IEF *Trending Topics*

Número 1
Diciembre 2017

Bitcoin, las claves de su precio

Juan Barenys González

Stagee IEF 2017
Premio Extraordinario de Bachillerato

Damián Querol Bonet

Director Ejecutivo IEF
Dirección Académica
IEF *Trending Topics*

Miquel Noguer Alonso
Jordi Martínez Llorente

Referées

#IEF*TrendingTopics*

www.iefweb.org

INSTITUT D'ESTUDIS FINANCERS

Índice

Introducción

1. Qué son las criptodivisas?

1.1. Historia de las monedas, el patrón oro, el papel moneda y la aparación de los bancos centrales

2. Bitcoin

2.1. ¿Cómo funciona?

2.2. Blockchain

2.3. Bitcoin sobreviniendo algunas debilidades del papel moneda

2.3.1. Criptodivisas para democratizar el dinero

2.4. Controversias

3. Tipos de criptodivisas

4. Bitcoin: Oferta y demanda

4.1. Oferta

4.1.1. Diferenciación con las monedas tradicionales

4.1.2. Como se introducen nuevos Bitcoins en la economía

4.1.3. Oferta monetaria en el tiempo

4.1.4. Bitcoin "*mining*"

4.1.5. Bitcoin como una "*commoditiy*"

4.1.6. Estado actual

4.2. Demanda

4.2.1. Transacciones que afectan al precio de Bitcoin

4.2.2. Acceptación general de la moneda

4.2.3. Regulación del gobierno

- Índice bitlegal.io
- Unión Europea
- Estados Unidos
- Resto del mundo

4.2.4. Noticias de eventos afectando: factor reputacional

5. Bitcoin Cash

5.1. ¿Por qué una nueva criptodivisa?

5.2. Críticas y controversias

5.3. Estado actual

6. Conclusión

Anexo: Evolución en el precio de las principales criptodivisas

#IEFTrendingTopics

Introducción

Introducción

En los últimos tiempos, las **criptodivisas** se han erigido como un posible medio alternativo de pago e intercambio que ha llamado la atención de gobiernos, entidades financieras, empresas y del público en general. Este interés por las criptodivisas no parece haber disminuído y cada vez hay más gente que se pregunta si en poco tiempo podríamos hacer todas nuestras transacciones con este tipo de monedas.

Este documento pretende explicar de una manera sencilla las principales **características de las diferentes criptodivisas y algunos factores que afectan a su precio de mercado.**

El documento presenta la siguiente estructura:

En el **primer capítulo** se describirá **qué son las criptodivisas:** una historia de las monedas, el patrón oro, el papel moneda, las tarjetas de crédito y débito y finalmente la aparición de las criptodivisas. A continuación, se hará referencia a las ventajas de Bitcoin sobreviniendo algunas debilidades del papel moneda y los bancos centrales, para acabar hablando de una ventaja que ofrece Bitcoin: el acceso a liquidez por parte de algunos actores que hasta ahora tenían vetada.

En el **segundo capítulo** pasaremos a comentar específicamente de **Bitcoin**, mencionando dos de sus principales características: su funcionamiento como mediador en una transacción y la tecnología blockchain.

En el **tercer capítulo** se expondrán los **diversos tipos de criptodivisas** actualmente con una mayor capitalización de mercado. Se explicarán de manera breve las diferencias técnicas entre ellas y las mejoras que suponen respecto a Bitcoin.

En el **cuarto capítulo** se hace una distinción entre **factores que afectan a la oferta y la demanda de Bitcoin**, que puede ser extendido a una gran parte de las criptodivisas. En el caso de la oferta, se estudiarán las diferencias que ésta presenta con las monedas tradicionales; cómo se introducen nuevos Bitcoins en la economía; la característica de la oferta monetaria en el tiempo; la función de "minar"; el papel de Bitcoin como materia prima (*commodity*) y el estado actual de la oferta. En el caso de la demanda, se expondrán las transacciones que afectan a su precio, la aceptación general de la moneda y la regulación del gobierno. En este último apartado encontraremos una selección de las principales novedades regulatorias de diferentes países, clasificadas según si pertenecen a la Unión Europea, a Estados Unidos, o a otras áreas geográficas (Canadá, China, Japón). A continuación, un conjunto de noticias relevantes que han tenido relevancia histórica en el precio de la criptodivisa.

En el **quinto** y último capítulo se expondrá exclusivamente **Bitcoin Cash**, una nueva criptodivisa surgida originalmente de un *hard fork* [1] realizado en la red Bitcoin. Se hablará de las razones que llevaron a la creación de esta nueva divisa y también de algunas controversias y críticas en las cuales se ha visto involucrada.

1 Un hard fork o partición es el proceso que se da cuando hay un desacuerdo o un cambio de normas entre los usuarios de una criptodivisa y esta se divide en dos sistemas que operan paralelamente. Cuando esto ocurre, el ledger o libro mayor se replica en los dos lados. Para más información sobre hard fork ver "5. Bitcoin Cash" y sobre el ledger o libro mayor ver "2.2 Blockchain".

1.¿Qué son las criptodivisas?

1.1. Historia de las monedas, el patrón oro, el papel moneda y la aparición de los bancos centrales

Con el objetivo de contextualizar y entender mejor la aparición de Bitcoin, podría ser útil hacer un breve repaso histórico a lo que ha sido el comercio y su monetización a lo largo de los siglos. Se podría establecer una distinción histórica[1] entre **cinco sistemas de intercambio**. Se explicará cómo cada nuevo sistema ha sido una actualización del anterior y en qué medida lo ha mejorado. Estas categorías son: el **intercambio directo, las monedas de oro** o metales preciosos, el **papel moneda**, las **tarjetas de crédito y débito** y, la última de todas, las **criptodivisas.**

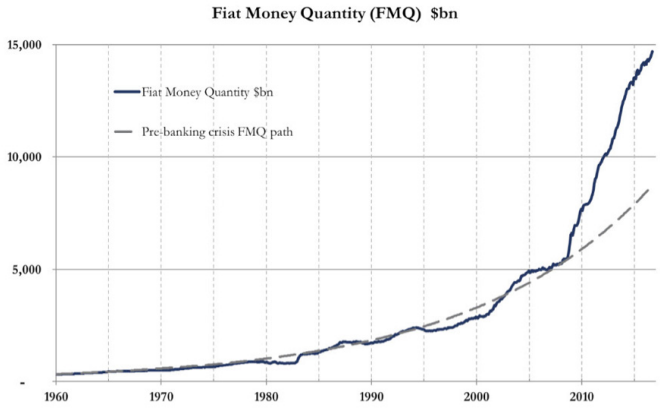
La primera de todas es el **intercambio**, es decir, intercambiar productos o servicios directamente con otros productos o servicios[2]. Éste era el sistema usado durante la Edad Antigua y Media: un individuo satisfacía sus necesidades (compraba un producto o servicio, por ejemplo, alguien que compraba grano) satisfaciendo él mismo las necesidades de otro (ofreciendo otro producto o servicio, por ejemplo, alguien que vendía los derivados de la leche que sus cabras generaban).

La segunda es la **aparición de la moneda de oro o metales preciosos**. El intercambio fue la forma dominante de comercio hasta el siglo I d.C., cuando tenemos constancia de la existencia de importantes y ampliamente aceptadas monedas, empezando por el *auerus* en la Antigua Roma. En los siglos sucesivos, la sucedieron como moneda de referencia en el comercio mundial el *sólido* en el Imperio Bizantino (siglos IV al XII), el *florín* de Florencia (siglos XIII al XV), el *florín alemán* o *gulden* (siglos XVII al XVIII), el *real de a ocho español* (siglos XVIII al XIX), el *pound inglés* (siglos XIX al XX) y finalmente el *dólar americano* (siglos XX hasta la actualidad)[3].

Algunas de estas monedas estaban hechas directamente de oro, plata y otros metales preciosos y su valor era intrínseco, es decir, la cantidad de oro, plata y otros materiales que constaba que contenían valía su equivalente en términos de la moneda. Por ejemplo, en tiempos del emperador Julio César, una unidad de *aurio* contenía en si misma 8 gramos de oro[4]. Por lo tanto, las podemos clasificar dentro del grupo de monedas hechas de metales preciosos, que contienen un valor intrínseco en sí mismas.

Otras de estas monedas mencionadas anteriormente pertenecían a la tercera categoría, pues fueron convertibles (al menos durante algún tiempo) a una **cantidad fija de oro**, en lo que se conocía como *sistema patrón oro* o *gold standard system*. Durante los años 20, por ejemplo, un dólar americano equivalía a 0,05 onzas de otro. El patrón oro estuvo vigente durante algunas décadas pero fue finalmente abandonado por todos los países a lo largo del siglo XX[5] .

En el siglo XVI, aparecieron los primeros **certificados escritos en papel** que equivalían a una cantidad fija de oro. Su plena implementación en el comercio internacional, sin embargo, no se consolidó hasta al cabo de 400 años[6].



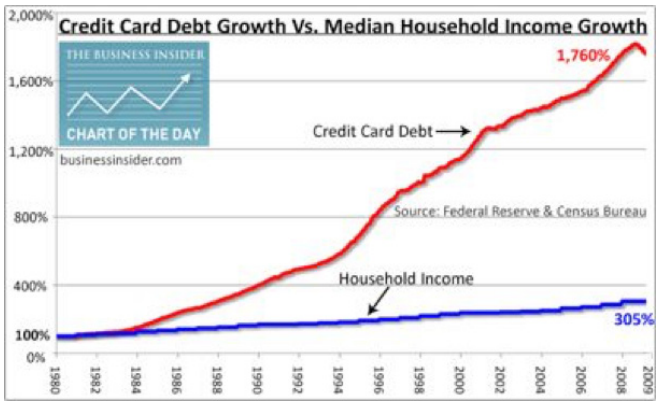
Fuente: St. Louis Fed (FRED), GoldMoney 1

1 Antonopoulos, A. M. (2014). Mastering Bitcoin (Second Edi). Sebastopol, CA: O'Reilly Media, Inc.
2 Smith, A. (2012). Wealth of Nations (English Ed).Wordsworth Editions Ltd.
3 Glyn, D. (2002). A History of Money: From Ancient Times to the Present Day (3rd Ed.). University of Wales Press.
4 Duncan-Jones, R. (1994). Money and Government in the Roman Empire. Cambridge University Press.
5 Mundell, R. A. (1997). Currency areas, common currencies, and EMU. American Economic Review, 87(2), 214.
6 Flandreau, M., & Jobst, C. (2009). The empirics of international currencies: Network externalities, history and persistence. Economic Journal, 119(537),

Es por eso que en las últimas décadas, el sistema predominante ha sido el del **papel moneda o *fiat currency***. En éste, los bancos centrales tienen el monopolio para ampliar o reducir la oferta monetaria, sin estar ligados a un tipo de cambio fijo con ningún valor (tampoco el oro). Por esta razón, en comparación con el patrón oro y otros, el valor de la moneda se basa exclusivamente en la confianza del público en que el banco central no ampliará demasiado la oferta monetaria con tal de que ésta mantenga su valor y no se deprecie, con el objetivo de alcanzar sus tres objetivos: servir de vehículo de intercambio, como unidad contable y como almacén de valor[7].

La cuarta categoría, las "**monedas de plástico**" son una actualización del último sistema de pago. A partir los años 80, en vez de intercambiar dinero en efectivo, también surge la posibilidad de pagar mediante un nuevo vehículo donde las entidades financieras, supervisadas por organismos gubernamentales y con un sistema contable centralizado, valida las transacciones que se realizan entre los diversos agentes. Es lo que se conoce como tarjetas de crédito o débito, dependiendo del uso contable que se les dé. En cualquier caso, los intercambios en tarjetas de crédito sólo afectan a la forma de pago, pues la moneda que se sigue usando es aquella provista por los bancos centrales.

Su total implementación fue más rápida que la del papel moneda. Sin embargo, aún se tardó unos años en ser un sistema de pago válido en muchos países del mundo[8].



Fuente: Federal Reserve & Census Bureau

Finalmente encontramos las **criptodivisas**, un nuevo sistema de pago que permite realizar transacciones de individuo a individuo (*peer-to-peer*) sin la necesidad de un sistema centralizado que valide la operación[9]. Pasaremos ahora a estudiar algunas características de Bitcoin, la primera criptodivisa que apareció y que actualmente tiene la mayor capitalización de mercado de todas las criptodivisas.

7 Asmundson, I., & Oner, C. (2012). What is money? Finance & Development, (September).
8 Calem, P. S., & Mester, L. J. (1995). Consumer Behavior and the Stickiness of Credit-Card Interest Rates. The American Economic Review, 85(5)
9 Ver "2.2 *Blockchain*"

Respecto a la **política monetaria**, como ha hecho notar el vicepresidente para la supervisión de la Fed, Randal Quarles[10], si el grado de aceptación de Bitcoin y otras criptomonedas sigue creciendo y, por lo tanto, también su uso, **podría suponer una amenaza para la política monetaria** de los bancos centrales, dado que el público utilizaría una moneda de la cual no pueden controlar su oferta.

Es por este motivo que ya hay propuestas para crear unas **criptodivisas controladas por los bancos centrales *(Central Bank Cryptocurrencies)*** en cuanto a su oferta pero donde la validación de las transacciones se realizara de forma descentralizada[11]. Es decir, mantener el componente del *ledger* descentralizado pero con una oferta de moneda controlada. La más famosa de estas propuestas es el *Fedcoin*[12], una CBCC controlada por la Reserva Federal de los Estados Unidos.

2. Bitcoin

2.1. ¿Cómo funciona?

Dado que Bitcoin es la criptodivisa con una capitalización de mercado más grande y la primera en aparecer[13], analizaremos a continuación su historia y su funcionamiento.

El usuario conocido como **Satoshi Nakamoto** (considerado el "padre fundador" del Bitcoin) introdujo las primeras 50 unidades de Bitcoin en circulación en el año 2009, esencialmente para demostrar que su método, basado en un sistema de blockchcain descentralizado, podía funcionar. La puesta en marcha de Bitcoin la realizaron voluntarios y entusiastas del mundo de la informática. El interés creció hasta el punto que Bitcoin comenzó a cotizar en 2010 en una bolsa japonesa online, Mt. Gox[14].

La mejor manera de explicar cómo se realiza una transacción en Bitcoins es comparándolo a cómo se hace con un sistema pago tradicional como las tarjetas de crédito.

10 Lam. E., (2017). What the World's Central Banks Are Saying About Bitcoin. Bloomberg.
11 Bech, M., (2017). Central bank cryptocurrencies. Bank for International Settlements.
12 Koning, JP., (2016). Fedcoin: A Central Bank-issued Cryptocurrency. R3 Reports.
13 Ver "3. Tipos de criptodivisas"
14 Trautman, L. (2007). Virtual Currencies; Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox? Richmond Journal of Law & Technology, 20(4).

Una **transacción que se realice con una tarjeta de débito o crédito ha de pasar forzosamente por un sistema centralizado** para que pueda ser validada y efectuada. Es decir, siempre interviene una tercera parte: o bien el propio banco y/o las empresas que fabrican las tarjetas (Visa, Mastercard, American Express…). Sin embargo, **en el caso de una criptodivisa,** por ejemplo el Bitcoin, **la validación de esta transacción se descentraliza en un sistema de libro mayor público fiscalizado por una red de ordenadores**[15].

En resumen, la principal ventaja que tiene una moneda como el Bitcoin respecto a cualquier otro medio de pago es que **se elimina completamente cualquier intermediario** y es este conjunto de ordenadores, y no una institución, quien valida la transacción[16].

En los párrafos siguientes se explica de una manera más amplia cómo funciona *blockchain* (la red de ordenadores que valida transacciones) y que es la que se usa en el caso de Bitcoin y otras criptodivisas[17].

2.2. *Blockchain*

Este sistema de libro mayor público mencionado anteriormente se llama *blockchain* y se podría resumir su funcionamiento de la siguiente manera.

En el caso de Bitcoin, su *blockchain* es una **base de datos distribuida, no centralizada en ningún punto, que se actualiza cada 10 minutos** con más datos e inputs. Cada *blockchain* es una base de datos en red, algo comparable a Internet pero más seguro, con un objetivo específico[18].

De esta manera, cualquier bloque (píldora de información dentro de una cadena de bloques: *blockchain*) que se une a la cadena del sistema **ha de ser validado**, es decir, ha de estar conforme con tota la información previa presente en la *blockchain*. Con cada nuevo bloque (transacción, actualización o dato), la cadena se actualiza completamente y es validada de manera descentralizada por todos los usuarios, cosa que la convierte en una herramienta de almacenaje muy segura.

La *blockchain* que sustenta la red bitcoin presenta diferentes mecanismos para evitar errores como el ***double spending*** (o prevención de que se gaste el mismo dinero en dos transacciones diferentes) y **el orden** con que las transacciones se realizan[19].

Especialmente respecto a este segundo aspecto, las transacciones en *blockchain* están protegidas por una "carrera matemática" que enfronta al atacante (aquel que quiere realizar una transacción en desacuerdo con las reglas de *blockchain*) con el resto de la red.

Una consecuencia de que los bloques se construyan uno encima del otro es que las transacciones al final de la cadena son más seguras, dado que el atacante habrá de superar la red durante una cantidad de tiempo más grande con tal de sustituir los bloques[20].

En definitiva, este elemento dinámico y su descentralización, permiten que esta tecnología sea **extremadamente eficiente almacenando datos ordenados en el tiempo** sin la posibilidad de poder revisarla o modificarla posteriormente. Sería altamente costoso o imposible rehacer toda la información previa contenida en *blockchain*. Los usuarios pueden tener más seguridad, transparencia y un mayor control sobre el flujo de datos[21].

Su principal ventaja es la posibilidad de validar transacciones entre dos partes, sin que ningún agente pueda actuar de manera oportunista, y sin que éstas tengan que ser validadas por un ente central.

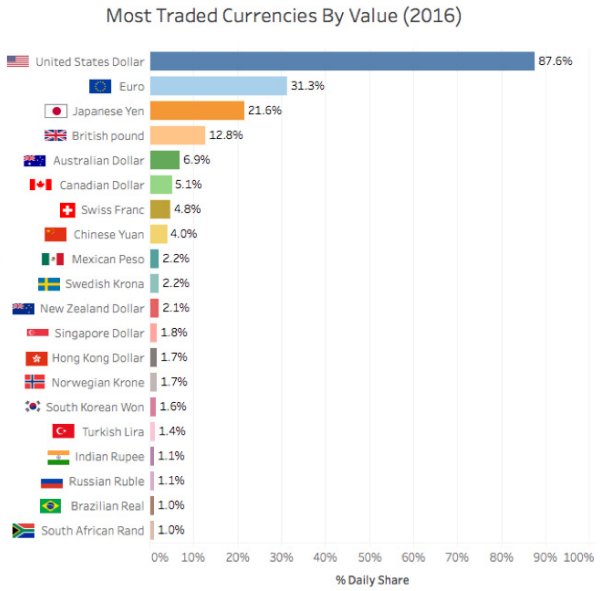
Esta **verificación descentralizada** nos ofrece un control sobre los datos previamente desconocido en Internet. De esta manera, podría compararse con transferir el mundo físico al mundo digital. Por ejemplo, podemos asegurarnos de que un usuario específico es el único beneficiario de Bitcoin y nadie más, de la misma manera que cuando entregamos un billete a alguien lo dejamos de tener nosotros y pasa a ostentarlo la otra persona.

La primera *blockchain* distribuida fue la conceptualizada por **Satoshi Nakamoto** para dar soporte y como principal estructura de la criptodivisa que él mismo creó, el Bitcoin. Más allá de Bitcoin se han creado **otras *blockchains***, en plataformas como Airbnb, en el mercado de la electricidad, en el mercado inmobiliario… todas ellas con el objetivo de registrar y validar transacciones de una forma descentralizada[22].

15 Ver "2.2 *Blockchain*"
16 How does Bitcoin work? (April 11th 2013). The Economist. http://money.cnn.com/infographic/technology/what-is-Bitcoin/
17 Ver "2.2 *Blockchain*"
18The great chain of being sure about things (October 31th 2015). The Economist.
19 Driscoll, S. (2013). How Bitcoin Works Under the Hood. http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html
20 Driscoll, S. (2014) The Essence of How Bitcoin Works. http://www.imponderablethings.com/2014/09/the-essence-of-how-bitcoin-works-non.html
21 Grinberg, R., Primer, B., Ecosystem, B., Sustainable, I. B., & Issues, L. (2012). Bitcoin: an innovative alternative digital currency. Hastings Sci. & Tech
22 Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton: Princeton University Press.

2.3. Bitcoin sobreviniendo algunas debilidades del papel moneda

Éste último sistema donde los bancos centrales son los únicos autorizados para imprimir papel moneda es hoy en día el mayoritariamente vigente en todos los países. El *Bank of International Settlements (BIS)* elaboró un informe el año 2016, donde afirmaba que cada día se realizan transacciones en **monedas controladas por los bancos centrales** (la más importante de ellas: el dólar) **por valor de 5,1 trillones de dólares frente a los $100 millones realizadas en Bitcoin**[23].

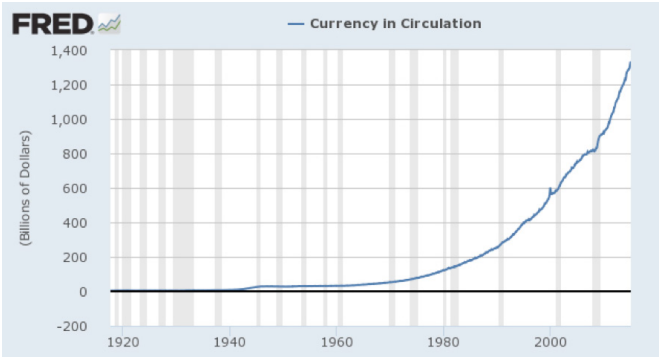


Fuente: Bank for International Settlements (BIS)

Cabe recordar que una gran parte de estas monedas que a lo largo de la historia se han implementado bajo el control de los bancos centrales han perdido casi todo su valor[24].

Tal y como veremos posteriormente, **en el caso de Bitcoin la oferta de moneda presenta unas características especiales:** la forma en que se produce el aumento de la oferta monetaria en el caso de Bitcoin es una de las grandes diferencias que la criptodivisa presenta respecto a sus predecesores[25].

Es por este motivo que algunos analistas han coincidido en señalar que **la política monetaria expansiva llevada a cabo por los bancos centrales en las décadas posteriores a la crisis ha favorecido la aparición de las criptodivisas**, puesto que ésta ha contribuido a la progresiva pérdida de credibilidad que las monedas tradicionales han experimentado[26].



Fuente: Board of Governors of the Federal Reserve System (US)

David Lee Kuo Chen, del Sim Kee Boon Institute for Financial Economics, se refiere en su libro "Handbook of Digital Currencies" a este fenómeno[27].

Expone cómo las criptodivisas han captado la atención de muchos inversores en un momento en el que la política de expansión monetaria llevada a cabo por los bancos centrales de todo el mundo ha hecho **subir el precio de los activos**. Dado que la reversión de esta política monetaria presentaba un alto grado de incertidumbre respecto a sus consecuencias, las criptodivisas han despertado el interés de aquellos que no se sentían cómodos con una moneda nacional soportada por una gran cantidad de deuda, en vez de activos.

Por otro lado, es prudente a la hora de determinar si Bitcoin se convertirá o no en una moneda de referencia, dado que actualmente es esencialmente un activo especulativo en tanto que ningún bien o servicio se valora principalmente en Bitcoin. Los inversores, pues, tendrían Bitcoin como un activo y su apreciación descansaría en la expectativa de que se convertiría en un medio de intercambio establecido.

Es cierto que, comparada con la volatilidad del dólar o el euro, los volúmenes de volatilidad en el mercado de Bitcoin son preocupantes, pues históricamente han podido disponer de monedas más estables. Sin embargo, en países de América Latina como Venezuela o Brasil, la moneda de los cuales experimenta volatilidades superiores o similares pero con una pérdida de valor constantec[28], este factor no será disuasorio para su uso. Se podría decir, por lo tanto, que la volatilidad es relativa.

23 Bank for International Settlements (2016). Triennial Central Bank Survey.
24 Helleiner E. (2003). The Making of National Money: Territorial Currencies in Historical Perspective . Cornell University Press.
25 En el capítulo"4.1 Oferta de Bitcoin" se explicará con más detalle cuáles son estas características y como diferencian Bitcoin del papel moneda.
26 European Central Bank ECB (2012). Virtual Currency Schemes. www.ecb.europa.eu
27 Lee Kuo Chen, D. (2015). Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments and Big Data. Sim Kee Bon Institute for Financial Economics, Singapore Management University.
28 Reuters (2017). Venezuela's January-September inflation 536 percent: National Assembly. https://www.reuters.com/article/us-venezuela-economy/venezuelas-january-september-inflation-536-percent-national-assembly-idUSKBN1CB25L

2.3.1 Criptodivisas permitiendo el acceso a liquidez

Otra de las funciones importantes de las criptodivisas que algunos autores ponen en valor es la **capacidad de estas para permitir el acceso a liquidez** y financiación a actores que previamente no tenían. Esto se debe al funcionamiento de las transacciones en criptodivisas que, como veremos posteriormente, consisten únicamente en un contrato privado entre dos partes, que permite el intercambio entre individuos eliminando cualquier intermediario[29].

Podemos ilustrarlo con dos ejemplos concretos que lo corroboran:

1) En el año 2012, **PayPal** bloqueaba el acceso a usuarios de más de 60 países del mundo, que no podían pagar ni cobrar con este mecanismo. A su vez, un gran número de entidades financieras presentaban restricciones similares. Es por esta razón que **Wordpress**, la plataforma líder en servicios de blogging y alojamiento web, emitió en noviembre de ese mismo año un comunicado donde se decía que *"no encontramos justo que un bloguero de Haití, Etiopía o Kenia tenga un acceso restringido a la blogosfera debido a la imposibilidad de recibir pagos".*

Por este motivo **permitieron pagar a los blogueros en Bitcoins** dado que era *"una moneda digital que, al no tener ninguna autoridad central, no hay manera de bloquear el acceso a países que se encuentran fuera de esta red"*[30].

2) Aún otro ejemplo, en Afganistán, donde las mujeres siguen sin poder tener cuentas bancarias propias. Si alguna vez una mujer llega a ganar dinero ha de transferirlo obligatoriamente y por ley a la cuenta de su marido, padre o hermano. Esto supone unos costes de transacción enormes incluso para enviar pequeñas cantidades de dinero. **Film Annex**, una institución educativa artística que paga cada año a 300.000 blogueros voluntarios que contribuyen a su blog, consciente de las dificultades de estas colaboradoras, **empezó a utilizar Bitcoin para poder pagar a las contribuidoras afganas**[31].

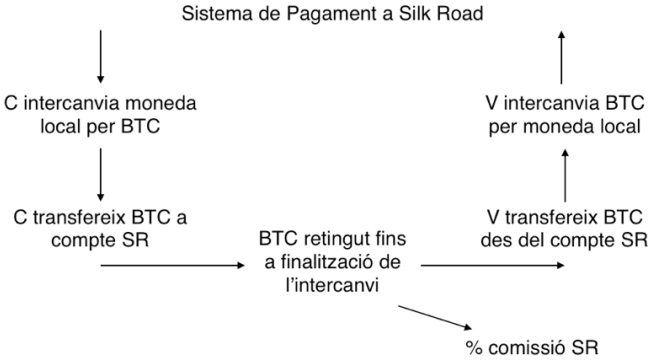
Hemos visto algunas de las buenas intenciones y el éxito que han tenido las criptodivisas a la hora de permitir el acceso a la liquidez a algunos agentes concretos que de otra manera lo tendrían más difícil. En contraste, veremos ahora algunas controversias en que la criptodivisa se ha visto involucrada.

29 Ver 2.2 *Blockchain*
30 Skelton, A. (2012). Pay Another Way: Bitcoin. Retrieved from https://en.blog.wordpress.com/2012/11/15/pay-another-way-Bitcoin/
31 Vigna P., Casey M.J., (2015), Cryptocurrency: How Bitcoin and Digital Money are Challenging the Global Economic Order, Random House Group

2.4. Controversias

Uno de los principales y primeros usos de Bitcoin fue como moneda en el mercado negro de drogas ilegales. **The Silk Road**[32] era uno de los principales sitios web donde estas operaciones se realizaban.

El FBI cerró la web en octubre de 2013 y arrestó a su fundador, Ross William Ulbricht, acusado de esconderse tras el pseudónimo "Dreat Pirate Roberts"[33].



Fuente: Elaboración propia basada en Christin, N. (2013) "Traveling the silk road"

Una moneda que **permite el anonimato completo** también puede ser usada para este tipo de transacciones[34]. Más allá de Silk Road también se ha tenido constancia del uso de Bitcoins y otras criptodivisas en la compra de armas[35], pornografía[36] y para financiar grupos terroristas[37].

32 Christin, N. (2013). Traveling the silk road. In Proceedings of the 22nd international conference on World Wide Web - WWW '13 (pp. 213–224).
33 Anderson, N., & Farivar, C. (2013, March 10). How the feds took down the Dread Pirate Roberts. Ars Technica.
34 Barratt, M. J. (2012). Silk road: Ebay for drugs. Addiction.
35 Rizzo, P. (2014). 25-Year-Old Arrested After Selling Gun for Bitcoin on Black Market. Coindesk.com. Retrieved from
36 Kelly, J. (2016). New partnership aims to clamp down on use of Bitcoin for child porn. Reuters. Retrieved from
37 Maxey, L. (2017) Terror Finance in the Age of Bitcoin. The Chiper Brief.

3. Tipos de criptodivisas

En este capítulo se explicarán y se definirán las **principales criptodivisas en funcionamiento actualmente,** ordenadas de mayor a menor capitalización de mercado. Tal y como se podrá observar, la mayoría son criptodivisas surgidas de la evolución y mejora de algunas características concretas de Bitcoin o de sus funciones.

En la seguiente tabla se muestra la **capitalización de mercado** y el **precio relativo** de las criptodivisas con una capitalización de mercado más grande[38]. (A fecha 20 de diciembre de 2017). Anexo a este documento se pueden encontrar la evolución en el precio de estas criptodivisas.

Nombre	Capitalización de Mercado	Precio Unitario
Bitcoin	$285.972.461.448	$17.069,90
Ethereum	$78.328.229.616	$812,08
Bitcoin Cash	$58.115.262.343	$3.445,70
Ripple	$29.778.548.209	$0,768694
Litecoin	$17.946.928.649	$329,98
Dash	$10.241.202.500	$1.319,05

3.1 Ethereum (ETH)

Apareció en el año 2015. Podemos definir Ethereum como una plataforma descentralizada que ofrece dos servicios principales: por un lado, **Smart Contracts** (contratos, la validación de los cuáles, la hace una red descentralizada) y **Dapps** (aplicaciones que usan *blockchain*). Este sistema desincentiva de una manera efectiva el fraude, el control o la interferencia de cualquier tercera parte[39].

Es posiblemente la criptodivisa más alejada de Bitcoin respecto a similitudes en sus características. Las aplicaciones funcionan con una moneda que es específica de Ethereum: el ether. Uno de los hechos más destacados de Ethereum es su partición en Ethereum (ETH) y Ethereum Classic (ETC). Es la criptodivisa que presenta una mayor capitalización de mercado después de Bitcoin.

3.2 Bitcoin Cash

A mediados de Julio de 2017, las principales compañías mineras de Bitcoins y otros agentes, que en ese momento representaban aproximadamente un 80-90% de toda la energía de computación (es decir, la energía necesaria tanto para realizar las validaciones propias de *blockchain* como para minar nuevos Bitcoin), votaron para incorporar una tecnología a Bitcoin llamada "*segregated witness*" (sabiduría segregada). Ésta hace que sea necesario verificar una menor cantidad de información en cada bloque de la cadena *blockchain*[40]. En otras palabras, que cada píldora de información de *blockchain* presentara una menor cantidad de contenido y por lo tanto fuese necesaria menos energía para procesarla.

Al mismo tiempo, otros mineros y desarrolladores creían que "*segregated witness*" no respondía al problema fundamental de Bitcoin, y por eso decidieron crear Bitcoin Cash. Éste se caracteriza, a diferencia de Bitcoin, por tener unos **bloques de un tamaño más grande en la cadena de *blockchain***, con un nivel ajustable de dificultad para asegurar la supervivencia de la cadena, así como del proceso de verificación de las transacciones[41].

3.3 Ripple

Ripple se define como una plataforma que permite realizar pagos con un coste muy bajo y en tiempo real. Fue lanzada en 2012.

Una de las principales diferencias que presenta con Bitcoin (que usa *blockchain* para validar las transacciones), es el sistema de ***consensus ledger*** (es decir, libro mayor de consenso[42]). En éste, a diferencia de Bitcon, no se mina, es decir, no se produce un aumento de la oferta monetaria mediante la resolución de algoritmos. Esto hace que se reduzca mucho la cantidad de energía utilizada[43].

3.4 Litecoin

Apareció en el año 2011 y fue una de las primeras criptodivisas que se implementaron en el mercado a parte de Bitcoin. Litecoin se basa en una red global de pago en línea que no está controlada por ninguna autoridad central y usa ***"Scrypt"* como un sistema de *"proof of work"***. El *proof of work* (sistema de prueba de trabajo) es una sistema que, para evitar comportamientos indeseados (por ejemplo ataques de denegación de servicio o spam) requiere que el cliente del servicio realice algún tipo de trabajo que tenga cierto coste y que sea verificado fácilmente en la parte del servidor.

38 CoinMarketCap coinmarketcap.com
39 Ethereum White Paper. A Next-Generation Smart Contract and Decentralized Application Platform. (2017). Github.
40 Song, J. (2017). Bitcoin Cash: What You Need To Know. Medium.
41 CoinTelegraph (August 7, 2017) Bitcoin Cash Posts Lacklustre Recovery
42 Una explicación más amplia en "2.1: Cómo funciona?" y "2.2: *Blockchain*".
43 Ripple White Paper. Correction to Ripple White Paper. (2015) https://ripple.com/dev-blog/correction-to-ripple-white-paper/

Normalmente el trabajo consiste en realizar un cómputo en el ordenador del cliente[44].

Aunque Litecoin presenta muchas similitudes con Bitcoin, es más rápida a la hora de generar bloques nuevos en su cadena de *blockchain*, y por lo tanto, confirma las transacciones de manera más rápida.

3.5 Dash

Dash (conocida originalmente como Darkcoin) ofrece una ventaja principal respecto a Bitcoin: **el anonimato.** De acuerdo con los expertos, es más difícil seguir una transacción realizada en Dash que en Bitcoins. Fue lanzada en 2014 y rápidamente adoptada por una gran número de usuarios.

En marzo de 2015, Darkcoin cambió su marca a DASH, como las siglas de "digital cash"[45]. La principal diferencia con Bitcoin es su sistema de validación de transacciones, que funciona de manera más rápida y más anónima.

4. Bitcoin: Factores de Oferta y Demanda

A continuación, una tabla que muestra de manera resumida los factores que afectan a la oferta y a la demanda de Bitcoins:

Factores que afectan la oferta	Factores que afectan la demanda
Oferta determinada algorítmicamente (sistema de minería)	Transacciones realizadas
	Aceptación general de la moneda
	Regulación del gobierno
	Noticias de eventos

4.1 Factores de Oferta de Bitcoin

4.1.1 Diferenciación con las monedas tradicionales

Tal como se ha expuesto anteriormente, no hay ningún ente central que regule la oferta de Bitcoin. Ningún gobierno ni ninguna autoridad centralizada, como pasa con las monedas tradicionales, puede manipular la oferta de Bitcoins. En su lugar, la moneda es gobernada por unas **normas criptográficas** que son hechas cumplir por una red descentralizada de ordenadores.

Paradójicamente, ya podemos saber exactamente la oferta de Bitcoin en cualquier momento del tiempo, sin saber cuál será la demanda. A diferencia de los bancos centrales, que intentan ajustar la oferta de moneda dependiendo de su demanda, esta manera de ofrecer Bitcoin se encuentra totalmente apartada de "escuchar" la demanda[46]. En otras palabras, **la oferta de Bitcoin sigue ampliándose de la misma manera independientemente de cuál sea la demanda en aquel momento.**

Por lo tanto, ya hay un primer factor a destacar: **la oferta de moneda no está sometida a ningún banco central ni gobierno**, sino al propio sistema, que crea nueva oferta mediante un **algoritmo matemático.**

4.1.2 Cómo se introducen nuevos Bitcoin en la economía

La oferta de Bitcoin se determina algorítmicamente[47]. Se basa en una función de oferta descendiente geométricamente.

Estos Bitcoins son dados como recompensa en un modelo de seguridad, basado en la teoría de juegos, que asegura que cada transacción es validada independientemente por actores completamente anónimos, que han de proveer electricidad como garantía de la acción de seguridad que han de realizar. **Si realizan satisfactoriamente la tarea de seguridad de validar transacciones, ganan, como recompensa basada en la probabilidad, esta cantidad de Bitcoins.**

En la siguiente tabla se muestran, por éste orden, las fechas, el número de bloque, el período, el número de Bitcoins contenidos en cada bloque, la estimación del año, el número de Bitcoins al inicio del período, el número de Bitcoins añadidos, el total de Bitcoins, el porcentaje de incremento que supone respecto al período anterior, y el porcentaje sobre el total de Bitcoin[48].

Date reached	Block	Reward Era	BTC/block	Year (estimate)	Start BTC	BTC Added	End BTC	BTC Increase	End BTC % of Limit
2009-01-03	0	1	50.00	2009	0	2625000	2625000	infinite	12.500%
2010-04-22	52500	1	50.00	2010	2625000	2625000	5250000	100.00%	25.000%
2011-01-28	105000	1	50.00	2011*	5250000	2625000	7875000	50.00%	37.500%
2011-12-14	157500	1	50.00	2012	7875000	2625000	10500000	33.33%	50.000%
2012-11-28	210000	2	25.00	2013	10500000	1312500	11812500	12.50%	56.250%
2013-10-09	262500	2	25.00	2014	11812500	1312500	13125000	11.11%	62.500%
2014-08-11	315000	2	25.00	2015	13125000	1312500	14437500	10.00%	68.750%
2015-07-29	367500	2	25.00	2016	14437500	1312500	15750000	9.09%	75.000%
2016-07-09	420000	3	12.50	2016	15750000	656250	16406250	4.17%	78.125%
2017-06-23	472500	3	12.50	2018	16406250	656250	17062500	4.00%	81.250%
	525000	3	12.50	2019	17062500	656250	17718750	3.85%	84.375%
	577500	3	12.50	2020	17718750	656250	18375000	3.70%	87.500%
	630000	4	6.25	2021	18375000	328125	18703125	1.79%	89.063%
	682500	4	6.25	2022	18703125	328125	19031250	1.75%	90.625%
	735000	4	6.25	2023	19031250	328125	19359375	1.72%	92.188%
	787500	4	6.25	2024	19359375	328125	19687500	1.69%	93.750%

Fuente: Bitcoin.it/wiki

44 Lee, C. (2011). LiteCoin.

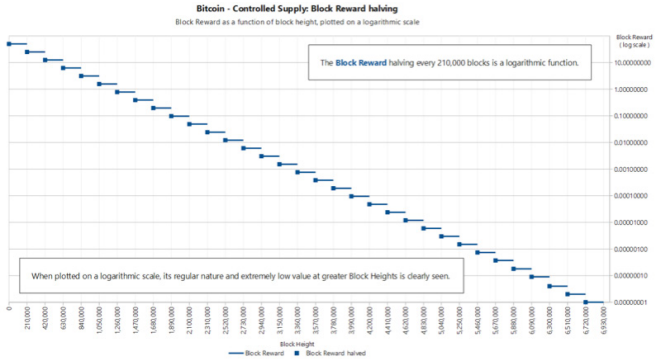
45 Duffield, E., & Diaz, D. (2014). Dash: A privacy-centric crypto-currency.

46 Ver "4.1.2 Cómo se introducen nuevos Bitcoin en la economía"

47 Antonopoulos, A. M. (2014). Mastering Bitcoin (Second Edi). Sebastopol, CA: O'Reilly Media, Inc.

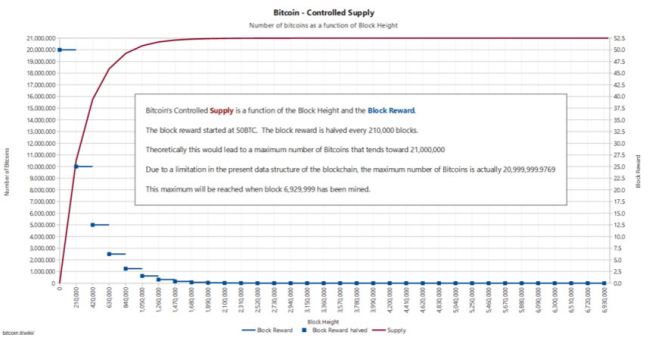
48 Yermack, D. (2015). Is Bitcoin a Real Currency? An Economic Appraisal. In Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data.

Aplicando una escala logarítmica a la recompensa en cada bloque como función del tamaño de este bloque, obtenemos el siguiente gráfico:



Fuente: Bitcoin.it/wiki

En el siguiente gráfico se puede apreciar claramente por qué a la función de oferta de Bitcoin se le llama "función de oferta descendiente geométricamente[49]."



Fuente: Bitcoin.it/wiki

Tal como se constata en el gráfico anterior, el número máximo de Bitcoins en circulación llegará a los 21 Millones. Cabe destacar, del anterior gráfico, el hecho de que 21 millones es una cantidad de Bitcoins **asintótica**. En otras palabras, nunca llegará a haber un total de 21 millones de Bitcoin en circulación, es la asíntota a la que la función tiende.

El **algoritmo** que define esta función se expresa matemáticamente de la siguiente forma:

$$\frac{\sum_{i=0}^{32} 210000\lfloor\frac{50.10^8}{2^i}\rfloor}{10^8}$$

El funcionamiento es, por lo tanto, bastante simple. **El sistema sabe exactamente qué cantidad de Bitcoin ha de haber en circulación en cada momento.** Por tanto, con tal de ampliar la oferta de Bitcoins, los diferentes participantes en el mercado tienen la opción de "minar", es decir, poner una computadora a trabajar para resolver un complicado algoritmo. Si la computadora consigue resolverlo, lógicamente se queda el Bitcoin.

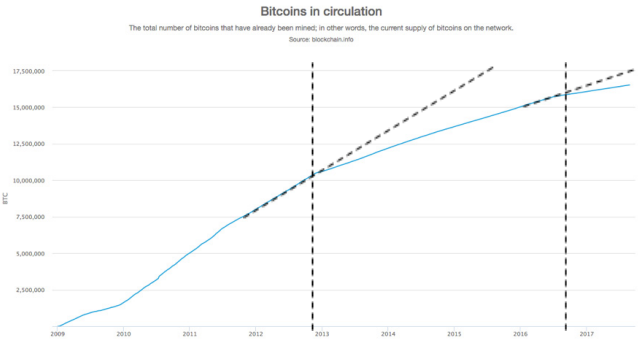
Metafóricamente, sería como si cada ordenador fuese un minero y se le repartiesen diferentes bloques de roca para minar. Éste los mina y si encuentra un Bitcoin en ellos se lo queda. Cuando haya muchos mineros, obviamente cada bloque de roca tendrá menos posibilidades de contener un Bitcoin, dado que lo que no puede pasar es que se incremente la ratio al que crece la oferta de Bitcoin[50].

A este último planteamiento hay que añadirle, como se muestra a continuación, el hecho de que cada 4 años la oferta de Bitcoin en cada bloque se divide entre dos.

4.1.3 Oferta monetaria de Bitcoins en el tiempo

La oferta monetaria se ajusta en el tiempo de la siguiente manera. **Cada 4 años, el número de Bitcoin contenidos en cada bloque se reduce a la mitad.** Por ejemplo, pasaron de 50 a 25 en noviembre de 2012 y de 25 a 12.5 en Julio de 2016.

Se puede observar claramente en el gráfico: la inclinación de la curva de oferta cambia substancialmente cada 4 años (en noviembre de 2012 y en Julio de 2016) para pasar a reducirse a la mitad.



Fuente: Coindesk.com

4.1.4 Bitcoin mining

En los últimos años, hemos tenido noticia de diversas "granjas" de minería con una gran cantidad de ordenadores que minan constantemente con tal de obtener Bitcoins[51].

49 Fuente: Coin Telegraph

50 Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 8437).

51 Kroll, J. a, Davey, I. C., & Felten, E. W. (2013). The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. The Twelfth Workshop on the Economics of Information Security (WEIS 2013), (Weis), 1–21.

Tal y como se explica el artículo referenciado, los "mineros" son **recompensados de dos formas: por su función de validar transacciones y por la actividad de minar.**

Los beneficios que genera esta actividad son cada vez menores en el número de Bitcoins obtenidos. En 2009, un ordenador podía conseguir hasta 200 Bitcoin en pocos días. En 2014, cuando el precio había ascendido a los $900, un solo ordenador tardaría hasta 98 años en conseguir un Bitcoin.

Esto es debido principalmente a la cantidad de mineros que hay en el mercado. Como hemos explicado, la oferta de Bitcoin es limitada y se determina algorítmicamente, su curva de crecimiento ya ha sido determinada previamente y por tanto, no se puede modificar. Por lo tanto, el hecho de que haya muchos mineros trabajando, reduce substancialmente la probabilidad de que un bloque contenga la cantidad Bitcoins deseada.

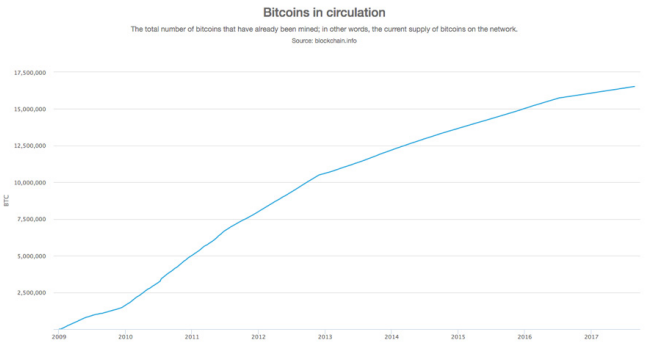
4.1.5 Bitcoin como una "*commodity*": por qué la oferta se parece al oro y los metales preciosos

Al tratarse de una moneda con una oferta creciente pero con una curva de crecimiento predeterminada algorítmicamente, como acabamos de ver en el apartado inmediatamente anterior, hace que se pueda equiparar Bitcoin con, por ejemplo, el oro. Hay una cantidad limitada de oro en el mundo y su oferta se amplía muy lentamente en el tiempo. Es por este motivo que se puede hablar más de **Bitcoin como una *commodity* o materia prima** que no como una moneda[52].

En el mercado del oro, donde muy pocas cantidades de oro se introducen cada año[53], **el precio varía mayoritariamente según su demanda y no según su oferta, puesto que esta se mantiene bastante estable en el tiempo.**

4.1.6 Estado actual

Ya conocemos el total de Bitcoin que se ofrecerán a lo largo de la historia: 21 millones de Bitcoins en el año 2140. De estos 21 millones de Bitcoins, tal y como muestra el gráfico, ya se han minado aproximadamente 15,7, es decir, el 75% del total[54].



Fuente: Coindesk.com

4.2 Factores de Demanda de Bitcoin

Uno de los aspectos importantes que explica por qué el precio de Bitcoin no ha hecho más que aumentar es una diferencia fundamental entre la demanda y la oferta de esta criptodivisa: **mientras la oferta de Bitcoin en el tiempo,** como hemos visto, **es limitada y su crecimiento disminuye** (cada vez se introducen menos cantidades de Bitcoin en la economía), **la demanda**, al menos en los últimos años, **no ha parado de aumentar** debido a los factores que veremos a continuación.

4.2.1 Transacciones que afectan al precio de Bitcoin

Más allá de las características propias de la oferta y la demanda de Bitcoin, una principal distinción que hay que hacer es en el **tipo de transacción que se realiza mediante Bitcoin**, para ver cuales condicionaron **realmente el precio de Bitcoin.** De acuerdo con el analista de mercados Venzen Khaosan, se pueden clasificar en dos grandes grupos[55]:

En primer lugar, tendríamos aquellas **transacciones donde dos usuarios de Bitcoin**, tanto el vendedor como el comprador, **realizan una transacción**. En este caso, como que los dos usan Bitcoin tanto para pagar como para cobrar, no ha hecho falta ninguna conversión de Bitcoin hacia otra divisa. Al no haber tenido que intercambiar Bitcoin por otra divisa, el precio del mismo no se ha visto afectado. **Este primer grupo de transacciones no afectan al precio de Bitcoin.**

En segundo lugar, cuando **uno de los dos agentes no es usuario de Bitcoin**, el precio sí se verá afectado, dado que **o bien el comprador o el vendedor tendrán que recurrir al mercado de Bitcoin para realizar la transacción.** En caso de realizar una compra, el comprador tendrá que ir al mercado de Bitcoin e intercambiarla por otra divisa, hecho que hará subir el precio de la misma, pues está ampliando la demanda.

52 Bergstra, J., & Weijland, P. (2014). Bitcoin: a money-like informational *commodity*. arXiv Preprint arXiv:1402.4778, (Mlic), 1–26. Retrieved from

53 Domanski, D., & Heath, A. (2007). Financial investors and *commodity* markets. BIS Quarterly Review, (March).

54 Fuente: *blockchain*.info

55 What Affects Bitcoin Price? (2014). CryptoCoin News.

En caso contrario, si lo que se quiere es vender Bitcoin fruto de la venta, el precio de mercado de Bitcoin tenderá a bajar, pues se estará ampliando la oferta.

Una ejemplificación del primer caso sería cuando un usuario que ya ostenta Bitcoin en su cartera compra un producto en Shopify, una plataforma de comercio electrónico que acepta Bitcoin como método de pago. Ni el comprador ni el vendedor han intercambiado Bitcoin por otra divisa, por lo tanto, el precio de Bitcoin no se ha visto afectado.

Una ejemplificación del segundo caso sería cuando un usuario aún no ostenta Bitcoin en su cartera y quiere comprar el mismo producto en Shopify[56]. En este caso, el comprador intercambiará, por ejemplo, euros por Bitcoin. Al ampliar la demanda de bitcoin, el precio unitario de Bitcoin tenderá a subir.

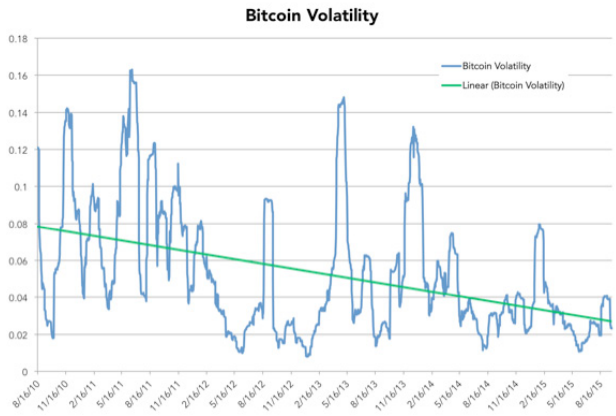
Entre los eventos que **no hacen subir sino bajar la demanda se encuentran**, según el mismo autor: **los vendedores que aceptan Bitcoin y que intercambian la moneda por otra divisa** haciendo bajar su precio, **los mineros "cashing out"** para pagar los gastos con monedas tradicionales y la conversión total o parcial de los **salarios pagados en Bitcoin a otras monedas.**

4.2.2 Aceptación general de la moneda

Como en cualquier activo, uno de los factores que hace que el precio del activo suba es el **incremento de demanda o expectativa de incremento de demanda** por parte del mercado. Si el mercado anticipa que Bitcoin se podría convertir en un activo o moneda de referencia en un futuro a la hora de realizar transacciones, el precio de Bitcoin subirá[57].

El precio relativo de Bitcoin se determina exactamente de la misma forma como se determina el **precio relativo** del euro, la libra esterlina, el yen o el dólar americano: a través de un mercado donde la oferta y la demanda fijan su precio[58].

Es cierto que se han observado episodios de fuertes subidas y bajadas en su precio[59]. Sin embargo, si observamos la tendencia a largo plazo, dado que el volumen de transacciones desde el año 2013 y 2014 ha crecido, la capitalización de mercado también ha crecido, y por lo tanto la volatilidad no ha parado de disminuir, de media[60].



Fuente: Btcvol.info

4.2.3 Regulación gubernamental

La **regulación** que se le aplica a la tecnología *blockchain* que es usada por una gran parte de las criptodivisas es relevante como factor de demanda en tanto que **muchas de estas criptodivisas se pro-claman como un activo libre de impuestos y, por lo tanto, del control de los gobiernos**[61].

Si se demuestra, por lo tanto, inevitable la intromisión de entes reguladores en este tipo de transacciones, las criptodivisas tenderán a bajar de precio, puesto que según se demuestra, uno de sus principales atractivos es la hipotética imposibilidad por parte de los órganos reguladores de seguirla.

Kevin V. Tu, de la *University of Maryland Francis King Carey School of Law, y Michael W. Meredith del United States District Court for the Western District of Texas* han escrito uno de los papers más influyentes respecto a la regulación de Bitcoin[62].

Los autores exponen cómo, inicialmente, bitcoin y el resto de criptodivisas "escaparon" del control de los órganos reguladores, pero que eso **ha ido cambiando a medida que crecía su popularidad.**

Explican cómo justo después de su creación, Bitcoin operó libremente, sin ninguna regulación establecida. La popularidad de Bitcoin, sin embargo, forzó a los órganos legales y reguladores tanto nacionales como internacionales a medir los potenciales riesgos-de una divisa descentralizada cada vez más popular.

Como resultado, la respuesta legal y reguladora ha sido muy diferente en los diferentes países.

56 shopify.com/Bitcoin
57 Kristoufek, L. (2015). What are the main drivers of the Bitcoin price? Evidence from wavelet coherence analysis. PLoS ONE, 10(4).
58 Antonopoulos, A. M. (2014). Mastering Bitcoin (Second Edi). Sebastopol, CA: O'Reilly Media, Inc.
59 Cheng, E. (2017) Bitcoin plunges 18% after topping $11,000 in extremely volatile trading. CNBC.
60 Ver gráfico

61 Twomey, P. (2013). HALTING A SHIFT IN THE PARADIGM: THE NEED FOR BITCOIN REGULATION. Trinity C.L. Rev, 1(16).
62 Tu, Kevin V. and Meredith, Michael W., Rethinking Virtual Currency Regulation in the Bitcoin Age (August 22, 2014). Washington Law Review, Vol. 90, 271-347, 2015

Uno de los elementos a tener en cuenta es el hecho de que Bitcoin es un **activo completamente nuevo que la legislación no contemplaba a la hora de regular,** y que por tanto, no encaja dentro de los esquemas reguladores previos a su aparición.

Los **intentos de categorizar Bitcoin** conllevan muchos problemas. En un plano muy general, la discusión se centra entre categorizar Bitcoin **como una moneda** o divisa o, por el contrario, **como una propiedad.** A pesar de que Bitcoin presenta similitudes con las dos, sus características únicas harían que hiciese falta una regulación totalmente nueva.

Los **tres problemas principales** que el legislador se encuentra a la hora de abordar este activo tienen que ver con tres características básicas que las criptodivisas presentan: **1) la inexistencia de un ente centralizado, 2) el anonimato y 3) la susceptibilidad al robo.** El hecho de no tener un ente centralizado hace que éste no pueda implementar leyes impuestas por el regulador ni facilitar información.

Los autores también destacan que un componente muy importante de la regulación financiera tiene que ver con la **capacidad del regulador para imponer requerimientos a una entidad centralizada y que éstos sean implementados.** Dado que Bitcoin no tiene una entidad centralizada que pueda implementar, por ejemplo, leyes contra el blanquero de capitales, tampoco puede monitorizar o reportar actividad sospechosa o aceptar y procesar requerimientos legales similares.

El anonimato también dificulta la provisión de información al órgano regulador. Normalmente, los métodos de pago identifican cada transacción con información personal de los usuarios. El factor anónimo que Bitcoin presenta hace que, incluso para los intermediarios, sea difícil informar de la identidad de aquellos que realizan las operaciones.

Por último, los **ciberataques** no son tampoco un problema menor para el legislador. Bitcoin presenta unos riesgos especiales pues, dado que se almacena electrónicamente y el sistema no permite deshacer las transacciones una vez realizadas, es altamente atractivo para los cibercriminales y muy susceptible al robo.

Por otra parte, **cada vez que un gobierno publica una nueva regulación o incluso opinión sobre la regulación de las monedas digitales, el precio de Bitcoin se ve normalmente afectado.** Incluso si las acciones del gobierno no están directamente relacionadas con las monedas digitales en concreto, hay impacto.

Un buen ejemplo de esto se puede encontrar en la crisis bancaria de Chipre, donde el gobierno rescató al sector bancario[63].

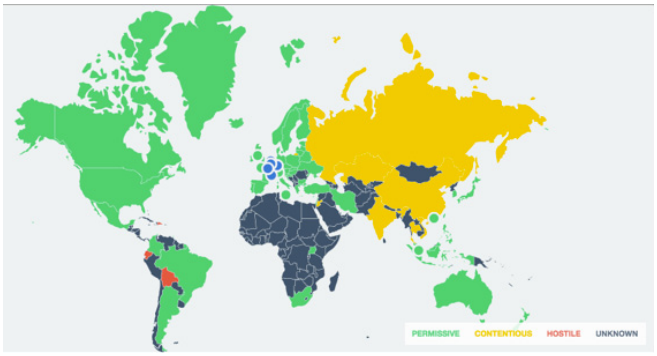
Fuente: CNN Money (Bitcoin prices surge post-Cyprus bailout: 28/03/2013)

Por supuesto, cada vez que se imponen restricciones el precio de Bitcoin cambia drásticamente. **Muchos gobiernos están proponiendo medidas para eliminar el anonimato.** Por ejemplo, ha habido propuestas para crear una supervisión de una tercera parte en los intercambios de Bitcoin[64].

Sobre **fiscalidad y privacidad de la moneda**, dado que el potencial de la moneda depende del uso que el público le dé, cuánto más efectiva se pruebe a la hora de hacer frente a estos retos, más buenas perspectivas habrá en cuanto a su uso y el precio subiría.

Índice bitlegal.io

El sitio web bitlegal.io ha elaborado un índice de "permisividad" legal del Bitcoin, clasificando los países según si son permisivos, contenciosos o hostiles al uso de las criptodivisas.



Fuente: bitlegal.io

En él se puede observar que la gran mayoría de países occidentales (incluidos Europa, América del Norte y Australia) tienen una actitud "permisiva", de acuerdo con este índice. Los más reservados son Rusia y Asia, y finalmente los hostiles, tan solo algunas localizaciones concretas de América del Sur. China ha mantenido una actitud cambiante, como veremos en el punto (Resto del mundo).

63 Ver "4.2.4 Noticias de eventos afectantes: factor reputacional"

64 Wirdum, Aaron V. (2016) European Banking Authority Proposes Virtual Currency-Specific Regulatory Body.

A continuación hacemos un repaso a las **principales medidas reguladoras o actuaciones legales** que han emprendido algunos de estos países y sus órganos reguladores nacionales o supranacionales.

Unión Europea

Una de las primeras características que cabe destacar de la legislación de la Unión Europea en materia de Bitcoin y otras criptodivisas es que **no existe una legislación específica que las regule** (o sea, no hay una "ley bitcoin"). Sí existen, sin embargo, **otras regulaciones y sentencias** que afectan a su uso o a los impuestos que se pueden aplicar.

Un ejemplo de estos impuestos que podrían ser aplicables a las transacciones con Bitcoin es el **impuesto VAT/GST,** que según la UE no es aplicable a la conversión entre el papel moneda tradicional y Bitcoin. Sin embargo, tal y como afirma el mismo organismo, VAT/GST y otros impuestos (como el **impuesto sobre la renta) aún se aplican a las transacciones que usan Bitcoin para adquirir bienes y servicios**[65].

En octubre de 2015, el **Tribunal de Justicia de la Unión Europea** afirmó que "el intercambio de monedas tradicionales por unidades de Bitcoin u otras monedas digitales está exenta de BAT" y que los "estados miembros han de exentar, excepto en el caso d'inter alia, transacciones relativas a otras monedas, notas bancarias y monedas usadas como legal tender, haciendo de Bitcoin una moneda muy opuesta a una *commodity*"[66]:

Por esta misma razón, de acuerdo con el **Banco Central Europeo, la regulación del sector financiero tradicional no es aplicable a Bitcoin** porque no incluye actores financieros tradicionales[67].

El **Banco Central Europeo** clasifica Bitcoin como una "*moneda virtual descentralizada que puede ser convertida"*. En Julio de 2014, la Autoridad Bancaria Europea avisó de que **los bancos europeos no podían actuar con monedas virtuales como Bitcoin hasta que no hubiera un régimen regulador establecido**[68].

En 2016, la **propuesta del Parlamento Europeo** para implementar una taskforce para monitorizar las monedas virtuales con tal de combatir el blanqueo de dinero y el terrorismo, fue aprobada con 541 votos a favor y 51 en contra, con 1 abstención. Es por eso que ha sido enviada a la Comisión Europea para que la considere[69].

La **Comisión Europea** ha presentado otra propuesta relevante "paralela" que tiene como objetivo prevenir la evasión fiscal, que requeriría también a los intercambios entre criptodivisas y *wallets* identificarse con tal de evitar actividades sospechosas[70].

Estados Unidos

El **Departamento del Tesoro** de Estados Unidos, con ciertas similitudes a lo que hizo la Unión Europea, clasificó Bitcoin como una moneda virtual descentralizada que podía ser convertible en 2014.

La ***Commodity* Futures Trading Comission**, CFTC, clasificó Bitcoin como una *commodity* en septiembre de 2015. Sin embargo, para la *International Revenue Service (IRS)*, Bitcoin es una propiedad sobre la cual se aplican impuestos[71].

En Marzo de 2017, la **Security Exchange Comission** (SEC) rechazó el primer ETF (fondo cotizado que replica el comportamiento de un índice) sobre Bitcoin[72]. Al hacerse pública la noticia, el valor de Bitcoin cayó inmediatamente un 8%.

Resto del mundo

En Canadá, Bitcoin ha sido clasificado simplemente como un activo "intangible" para la **PPSA**. Sin embargo, está regulado bajo el protocolo contra el blanqueo de capitales y la financiación terrorista[73].

China

En China, mientras que los agentes privados pueden tener en propiedad y comerciar con Bitcoin, la regulación prohíbe a las entidades financieras que hagan lo mismo.

El 5 de diciembre de 2013, el **People Bank of China** (PBOC) hizo el primer paso para regular Bitcoin cuando prohibió a las entidades financieras autorizar transacciones de Bitcoin[74].

El 16 de diciembre de 2013 se especuló con la posibilidad de que el banco central chino estuviera impulsando una reforma reguladora para prohibir el proceso de pago de terceras partes mediante Bitcoin[75], cosa que fue negada por la misma institución[76].

65 The Law Library of Congress Global Legal Research Center. (2014). Regulation of Bitcoin in Selected Jurisdictions.
66 Court of Justice of the European Union. Press Release No 128/15.
67 European Central Bank (2012). Virtual Currencies Scheme.
68 European Bankin Authority. (2014). EBA opinión on "virtual currencies".
69 European Parliament Press Room. (2016). MEPs call for virtual currency watchdog to combat money laundering and terrorism.
70 Coleman, L. (2017). The European Union Wants to Identify Bitcoin Users. Crypto Coin News.
71 International Revenue Service (2014). IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply.
72 Rubio, A. (2017). La SEC dice "no" al primer ETF sobre el Bitcoin. El Economista.
73 Rubenfeld, S. (2014). Canada Enacts Bitcoin Regulations. The Wall Street Journal.
74 Bloomberg News (2013). China Bans Financial Companies From Bitcoin Transactions.
75 Wile, R. (2013). Bitcoin's Outlook In China Is Not Looking So Good Right Now. Business Insider
76 Del Rey, J. (2013). China Bitcoin Exchange CEO: We're Not Giving Up Yet. All things D.

En abril de 2014 el PBOC ordenó a los bancos comerciales y a las compañías de pago cerrar cuentas que usaban Bitcoin.

El 30 de setiembre de 2017, el estado chino anunció que incluirían regulación sobre Bitcoin en sus **"Principios Generales de Derecho Civil de la República Popular China"**[77], y que éste sería tratado como una "propiedad virtual". La noticia fue bien recibida por los mercados pues desmentía el rumor de una prohibición absoluta de cualquier criptodivisa en China[78].

El comercio con Bitcoin es hoy legal en China[79],a pesar de algunos incidentes en materia reguladora recientes, como el de febrero de 2017, cuando algunas transacciones con Bitcoin fueron prohibidas o retrasadas sin previo aviso.

Japón

Japón reconoce oficialmente Bitcoin y las monedas digitales como monedas[80].

De acuerdo con el **Nikkei Asian Review**, el febrero de 2016, *"los reguladores financieros japoneses han propuesto que las monedas digitales pasen a ser un método de pago equivalente al de las monedas convencionales"*[81].

Finalmente, en 2017, el gobierno del país reconoció oficialmente Bitcoin como un método de pago[82].

4.2.4 Noticias de eventos: factor reputacional

Ha sido demostrado que **las noticias que se publican en medios especializados y no especializados también influyen el precio de Bitcoin significativamente.** Por ejemplo, noticias sobre fallos o pirateo de webs relacionadas con Bitcoin pueden causar pánico y disrupción entre los usuarios de Bitcoin. También noticias negativas sobre la permisividad del gobierno y la regulación, así como del uso ilegal de Bitcoin en transacciones de narcóticos o blanqueo de dinero.

A continuación se muestra la evolución del precio de Bitcoin aplicándole una escala logarítmica. Así puede apreciarse que las mayores subidas en el precio se produjeron entre 2011 y 2014, habiéndose "moderado" en términos porcentuales de crecimiento desde ese momento.

Sobre el gráfico, ejemplos de algunas noticias relevantes que se han publicado y que han tenido una cierta incidencia sobre el precio.

Fuente: Elaboración propia con datos de cryptocoinsnews.com

1. Artículo en Gawker

El 1 de junio de 2011, Bitcoin aparece por primera vez en un medio importante. Se trata de Gawker, y en el artículo se hace referencia a The Silk Road, una de las páginas web dedicadas al comercio con Bitcoin[83]. La publicación del artículo y su repercusión hacen que Bitcoin pase de $9,21 a $29,5 en pocos días.

2. Mr. Gotx hackeada

19 días después de la publicación del artículo, la página web relacionada con Bitcoin Mr. Gotx fue hackeada. Esto hizo que el precio descendiera en un corto período de tiempo[84].

3. Rescate de Chipre

A finales de marzo de 2013, se produjo el rescate de Chipre[85]. Este tipo de eventos son un ejemplo de cómo noticias negativas macroeconómicas afectan positivamente Bitcoin, que es visto en éste caso como un refugio. El precio osciló entre los $74 y $213.

4. Hearing en el Senado de Estados Unidos + Declaración Banco Central Chino

Dos importantes noticias en noviembre de 2013 influyeron positivamente en el precio de Bitcoin, ya que representaban ambas noticias pasos hacia la aceptación más amplia de la criptodivisa. Estos dos hechos hicieron que el precio ascendiera de los $685 a los $1,075, traspasando por primera vez la barrera de los $1,000. En primer lugar, el hearing sobre Bitcoin que fue llevado a cabo en el Senado de Estados Unidos[86]. En segundo lugar, el Banco Central Chino permitió el comercio con Bitcoin y otras criptodivisas[87].

77 Haig, S. (2017) Virtual Currencies Expected to be Regulated in China. Jet.com
78 Goh, B. (2017) China's bitcoin market alive and well as traders defy crackdown. Reuters.
79 Kelion, L. (2013). Bitcoin sinks after China restricts yuan exchanges. BBC News
80 Smart, E. (2016). Japan Officially Recognizes Bitcoin and Digital Currencies as Money. Bitcoin News.
81 Nikkei Asian Review. (2016). Japan eyes treating Bitcoins the same as real money.
82 Kharpal, A. (2017). Bitcoin value rises over $1 billion as Japan, Russia move to legitimize cryptocurrency. CNBC.
83 Gawker. (2016). The Underground Website Where You Can Buy Any Drug Imaginable.
84 Chapman, S. (2011). Bitcoin market flash-crash and database leak from Mt.Gox. ZDNet.
85 Farrell, M. (2013). Bitcoin prices surge post-Cyprus bailout. CNN Money.
86 On Bitcoin. (2013). Senate Committee Listens to Bitcoin Experts, Expresses Open-Mindedness.
87 Century, A. (2013). Bitcoin Gets a Cautious Nod From China's Central Bank. The New York Times.

5. Bitcoin objecto de impuestos

El 26 de abril de 2014, IRS declaró que Bitcoin podía ser objeto de impuestos en tanto que era considerado una propiedad[88]. El precio descendió en esas fechas de $581 a $403.

6. Encarcelamiento de Charlie Shem i hackeo de BitInstant

Otra bajada importante se produjo a finales de 2014 y principios de 2015 debido, también, a dos eventos remarcables. El precio pasó de $313 a $200. El primero fue la detención de Charlie Shem, CEO del sitio web de intercambio de Bitcoin BitInstant[89]. En segundo lugar, BitStamp, almacén de carteras Bitcoin fue hackeado, robando un total de 18,866 Bitcoins[90].

7. Bitcoin exento de impuestos según la UE

En octubre de 2015, la Unión Europea declaró que no se aplicaba el impuesto VTA sobre el intercambio de Bitcoin[91]. El precio ascendió hasta los $446.

8. Victoria de Trump en Estados Unidos

Curiosamente, en noviembre de 2016, cuando Trump ganó las elecciones presidenciales en Estados Unidos, el precio de Bitcoin pasó de los $726 a los $1,000, de acuerdo con algunos analistas, debido a su uso como valor refugio frente a la incertidumbre de los mercado[92].

9. Aparición de Bitcoin Cash

A principios de agosto de 2017, se produce el *fork* en Bitcoin que lleva a la aparición de Bitcoin Cash. El precio de Bitcoin aumenta desde los $2,787 a los $4,000.

5. Bitcoin Cash

5.1 ¿Por qué una nueva criptodivisa?

El 1 de agosto de 2017, un grupo de desarrolladores chinos activó Bitcoin Cash. Conocido técnicamente con el nombre de Segwit2, convirtiéndose en la **primera criptomoneda en separarse de Bitcoin**[93].

88 Rubin, R. Dougherty, C. (2014). Bitcoin Is Property Not Currency in Tax System, IRS Says. Bloomberg.
89 Inside Bitcoins. (2014). Charlie Shrem Sentenced: Former Bitcoin Entrepreneur Gets Two Years in Prison.
90 Higgins, S. (2015). Bitstamp Claims $5 Million Lost in Hot Wallet Hack. Coin Desk.
91 Clink, M. (2015). Bitcoin now tax-free in Europe after court ruling. CNBC.
92 Schell, A. (2016). Street processes Trump win; Dow 46 from record close. USA Today.
93 BBC (2017). Qué es es el Bitcoin cash, la nueva moneda nacida del Bitcoin que ya vale más de US$450.

Bitcoin Cash se define como una criptodivisa completamente nueva. Este nuevo sistema presenta **2 principales diferencias** con el original[94]:

- Aumenta el tamaño de cada bloque de *blockchain* a 8MB (frente al 1MB que conforma Bitcoin).

- Elimina SegWi[95] y lo cambia por otro código.

Las razones para hacerlo eran diversas y bastante técnicas y complicadas: resumiéndolo mucho, hay usuarios que piensan que sólo con el aumento de tamaño del bloque y otras novedades que incorpora Bitcoin Cash, será capaz de sobrevivir esta criptodivisa y por tanto están dispuestos a intercambiar sus Bitcoins por Bitcoin Cash.

La manera en la que las dos criptodivisas se han separado es mediante un ***fork***. Un "*fork*" se define como una **divergencia permanente** entre las dos monedas. Llegado el momento, a los "mineros" se les dio la opción de redirigir toda su capacidad de computación hacia una nueva criptodivisa o, por el contrario, mantenerse en Bitcoin.

Andreas M. Antonopoulos explica en una ponencia cómo se producen este tipo de "*hard forks*" en la tecnología *blockchain*[96].

"Hay un proceso que se da cuando hay un desacuerdo o un cambio de normas, donde Bitcoin se puede dividir en 2 sistemas que operan paralelamente. La razón por la cual esto pasa es que, cuando uno tiene una coordinación de 10,000 ordenadores alrededor del mundo, si estos disienten entre ellos, el que disiente se queda fuera de la red temporalmente hasta que vuelve a asentir otra vez."

Añade que este tipo de fenómenos son diferentes al que se ha producido en el caso de Bitcoin Cash.

A continuación pasa a especificar cuáles son las reglas que han cambiado en Bitcoin Cash:

"En Bitcoin 1 bloque de 1MB es ofrecido cada 10 minutos, 6MB cada hora, 144MB cada día. Ha surgido un grupo de usuarios de la red Bitcoin que ha cuestionado el tamaño y la temporalidad. Es en este momento cuando deciden cambiar ellos las reglas. Este tipo de fenómeno se llama contentious fork".

Respondiendo a la pregunta sobre qué pasa con el número de Bitcoin en cada cartera antes y después del *fork* prosigue:

"Cuando se produce un fork de este tipo, el libro mayor se replica en los dos lados. Esto significa que si previamente al fork tenías un valor, los dos sistemas, al tener los mismo ancestros, lo guardan aún y por tanto mantienes el valor.""

94 Bitcoin.com. (2017). Differences Between Bitcoin Cash and Bitcoin.
95 Ver "3.3 Bitcoin Cash"
96 Antonopoulos, A. (2017). Bitcoin Q&A: What happens to our Bitcoins during a hard *fork*?

Ante las incertidumbres, el autor recomienda asegurarse de que el usuario es el verdadero propietario del *wallet*, pues sólo en este caso podrá saber si su valor en Bitcoin se mantendrá o no.

5.2 Críticas y controversias

Ya se han producido algunas controversias respecto al precio de Bitcoin Cash que, si bien en un primer momento presentaba una evolución positiva, últimamente están surgiendo dudas acerca de su futuro.

El 4 de agosto de 2017, tan sólo cuatro días después de que se produjese el *hard fork* entre Bitcoin y Bitcoin Cash, el precio de la nueva acuñada criptomoneda descendió un 30%[97].

Fuente: Coindesk.com

Algunos analistas atribuyeron este gran descenso en el precio a los inversores que quisieron vender la nueva moneda o intercambiarla otra vez por Bitcoin, si se encontraron con que se habían cambiado los valores de los cuáles ellos eran propietarios.

5.3 Estado actual

A modo de conclusión de todo este capítulo, podríamos decir que Bitcoin Cash **es sólo otra criptodivisa más**, eso sí, completamente nueva, pero que tal como se puede apreciar en el gráfico de la evolución del precio[98], se ha desvinculado en principio de su creador original "Bitcoin", pues **no se correlacionen con un tipo de cambio fijo** ni nada parecido, sino que el precio relativo de una y otra continúa siendo determinado en el mercado libremente[99].

97 Cheng, E. (2017) New 'Bitcoin cash' crashes 30% Friday in volatile first week of trading; original Bitcoin steady .CNBC.
98 Ver Anexo
99 Mengerian. (2017) Bringing Stability to Bitcoin Cash Difficulty Adjustments. Medium.

6. Conclusión

Nos encontramos **lejos de un consenso** en materia de opiniones respecto al fenómeno Bitcoin y otras criptodivisas. En general se pueden encontrar una amplia disparidad de criterios.

Los más entusiastas aseguran que Bitcoin es la revolución monetaria definitiva, que en tanto que permite transacciones anónimas descentralizadas, acabará sustituyendo en un periodo corto de tiempo las formas de pago tradicionales y el papel moneda.

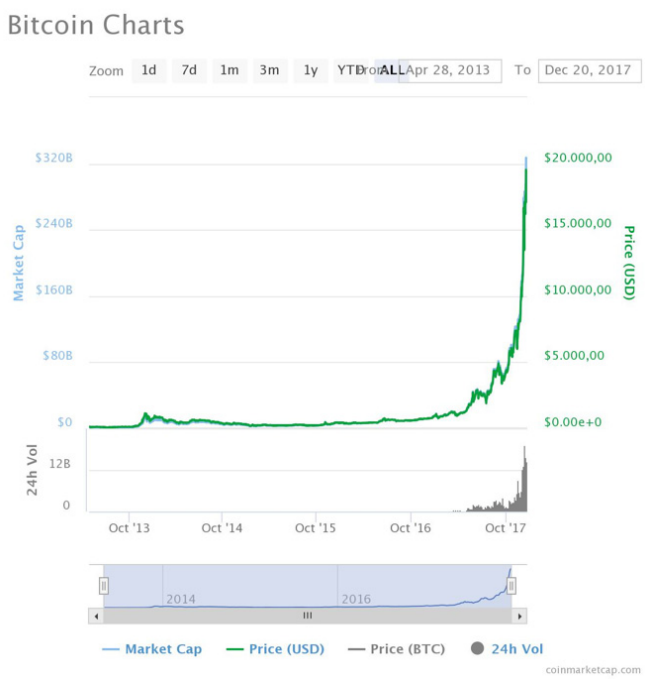
Otros, más conservadores, piensan que las monedas digitales son sólo otra burbuja, donde los agentes que adquieren Bitcoin sólo lo hacen con el objetivo de especular con su precio sin tener ninguna intención de crear valor.

Es **materialmente imposible hacer una predicción acertada ex-ante de cuál será el futuro de Bitcoin.** Si finalmente se convertirá en una moneda de referencia o si se trata sólo de una burbuja similar a la del punto.com de principios de siglo. Lo que sí sabemos es que el interés por este fenómeno se mantiene intacto. Basta con echar un vistazo a los periódicos económicos y también generalistas más importantes del mundo, donde no hay ningún día en que no aparezca una noticia relacionada con las criptodivisas, respecto a su evolución en el mercado, su regulación o nuevas funciones adquiridas.

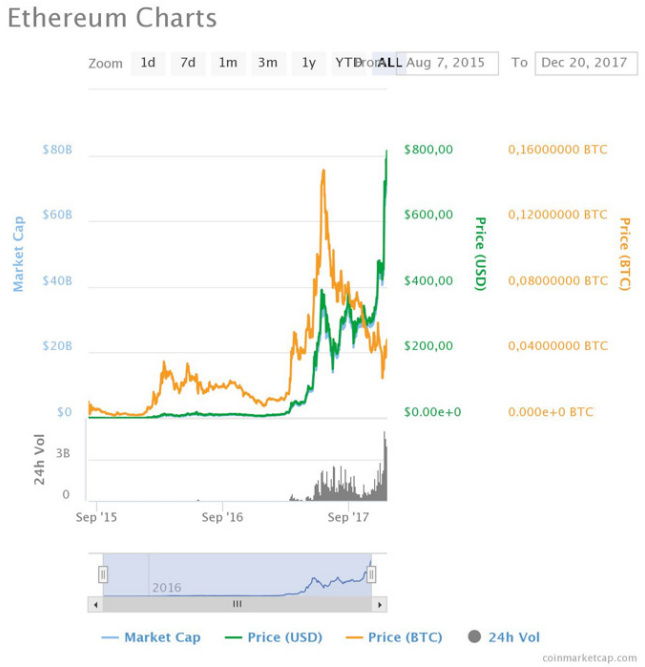
Como frase resumen del documento, acompañamos una cita del experto en monedas digitales Andreas M. Antonopoulos sobre el futuro de Bitcoin:

"No sé si Bitcoin se convertirá en una moneda de referencia. Es materialmente imposible saberlo. Sólo podemos hacer elucubraciones al respecto. Pero creo que podemos estar bastante seguros de que alguna forma de moneda digital basada en un libro mayor criptográfico compartido y abierto es el futuro que nos espera. No sé si se llamará Bitcoin o de otra manera, pero podemos empezar a estar bien seguros de que estará ampliamente basado en estas ideas".

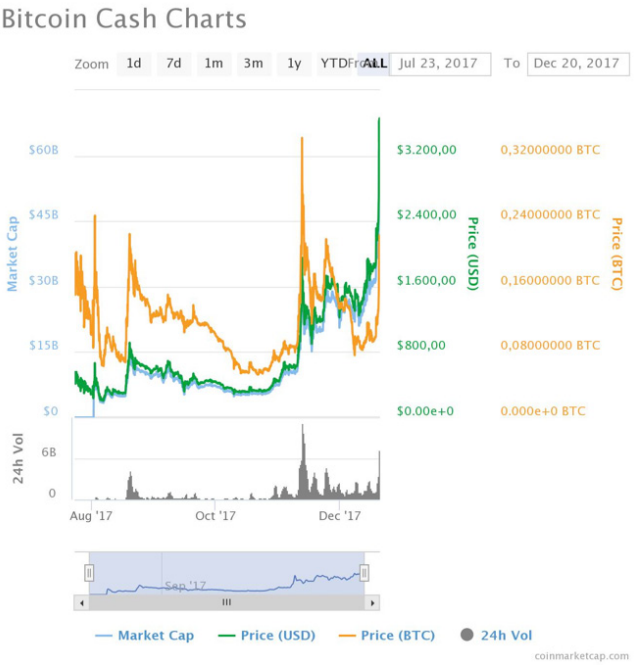
Anexo: Evolución en el precio de las principales criptodivisas



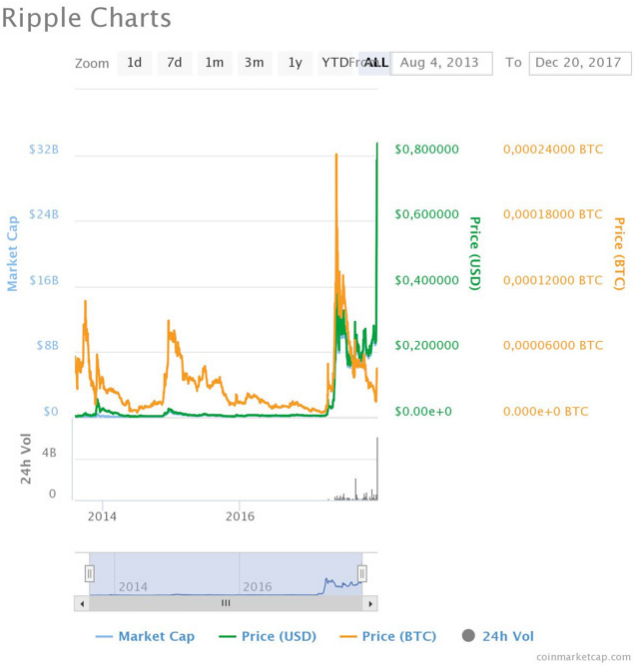
Fuente: coinmarketcap.com



Fuente: coinmarketcap.com



Fuente: coinmarketcap.com



Fuente: coinmarketcap.com

Fuente: coinmarketcap.com

Fuente: coinmarketcap.com

IEF *Trending Topics*