Bitcoin: proyecto y realidad

Bitcoin: proyecto y realidad

Autor/es

José Antonio Sánchez Berges

Director/es

Carolina Ibor Monesma

Facultad de Empresa y Gestión Pública / UNIZAR

2023

El presente trabajo ha sido realizado por José Antonio Sánchez Berges, estudiante de la Facultad de Empresa y Gestión Pública de la Universidad de Zaragoza, bajo la dirección de Dña Carolina Ibor Monesma, profesora perteneciente al Departamento de Análisis Económico, dentro del área de Fundamentos del Análisis Económico.

El objetivo de este trabajo es realizar una investigación acerca de Bitcoin, una nueva tecnología que aspira a convertirse en un activo monetario a nivel global. Esta invención ha tenido gran repercusión, hoy en día todos hemos oído hablar de ella y son numerosas las veces que aparece en los medios de comunicación.

Bitcoin, la primera *criptomoneda*, ha surgido como respuesta a una serie de preocupaciones respecto al actual paradigma, tanto económico como digital. La revolución Bitcoin combina una moderna tecnología, la tecnología *blockchain*, con ideas económicas existentes desde siglos atrás. Mediante un apropiado diseño algorítmico de la arquitectura de la red, se consigue solucionar problemas monetarios tradicionales tales como la necesidad de un tercero de confianza para asegurar las transacciones no presenciales o la polémica manipulación de la masa monetaria por agentes individuales.

Ha trascurrido ya más de una década desde que surgió Bitcoin, por tanto, contamos con cierto margen para su análisis. Tal ha sido el desarrollo de la moneda en este tiempo que su uso se ha extendido a lo largo del mundo, alcanzando incluso el estatus de moneda oficial en El Salvador, aunque, como veremos en mayor profundidad, este primer caso de oficialidad tiene matices especiales.

Índice

Introducción

Dentro de un sistema económico, uno de los componentes más importantes para comprender su funcionamiento es la moneda, el sistema monetario. La moneda juega una serie de papeles esenciales: medio de pago, unidad de cuenta y reserva de valor. Su existencia es esencial para la operativa de las economías –y sociedades– modernas. Es en este contexto donde surge esta nueva moneda, Bitcoin, que aspira a convertirse en un activo monetario con vocación global debido a lo especial de sus características particulares. Su fama, merecida por su novedad, es uno de los motivos que han suscitado esta investigación.

Para facilitar la comprensión de este novedoso sistema, indagaremos en los antecedentes tecnológicos que preceden a Bitcoin, así como en la línea de argumentación ideológica que comparten tanto sus predecesores como los principales personajes envueltos en su nacimiento. Después de esto, explicaremos el funcionamiento de Bitcoin introduciéndonos en la tecnología de la que se sirve, la tecnología *Blockchain*, debido a que es uno de los principales factores –por no decir el que más– que diferencian a Bitcoin de los activos monetarios tradicionales.

Otro aspecto que hemos considerado de interés es la trayectoria que ha seguido esta criptodivisa. Bitcoin surgió en 2009, hace ya catorce años desde el momento actual, lo cual nos concede un plazo de estudio que, aunque no definitivo, puede resultar interesante a la hora de juzgar si este nuevo aspirante a activo monetario se ha mantenido fiel a los ideales por los que surgió o si, por el contrario, ha llevado un camino distinto al que pretendía su creador.

Bitcoin supone una revolución sin parangón en el ámbito monetario, una revolución que bien podría acabar afectando a todo el mundo. Es por eso que resulta necesario saber por qué surgió Bitcoin, qué pretendía, cómo lo pretendía lograr y si lo está consiguiendo a día de hoy.

¿Por qué Bitcoin?

Las cosas no son útiles por sí mismas, son útiles en la medida en las que nos podemos servir de ellas para facilitarnos de una u otra forma. Todos los nuevos inventos, el desarrollo de nuevas tecnologías, tienen sentido en cuanto que solucionan – o facilitan la solución de – problemas existentes, problemas de los cuales, en ocasiones, no somos ni siquiera conscientes.

Es por esto que, a la hora de hablar de Bitcoin, antes siquiera de concretar qué es, nos parece lo más adecuado contextualizar por qué surge, es decir, investigar e identificar cuáles son los hechos más relevantes implicados en el nacimiento de esta moneda tan especial.

Contexto

Nos encontramos en los inicios de la década de los 80, las revoluciones tecnológicas que se han ido consiguiendo están a punto de cristalizar en la creación de Internet, en 1982, lo que supondrá uno de los mayores hitos en la historia de la humanidad. A la par que se dan grandes avances en el campo de la transmisión de información –Internet no es más que una red de información prácticamente instantánea a nivel global– se incrementa la preocupación de los individuos por el acceso a y el uso de su información personal.

Por otro lado, tenemos que prestar atención a otro campo que está íntimamente ligado a Bitcoin: el ámbito monetario. En 1971 se produjo el definitivo abandono del patrón Bretton Woods después de anular el presidente estadounidense, Richard Nixon, la convertibilidad del dólar en oro. Tras esto, el sistema monetario cambia radicalmente, de estar basado en una doble relación divisas-dólar casi fija, con margen de fluctuación de 1% respecto a la paridad establecida originalmente, y dólar-oro fija, 35 dólares por onza de oro, a un sistema en el que el dinero no tiene valor intrínseco ni está respaldado por ningún activo real, sino que es una promesa de pago -o, mejor dicho, una promesa de aceptación de pago- de los Estados. Surge así el dinero "fiat" [1], un dinero que recibe este nombre precisamente porque su existencia no está respaldada por nada que no sea la ley imperante en cada territorio.

Una vez resaltados los factores más característicos del momento, tanto a nivel tecnológico como a nivel monetario, estos conllevan varias consecuencias: un crecimiento exponencial del caudal de flujos de información; una creciente preocupación por la privacidad dadas las nuevas formas de comunicación; una sumisión total, no *de iure* pero si *de facto*, a terceros para todas aquellas transacciones monetarias que no sean en efectivo; un periodo altamente inflacionario en los años iniciales del patrón *fiat*. Es este el caldo de cultivo que va a conducir a varias personas a intentar adaptar los avances tecnológicos al mundo monetario, en busca de protección frente a la falta de privacidad que representan los nuevos sistemas de información (Internet) y de alguna solución a los problemas que presenta el nuevo sistema monetario.

[1] "Fiat" viene del latín, significa "hágase" o "que así sea"

La criptografía

La criptografía se define como el arte de escribir con clave secreta, es decir, la criptografía es una forma de transmitir información de tal forma que el contenido de la misma no sea inteligible por quien no deseamos.

Esta disciplina ha ido evolucionando a la par que lo hacían las formas de comunicarse, pues la necesidad de mantener informaciones sensibles fuera del alcance de terceros va de la mano con la necesidad de transmitir las mismas. La llegada de Internet supuso a su vez una nueva forma de realizar pagos, los pagos "*online*", lo cual implicaba que la información de carácter económico –uno de los tipos más sensibles– pudiera ser más accesible.

Es de esperar pues que a un avance en los medios de comunicación le sigan avances en el mundo de la criptografía y, como hacíamos referencia en el anterior apartado, tras la llegada de Internet y la era digital la desconfianza respecto a la privacidad de la información era creciente.

David Chaum, pionero "crypto"

David Chaum, nacido en Estados Unidos en 1955, es un doctor en informática y administración de empresas por la Universidad de California. Fue promotor y organizador de las primeras conferencias mundiales sobre criptografía y criptología, conocidas como *Crypto*, que se celebran desde 1982 en Santa Barbara (California). Fue en estas conferencias, concretamente en la primera, Crypto'82, donde Chaum presentó al mundo su artículo "Blind Signatures for Untraceable Payments*"* (Firmas Ciegas para Pagos Irrastreables) el cual supuso tal revolución que desde entonces Chaum pasaría a ser considerado el padre del dinero digital. En este documento, el genial criptógrafo presentaba un sistema que convertía en anónimas las transacciones *online* de dinero mediante la introducción de "firmas digitales ciegas". Chaum siguió con sus investigaciones sobre la privacidad de la información en los pagos, y en 1988, junto con otros dos criptógrafos, Amos Fiat y Moni Naor, mejoró el sistema que ya había creado para que fuera capaz de realizar transacciones *offline* y habilitó la detección del doble gasto.

David Chaum continua a día de hoy activo en el mundo de la criptografía, sigue acudiendo con asiduidad a las conferencias *Crypto* anuales que él mismo impulsó y es considerado una eminencia dentro del mundo de la criptografía, su asesoramiento y opinión son altamente valorados en nuevos proyectos y en los debates sobre las cuestiones más significativas sobre las criptomonedas. Además de esto, su forma de ver el mundo y sus innovaciones criptográficas fueron las raíces de un movimiento que está profundamente relacionado con Bitcoin: el movimiento "cypherpunk". ("David Chaum", 2023)

El manifiesto Criptoanarquista, firmado por Timothy C. May

Timothy May, nacido el 21 de diciembre de 1959 en Bethesda, EEUU, fue técnico informático, escritor, ingeniero electrónico y científico senior en Intel. Disfrutó en vida de un respeto y admiración general dentro del mundo informático y criptográfico. Sus trabajos más relevantes son "A New Physical Mechanism for Soft Errors In Dynamic Memories" (Un nuevo mecanismo físico para errores leves en memorias dinámicas) y "Alpha Particle-Induced Soft Errors in Dynamic Memories" (Particulas alfa inducen errores en memorias dinámicas), este último firmado también por Murray Wood. Estos

trabajos trataban sobre como la radiación afecta a los componentes de los circuitos eléctricos integrados, especialmente a los valores almacenados – esto es a lo que se refiere con memorias dinámicas – llegando a modificarlos, lo cual reduce su fiabilidad. Siempre mostró una actitud liberal y de la unión de sus conocimientos informáticos y sus ideas surgió el *Manifiesto Criptoanarquista* (Maldonado, 2019)

El criptoanarquismo fue definido por el matemático Vernor Vinge como "la realización ciberespacial del anarcocapitalismo". Sus inicios se remontan a la década de los 80 y sus ideales fueron plasmados en un manifiesto que se popularizó en 1992, aunque se cree que ya circulaba por grupos afines a este ideario varios años antes. El escrito, firmado por Timothy C. May, es breve y conciso. En él se adelantan las posibilidades que abrirá la tecnología en el ámbito de la privacidad de la información y en especial de las interacciones económicas, se avisa de cómo los Estados intentarán frenar el uso de estas tecnologías aludiendo "preocupaciones de seguridad nacional" (principalmente narcotráfico y comercialización de servicios ilegales) y compara la revolución que estas nuevas tecnologías supondrán con la que supuso en su momento la invención de la imprenta tanto en aspectos productivos y comerciales como, esencialmente, en la estructura de poder social, estructura íntimamente ligada a la información y su disponibilidad (Maldonado, 2016).

El Manifiesto Cypherpunk, firmado por Eric Huges

Este movimiento, cuyo origen tiene lugar al final de la década de los 80, surge como respuesta a la creciente integración de la tecnología en la vida social y a los riesgos que entraña ("Cypherpunk", 2023). El movimiento Cypherpunk dibuja un futuro en el cual los avances tecnológicos son tales que se han mezclado de manera intrínseca con la vida humana. Este futuro es presentado de forma distópica, mostrando un mundo marcado por la desigualdad y por la explotación corporativa, ya que los avances tecnológicos pueden derivar en formas de control exhaustivo de, prácticamente, la totalidad de la información existente (Carvajal Villaplana, 2001)

Las ideas básicas de este movimiento cristalizan en un documento, conocido como el Manifiesto Cypherpunk, publicado en marzo de 1993 por Eric Hughes, que es una oda a la privacidad y la libertad de información. El manifiesto está dividido en cinco partes: "Cypherpunk", "Sociedad", "El sistema", "La visión" y "¿Dónde estamos?". Comienza por caracterizar al cypherpunk como una persona que tiene una visión distinta al resto de la sociedad debido a sus conocimientos informáticos y cibernéticos, es por esto que los cypherpunks alcanzan una mayor comprensión del momento en que se encuentra la sociedad. Las principales reivindicaciones del movimiento son: mayor privacidad, el uso de la criptografía para defender la privacidad y la libertad de expresión en la era digital; una descentralización progresiva para dificultar la censura y el control gubernamental; libertad de información y libertad de acceso a la misma.

A nadie escapan las similitudes de este ideario con los motivos que guiaron las investigaciones de David Chaum y con características del criptoanarquismo.

El movimiento Cypherpunk comparte directamente dos características básicas con Bitcoin: un deseo de liberación frente a sistemas centralizados y opresivos y una visión optimista sobre cómo puede la tecnología ayudarnos y transformar la sociedad.

Wei Dai y el "b-money"

Wei Dai, nacido en China en 1976, es un miembro destacado del movimiento Cypherpunk. Haciendo honor al movimiento, la vida privada de Dai es poco conocida, pero sabemos que es graduado por la Universidad de Washington en Ciencias de la Computación y que ha trabajado para gigantes tecnológicos como Microsoft y TerraSciences, siempre en el campo de la criptografía y la implementación de sistemas informáticos (Bastardo, 2019),

El proyecto presentado por Dai con el nombre de "b-money" fue lanzado en 1998 y constituye el primer esbozo de una moneda digital descentralizada. El *b-money* es un sistema en el que los usuarios podrían enviar y recibir pagos de forma segura y anónima sin necesidad de intermediarios, pero ahí no reside su importancia, ya que recordemos que David Chaum había presentado, más de una década antes, sistemas con estas características. La innovación que introduce el sistema de Wei Dai es la posibilidad de que los usuarios sean participes de la emisión de la moneda unido a que sean capaces de validar las transacciones, lo cual elimina por completo la necesidad de una entidad central que regule la masa monetaria. Es aquí donde surgen por primera vez conceptos como la "Proof of Work" o Prueba de Trabajo, libro contable colectivo o criptografía de clave pública, conceptos que, como más tarde veremos, son la base de Bitcoin.

Finalmente, *b-money* no fue implementado en su forma original, pero muchas de sus ideas serán incorporadas en el desarrollo de Bitcoin y otros proyectos de criptomonedas, y pasará a ser considerado uno de los ejemplos más tempranos de como la tecnología puede crear una moneda descentralizada y sin intermediarios (Maldonado, 2019)

A modo de curiosidad, Wei Dai fue considerado durante tiempo como el posible creador de Bitcoin dadas las similitudes de su sistema con el funcionamiento de la red Bitcoin, así como por ser uno de los pocos nombres que aparecen mencionados en el Libro Blanco[2] de Bitcoin.

El nacimiento de Bitcoin

Bitcoin fue presentado al mundo a través de un documento firmado por Satoshi Nakamoto, el seudónimo utilizado por la persona o el grupo de personas que se encuentra detrás de la creación de la criptomoneda, que constituye el Libro Blanco de Bitcoin y que fue enviado por Nakamoto el 31 de octubre de 2008 a un reducido círculo de criptógrafos. En este documento, de nombre "Bitcoin, a Peer-to-Peer Electronic Cash System", fueron presentadas por primera vez tanto la filosofía como la arquitectura de Bitcoin, que se convertiría en la primera criptomoneda de la historia.

En su escrito, Nakamoto comienza haciendo una crítica al comercio *online*, el cual ha terminado por depender, casi exclusivamente, de las instituciones financieras como terceros de confianza para asegurar los pagos electrónicos (Nakamoto, 2008). Comenta la imposibilidad actual de realizar transacciones totalmente irreversibles y cómo esto hace crecer la necesidad de confianza en el sistema. Los costes asumidos en forma de confianza y en forma monetaria, debido a la necesidad de intermediación, son presentados como indeseables y como salvables gracias a la red bitcoin. Bitcoin presenta un sistema de pago

[2] En el contexto criptográfico, un "Libro Blanco" hace referencia al documento que resume las principales características y especificaciones técnicas de un proyecto *blockchain*,

electrónico con transacciones computacionalmente irreversibles, que sustituye en las transacciones la confianza por una prueba criptográfica y que resuelve el problema del doble gasto mediante "un servidor de sellado de tiempo, distribuido y *peer-to-peer*, para generar la prueba computacional del orden cronológico de las transacciones" (Nakamoto, 2008).

El lanzamiento de este manifiesto es considerado el origen de Bitcoin, ya que es el texto fundamental para la comprensión de la filosofía y objetivos de Bitcoin, así como porque en él se encuentran todas las explicaciones técnicas acerca de la arquitectura y funcionamiento de la red.

¿Qué es Bitcoin?

Bitcoin es una criptomoneda, es decir, "es un medio digital de intercambio que utiliza criptografía fuerte para asegurar las transacciones, controlar la creación de unidades adicionales y verificar la transferencia de activos usando tecnologías de registro distribuido" ("Criptomoneda", 2023). Pero la esencia de Bitcoin no recae en ser un activo digital capaz de reunir las características para ser considerado dinero, sino en la arquitectura que construye su sistema, la cual le permite funcionar de manera totalmente descentralizada. Bitcoin funciona en una red de pagos distribuida "*peer-to-peer*" –es decir, entre pares o entre iguales– que utiliza tecnología *blockchain* para registrar y verificar las transacciones, se sirve de la criptografía para dotar de seguridad a la red y del sistema PoW (del inglés *Proof-of-work)* para evitar el doble gasto, generando así un sistema de consenso entre los participantes que permite a cualquier usuario verificar y validar las transacciones, eliminando así la necesidad de un intermediario que dote de confianza a la red (Nakamoto, 2008).

Bitcoin y otras criptomonedas

Hoy en día ya estamos familiarizados con el término *criptomoneda* gracias a Bitcoin, que fue la primera, y a otras criptomonedas que han surgido después. Es un término amplio, que engloba a todos aquellos instrumentos de pago basados en tecnología criptográfica, dentro del cual podemos encontrar una gran variedad de tipos de monedas.

Una de las principales divisiones dentro de este tipo de monedas es la que se da entre Bitcoin y *Altcoins*, englobando este término a todas aquellas que no son Bitcoin. Esta diferenciación entre Bitcoin y las demás se hace debido a que tanto su objetivo como, en respuesta, su diseño, son muy diferentes al resto.

Debemos recalcar que, al igual que con sus homólogas no criptográficas, la cantidad de contextos en los que puede surgir la necesidad de crear un medio de pago digital es tan inmensa como lo pueden ser las características del mismo. Por tanto, no entraremos a explicar las diferencias en cuanto al funcionamiento o al objetivo de cada una de las miles de criptomonedas que existen actualmente, pero comentaremos los principales tipos:

- Los tokens. Son criptomonedas que se crean en plataformas *blockchain* específicas y que tienen utilidad dentro de ese ecosistema. Como ejemplo más famoso encontramos

Binance Coin, una moneda asociada a la plataforma Binance, uno de los mayores proveedores de infraestructuras *blockchain* del mundo.

- Criptomonedas de plataforma. Estas criptomonedas son la base de una plataforma *blockchain* pero, a diferencia de los tokens, son usadas como pago – e incentivo – a las aplicaciones descentralizadas que se construyen dentro de la plataforma. Sin duda el ejemplo más famoso es Ether, la segunda criptomoneda más usada tras Bitcoin, que sirve para realizar operaciones dentro de la red Ethereum, red que se ha ganado su fama gracias a la introducción de un nuevo concepto revolucionario: los contratos inteligentes.
- Las Stablecoins. Aquellas diseñadas con objetivo de mantener un valor estable, generalmente vinculadas a monedas fiduciarias o a activos como el oro. La más popular es Tether, cuyo valor está ligado al dólar.
- Las criptomonedas cuyo objetivo principal es la privacidad. Son todas aquellas que se centran principalmente en conseguir gran privacidad en cuanto a los datos personales y anonimidad en las transacciones. Un ejemplo sería Monero, la más actualizada en cuanto a sistemas que mayor éxito consiguen en dicho objetivo.
- Criptomonedas regionales. Son monedas que operan dentro de una comunidad o región, cuya utilidad recae en agilizar las relaciones económicas entre los usuarios. El caso más sonoro es el de M-Pesa, una criptomoneda que opera en Kenia.
- Criptomonedas recreativas, aquellas que se utilizan en videojuegos o aplicaciones relacionadas con el entretenimiento. La que más fama tiene es Decentraland, asociada a la plataforma de mismo nombre, un juego basado en realidad virtual dónde compras parcelas de tierra para construir en ellas,

Como podemos apreciar, son muchos los tipos de criptomonedas que encontramos, aun así, pasar por alto la gran diferencia que presentan todas con Bitcoin sería un despiste calamitoso. Pero, ¿por qué es tan diferente? Porque su objetivo es mucho más ambicioso: Bitcoin surge con la idea de llegar a convertirse en la base de un patrón económico, como antes lo era el oro, y facilitar las transacciones descentralizadas, es decir, que podamos realizar pagos entre personas sin la necesidad de una autoridad central que realice y asegure las mismas. La descentralización de las transacciones no hace a Bitcoin especial ya que existen otras criptomonedas capaces de replicar esta característica. Lo que si resulta diferente de Bitcoin respecto de las demás monedas es el hecho de que su valor no está supeditado a nada que no sean las leyes de oferta y demanda, es decir, Bitcoin es valioso en la medida que nosotros así lo consideremos, no se pueden tomar acciones unilaterales para modificar su valor. Está condición de tener "valor no dependiente" unida a la limitación cuantitativa – solo existirán 21 millones de bitcoins –, a la irrevocabilidad de las transacciones y a la inconfiscabilidad, son las características principales que convierten a bitcoin en un gran candidato a activo monetario, capaz de funcionar como reserva de valor patrimonial, como unidad de cuenta y como medio de intercambio. El valor del resto de criptomonedas sí que está supeditado a la acción de terceros y lo puede estar de dos formas: aquellas cuyo valor se liga al de otro tipo de activo, como el caso de las Stablecoins, y es entonces una obligación –en este caso, mantener estabilidad de valor respecto a otro activo– del emisor con los tenedores, o aquellas cuyo valor reside en la utilidad que aportan dentro de plataforma en la que funcionan, como el caso de las criptomonedas de plataforma, los tokens o las criptomonedas recreativas, cuya propia existencia no tiene sentido fuera del ecosistema que las alumbró.

Por todo esto, Bitcoin forma parte de una categoría distinta a todas las *altcoins*, porque su propuesta de valor es convertirse en un activo monetario global, cuyo funcionamiento es totalmente descentralizado, su valor independiente de la acción de

terceros y su cantidad limitada. No queremos sugerir que el resto de criptomonedas no sean valiosas, sino que su valor depende de su capacidad de proporcionar otro tipo de servicios distintos a los que ofrece Bitcoin, como una mayor privacidad, apoyar un proyecto *blockchain* o divertirte dentro de una plataforma recreativa.

Bitcoin y las CBDC

Las "Central Banks Digital Currencies" (CBDC) (Monedas Digitales de Banco Central), son un nuevo tipo de activo monetario creado por los bancos centrales. Actualmente son proyectos que se encuentran en desarrollo a lo largo del mundo, pero ninguno ha sido implantado plenamente en la sociedad. Las CBDC, como las define el Banco de España, son un nuevo tipo de dinero emitido electrónicamente por los bancos centrales, por tanto, comparten la mayoría de características que presenta el actual dinero *fiat*.

En la comparativa con Bitcoin, que inconscientemente se suele dar en el imaginario colectivo, son pocas las similitudes e importantes las diferencias. Si hablamos de la parte que comparten estos tipos de activos, podemos encontrar que ambos son activos monetarios y también que ambos son, por su naturaleza, activos digitales. Estas características no son novedosas en el ámbito monetario, puesto que todo activo financiero es esencialmente no tangible: en la medida en la que los activos financieros son una obligación, una "promesa de", la representación de esta obligación puede realizarse de cualquier forma, ya sea por escrito, a través de métodos informáticos o en nuestra propia mente.

Más explicación merecen sin embargo las diferencias, pues recaen en la propia esencia de estos activos. El valor de las CBDC está condicionado por la acción de los bancos centrales y de los estados que las respaldan mientras que Bitcoin no sufre este tipo de dependencia, como explicábamos en el apartado anterior. Esto implica que, si un Estado lo desea, este pueda financiarse a través de la emisión de nueva moneda y, por tanto, su CBDC experimente inflación. En este contexto, lo que se esperaría de Bitcoin es una revalorización frente a la moneda digital estatal, lo cual es una ventaja ya que Bitcoin no depende de la responsabilidad financiera de otro agente. Aquí aparece otra de las diferencias esenciales entre estos activos, la emisión de nuevos bitcoins funciona de forma totalmente descentralizada, mientras que la de las CBDC responde en última estancia a la voluntad estatal. Dentro de esta diferencia se engloban otras como el límite programado de la oferta de bitcoins o la posibilidad de que cualquier usuario participe en el proceso de emisión, frente al monopolio que ejercen los bancos centrales sobre su moneda –si bien es cierto que existen agentes dentro de nuestro sistema económico autorizados por los Bancos Centrales para aumentar la masa monetaria–.

Si hablamos de centralización vs. descentralización, otro aspecto donde aparece esta diferencia es en las transacciones: las transferencias de CBDCs quedarán supeditadas a la autorización del banco central, o a la de bancos privados que cuenten con el visto bueno del banco central, mientras que con Bitcoin es la comunidad la responsable de realizar y certificar la transferencia. De hecho, esta es una característica que comparte Bitcoin con el dinero en efectivo: no dependemos de otros agentes para realizar trasferencias entre usuarios y, por tanto, no tenemos que aportar información como el nombre o el motivo de la transferencia. Este es precisamente uno de los factores que impulsan el lanzamiento de las CBDCs: tener una mayor trazabilidad del dinero. Aunque es cierto que existen proyectos de estas "monedas digitales estatales" en los cuales el control de las

transacciones puede ser más o menos intenso por parte del banco central, el factor de que necesitarán contar con la autorización de terceros agentes para darse es inamovible.

Por último, encontramos diferencias en cuanto a la propiedad de las monedas. Las CBDCs son, otra vez por definición, instrumentos estatales, concretamente una forma de financiación que emplean estos entes políticos. Bitcoin es, al contrario, de nadie y de todos a la vez, es decir, nadie es dueño suyo en el sentido de que no está supeditado a los intereses de nadie en particular. Esta diferencia se daría, en cualquier caso, aunque la paternidad de Bitcoin hubiera sido estatal, puesto que su propio funcionamiento condiciona su posible propiedad. Notar la importancia de esta diferencia, puesto que la prioridad de las monedas estatales siempre será el Estado y, por tanto, en última instancia serán subordinadas a los objetivos políticos – como puede ser la estabilización macroeconómica o el rescate de un sector clave – mientras que Bitcoin solo tiene como objetivo resultar útil a sus usuarios.

Como advertíamos, las diferencias entre Bitcoin y las CBDCs son esenciales, mientras que las similitudes son meramente anecdóticas. Bitcoin es mucho más parecido al oro que a las CBDCs que, por así decirlo, son similares a los apuntes electrónicos de los depósitos que figuran en las cuentas de los bancos comerciales.

Particularidades de Bitcoin

Una vez que hemos explicado las diferencias entre Bitcoin y los nuevos criptoactivos "similares", las demás criptomonedas y las nuevas monedas digitales de los bancos centrales, podemos ir construyendo una idea más clara sobre lo que es Bitcoin.

No obstante, definir Bitcoin en base exclusivamente a sus características técnicas sería realizar un análisis con algo de miopía, pues las implicaciones que tendría su adopción como base del sistema monetario significarían asentar una serie de conceptos cuyo alcance no se limita solo al ámbito económico. A continuación, enumeraremos la totalidad de las características más representativas de Bitcoin, tanto las económicas como las sociales o ideológicas:

- Tiene una oferta finita, concretamente de 21 millones de bitcoins.
- Respecto a la emisión: La *blockchain* está programada para que el tiempo que cuesta minar un nuevo bloque se mantenga cercano a los 10 minutos. La recompensa por cada bloque – en bitcoins – se reduce a la mitad cada 210.000 bloques en un proceso denominado *halving*. El bloque génesis otorgó, en 2009, 50 bitcoins. El primer halving tuvo lugar en 2012, reduciendo la recompensa a 25 bitcoins, el segundo tuvo lugar en 2016 y la redujo a 12.5 bitcoins y actualmente la recompensa se encuentra en 6.25 bitcoins tras el halving ocurrido en 2020
- El coste computacional y, por tanto, económico de minar un bloque es creciente debido al aumento de usuarios, el cual implica mayor poder computacional total y hace necesario aumentar la dificultad.
- El tamaño de bloque, la información que puede contener, está limitado a 1 megabyte.
- Libre acceso a la red para cualquier persona.
- Libre participación en el proceso de emisión y, a su vez, descentralización total de las transacciones.
- Pseudoanonimato, es decir, los datos personales permanecen ocultos pero no así los datos públicos, como el pseudónimo asociado a un participante de la red.
- Trazabilidad total de las transacciones efectuadas dentro de la red

En síntesis, Bitcoin es un activo digital que funciona como activo monetario y cuyo valor no tiene ningún tipo de aval. Su pretensión es convertirse en base del sistema monetario mundial, es decir, servir como reserva de valor, unidad de cuenta y medio de pago a nivel global. Para alcanzar este objetivo, Bitcoin se sirve de las características comentadas en este punto pero, en su camino hacia él, Bitcoin afectará a otros ámbitos de la vida que también merecen consideración.

Luces y sombras

La revolución que pretende significar Bitcoin es una revolución que, de darse, afectará a una serie de aspectos que son de interés general. Todas las revoluciones conllevan cambios y las consecuencias de estos cambios pueden tener tanto su parte positiva como su parte negativa. A continuación, nombraremos los hechos más controversiales que se asociarían a la adopción de Bitcoin como base del sistema monetario.

La escasez programada

Este es uno de los aspectos más importantes en el contexto monetario. Bitcoin tiene una oferta finita de 21 millones de bitcoins, esto es de extrema importancia ya que no conocemos ningún otro activo cuya escasez vaya a ser significativa en el corto y medio plazo[3]. Hecho esencial si estamos hablando de un activo monetario.

El primero de los efectos que podemos esperar es una apreciación frente a los demás bienes, al ser finita la cantidad de bitcoins pero "no" la de los demás bienes, estos irán abaratándose en términos de Bitcoin. Es decir, Bitcoin es una moneda deflacionaria.

Siguiendo con los efectos derivados de la apreciación, una moneda con esta característica se vuelve idónea para cumplir la función de reserva de valor. Frente a las monedas fiduciarias –las cuales han demostrado históricamente una pérdida de valor inmensa a largo plazo– el uso de bitcoin como reserva de valor sería mucho más beneficioso. El oro, otro activo que sirve como reserva de valor y que se suele comparar con bitcoin, sale también vencedor en la comparación con las monedas fiduciarias, pero no tiene nada que hacer contra bitcoin ya que la escasez del oro es relativa mientras que la de bitcoin es real e inamovible.

En relación con la apreciación comentada, encontramos otro de los efectos que produce la total rigidez de la oferta monetaria. Este tipo de sistema monetario desincentiva la circulación del dinero. Cuando tenemos una moneda que constantemente tiende a revalorizarse frente a todo lo demás la gente se vuelve más reacia a usarla y más propensa a atesorarla.

Una oferta monetaria no modificable y, en última estancia, una masa monetaria fija, tiene aspectos positivos y negativos. Como parte positiva, se elimina la posibilidad de autofinanciación actual que tienen los gobiernos mediante la continua expansión de la masa monetaria soportada obligatoriamente por los tenedores de sus respectivas monedas. Como parte negativa, se pierde la posibilidad de ajustar la masa monetaria para afectar a la economía, instrumento de utilidad considerable.

---

[3] Sobre este tema, que puede resultar chocante a priori, comentar las ideas del economista Julian L. Simon, uno de los principales enemigos de la teoría del crecimiento malthusiano, quien en su libro *El último recurso* explica como los continuos avances tecnológicos afectan a la disponibilidad de los recursos naturales, pudiendo esta aumentar pese a los continuos aumentos en su consumo. Como ejemplo ofrece el caso del oro, el metal más escaso de la Tierra, que lleva siendo extraído miles de años, cada vez en mayores cantidades, pero que sigue sin desaparecer y, para más inri, con la vista en el horizonte y el desarrollo de la "minería espacial", la cual supondría un aumento exponencial en la disponibilidad de oro.

El consumo de energía

Uno de los aspectos más controvertidos que rodean a Bitcoin es el del consumo energético asociado a su producción. Como ya sabemos, Bitcoin vive y crece dentro de la red, lo cual implica una gran cantidad de terminales gestionando continuamente la *blockchain*. Para minar un bitcoin, necesitamos estar codificando gran cantidad de datos y tratar de resolver –mediante el método de prueba y error– un problema matemático altamente complejo. Esto se traduce en el uso de grandes cantidades de energía por parte de los terminales, cantidades que, como hemos explicado en apartados anteriores, son crecientes en el tiempo.

Según un estudio publicado en 2021 el consumo anual de la red bitcoin es de 113,89 teravatios hora (TWh). El mismo estudio realiza una comparativa con otras industrias relacionadas y concluye que el consumo anual de la industria bancaria tradicional es de 263,72 TWh y el de la industria del oro 240,61 TWh. Para ayudar a contextualizar mejor, el consumo anual de España es de 276,13 TWh.

Tras la anterior comparativa, y teniendo en cuenta la ya notable expansión global de Bitcoin, podemos concluir que el consumo energético de la red es considerable para la poca edad que tiene y, de seguir bitcoin su crecimiento, en el futuro podría cobrar mayor importancia de la que ya supone para el consumo energético del planeta.

Un aspecto importante a la hora de hablar del consumo energético es el llamado "mix eléctrico", lo que vendría a ser la división del consumo energético según sus fuentes. La empresa Batcoinz, especializada en el análisis del impacto de la minería, ha realizado una comparativa sobre el uso de energías renovables de diferentes industrias en los años 2018-2023 y, según su trabajo, la minería de bitcoin es la actividad que usa mayor energía sostenible (52.6%) siendo renovables el 38% de las mismas. Estos datos muestran la preocupación que existe dentro del mundo Bitcoin sobre la importancia de la responsabilidad en cuanto al tipo de consumo energético. Es más, en 2021 se firmó un acuerdo conocido como "Crypto Climate Accord" (https://cryptoclimate.org/), suscrito por más de doscientas cincuenta empresas del ámbito de las criptomonedas y *blockchain*, cuya intención es sensibilizar sobre el gran aumento del consumo energético mundial y promover un uso de energías renovables en la tecnología *blockchain*, por ejemplo mediante el uso del *hastag* #ProofOfGreen en clara sintonía con el famoso concepto de *Proof Of Work*.

Respecto a las fuentes de energía no sostenibles, es decir, las provenientes de combustibles fósiles, si hablamos de cifras, según el informe *The Carbon Footprint of Bitcoin*, publicado en la revista científica *Joule* en 2022, actualmente Bitcoin genera entre 22 y 23 millones de toneladas métricas de CO2, lo que es similar a la huella de carbono de países como Serbia o Montenegro, que no representan siquiera el 0,00001% de las emisiones totales de CO2 en 2022. (RTVE, 2022).

Bitcoin ofrece una nueva solución a uno de los problemas más frecuentes de las energías renovables: qué hacer con la energía sobrante. Las fuentes de energía renovables no presentan estabilidad en cuanto a la producción ya que depende de recursos naturales, muchas veces incontrolables, como la luz solar o el viento. Esto provoca que se den situaciones dónde haya un exceso de energía que se desperdicia. Bitcoin tecnología que hace uso intensivo de la energía, podría aprovecharse de estas situaciones de exceso energético.

La exclusión financiera

Uno de los objetivos más deseables a nivel general para todo sistema monetario es ser accesible para todos los ciudadanos, puesto que una de las condiciones para que un activo se convierta en dinero es la aceptación generalizada de su uso como tal: cuantas más personas lo usen mejor. Un dinero cuyo acceso sea limitado tendrá problemas para desarrollar su función. Analizando esta situación desde una perspectiva social, lo más deseable es que aquel dinero que escojamos sea lo más accesible posible, ya que no poder usar el dinero, o los servicios asociados a él, supone una limitación muy grande para el desarrollo de las personas. Desde un punto de vista puramente ético, no parece justo escoger un dinero o establecer un sistema monetario que resulte excluyente para potenciales usuarios.

Cuando hablamos del acceso al dinero, o al sistema monetario en general, tenemos que hacer una distinción importante. Nuestro dinero sigue siendo físico, por lo que el acceso está casi asegurado para todas aquellas personas que formen parte de una sociedad en la que existe un activo monetario que desempeñe tal función –siempre que posean una fuente de ingresos, por supuesto–. Ahora bien, otra cosa muy distinta son los servicios asociados a él, lo que conocemos como servicios financieros, como pueden ser el acceso a una cuenta bancaria, a créditos o a seguros, tener una tarjeta de crédito, etc.

El Banco Mundial define la inclusión financiera como el conjunto de acciones encaminadas a posibilitar el acceso, a las personas y empresas, a servicios financieros útiles y asequibles prestados de manera responsable y sostenible. Presenta el asunto como un problema de vital importancia, ligado, por ejemplo, a la consecución de 7 de los 17 Objetivos de Desarrollo Sostenible (ODS) o la reducción de la pobreza extrema (Banco Mundial, 2023). Las posibles causas de la exclusión financiera pueden englobarse en dos: falta de acceso geográfico a las instituciones y/o las restricciones impuestas por los prestadores de servicios – historial crediticio, ingresos mínimos, documentación personal, etc –.

Como comentábamos antes, no poder acceder a estos servicios supone una gran dificultad para el desarrollo de las personas, ya que resultan mucho más complicados tanto el ahorro como la custodia del dinero y se pierde la posibilidad de acceso a seguros y créditos –opción ampliamente utilizada en las sociedades de hoy en día, de gran utilidad financiera– para invertir en educación, vivienda o emprendimiento.

Una vez explicadas las desventajas de no poder acceder a los servicios financieros, toca poner cifras al problema. Según los datos que ofrece el Banco Mundial, para personas de 16 años en adelante, en 2011 el 50,63% tenía una cuenta bancaria mientras que para 2021 el porcentaje había escalado hasta un 76,2% (Banco Mundial, 2023). Podemos observar cómo los esfuerzos que se han llevado a cabo desde organizaciones, así como desde el compromiso de gran cantidad de países, se han traducido en una progresiva reducción de la exclusión bancaria.

Nótese un problema sobre el que aún no hemos incidido al hablar de la exclusión financiera: la exclusión financiera depende, en última instancia, de la voluntad de las entidades financieras. Una vez superadas las barreras de acceso geográfico, el principal freno para la inclusión financiera antes de la actual era digital, seguimos dependiendo de los requisitos impuestos por las entidades financieras o los Estados. Desde un punto de vista ético, lo más deseable sería un sistema en el cual el acceso a este tipo de servicios sea lo más libre posible y si, esto implica reducir el poder que tienen los Estados y las entidades para permitir o denegar tal acceso. Una solución a este problema la encontramos

en Bitcoin. Bitcoin, gracias a que no está controlado por ninguna entidad central, permite su uso a cualquier usuario que tenga acceso a Internet y, además, el hecho de no necesitar intermediarios elimina cualquier tipo de restricción a sus usuarios – tal como podría ser la documentación del usuario–. Por tanto, Bitcoin elimina todas las trabas legislativas y políticas que presentan las actuales entidades financieras para sustituirlas por la única barrera que impone a sus usuarios: el acceso a internet.

Pero vamos a tomar en consideración este requisito que impone Bitcoin para su uso ¿Cuántas personas cuentan con acceso a Internet? Según las estimaciones (Galeano, 2023) en torno a dos tercios de la población mundial cuenta con acceso a Internet (64%). Este porcentaje es menor al anterior sobre el número de personas que tienen una cuenta bancaria pero ese porcentaje estaba restringido por el mínimo de edad de 15 años. El porcentaje comentado de personas mayores de 15 años con cuenta bancaria es el 76,2% pero, si corregimos ese resultado según los datos del propio Banco Mundial para el total de población, se convierte en un 53,55% (Banco Mundial, 2022). No existen información precisa sobre el acceso a servicios financieros para personas menores de 16 años, por tanto, no se pueden extraer conclusiones definitivas sobre los efectos de la barrera que supone el acceso a internet respecto a las otras barreras ya existentes.

A modo de síntesis, la exclusión financiera es un problema que, pese a ir reduciéndose, sigue afectando a un gran número de personas alrededor del mundo. El avance de la digitalización soluciona problemas de acceso a estos servicios asociados a la cercanía geográfica de entidades financieras, pero, aun así, siguen existiendo otro tipo de barreras impuestas por los Estados y las propias entidades, barreras que, consideremos más o menos apropiadas, siguen siendo impuestas coercitivamente a la población limitando su acceso a los servicios que ofrecen este tipo de entidades y, por tanto, limitando también sus posibilidades de desarrollo. Merece la pena también recalcar que las facilidades de acceso y uso que ofrece Bitcoin están acompañadas, actualmente, por una serie de riesgos tales como su volatilidad, la dificultad de entendimiento respecto a su funcionamiento o las estafas cibernéticas. Como conclusión, desde el punto de vista de la inclusión financiera, no conocemos ninguna tecnología que facilite tanto el acceso a servicios financieros como lo hace Bitcoin.

Actividades ilegales

La irrevocabilidad de las transferencias, el pseudo-anonimato y la inexistencia de control convierten a Bitcoin en el mejor método de pago para la compra-venta de productos de forma clandestina, lejos del control gubernamental. Pese a esto, cabe recordar que hoy en día el medio de pago más utilizado para este tipo de actividades son las monedas *fiat* y también que, pese a favorecer en muchos aspectos esta operativa, si alguien comerciara con actividades o servicios ilegales usando Bitcoin, se expondría a la posibilidad de que relacionaran su identidad pseudónima con él y, por tanto, se tenga acceso al historial completo de transacciones asociadas a esa identidad.

El caso más famoso sobre actividades ilegales y Bitcoin es el del portal web *Silk Road*. La web fue creada a principios de 2011 por Ross Ulbrich, ubicada en la red Tor – conocida también como "internet profundo" –. Silk Road funcionaba como un mercado negro de drogas *online*, cuyos pagos se realizaban a través de bitcoins. El sitio web ganó gran fama y contó con un número importante de usuarios. Las claves de su popularidad fueron el pago en bitcoin, un sistema de reseñas sobre el vendedor, y un método de pago denominado "Escrow" que consiste en que un tercero retiene el pago hasta que las partes

confirman que la transacción se ha llevado a cabo de manera correcta. Este mercado se mantuvo operativo hasta octubre de 2013, cuando el FBI lo cerró y apresó a su fundador.

Ross Ulbrich fue condenado a cadena perpetua tras ser hallado culpable de siete delitos, pero su creación, Silk Road, parece seguir funcionando en el internet profundo, ya que solo un mes después de su cierre varias revistas, como Forbes y Vice, informaron de que había vuelto a haber actividad en la web.

¿Cómo funciona Bitcoin?

Tras haber explicado porqué surge Bitcoin y concretar qué es exactamente, tenemos que explicar la forma en la que Bitcoin pretende alcanzar sus objetivos, pues la tecnología de la que se sirve, así como las elecciones en cuanto a la orientación de esa tecnología, está intrínsecamente conectada con lo qué es y lo que quiere aportar Bitcoin.

¿Qué es una *blockchain*?

El término b*lockchain* (cadena de bloques) hace referencia a un tipo de tecnología usado para mantener una base de datos.

Una *blockchain* es una base de datos distribuida entre varios participantes, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí matemáticamente (Preukschat, 2017). Una de las claves de esta tecnología es que se basa en la confianza entre participes y no en una entidad central encargada de su supervisión. Esta confianza se logra mediante el consenso de una red global de ordenadores que gestionan una enorme base de datos.

Cuando hablamos de la tecnología *blockchain*, hay una serie de elementos básicos que debemos conocer para poder comprender su funcionamiento, los cuales vamos a describir brevemente (Díez García & Gómez Lardies, 2017, pp. 23-26):

- Nodos. Son los integrantes de la red, pueden ser desde un ordenador personal a una mega computadora, es decir, son todos aquellos terminales con acceso a internet y capacidad computacional.
- Un protocolo estándar. Es un software informático que otorga un estándar común para definir la comunicación entre los nodos, es decir, es el "lenguaje" particular que se usa en esa red.
- Una red entre pares. Hemos definido los integrantes y el modo de comunicación entre ellos, la red entre pares es el sistema formado por los nodos relacionados entre sí mediante el protocolo estándar. El apellido "entre pares" que lleva este tipo de red es debido a que no existe jerarquía entre los nodos, todos tienen el mismo control –entendido como derecho a: registrar, validar y almacenar la información– sobre la red que los demás participantes.
-

Estos son los elementos que forman una *blockchain*, pero para comprender mejor la esencia de este tipo de tecnología debemos hacer referencia a otros elementos que la integran (Díez García & Gómez Lardies, 2017, pp. 26-30):

- La criptografía. “Arte de escribir con clave secreta o de un modo enigmático”. Es la encargada de dotar de seguridad a la red. Mas allá de que los ordenadores usen el protocolo común para comunicarse entre ellos, la información de la red está encriptada de forma que si alguien quisiera modificar o acceder de manera desleal a partes de la información que alberga la red lo tuviera extremadamente complicado.
- La cadena de bloques. Este tipo de almacenamiento de información se basa en que cada registro de información, cada bloque, contiene toda la anterior información más la nueva. Cuando se añade un nuevo bloque, este ha de ser validado y una vez lo ha sido permanecerá invariable dentro de la cadena y esta empezará a trabajar en la emisión del siguiente bloque, del que formará parte el anterior, y así sucesivamente. Esto es lo que hace que este tipo de registro se llame “cadena” de bloques.
- El consenso. Es lo que permite que se actualice la cadena de bloques, es decir, la *blockchain* debe contar con un protocolo común para los usuarios que permita verificar y confirmar las transacciones realizadas y, por tanto, asegurar su irreversibilidad. Para que se pueda llegar a este consenso, el protocolo debe proporcionar a todos los usuarios una copia actualizada e inalterable de las operaciones realizadas en la cadena.

Merece la pena comentar aquí que no todas las *blockchain*s funcionan de la misma forma, aunque se compongan de los mismos elementos. Las *blockchain*s pueden ser públicas/privadas dependiendo de si cualquier persona sin ser usuario puede acceder o no a la cadena de bloques, abiertas/cerradas si cualquier persona puede o no convertirse en usuario, descentralizadas/distribuidas dependiendo de si todos los usuarios tienen el mismo poder sobre la red y pseudónimas/anónimas dependiendo del nivel de información del usuario requerido para realizar transferencias en la red.

Según estas especificaciones sobre el funcionamiento de una *blockchain*, podemos identificar a la *blockchain* de Bitcoin como: abierta, pública, descentralizada y pseudónima.

La *blockchain* de Bitcoin. Funcionamiento interno

Cada *blockchain* funciona de una forma particular, por tanto, la forma más ilustrativa para comprender el funcionamiento de Bitcoin es explicar cómo es el proceso mediante el cual se gestiona y expande su cadena de bloques.

Ingreso en la red

Para operar en la *blockchain* es necesario inicialmente crear una *hardware wallet* (billetera digital), que es una aplicación o servicio que permite almacenar y gestionar las claves públicas y privadas necesarias para interactuar con la *blockchain* de Bitcoin. La billetera creará una clave privada, una clave pública asociada a esa clave privada y una dirección Bitcoin, que es la que permitirá recibir fondos y realizar transacciones en la *blockchain*, asociada a esa clave pública. La clave privada es un número de 256 bits generado de forma aleatoria, mediante criptografía. Se usa la clave privada para generar una clave pública asociada y una vez obtenida, se vuelve a aplicar metodología criptográfica para ocultar y reducir el tamaño de la clave pública. El resultado obtenido será nuestra dirección Bitcoin. Para aumentar la integridad de la dirección Bitcoin y evitar errores en la escritura o manipulación de la misma, se añade un código de control, también

conocido como *checksum*. Este código se calcula a partir de los primeros caracteres del hash de la dirección. Al verificar el código de control, se puede detectar si hay algún error en la dirección. Finalmente, la dirección Bitcoin se codifica en Base58, lo que la hace más legible (Preukschat, 2017).

Cabe destacar que existen diferentes tipos de direcciones Bitcoin, como las direcciones *segwit* (compatible con *Segregated Witness*) y las direcciones P2SH (*pay-to-script-hash*), que pueden tener diferentes formatos y cálculos asociados, pero el proceso básico de generación es similar al descrito anteriormente.

Es importante tener en cuenta que la generación de una dirección Bitcoin es un proceso unidireccional. A partir de una dirección, no es posible obtener la clave privada asociada, lo que brinda seguridad y privacidad a los usuarios de Bitcoin.

¿Dónde están mis bitcoins?

Uno de los errores más comunes a la hora de comprender el funcionamiento de Bitcoin suele ser pensar que nuestros bitcoins están en algún sitio en particular, lo más común es creer que están en nuestra billetera digital, de alguna forma apartados del resto de bitcoins. Nada más lejos. Los bitcoins, activos digitales, no existen ajenos a la cadena.

Los bitcoins se almacenan en la *blockchain* de Bitcoin, que es un registro público descentralizado de todas las transacciones de Bitcoin realizadas. Cada transacción registra el movimiento de bitcoins desde una dirección de origen a una dirección de destino en la *blockchain*.

La billetera digital contiene las claves privadas necesarias para demostrar la propiedad y autorizar el gasto de los bitcoins asociados con las direcciones correspondientes. Cuando se realiza una transacción, la billetera firma digitalmente la transacción con la clave privada correspondiente para demostrar la propiedad de los bitcoins y autorizar su transferencia.

En resumen, los bitcoins en realidad residen en la *blockchain* y se transfieren de una dirección a otra mediante transacciones validadas y registradas en la *blockchain*. Para realizar estas transferencias se utilizan las claves privadas, las públicas y la dirección asociada a estas, es por esto que para operar en la red Bitcoin es necesario tener una billetera digital (Preuksach, 2017).

Transacciones dentro de la *blockchain*

Una vez creada la dirección Bitcoin, ya podemos recibir fondos y realizar transacciones dentro de la cadena. En este punto es necesario dar respuesta a una pregunta esencial: ¿Cómo obtenemos Bitcoins? Las respuestas son tres: recibir bitcoins de un usuario que ya los posea, comprar Bitcoin en un *exchange*[4] o participar en actividades de minería.

Para continuar con nuestro ejemplo, escogeremos la primera y la segunda forma –que, en realidad, dentro de la cadena son el mismo proceso– y reservaremos el apartado de la minería de Bitcoin para explicarlo detalladamente más adelante debido a su relevancia y complejidad.

[4] Un *exchange* de criptomonedas es una plataforma donde se realizan los intercambios de estas a cambio de dinero *fiat* u otras criptomonedas.

Imaginemos pues que alguien que tiene bitcoins desea enviárnoslos, o, mejor dicho, según la anterior explicación, desea transferirnos su titularidad. El usuario dará desde su billetera la orden de transferencia a nuestra dirección Bitcoin y el mensaje enviado a la red constará de: nuestra clave pública –la cual está asociada a nuestra dirección–, el saldo transferido y su firma -generada a través de su clave privada-. Inicialmente estas transacciones son recopiladas en la *mempool*[5], esperando a que los nodos se ocupen de ellas. Una vez los nodos reciban esta información, en primera instancia se asegurarán de que la transacción tenga campos correctos, como entradas y salidas válidas, tamaño adecuado y firma digital. Después de esto, los nodos utilizan la clave pública asociada con la dirección de origen para verificar la firma y confirmar que la transacción ha sido autorizada por el propietario de los fondos. El siguiente paso es asegurarse de dos cosas: que la dirección de origen tiene los bitcoins necesarios para realizar la transacción y que esos bitcoins no se estén intentando gastar al mismo tiempo en otras operaciones. Todo esto se consigue mediante el seguimiento de las transacciones efectuadas anteriormente en la *blockchain*. Una vez comprobados todos los requerimientos anteriores por un nodo, este lo propaga por la red al resto de nodos para que puedan validarla también, lo cual ayuda a garantizar el consenso y la integridad de la *blockchain*.

La transferencia se materializa cuando es incluida en un nuevo bloque de la cadena, lo cual significa que tiene que "minarse" un nuevo bloque que contenga esa información y que este sea aceptado dentro de la cadena.

Antes de abandonar este apartado hay que comentar una particularidad de la operativa de la *blockchain* de Bitcoin: cuando se realiza un movimiento de bitcoins de una dirección a otra, en el caso de que no se transfiera la totalidad de ellos, es necesario especificar el nuevo destino de todo el contenido, es decir, si tenemos diez bitcoins y queremos transferir cinco, tendremos que especificar la dirección donde enviamos esos cinco –recordemos, con su clave pública– y que los otros cinco restantes nos los enviamos a nuestra propia dirección o, como también se suele hacer, a una dirección distinta que también controlemos nosotros.

"Minería" y prueba de trabajo

Cuando escuchamos hablar de Bitcoin uno de los conceptos que aparecen con mayor frecuencia es el de *minería*. La utilización de este término hace referencia al proceso mediante el cual se obtiene un nuevo bloque en la *blockchain* y es denominada así por su similitud metafórica con el proceso de obtención del oro. Obtener oro es una ardua tarea que básicamente consiste en remover grandes cantidades de tierra para encontrar pequeños fragmentos del material. El proceso de obtención de un nuevo bloque es similar en cuanto a que es preciso realizar una gran cantidad de pruebas hasta hallar un número que resuelva un problema matemático, lo que denominamos "prueba de trabajo" y es uno de los conceptos intrínsecos del funcionamiento de la cadena Bitcoin.

Siguiendo con el ejemplo utilizado en el punto anterior, habíamos dejado la transferencia en la *mempool*, esperando a que fuera incluida en un bloque para ser consumada. Los nodos acceden a la *mempool* y recopilan un conjunto de transacciones válidas, las agrupan y forman un nuevo bloque candidato que contendrá otros datos como

[5] La *mempool* es un registro de las transacciones que son conocidas por la red, pero que aún no están incluidas en la cadena de bloques.

el *hash* del bloque anterior, la raíz de Merkle[6], una marca de tiempo y un *nonce* (*"*number only used once", número usado solo una vez). Para facilitar el seguimiento de la explicación creo necesario incidir en que el hash de un bloque es una forma de resumir la información contenida en un bloque para comprobar su integridad, por tanto, el del bloque anterior funciona como una comprobación de que la información contenida en la cadena hasta ese nuevo bloque es veraz y ha sido comprobada y validada. Esto hace que sea sencillo asegurar la integridad de la cadena antes de producir el siguiente bloque. Una vez construido el bloque candidato, se procede a la resolución de un problema criptográfico, computacionalmente costoso, que es lo que llamamos prueba de trabajo. La resolución de este problema consiste en ir probando distintos valores para el *nonce* de forma que, unido al resto de la información contenida en el bloque, el resultado que nos dé tras aplicar una función criptográfica cumpla los requisitos de dificultad establecidos por la red –comenzar con un determinado número de ceros –.

Es imperativo comprender la importancia de este proceso de "minería", la prueba de trabajo es nombrada de tal manera debido a que la resolución del problema funciona precisamente como prueba de trabajo. Hallar un *nonce* que, combinado con el resto de información, tras aplicarle una función criptográfica unidireccional[7], nos dé como resultado un hash que cumpla los requerimientos de dificultad implica realizar un gran número de pruebas. Tal es la dificultad de la prueba de trabajo que la red Bitcoin, que a finales de 2022 tenía una capacidad computacional de 250 EH/s –doscientos cincuenta cuatrillones de hashes por segundo– (González, 2022), tarda una media de diez minutos en hallar un hash válido. Incrementar la dificultad exponencialmente sería tan sencillo como requerir que el resultado comience con un cero más. Todo este proceso no solo requiere tiempo y capacidad computacional, sino que implica también un alto coste económico sobre todo por el coste de la energía empleada por los nodos para resolver el problema.

Una vez encontrada una solución para la prueba de trabajo ya tenemos un bloque válido, el minero anuncia el bloque a través de la red de nodos de Bitcoin. Esto implica transmitir el bloque a otros nodos para que puedan verificar su validez y agregarlo a sus propias copias de la blockchain. Los nodos de la red verifican la validez del bloque recibido realizando comprobaciones adicionales para asegurarse de que las transacciones sean válidas, que el bloque no contenga transacciones duplicadas o intentos de doble gasto y que cumpla con las reglas de consenso establecidas por la red de Bitcoin. Comprueban que el nonce propuesto por el minero combinado con el resto de información del bloque, la cual han vuelto a revisar, es una respuesta válida para la prueba de trabajo.

Una vez superado el proceso de validación, el minero que ha conseguido el nuevo bloque recibe dos recompensas: nuevos bitcoins que se crean al formar un bloque, lo cual se conoce como "recompensa del bloque" – actualmente, 6.25 bitcoins – y las comisiones pagadas en concepto de tarifa de transacción. Tras esto, los mineros inician de nuevo el proceso de minería para el siguiente bloque y así se hace sucesivamente para seguir ampliando la cadena.

---

[6] Se entiende como "raíz de Merkle" al hash único resultado de haber ido aplicando hashes a diferentes niveles de información relacionados.

[7] Las funciones unidireccionales son aquellas que tienen la propiedad de ser fáciles de calcular, pero difíciles de invertir.

Trayectoria de Bitcoin

Llegados a este punto, tenemos una visión más precisa de lo que es Bitcoin, así como de lo que pretendía ser cuando surgió. Es momento, pues, de analizar el recorrido de Bitcoin desde su alumbramiento, teniendo en cuenta, precisamente, los objetivos que pretendía alcanzar esta tecnología.

Pese a que ya hayamos acotado en puntos anteriores las pretensiones de Bitcoin, podemos sintetizarlas todas ellas en una sola: convertirse en la base que articule un sistema monetario global, como lo fue el oro en su momento. Para medir el desempeño de Bitcoin respecto a ese objetivo podemos servirnos de varias métricas a fin de contextualizar y medir su progreso, algunas de ellas son: número de usuarios, evolución del número de operaciones realizadas con él, evolución del precio, volatilidad del mismo y regulaciones sobre Bitcoin, entre otras.

El objetivo de Bitcoin es ambicioso, el más grande posible en su categoría, por tanto, teniendo en cuenta su corta vida –catorce años hoy en día– no podemos esperar grandes triunfos puesto que, aunque sea quizás la mejor tecnología conocida hasta la fecha para alcanzar tal objetivo, la propia inmensidad de su tarea imposibilita su consecución en un corto o medio plazo.

Usuarios y transacciones

Sin duda unas de los mejores indicadores que podemos observar para juzgar el desempeño de un activo monetario son el número de usuarios y el número de transacciones que se realizan. Estas variables nos permiten formar una idea sobre la importancia de la moneda. Pese a estar relacionadas, tienen ciertas diferencias a la hora de analizarlas.

Número de usuarios

El número de usuarios únicos dentro de la red Bitcoin es incalculable. Por su propia operativa, nos es imposible averiguar si una persona tiene varias direcciones bitcoin bajo su control. De igual forma, la propiedad de un bitcoin puede estar repartida entre cientos de tenedores, por tanto, no pretenderemos aquí dar una imagen exacta sobre cuántas personas individuales son poseedores, sino que presentaremos una serie de datos para, al menos, tener cierta idea al respecto. A finales de 2022, la web Crypto.com estima un crecimiento anual de usuarios de bitcoin de 183 millones a 219 millones (Herrera, 2023), por otra parte, la web Statista.com ofrece la estadística sobre usuarios de monederos bitcoin – término explicado en el apartado 3 – para el primer trimestre de 2023, cifrándola en 85 millones (Fernández, 2023). Por su parte, la firma de criptoanálisis IntoTheBlock, comenta en septiembre de este mismo año que su estimación de usuarios de Bitcoin alcanza un récord y se sitúa en 48,5 millones (Mutuma, 2023).

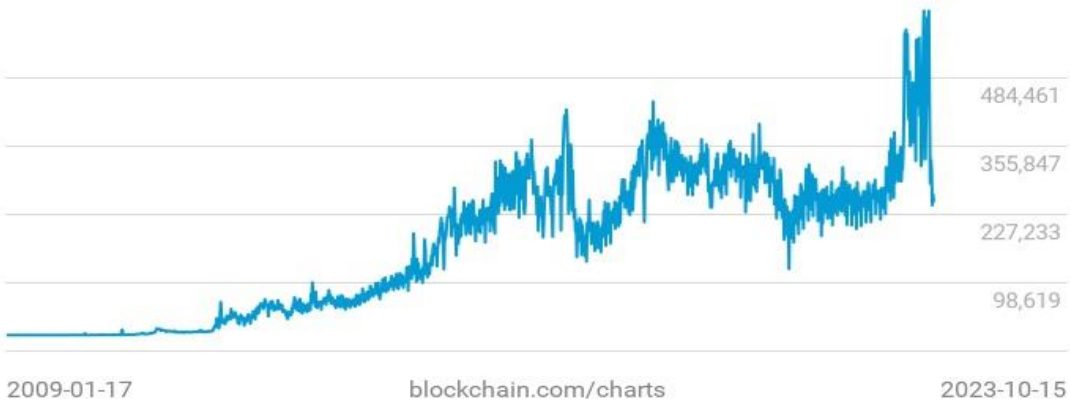
Las cifras son dispares y hay que tener en cuenta que se pueden tener varias direcciones bitcoin, hay personas que pueden ser dueños de varios terminales con los que participar de la red Bitcoin, etc. Por tanto, no sacaremos conclusiones basándonos en las cifras inexactas, sino que nos limitaremos a recalcar el buen desempeño atrayendo usuarios que ha tenido esta nueva tecnología, que cuenta con millones de ellos en menos de dos décadas de vida, superando el número de tenedores de otras divisas tradicionales ya existentes.

Evolución de las transacciones

Tras haber observado el gran número de usuarios con los que cuenta actualmente Bitcoin, es lógico deducir que las transacciones, aunque solo sea por el aumento de usuarios, habrán incrementado notablemente también. Al menos, sobre las transacciones sí que podemos obtener datos exactos, pues precisamente la blockchain funciona como libro mayor donde se anotan todos los intercambios realizados.

Figura 1

Transacciones confirmadas por día



Fuente: *Blockchain.com* (https://www.blockchain.com/explorer/charts/n-transactions).

El gráfico nos muestra una tendencia creciente en la cantidad de transacciones. Poniéndole números al asunto, un año tras el lanzamiento de Bitcoin, a finales de 2010, se realizaban en torno a 500 al día, mientras que, en estas fechas, concretamente el 15 de septiembre de 2023, se alcanzó un máximo histórico de 703.517, un aumento aproximado del 1400%. Pese al gran aumento, 700.000 transferencias diarias ni siquiera alcanzarían el número de transacciones económicas que se realizan en una ciudad durante un día.

Precio

El precio de Bitcoin es, sin duda, uno de los aspectos más importantes del mismo. Hasta el momento, podemos afirmar que el hecho más relevante en la joven historia de Bitcoin es haber pasado de no ser valioso a ser valorado por el mercado. Esto significaba que lo que ofrece bitcoin, ser partícipe de su red –o, de una forma más reducida, atesorar el fruto del trabajo de la red, bitcoins–, fue lo suficientemente valioso como para que alguien estuviera dispuesto a pagar por ello. Bitcoin se convirtió en dinero cuando alguien usó dinero para comprar Bitcoin, curioso. Este hecho se produjo en octubre de 2009, cuando una casa de cambio *online*, New Liberty Standard, vendió bitcoins al precio de 0.00094$. Poco después, en mayo de 2010 se usaron por primera vez en el mercado real bitcoins como forma de pago, fueron 10.000 bitcoins a cambio de 2 pizzas que valían un total de 25$, lo cual situaba el precio de bitcoin en 0.0025$. El buen desempeño en sus inicios de la red llamó la atención de pequeñas comunidades de criptógrafos y más simpatizantes de las ideas que nutren a Bitcoin, como los anarcocapitalistas (Ammous, 2019).

En sus etapas iniciales, el valor de estas monedas se debía a su característica de ser "coleccionables", es decir, su número es finito y sirven a unos propósitos muy especiales. Sobre cómo valorar los bitcoins, Nakamoto sugiere en una publicación en el foro *online* "Bitcoin Forum" que los bitcoins no reparten dividendo ni potencial futuro dividendo, así que deben ser valorados no como una acción, más como un coleccionable o un *commodity* (Satoshi, 2010)

Figura 2

Precio de Bitcoin en USD

Fuente: *Crypto.com* (https://crypto.com/price/es/bitcoin).

Dos grandes movimientos ocurrieron en cuanto al precio de la divisa y no se pueden apreciar con claridad en la anterior figura, ya que la escala no lo permite. En 2011, el precio pasó de unos centavos a 30$ para derrumbarse acto seguido. A inicios de diciembre de 2013 su valor rondaba los 200$, pero comenzó una escalada que lo elevó a máximos cercanos a los 1000$ en febrero del 2014, para descender posteriormente y mantenerse entre los 200-500 durante los próximos años.

El primer movimiento brusco que nos permite apreciar la escala es el que se da entre 2017-2019. El precio de Bitcoin se situaba en torno a los 1000$ para mediados de 2017, ascendió hasta un pico cercano a los 17.000$ para enero de 2018, y comenzó un descenso hasta tocar suelo cercano a los 3.500$ a inicios de 2019. Tras el descenso volvió a recuperarse, y se mantuvo entre 6.000$ y 10.000$ hasta finales de 2020. Es a partir de aquí cuando la gráfica revela el porqué de su escala, ya que desde ahí comienza una meteórica subida del precio hasta superar los 60.000$ en mayo de 2021. El precio sufrió también una gran caída, reduciéndose hasta estar cercano a los 30.000$ en agosto de ese mismo año, para volver a recuperarse y alcanzar su máximo histórico en diciembre de 68.789,63$. Tras esto, Bitcoin sufrió una nueva caída en su precio, y a finales de 2022 tocó un nuevo suelo cerca de los 16.000, se recuperó y en lo que llevamos del presente año 2023 se mantiene entre 20.000-30.000.

Estos han sido los movimientos en el precio más destacables, pero quedarnos en el movimiento en sí, sin tratar de buscar las causas del mismo, de poco interés nos resultaría para el presente trabajo, es por eso que vamos a proceder a analizar los factores que más influencia han tenido sobre el precio de Bitcoin durante estos movimientos.

Oferta inelástica

Lo primero que tenemos que entender a la hora de analizar los movimientos del precio de esta criptodivisa es que la oferta es completamente inelástica, es decir, es insensible a cambios en la demanda. Esto se debe a las características de la arquitectura de la red Bitcoin, comentadas en el tercer apartado de este trabajo, que consiguen que el tiempo que cuesta minar un bloque de bitcoins se mantenga estable en torno a los 10 minutos. Así hasta minar el último bloque y que la oferta se quede fija. La inelasticidad de la oferta implica que, ante cambios en la demanda, sea el precio el que absorba toda la variación. Si la oferta de Bitcoin fuera modificable, los aumentos (reducciones) en la demanda conllevarían aumentos (reducciones) en la producción, por tanto, una mayor (menor) oferta contrarrestaría parcialmente el aumento (disminución) del precio. Es decir, la insensibilidad de la oferta implica, necesariamente, mayor volatilidad. Un ejemplo de esto podemos encontrarlo considerando el precio de Bitcoin en 2021 y 2022: en una situación global complicada, con una reducción de la actividad económica debido a la pandemia y una crisis energética, los gobiernos abrazaron las políticas fiscales expansivas, lo cual se tradujo en un exceso de liquidez global que bien pudo ser uno de los principales condicionantes en esa época donde se produjeron grandes variaciones en el precio de la divisa.

En el contexto de Bitcoin, una tecnología que nació como una revolución, lo que podíamos esperar es una demanda creciente para sus años iniciales. Una demanda creciente combinada con una oferta inelástica da como resultado aumentos en el precio, pero este efecto no es el único que tenemos que considerar.

Los halving

Halving es el proceso mediante el cual la recompensa obtenida por minar un bloque en la cadena, los nuevos bitcoins, se reduce a la mitad, esto sucede cada 210.000 bloques minados. La recompensa inicial otorgaba 50 bitcoins por cada bloque y, tras varios halvings, se encuentra actualmente en 6.25 bitcoins.

Este proceso es de especial importancia para el mercado de bitcoins. Como comentábamos antes, la producción de bitcoins es independiente de la demanda y, además, como consecuencia del halving, disminuye progresivamente. A priori, el efecto que podemos esperar de este proceso es una apreciación de los bitcoins. Otro efecto derivado de este proceso, más en concreto del aumento de precio de la criptodivisa, es un aumento de la demanda de todos aquellos que la consideren refugio de valor.

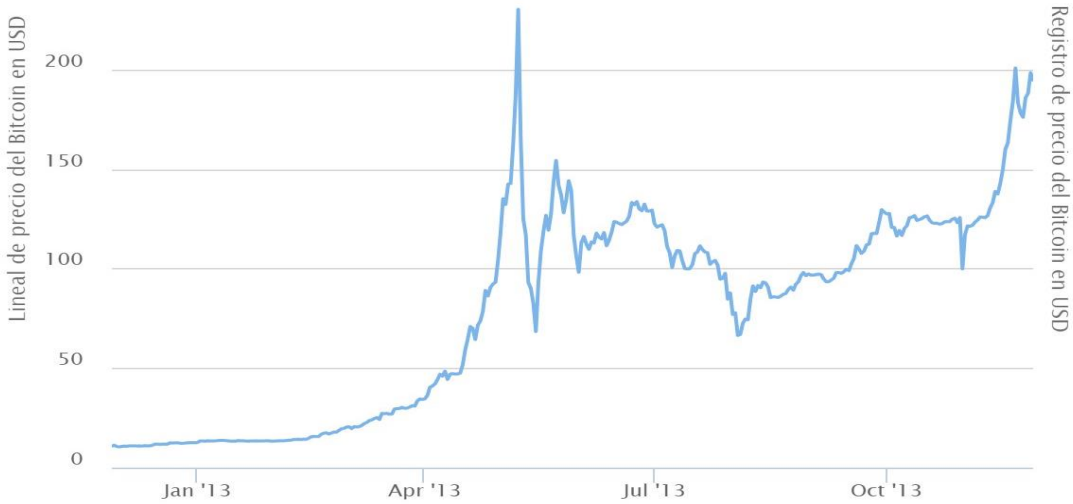
Otro factor que se ve afectado por esta reducción de la recompensa es el coste de minar un bitcoin. Esto implica que para el mismo coste de producción se obtienen la mitad de bitcoins, es decir, minar un bitcoin se vuelve el doble de caro de lo que venía siendo. Este efecto se une a los anteriormente comentados, derivados de la disminución en la producción de nuevos bitcoins, y conducen a un mayor aumento del precio de Bitcoin.

Una vez analizados teóricamente los efectos de este proceso, vamos a proceder a analizar los movimientos en el precio de Bitcoin tras cada uno de los halvings ocurridos hasta la fecha. Dado que el precio es una variable influenciada por una gran cantidad de factores, intentaremos encontrar una tendencia general analizando en conjunto los tres halvings que se han producido hasta la fecha. Para ello consideraremos el periodo de un año tras el momento de la reducción en el flujo de producción de bitcoins[8].

[8] Ha sido imposible conseguir datos precisos sobre la tasa de crecimiento diaria del precio, que habrían permitido una visión general de toda la trayectoria y de los cambios estudiados. Por tanto, mostraremos simplemente la evolución del precio ajustando las escalas.

Figura 3

Precio de Bitcoin en USD 12/2012 – 12/2013 (Primer halving, 28-11-2012)



Fuente: *Buy Bitcoin Everywhere* (https://buybitcoinworldwide.com/es/precio/).

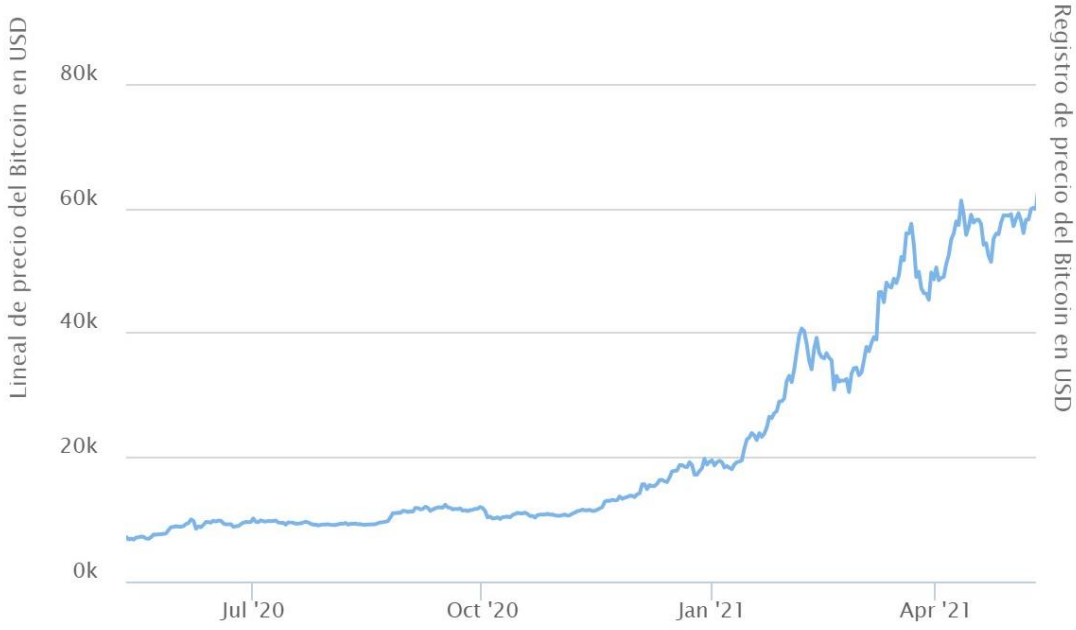
Figura 4

Precio de Bitcoin en USD 07/2010 – 07/2011 (Segundo halving, 09-07-2016)

Fuente: *Buy Bitcoin Everywhere* (https://buybitcoinworldwide.com/es/precio/).

Figura 5

Precio de Bitcoin en USD 05/2020 – 05/2021 (Tercer halving, 11-05-2020)



Fuente: Buy Bitcoin Everywhere (https://buybitcoinworldwide.com/es/precio/).

Como podemos observar, el precio tras un año de la reducción de la producción de bitcoins se ve ampliamente aumentado. Es realmente difícil explicar con exactitud la influencia del halving en la cotización de Bitcoin, dado que el precio está condicionado por una gran cantidad de factores, algunos de ellos analizados en este apartado, aun así, podemos intuir que estos procesos conducen a una apreciación de Bitcoin.

Las regulaciones

Un aspecto de especial importancia es la sensibilidad del precio de bitcoin a las regulaciones. Al tratarse de una tecnología nueva, desconocida para la mayoría de la población, la legislación ha de ir adaptándose a este nuevo activo y, precisamente por su vocación de dinero global, el valor de Bitcoin está íntimamente ligado a su aceptación por el resto de personas. Es decir, si un número importante de países -o alguno de los más importantes- restringiera el uso de Bitcoin, sería de esperar una reducción en su precio.

Para obtener una idea más ajustada de la sensibilidad del precio de la criptodivisa ante las regulaciones, vamos a comentar los cambios más significativos en su precio que hayan sido motivados por acciones políticas o regulatorias (Cámara de Comercio España-Corea, 2023; ¿Es legal Bitcoin? Una actualización de 2021 sobre la materia, 2021).

- Noviembre de 2013, Yi Gang, representante del Banco Central de China, afirma públicamente que los ciudadanos deberían poder poseer libremente bitcoins, instaurando un sentimiento optimista en la comunidad. El precio de la criptodivisa rápidamente subió de 200$ a un máximo de de 1200$.
- 5 de diciembre de 2013, China prohíbe a las instituciones financieras las transacciones en bitcoins. El precio, que venía de alcanzar su máximo, sufre una caída que lo lleva a los 386$ para abril de 2014, una reducción de más del 50% en apenas cuatro meses.
- 2018. China prohíbe los *exchanges* y persigue las páginas web de casas de cambio internacionales que operen con criptodivisas. India declara que bitcoin no será reconocido como moneda de curso legal en su país. Varios países como Lituania, Indonesia o Arabia Saudí entre otros, establecen medidas restrictivas para la compraventa de criptodivisas. La conjunción de regulaciones negativas sobre Bitcoin alrededor del mundo empujó su precio desde el máximo a inicios de año cercano a 20.000$ a bajar de 4.000$ a finales de ese mismo año.
- Julio de 2021, China presenta una nueva regulación ambiental mucho más restrictiva para los mineros de Bitcoin. La cotización, de mitad de julio a mitad de agosto, se redujo de un techo superior a los 46.000$ a precios inferiores a 30.000$.
- Agosto de 2023, Corea del Sur prohíbe la compraventa anónima de criptomonedas. El precio de Bitcoin se encontraba en 31.150$ y comenzó una bajada que lo condujo a rebajar los 26.000$ a finales de septiembre. Tras esto, el precio ha corregido mostrando una tendencia alcista hasta la fecha.

Como hemos podido comprobar, el precio de Bitcoin es bastante sensible a las regulaciones. Esto no es de extrañar, pues el valor de Bitcoin está íntimamente relacionado con la aceptación y uso del mismo, por tanto, todas aquellas regulaciones que limiten su uso serán perjudiciales, mientras que aquellas que defiendan su custodia o uso serán beneficiosas.

La relación del valor de Bitcoin con las regulaciones implica una mayor volatilidad, ya que, a diferencia de los factores hasta ahora comentados –inelasticidad de la oferta y halvings–, este factor tiene un componente de incertidumbre, es decir, nadie sabe cuándo se van a producir cambios regulatorios ni el sentido de esos cambios. Por tanto, por la propia naturaleza del proceso, este factor condicionante del precio es el que mayor volatilidad puede aportar al precio de Bitcoin. Para ser más claros, si mañana la Unión Europea o Estados Unidos decretaran ilegal la tenencia de bitcoins, lo que podríamos esperar es una reducción drástica de su precio. De la misma forma, si estos entes políticos aprobaran la posibilidad de pagar impuestos en bitcoins, la apreciación de la criptodivisa sería extraordinaria.

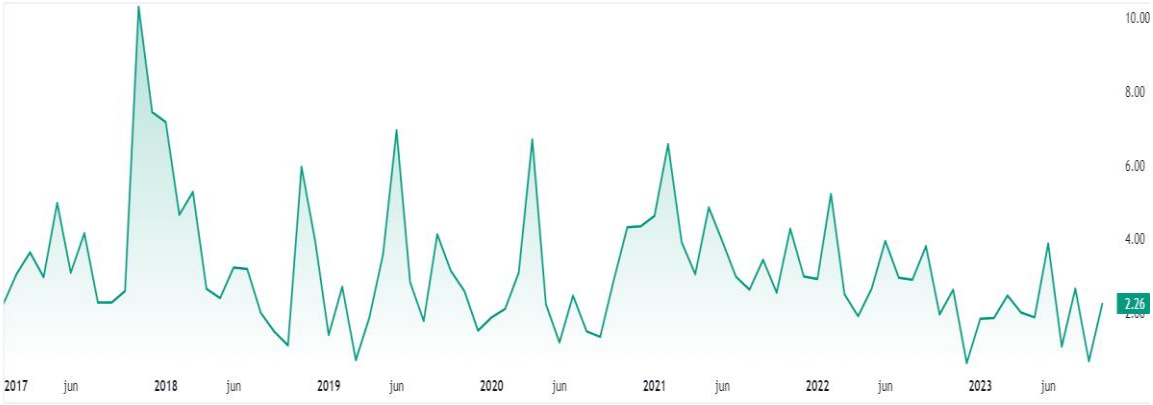
La mayoría de regulaciones restrictivas se han dado en países asiáticos, sobresaliendo por encima de todos el caso de China, que es el país que más ha perseguido la actividad de la red Bitcoin, así como por lo general el uso de criptomonedas. Por su parte, Estados Unidos y Europa se han mostrado relativamente pasivos al respecto y las regulaciones sobre la materia prácticamente no han tenido repercusiones en el precio de Bitcoin. Es llamativo el contraste entre China, una de las mayores economías del mundo gobernada de manera totalitaria, y Estados Unidos y Europa, las otras grandes economías del planeta, con gobiernos caracterizados por un mayor respeto a la libertad individual que el chino.

La volatilidad

Tras haber analizado el precio y las principales variables que lo condicionan, podemos extraer una serie de conclusiones sobre la volatilidad de Bitcoin. Aun así, antes de lanzarnos a ello, presentaremos datos concretos sobre la volatilidad de esta criptodivisa y de otras divisas tradicionales.

Figura 6

Tasa de volatilidad diaria BTC



Fuente: *Tradingview.com* (https://es.tradingview.com/symbols/BVOL24H/).

Este gráfico nos muestra la volatilidad diaria de Bitcoin, desde 2017 hasta hoy en día, que actualmente es de 2.28%. Por otra parte, la volatilidad diaria del par EUR/USD se encuentra en 0.838%, la del USD/JPY es de 0.192%. (Calculadora de volatilidad de Forex, 2023). Por lo general, la volatilidad diaria de las divisas tradicionales es extremadamente menor que la de Bitcoin, ya que el mercado de divisas, en contraposición, es un mercado maduro y relativamente estable. Sin embargo, lo interesante en este punto es la evolución que ha seguido la volatilidad. Como podemos observar en el gráfico, la volatilidad muestra una tendencia descendente, y según un estudio de Glassnode (Diestéfano, 2023), la volatilidad semanal fue, en agosto de este mismo año, un 3.6%, situándose así en cifras inferiores al 95% de la historia de Bitcoin. La volatilidad mensual alcanzó mínimos no registrados desde 2020, y se situó por debajo del 97% de la historia de Bitcoin.

La volatilidad de la criptodivisa sigue siendo mucho mayor que la de las divisas tradicionales, pero, con una mirada más amplia, el camino que ha recorrido hasta hoy en día Bitcoin es un camino de progresiva reducción de la volatilidad. Teniendo en cuenta los factores analizados en el apartado anterior, referidos a la sensibilidad del precio de Bitcoin, podemos observar que los principales hechos que afectaron a su precio – la mayoría de las regulaciones y los dos primeros halvings- se produjeron hasta 2018. También hemos comprobado, en el apartado referido a usuarios y transacciones, como se ha producido un aumento en el número de tenedores de bitcoins, en un proceso que podríamos asimilar al ciclo de vida normal de un producto, dónde las primeras etapas del ciclo se caracterizan por un aumento en su consumo tras ir superando el desconocimiento del público y el miedo asociado a la novedad. El aumento de usuarios y transacciones,

volviendo más líquido el mercado, y el paso del tiempo, ganando popularidad la criptodivisa y afrontando las regulaciones -lógicamente más numerosas en sus primeros años de vida-, son factores que claramente reducen la volatilidad de los años iniciales de Bitcoin.

La volatilidad de Bitcoin sigue siendo elevada respecto a las otras divisas, pero el dato descontextualizado de poco nos sirve. Si tenemos en cuenta que este tipo de activo no ha existido jamás, que sus competidores no criptográficos forman un mercado con décadas de tradición y millones de partícipes, que le ha rodeado una inestabilidad legislativa especialmente en sus primeros años y, con especial significado económico, que la producción de nuevos bitcoins no está relacionada con la demanda y se reduce progresivamente–, podemos concluir que es de esperar una progresiva reducción en la volatilidad de Bitcoin, con más razón si la criptodivisa sigue avanzando en su objetivo de convertirse en la base del sistema monetario global, ganando fama, usuarios y estabilidad legal.

Antes de concluir este apartado, es necesario hacer una mención al papel que ha tenido la especulación en la volatilidad. Desde sus inicios, Bitcoin ha sido objeto de compra por gente con meros intereses especulativos. La gran fama, así como los aumentos exponenciales de precio en sus etapas iniciales, han hecho de este activo una tentación para un gran número de "oportunistas", que han comprado bitcoins con objetivos distintos a los que su creador pretendía.

El caso de El Salvador

Este país, el más pequeño de todo América Central, se ha convertido en el primero en reconocer Bitcoin como moneda de curso legal, esto implica que las empresas que ahí operan están obligadas a aceptar los pagos en esta criptodivisa o que se puedan pagar impuestos con ella. Existían otros países como Japón, que fue el pionero, que aceptaban pagos en Bitcoin, pero es distinto permitir el pago -siempre que las dos partes acepten- que obligar a aceptar esa forma de pago.

La economía salvadoreña presenta un crecimiento moderado pero estable, con una tasa de crecimiento anual del 2.5% entre 2013 y 2019, unido a una progresiva reducción de la desigualdad – con una rebaja del índice de Gini de 0.54 en 1998 a 0.38 en 2019 – alcanzando el nivel más bajo de toda la región (Banco Mundial, 2023) Actualmente la economía salvadoreña ocupa el lugar 101 por volumen de PIB y, pese a los desafíos, "El Salvador tiene un gran potencial para impulsar un crecimiento económico dinámico, inclusivo y resiliente" (Banco Mundial, 2023),

Bitcoin Beach

La historia de Bitcoin en El Salvador comienza con un proyecto inédito y revolucionario, el conocido como "Bitcoin Beach" (Playa Bitcoin), que nació en un pequeño pueblo costero llamado El Zonte. Su promotor, Michael Peterson, es un empresario estadounidense que se mudó en 2005 a El Zonte, enamorado de las olas que bañan sus paradisiacas playas. Movido por su fe cristiana, desde su llegada a este pequeño pueblo fundó una asociación que da apoyo social a la comunidad y a los misioneros evangélicos. Pero lo que Peterson no se imaginaba es que, en 2019, su lucha por el desarrollo social y económico de la zona llegara a oídos de un misterioso criptomillonario. La revista *Forbes* (Kofman, 2020*)* narra esta curiosa historia, en la que un inversor anónimo compró bitcoins cuando apenas valían 0.05$ y los mantuvo años intactos hasta que la revalorización de su inversión alcanzó varios millones de dólares. Este afortunado

inversor decidió entonces utilizar parte de su riqueza de manera solidaria y, tras la búsqueda de un perfil adecuado, se puso en contacto con Peterson y le otorgó una donación de seis cifras. Esta donación, hecha en bitcoins, tenía como objetivo desarrollar una pequeña economía circular con la criptodivisa como base del sistema monetario. La única condición que puso el donante fue que las transmisiones de dinero se realizaran en bitcoins, sin convertirlos a otra divisa. El objetivo inicial era introducir la criptodivisa en la economía a través de las remuneraciones de los proyectos sociales, así como aceptar el pago de bienes y servicios que ofertaban las asociaciones surgidas de la donación, cuyo objetivo es promover el desarrollo económico-social de El Zonte. El plan surgió efecto y Bitcoin comenzó a circular en la economía del pequeño pueblo, pero el verdadero punto de inflexión fue la instalación de un cajero Bitcoin, que mejoró enormemente la liquidez de la moneda. Las iniciativas sociales entraron en sinergia con las posibilidades que abría la nueva moneda -es decir, acceso a servicios financieros- y el proyecto creció rápidamente en la zona. Hoy en día Bitcoin Beach es un referente mundial de economía basada en Bitcoin, de hecho, en 2020 superaron el récord diario de transacciones en bitcoins para una misma zona, alcanzando durante uno de los festivales que organiza el pueblo más de 2.000.

Ley Bitcoin

El 9 de junio de 2021 El Salvador se convirtió en el primer país del mundo en tratar a Bitcoin como moneda de curso legal, a través de la que fue conocida como "ley Bitcoin"[9]. Para entender por qué ahí, antes que en cualquier otro lugar, tenemos que prestar atención a tres importantes factores: la importancia del envío de remesas de dinero desde el exterior, el éxito de Bitcoin Beach y el apoyo político. De todos estos factores, sin duda el más decisivo fue el apoyo político, ya que en última instancia todo depende de decisiones políticas. Este apoyo lo encontró la criptomoneda en la figura del carismático y controvertido líder político salvadoreño, Nayib Bukele, quien alcanzó la presidencia en 2019 cuando para entonces ya llevaba tiempo mostrando públicamente su apoyo a Bitcoin.

La ley consta de 16 artículos y dota a Bitcoin de la mayoría de los derechos con los que cuentan todas las monedas oficiales como: posibilidad de tributar en bitcoins, posibilidad de expresar cualquier precio en dicha moneda, obligatoriedad en cuanto a su aceptación, etc. No obstante, existen dos particularidades que debemos comentar. La primera es que la unidad de cuenta de El Salvador seguirá siendo el dólar, así lo indica el artículo 6, el cual impone el dólar como unidad contable. Lo que implica este artículo es que, aunque se acepte el pago de los impuestos en bitcoins como indica el artículo 4, tendremos que realizar el cálculo de las imposiciones a través del tipo de cambio dólar-bitcoin que se establezca y por tanto una persona no puede realmente llevar su contabilidad en bitcoin, es decir, "bitcoinizarse". Es necesario aclarar esta cuestión ya que, si fuera posible tanto llevar una contabilidad únicamente en bitcoins como el pago a través de ellos, habría sido una medida mucho más revolucionaria y habría significado una mayor confianza en el uso de la moneda. La otra particularidad que queda de comentar está relacionada con la anterior, se trata del riesgo de cambio soportado por todos aquellos agentes que reciban un pago en bitcoin y decidan convertirlo en dólares. El artículo 8 explica que el Estado dotará de los medios necesarios para realizar conversión automática en bitcoins, no obstante, en el transcurso del tiempo entre el

[9] Decreto 57 de 2021 [con fuerza de ley]. Ley Bitcoin. 8 de junio de 2021. D.O. No. 110.

momento en que se recibe el pago y el que se da la orden de cambio existe un riesgo de cambio que ha terminado siendo asumido por el Estado, es decir, esta ley socializa el riesgo de cambio de todas aquellas personas que reciban pagos en bitcoins y deseen recibirlos en dólares.

La "ley Bitcoin" es una ley innovadora en la materia, pero también es una ley inmadura cuyo texto original es ambiguo, sobre todo en los aspectos que hemos destacado. Es a la vez una ley atrevida pero precavida: atrevida por ser la primera en otorgarle a Bitcoin la mayoría de derechos con los que cuenta una moneda de curso legal; precavida porque no permite utilizarla como unidad contable y esta es una de las características esenciales de una moneda.

El camino recorrido, el camino por recorrer

Dos años han pasado desde la aprobación de la "ley Bitcoin" y cuatro desde el nacimiento de "Bitcoin Beach". Una encuesta realizada en enero de 2022 por la cámara de comercio de El Salvador (Cámara de Comercio e Industria, 2022) muestra que el 91`7% de los empresarios han considerado indiferente la adopción de Bitcoin, mientras que el 4`7% piensa que les ha perjudicado, situándose levemente por encima de los que piensan que les ha favorecido. La misma encuesta muestra que solo el 13`9% de los encuestados realizó o recibió pagos en bitcoins.

El actual gobierno salvadoreño es opaco sobre sus reservas de bitcoins y sobre sus finanzas en general, es difícil encontrar datos sobre su uso y la única fuente de información sobre la inversión pública en bitcoins son las redes sociales de su presidente. Aun así, los datos presentados muestran que a Bitcoin le está costando arrancar en El Salvador, pero también revelan que es una realidad, que se está usando.

El caso de El Salvador podría considerarse como un experimento, un experimento dentro de otro experimento como está siendo Bitcoin, que a su vez comenzó albergando otro experimento más pequeño: Bitcoin Beach. En definitiva, El Salvador es uno de esos lugares a los que tenemos que prestar atención para tener una idea más actualizada de lo que puede ser Bitcoin, pero tampoco podemos pretender que este caso sea modélico para el resto de países ya que los factores que afectan a Bitcoin son distintos en todo el mundo y, además, cambiantes.

Conclusiones

Una vez completado el análisis de la vida de Bitcoin, desde sus antecedentes cuando aún siquiera existía, pasando por su nacimiento y sus inicios hasta llegar al momento actual, podemos extraer una serie de conclusiones que servirán para formarnos una idea bastante fiel de lo que es Bitcoin.

Comenzábamos este trabajo comentando que el objetivo de este invento era convertirse en dinero. Si tenemos en cuenta una de las principales teorías sobre el origen del dinero, la teoría de Carl Menger, observaremos que un activo no se monetiza de la noche a la mañana, sino que sigue un proceso. Este proceso, de forma resumida, comienza cuando un activo asume la función de depósito de valor, posteriormente, la asunción generalizada como depósito de valor conducirá a que los agentes comiencen a aceptarlo también como medio de pago y, por último y lógicamente, cuando la gente ahorre y pague a través del mismo activo, este terminará por ser usado como unidad de cuenta. Bitcoin no comenzó funcionando como depósito de valor, pues su precio no mostró estabilidad –

ni podría haberlo hecho ya que hablamos de un activo emergente– sino que lo que sucedió fue que mostró un aumento exponencial en su precio, pasando por una etapa inicial de elevada volatilidad y es ahora cuando su precio comienza a ser más estable. En cuanto al siguiente paso del camino, el reciente aumento en las transacciones y en el número de usuarios nos conduce a pensar que cada vez está siendo más utilizado como medio de pago, y podemos encontrar ejemplos de empresas – precisamente empresas punteras como Microsoft o Starbucks– que aceptan pagos en esta criptodivisa. El último paso que le queda a Bitcoin es ser adoptado como unidad de cuenta y este es el más lento y difícil.

Tras repasar su camino, podemos concluir que aún queda por recorrer y para ver si esto sucede tendremos que esperar, pues son tantas las variables que afectan a este proceso que se torna difícil aventurar un resultado final – tampoco es ese el objetivo de este trabajo –. No obstante, Bitcoin ya ha recorrido la primera parte del camino para convertirse en base de sistemas monetarios, y lo que vaya a suceder de ahora en adelante es una completa incógnita. Hemos visto que Bitcoin cuenta con las características estructurales y – en relación con ellas – monetarias necesarias para alcanzar su objetivo, pero aun así el desenlace dependerá de decisiones sociales y políticas. Lo que también podemos concluir es que si Bitcoin termina por lograr su objetivo estaremos ante una revolución sin parangón en el ámbito monetario e incluso en el social.

Me gustaría hacer una mención especial a la tecnología *blockchain* ya que, pese a no ser uno de los temas principales del trabajo, he tenido que indagar sobre su funcionamiento y posibles aplicaciones. Creo sinceramente que este tipo de tecnología será considerada uno de los mayores avances del presente siglo y confío en que en los próximos años veremos como comienza a ser usada en muchos sectores como el de seguridad o en los medios de comunicación.

Otro tema que aparece en el trabajo y es merecedor de mención son las CBDCs, sin duda una nueva idea de monedas que está a punto de hacerse realidad y que estará en competencia directa con Bitcoin. En mi opinión, ambas serán las opciones en una de las decisiones más importantes que tendrá que tomar la sociedad en esta era digital: Bitcoin o CBDCs.

Bibliografía

Adeyanju, Craig. (30 de octubre de 2017). *Bitcoin vs Dólar estadounidense: casos de volatidiad. Cointelegraph.* (https://es.cointelegraph.com/news/bitcoin-vs-us-dollar-heres-how-the-dollar-compares-to-bitcoin-in-terms-of-volatility).

Ammous, Saifedean. (2018). *El patrón Bitcoin.* (12ª edición). Deusto.

Decreto 57 de 2021 [con fuerza de ley]. Ley Bitcoin. 8 de junio de 2021. D.O. No. 110. Disponible en (https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/2/2020-2029/2021/06/E75F3.PDF).

Banco Munidal. (3 de octubre de 2023). *El Salvador: panorama general* (https://www.bancomundial.org/es/country/elsalvador/overview).

Banco Mundial. 11 de mayo de 2023. *Inclusión financiera.* (*https://www.bancomundial.org/es/topic/financialinclusion/overview*

Banco Mundial. *Población total 2022.* (*https://datos.bancomundial.org/indicator/SP.POP.TOTL*).

Bastardo, Javier. (28 de abril de 2019). *Wei Dai: creador de un precedente para Bitcoin.* Criptonoticias. (https://www.criptonoticias.com/educacion/wei-dai-creador-precedente-bitcoin/).

Calculadora de volatilidad de Forex. (s.f.). Investing. Consultado el 20 de octubre de 20023 de https://es.investing.com/tools/forex-volatility-calculator).

Cámara de Comercio e Industria de El Salvador. (2022). *Primer sondeo empresarial 2022.* (https://camarasal.com/wp-content/uploads/2022/03/SondeoEmpresarial35422_FINAL10032022.pdf).

Cámara de Comercio España-Corea. *Corea del Sur prohíbe la compraventa anónima de criptomonedas.* Recuperado el 20 de octubre de 2023 de (https://www.camaracomercioespanacorea.es/es/comunicacion/noticias/723-corea-del-sur-prohibe-la-compraventa-anonima-de-criptomonedas.html).

Carvajal Villaplana, Álvaro. (Diciembre de 2001). "El Cypherpunk: crítica a la tecnología informática". *Revista de comunicación*. (https://revistas.tec.ac.cr/index.php/comunicacion/article/view/1249/1153).

Cota, Isabella. (2 de septiembre de 2023). "Dos años de bitcoin en El Salvador de Bukele: un experimento opaco con una moneda poco utilizada". El País. (https://elpais.com/america/economia/2023-09-02/dos-anos-de-bitcoin-en-el-salvador-de-bukele-un-experimento-opaco-con-una-moneda-poco-utilizada.html).

Criptomoneda. (16 de febrero de 2023). En *Wikipedia* (https://es.wikipedia.org/w/index.php?title=Criptomoneda&oldid=149315121).

Cypherpunk. (27 de marzo de 2023). En *Wikipedia*. (https://en.wikipedia.org/w/index.php?title=Cypherpunk&oldid=1146791468).

David Chaum. (20 de febrero de 2023). En *Wikipedia* https://es.wikipedia.org/w/index.php?title=David_Chaum&oldid=149397048).

Diestéfano, Bárbara. (9 de agosto de 2023). "«Varias métricas de volatilidad de bitcoin están colapsando»*:* Glassnode*", Criptonoticias.* (https://www.criptonoticias.com/mercados/varias-metricas-volatilidad-bitcoin-estan-colapsando-glassnode/).

¿Es legal Bitcoin? Una actualización de 2021 sobre la materia. (s.f.). Cointelegraph. Recuperado el 18 de octubre de 2023 en (https://es.cointelegraph.com/learn/is-bitcoin-legal).

Fernández, Rosa. (23 de mayo de 2023). "Evolución trimestral del número de usuarios del monedero blockchain a nivel mundial del primer trimestre de 2017 al primer trimestre de 202". *Statista*. (https://es.statista.com/estadisticas/710401/bitcoins-usuarios-mundiales-semestrales-del-wallet-blockchain/

Galeano, Susana (26 de enero de 2023). *"El número de usuarios de internet en el mundo crece un 1,9% y alcanza los 5.160 millones". Marketing Ecommerce*. Recuperado el 16 de agosto de 2023. https://marketing4ecommerce.net/usuarios-de-internet-mundo/#:~:text=De%20acuerdo%20con%20el%20informe,(7.910%20millones%20de%20personas)).

González, Jesús (25 de diciembre de 2022). "¿Qué es el hashrate de Bitcoin?". *Criptonoticias,*. Recuperado el 15 de agosto de 2023. (https://www.criptonoticias.com/criptopedia/que-hashrate-bitcoin/).

Herrera, Jesús. (19 de enero de 2023). "Número de usuarios de Bitcoin y criptomonedas creció 40% en 2022: reporte" *Criptonoticias.* (*https://www.criptonoticias.com/comunidad/adopcion/numero-usuarios-bitcoin-criptomonedas-crecio-40-2022-reporte/*).

Koffman Tatiana. (14 de julio de 2020). *This El Salvador Village Adopts Bitcoin As Money*. Forbes. (https://www.forbes.com/sites/tatianakoffman/2020/07/14/this-el-salvador-village-adopts-bitcoin-as-money/?sh=734f85d92044).

Maldonado, José (3 de mayo de 2019). "¿Quién es Wei Dai?" *Bit2me Academy*. Recuperado el 20 de febrero de 2023. (https://academy.bit2me.com/quien-es-wei-dai/).

Maldonado, José (5 de abril de 2019). *¿Quién es Timothy May?*. Bit2me Academy. Recuperado el 20 de Febrero de 2023. (https://academy.bit2me.com/quien-es-timothy-may/).

Maldonado, José. (24 de diciembre de 2016). *Manifiesto Criptoanarquista*. Bit2me Academy. Recuperado el 20 de febrero de 2023. https://academy.bit2me.com/manifiesto-criptoanarquista/).

Maxwell, Mutuma. (3 de septiembre de 2023). "El optimismo se dispara en el criptoespacio: los poseedores bitcoin superan ya los 48,5 millones". *Cryptopolitan*. (https://www.cryptopolitan.com/es/el-optimismo-se-dispara-los-titulares-de-btc-ahora-superan-los-48-5-millones./).

Nakamoto, Satoshi. (2009). *Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer* [en línea]. En Bitcoin.org. [Consulta: 08-02-2023]. Recuperado de: (https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf).

Precio de Bitcoin en USD (s.f). Crypto.com. Recuperado el 15 de diciembre de 2023 en (https://crypto.com/price/es/bitcoin).

Precio de Bitcoin en USD (s.f). Buy Bitcoin Worlwide. Recuperado el 15 de diciembre de 2023 en (https://buybitcoinworldwide.com/es/precio/).

Preukschat, A., Kuchkovsky, C., Goméz Lardies, G., Díez García, D. & Molero, I. (2017). *Blockchain: la revolución industrial de internet.* (10ª ed.). Barcelona, Centro Libros PAPF.

Radio Televisión Española. (11 de octubre de 2022). *El nuevo récord de las emisiones de CO2 complica cumplir con el objetivo de un calentamiento global de 1,5 grados.* (*https://www.rtve.es/noticias/20221111/emisiones-globales-co2-record-2022/2408743.shtml#:~:text=5%20min.-,Las%20emisiones%20globales%20de%20CO2%20alcanzar%C3%A1n%20un%20nuevo%20r%C3%A9cord%20en,Sharm%2DEl%20Sheik%2C%20Egipto*).

Satoshi. (27 de agosto de 2010). Bitcoins are most like shares of common stock. [Mensaje 24]. Mensaje dirigido a https://bitcointalk.org/index.php?topic=845.msg11403#msg11403

Silk Road. (22 de septiembre de 2022). En *Wikipedia*. https://es.wikipedia.org/w/index.php?title=Silk_Road&oldid=146194444

Transacciones confirmas por dia (s.f.). Blockchain.com., Recuperado el 15 de diciembre de 2023 en (https://www.blockchain.com/explorer/charts/n-transactions).

Volatilidad diaria de Bitcoin (s.f.). Tradingview.com. Consultado el 15 de diciembre de 2023 en (https://es.tradingview.com/symbols/BVOL24H/).