

JUNIO 2021

**CUNEF**

COLEGIO UNIVERSITARIO DE  
ESTUDIOS FINANCIEROS

BITCOIN Y LA DESNACIONALIZACIÓN DEL DINERO:  
¿PATRÓN MONETARIO O BURBUJA ESPECULATIVA?

RODRIGO FLORO SOLER

TUTOR: LUIS ALFREDO JIMÉNEZ FERNÁNDEZ

## Contenido

Introducción.....	3
Abstract.....	3
1. ¿Cómo hemos llegado hasta aquí? .....	4
2. ¿Cómo funciona la red Bitcoin? .....	16
3. Críticas más comunes hacia Bitcoin .....	28
4. Evolución de Bitcoin: Desde 2008 hasta hoy .....	42
5. Situación regulatoria .....	53
6. Bitcoin frente a CBDC.....	57
7. Bitcoin en las empresas e IIC.....	63
8. Conclusiones .....	68
9. Glosario de términos.....	71
Bibliografía .....	73
Ilustración 1 La moneda lidia electrum.....	5
Ilustración 2 Evolución del precio del oro (valores reales). Fuente: Macrotrends.....	9
Ilustración 3 Composición de las reservas de divisas mundiales. Fuente: FMI. ....	10
Ilustración 4 Cantidad y tipos de salidas. Fuente: FMI .....	11
Ilustración 5 Tipos de interés de referencia en las principales economías del mundo. Fuente: Reuters. .	12
Ilustración 6 Creación de dinero en EEUU. Fuente: Gavekal. ....	13
Ilustración 7 Investigación y Calendario de CBDC. Fuente: Deutsche Bank. ....	14
Ilustración 8 Árbol del dinero diseñado por Adrian y Mancini-Griffoli. Fuente: FMI. ....	15
Ilustración 9 Esquema de una transacción en Bitcoin. Fuente: Nakamoto,2008. ....	17
Ilustración 10 Evolución de las recompensas por bloques de Bitcoin. Fuente: Bit2me .....	18
Ilustración 11 Desglose de todas las recompensas por bloque de la red. Fuente: Bit2me. ....	19
Ilustración 12 Oferta de bitcoin y tasa de crecimiento.....	20
Ilustración 13 Esquema de funcionamiento de Blockchain con bitcoin. Fuente: Euromoney .....	22
Ilustración 14 Relación entre la clave privada, clave pública y la dirección de Bitcoin. Fuente: O'Reilly...	23
Ilustración 15 Ejemplo de una dirección pública de Bitcoin. Fuente: Bit2me .....	24
Ilustración 16 Mayores casas de cambio por volumen (en miles de millones de dólares. Fuente: Coinmarketcap.com.....	25
Ilustración 17 Ejemplo de una transacción de bitcoin. Fuente: Mastering Bitcoin. ....	26
Ilustración 18 Diferencia entre registro centralizado y el registro en Bitcoin. Fuente: BIS.....	26
Ilustración 19 Cadena de transacciones en la red. Fuente: Mastering Bitcoin.....	27

Ilustración 20 Bitcoin: Consumo de electricidad estimado. Fuente: Universidad de Cambridge. ....	31
Ilustración 21 Consumo eléctrico de Bitcoin comparado con países. Fuente: Universidad de Cambridge. .....	31
Ilustración 22 Comunicado de Elon Musk en Twitter. ....	32
Ilustración 23 Comparación emisiones de CO2 totales y de Bitcoin. Fuente: Our World in Data.....	33
Ilustración 24 Evolución de las fuentes de energía buscada por los mineros. Fuente: VanEck .....	34
Ilustración 25 Poder adquisitivo del dólar desde 1913. Fuente: Gold Telegraph.....	36
Ilustración 26 Volatilidad histórica del oro y Bitcoin anualizadas en periodos de 60 días. Fuente: Deutsche Bank. ....	37
Ilustración 27 Volatilidad de Bitcoin y de otros activos tradicionales. Fuente: Deutsche Bank.....	37
Ilustración 28 Evolución de la volatilidad de 90 días de retornos anualizados de Bitcoin frente a activos tradicionales. Fuente: Hougan & Lawant.....	38
Ilustración 29 Porcentaje de actividades ilegales usando Bitcon. Fuente: Chainanalysis .....	39
Ilustración 30 Portada incluida en la primera emisión de bitcoin. ....	42
Ilustración 31 Primeros años de historia de Bitcoin. Fuente: Andreas Antonopoulos.....	43
Ilustración 32 Artículo de la revista Forbes en diciembre de 2018. Fuente: Forbes .....	44
Ilustración 33 Artículo de Financial Times en Abril de 2018. Fuente: Financial Times.....	44
Ilustración 34 Artículo de Bloomberg en marzo de 2018. Fuente: Bloomberg .....	44
Ilustración 35 Evolución precio de bitcoin en 2019. Fuente: Cointelegraph.....	45
Ilustración 36 Datos mensuales de inflación en EEUU. Fuente: Bloomberg. ....	45
Ilustración 37 Volumen de transacciones diarias de Bitcoin y otras materias primas. Fuente: Deutsche Bank. ....	46
Ilustración 38 Porcentaje de encuestados que afirma tener o usar criptomonedas. Fuente: Statista. ....	47
Ilustración 39 Evolución precio de bitcoin desde su creación. Fuente: Deutsche Bank.....	48
Ilustración 40 Correcciones históricas de Bitcoin. Fuente: CoinMarketCap.com.....	49
Ilustración 41 Cheque pagado a los hogares estadounidenses durante la pandemia. ....	57
Ilustración 42 Funcionamiento de la arquitectura híbrida CBDC. Fuente: BIS .....	58
Ilustración 43 Países con bancos centrales participantes. Fuente: BIS .....	59
Ilustración 44 Motivaciones para emitir CBDC. Fuente: BIS.....	59
Ilustración 45 Diferencia entre un sistema monetario centralizado y descentralizado. Fuente: IE .....	62
Ilustración 46 Flor del dinero. Fuente: Bech y Garrat (2017) .....	63
Ilustración 47 Empresas con bitcoin en su balance en mayo de 2021. Fuente: BitcoinTreasuries.org.....	64
Ilustración 48 Mapa de comercios que aceptan criptomonedas y de cajeros ATM. Fuente: Coinmap.org .....	65
Ilustración 49 Correlación de Bitcoin con las Renta Variable de grandes empresas. Fuente: Hougan y Lawant (2021) .....	67
Ilustración 50 Correlación de Bitcoin con la Renta Variable de pequeñas empresas. Fuente: Hougan y Lawant (2021) .....	67
Ilustración 51 Correlación de Bitcoin con el oro. Fuente: Hougan y Lawant (2021) .....	67

## **Introducción**

Decía Friedrich A. Hayek, premio nobel de economía en 1974, que el dinero es uno de los mayores instrumentos de libertad jamás inventado. Sin embargo, el dinero del que disfrutaban las sociedades hoy en día tiene poco que ver con el que ha sido durante la mayor parte de la historia.

A lo largo de este trabajo vamos a repasar los sistemas monetarios que se han dado hasta la fecha, primero, en el que el oro circulaba físicamente, para luego hacerlo a través de billetes respaldados por lingotes en las cámaras de los bancos. Tras la II Guerra Mundial el oro pasa a un segundo plano al convertirse el dólar americano en el eje del sistema, que a su vez se respaldaba por oro. En 1971 se suspende la convertibilidad del dólar en oro y entramos en el sistema actual, donde las distintas monedas no tienen un respaldo (además de la confianza) y fluctúan los tipos de cambio entre ellas libremente.

Posteriormente se estudiará el funcionamiento de Bitcoin además de las funciones clave que tiene la red y que posibilitan su correcto desempeño, como son la prueba de trabajo, las funciones hash etc. Una vez visto cómo se hace y se registra una transacción en esta red, haremos una recopilación de las críticas más comunes hacia la criptomoneda y a la red.

En el siguiente capítulo analizaremos la evolución que ha tenido Bitcoin, centrándonos principalmente en el auge de 2020 y los siguientes capítulos consistirán en explicar la situación regulatoria en la que se encuentra y posteriormente una comparación con las CBDC.

El último capítulo irá dedicado a hacer un análisis de las empresas que ahora mismo apuestan por Bitcoin, ya sea con compras directas y manteniéndolo en el balance, o por aceptarlo como medio de pago. Finalmente veremos de forma resumida cual es la situación de las IIC respecto a esta criptomoneda.

## **Abstract**

As Friedrich A. Hayek, 1974 economics nobel winner, stated: money is one of the major instruments of freedom ever conceived. Nevertheless, current money is far different from what it used to be.

Along this work, we will go over all monetary systems. Firstly, when the gold was a physical asset; then, when the money was supported by it. After the IIWW, U.S. dollar ousted gold as the axe of the system. In 1971 U.S dollar ceased to be convertible in gold and we began the current system where various coins do not have any sort of support (except the confidence) and their convertibility consequently fluctuates.

Afterwards, bitcoin working will be studied as well as key roles of the net which ensures its correct development, like work's proof, hash functions... Once detailed the working of this net, we will gather the most common critics against the cryptocurrency and the net.

In the next chapter, we will analyse bitcoin's evolution focusing on its 2020 rise and its regulation. Eventually, we will compare bitcoin with CBDC.

Last chapter will be dedicated to an analysis of companies that bet on bitcoin by direct purchases, keeping it into the balance sheet or accepting it as a payment method. Finally, we will see a summary of the IIC situation with respect to this cryptocurrency.

## **1. ¿Cómo hemos llegado hasta aquí?**

Al igual que otras instituciones fundamentales en toda sociedad como el lenguaje, el dinero se desarrolló como algo espontáneo, a través de un proceso de prueba y error en el que participaban todos los agentes económicos a través de ofrecer un determinado producto o metal (oro) como medio de pago o en su lugar, aceptarlo como compensación por la entrega de productos o desarrollo de servicios.

El principal problema que tenía que resolver el dinero era el de la doble necesidad que se debía satisfacer con el trueque. Para realizar un intercambio con el sistema de trueque se tenían que dar dos circunstancias al mismo tiempo: yo tengo que encontrar a una persona que ofrezca el producto que deseo adquirir y, a su vez, tengo que disponer de aquello que desea la persona que ofrece el producto.

Este sistema era muy ineficiente y limitaba el comercio a los productos y servicios más básicos, haciendo con ello que la economía no creciera y fuera prácticamente de subsistencia. Gran parte de esa ineficiencia era producto no sólo de no poder distinguirse vendedor y comprador, también de la ausencia del precio.

Tener un sistema de precios es algo esencial en una economía, al ser una representación de las valoraciones que los individuos hacen de los bienes y servicios los precios son las señales en la economía.

Antes de llegar al uso de los metales como medio de pago se comerciaba con otros productos como alimentos (el té fue una forma de dinero en Asia) o la sal.

Sin embargo, fueron los metales preciosos los que se convirtieron en el medio de intercambio más generalizado por su enorme liquidez en relación a otros productos y por ser considerados válidos para las funciones concomitantes y subsidiarias del dinero (Menger, El Dinero, 1892).

Generalmente siempre se ha formulado que funciones del dinero son tres:

1. Medio de pago: Se refiere a su intercambiabilidad por otros bienes y servicios debido a que es aceptada de forma generalizada.

2. Depósito de valor: Hace referencia a la posibilidad de atesorar la moneda y conservar su poder adquisitivo en el futuro.
3. Unidad de cuenta: Referenciado a poder medir cualquier bien o servicio en términos de la moneda.

Además de las funciones del dinero, el economista inglés William Stanley Jevons detalla propiedades de la que podía disfrutar el buen dinero (Jevons, 1875):

- Utilidad y valor.
- Portabilidad.
- Indestructibilidad.
- Homogeneidad.
- Divisibilidad.
- Cognoscibilidad.

Al igual que Menger, Jevons concluyó que los metales preciosos eran los que mejor cumplían con esas propiedades y es que “Algunos metales parecen haber sido escogidos por la naturaleza para ser empleados como dinero por encima de otras sustancias, al menos cuando actúan como medio de cambio y depósito de valor” (Jevons, 1875).

En cuanto al origen del dinero, para Carl Menger “El dinero no es una creación de la ley (...) sino un fenómeno de origen social” (Menger, El Dinero, 1892). Con ello recalca que la creación del dinero como institución no procede de una creación fruto de la ley o de las autoridades, sino de un proceso dinámico compuesto por la actuación de todos los agentes participantes en la economía que a través de un proceso de prueba y error llegaron a usar determinados metales preciosos como dinero.

Dentro de los metales preciosos el que más importancia asume es el oro debido a dos características fundamentales: el oro es químicamente tan estable que es prácticamente imposible destruirlo, además no se puede sintetizar a través de otros materiales y sólo se extrae a través de su mineral no refinado, el cual es difícil de encontrar (Ammous, 2018)

Las primeras monedas de oro que se conocen se acuñaron en Lidia, alrededor del siglo VII a. de C. Esta moneda era conocida como electro y consistía en una aleación con plata.

*Ilustración 1 La moneda lidia electrum*



Con el paso del tiempo los griegos adoptaron el oro como moneda, la cual se extendió desde la Grecia Continental a la Grecia Magna y a Sicilia. La moneda era diferente en función de la ciudad en la que nos encontrásemos, estando en Tebas la Estatera, el Terradracma en Atenas, el Didracma en Tarento, etc.

Con la extensión del uso del oro y otros metales preciosos como la plata la sociedad se encaminó hacia la primera forma de patrón monetario.

Antes de entrar en los distintos sistemas o patrones monetarios debemos explicar en qué consisten estos.

El patrón monetario es una medida de valor por la que se rige un sistema monetario. La fijación del sistema se puede hacer de determinadas formas, anclando a un metal precioso (en este caso oro) la moneda nacional en función del contenido del oro de la propia moneda o de las cantidades de oro de la que disponga en sus reservas los bancos centrales.

### **1.1 Patrón Oro Clásico**

Este patrón monetario se caracterizaba fundamentalmente por el uso del oro acuñado en monedas siendo éstas curso legal, estando aceptadas como medio de pago generalizado (López Zafra, 2014).

Mediante este sistema la relación existente entre las distintas monedas se basaba en establecer relaciones entre ellas en función del oro contenido.

Con el paso de los siglos se dieron muchos casos de reducción del contenido del oro en la moneda con el objetivo de devaluarla y estas acciones han jugado un papel fundamental en el devenir de las sociedades que sufrieron estas actuaciones. A continuación, podemos ver unos ejemplos:

En la Antigua Roma, durante los mandatos de Nerón, Caracalla y Diocleciano el áureo y el denario vieron reducidos sus contenidos en oro y plata respectivamente: el denario pasó de 3.9 gramos de plata a apenas cubrir el alma de bronce de la moneda mientras que el áureo redujo su contenido de oro desde los 8 gramos a los 4,5 de una nueva moneda conocida como el sólido (Ammous, 2018).

El camino que siguió Roma es de sobra conocido, esas medidas, unidas a otras como el control de precios provocaron una crisis en el Imperio que con el paso de los años desembocaría en su caída hasta derrumbarse por completo en el 476 d.C.

Otra suerte corrió el Imperio romano de oriente, que bajo el mandato de Constantino el Grande adoptó el sólido como moneda, una vez que Constantino se comprometió en no recortar los 4,5 gramos de oro de la moneda que posteriormente se conocería como besante. Mientras Roma sucumbía a los bárbaros Bizancio sobrevivió durante más de mil años y su moneda sirvió como fuente de inspiración para el dinar islámico (Ammous, 2018).

Podemos encontrar otro ejemplo cómo la alteración de la moneda puede arruinar un país entero en la experiencia de John Law en Francia, cuyas políticas de emisión de moneda y destrucción del

poder adquisitivo llevaron a Francia a la quiebra en 1726, al igual que la Compañía del Mississippi la cual también había dirigido (López Zafra, 2014).

## **1.2 Patrón Oro y billetes de papel**

El sistema monetario donde el oro u otros metales circulaban como moneda tenía un coste evidente que era el coste de transporte. El hecho de tener que comerciar con monedas pesadas para comerciar constituía un problema para los agentes económicos.

Por lo tanto, se buscó un mecanismo que pudiera ofrecer las ventajas del anterior sistema pero que al mismo tiempo eliminase esa gran desventaja que era el tener que transportar físicamente el dinero.

Primero aparecieron los billetes de banco, que constituían un certificado de la cantidad de oro que tenía depositada en el banco el dueño de dicho certificado. Es por eso por lo que, aunque oficialmente no se recoge en la legislación hasta tiempo más tarde, en la práctica Inglaterra por ejemplo, estaba de facto en un estándar de papel moneda desde 1797 (Kemmerer, 1944).

Esos certificados podían usarse como medio de pago y posteriormente entre los diversos bancos se liquidarían las cantidades de oro correspondientes.

Sin embargo, este sistema trajo serios problemas en tanto en cuanto no se estableció la obligatoriedad de un coeficiente de caja del cien por cien respecto al oro depositado y los bancos encontraron una actividad sumamente rentable en el hecho de emitir certificados por importe superior al oro que tenían depositado (Huerta de Soto, 1998).

En el periodo de entreguerras se discutió los problemas de la economía internacional, y la vuelta al patrón oro fue considerada como una condición para restaurar el equilibrio perdido (García Ruiz, 1992).

Así, durante la década de los 20, se reinstauró el oro, pero el patrón oro clásico fue sustituido por un patrón de lingotes (Gold Bullion Standard) con el cual las naciones ya no acuñaban monedas de oro, sino que respaldaban su dinero (billetes y monedas) con lingotes de oro que se almacenaban en las reservas de los bancos centrales.

Este sistema hizo más fácil a los gobiernos y a las autoridades monetarias manipular la oferta de la moneda (Kemmerer, 1944). De la misma manera que siglos antes lo habían hecho los bancos comerciales, emitiendo más moneda que el oro realmente depositado. En 1913, año de creación de la Reserva Federal, sólo se respaldaba con oro un 40% de los billetes emitido, reduciéndose al 25% en 1945 y eliminándose la obligatoriedad de respaldo en 1968 (López Zafra, 2014).

Entre que no se reinstauró de forma correcta el sistema monetario (Reino Unido forzó a que la paridad de su moneda fuese la misma que en la preguerra) y el Crack de 1929 los países fueron abandonando uno a uno el patrón de oro en lingotes (Ver Ilustración 1).

Tabla 1 Salida de los países del patrón oro 1929-1936. Fuente: Kemmerer, 1944.

1929	1931	1932	1933	1934	1935	1936
Argentina, Austria y Uruguay	Brasil, Alemania, Reino Unido, India, Noruega, Dinamarca, Suecia, Canadá y Japón	Chile y Perú	Estados Unidos	Italia	Bélgica	Polonia, Francia y Holanda

El caso de Estados Unidos fue sin duda el más llamativo, pues en 1933 el presidente Franklin D. Roosevelt recibió un poder para prohibir exportaciones y atesoramiento de oro no ya sólo en tiempos de guerra, sino “en cualquier periodo de emergencia nacional declarado por el presidente” (López Zafra, 2014).

Con esta medida el dólar fue devaluado hasta los 35 dólares por onza de oro.

### 1.3 Bretton Woods

Con el fin de la II Guerra Mundial el Sistema Financiero se transformó por completo.

Los acuerdos de Bretton Woods tenían por objetivo que el nuevo sistema monetario internacional garantizara la estabilidad del tipo de cambio, promoviera el crecimiento económico y que los países no optaran por la devaluación competitiva que pudiera perjudicar el comercio internacional.

Además de la creación de dos nuevas instituciones, como lo eran el FMI y el Banco Mundial, el cambio más importante radicaría en que el oro físico dejaría de ser la reserva de los bancos centrales para poner en su lugar al dólar americano, y éste estaría anclado al oro a un precio de 35\$ la onza de oro, mientras las monedas de otros países estarían ancladas a un tipo fijo respecto al dólar.

Este sistema por tanto también tenía un anclaje, el gobierno americano no podía expandir la oferta monetaria debido a que tenía que mantener el cambio en 35 dólares frente a la onza de

oro, mientras que los gobiernos de otros países a su vez no podían expandir su oferta monetaria por tener que estar anclado a un tipo fijo al dólar.

Esto condujo a un sistema de reserva global basado en un tándem oro-dólar, pero siendo las reservas de dólares el elemento más dinámico y el principal a la hora de establecer sus reservas otros bancos centrales.

Sin embargo, aunque el tipo de cambio era fijo, se podía ajustar frente al dólar si el FMI acordaba que la balanza de pagos de un país se encontraba en una situación de desequilibrio estructural.

Cerca del final del sistema de Bretton Woods el FMI creó los derechos especiales de giro (DEG) que tenía por objetivo aumentar la liquidez internacional (López Zafra, 2014).

Finalmente, en 1971 Nixon acabó con el sistema de Bretton Woods principalmente porque el déficit comercial y las políticas expansivas de Estados Unidos lo hicieron insostenible y los tipos de cambio fijos empezaron a verse muy presionados (Ocampo, 2017).

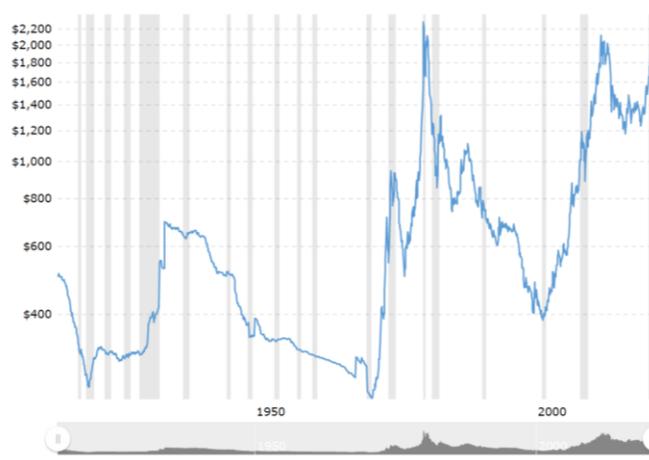
#### 1.4 Sistema de monedas fiat

En 1971 el presidente estadounidense Richard Nixon declara la suspensión de la convertibilidad del dólar en oro como medida provisional<sup>1</sup>.

Con esta medida se pone fin a los acuerdos de Bretton Woods y entramos en un entorno en el que las monedas no están ancladas a ningún metal en una determinada cuantía, por lo que ese corsé que tenían los gobiernos desaparece y pueden empezar a aumentar la masa monetaria sin respaldo.

De hecho no es casualidad que tras el anuncio de Nixon de 1971 el precio del oro se disparase, al tiempo que Estados Unidos aumentaba la oferta monetaria (ver Ilustración 2)

Ilustración 2 Evolución del precio del oro (valores reales). Fuente: Macrotrends



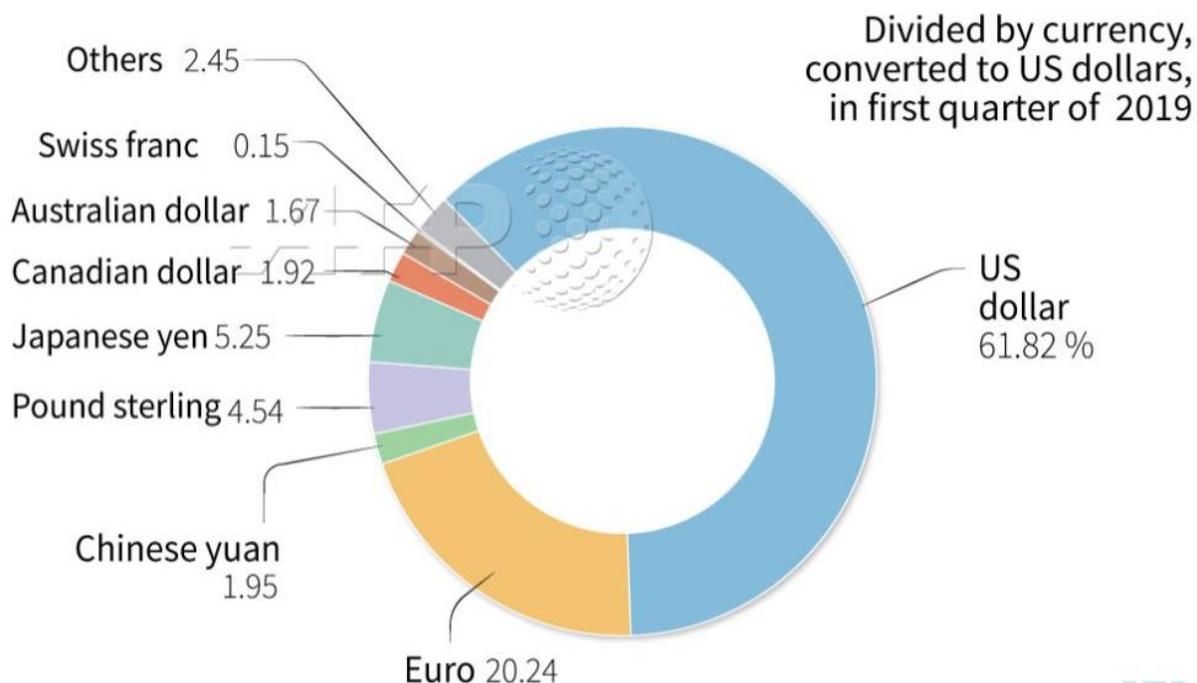
<sup>1</sup> <https://www.federalreservehistory.org/essays/gold-convertibility-ends>

El abandono de la convertibilidad de dólares en oro llevó a dos procesos para reformar el sistema monetario internacional (Ocampo, 2017).

Esos problemas eran el intento de reconstruir un sistema de paridades de tipo de cambio entre las monedas más importantes y el segundo problema fue la negociación para diseñar un nuevo sistema monetario internacional.

La mayoría de los países optaron por establecer un sistema de tipos de cambio flotantes siendo el dólar la moneda más utilizada como pago y como reserva en todo el mundo y así sigue hasta día de hoy (ver Ilustración 3).

Ilustración 3 Composición de las reservas de divisas mundiales. Fuente: FMI.



Por tanto, desde 1971 nos encontramos en un sistema de monedas fiduciarias donde generalmente tienen un tipo de cambio flotante<sup>2</sup>, bien sea flotación sucia o flotación libre, y entre ellas compiten entre sí como activos de reserva y medios de pago internacionales.

A diferencia de los tipos de cambio fijos, la flotación en los tipos de cambio viene determinado por el mercado y nos encontramos con varios tipos (Duttgupta, Fernandez, & Karacadag):

- Tipos de cambio dentro de bandas de fluctuación: La moneda se mantiene dentro de ciertos márgenes de fluctuación de por lo menos  $\pm 1\%$  en torno a un tipo de cambio central —o el margen entre los valores máximo y mínimo del tipo de cambio excede del 2%— y el tipo central o los márgenes se ajustan periódicamente a una tasa fija o en respuesta a

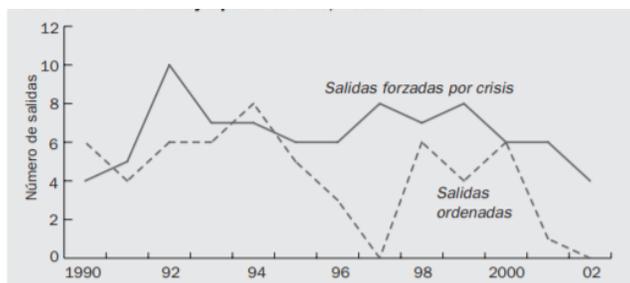
<sup>2</sup> Es cierto que aún existen excepciones como es el caso del Yuan chino que presenta tipos de cambio fijos respecto otras monedas como el dólar.

cambios de determinados indicadores cuantitativos. El grado de flexibilidad del tipo de cambio y el grado de independencia dependen de la amplitud de la banda.

- Flotación dirigida: La autoridad monetaria trata de influir en los movimientos del tipo de cambio sin especificar una trayectoria predeterminada ni un objetivo concreto para el tipo de cambio.
- Flotación independiente: El tipo de cambio queda determinado por el mercado, y la intervención en el mercado cambiario es esporádica y discrecional, y normalmente tiene por objeto moderar la tasa de variación y evitar fluctuaciones excesivas del tipo de cambio, pero no establecer su nivel.

En la siguiente imagen se puede observar la cantidad de salidas que se han producido de tipos de cambio fijos a tipos flexibles (Ver Ilustración 4)

Ilustración 4 Cantidad y tipos de salidas. Fuente: FMI



Este sistema de tipos de cambio flotantes con un régimen de monedas fiat provocó que los bancos centrales de gran parte del mundo pudieran expandir la oferta monetaria de una manera más agresiva.

### 1.5 Actuación de las autoridades monetarias tras la Gran Recesión

La crisis financiera de 2008 provocó un antes y un después en nuestros sistemas financieros.

El 26 de noviembre de 2008 la Reserva Federal, con Bernanke a la cabeza inició un plan para imprimir 1,7 billones de dólares<sup>3</sup> en los siguientes 18 meses (Haslam & Lamberti, 2015) que usarían para rescatar el sistema financiero estadounidense.

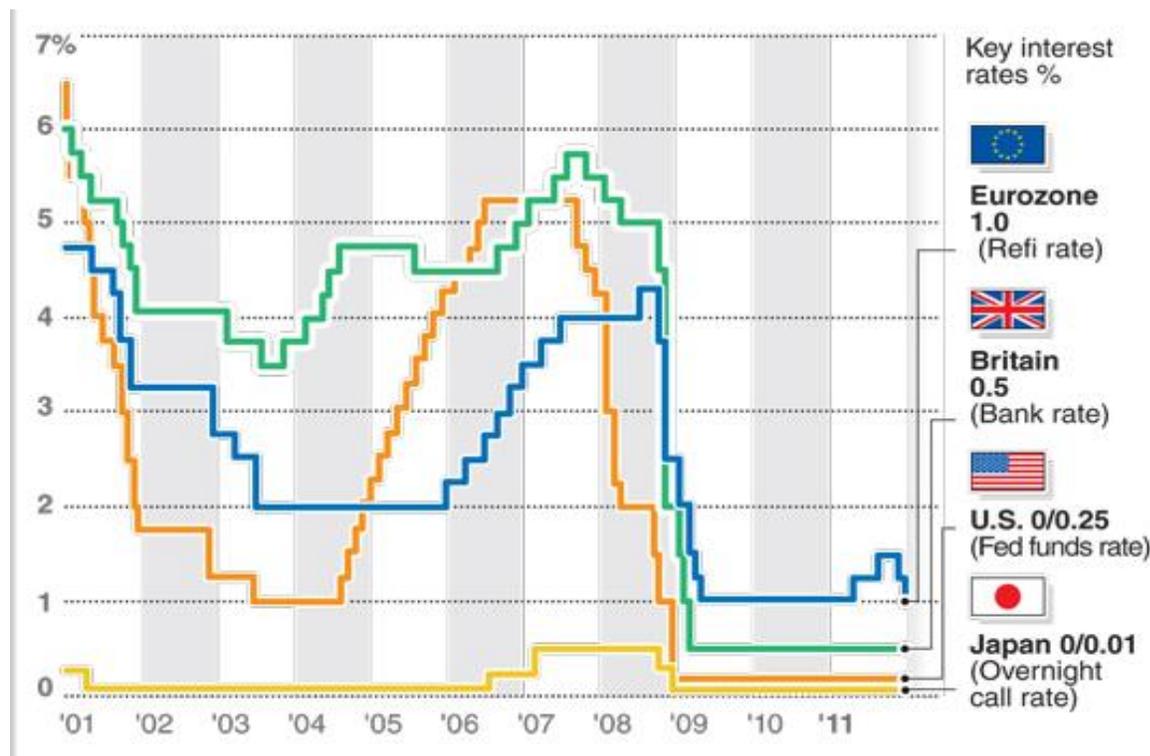
Esta política de impresión de dinero fue seguida por la amplia mayoría de bancos centrales de todo el mundo para dar respuesta a la crisis financiera.

La impresión de dinero per se dio paso a otras políticas más complejas pero cuya finalidad era exactamente la misma, como son por ejemplo los programas de flexibilización cuantitativa o QE por sus siglas en inglés.

Estas políticas fueron acompañados por las rebajas de los tipos de interés de referencia(ver Ilustración 5).

<sup>3</sup> Notación europea.

Ilustración 5 Tipos de interés de referencia en las principales economías del mundo. Fuente: Reuters.



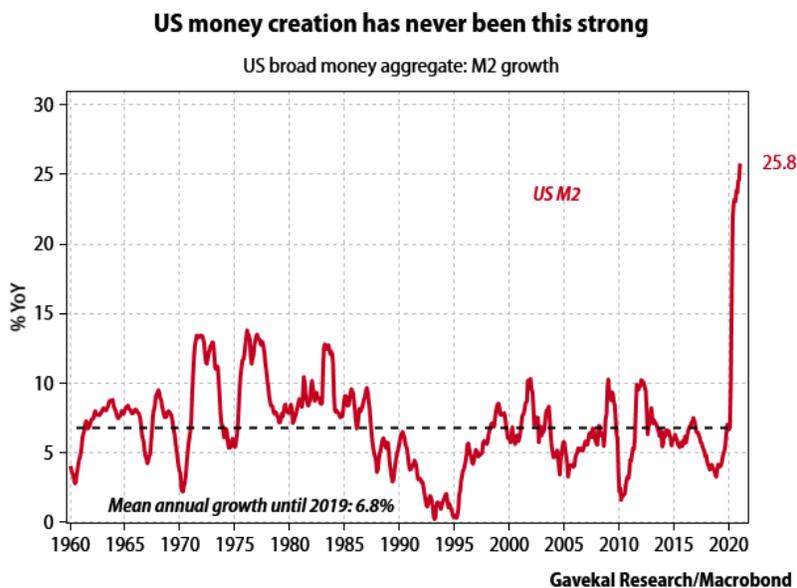
Aunque a partir de 2015 la Reserva Federal fue reduciendo los estímulos y aumentando progresivamente los tipos de interés, otras economías como la Eurozona siguieron el camino inverso, empezando en ese periodo con las políticas monetarias no convencionales, anunciando su programa de compra de activos y posteriormente reduciendo el tipo de interés de referencia al 0%.

Si ya muchos economistas denunciaban el exceso de liquidez que había en la economía, la crisis del Covid-19 intensificó esto en el momento que las autoridades monetarias decidieron conceder tanta liquidez al sistema como fuera necesario.

En Estados Unidos el tipo de referencia fue recortado un 1,5% hasta situarse en el rango de 0-0,25 al tiempo que se reactivaban los programas de compras. La masa monetaria (medida por el

incremento de M2) en Estados Unidos ha aumentado a un nivel sin precedentes (Ver Ilustración 6).

Ilustración 6 Creación de dinero en EEUU. Fuente: Gavekal.



En Europa se hizo las terceras series de operaciones de refinanciación a largo plazo o TLTRO III por sus siglas en inglés, y, además de continuar con los programas de compras de activo, incluyeron un programa especial de compras debido a la emergencia por la pandemia (PEPP).

Aunque sólo se haya puesto como ejemplo a Estados Unidos y la Eurozona, estas políticas expansivas han sido llevadas a cabo por una gran cantidad de países<sup>4</sup>.

Sin embargo, la crisis financiera de 2008 provocó algo más.

El 1 de noviembre de 2008, un (o unos) programador informático bajo el seudónimo de Satoshi Nakamoto envió un correo electrónico en el que anunciaba que estaba trabajando en un “nuevo sistema de dinero electrónico que utiliza por completo una red peer-to-peer (P2P) sin la necesidad de un tercero de confianza”. A esa red la llamaría Bitcoin<sup>5</sup>.

En octubre de 2009 una casa de cambio llamada New Liberty Standard decidió vender 5050 bitcoin por 5,02 dólares, registrándose así la primera compra de esta criptomoneda con dinero.

<sup>4</sup> <https://www.icmagroup.org/Regulatory-Policy-and-Market-Practice/covid-19-market-updates/monetary-policy/>

<sup>5</sup> El lector observará que a lo largo del trabajo verá la palabra escrita tanto con mayúscula como con minúscula, refiriéndose la primera a la red per se y la segunda haciendo referencia a la criptomoneda de la red (tanto en singular como en plural, pues es un error añadirle una “s” al final).

El 22 de mayo de 2010 otra persona pagó con 10.000 bitcoin dos pizzas que costaban 25 dólares siendo esta la primera vez que el bitcoin se usaba como medio de intercambio (Ammous, 2018).

Con el paso de los años se dieron a conocer la red y la criptomoneda cada vez más, posibilitando que en países que sufrían controles de capitales o cuya moneda nacional había perdido su poder adquisitivo los ciudadanos pudieran transaccionar con ella o recibirla desde el extranjero.

Tras la crisis del Covid-19 el interés de los agentes económicos en las criptomonedas, pero particularmente en el bitcoin, aumentó, ya fuesen por motivos especulativos o por creencia de que podrían mantener su poder adquisitivo en bitcoin, lo cierto es que en 2020 y 2021 los precios de las criptomonedas (y el número de estas) han vivido sus mayores subidas.

Esto ha provocado que bitcoin haya experimentado una escalada constante hasta alcanzar los 60.000 dólares y con ello atraer la atención de reguladores y autoridades monetarias.

Se ha avanzado rápidamente este 2020 y 2021 en los proyectos llevados a cabo por los bancos centrales (Ver Ilustración 7).

Ilustración 7 Investigación y Calendario de CBDC. Fuente: Deutsche Bank.



Los bancos centrales han empezado a diseñar el camino para emitir en un futuro cercano su propio dinero digital o CBDC por sus siglas en inglés. Los tokens de CBDC que estén en manos del

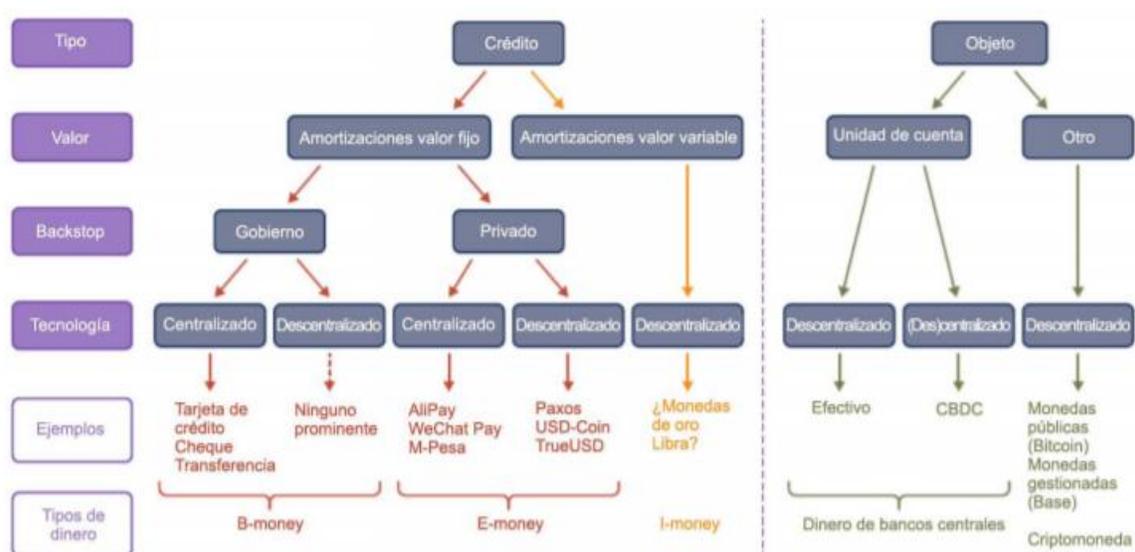
público en general se sustituirán por efectivo y con ello no acabarán con la función de los depósitos bancarios (Conthe).

### Clasificación de los medios de pago actuales:

El término “teoría institucional del dinero” señalado por Antonio Sáinz de Vicuña enfatiza que el dinero actual consiste en un crédito frente al banco central emisor y también el saldo acreedor de depósitos a la vista (Giovanoli, 2004).

Sin embargo, se puede adoptar una perspectiva más amplia y clasificar los medios de pago existentes junto con los aparecidos más recientemente como un “árbol del dinero” (Adrian & Mancini-Griffoli, 2019).

Ilustración 8 Árbol del dinero diseñado por Adrian y Mancini-Griffoli. Fuente: FMI.



La primera clasificación es en función de su tipo en “créditos” (como pueden ser depósitos bancarios) u “objetos” (billetes y moneda física). La última clasificación hace referencia a la tecnología donde se especifica si es a través de un sistema centralizado o descentralizado como puede ser Bitcoin u otras criptomonedas que utilicen la tecnología *blockchain* (Conthe).

Nosotros a lo largo de este trabajo detallaremos el funcionamiento de la red Bitcoin para posteriormente tratar muchas de las críticas a la criptomoneda y poder hacer un análisis de si realmente esas críticas están fundadas o si se trata de críticas sin respaldo creadas por el desconocimiento acerca de la criptomoneda. Los siguientes capítulos harán referencia a cómo ha evolucionado la red y el precio de la moneda y la someteremos a un análisis de las propiedades monetarias para ver si se ajusta a estas. El capítulo siguiente estará dedicado a bitcoin dentro de las carteras de inversores y fondos de inversión. Acabaremos con una comparación entre las

criptodivisas emitidas por los bancos centrales (CBDC) y el bitcoin y analizaremos el futuro que le puede devenir a través de un estudio de las regulaciones por parte de las autoridades.

## 2. ¿Cómo funciona la red Bitcoin?

Lo primero que tenemos que hacer es una definición de lo que son las criptomonedas, veremos dos definiciones diferentes, la primera por parte de una autoridad monetaria y la otra por la propia criptocomunidad.

- Representación digital de valor, no emitida por un banco central, una entidad de crédito o una institución de dinero electrónico, que en algunas circunstancias puede ser utilizado como una alternativa al dinero (ECB, 2015). Aunque esta definición ha cambiado con el paso del tiempo, más recientemente, la regulación MiCA dice que *“son representaciones digitales de valor o derechos que pueden transferirse y almacenarse electrónicamente, utilizando DLT o tecnología similar”*.
- Moneda basada en la criptografía. A diferencia de las monedas emitidas por bancos centrales, se generan con la resolución de problemas matemáticos basados en criptografía. Su valor está sujeto a variación de precios dependiendo de la oferta y demanda de los mercados<sup>6</sup>.

Describir Bitcoin es algo que puede resultar complejo (Gigi, 2019), puedes pensar en él como una red para enviar dinero de un lugar a otro, como una moneda o directamente como un mero contrato social automatizado. Por eso, antes de describirlo, nos vamos a centrar en su funcionamiento y en sus dos grandes características: Descentralización e Inmutabilidad.

### 2.1 Un sistema de efectivo electrónico peer-to-peer (P2P)

Una moneda electrónica se puede definir como una cadena de firmas digitales. Cada dueño transfiere la moneda al próximo al firmar digitalmente un hash<sup>7</sup> de la transacción previa y la clave pública del próximo dueño y agregando estos al final de la moneda. Un beneficiario puede verificar las firmas para verificar la cadena de propiedad (Nakamoto, 2008).

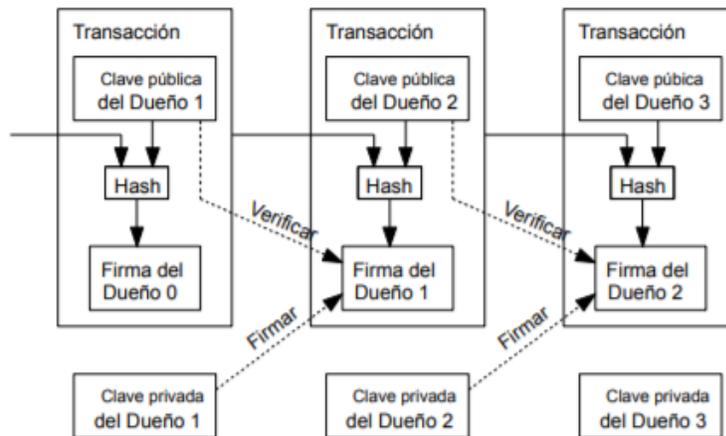
Es una red entre pares (P2P) en la que todos los miembros comparten los mismos derechos y obligaciones por lo que la red está descentralizada y por tanto no dependa de un servidor central que imponga las reglas del juego.

---

<sup>6</sup> <https://www.criptonoticias.com/criptopedia/glosario/>

<sup>7</sup> La función hash permite tomar cualquier flujo de datos como entrada y transformarlo en una cadena de longitud fija mediante una función matemática no reversible. Permite identificar un conjunto de datos públicamente sin revelar nada de los mismos.

Ilustración 9 Esquema de una transacción en Bitcoin. Fuente: Nakamoto, 2008.



El problema que tiene esto es que no se puede hacer la verificación de que el dueño no haya hecho un doble gasto. Los objetos digitales no son escasos y por tanto se pueden reproducir hasta el infinito.

Pensemos en un archivo que enviamos por correo electrónico. El archivo no desaparece en el momento que nosotros los enviamos, sino que se crea una nueva copia que será enviada mientras nosotros tenemos la nuestra en el ordenador.

Lo que provoca eso es que para los pagos que no sean en metálico, requieran de la necesidad de un tercero de confianza (Bancos) que se encarga de la transferencia monetaria entre el emisor del dinero y el receptor.

El gran inconveniente que tiene este sistema es la obligatoriedad de tener que confiar en un tercero de confianza que puede verse comprometido en algún momento, o tener que rendir cuentas antes los reguladores del país en el que opera poniendo así en peligro la privacidad de la transacción.

Si a esto le añadimos los costes en comisiones y tiempo de espera en la transacción, nos queda un sistema muy ineficiente e impropio del año 2021, caracterizado por una tecnología avanzada que posibilita un mundo globalizado donde dos personas pueden conectarse entre sí al instante sin importar el lugar donde se encuentren.

Bitcoin elimina los inconvenientes de este sistema al ser el primer objeto digital limitado de manera verificable. Gracias a eso, las ventajas de los pagos en metálico (falta de intermediarios e irrevocabilidad de las transacciones) pueden trasladarse al mundo digital (Ammous, 2018).

Por tanto, una descentralización del sistema como la que hace Bitcoin, resuelve tres problemas al que se enfrenta un sistema centralizado como son: Un sistema dependiente de un único punto (y los peligros que conllevaría un fallo en ese punto), la exclusión de personas que no tienen acceso a cuentas bancarias y los altos costes de transacción y de tiempo que se producen en el sistema actual.

## 2.2 Prueba de trabajo

La prueba de trabajo de Bitcoin (PoW, por sus siglas en inglés) es el mecanismo que diseñó Satoshi Nakamoto para eliminar la necesidad de confiar en un tercero.

En el momento que se haga una transferencia desde una cuenta a otra, todos los miembros de la red pueden comprobarlo y posteriormente los nodos competirán por actualizar el libro de transacciones con la creación de un nuevo bloque, que será creado en media cada 10 minutos<sup>8</sup>.

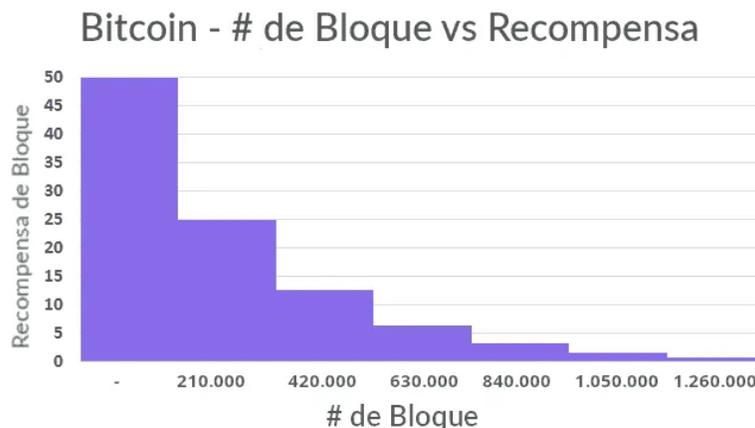
La forma que tienen los nodos para registrar las transacciones es a través de la poner a disposición de la red su ordenador (durante los primeros compases de la red) que se encarga de resolver complejos problemas matemáticos pero cuya verificación es sencilla<sup>9</sup>.

Una vez resuelto el problema matemático y validado por los otros nodos, tenemos un nuevo bloque y al nodo que lo ha hecho se le recompensa con las comisiones pagadas por los usuarios y con nuevos bitcoin que serán añadidos a la oferta monetaria (recompensa por bloque). Este proceso es conocido como minería, y a los nodos que compiten por registrar las transacciones se les conoce como mineros.

Durante los primeros cuatro años de existencia de la red, la recompensa era de 50 bitcoin. El 28 de noviembre de 2012 tuvo lugar la primera reducción a la mitad, cayendo la recompensa a 25 bitcoin por bloque. El 9 de julio de 2016 cayó a 12,5 y finalmente, el año pasado cayó a 6,25.

Esto se produce por **el proceso halving**, que reduce las recompensas a la mitad cada vez que se crean 210.000 bloques o lo que es lo mismo que aproximadamente unos 4 años.

*Ilustración 10 Evolución de las recompensas por bloques de Bitcoin. Fuente: Bit2me*



<sup>8</sup> Esto no significa que cada 10 minutos exista un nuevo bloque, puede ser que uno tarde 15 minutos en producirse y otros 5, pero en media estos bloques tardan unos 10 minutos.

<sup>9</sup> Hablaremos más Adelante acerca de cómo esta sencilla verificación elimina los incentivos perversos de incluir transacciones fraudulentas en la red.

Satoshi Nakamoto explicó en su *paper* que “Esta adición estable de una cantidad constante de monedas nuevas es análoga a mineros de oro gastando recursos para agregar oro a la circulación. En nuestro caso, es el tiempo del CPU y la electricidad que se gasta” (Nakamoto, 2008).

Estas recompensas por bloques también constituyen un incentivo positivo para los nodos que tengan capacidad de potencia de CPU superior al resto para que encuentre más rentable jugar con las reglas recibiendo una cantidad de monedas superior al resto a que no defraudar a través de transacciones fraudulentas.

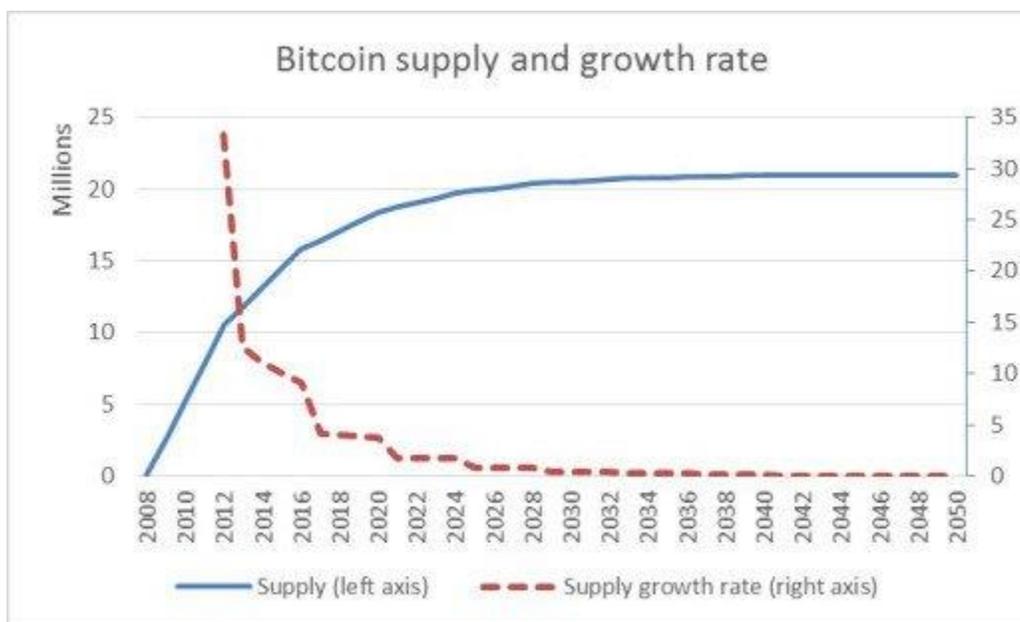
De acuerdo con esta programación, la cantidad total de bitcoin que se emitirán está fija en los 21 millones al que se irá acercándose de forma asintótica, estimándose que los últimos sean en el año 2140 (Ammous, 2018).

En las siguientes imágenes podemos observar el desglose de todos los *halving* y la oferta comparada con su tasa de crecimiento.

Ilustración 11 Desglose de todas las recompensas por bloque de la red. Fuente: Bit2me.

Bloque	Era recompensa	BTC/bloque	BTC Inicio	BTC añadido	BTC Finales	Incremento BTC	% BTC del límite en circulación
0	1	50,00000000	0,00000000	10,500,000,000000	10,500,000,000000	Infinito	50,00000006%
210000	2	25,00000000	10,500,000,000000	5,250,000,000000	15,750,000,000000	50,00000000%	75,00000008%
420000	3	12,50000000	15,750,000,000000	2,625,000,000000	18,375,000,000000	16,66666667%	87,50000010%
630000	4	6,25000000	18,375,000,000000	1,312,500,000000	19,687,500,000000	71,42857140%	93,75000010%
840000	5	3,12500000	19,687,500,000000	656,250,000000	20,343,750,000000	33,33333330%	96,87500011%
1050000	6	1,56250000	20,343,750,000000	328,125,000000	20,671,875,000000	16,12903230%	98,43750011%
1260000	7	0,78125000	20,671,875,000000	164,062,500000	20,835,937,500000	0,79365079%	99,21875011%
1470000	8	0,39062500	20,835,937,500000	82,031,250000	20,917,968,750000	0,39370079%	99,60937511%
1680000	9	0,19531250	20,917,968,750000	41,015,625000	20,958,984,375000	0,19607843%	99,80468761%
1890000	10	0,09765625	20,958,984,375000	20,507,812500	20,979,492,187500	0,09784736%	99,90234386%
2100000	11	0,04882812	20,979,492,187500	10,253,905200	20,989,746,092700	0,04887585%	99,95117198%
2310000	12	0,02441406	20,989,746,092700	5,126,952600	20,994,873,045300	0,02442599%	99,97558604%
2520000	13	0,01220703	20,994,873,045300	2,563,476300	20,997,436,521600	0,01221001%	99,98779307%
2730000	14	0,00610351	20,997,436,521600	1,281,737100	20,998,718,258700	0,00610426%	99,99389658%
2940000	15	0,00305175	20,998,718,258700	640,867500	20,999,359,126200	0,00305194%	99,99694833%
3150000	16	0,00152587	20,999,359,126200	320,432700	20,999,679,558900	0,00152592%	99,99847420%
3360000	17	0,00076293	20,999,679,558900	160,215300	20,999,839,774200	0,00076294%	99,99923713%
3570000	18	0,00038146	20,999,839,774200	80,106600	20,999,919,880800	0,00038146%	99,99961859%
3780000	19	0,00019073	20,999,919,880800	40,053300	20,999,959,934100	0,00019073%	99,99980932%
3990000	20	0,00009536	20,999,959,934100	20,025600	20,999,979,959700	0,00009536%	99,99990468%
4200000	21	0,00004768	20,999,979,959700	10,012800	20,999,989,972500	0,00004768%	99,99995236%
4410000	22	0,00002384	20,999,989,972500	5,006400	20,999,994,978900	0,00002384%	99,99997620%
4620000	23	0,00001192	20,999,994,978900	2,503200	20,999,997,482100	0,00001192%	99,99998812%
4830000	24	0,00000596	20,999,997,482100	1,251600	20,999,998,733700	0,00000596%	99,99999408%
5040000	25	0,00000298	20,999,998,733700	0,625800	20,999,999,359500	0,00000298%	99,99999706%
5250000	26	0,00000149	20,999,999,359500	0,312900	20,999,999,672400	0,00000149%	99,99999855%
5460000	27	0,00000074	20,999,999,672400	0,155400	20,999,999,827800	0,00000074%	99,99999929%
5670000	28	0,00000037	20,999,999,827800	0,077700	20,999,999,905500	0,00000037%	99,99999966%
5880000	29	0,00000018	20,999,999,905500	0,037800	20,999,999,943300	0,00000018%	99,99999984%
6090000	30	0,00000009	20,999,999,943300	0,018900	20,999,999,962200	0,00000009%	99,99999993%
6300000	31	0,00000004	20,999,999,962200	0,008400	20,999,999,970600	0,00000004%	99,99999997%
6510000	32	0,00000002	20,999,999,970600	0,004200	20,999,999,974800	0,00000002%	99,99999999%
6720000	33	0,00000001	20,999,999,974800	0,002100	20,999,999,976900	0,00000001%	100,00000000%
6930000	34	0,00000000	20,999,999,976900	0,000000	20,999,999,976900	0,00000000%	100,00000000%

Ilustración 12 Oferta de bitcoin y tasa de crecimiento.



Cada uno de los bitcoin que componen la oferta monetaria, está dividido a su vez en 100 millones de satoshis<sup>10</sup> que hace que pueda ser vendible en todas las escalas de la misma forma que con el patrón oro se usaban otros metales como la plata para hacer frente a pagos más pequeños.

### 2.3 Ajuste de dificultad

El ajuste de dificultad es el sistema que imposibilita que el aumento de valor de bitcoin produzca en los mineros un incentivo a instalar mayor capacidad de procesamiento y, con ello, a registrar bloques de forma más rápida recibiendo los bitcoin como recompensa y minándose así antes de tiempos los 21 millones.

De la misma forma que la fiebre del oro produjo que muchos ciudadanos de Estados Unidos lo dejaran todo para ir al oeste (más en concreto a California) a minar oro, que el precio de bitcoin aumente, incentiva a los nodos a poner a disposición de la red mayor procesamiento con el objetivo de hacerse antes que nadie con las recompensas. Si no se modificase nada, esta mayor capacidad de procesamiento haría que se minasen los 21 millones de bitcoin antes del 2140.

Sin embargo, gracias al ajuste de dificultad este hecho no se puede producir. El ajuste de dificultad lo que hace es hacer cada vez más complejos los problemas matemáticos de modo que, aunque la capacidad de procesamiento haya aumentado, la dificultad en encontrar la solución también lo haya hecho y por tanto se siga manteniendo la media de producción de bloques en unos 10 minutos. Esta es una de las características más importantes de la red Bitcoin y que la diferencian de prácticamente todas las demás criptomonedas.

La capacidad de procesamiento ha aumentado tanto que hace años que dejó de ser posible minar bitcoin a través de una CPU y entraron en escena los Circuitos Integrados para Aplicaciones

<sup>10</sup> En este caso, el plural sí se puede escribir como satoshis.

Específicas (ASIC, por sus siglas en inglés). Estos equipos se volvieron los más comunes a la hora del minado.

Mientras el ajuste de dificultad hace aumentar la complejidad de los problemas y por tanto el coste de resolver la prueba de trabajo se dispara, **el coste de verificación se mantiene constantes en niveles muy próximos a cero.**

Esta asimetría entre el coste de resolver la prueba y de trabajo y el de verificación es lo que hace a la red tan segura. Para resolver la prueba de trabajo, el coste (electricidad) para un nodo es creciente debido a la cantidad de nodos que están compitiendo por registrar las transacciones. Sin embargo, una vez el nodo completa el bloque el resto de nodos puede verificar que esas transacciones sean correctas de una forma muy sencilla y apenas sin coste, lo que provoca que el incentivo para registrar transacciones fraudulentas no existe, debido a que los nodos tendrían que asumir un gran coste mientras que la posterior verificación apenas lleva tiempo y su coste es cercano a cero, por lo que nadie va a desperdiciar sus recursos intentando añadir transacciones que no se correspondan con la realidad.

## **2.4 Tecnología *blockchain***

Mientras que en capítulos posteriores nos centraremos más en detalle en el motivo de por qué esta tecnología consigue el máximo de su eficacia en la red Bitcoin, ahora mismo nos centraremos en explicar en qué consiste la tecnología *blockchain*.

Se trata de una tecnología que posibilita el almacenamiento de forma creciente de datos ordenados en el tiempo sin posibilidad de modificación ni revisión y sin necesidad de una autoridad centralizada que garantice el correcto funcionamiento de la red (Domingo, 2019).

Su funcionamiento consiste en una cadena de bloques que tienen información codificada de una transacción en la red. El hecho de estar encadenados posibilita la transferencia de datos o valores con una codificación segura a través del uso de la criptografía (Molano, 2019).

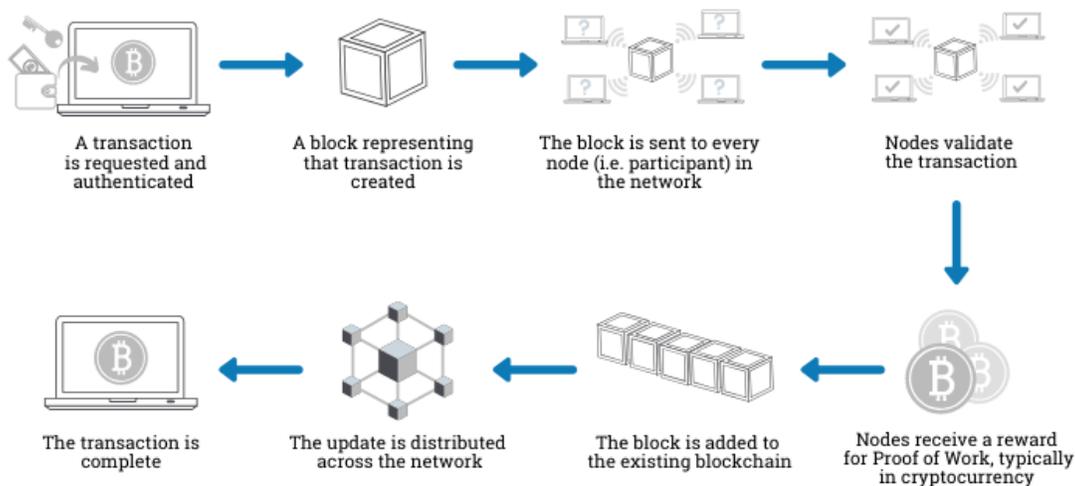
Podemos establecer una clasificación de *blockchain* en función de quién puede acceder a los datos (Bashir, 2017).

- *Blockchain* pública: Son redes de código abierto en las que cualquier persona puede participar. Bitcoin presenta una cadena de bloques de este estilo, donde cualquier usuario participa libremente en las transacciones y pueden verse recompensados por ello. Los libros de cuentas no pertenecen a nadie y cualquiera puede acceder a ellos libremente.
- *Blockchain* privada: Son redes cerradas donde no puedes participar si no eres un miembro de los que organizan esa cadena de bloques. En este caso si no eres miembro no tienes acceso al libro ni al historial. Por ejemplo, en la red bancaria, donde los miembros comparten el libro sólo entre ellos.

- *Blockchain* semi-privada: En este caso, tendríamos una mezcla de las dos anteriores, estando la privada en control de unos miembros y sin la posibilidad de acceder a esa información y la otra parte pública con información disponible para todos los usuarios.

Ilustración 13 Esquema de funcionamiento de Blockchain con bitcoin. Fuente: Euromoney

## How does a transaction get into the blockchain?



### 2.5 Función Hash

En este apartado vamos a analizar cómo la red se nutre de la función Hash para su correcto desempeño.

La función *hash* fue definida al principio del capítulo y consiste en que se pueda localizar un conjunto de datos de forma pública, pero sin revelar nada de esos datos.

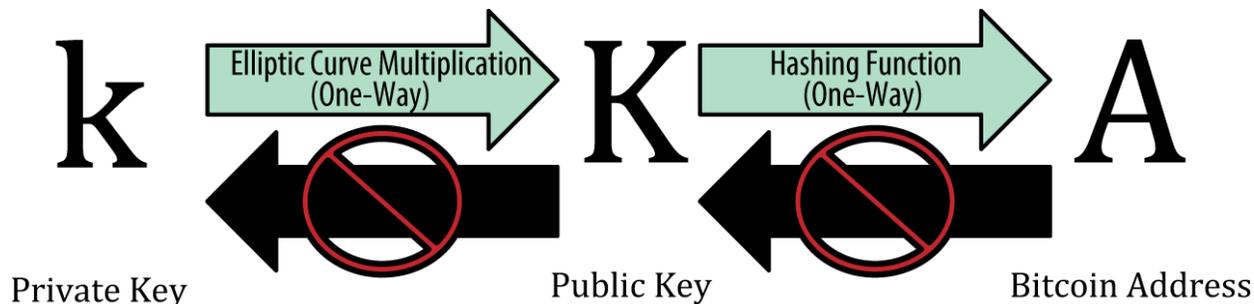
Las funciones *hash* son por tanto, unidireccionales y son muy fáciles de computar en una dirección pero no lo puedes hacer en dirección contraria. Por ejemplo, puedes preguntar a alguien el resultado de multiplicar los números 8 y 9 y la resolución te dará 72, en cambio si tienes el número 72 hay una infinidad de caminos para haber llegado a este número, haciéndose imposible el establecer el camino que ha conducido a ese resultado, esta es la base de la criptografía.

La criptografía hace que un ordenador no pueda revertir matemáticamente una operación y se usa en el mundo de las criptomonedas para resolver el dilema de los generales bizantinos. El problema de los generales bizantinos es el de distintas partes que no confían entre sí y hay que buscar una solución sin implantar un tercero de confianza (Domingo, 2019).

Lo primero que se produce es que se genera de forma aleatoria una llave privada que será la que de acceso a una persona a sus bitcoin. A partir de esa llave privada y mediante una multiplicación

de curva elíptica (una función criptográfica de un sentido) se genera una llave pública (Antonopoulos, Mastering Bitcoin, 2017). Desde la llave pública a partir de una función hash se genera una dirección.

*Ilustración 14 Relación entre la clave privada, clave pública y la dirección de Bitcoin. Fuente: O'Reilly.*



## 2.6 Actores principales

1. **Nodos:** Son los participantes de los equipos que constituyen la red de Bitcoin. Su objetivo es almacenar y distribuir copias actualizadas de las operaciones que se efectúan.
2. **Mineros:** Es un subgrupo dentro de los nodos, encargados de crear los bloques a través de poner a disposición de la red capacidad de procesamiento para resolver los problemas matemáticos
3. **Holders:** Inversores, propietarios o empresas que poseen bitcoin.
4. **Brokers** y casas de cambio: Son las compañías que ofrecen los servicios básicos de compra y venta de las criptomonedas y operan como plataformas para distintos tipos de servicios financieros relacionados con las criptomonedas.

## 2.7 ¿Cómo se hacen transacciones?

Ahora vamos a analizar cómo una persona puede transferir a otra sus bitcoin en lo que sería una transacción simple de compra de un bien o servicio.

Alguien puede conseguir bitcoin de diversas maneras:

- a. Ser pagado en bitcoin<sup>11</sup>.
- b. Comprarlos a través de dinero fiat: Ya sea en un cajero ATM, en una casa de cambio o adquiriéndoselo a un particular.
- c. Minería.

<sup>11</sup> En Estados Unidos se ha vuelto cada vez más común el número de empresas que ofrecen a sus empleados pagarles el salario en Bitcoin. Fuente: <https://www.bitwage.com/>

Una vez en posesión de la criptomoneda, para realizar una transacción se necesitan dos cosas, una dirección y una clave privada.

La propiedad de bitcoin se reconoce a través de claves, direcciones y firmas. Las claves van a posibilitar al usuario beneficiarse de los aspectos positivos de la red a través de confianza y control descentralizado, y el reconocimiento de la propiedad (Antonopoulos, Mastering Bitcoin, 2017).

Podemos hacer un símil con unas consignas del aeropuerto donde las propias consignas serían como la Red Bitcoin, la clave pública o dirección sería el número de taquilla y la clave privada sería la llave del dueño para poder abrirla.

Cuando una persona quiere enviar bitcoin a otra, utiliza su clave o claves privada/s para firmar cada una de las entradas de la transacción (el origen). Esto es realizado de forma transparente por el monedero, esa es su tarea.

Los bitcoin se almacenan en unos monederos virtuales (wallets) desde los que podremos enviar y recibirlos. Una vez creado el monedero para el usuario, la aplicación genera aleatoriamente una clave privada junto con la dirección Bitcoin del propietario.

Con la clave privada podrás acceder a tus bitcoin y la clave pública te identificará anónimamente, de una manera similar a tu correo electrónico (Domingo, 2019). La clave privada está compuesta de 77 dígitos y en el capítulo siguiente explicaremos las repercusiones que conlleva ese hecho.

Cuando una persona quiere enviar a otra cierta cantidad de bitcoin, lo que necesita saber es la clave pública de la persona que va a recibir el dinero. En la siguiente imagen podemos observar un ejemplo de como sería una dirección a través de un código QR.

*Ilustración 15 Ejemplo de una dirección pública de Bitcoin. Fuente: Bit2me*



Sin embargo, un concepto que necesita ser aclarado es el lugar donde están los bitcoin. No están en el monedero de los usuarios, sino que está en la red y su existencia desde el día de la emisión y todas las transacciones están replicadas en el libro mayor del que cada ordenador tiene una copia (Domingo, 2019).

Comentábamos anteriormente que para hacerse con la moneda una persona puede ir a casas de cambio y a un tipo de cambio (variará de una casa de cambio a otra) dependiente de la oferta y la demanda puede adquirirlo.

Ilustración 16 Mayores casas de cambio por volumen (en miles de millones de dólares. Fuente: Coinmarketcap.com

#	Nombre	Puntaje del exchange	Volumen (24h)	Liquidez prom.	Weekly Visits	# Mercados	# Monedas	Compatible con fiat
1	 Binance	9.9	\$56,589,448,727 ▼ 2.76%	663	34,690,815	1192	355	AED, ARS, AUD and +43 more
2	 Huobi Global	9.3	\$18,517,628,627 ▼ 26.03%	651	1,883,132	948	320	ALL, AUD, BRL and +47 more
3	 Coinbase Pro	8.7	\$5,463,840,940 ▼ 3.12%	509	5,263,535	171	57	USD, EUR, GBP
4	 Kraken	8.4	\$3,476,406,631 ▼ 6.92%	474	5,372,402	284	62	USD, EUR, GBP and +4 more
5	 KuCoin	8.2	\$2,752,219,340 ▼ 3.87%	416	1,268,622	686	300	TOKEN
6	 Bitfinex	8.2	\$2,001,680,931 ▼ 31.63%	454	1,080,043	301	132	USD, EUR, GBP and +1 more
7	 Bithumb	8.1	\$3,638,647,764 ▲ 0.64%	238	1,596,806	208	170	KRW
8	 Gate.io	7.9	\$1,402,372,359 ▼ 37.09%	407	832,673	1119	581	--

Si ahora nos centramos en que una persona quiere comprar un producto en un determinado establecimiento el procedimiento sería el siguiente:

Supongamos que un negocio acepte pagos tanto en la moneda local como con bitcoin, mientras que los precios están en términos de la moneda nacional, el comerciante puede, a través de un código QR publicar el listado de precios en bitcoin y la dirección del establecimiento. En el momento que un cliente escanee desde su móvil el código QR puede llevar a cabo la transacción con la misma rapidez con la que se haría un pago con tarjeta de crédito.

Para que entendamos el proceso de una manera sencilla podemos decir que al ordenar una transacción le estamos diciendo a la red que como propietario de cierta cantidad de bitcoin autorizamos la transferencia de algunos o todos esos bitcoin a otro propietario. Estas transacciones funcionan como un libro de contabilidad de doble entrada (Antonopoulos, Mastering Bitcoin, 2017).

Ilustración 17 Ejemplo de una transacción de bitcoin. Fuente: Mastering Bitcoin.

Transaction as Double-Entry Bookkeeping			
Inputs	Value	Outputs	Value
Input 1	0.10 BTC	Output 1	0.10 BTC
Input 2	0.20 BTC	Output 2	0.20 BTC
Input 3	0.10 BTC	Output 3	0.20 BTC
Input 4	0.15 BTC		
Total Inputs: 0.55 BTC		Total Outputs: 0.50 BTC	
	Inputs 0.55 BTC		Outputs 0.50 BTC
	-		Difference 0.05 BTC (implied transaction fee)

En la transacción hecha aparece el reconocimiento de propiedad de los bitcoin transferidos en forma de firma digital del titular, esto es validado por cualquier nodo de la red. Por lo que podemos decir que un gasto equivale a firmar una transacción cuyo valor es traspasado a un nuevo propietario identificado por su dirección. La transacción puede ser usada como entrada para una nueva, formándose de acuerdo a esto una cadena de propiedad a medida que el valor intercambiado varía de una transacción a otra, como se puede ver en la siguiente imagen (Antonopoulos, Mastering Bitcoin, 2017).

La diferencia entre una transacción válida en un registro centralizado de otra en un registro como Bitcoin es que el protocolo establece normas para llegar a un consenso sobre las actualizaciones del registro y su orden en lugar de un banco que ajuste saldos e informe a los vendedores de que se le ha pagado.

Ilustración 18 Diferencia entre registro centralizado y el registro en Bitcoin. Fuente: BIS



Ilustración 19 Cadena de transacciones en la red. Fuente: Mastering Bitcoin



En la imagen se puede observar que las transacciones forman una cadena, en la que las entradas de la última transacción equivalen a los *outputs* de transacciones anteriores. Es la clave del pagador (en la imagen Alice) la que desbloquea los *outputs* de las transacciones anteriores diciendo así a la red que es ella la legítima poseedora de esos fondos.

Cuando nosotros analizamos una transacción hecha en la red vamos a observar que el importe total pagado es superior con el precio del bien o servicio adquirido y esto es debido a las comisiones (bitcoin fees) a pagar para recompensa del minero que ejecute el bloque con esa transacción.

La comisión se puede modificar libremente con la intención de que tu transacción se ejecute de la forma más rápida. Si una persona decide añadir una alta comisión en su transacción, el minero tendrá incentivos para ejecutar primero esa transacción y por tanto se confirmará antes que el resto.

### 3. Críticas más comunes hacia Bitcoin

#### 1. Bitcoin no tiene ningún respaldo.

Esta puede que sea la crítica más común a la criptomoneda y se basa en que no hay nada detrás de Bitcoin que respalde el valor.

Sin embargo, este concepto de valor intrínseco no es más que un concepto ambiguo e indefinido fruto de escuelas de pensamiento económico que plantean una valoración objetiva, ignorando la realidad, en la que es cada ser humano quien otorga valor a algo de forma subjetiva, de forma que el valor no es una cualidad intrínseca de los bienes sino que es una cualidad que proviene de la relación de los bienes con la persona que los necesita (Menger, Principios de Economía Política, 1871).

Aunque es a Carl Menger al que se le considera el primero en recalcar de forma apropiada que el valor no es una cualidad intrínseca de los bienes, lo cierto es que, al igual que muchos de los teoremas fundamentales de la Escuela Austriaca de Economía, tiene su origen en los escolásticos de Salamanca (Huerta de Soto, 1998). Luis de Molina (1535-1601) ya puso de manifiesto que “no depende del atributo propio de los bienes ni de su propiedad intrínseca, sino que es el resultado del beneficio que deseen obtener los hombres y al mismo tiempo de la importancia que signifique para ellos este beneficio” (Schumpeter, 1954).

El oro ha tenido siempre una valoración superior sobre sus propiedades orfebres e industriales precisamente por el hecho de que la valoración subjetiva de los seres humanos que hacían de sus propiedades para mantener el valor y usarlo como medio de cambio.

Por lo apuntado anteriormente, no es posible determinar el valor intrínseco de Bitcoin, ya que es un concepto no aplicable al mundo real, donde las personas deban determinar si un determinado activo les brinda utilidad (a través de la satisfacción de necesidades) y por tanto sean esas mismas personas las que valoren el bien a través de la utilidad que este les proporciona (Menger, Principios de Economía Política, 1871).

En los capítulos anteriores estudiamos las funciones que debía tener un activo para ser utilizado como medio de cambio, así como el funcionamiento de la red de Bitcoin, y en capítulos posteriores analizaremos algunas de las empresas que decidieron incluir esta criptomoneda en sus balances como sustitutos o complemento del dinero fiat. Con esa información podemos afirmar que es considerado como un activo que cumple una función de depósito de valor a largo plazo y que esos mismos participantes consideran ajena a las monedas fiat convencionales cuya oferta desde 2008 se ha expandido de una manera sin precedentes.

Otra función que es generalmente valorada por los usuarios, es la red P2P descentralizada que funciona a través de los nodos y mineros, donde cualquier persona tiene libertad absoluta para acceder al registro de transacciones, enviar su dinero de forma instantánea a cualquier parte del mundo etc y que todo ello sea soportado a través de la Prueba de Trabajo que hace reflejar de forma fiel los movimientos que se producen diariamente en la red.

Otro apunte que se podría hacer sobre esta crítica es que es mayormente promulgada por reguladores y defensores del sistema monetaria existente en la actualidad. Sin embargo, lo único que respalda a las monedas nacionales son las leyes de curso legal o forzoso. Muchos economistas argumentan que el respaldo de las monedas proviene de las economías nacionales que las respaldan. No obstante, una economía sólida que presencia un aumento de la masa monetaria sin previo aumento del ahorro verá la estructura de etapas productivas alterada de forma artificial originando ciclos de auge y recesión que pueden dañar tanto a la moneda en cuestión (por depreciación) como a la economía por las malas inversiones realizadas fruto de políticas monetarias expansivas (Huerta de Soto, 1998).

## 2. Bitcoin será prohibido si las autoridades lo desean.

Esta crítica se ha acentuado últimamente y la India ha sido el primer país que se ha propuesto multar a aquellos usuarios que tengan bitcoin<sup>12</sup>. No obstante, desde hace años ha habido muchos países en los que las autoridades se han mostrado deseosas de poner fin al uso de criptomonedas con el fin de que la única alternativa que tengan sus ciudadanos sea usar sus monedas nacionales.

El hecho de que ninguna autoridad por el momento haya logrado de forma efectiva poder prohibir la tenencia, minería e intercambio de bitcoin debería hacernos una idea de lo tremendamente dificultoso que es el hecho de lograrlo.

Es más, la misma India ya intentó algo parecido en el siglo pasado con unas consecuencias nefastas. En las décadas de 1970 y 1980, en el apogeo de lo que se conocía como la Licencia Raj, los indios solo podían tener divisas para un propósito específico y con un permiso del banco central. Si un empresario compraba divisas para pasar más de dos días en París y uno en Frankfurt, y en su lugar pasaba dos días en Alemania, el Banco de la Reserva de la India exigiría saber por qué se había desviado del permiso de divisas. Los infractores eran amenazados habitualmente con multas y penas de cárcel de hasta siete años. Surgió un mercado negro, con todos sus elementos desagradables, de divisas. El gobierno redobló sus esfuerzos y sometió a quienes trafican con divisas ilícitas a detención preventiva, generalmente reservada para terroristas. El sistema empobreció a los indios e hizo imposible que las empresas indias pudieran competir globalmente (Rajagopalan, 2021).

Debido a la naturaleza descentralizada de Bitcoin es muy difícil prohibir que los usuarios hagan transacciones en ella y abriría un debate acerca de su jurisdicción internacional. Dado que es una

---

<sup>12</sup> <https://www.reuters.com/article/uk-india-cryptocurrency-ban-idUSKBN2B60QP>

situación muy improbable el que todos los países se pongan de acuerdo para establecer las mismas leyes, se puede abrir la veda para que unos países aprovechen la oportunidad de atraer todos esos flujos al no establecer una prohibición sobre la criptomoneda.

Posteriormente a la India, el Banco Central de Turquía comunicaba, el 16 de abril de 2021, prohibía el uso de criptomonedas como medio de pago, bien sea directo o indirecto<sup>13</sup>.

Los volúmenes de transacciones con criptomonedas alcanzaron los 218000 millones de liras (unos 27000 millones de dólares) desde febrero a finales de marzo, lo que es más de 30 veces el volumen negociado el mismo periodo del año pasado.

Otro aspecto a tener en cuenta, es que la prohibición de la criptomoneda o una excesiva regulación por parte de países más desarrollados en cuanto a libertad económica y respeto a los derechos de propiedad (por ejemplo, Estados Unidos), es algo que cada vez puede resultar más difícil.

Ya hay muchas compañías cotizadas que tienen criptomonedas en sus balances<sup>14</sup>, al igual que inversores como Ray Dalio, Paul Tudor Jones, Stanley Druckenmiller e incluso senadores estadounidenses y gobernadores, los bancos pueden custodiar criptoactivos, empresas como PayPal o MasterCard lo han aceptado en sus plataformas etc.

En este punto, sería muy difícil prohibir el uso de las criptomonedas como medio de pago o establecer una regulación tan estricta que en la práctica desaparezcan los incentivos a usar esas monedas. Conforme pase el tiempo, cada vez más empresas se van uniendo al mundo de las criptomonedas y con ello aumentará la dificultad para penalizarlas o bloquearlas.

### 3. Bitcoin desperdicia electricidad.

Este es uno de los temas más controvertidos debido a que es cierto que el coste de electricidad para minar bitcoin ha crecido los últimos años y la red ya ha superado a países como Argentina en cuanto al consumo de electricidad<sup>15</sup>.

---

<sup>13</sup> <https://www.reuters.com/technology/turkey-bans-use-cryptocurrencies-payments-sends-bitcoin-down-2021-04-16/>

<sup>14</sup> <https://bitcointreasuries.org/>

<sup>15</sup> <https://www.bbc.com/news/technology-56012952>

Ilustración 20 Bitcoin: Consumo de electricidad estimado. Fuente: Universidad de Cambridge.

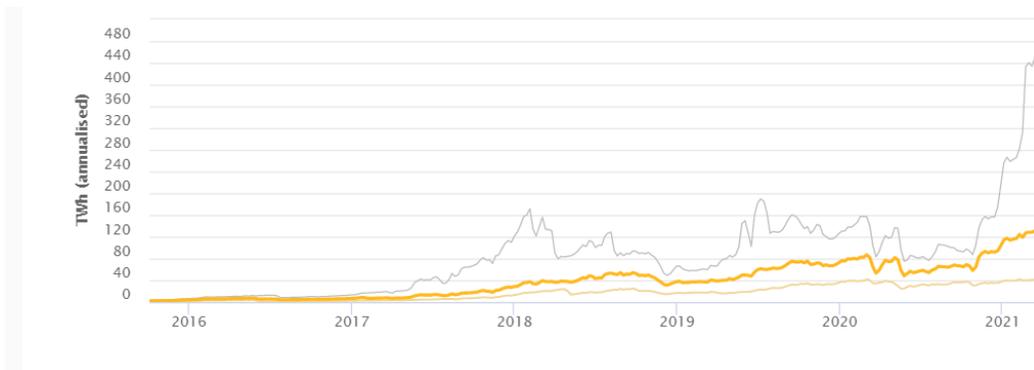


Ilustración 21 Consumo eléctrico de Bitcoin comparado con países. Fuente: Universidad de Cambridge.



Lo primero que tenemos que explicar es que, al llevarse a cabo una transacción libremente acordada entre dos partes, un tercero no puede ser quien valore la utilidad de dicha transacción en tanto en cuanto, esta únicamente compete a las partes que participan. En este caso, son los mineros de la red los que a través de sus decisiones de minar o no hacerlo en función de los costes de electricidad los únicos a los que compete el poder juzgar la utilidad de la transacción, siéndolo esta si finalmente deciden incurrir en esos costes o siendo un desperdicio en caso de que no quieran incurrir debido a que la recompensa obtenida (los bitcoin) no compensa los costes incurridos. La utilidad depende de la satisfacción que le otorga al agente, debido a la satisfacción de sus necesidades, ese agente acepta incurrir en un coste para poder acceder a un bien o servicio.

Al mismo tiempo, como explicamos anteriormente, una de las características fundamentales de la red es la prueba de trabajo y la asimetría existente entre los costes de verificación y los de resolución de los problemas matemáticos.

El aumento del coste de electricidad necesario para la resolución de complejos problemas y poder crear bloques lo que produce es una red mucho más segura que redundante en beneficio de todos los usuarios, por lo que no sería conveniente afirmar que la minería es un desperdicio de electricidad.

#### 4. Bitcoin es contaminante.

Cuando el pasado mes de mayo Elon Musk decidió suspender la posibilidad del uso de bitcoin como medio de pago para los coches Tesla, intensificó el debate acerca de las emisiones de CO<sub>2</sub> de la red Bitcoin debido a la minería.

El empresario, quiso dejar de aceptar bitcoin alegando que la contaminación de la red Bitcoin era un problema para el medio ambiente.

*Ilustración 22 Comunicado de Elon Musk en Twitter.*

Tesla has suspended vehicle purchases using Bitcoin. We are concerned about rapidly increasing use of fossil fuels for Bitcoin mining and transactions, especially coal, which has the worst emissions of any fuel.

Cryptocurrency is a good idea on many levels and we believe it has a promising future, but this cannot come at great cost to the environment.

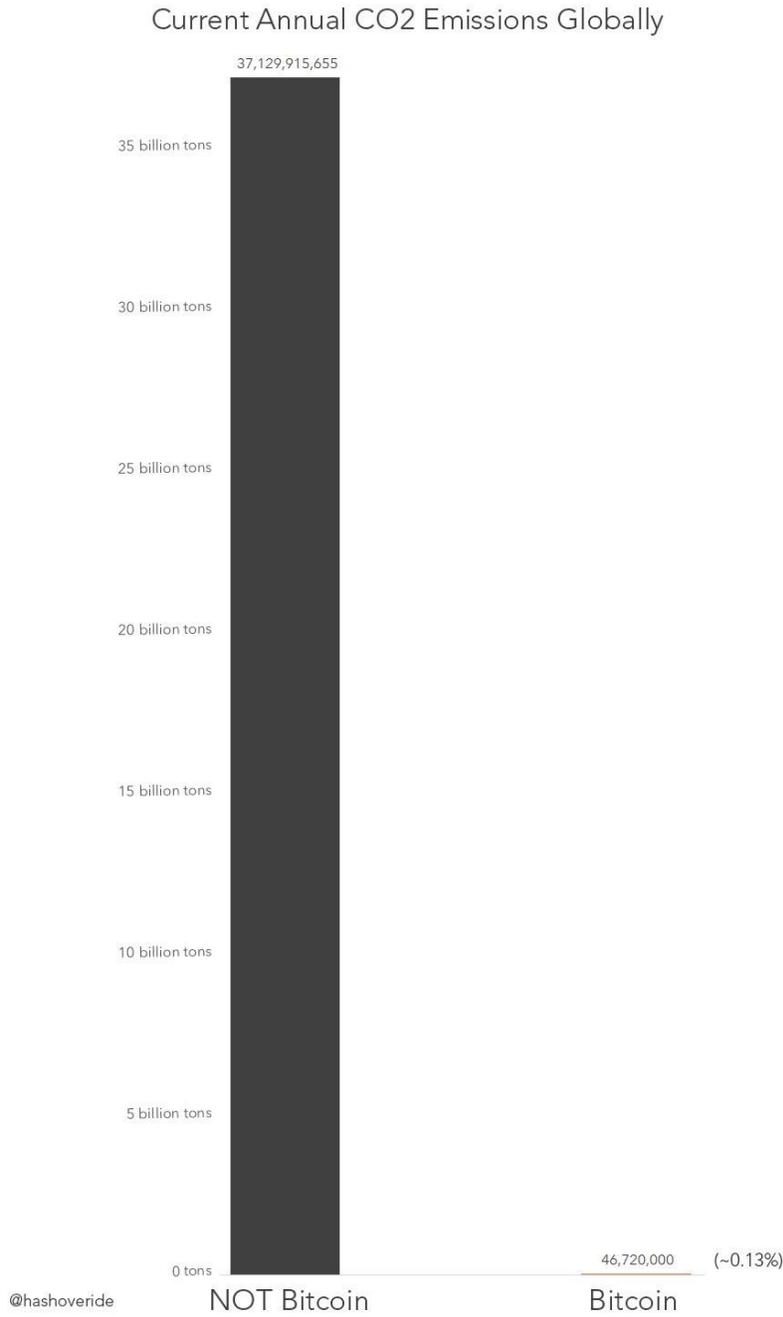
Tesla will not be selling any Bitcoin and we intend to use it for transactions as soon as mining transitions to more sustainable energy. We are also looking at other cryptocurrencies that use <1% of Bitcoin's energy/transaction.

En el siguiente gráfico podemos observar las emisiones de dióxido de carbono totales y las que son producidas por la red Bitcoin.

Podemos observar que aún está muy lejos de ser un problema en cuanto a las emisiones de CO<sub>2</sub> ya que a pesar de haber crecido de una manera sin precedentes el último año, la cantidad de emisiones que representa sobre el total no alcanza ni el 0,13%.

Es cierto que una parte de la minería usa como fuente de energía combustibles fósiles como el carbón (sobre todo los mineros de China), y lógicamente eso tiene un impacto en cuanto a emisiones de dióxido de carbono.

Ilustración 23 Comparación emisiones de CO2 totales y de Bitcoin. Fuente: Our World in Data



Aunque parte de la minería se haga usando carbón para generar electricidad, muchos mineros optan por usar energías renovables como fuente de energía para producir la electricidad necesaria para minar bitcoin.

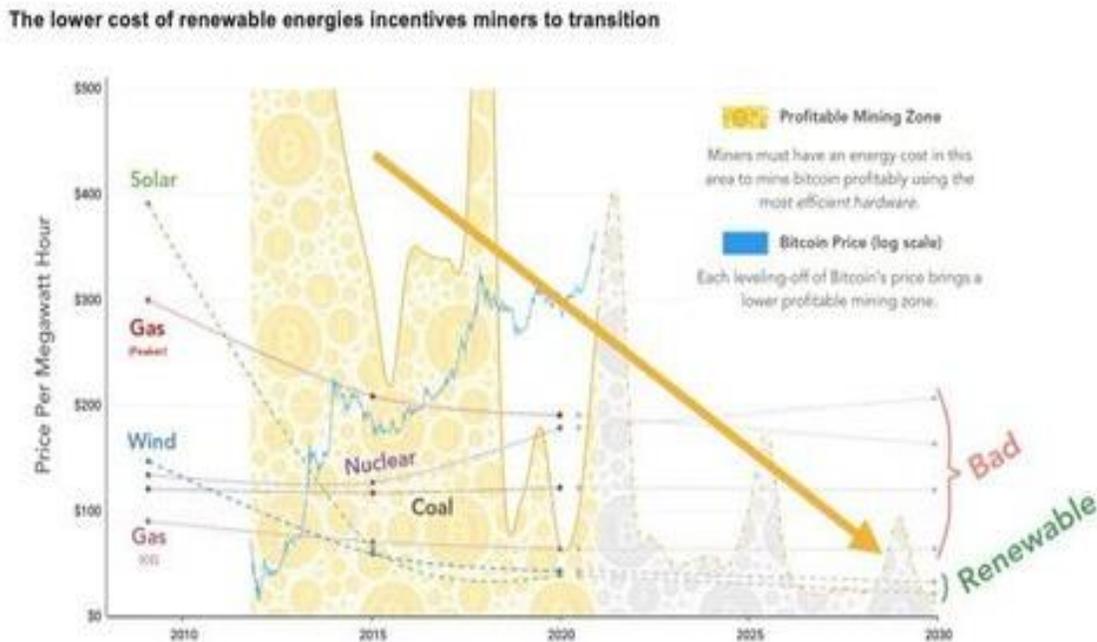
Un usuario puede minar bitcoin en cualquier parte del mundo, lo cual puede producir que los mineros tengan acceso a fuentes de energía que no están disponibles para otras aplicaciones,

como por ejemplo la energía hidroeléctrica. En regiones como Sichuan y Yunnan hay una enorme cantidad de esta energía disponible cada año mientras que su demanda apenas satisface una parte muy pequeña de esta energía y la capacidad de almacenamiento es muy limitada, convirtiendo estas regiones en el entorno ideal para minar bitcoin mediante una energía abundante, barata y renovable. Es por eso por lo que no debe sorprender que esas regiones sean de las más importantes del mundo en cuanto a minado, siendo el 10% en la época seca y el 50% en la época húmeda.

Algunas estimaciones llegan a situar en más de un 75% los mineros que usan energías limpias en sus actividades, si bien es cierto que el porcentaje total de consumo de energía de los mineros que proviene de estas energías es de un 40% (VanEck).

Si además observamos que las energías que en el futuro van a convertirse en las más baratas como la hidroeléctrica, solar y eólica y que, los mineros de bitcoin buscan las fuentes de energía más baratas, no nos debe extrañar que cada vez las emisiones de dióxido de carbono sean menores.

Ilustración 24 Evolución de las fuentes de energía buscada por los mineros. Fuente: VanEck



## 5. Bitcoin es demasiado volátil.

La volatilidad histórica de bitcoin ha sido muy alta para lo que se espera de un activo que pueda ser usado como medio de pago. Por este motivo, son estas altas variaciones en el precio uno de los mayores problemas que tiene actualmente.

A lo largo de su vida, la criptomoneda bitcoin ha experimentado grandes caídas y subidas respecto a otras monedas como el dólar que han provocado que sea vista como un activo con un riesgo muy grande.

Que la volatilidad sea tan alta afecta directamente a una de las propiedades básicas que debe tener un activo para ser considerado como medio de cambio: La función de unidad de cuenta.

Lo que sí es cierto es que es una tecnología que está en alza, con una oferta monetaria fija y apenas un ínfimo porcentaje de la población usando las criptomonedas, las enormes fluctuaciones de demanda son las que provocan movimientos tan bruscos en sus precios. En poco más de una década Bitcoin ha conseguido (En sus niveles máximos) una capitalización de mercado de más de un billón de dólares y ha conseguido ya ser una décima parte de la capitalización del oro y estar cerca de igualar la capitalización de la plata.

Un proceso de crecimiento tan rápido requiere de volatilidad y sobre todo una volatilidad al alza (upward volatility) que viene asociada con una volatilidad a la baja (downside volatility). Lo más seguro es que esa volatilidad le ayude a alcanzar un mayor tamaño en cuanto a capitalización de mercado y atraiga a un mayor número de usuarios.

A medida que crezca el número de usuarios y la demanda no se vea sometida a fluctuaciones tan agresivas la volatilidad de la moneda se irá reduciendo.

Hay una función, la más importante de Bitcoin, que para algunos tenedores no les afecta la alta volatilidad, y es la función de depósito de valor, eso se ha materializado en la popularización del "HODL" por parte de algunos de los mayores tenedores de la criptomoneda, que en la gran corrección vivida este año, siguen apostando por mantener sus bitcoin. Aunque se pueda confundir excesos de volatilidad con incapacidad para actuar de reserva de valor a largo plazo, esto realmente no es así al igual que por no ser volátil no tiene por qué ser un buen depósito de valor. Un ejemplo sería el dólar, que siendo un activo muy poco volátil, a lo largo del tiempo desde la creación de la Reserva Federal ha perdido más de un 99.5% de su poder adquisitivo.

Ilustración 25 Poder adquisitivo del dólar desde 1913. Fuente: Gold Telegraph.



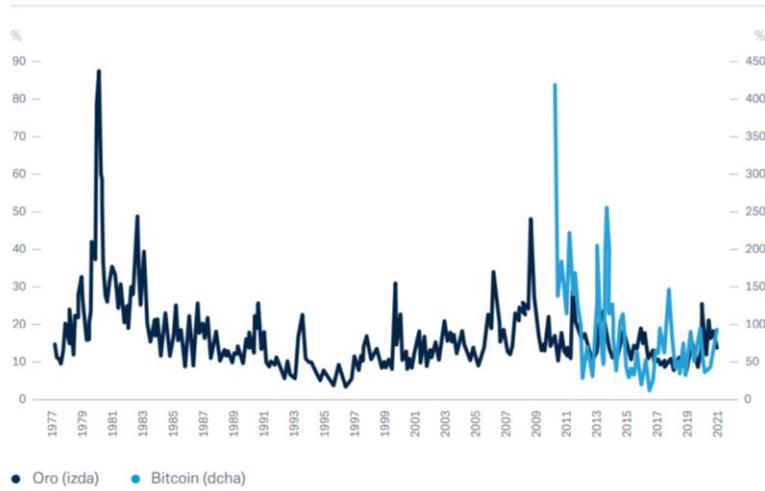
Aunque se puede argumentar que la destrucción del poder adquisitivo del dólar se ha producido a lo largo de los últimos 100 años pero que en el corto plazo se ha mantenido sin sobresaltos, no es menos cierto que, vivimos en un mundo en el que el dólar, el euro, la libra etc no están presentes en todos los países. Sesgados por la costumbre de tener monedas relativamente estables en los países occidentales, nos solemos olvidar de aquellos países en una situación económica peor, con autoridades monetarias y gubernamentales que llevan a cabo medidas económicas y monetarias que pueden dañar la economía y la moneda del país. Es muy larga la lista de países en los que, en algún momento de la historia reciente, ha destrozado el poder adquisitivo de su moneda en un corto periodo de tiempo. Es por eso por lo que Bitcoin, aun con sus enormes fluctuaciones, es muy valorado en países como Venezuela, Argentina, Turquía, Irán etc, todos ellos países que en los últimos tiempos han impreso tanta cantidad de dinero que la confianza en sus monedas nacionales se ha desplomado por completo.

Por poner un solo ejemplo, la lira turca se desplomó un 15% el día que Erdogan destituyó al presidente del Banco Central de Turquía<sup>16</sup>.

No obstante, la comparación que quizá fuese más adecuada para analizar la volatilidad de Bitcoin sería con el oro, dado que los partidarios de esta criptomoneda lo proclaman como el nuevo "oro digital". Como podemos ver en la siguiente imagen, ni siquiera el oro se ha librado de altos periodos de volatilidad.

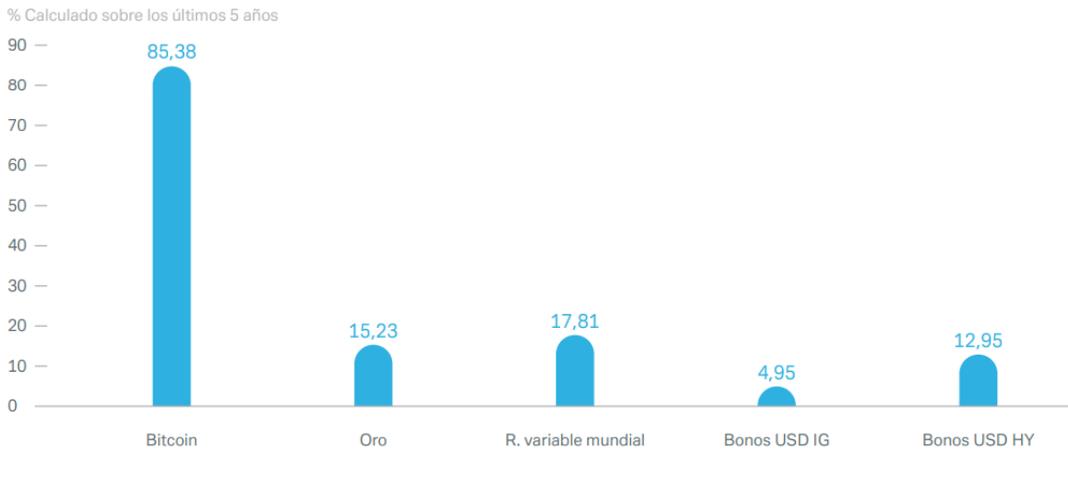
<sup>16</sup> <https://www.bbc.com/news/business-56479702>

Ilustración 26 Volatilidad histórica del oro y Bitcoin anualizadas en periodos de 60 días. Fuente: Deutsche Bank.



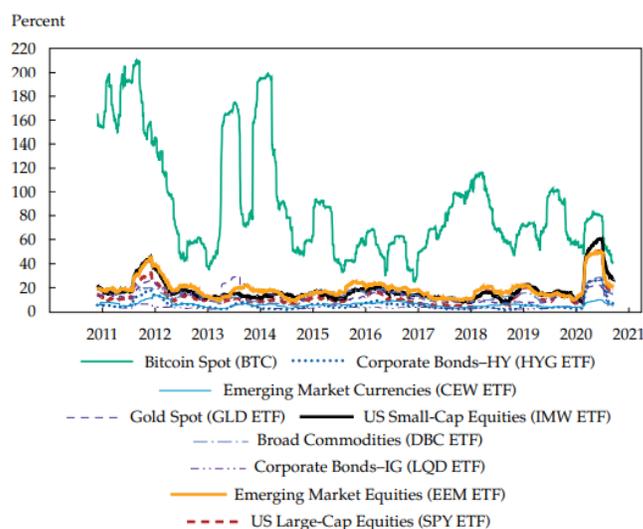
Aunque es cierto que la situación anterior no es la habitual y que Bitcoin es más volátil que el resto de activos tradicionales.

Ilustración 27 Volatilidad de Bitcoin y de otros activos tradicionales. Fuente: Deutsche Bank.



Si lo comparamos a través de las desviaciones estándar de 90 días sobre una base anual nos encontramos con lo siguiente (Hougan & Lawant, 2021)

Ilustración 28 Evolución de la volatilidad de 90 días de retornos anualizados de Bitcoin frente a activos tradicionales. Fuente: Hougan & Lawant.



## 6. Bitcoin es usado para actividades ilegales.

Es muy común relacionar Bitcoin con la Deep Web, el lugar de internet donde se pueden comprar productos generalmente ilegales ya sean sustancias estupefacientes o armas.

Las autoridades monetarias advierten que no está claro que las criptomonedas tengan un estatus legal absoluto y que los actores clave no están regulados o supervisados y están expuestos a los riesgos que la regulación generalmente mitiga (ECB, 2015).

Sin embargo, se ha demostrado que pagar en bitcoin no otorga una privacidad absoluta a las partes y que la moneda deja un rastro digital que puede ser utilizado por las autoridades para localizar a los partícipes en la actividad ilícita.

Homeland Security Investigations e IRS-Criminal Investigations aplican unas técnicas para rastrear transacciones blockchain de Bitcoin con la implementación del software de análisis especializado desarrollado por Chainalysis, que ya les ha servido en otras ocasiones para acabar con negocios ilegales<sup>17</sup>.

Chainalysis proporciona mediante su software un estilo especializado de visualización de datos para el 'seguimiento del dinero' a través de transacciones de bitcoin, una técnica que emplean agencias gubernamentales, intercambios de criptomonedas e instituciones financieras tradicionales, la cual complementa y actúa en una función de soporte más que de arquitecto para resolver casos, tal como declaró su fundador Jonathan Levin<sup>18</sup>.

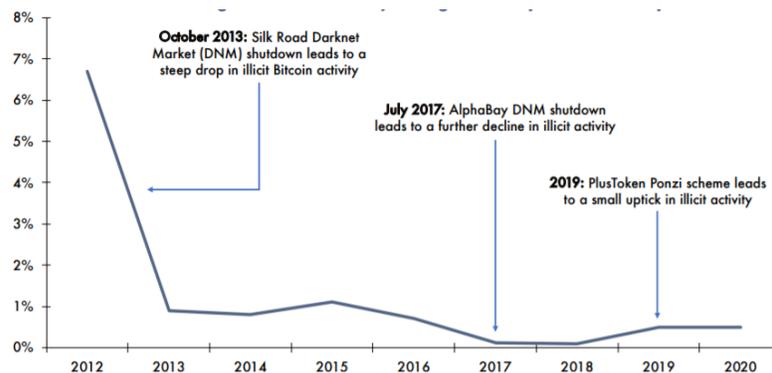
<sup>17</sup> <https://es.cointelegraph.com/news/us-authorities-analyze-bitcoin-transactions-to-shut-down-child-porn-ring>

<sup>18</sup> <https://blog.chainalysis.com/reports/chainalysis-doj-welcome-to-video-shutdown>

Por tanto se pueden establecer relaciones entre las direcciones de la red y la vida real y es complicado eliminar todo el rastro de fondos de una dirección Bitcoin y la estructura de la cadena de bloques de la red no es el sistema más adecuado para proteger la privacidad.

El propio informe de Chainalysis las actividades ilícitas pagadas con criptomonedas supone menos un 0.5% de la actividad total de las criptomonedas.

Ilustración 29 Porcentaje de actividades ilegales usando Bitcoin. Fuente: Chainalysis



En cambio, casi todas las estimaciones de actividades ilícitas en las economías a través del sistema financiero y las monedas tradicional varían entre un 2 y un 4 por ciento del producto interior bruto mundial (Morell, 2021).

Sí es cierto que, dentro de las criptomonedas, bitcoin es la más utilizada para este tipo de transacciones, pero sin embargo esto se debe a que Bitcoin representa el 60% del mercado de las criptomonedas, repartiéndose el otro 40% más de 4000 criptomonedas (Morell, 2021)

Existen muchos cuerpos que se dedican a la supervisión del uso de las criptomonedas, algunos ejemplos son:

- FATF: Esta institución, a diferencia de las tres siguientes que operan en Estados Unidos, es a nivel internacional y es un organismo de control contra el lavado de dinero y la financiación del terrorismo<sup>19</sup>
- FinCEN: Esta institución estadounidense contra los delitos financieros tiene como misión salvaguardar el sistema financiero evitando un uso ilícito, así como combatir el lavado de dinero y la recopilación, análisis y difusión de la inteligencia financiera<sup>20</sup>. Los administradores o cambistas deben registrarse ante FinCEN (Rosembuj).
- CFTC: La Commodity Futures Trading Commission se encarga de promover la integridad, resiliencia y transparencia de los mercados de derivados en Estados Unidos. Incorporamos esta institución porque fue quien, en 2015, consideró a Bitcoin como una *commodity*.

<sup>19</sup> <https://www.fatf-gafi.org/about/whoweare/>

<sup>20</sup> <https://www.fincen.gov/>

- OCC: La Office of the Comptroller of the Currency es responsable de la supervisión de bancos nacionales en Estados Unidos. Vigila porque se provea libre acceso a servicios financieros, se trate a los clientes de una manera justa y se cumpla la ley y las regulaciones.

## 7. Te pueden robar tus claves del monedero.

Debido al hecho de que la clave privada sea la llave que da acceso a los bitcoin que almacena una persona, se ha puesto de manifiesto el peligro que podría conllevar el que toda la riqueza de una persona almacenada en la red pudiera estar en peligro si se comprometiese la clave privada del poseedor de los bitcoin.

La clave privada consiste en 256 bits o lo que es lo mismo 77 dígitos. Las posibles combinaciones para encontrar la combinación correcta de una clave privada son prácticamente ilimitadas. Son cifras que ni siquiera pueden ser reproducidas de forma fiel por nuestro cerebro por no tener un equivalente en el mundo físico y ser más propias del mundo de la cosmología (Antonopoulos, Bitcoin explicado en el taller de conceptos básicos de Bitcoin CBP Prep).

10 elevado a 77 es un número tan alto que para hacernos una idea lo podríamos comparar con el número de átomos del universo visible, que está estimado en 10 elevado a 80 átomos.

De hecho, constituiría un riesgo mayor el hecho de perder las claves y no poder recuperar el dinero que a que te las puedan robar. Para evitar el primer escenario, es conveniente que el usuario establezca alguna medida previsoras frente a la pérdida de las claves, de forma similar al que hace una copia de las llaves de su casa por si en algún momento pierde estas.

## 8. Bitcoin puede ser hackeado.

Muy a menudo se puede leer acerca del posible hackeo que puede tener la red por parte de un atacante que tuviera el objetivo de robar, efectuar transacciones falsas, modificar la red o simplemente destruirla. No obstante, vamos a analizar por qué la sencillez y simplicidad de la red y su descentralización hacen garantizar su seguridad.

El hecho de que sea mucho más difícil atacar Bitcoin que cualquier red centralizada, es que no hay servidores centrales de los que dependa la red, si no fuera así, bastaría con dañar esos servidores centrales para poner en jaque a todo el sistema.

Manipular las transacciones para robar dinero no tiene cabida en la red debido a que, como explicamos en el capítulo pasado, el resto de nodos de la red tiene que verificar las transacciones y esto no les supone ningún coste. Podría pensarse en qué pasaría si los nodos de repente sí las aceptaran, pero esto sería una contradicción, pues aceptar una transacción fraudulenta

equivaldría a socavar la confianza en la red Bitcoin y tanto ella como la moneda se hundirían haciendo que los nodos perdieran la riqueza que tenían acumulada en la criptomoneda.

El escenario en la que una mayoría socavase la integridad de la red, aceptando transacciones fraudulentas o ataques de doble gasto es lo que se ha conocido como el ataque del 51% (Ammous, 2018).

Sin embargo, es un escenario que parece muy improbable, en parte por la asimetría de costes de la prueba de trabajo y el coste de verificación y no menos importante, por la potencia de hash necesaria para llevar a cabo un acto así. Para conseguir tal potencia de *hash* se debería moviliza una ingente cantidad de recursos en equipo de minería de Bitcoin que elevaría su precio, compensando a los mineros actuales que podrían invertir una mayor cantidad de recursos en la minería, haciendo que la potencia de *hash* necesaria para poder modificar la red fuera aún mayor (Ammous, 2018).

Se acrecentaron las dudas por los ataques que sufrió una casa de cambio llamada MtGox, esta no ha sido la única, pues otras como Bitfinex por ejemplo, fueron atacadas. Sin embargo, esto corresponde más a aplicaciones que se crean por encima, sin haberse desarrollado de forma segura (Domingo, 2019).

#### 4. Evolución de Bitcoin: Desde 2008 hasta hoy

En la primera emisión de la moneda, Satoshi Nakamoto incluyó en el mensaje una portada del diario The Times en el que se informaba de que el gobierno británico estaba dispuesto a hacer un segundo rescate bancario.

*Ilustración 30 Portada incluida en la primera emisión de bitcoin.*



Que fuese en 2008 el año que Nakamoto diseña su programa, indica la desconfianza que tenía hacia el sistema financiero orquestado por bancos centrales, capaces de imprimir cualquier cantidad de dinero sin ningún respaldo.

El plan iniciado por la Reserva Federal, liderada por Ben Bernanke, para rescatar el sistema bancario norteamericano suponía que la Fed estaba lista para inyectar en el mercado una enorme cantidad de dólares de nueva creación. Ese camino pronto sería copiado por la práctica totalidad de los países en dificultades que vieron en esa alternativa la solución para estabilizar sus economías.

El paper de Satoshi Nakamoto, de apenas nueve páginas, donde establecía un sistema de dinero digital y transacciones entre pares se llamaba “Bitcoin: A P2P Electronic Cash System” (Nakamoto, 2008).

Como puntualizábamos anteriormente, la gran revolución de este sistema era que por fin se lograba acabar con el problema del doble gasto (double-spend problema, en inglés) que era el conflicto fundamental de cualquier sistema de dinero electrónico (Domingo, 2019).

Para sistemas de dinero electrónico siempre se había necesitado de una tercera parte de confianza (ya fuese un banco o una empresa como Paypal) debido a que era quien se encargaba de vigilar que las personas no usasen dos veces el mismo dinero. Sin embargo, implicar a terceras partes generaba otros inconvenientes como encarecimiento de las transacciones o la lentitud de estas.

#### 4.1 Génesis, primera transferencia de dinero y las pizzas más caras de la historia.

En enero de 2009 Satoshi Nakamoto distribuyó al público la primera versión del software para crear un nodo de bitcoin y con ello se empezó a poder minar las criptomonedas.

Al primer bloque de la red se le dio el nombre de Génesis y fue minado por Satoshi Nakamoto siendo la cantidad de recompensa de 50 bitcoin (Domingo, 2019).

Una semana después, Hal Finney se convierte en el segundo minero de la red.

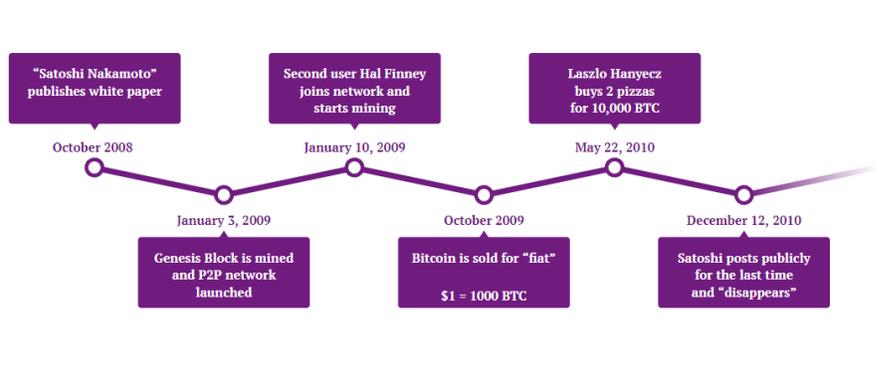
El primer intercambio que se produce entre una moneda fiat (en este caso eran dólares estadounidenses) y bitcoin se hizo en una casa de cambio llamada New Liberty Standard que compró a un miembro de la red 5050 bitcoin por 5,02 dólares siendo el primer tipo de cambio oficial de la historia cerca de mil bitcoin por cada dólar (Domingo, 2019).

Es el 22 de mayo de 2010 cuando se efectúa la primera compra de un producto con bitcoin. Laszlo Hanyecz pasó a la historia cuando decidió pagar dos pizzas de 25 dólares con 10.000 bitcoin, convirtiéndose a día de hoy en las pizzas más caras de la historia.

En diciembre de 2010 Satoshi Nakamoto publica su último mensaje y ha permanecido desaparecido desde entonces. Aunque ha habido muchas acusaciones sobre quién era la persona detrás de esta red e incluso algunas personas se han autoproclamado ser tal, lo cierto es que aún no se ha podido demostrar de forma convincente quién o quiénes son las personas que hay bajo este seudónimo.

A modo de resumen, en la siguiente imagen podemos encontrar los acontecimientos más importantes que se produjeron en los primeros 22 meses de historia de la red.

Ilustración 31 Primeros años de historia de Bitcoin. Fuente: Andreas Antonopoulos.



#### 4.2 El Crash de 2018

Desde que Bitcoin alcanzase sus precios máximos históricos en 2017, desde finales de ese mismo año hasta diciembre de 2018 se produjo una caída muy brusca en el precio de la criptomoneda.

En un año el valor de la criptomoneda cayó cerca del 80% desde los casi 20.000 dólares a situarse por debajo de los 3.500<sup>21</sup>.

Esta subida tan repentina del precio se debía fundamentalmente en la fiebre especulativa que despertó entre los pequeños inversores (principalmente chinos)<sup>22</sup>, algo diferente a lo que ha ocurrido en 2020. Los pequeños inversores o los agentes que tienen motivos más puramente especulativos tienden a entrar en pánico más fácilmente y a reaccionar de una manera más brusca ante noticias negativas.

Uno de los principales motivos fueron las amenazas de las regulaciones de los gobiernos, primero fue Corea del Sur que afirmó haber comenzado a plantearse la prohibición de los portales de intercambio de criptomonedas. Posteriormente fue China la que se sumó a las amenazas de las regulaciones.

Curiosamente, son los mismos motivos por los que en mayo de 2021 las criptomonedas, y en particular Bitcoin, han vuelto a sufrir grandes caídas de precios.

Para muchos, aquella enorme caída acabaría por completo con el proyecto de la criptomoneda.

El hecho de que hubiera caído más de un 80% y que China anunciase severas regulaciones implicaría que tuviera los días contados. Sin embargo, en 2020 las criptomonedas en general y, Bitcoin en particular, vivirían algo totalmente diferente.

*Ilustración 32 Artículo de la revista Forbes en diciembre de 2018. Fuente: Forbes*



*Ilustración 33 Artículo de Financial Times en Abril de 2018. Fuente: Financial Times*



*Ilustración 34 Artículo de Bloomberg en marzo de 2018. Fuente: Bloomberg*

Economics

## **Bitcoin Is Worthless, Bubble May Pop Soon, Allianz Global Says**

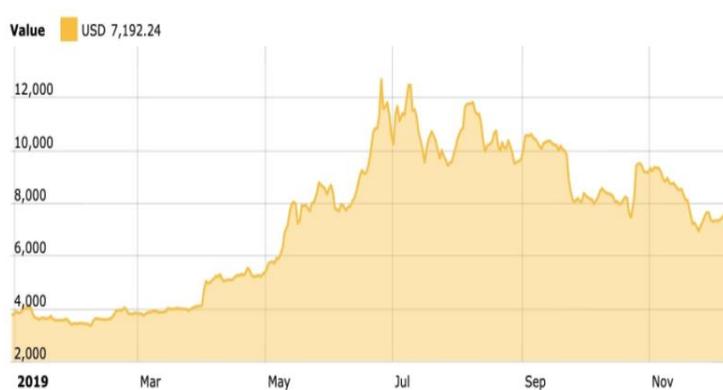
Con el comienzo de 2019, la criptomoneda empezó un nuevo rally la primera mitad de año, volviendo a superar los 10.000 dólares, cuando apenas unos meses antes, se le había dado por muerta. Sin embargo, el segundo semestre volvió a vivir una nueva bajada, aunque esta vez fue

<sup>21</sup> <https://www.bbc.com/mundo/noticias-46376535>

<sup>22</sup> <https://www.expansion.com/mercados/divisas/2020/11/19/5fb621ace5fdea7b2b8b459c.html>

más suave de lo que se produjo el año anterior y acabó por encima de los 7.000 dólares, un 80% superior a los niveles donde había empezado.

Ilustración 35 Evolución precio de bitcoin en 2019. Fuente: Cointelegraph.



### 4.3 Bitcoin: La revolución de las monedas digitales desde la crisis del Covid-19

Tras el desplome de Bitcoin a finales de 2018 y un año posterior donde apenas hubo modificaciones importantes de su precio toda la situación cambia a raíz de 2020.

Para hacer frente a la situación causada por el coronavirus donde la economía hacía frente a una situación muy preocupante, las autoridades monetarias inyectaron ingentes cantidades de dinero para dar un estímulo a la economía y que no se estancase del todo.

Aunque a corto plazo esto tiene un efecto positivo evidente, estas acciones tienen efectos negativos que se reflejan sino al instante, posteriormente. El efecto negativo más preocupante es la inflación, el hecho de que aumentar la liquidez de una forma tan agresiva en el sistema provocase subidas de precios tan elevadas que debilitase el poder adquisitivo de las monedas.

Así se reflejó en los datos de inflación en Estados Unidos el pasado mes de abril, donde la inflación subyacente MoM (Month over Month) alcanzó niveles nunca vistos desde 1981, por su parte la inflación subyacente anualizada alcanzaba más del 3% y la inflación anualizada llegó al 4,2% el mayor nivel desde Septiembre de 2008.

Ilustración 36 Datos mensuales de inflación en EEUU. Fuente: Bloomberg.



Es entonces cuando algunos agentes económicos empiezan a optar por adquirir metales preciosos como el oro, o criptomonedas como el bitcoin, con la intención de intentar salvaguardar el poder adquisitivo de su dinero.

Desde abril de 2020 se produjo una evolución alcista del precio del bitcoin sin precedentes, superando el nivel máximo histórico de 17000 dólares que se alcanzó en 2017 hasta alcanzar los más de 60.000 dólares en marzo de 2021.

No obstante, no fue bitcoin la única criptomoneda que vio subir sus precios durante la pandemia. En el mercado se ha observado el último año una auténtica revolución de las criptomonedas, haciendo posiblemente uno de los temas más controvertidos en el mundo económico. Muchas criptomonedas han alcanzado máximos históricos en sus precios (Ether, XRP, Dogecoin, etc) cuando muchas de ellas ni siquiera eran conocidas por la mayoría de los intervinientes en los mercados. Más concretamente, el Dogecoin, fue una criptomoneda surgida de lo que hoy en día llamamos un “meme” lo que refleja que el aumento de valor de las criptomonedas no se ha producido únicamente como motivo de atesoramiento a largo plazo, sino que en parte ha venido provocado por motivos especulativos.

Con la revolución de las criptomonedas, algunos inversores institucionales se empezaron a plantear la idea de incluir estos activos digitales en sus inversiones (Deutsche Bank, 2021). Este interés ha ido en aumento a medida que crecía la oferta de nuevos vehículos de inversión (carteras a futuros, ETF's, etc.) y ese aumento de nuevos productos que atraigan inversores institucionales y minoristas podría diversificar el mercado.

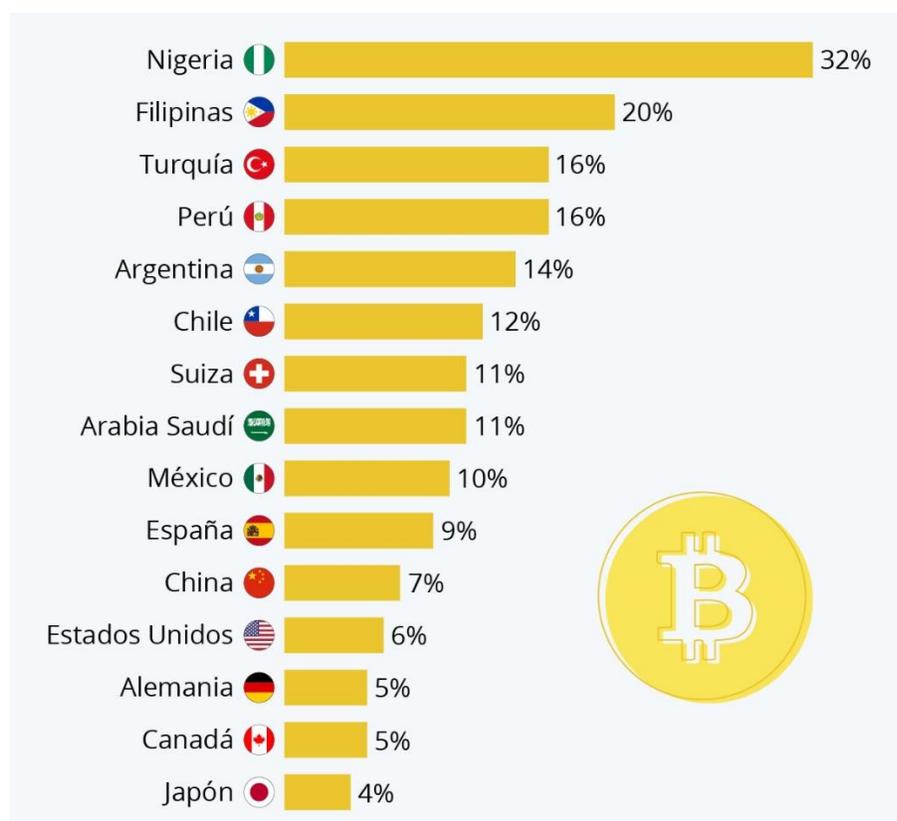
Las transacciones diarias que se hacen hoy en Bitcoin siguen estando muy por debajo de las que se hacen, por ejemplo, con el oro y otras materias primas.

Ilustración 37 Volumen de transacciones diarias de Bitcoin y otras materias primas. Fuente: Deutsche Bank.



Es importante que hablemos de la importancia relativa que tiene en cada país Bitcoin, en la siguiente imagen podemos observar una encuesta que realizó Statista a una muestra de ciudadanos de distintos países en los que se les preguntaba si tenían bitcoin.

Ilustración 38 Porcentaje de encuestados que afirma tener o usar criptomonedas. Fuente: Statista.



No es de extrañar que países como Turquía, Filipinas y Nigeria ocupen los escalones del podio. Como comentamos anteriormente, los aspectos más positivos de Bitcoin tienen más importancia en territorios con poco respeto por los derechos de propiedad y donde la libertad económica es muy baja, que suelen venir acompañados de monedas débiles frutos de las acciones de gobiernos menos autoritarios, que menoscaban la confianza e integridad de sus bancos centrales al hacerlos completamente dependientes de sus intereses.

En síntesis, la evolución del precio del bitcoin desde su creación hasta romper la barrera de los 60000 dólares ha seguido esta evolución.

Ilustración 39 Evolución precio de bitcoin desde su creación. Fuente: Deutsche Bank.



Si separamos los resultados por los retornos trimestrales nos encontramos lo siguiente

Tabla 2 Retornos trimestrales y anuales (en porcentaje) de Bitcoin desde 2010. Fuente: Bitwise Asset Management.

Año	T1	T2	T3	T4	A final de año
2010			25.03	384.65	505.94
2011	161.54	1952.74	-68.08	-8.16	1473.76
2012	4.03	36.53	84.59	9.12	186.08
2013	604.58	2.23	43.02	447.24	5537.40
2014	-40.31	41.03	-39.58	-16.92	-57.74
2015	-24	7.55	-10.18	82.17	33.74
2016	-3.33	61.73	-9.25	58.44	124.81
2017	11.48	127.63	77.29	222.1	1349.04
2018	-50.67	-7.69	3.40	-44.17	-73.71
2019	11.4	174.4	-26.28	-13.74	93.95
2020	-9.36	41.12	17.21		49.93

#### 4.4 Elon Musk inicia la caída de 2021

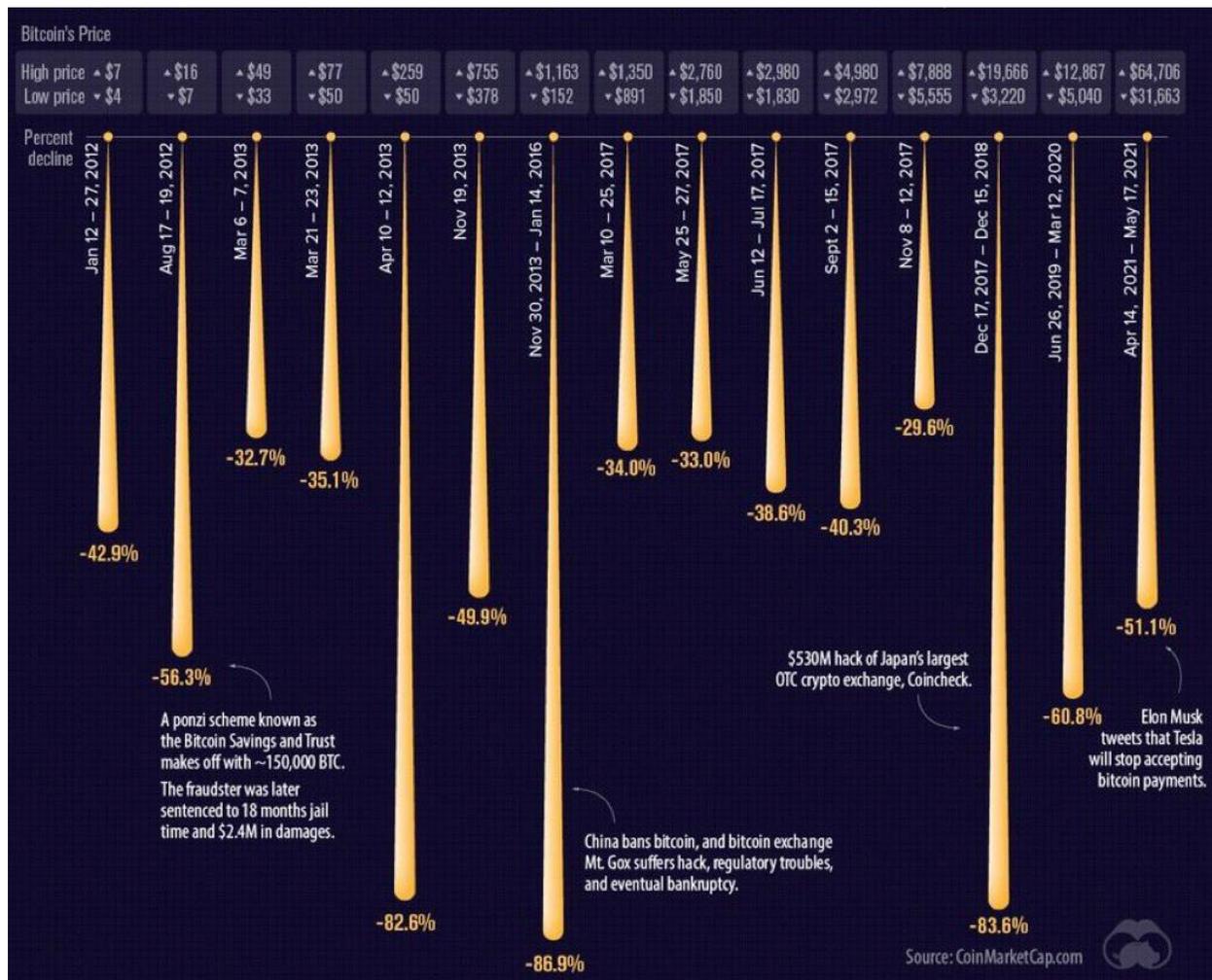
Anteriormente, se mencionó el anuncio del empresario norteamericano Elon Musk, en el que Tesla dejaría de aceptar bitcoin como medio de pago. Seguido a esto, la criptomoneda entró en una dinámica bajista muy pronunciada.

Seguido del efecto Musk, China anunció la prohibición a sus instituciones financieras, este anuncio vino acompañado de nuevas bajadas en su precio, que alcanzó un máximo de casi 65000 dólares hasta llegar a perder los 40.000 dólares a finales de mayo de 2021.

Esta corrección iniciada por Elon Musk ha vuelto a poner a Bitcoin en el punto de mira por parte de muchos miembros del mercado. Se volvieron a repetir los mismos argumentos que en 2018<sup>23</sup>.

Aunque es una gran caída, lo cierto es que la criptomoneda ha atravesado por correcciones incluso mayores y conviene poner en perspectiva estas.

Ilustración 40 Correcciones históricas de Bitcoin. Fuente: CoinMarketCap.com



<sup>23</sup> <https://www.bitcoinisdead.org/>

#### 4.5 ¿Cumple Bitcoin las propiedades para ser una moneda?

Desde que Richard Nixon cerró la ventanilla del oro en 1971 provocando que las monedas nacionales pasaran a ser respaldadas por la confianza y no por un metal o bien físico, una parte de la academia económica, representada por economistas de la escuela austriaca, cuyo máximo exponente en aquel momento era F.A. Hayek (Premio Nobel de Economía en 1974) alertó de que el nuevo sistema monetario conduciría a la pérdida de una de las propiedades fundamentales del dinero: El depósito de valor.

Recordemos que las tres funciones fundamentales del dinero, como comentamos anteriormente, consistían en: Unidad de cuenta, medio de pago y depósito de valor.

- **Unidad de cuenta:** El hecho de poder cuantificar los bienes a través de unidades de dinero facilita la fijación de los distintos precios. Además de facilitar la fijación de precios de la economía en cuestión, disminuye los costes de transacción al eliminar el número de precios en los que están expresados los productos. Por ejemplo, si en una economía hay cuatro productos, A, B, C y D y ninguno realizara las funciones del dinero, tendríamos seis tasas diferentes (A:B, A:C, A:D, B:C, B:D y C:D). Si por el contrario, A fuese considerado como dinero, sólo necesitaríamos trabajar con tres tasas (A:B, A:C y A:D). Con esto llegamos a la conclusión de que si existen  $n$  productos, y no hay numerario, cada uno de los  $n$  productos tendría  $n-1$  precios, dando un total de  $n*(n-1)$  precios en la economía, en cambio si existiese el dinero, existirán  $n-1$  precios (Jimenez, 1994).
- **Medio de cambio:** La función que consiguió resolver el problema del trueque, el hecho de ser generalmente aceptado para poder intercambiar por bienes y servicios.
- **Depósito de valor:** Un dinero eficiente nos permitiría preservar nuestra riqueza a lo largo del tiempo en forma de este. Actualmente es lo que más puesto en duda está, pues, desde que las autoridades monetarias se libraron del corsé que el oro les suponía, tuvieron vía libre para aumentar la cantidad de dinero emitido y con ello la moneda ir perdiendo poder adquisitivo a lo largo del tiempo.

#### **Función de unidad de cuenta en Bitcoin**

Debido a la altísima volatilidad en comparación con las monedas tradicionales, esta función no la cumple Bitcoin por el momento.

En primer lugar, los bienes y servicios denominados en bitcoin suponen un porcentaje irrisorio sobre el total, por lo que aún tendría un largo recorrido por delante en este sentido.

Segundo que, las grandes fluctuaciones que tiene en su precio hace que sea muy ineficiente denominar el precio de los bienes y servicios en términos de esta criptomoneda, porque esas variaciones de precio provocarían el tener que estar ajustando constantemente los precios de los productos denominados así.

En último lugar, debido al encarecimiento que ha tenido Bitcoin el último año, en el caso de que siga progresando con el paso de los años y siga aumentando su valor, lo más seguro es que los precios no se denominen en unidades enteras de bitcoin, sino que se utilice una denominación menor como pueden ser los satoshis, con el objetivo de no comerciar los precios mediante unidades decimales de la criptomoneda.

Sin embargo, hay otros factores que no debemos pasar por alto. Por ejemplo, el sistema monetario de tipos de cambio flexibles y las fluctuaciones de unas divisas frente a otras, ha dificultado en parte el comercio internacional y los precios existentes, al no tener un tipo de cambio fijo se incorpora un riesgo que antes no estaba, a que el movimiento de una divisa frente a la otra pueda perjudicar los intereses económicos de una empresa.

El patrón oro resolvía este problema, precios conocidos y sin el riesgo de tipo de cambio de una moneda frente a la otra.

### **Función de medio de pago en bitcoin**

El nacimiento de Bitcoin supuso un mecanismo de pago tanto a nivel nacional como internacional alternativo a las monedas emitidas por los bancos centrales. Fue la primera moneda privada relativamente exitosa en ser aceptada como medio de pago por parte de algunos agentes económicos.

Bitcoin presenta una ventaja frente al oro ya que cualquier usuario puede enviar sus monedas a cualquier parte del mundo sin permiso de nadie y sin exponer su identidad (Ammous, 2018). Además resulta mucho menos costoso mover el dinero a través de las claves privadas que de provisiones físicas de oro.

También, se comentaron las ventajas frente al sistema tradicional, sobre todo a la hora de efectuar pagos y envíos de dinero internacionales. En el sistema tradicional, tienes que recurrir a algún tipo de entidad (generalmente bancos) y por tanto tener que pagar las comisiones que cobren. A eso se le une la lentitud del envío hasta que el dinero llegue finalmente al receptor, además del peligro de que la autoridad gubernamental controle las transferencias de dinero con otros países (un riesgo mucho más presente en los países en vías de desarrollo).

Posteriormente hablaremos de las empresas que están aceptando bitcoin como pago, fundamentalmente haremos el análisis de empresas en Estados Unidos.

Respecto a la situación legal de las criptomonedas como medio de pago, en la sentencia del TJUE del 22/10/2015 acerca de las operaciones de compraventa de divisas el TJUE concluye que “la divisa bitcoin no puede calificarse de bien corporal puesto que (...) no tiene ninguna finalidad distinta de la de ser un medio de pago”<sup>24</sup>.

Apoyando la anterior sentencia del TJUE, nos encontramos con la Directiva de la Unión Europea 2019/770 en la que en el punto 23 aclara que “Las representaciones digitales de valor, como los

---

<sup>24</sup> <https://curia.europa.eu/juris/document/document.jsf?docid=170305&doclang=ES>

vales electrónicos o los cupones electrónicos, son utilizadas por los consumidores para pagar diferentes bienes o servicios en el mercado único digital. Tales representaciones digitales de valor son cada vez más importantes en relación con el suministro de contenidos o servicios digitales, por lo que deben considerarse un método de pago en el sentido de la presente Directiva”<sup>25</sup>

### **Función de depósito de valor en Bitcoin**

La función de depósito de valor es la que se le ha presupuesto a la criptomoneda como la gran característica inherente a ella.

Generalmente se suele explicar que los recursos presentes en la Tierra son escasos, sin embargo, con los avances tecnológicos e innovaciones lo que se ha hecho es que cada vez tengamos acceso a recursos que no estaban disponibles anteriormente y con ello se consigue que un bien en teoría escaso (como por ejemplo los combustibles fósiles o el oro) no se haya vuelto más “escaso” una vez se encuentra o se consume debido al descubrimiento de nuevos yacimientos gracias a las nuevas tecnologías.

Es el tiempo humano destinado a la exploración y extracción de los materiales el que es escaso (Simon, 1986).

En cambio, en la red Bitcoin, debido a cómo está programado, encontramos un bien estrictamente escaso. Independientemente del número de mineros, usuarios, o de su demanda, sólo existirán 21 millones de bitcoin.

El hecho de ser estrictamente limitado es lo que lo diferencia de todas las formas anteriores de dinero. Incluso en un sistema monetario que fuese un patrón oro, este puede verse depreciado si un año se descubren nuevos yacimientos que expandan la oferta de oro a nivel mundial. De hecho, las importaciones de metales preciosos que hizo España de América del Sur tuvieron severas consecuencias para la economía española.

Bitcoin podrá tener un valor en aumento y aun así no habría forma de que se devaluase por medio de nuevas creaciones, la fiebre del oro que se dio en Estados Unidos no podría darse ahora.

---

<sup>25</sup> <https://www.boe.es/doue/2019/136/L00001-00027.pdf>

## 5. Situación regulatoria

Al tiempo que la demanda de los activos digitales ha aumentado de una forma espectacular desde abril de 2020, las autoridades de todo el mundo han avanzado en sus marcos regulatorios para incluir estos criptoactivos en sus normativas. Un ejemplo de esto fue la Unión Europea, que propuso una única regulación para todos los criptoactivos no cubiertos por la normativa existente (Deutsche Bank, 2021). Está previsto que a finales de 2021 se establezca un reglamento relativo a los mercados de las criptomonedas (MiCA, por sus siglas en inglés).

El Reglamento MiCA no estará disponible hasta 2024 y en él encontramos una serie de aspectos clave en torno a las criptomonedas<sup>26</sup>:

- Impondrá distintos niveles de autorización a los emisores de los diferentes tipos de activos.
- Regulará requisitos de capital, conflictos de interés, gobernanza, custodia de activos de reserva, gestión de reclamaciones etc.
- Impondrá requisitos más estrictos para los tokens con referencia a activos importantes y los tokens de dinero electrónico con referencia a una sola moneda.
- Los criptoactivos estarán sujetos a reglas para evitar el abuso de mercado.
- Los reguladores nacionales autorizarán y supervisarán a los proveedores de servicios de criptoactivos y ESMA establecerá un registro de dichas empresas.

La regulación varía de unos países a otros de forma sustancial, en este trabajo ya hemos mencionado tres países que han establecido regulaciones muy restrictivas ante el uso de las criptomonedas: India, Turquía y China. Otros países con regulaciones extremadamente severas con Bangladesh, Vietnam, Ecuador, Bolivia, Nepal, Irán etc.

Si hacemos un primer análisis de los países donde la regulación es mucho más estricta podemos sacar una primera conclusión en claro: Salvo China, todos son países cuya moneda nacional se deprecia constantemente fruto de las acciones de las autoridades monetarias, mucho más dependientes de los gobiernos que en las economías occidentales.

India en la década de los 70 ya estableció prohibiciones a la tenencia de monedas extranjeras, el desplome de valor del Sucre en Ecuador provocó que el país tuviera que dolarizarse como única solución para arreglar el desastre económico que había causado y en Turquía se tuvo que introducir una nueva unidad monetaria quitándole seis ceros a la moneda antigua.

Por estos motivos, las regulaciones más estrictas hacia las criptomonedas suelen venir fruto de eliminar la alternativa a las monedas nacionales debido a la falta de valor de estas. Bitcoin hace de competencia a esas monedas, las monedas nacionales sufren constantes depreciaciones que

---

<sup>26</sup> [https://ec.europa.eu/info/sites/default/files/business\\_economy\\_euro/banking\\_and\\_finance/200924-presentation-proposal-crypto-assets-markets\\_en.pdf](https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/200924-presentation-proposal-crypto-assets-markets_en.pdf)

dificultan el ahorro y la posibilidad de preservar el valor del tiempo no sólo a largo plazo, sino incluso en periodos inferiores a un año.

Respecto a China, la situación es diferente, el Yuan se encuentra en máximos de tres años frente al dólar americano y con el crecimiento del país y el desarrollo de los mercados financieros lo más probable es que asistamos a una cada vez mayor demanda de la divisa china y por tanto una reducción en la del dólar norteamericano.

En mayo de 2021 China prohibió a las instituciones financieras y de pago ofrecer servicios relaciones con las criptomonedas. Bajo esta prohibición, los bancos y las instituciones de pago no pueden ofrecer estos servicios a sus clientes, como puede ser el trading y la gestión de estas monedas.

No es esta la primera vez que el gobierno chino actúa frente a Bitcoin, ya en 2017 cerró en su país varias casas de cambio y en 2019 el Banco Central de China emitió una nota en la que avisaba que bloquearía el acceso a todo cambio con criptomoneda tanto doméstico como extranjero además de sitios webs de ICO (Initial Coin Offering).

No es casualidad que China sea uno de los países que más restricciones quiere establecer a las criptomonedas. Es, sin duda, uno de los países que más han avanzado en el proyecto de las monedas digitales de banca central con vistas al yuan digital (DCEP) y por tanto que haya alternativas como las criptomonedas privadas que hicieran que su yuan digital tuviera un uso menor de lo que tendría si a la población no se le permitiera otras alternativas.

Los objetivos de la regulación de las criptomonedas se pueden clasificar en tres categorías: Luchar contra el uso de fondos para actividades ilícitas, proteger a consumidores e inversores frente al fraude y garantizar la integridad de los mercados y de los sistemas de pagos (BIS, 2020).

### **Situación fiscal en España:**

#### *Actividades económicas relacionadas con las criptomonedas*

En el capítulo anterior comentamos varias regulaciones que concedían a las criptomonedas la figura de medio de pago. Las criptomonedas permiten a sus tenedores comprar bienes y servicios a empresas que acepten criptomonedas como medio de pago.

#### 1. Criptomonedas como inversión o especulación

El apartado 1 del artículo 33 de la LIRPF establece que:

“Son ganancias y pérdidas patrimoniales las variaciones en el valor del patrimonio del contribuyente que se pongan de manifiesto con ocasión de cualquier alteración en la composición de aquél, salvo que por esta Ley se califiquen como rendimientos”<sup>27</sup>

Cuando se cambia una criptomoneda por divisas como el euro o dólar se produce una alteración patrimonial, ya sea ganancia o pérdida. El importe de la variación patrimonial cuando se

---

<sup>27</sup> <https://www.boe.es/buscar/act.php?id=BOE-A-2006-20764>

transforme las monedas virtuales en dinero constituye una renta del ahorro conforme al artículo 46.b) de la Ley del IRPF (Isidro Nuñez, Guaita Martínez, & Carracedo Garnateo, 2018).

## 2. Minería de Bitcoin

Ya hemos descrito anteriormente la actividad que realizan los mineros, poniendo capacidad de procesamiento al servicio de la red y consiguiendo por ello bitcoin a modo de recompensa.

Ante esta actividad la Agencia Estatal de Administración Tributaria distingue dos tipos de actividades:

**Operaciones de minado que obtienen criptomonedas como prestación:** Sujeto al Impuesto de actividades económicas (IAE) clasificado en el epígrafe 831.9<sup>28</sup>.

**Arrendamientos de servicios informáticos para minado:** Este servicio está sujeto a IVA e IAE y se clasifica en el epígrafe 859.

### Blanqueo de capitales

El blanqueo de capitales incluye todas las acciones e instrumentos utilizados para legalizar los activos monetarios creados en actividades delictivas.

El Grupo de Acción Financiera Internacional (GAFI) es un organismo dependiente de la OCDE que define unos parámetros para luchar contra el blanqueo de capitales y la financiación del terrorismo. Los países vinculados han tenido que firmar acuerdos para cumplir estos propósitos.

España concretamente, pertenece desde 1990 y ha implantado una serie de leyes para cumplir con estos requisitos. En España existe el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (SEPBLANC)<sup>29</sup>.

Desde el SEPBLANC se ha elaborado un listado de operaciones de riesgo y una serie de sujetos que deben tener especial cuidado con el trato de estas operaciones (entidades de crédito, aseguradoras, casas de cambio etc).

Con el auge de las criptomonedas que equivalen a una digitalización del dinero el reto es mayúsculo para estas instituciones que tendrán que establecer una serie de normas y un control para evitar el uso de estos medios con instrumento para el blanqueo de dinero.

### **Situación fiscal en Estados Unidos:**

En este apartado vamos a estudiar cómo está tratada fiscalmente Bitcoin en la primera potencia económica.

---

<sup>28</sup> <https://www.iae.com.es/epigrafe/1-831-9>

<sup>29</sup> <https://www.sepblac.es/es/>

Las ventas y conversiones, así como donaciones y pagos en criptomonedas deben ser reportadas por los ciudadanos estadounidenses. El IRS identifica las criptomonedas como propiedad y las reglas fiscales que aplican a las transacciones de propiedad que han tenido una alteración en su valor también se aplicará a las criptomonedas<sup>30</sup>. Desde 2019, el IRS obliga a responder “sí” o “no” acerca de si tuvo transacciones con monedas virtuales durante el último año.

A continuación, vamos a analizar una lista de las acciones más comunes con criptomonedas que están sujetas a impuestos:

- Vender criptomonedas por dólares: Equivale a realizar la ganancia patrimonial de tus bitcoin.
- Pagar con criptomonedas por bienes y servicios: Por ejemplo pagar un coche Tesla con bitcoin.
- Comprar una criptomoneda con otra.
- Mineros que reciben bitcoin.
- Recibir tu salario en criptomonedas.

Las transacciones deben ser reportadas a su valor de mercado en dólares.

Sin embargo, hay una serie de actividades con criptomonedas que no están sujetas a impuestos en Estados Unidos:

- Comprar criptomonedas con dólares y/o mantenerlas en tu cartera.
- Transferencias de criptomonedas entre diferentes carteras.
- Donaciones de criptomonedas a organizaciones sin ánimo de lucro
- Transferencias de criptomonedas entre carteras y Coinbase.

Como comentábamos anteriormente, la sentencia del Tribunal de Justicia de la Unión Europea consideraba a las criptomonedas como medio de pago. Esto implicaría que no se trataría como un valor mobiliario.

El conflicto al que se enfrentan los reguladores es que, una vez que los cryptoactivos son considerados como medios de pago, el tratamiento de estos es de una suma complejidad. Pues puede no llegar a ser considerados como una moneda por parte de los reguladores al no existir un banco central que la emita, y por tanto una autoridad monetaria que vele por el correcto funcionamiento, lo que podría llegar a acarrear problemas de inseguridad jurídica.

En el caso de Estados Unidos, FinCEN requiere a muchos agentes económicos (instituciones financieras, empresas bursátiles etc) un *reporting* e información acerca de sus transacciones con estos activos digitales. En el capítulo tercero de este trabajo ya se comenta el papel de esta institución en velar porque no se pueda usar como financiación de actividades ilegales.

---

<sup>30</sup> <https://www.irs.gov/businesses/small-businesses-self-employed/virtual-currencies>



“mayorista” que está diseñado para tener un acceso restringido a instituciones financieras y equivaldría a las cuentas de reservas y liquidación que tienen en estos momentos esas instituciones con los bancos centrales (BIS, 2021).

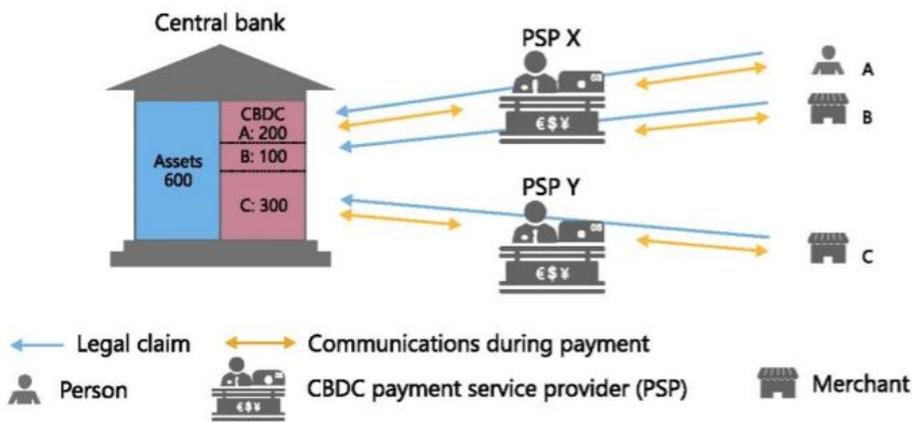
De la misma manera que las criptomonedas tiene como uno de los motivos de su creación la facilidad y rapidez para transferir el dinero entre lugares lejanos sin grandes costes de tiempo y dinero, los bancos centrales empezaron a estudiar los proyectos de las CBDC para intentar solucionar parte de estos problemas y combinar así los aspectos positivos de las criptomonedas privadas junto con los aspectos positivos del dinero fiat (que son el reconocimiento legal del medio de pago, la confianza como respaldo, el acceso a toda la población etc.).

El diseño de las CBDC tiene como uno de los principales objetivos preservar el sistema financiero en dos niveles entrelazados de manera público-privado. Desde una perspectiva del usuario, una CBDC que se precie debe proporcionarle un entorno digital resiliente e inclusivo para complementar al efectivo físico pero que no dañe a las instituciones financieras privadas (BIS, 2021).

La investigación que llevó a cabo el Banco Internacional de Pagos analizaba las arquitecturas CBDC híbridas donde las entidades financieras privadas no pierdan su papel en un nuevo sistema donde el banco central pueda tener pasivos directamente con los ciudadanos.

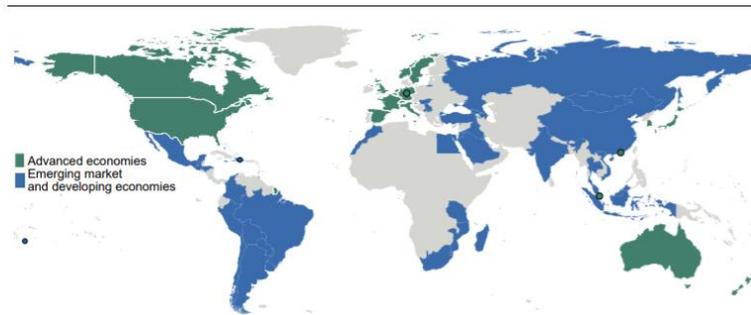
Los usuarios tienen varias opciones, una es pagando con CBDC al igual que hoy se puede hacer con una tarjeta de débito. Sin embargo, en lugar de que estos intermediarios reserven transacciones en sus propios balances, como es el caso hoy, simplemente actualizarían el registro de quién posee qué balance de CBDC. El CBDC por tanto sería un derecho similar al efectivo frente al banco central y este evita las tareas operativas de abrir cuentas y administrar los pagos de los usuarios que recaerían en las entidades financieras privadas. Además, esta estructura permitiría operar al banco central en caso de que el sector financiero privado tuviese algún problema técnico (BIS, 2021).

Ilustración 42 Funcionamiento de la arquitectura híbrida CBDC. Fuente: BIS



En 2020 se hizo un informe en el que participaban 65 bancos centrales de todo el mundo que representaban más del 70% de la población mundial y más de un 90 de la producción.

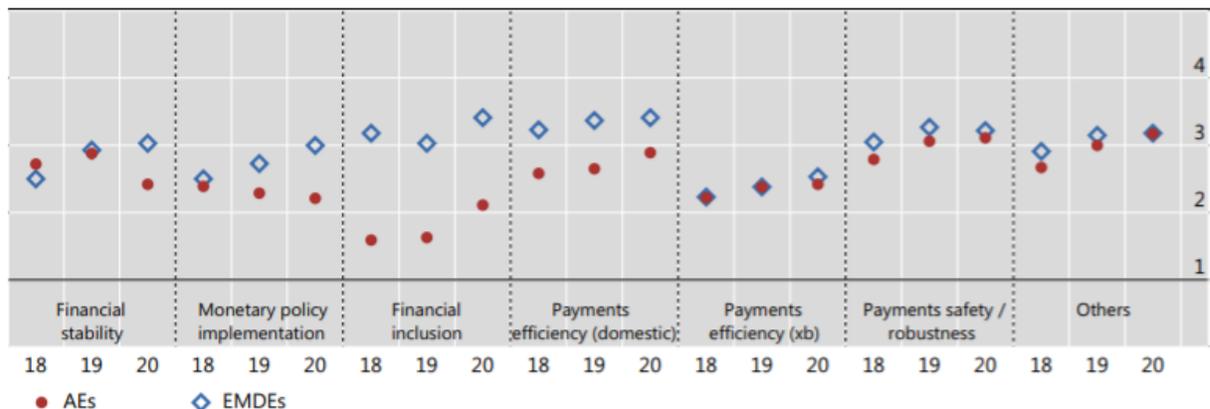
Ilustración 43 Países con bancos centrales participantes. Fuente: BIS



Debido al planteamiento de los bancos centrales de emitir sus propias CBDC se les realizaron una serie de preguntas acerca de las motivaciones para hacerlo, como la estabilidad financiera, eficiencia de pagos y seguridad, etc (BIS, 2021).

Los resultados fueron los siguientes:

Ilustración 44 Motivaciones para emitir CBDC. Fuente: BIS



(1) = "Not so important"; (2) = "Somewhat important"; (3) = "Important"; (4) = "Very important".

Mientras que los puntos rojos hacen referencia a las economías avanzadas, los azules se refieren a las emergentes, y de los resultados se desprende que en las emergentes tienen una motivación mayor para la emisión de CBDC que las economías avanzadas.

Es la eficiencia de pagos a nivel doméstico la cuestión a la que se le ha dado más importancia en los países emergentes y la seguridad de los pagos lo que más han valorado las economías desarrolladas.

La mayoría de los bancos centrales están explorando la posibilidad de emitir CBDC, pero según el informe del Banco Internacional de Pagos, el despliegue generalizado de las CBDC todavía parece lejano. Aunque haya intereses en la emisión de la CBDC, sus motivaciones varían de un lugar a otro.

La coordinación de las políticas sobre CBDC van en camino de intensificarse en el futuro según se vayan resolviendo las complejidades a las que se enfrentan (BIS, 2021).

Las criptomonedas digitales emitidas por los bancos centrales aún tienen que resolver problemas como son (Deloitte, 2020):

- Privacidad: Este es uno de los temas más controvertidos. El hecho de operar con estas criptomonedas implicaría que los bancos centrales y por ende, los gobiernos, tendrían acceso a toda la información acerca de todas las transacciones económicas que realizan los agentes económicos.
- AML/KYC: En este momento no está claro cómo se aplicarían en la práctica los requisitos AML a las modalidades anónimas de CBDC (BIS, 2018). Emitir una CBDC que no cumpla estos requisitos y normas tributarias o de supervisión no sería recomendable.
- Ciberseguridad: En los últimos años se ha vivido un crecimiento de los ciberataques y los bancos centrales deberían contar con un sistema de seguridad que pudiese hacer frente a estos ataques. Debido a que las CBDC estarían abiertas a un enorme número de ciudadanos esto podría hacer que fuese un sistema más vulnerable por el hecho de tener más posibles puntos de ataque.
- Regulación: Los problemas regulatorios se refieren a que no todos los bancos centrales están facultados para emitir monedas digitales y ampliar el acceso a las cuentas. Además, estaría a considerar el que CBDC fuera una “moneda de curso legal” que esté sujeto a la legislación vigente (BIS, 2018).

Un problema que se debe mencionar aparte, es el poder que daría a las autoridades monetarias la implantación de CBDC si al mismo tiempo se establecen medidas que penalicen el uso de efectivo en la economía.

En el primer punto comentábamos que la privacidad es uno de los principales retos a los que se enfrentan las monedas digitales. El hecho de que las autoridades monetarias tengan acceso a las transacciones de los agentes económicos (que serán más transacciones cuanto más se penalice el efectivo o el uso de criptomonedas) les da poder para:

- El gobierno donde actúa la autoridad monetaria puede establecer impuestos sobre cualquier transacción.
- Imposibilitar actividades que fuesen prohibidas por la ley: Aunque en principio se pueda pensar en esto como algo positivo, lo cierto es un arma de doble filo en tanto en cuanto un gobierno puede establecer prohibiciones en función de sus intereses políticos. Por ejemplo, en una dictadura como China, el gobierno tendría un poder absoluto para bloquear cualquier transacción que no le interesase, como por ejemplo compras a una empresa cuyos directivos hayan puesto en cuestión al propio gobierno.
- Las autoridades pueden elegir a quién repartir fondos y a quién no: Este problema se refleja en el hecho de que los responsables podrían decidir de una manera selectiva a qué empresas o ciudadanos podrían aumentar los fondos hacia ellos y a quiénes no. Si por ejemplo un sector es visto por parte de las autoridades como favorable ellos pueden decidir dotar a las empresas pertenecientes al sector del dinero de nueva creación, pudiendo con ello marcar una pauta sobre la estructura productiva de su país.
- Las autoridades tendrían acceso a toda la información de los individuos. Esta cuestión no es algo menor, socavaría el derecho a la privacidad de los ciudadanos y, en los países más autoritarios como China, serviría para hacer un seguimiento completo de las actividades de los ciudadanos.

Una vez analizado lo que son las CBDC y los datos referentes a su situación actual, ahora analizaremos qué diferencias hay entre la moneda bitcoin y las CBDC emitidos por los bancos centrales.

Para hacer un análisis eficiente primero tenemos que aclarar de nuevo que las CBDC no son criptomonedas propiamente dichas, sino que sirven como un mecanismo de pago digital.

### **Dinero privado vs dinero respaldado por el gobierno**

Sin duda alguna, la diferencia más importante entre las criptomonedas privadas en general (y el bitcoin en particular) y las criptomonedas de banca central, es la naturaleza privada o pública de estas.

El dinero privado es aquel medio de cambio aceptado por muchos agentes y que es emitido por una entidad privada o por individuos, mientras que el dinero público es aquel emitido por bancos centrales a los cuales el poder político le ha otorgado el derecho de la emisión de la moneda nacional.

Uno de los ejemplos más representativos del funcionamiento de una gran economía con diferentes monedas privadas compitiendo entre sí, tuvo lugar en Estados Unidos en el siglo XIX donde la banca privada funcionaba con total libertad para emitir sus certificados (Hayek, 1976).

### **Activo real vs activo financiero**

Además, los CBDC, como se comentó anteriormente, son considerados un pasivo en el balance de los bancos centrales mientras que Bitcoin es un activo real, debido a no ser ninguna obligación financiera para nadie.

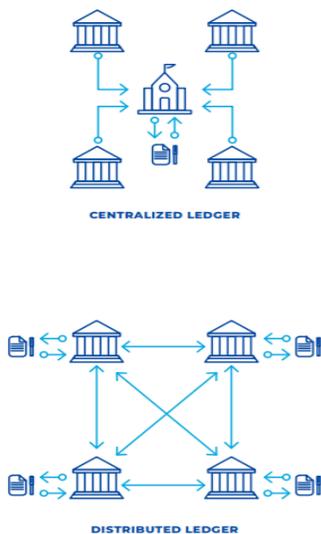
La diferencia entre un activo real y un activo financiero es que el segundo es la mera obligación de pago (reconocimiento de un pasivo) lo cual hace que el valor de ese activo esté ligado a la capacidad del deudor para hacer frente a ese pasivo. Eso provoca que pueda perder valor ese activo si la condición del banco central o del gobierno se deteriora porque, por ejemplo, emita cantidades ingentes de dinero.

Este problema no lo tiene Bitcoin, debido a que no representa un activo financiero ligado a un actor central que pueda controlar la política monetaria y, por ende, al no constituir un pasivo, no se puede ver depreciado por un decrecimiento en la credibilidad de un actor central, porque ni tal actor existe, ni el bitcoin representa un compromiso de pago para ningún agente.

### Descentralización vs Centralización

Mientras la red Bitcoin es una red descentralizada cuyo funcionamiento se basa en una red de nodos interconectados donde ninguno tiene más poder que otro y todos se someten a las mismas reglas, CBDC requiere de un sistema centralizado donde los bancos centrales se encargarán de la emisión con el objetivo de servir a sus políticas públicas.

Ilustración 45 Diferencia entre un sistema monetario centralizado y descentralizado. Fuente: IE



## Transmisión descentralizada vs Trasmisión centralizada

Un activo monetario puede clasificarse como activo de transmisión descentralizada o centralizada.

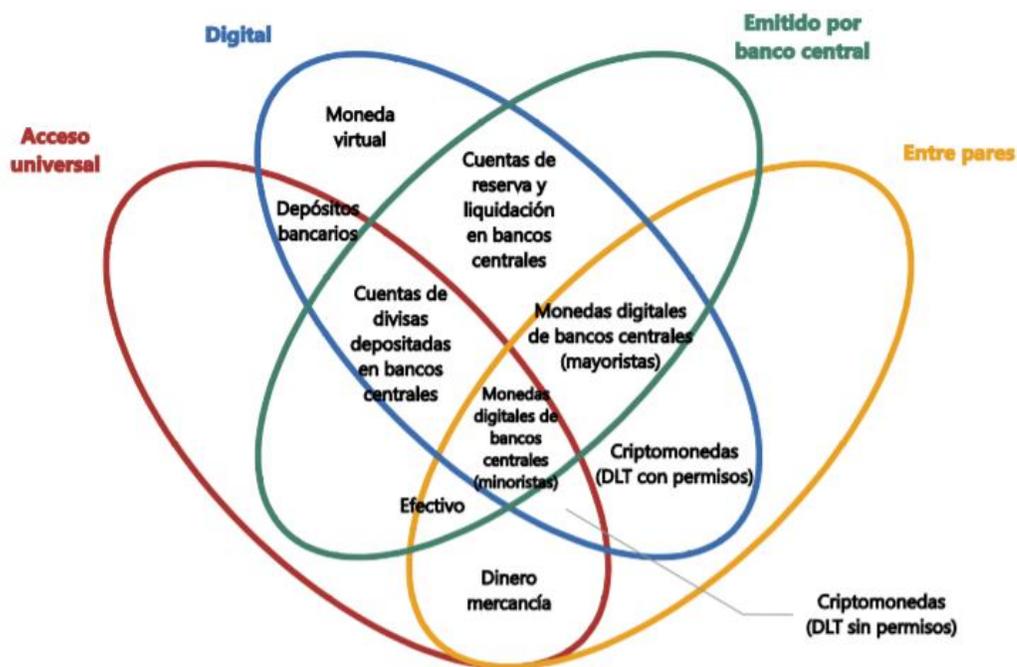
Bitcoin da la posibilidad al poseedor de transferir unidades monetarias a cualquier otra persona y cualquier nodo puede verificar ese intercambio y añadirlo al bloque de transacciones.

Un ejemplo de transmisión descentralizada sería el dinero en efectivo, ya que los usuarios de la moneda pueden intercambiarla libremente sin conocimiento de la autoridad pertinente.

En cambio, las CBDC son activos de transferencia centralizada en tanto en cuanto los intercambios deben ser validados por una autoridad, bien sea el banco central o un banco privado en el sistema híbrido que se explicó anteriormente.

Haciendo una última clasificación, y un resumen de las propiedades clave de los distintos tipos de dinero podemos estudiar a continuación la flor del dinero. Bech y Garrat en su informe llamado «Criptomonedas de bancos centrales» de 2017 elaboraron lo que se llama una flor del dinero en función de cuatro propiedades (Bech & Garratt, 2017): Acceso Universal, Digital, Emitido por un banco central y si es P2P.

Ilustración 46 Flor del dinero. Fuente: Bech y Garrat (2017)



## 7. Bitcoin en las empresas e IIC

El número de empresas que decidieron incluir bitcoin en sus balances aumentó de manera notable en 2020 liderados por Microstrategy, donde Michael Saylor, como CEO de la compañía,

ha emprendido una estrategia muy agresiva al transformar prácticamente los 700 millones de dólares que tenía la empresa en efectivo en bitcoin.

Según las estimaciones, en Estados Unidos ya había más de 2300 empresas que aceptaban bitcoin, incluso algunos equipos deportivos ya acordaron vender los abonos de temporada de esta forma (Deloitte, 2021). Aunque aún falte un camino muy grande por recorrer, no es menos cierto que el último año son muchas las empresas que se han sumado a esta tendencia.

En el siguiente cuadro podemos ver un listado de las empresas públicas y cotizadas más grandes de Estados Unidos y otros países que incluyen en su balance esta criptomoneda.

Ilustración 47 Empresas con bitcoin en su balance en mayo de 2021. Fuente: BitcoinTreasuries.org

BitcoinTreasuries.org	Symbol	Market Cap	% BTC	Purchases/Filings	Cost Basis USD	Today's Value	NgU	Bitcoin	/21M
MicroStrategy inc.	US NADQ:MSTR	\$5,280,941,440	89%	250M Aug, 175M Sep 2020, Learn	√\$2,226,000,000	\$4,674,750,792	2.1x	B 91,579	.436%
Tesla, Inc.	US NADQ:TSLA	\$757,554,688,042	0.3%	Ann (estimate 48k btc)	√\$1,500,000,000	\$2,205,191,520	1.5x	B 43,200	.208%
Square inc.	US NADQ:SQ	\$94,111,027,728	0.4%	50M Bitcoin Investment Whitepaper	√\$220,000,000	\$409,747,045	1.9x	B 8,027	.038%
Marathon Digital Holdings	US NADQ:MARA	\$2,272,936,894	12%	Jan 25th Ann	√\$161,539,500	\$276,912,841	1.7x	B 5,425	.026%
Coinbase Global, Inc.	US NADQ:COIN	\$56,496,109,082	0%	S1 filing	? \$276,912,841	\$276,912,841		B 4,487	.021%
Galaxy Digital Holdings	CA TSE:GLXY	\$2,678,658,747	8%	\$134M on Jun-30-2020	? \$204,184,400	\$204,184,400		B 4,000	.019%
Bitcoin Group SE	DE ADE:DE	Not on G.F. ↘	-	Fin report	? \$204,184,400	\$204,184,400		B 4,000	.019%
Hut 8 Mining Corp	CA TSX:Hut-8	\$712,299,888	23%	Q2 2020	√\$39,303,111	\$165,032,041	4.2x	B 3,233	.015%
NEXON Co. Ltd	US TYO:3859	Not on G.F. ↘	-	100M Apr 2021	√\$100,000,000	\$87,646,154	0.9x	B 1,717	.008%
Riot Blockchain, Inc.	US NADQ:RIOT	\$2,231,518,012	3.6%	\$7.2M on Jun-30-2020	√\$9,930,000	\$79,887,147	8.0x	B 1,565	.007%
Voyager Digital LTD	CA CSE:VYGR	\$188,844,956	38%	March 31 2020	√\$7,927,182	\$63,246,118	8.0x	B 1,239	.006%
Seelee AS	NO AKER:NO	Not on G.F. ↘	-	March 2021	√\$58,599,450	\$59,723,937	1.0x	B 1,170	.006%
Meitu	HK SEHK:1357	Not on G.F. ↘	-	Statement	√\$49,500,000	\$48,029,245	1.0x	B 941	.004%
Argo Blockchain PLC	US OTCPK:ARBKF	\$507,742,529	9.3%	December 2020	? \$47,319,735	\$47,319,735		B 927	.004%
Bitfarms Limited	CA CSE:BITF	\$984,361,733	3.4%	Ann	? \$16,817,350	\$33,179,965	2.0x	B 650	.003%
Coin Citadel Inc	US OTCMKTS:CCTL	Not on G.F. ↘	-	December 2015 report	√\$184,390	\$26,186,649	142x	B 513	.002%
Bit Digital, Inc.	US NADQ:BTBT	\$489,195,552	5.3%	Jan. 2021	? \$24,936,020	\$24,936,020		B 489	.002%
Cypherpunk Holdings Inc.	CA CSE:HODL	\$24,797,807	74%	\$1.63M on Jun-30-2020 +60BTC	? \$5,637,663	\$18,366,387	3x	B 360	.002%
Hive Blockchain	CA CSE:HIVE	\$1,322,014,401	1%	Report	? \$16,334,752	\$16,334,752		B 320	.002%
BIGG Digital Assets Inc.	CA CNSX:BIGG	\$322,348,285	5%	SEDAR Reports	√\$2,690,387	\$15,313,830	5.7x	B 300	.001%
Advanced Bitcoin Technology	DE ABT:GR	Not on G.F. ↘	-	Q1 2018	√\$2,117,978	\$12,957,746	6.1x	B 254	.001%
DMG Blockchain Solutions	CA TSX-V:DMGI	\$137,347,651	8%	SEDAR Reports	? \$11,230,142	\$11,230,142		B 220	.001%
DigitalX	AU ASX:DCC	\$47,146,997	23%	215 BTC 2019	√\$874,835	\$10,974,912	13x	B 215	.001%
Digihost Technology Inc.	CA TSXV:DGHLV	Not on G.F. ↘	-	Feb. 2021	√\$6,890,000	\$9,377,169	1.4x	B 184	.001%
Fortress Blockchain	CA TSXV:FORT	Not on G.F. ↘	-	Q3 2020	? \$8,330,724	\$8,330,724		B 163	.001%
CleanSpark Inc	US NASDAQ:CLSK	\$501,082,031	1%	Ann	? \$7,299,592	\$7,299,592		B 143	.001%
Banxa Holdings Inc	CA OTCMKTS:BNXAF	\$205,733,753	3%	Ann	? \$6,942,270	\$6,942,270		B 136	.001%
Neptune Dash Technologies	CA TSXV:DASH	Not on G.F. ↘	-	Q3 2020	? \$4,645,195	\$4,645,195		B 91	.000%
Mode Global Holdings	UK LON:MODE	Not on G.F. ↘	-	2020 Ann	√\$975,089	\$4,333,620	4x	B 85	.000%
BTCS Inc.	US OTCQB:BTCS	Not on G.F. ↘	-	Filing	? \$4,008,854	\$4,008,854		B 79	.000%
FRMO Corp.	US OTCMKTS:FRMO	\$627,181,972	0.5%	March 21, 2020	? \$3,207,737	\$3,207,737		B 63	.000%
MOGO Financing	CA NADQ:MOGO	\$475,824,657	0.5%	ann	? \$2,552,305	\$2,552,305		B 50	.000%
Phunware, Inc.	US NADQ:PHUN	\$96,848,117	1.4%	Ann	√\$1,499,831	\$1,316,989	1x	B 26	.000%
BlackRock	US NYSE:BLK	\$125,605,408,050	0.0%	ann	√\$360,000	\$313,934	1x	B 6.15	.000%

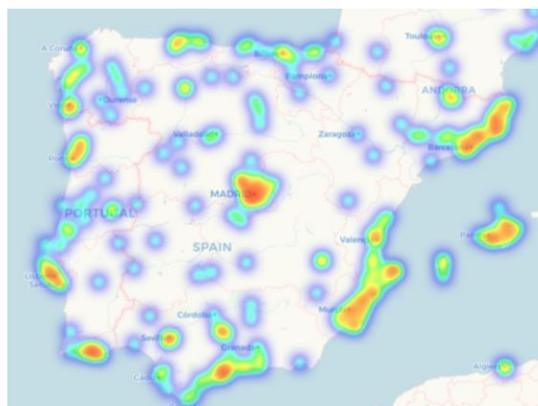
Las compañías que aceptan criptomonedas como medio de pago por sus productos o servicios pueden hacerlo por distintos motivos:

- Acceder a un grupo demográfico nuevo: Un estudio analizó que el 40% de los clientes que pagan con criptomonedas son nuevos clientes de la empresa y el volumen de sus compras representan el doble que los usuarios de tarjetas de crédito (Deloitte, 2021).
- Introducir las criptomonedas en la empresa puede ayudarla a crecer en el proceso de digitalización, modernizando a la empresa y preparándola para un nuevo futuro donde se puedan incluir las CBDC.
- Podría permitir acceso a nuevo capital y liquidez a través de inversiones tradicionales que han sido *tokenizadas* así como a nuevas clases de activos.
- Las criptomonedas posibilitan una distribución de ingresos precisa y en tiempo real además de mejorar la transparencia para facilitar las labores de back office.

Una empresa puede optar por aceptar las criptomonedas como medio de pago y luego convertirlo a la moneda nacional correspondiente y por tanto manteniendo las criptomonedas fuera de los libros. Mantener este sistema, sin añadir bitcoin al balance de la empresa, es la manera más sencilla y rápida de adentrarse en el mundo de los activos digitales (Deloitte, 2021).

En España la situación de comercios que aceptan criptomonedas y cajeros ATM presenta la siguiente situación

*Ilustración 48 Mapa de comercios que aceptan criptomonedas y de cajeros ATM. Fuente: Coinmap.org*



### ¿Pueden invertir las IIC en criptomonedas?

Una duda que ha surgido recientemente es la de si las instituciones de inversión colectiva en este país pueden invertir en criptomonedas. Respecto a esta cuestión, la CNMV aclara que:

“Si las IIC son UCITS o armonizadas, pueden tener exposición a criptomonedas a través de instrumentos financieros cuya rentabilidad se encuentre vinculada a tales monedas, que no incluyan un derivado implícito (ETC, ETN y cualquier instrumento de los denominados “Delta one”). Dichos instrumentos serían aptos siempre que dispongan de negociación diaria, en la que el precio de mercado se determine a partir de operaciones de compraventa realizadas por

terceros (ya que en este caso no haría falta realizar “lookthrough” del instrumento). Asimismo, podrían invertir en valores o instrumentos financieros cotizados de entidades que cumplan los requisitos del artículo 48.1 a) RIIC y que a su vez tengan inversiones en criptomonedas. Por lo que se refiere a las CuasiUCITS reguladas en el art. 72 del RIIC, además de lo anterior, éstas podrán invertir dentro del coeficiente de libre disposición en IICIL españolas o extranjeras similares, (y derivados sobre estas instituciones), o en otras IIC no UCITS que tengan exposición a criptomonedas (art 72.1.d) del RIIC). Sin embargo, no es posible invertir en derivados cuyo subyacente sean criptomonedas, dado que no es uno de los subyacentes aptos de acuerdo con el artículo 2.6 de la Orden 888/2008, de 27 Preguntas y respuestas sobre la normativa de IIC, ECR y otros vehículos de inversión colectiva cerrados 13 de marzo, sobre operaciones de las instituciones de inversión colectiva de carácter financiero con instrumentos financieros derivados. Por otro lado, las IIC de Inversión Libre reguladas en el art. 73 del RIIC también podrían tener exposición a criptomonedas a través de derivados, dado no hay limitación en el subyacente, y siempre que la liquidación del derivado no suponga la entrega de la criptomoneda, si bien estas IIC solo pueden comercializarse entre inversores profesionales. Por último, teniendo en cuenta que la inversión en criptomonedas se trata de una inversión de alto riesgo, cuyo precio conlleva un alto componente especulativo (tal y como se ha puesto de manifiesto en el comunicado conjunto de la CNMV y el Banco de España sobre el riesgo de las criptomonedas como inversión de 9 de febrero de 2021), el folleto y el DFI deberán incluir una mención expresa y destacada acerca de la exposición a criptodivisas y de los riesgos que puede conllevar, incluidos los riesgos específicos sobre su formación de precios y su liquidez señalados en dicho Comunicado.”

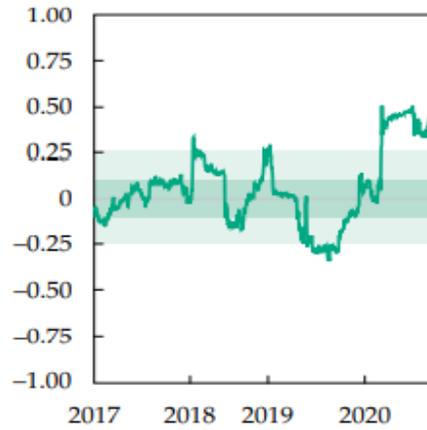
Las instituciones de inversión que quieren invertir en Bitcoin y no utilizar su moneda a modo de atesoramiento deben ser conscientes que desde que la criptomoneda fue creada ha tenido tres características marcadas (Hougan & Lawant, 2021):

- Altos retornos: En el capítulo de la evolución de Bitcoin analizábamos en el final, a modo de resumen, la evolución del precio, así como sus acontecimientos más importantes desde su creación. Viendo la evolución que ha tenido el precio nos encontramos ante posiblemente el activo con mejor comportamiento de la última década.
- Alta volatilidad: Acompañando a las altas rentabilidades, este criptoactivo por el momento presenta una volatilidad altísima, muy superior a los activos tradicionales. La institución que quiera incluir bitcoin en sus carteras debe saber que puede llegar a incrementar de una forma sustancial la volatilidad de la cartera. Se ha vuelto a poner de manifiesto con la corrección que se produjo en mayo de 2021 por las amenazas de China.
- Baja correlación con activos tradicionales: Una de las características más importantes de la criptomoneda es que sus retornos tienen que ver con lo que esté pasando en el mercado de renta variable, renta fija e incluso oro (Hougan & Lawant, 2021)

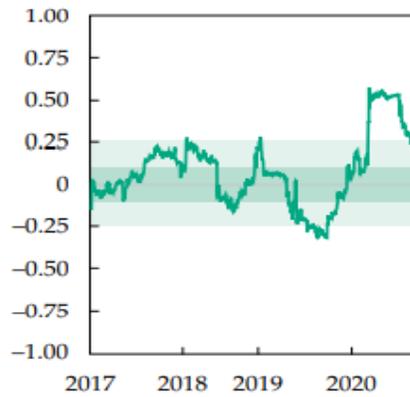
En los siguientes gráficos podemos observar la correlación de Bitcoin con la renta variable de grandes y pequeñas empresas (estadounidenses) y con el oro.

Las bandas de fluctuación entre -0.25 y 0.25 se pueden considerar como de una baja correlación.

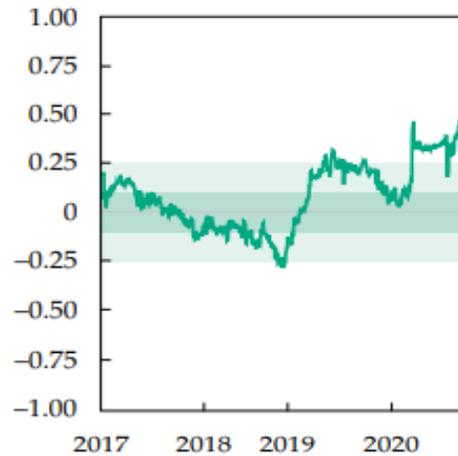
*Ilustración 49 Correlación de Bitcoin con las Renta Variable de grandes empresas. Fuente: Hougan y Lawant (2021)*



*Ilustración 50 Correlación de Bitcoin con la Renta Variable de pequeñas empresas. Fuente: Hougan y Lawant (2021)*



*Ilustración 51 Correlación de Bitcoin con el oro. Fuente: Hougan y Lawant (2021)*



No debe sorprender la baja correlación que tiene con estos activos porque Bitcoin aún es muy reciente y los principales conductores del precio de la criptomoneda son diferentes a los principales conductores en ese tipo de activos. Por ejemplo, en las correcciones de Bitcoin se ha puesto de manifiesto que aún hay miembros del mercado por motivos especulativos que pueden reaccionar muy bruscamente ante una noticia negativa, o al contrario, subidas de precio que atraigan a más miembros del mercado y por tanto continúe esa escalada de precios.

## 8. Conclusiones

En la elaboración de este trabajo hemos hecho una explicación de las principales funciones de Bitcoin y cómo funciona la red.

Al ser una red P2P todos los miembros tienen los mismos derechos y se prescinde de la necesidad de contar con un tercero de confianza y por tanto los efectos negativos, que se derivan de la existencia de ese tercero, desaparecen al establecerse una red entre pares.

Gracias a la prueba de trabajo, Bitcoin se asegura de evitar las transacciones fraudulentas, no existe ningún incentivo a malgastar capacidad de procesamiento sabiendo que la verificación apenas tiene coste. El hecho de contar con este protocolo, produce que la red tenga una grandísima seguridad y no quepan los posibles ataques a la red.

Respecto a la tecnología *blockchain*, que es totalmente necesaria para el correcto funcionamiento de Bitcoin, hemos visto que también tiene desventajas y que, fuera del ámbito de la descentralización que se le debe suponer a una criptomoneda, es una tecnología que tiene desventajas y que supone unos costes mayores que tener un sistema centralizado.

En el capítulo en el que analizamos las críticas más comunes hacia la criptomoneda hemos podido comprobar que los datos analizados desmontan muchos de los argumentos que justifican esas críticas.

Por ejemplo, atendiendo al valor intrínseco, acusar a Bitcoin de falta de este es desconocer el funcionamiento práctico de la economía, malinterpretando el concepto de valor como si de algo objetivo se tratara y lo cierto es que proviene estimaciones subjetivas proyectadas por los agentes económicos.

El mayor inconveniente que presenta Bitcoin actualmente es la volatilidad, y las caídas producidas el pasado mes de mayo no son sino una muestra más de que aún tiene largo recorrido por delante para intentar estabilizar el precio y evitar las grandes fluctuaciones.

Ese inconveniente es clave a la hora de evaluar si cumple las funciones principales que se le deben suponer al dinero. Mientras el activo presente altos niveles de volatilidad no puede tener

capacidad de unidad de cuenta al ser sumamente complicado el establecer una medición de los bienes y servicios de una economía en términos de un activo altamente volátil.

En cuanto a la capacidad de ser usado como medio de pago, lo cierto es que aún tiene recorrido por delante, en especial en las transacciones de importes más reducidos, si bien es cierto que esta tendencia está en aumento y cada vez son más las empresas que aceptan esta moneda como medio de pago<sup>31</sup>.

La función de depósito de valor para mantener el poder adquisitivo de la moneda en el largo plazo es muy importante. Con el sistema monetario actual, a través de la inflación se produce una reducción del poder adquisitivo de las monedas nacionales.

Al no estar respaldadas por oro, los bancos centrales se libraron de corsés que les impidieran aumentar la masa monetaria a su antojo y ello redundó en depreciaciones de la moneda.

Bitcoin es diferente, ha logrado redefinir el concepto de escasez, que suele ser un concepto relativo para las materias primas, y ha conseguido la escasez absoluta, no existirán más de 21 millones de bitcoin. Es por eso por lo que no se puede erosionar el poder adquisitivo de la moneda a través de nuevas emisiones y por tanto constituye una gran alternativa como reserva de valor a lo largo del tiempo.

Finalmente, debemos comentar las conclusiones a las que llegamos respecto a la comparación de Bitcoin con las CBDC.

Es cierto que las CBDC presentan los aspectos positivos que puede presentar las monedas nacionales junto con algunos aspectos positivos de las criptomonedas privadas. Sin embargo, las CBDC siguen teniendo las principales desventajas del dinero fiat junto con unas dificultades nuevas que se le añadirían.

Las dos principales desventajas de las CBDC son la pérdida por completo de la privacidad de los agentes económicos a la hora de llevar a cabo sus pagos y sus transacciones y el aumento de la capacidad del banco central de crear inflación o redistribuir la riqueza, es decir, el hecho de establecerse relaciones más directas entre el banco central y los ciudadanos haría que la emisión de activos digitales llegara directamente a estos y por tanto la inflación aumentase a unos niveles superiores a los que lo estaba haciendo.

Esos dos inconvenientes por sí solos ya constituyen una amenaza muy grande para una parte de los agentes económicos en el momento en el que pierden su privacidad y una parte de su riqueza acumulada en esos activos.

Aunque estos efectos negativos sean menos perjudiciales para la sociedad en países desarrollados, con plena seguridad jurídica y una defensa de los derechos de propiedad, lo cierto

---

31

[https://public.tableau.com/app/profile/lon.grimes/viz/BitcoinHeldInInstitutionalTreasuries\\_16149600579070/Story1](https://public.tableau.com/app/profile/lon.grimes/viz/BitcoinHeldInInstitutionalTreasuries_16149600579070/Story1)

es que aumentan conforme nos vamos a países más autoritarios o cuya seguridad jurídica es prácticamente inexistente.

No hablamos sólo de países en vías de desarrollo o en una situación económica débil, sino que en este grupo en el que los efectos negativos de la emisión de activos digitales son más notorios incluiríamos a China.

China es uno de los países que más han avanzado en su proyecto de CBDC al tiempo que ha sido uno de los que más amenazas ha vertido contra Bitcoin. No es de extrañar esto, ya hemos comentado que el hecho de emitir una CBDC otorgaría al banco central y, por ende, a las autoridades políticas del país un control de las transacciones que hacen sus ciudadanos, y eso equivaldría a aumentar el control que el gobierno chino tuviera sobre su población.

Es por esto, por lo que, para una parte de los ciudadanos, la alternativa de Bitcoin resulta eficiente, más en los países donde la moneda nacional pierde prácticamente todo su valor.

Es cierto que aún hay una parte de tenedores de bitcoin y otras criptomonedas cuyo único motivo es el especulativo para ganar dinero a corto plazo. Sin embargo, además de que estos últimos no son la mayoría de esta red, también cada vez hay una cantidad mayor de empresas grandes e inversores usando esta criptomoneda como mera reserva de valor a largo plazo.

Conforme pase el tiempo, si cada vez el número de usuarios de Bitcoin aumenta, lo más seguro es que se estabilice el precio y con ello se reduzca la enorme volatilidad que presenta ahora mismo, eso sacaría a los usuarios que entraron con objetivos de ganar dinero a corto plazo que llevaría a su vez a más estabilización del valor, al salirse los miembros más tendentes a vender como reacción a nuevas noticias.

Puede que los argumentos esgrimidos en este trabajo no sean suficiente como para justificar un nuevo patrón monetario y que girase en torno a una criptomoneda privada, pero lo que sí es cierto es que Bitcoin es mucho más eficiente de lo que suele esgrimirse por parte de la economía académica, de los medios de comunicación etc que lo menosprecian o lo tachan de burbuja al tiempo que lo asemejan a los tulipanes en Holanda.

Bitcoin es algo mucho más profundo, que requiere de un estudio avanzado para poder entender todas las posibilidades que ofrece y por tanto así establecerse un justo análisis y debate.

## 9. Glosario de términos.

**Altcoin:** Se puede traducir como criptomoneda alternativa al bitcoin.

**Bitcoin (con B mayúscula):** se utiliza para describir el concepto de bitcoin, la red y el protocolo que mantienen su blockchain y su criptomoneda.

**bitcoin (con b minúscula):** se refiere a la unidad de la criptomoneda basada en la red homónima. Su abreviación se conoce como BTC.

**Blockchain:** Cadena de bloques de datos enlazados con criptografía que se añaden progresivamente uno tras otro. En las criptomonedas, estos bloques registran las transacciones validas realizadas con ellas. Esta se puede dividir en cadenas de bloque privadas, públicas o semipúblicas.

**Bloque Génesis:** Hace referencia al primer bloque producido y verificado, hecho por Satoshi Nakamoto en 2009 y a partir de él se encadenaron los sucesivos bloques.

**Cartera (Wallet):** Software que gestiona cuentas y llaves de la red de Bitcoin donde poder enviar y recibir bitcoin.

**Casa de Cambio:** Es donde se realizan las operaciones de cambio de moneda, cada casa de cambio ofrece bitcoin a tipos de cambio con otras monedas que pueden llegar a variar.

**CBDC:** Abreviatura de “Central Bank Digital Currency”. Es una criptomoneda emitida por un banco central.

**Clave pública:** Línea de caracteres alfanuméricos que se encuentra matemáticamente asociada con la clave privada y que se utiliza para derivar una dirección pública.

**Clave privada:** Línea alfanumérica asociada matemáticamente a la dirección pública y con la que su dueño puede firmar mensajes para verificar su identidad y/o hacer transacciones.

**Criptografía:** Técnica destinada a la protección de datos de cualquier tipo usando códigos que ocultan la información.

**Criptomoneda:** Moneda basada exclusivamente en la criptografía.

**Cypherpunk o Ciberpunk:** Movimiento contracultural de tradición libertaria. Este movimiento generado a partir del uso de internet defiende la criptografía para proteger los derechos de privacidad de las personas.

**Doble Gasto:** Defecto por el que el dinero digital puede gastarse más de una vez.

**Hash:** Una función, pilar de la tecnología blockchain, por la que los algoritmos se encargan de asegurar la autenticidad de los datos y proteger las contraseñas y la veracidad de los documentos electrónicos.

**Hodl:** Término en inglés que hace referencia a “mantener” pero que presenta un error ortográfico debido a un error de un usuario a la hora de escribirlo. Ahora mismo hace referencia a “Hold on for dear life”.

**Nodo:** Se trata de los participantes, es un ordenador o servidor capaz de transmitir la información o verificar la cadena de bloques.

**Minero:** Subgrupo de los nodos encargados de realizar las operaciones, produciendo los bloques de blockchain y recibiendo bitcoin por su trabajo.

**P2P:** Red entre pares que tienen los mismos derechos. No hay ningún miembro de esta red que tenga privilegios o una posición dominante.

**PoW:** Prueba de trabajo que hace que los mineros tengan que resolver, a través de capacidad de procesamiento, problemas matemáticos para poder registrar las transacciones y completar bloques.

**Token:** Una unidad de valor que una organización crea para gobernar su modelo de negocio y dar a los usuarios la posibilidad de interactuar con sus productos con esa unidad.

## Bibliografía

- Adrian, T., & Mancini-Griffoli, T. (2019). *The Rise of Digital Money*.
- Ammous, S. (2018). *El patrón Bitcoin*. DEUSTO.
- Antonopoulos, A. (2017). *Mastering Bitcoin*. O'Reilly.
- Antonopoulos, A. (s.f.). Bitcoin explicado en el taller de conceptos básicos de Bitcoin CBP Prep. Obtenido de <https://www.youtube.com/watch?v=FYo5E7zT-vM&t=2339s>
- Bashir, I. (2017). *Mastering Blockchain*.
- Bech, & Garratt. (2017). *Criptomonedas de bancos centrales*.
- BIS. (2018). *Monedas Digitales emitidas por Banco Central*.
- BIS. (2020). *Regulación de las criptomonedas: Evaluación de reacciones del mercado*.
- BIS. (2021). *Digital currencies and the future of the monetary system*.
- BIS. (2021). *Ready, steady, go? Results of the third BIS survey on central bank digital currency*.
- Conthe, M. (s.f.). *El Futuro Del Dinero*.
- Deloitte. (2020). *Are CBDCs the money of tomorrow?*
- Deloitte. (2021). *Corporates using crypto*.
- Deutsche Bank. (2021). *Historia de dos hermanas: Criptomonedas y CBDC*.
- Dinero, L. D., & Hayek, F. (1976).
- Domingo, C. (2019). *Todo lo que querías saber sobre Bitcoin, Criptomonedas y Blockchain y no te atrevías a preguntar*.
- Duttagupta, R., Fernandez, G., & Karacadag, C. (s.f.). *Transición hacia un tipo de cambio flexible*. Fondo Monetario Internacional.
- ECB. (2015). *Virtual currency schemes*.
- García Ruiz, J. (1992). *Patrón oro, banca y crisis*.
- Gigi. (2019). *21 Lessons*.
- Giovanoli, M. (2004). *International Monetary Law*.
- Haslam, P., & Lamberti, R. (2015). *When Money Destroys Nations*.
- Hayek, F. (1976). *La Desnacionalización del Dinero*.
- Hougan, M., & Lawant, D. (2021). *Cryptoassets: The guide to Bitcoin, Blockchain, and cryptocurrency for investment professionals*.

- Huerta de Soto, J. (1998). *Dinero, Crédito Bancario y Ciclos Económicos*.
- Isidro Nuñez, F., Guaita Martínez, J., & Carracedo Garnateo, P. (2018). *Las criptomonedas: Digitalización del dinero 2.0*.
- Jevons, W. S. (1875). *Money and the Mechanism of Exchange*.
- Jimenez, F. (1994). *Dinero, Inversión, Financiamiento Ahorro Financiero*.
- Kemmerer, E. W. (1944). *Gold and the Gold Standard: The Story of Gold Money, Past, Present and Future*.
- López Zafra, J. (2014). *Retorno al patrón oro*. DEUSTO.
- Menger, C. (1871). *Principios de Economía Política*.
- Menger, C. (1892). *El Dinero*.
- Menger, C. (s.f.). *Principios de Economía Política*.
- Molano, N. (2019). *Claves para entender la tecnología blockchain*. BBVA. Obtenido de <https://www.bbva.com/es/claves-para-entender-la-tecnologia-blockchain/>
- Morell, M. (2021). *An Analysis of Bitcoin's Use in Illicit Finance*.
- Nakamoto, S. (2008). *Bitcoin: A P2P Electronic Cash System*.
- Ocampo, J. A. (2017). *Resetting the International Monetary (Non)System*.
- Rajagopalan, S. (19 de 03 de 2021). India Bitcoin Ban Would Be a Terrible Idea. Obtenido de <https://www.bloomberg.com/opinion/articles/2021-03-19/bitcoin-ban-proposed-in-india-is-a-bad-idea>
- Rosembuj, T. (s.f.). *Bitcoin*. El Fisco.
- Schumpeter, J. (1954). *Historia del Análisis Económico*.
- Simon, J. (1986). *El último Recurso*.
- VanEck. (s.f.). Obtenido de <https://www.vaneck.com/es/en/>.