generar un bloque de forma deshonesta sería que un minero consiguiera acaparar, sobornar o convencer a más del 50% de los mineros de la red. Para ser más precisos, lo que debería hacer es conseguir acaparar o poner bajo sus órdenes más del 50% del poder computacional total que hay en la red Bitcoin (que es la suma total del poder computacional o de la CPU que tiene cada uno de los mineros en sus respectivos ordenadores). Sólo entonces conseguiría que, por simple probabilidad estadística, fuera él, o uno de los que están a sus órdenes, lo que la mayoría de las veces serían los primeros en generar el nuevo bloque.

7. Smart Contracts y DAOS, más allá del sistema de pagos Bitcoin

Con los años, la gente dijo, en una Blockchain no sólo podemos registrar dinero digital sino que también se podría registrar otras cosas. Se podrían registrar acciones de una empresa, títulos de propiedad de una casa, propiedad intelectual, votos...

Y hace unos 4 años, un genio que sí tiene nombre y apellido reales, Vitalik Buterin, fue más allá y dijo: ¿Qué tal si, utilizando la misma filosofía del Bitcoin, la misma tecnología o protocolo Blockchain, construimos una plataforma que, además de permitir hacer transacciones de criptomonedas y registrar o transferir activos de valor, nos permita registrar y enviar acuerdos entre las personas? Sería algo parecido a los contratos legales pero aplicado al mundo digital y concretamente en una Blockchain específica. Los que darían fe de estos contratos serían los mismos que en la Blockchain Bitcoin daban fe de que las transacciones efectivamente se habían producido y eran válidas, es decir, los mineros. Y así surgió una nueva Blockchain, Ethereum, que incorporaba el concepto de los "Smart contracts" o contratos inteligentes que quedaban registrados y validados de manera descentralizada.

Por otra parte, es interesante ver que estos Smart Contracts no sólo pueden trabajar con dinero, acciones de empresas, o un voto, sino que, además, pueden controlar objetos. Y es allí donde surge el concepto de la propiedad inteligente.

Para explicar un poco más cómo funciona todo esto, propongo la explicación de un posible modelo de servicio o negocio que adoptaría la estructura organizativa de una DAO, es decir, una Organización Autónoma Descentralizada. Con la entrada en escena el 2016 de lo que se conoce como DAOs podemos estar ante un cambio de paradigma total con respecto a la manera de organizarse y gestionarse de las empresas, partidos políticos, entes públicos, cooperativas, entidades sin ánimo de lucro y cualquier tipo de asociación entre grupos de personas que se constituyan como organización para el logro de un objetivo común. Las DAOS, como su nombre indica, son organizaciones descentralizadas de personas, es decir, organizaciones que no están dirigidas por ningún ente central, ningún director o directivo y que tampoco tienen ningún consejo de administración, es decir, organizaciones donde las decisiones las toman todos los miembros por igual. Las DAOs vendrían a tener un funcionamiento similar a las cooperativas, si hacemos un paralelismo con organizaciones que tienen como objetivo la gestión económica de una actividad, o con un partido como la CUP, si el paralelismo lo hacemos con organizaciones que tienen como objetivo la gestión política.

La diferencia clave es que, gracias a la aportación de recientes invenciones tecnológicas como las criptomonedes, las Blockchains o los Smart Contracts, estas organizaciones descentralizadas ahora se podrán gestionar de forma totalmente automática, de forma autónoma, es decir, sin gestores ni directivos ni administradores. Lo único que habrá será propietarios o responsables finales de las decisiones que se acaben tomando y, por tanto, responsables de asumir las pérdidas o beneficios económicos y / o sociales de estas organizaciones, pero no habrá directivos que se encarguen de organizar los miembros ni de gestionar su funcionamiento ni de organizar la manera de tomar las decisiones (a recalcar que hablamos del MODO de tomar las decisiones, no la toma de decisiones en sí). Esta gestión o administración será efectuada por un programa informático, un Smart Contract.

Con la proliferación de las DAOs a través de Internet podríamos estar ante una situación similar a la que sucedió con la entrada en escena de la Revolución Industrial y las máquinas, es decir, el desplazamiento de la mano de obra . En este caso, sin embargo, los grandes desplazados serían los directivos. Evidentemente no se trataría de un desplazamiento o desaparición total porque siempre habrá modelos de organizaciones que, por los objetivos que persigan y por el sector donde estén involucradas, siempre será mejor que estén centralizadas o que no estén automatizadas. Por lo tanto, acabarán conviviendo todos los modelos en paralelo pero, seguro que muchas de las organizaciones o empresas que conocemos hoy en día serán sustituidas por estos nuevos modelos descentralizados y autónomos, sobre todo muchas de las tecnológicas actuales (Facebook, whatsapp, Airbnb, ubber, etc que se sabe que, por el hecho de estar centralizadas, han sucumbido al uso ilícito de los datos que circulan por sus redes) tendrán una competencia feroz con las DAOs y aparecerán miles de nuevas sobre conceptos que, hasta ahora, no sabíamos ni que se podían necesitar.

Vamos a verlo con un ejemplo práctico de una DAO que incorporaría conceptos como Blockchain, criptomonedes, Smart Contracts e incluso, lo que se llama Internet of Things, es decir, la nueva Internet en la que cualquier objeto (un coche, una lámpara, una nevera, etc) puede estar conectado a Internet y comunicándose con ordenadores, servidores, con tu móvil o, incluso, con otros objetos que también estén conectados a la red:

Imaginemos que una asociación de vecinos de un barrio o de un pueblo (pongamos 250 personas), con poco más de lo que tienen en el bolsillo (pongamos una media de 150 eur) Y, ya que estamos puestos en este mundo de las criptomonedes, el crowdfunding se haría a través de una Blockchain, es decir, se haría con una herramienta descentralizada (de estos crowdfounding concretos, en el mundo de las criptomonedes y las Blockchains , se hacen muchos, quizás demasiados! y se llaman ICOs: Initial Coin Offering). Entonces, cada miembro invierte la cantidad que desea y, una vez se han reunido el dinero suficiente para poder pagar un informático y el coche, se adquiere el coche, unos voluntarios lo pintan de color amarillo y negro (taxi), el informático abre y asocia un "monedero" Bitcoin para el coche a nombre de la asociación (con una dirección o cuenta asociada), y se pide al mismo informático que programe un Smart Contract en el que cada vez que un pasajero se suba el taxi, le empiece a facturar por segundo. Y cada vez que se baje, cierre la cuenta. Además, este coche, cuando ve que se está quedando sin combustible se va a la estación de servicio y paga el combustible de su propio "monedero". También cuando detecta que tiene alguna avería se va al taller más próximo para que lo arreglen y paga de su bolsillo. Una vez al mes, nos paga a todos las ganancias generadas (proporcionalmente al que pusimos) y, si lo hemos utilizado nosotros mismos, nos lo descuenta del saldo a fin de mes. Cada año paga religiosa y automáticamente los impuestos, porque, obviamente, el coche es un ciudadano responsable. Con ello se consiguen 3 cosas principales:

1) Se aporta un nuevo servicio a la comunidad: un servicio de taxi más económico (recordemos que este sería un taxista que hace turnos de mañana, tarde y noche seguidas, no descansa ningún día del año y que, por tanto, puede cobrar una tarifa más barata para cada carrera).
2) Con suerte (sobre todo si no lo usamos nosotros mismos) sacamos alguna ganancia a finales de mes.
3) Potenciamos las ideas de la economía del Decrecimiento o la economía del Desarrollo (en vez de la tradicional Economía del Crecimiento) porque se reduce ostensiblemente

la necesidad de que cada persona tenga que comprar y disponer de su coche personal y se reduce ostensiblemente el impacto sobre el medio ambiente

La realidad es que, todo esto que acabo de describir, técnicamente ya se puede hacer a día de hoy. El único problema son, evidentemente, las regulaciones que aún no permiten circular coches totalmente automáticos para las ciudades y, por tanto, la ausencia de coches automáticos que estén en venta actualmente. Otro motivo que puede explicar que todavía nadie haya llevado a la práctica esta idea podría ser el hecho de que seguramente Google o alguna otra empresa están esperando a tenerlo todo bien probado y aprobado para hacerlo ellos a gran escala y hacerse con el gran mercado de la movilidad que se avecina en los próximos años.

8. Conclusiones

Con esta combinación de tecnologías expuesta emerge algo increíble: el Internet del valor. Los últimos 20 años hemos vivido en la llamada Internet del conocimiento y ahora, con esta nueva Internet del valor, se crearán de forma efectiva identidades basadas en la reputación. Cada vez que vamos a recibir una calificación positiva en una venta, cada vez que enseñamos o explicamos algo nuevo en la red o que colaboramos con nuestra comunidad o que más seguidores nos sigan o que más likes o retweets nos hagan, esta identidad crecerá. La reputación será uno de los conceptos claves de la década de los 20s porque quizás podremos agruparlas todas en una gracias a la tecnología Blockchain. Y esta reputación nos permitirá interactuar, llegar a acuerdos, comerciar y trabajar con personas de todo el mundo sin necesidad de que confiamos directamente o, incluso, sin la necesidad de habernos conocido previamente.

Finalmente, si el potencial de estas tecnologías se cumple, es decir, si la gente acaba teniendo la confianza necesaria en estos sistemas como para confiar en ella más que en las empresas intermediarias de hoy en día y si tenemos en cuenta un fenómeno que está sucediendo desde hace uno años en el mundo, que es la rápida llegada de la telefonía móvil en la mayoría de la población mundial, podemos estar seguros que estamos realmente ante un cambio a gran escala y de proporciones mayúsculas. Pensemos que, hoy en día, hay 2.500 millones de personas en el mundo que tienen un teléfono móvil pero que no tienen acceso a una cuenta bancaria (el claro ejemplo es Ecuador donde casi el 100% de la población tiene móvil y sólo el 40% tiene una cuenta bancaria).

Vemos que esta Internet del valor no solo nos podría permitir rehacer el sistema o las maneras de organizarnos, revivir la confianza en las democracias, o ser actores centrales de la construcción de una sociedad más equitativa, sostenible y próspera; sino que nos podría permitir integrar a millones de personas excluidas del planeta, dándoles acceso a los servicios financieros básicos y dándoles la posibilidad de ganarse una reputación o un trabajo a distancia y ofrecerles un puente para conectarse con el resto de la sociedad que, hasta el día de hoy, nadie les había podido ofrecer.

Lo único necesario es ensanchar la base de gente que adopte y utilice Bitcoin (o cualquier Blockchain de carácter público y Open Source) y que siga los principios ideológicos de Satoshi Nakamoto en la creación de este nuevo mundo: la privacidad, la descentralización por el bien de la comunidad, la transparencia y la libertad.

Si no hay una mayoría de la población que opte por una Blockchain pública / Open Source para la gestión de pagos, registros varios o el establecimiento de contratos inteligentes y DAOs, habrá que resignarse a la misma situación de siempre: Estados y monopolios bancarios o corporativos que continuarán invadiendo privacidades, coartando libertades y manipulando la evolución natural de las sociedades.

No desaprovechemos esta magnífica oportunidad.

Referencias

[1]S. Nakamoto, "Bitcoin: A Peer Available:https://bitcoin.org/bitcoin.pdf

[2]Vitalik Buterin, A. di Lorio, C. Hoskinson, and M. Alisie, "Ethereum whitepaper," 2013. [Online].
Available:https://github.com/ethereum/wiki/wiki/White-Paper

[3]elBitcoin.org, "Bitcoin: La moneda del futuro", 2012

[4]AM Antonopoulos, "Mastering Bitcoin. Unlocking Digital Cryptocurrencies ", 2014.

[5]Diego Gutierrez Zaldivar, "De Internet of knowledge a Internet of value ", 2016[Online]. Available: https://www.youtube.com/watch?v=ArPsn--ExFE

[6]A. Back, "Hashcash2002. [Online]. Available:http://www.hashcash.org/papers/hashcash.pdf

[7]Court of Justice of the European Union, "The exchange of traditional currencies for unidos of the 'Bitcoin' virtual currency is exento from VAT", 2015 [Online]. Available:
http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150128en.pdf

[8]Ibn Jaldún: el Mediterráneo en el siglo XIV : auge y declive de los imperios

[9]Sentencia del Tesoro de EEUU. Disponible :
https://www.fincen.gov/news/testimony/statement-jennifer-shasky-calvery-director-financial-crimesenforcement-network

[10] Blomberg, "Five Reasons the Winklevoss Bitcoin ETF Should Be Approved", 2016 [Online]. Available: https://www.bloomberg.com/view/articles/2016-11-01/five-reasons-the-winklevoss-bitcoin-etf-should-beapproved