
Universidad de Valladolid

**Facultad** de **Ciencias Económicas** y **Empresariales**

**Trabajo de Fin de Grado**

**Grado** en **Administración y Dirección de Empresas**

# Bitcoin y la Crisis Financiera

Presentado por:

***Natalia García Casado***

Tutelado por:

***Gabriel de la Fuente Herrero***

*Valladolid, 21 de junio de 2019*

**RESUMEN**

Estudio descriptivo de la tecnología que sustenta a Bitcoin, la crisis del 2008 y su relación con el nacimiento de la criptomoneda. También se realiza un breve análisis sobre cómo bitcoin podría mejorar el sistema financiero actual. En el último epígrafe del trabajo se realiza un estudio empírico de la criptomoneda a través de la evolución de su rentabilidad y los valores de su beta en el modelo CAPM, tomando como cartera de mercado al S&P500, con el objetivo de caracterizar a Bitcoin actualmente. Los resultados del estudio empírico muestran que actualmente Bitcoin se comporta como un activo especulativo, si bien de cara al futuro no se puede establecer claramente su evolución.

**ABSTRACT**

Descriptive analysis of the technology that uses Bitcoin, the crisis of 2008 and its relationship with the origin of the cryptocurrency. Moreover, an analysis is made on how Bitcoin could improve the financial system. Lastly, an empirical study is made using the CAPM model to classify the cryptocurrency. For the study, the S&P500 is used as market portfolio, and the records of the study begin in 2010 until now. The results of the study show that Bitcoin can be classified as a speculative asset, although in the future is not so clear that the cryptocurrency will behave like that, it might be or not.

JEL CLASSIFICATION: E42, G01 y G15

## TABLA DE CONTENIDOS



## ÍNDICE DE GRÁFICOS

# 1. INTRODUCCIÓN

En diciembre de 2017, bitcoin alcanzó cotizaciones récord, superando los 20.000 dólares norteamericanos (en adelante, USD) e impulsando el mercado de criptomonedas. Esta criptomoneda surgió en el 2008, tan solo unos meses después de la caída de Lehman Brothers y en poco tiempo ganó muchísima popularidad. Bitcoin fue diseñada por Satoshi Nakamoto y desde un primer momento supuso una revolución, porque presentaba soluciones a problemas que hasta entonces nunca habían sido resueltos.

El objetivo de este trabajo es analizar la naturaleza y evolución de bitcoin y evaluar su potencial para mejorar ciertos aspectos del sistema financiero. Pero es imposible entender por qué una criptomoneda, que no tiene el respaldo de ningún banco central, es capaz de alcanzar cotizaciones tan altas como los 20.000 USD, sin un análisis primero de la tecnología que hay detrás de bitcoin, concretamente el *blockchain* o cadena de bloques. Sin comprender esta tecnología no es posible entender el potencial de bitcoin. Por ello el primer punto del trabajo se centra en explicar esta tecnología, centrándose específicamente en la *blockchain* de bitcoin.

Una vez explicada la tecnología *blockchain*, el trabajo analiza la crisis del 2008 y las debilidades que se dieron en el sistema que condujo a la crisis económica. Seguidamente, se describen los precedentes y orígenes de la criptomoneda, que son un aspecto importante para entender el entusiasmo que este sistema “entre iguales” o P2P (*Peer to Peer*) genera, y de su relación con la crisis económica. La discusión teórica termina con un breve análisis de cómo Bitcoin podría mejorar el sistema financiero actual.

El último epígrafe del trabajo trata de caracterizar la criptomoneda a través del análisis del modelo CAPM, tomando como cartera de mercado el S&P500. Además, no solo se compara con el índice de mercado, sino también con otros cuatro activos que cotizan en dicho índice. El objetivo de este último apartado es dilucidar a través del análisis descriptivo del comportamiento de los precios si los propietarios de bitcoins lo pueden estar utilizando como activo refugio o como un activo especulativo.

## 2. *BLOCKCHAIN*

Bitcoin es una criptomoneda que permite realizar transacciones P2P o entre iguales, que apareció por primera vez poco después de la caída de Lehman Brothers. Para algunos autores, Bitcoin supone la mayor innovación en el mundo de las finanzas desde los Médici[1]. La novedad principal consiste en la tecnología *blockchain,* que utilizó Satoshi Nakamoto para diseñar Bitcoin. Por tanto, para entender el valor y potencial de Bitcoin es necesario entender cómo funciona esta tecnología.

El problema que resolvió Bitcoin y más tarde el resto de las criptomonedas se suele ejemplificar con el llamado "Problema de los Generales Bizantinos":

> "Cinco generales bizantinos se encuentran de campaña en Asia. Deben ponerse de acuerdo para atacar al ejército persa, y hacerlo simultáneamente. Si cualquiera de ellos lo intentara por separado, se enfrentaría a un fracaso cierto: la derrota y la muerte o la esclavitud de por vida. Nadie los coordina y podría darse perfectamente la eventualidad de que uno de ellos fuera un traidor. Una mañana se recibe en uno de los campamentos el siguiente mensaje: "El ataque se producirá el día tal". No lleva el aval del emperador ni de ninguna autoridad central. ¿Cómo puede el destinatario tener la certeza de que se trata de una orden verdadera y no de una añagaza del enemigo?"[2].

Este problema fue resuelto por Bitcoin, a través de la tecnología *blockchain* o cadena de bloques. Preukschat (2017: 25) define una *blockchain* como "una base de datos que se halla distribuida entre diferentes participantes, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí matemáticamente". Para la revista *The Economist*[3]*,* la tecnología *blockchain* es "la gran cadena que permite estar seguro sobre las cosas", y la industria financiera ha renombrado a esta tecnología como

[1] Villarejo, M (2017). "El Bitcoin y sus límites". Actualidad Económica/Expansión. Disponible en : https://bit.ly/2j5vqp0 [Consultado: 1/07/2018].
[2] Ibid.
[3] The Economist. "The great chain of being sure about things". The Economist. Disponible en: https://hbs.me/2OhpKZT [Consultado: 22/05/2018].

"Distributed Ledger", que en español podría traducirse como "libro mayor distribuido" (Tapscott & Tapscott, 2016: 8).

Para que una *blockchain* sea considerada como tal tiene que contar con los siguientes elementos: nodos, protocolo estándar, *Peer-to-Peer* y un sistema descentralizado (Preukschat, 2017). Los nodos son los ordenadores que están conectados a la *blockchain* siguiendo un mismo protocolo (Preuckschat, 2017). Este protocolo, por tanto, es el software informático que permite la comunicación entre ellos, y la *Peer-to-Peer* (P2P) es la red de nodos conectados entre sí (Preuckschat, 2017). Por último, la descentralización implica que la información no esté controlada por una única entidad, si no que todos los ordenadores o nodos de la cadena de bloques son iguales entre sí (Preuckschat, 2017).

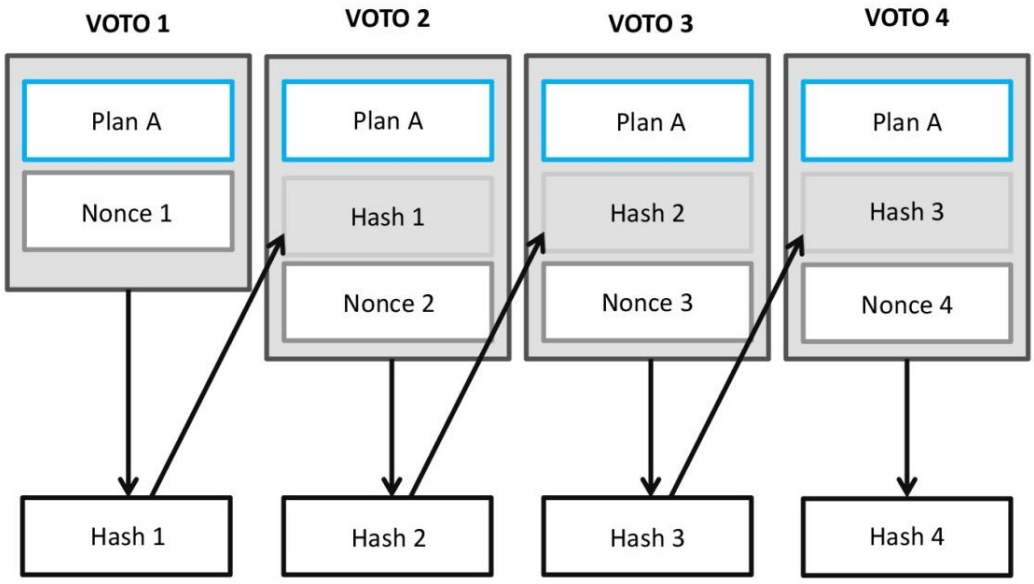
Toda *blockchain* se sustenta en tres pilares básicos que son: la criptografía, la propia cadena de bloques y el consenso (Preukschat, 2017). La criptografía permite el anonimato y que no se produzcan robos, manipulación e introducción errónea de información (Preukschat, 2017). La *blockchain* es la "base de datos[4]" y sigue siempre el mismo protocolo para así validar la información (el nuevo bloque), e incorporarla a la cadena (Preukschat, 2017). El consenso se sustenta en el protocolo de la *blockchain* que los nuevos bloques deben cumplir para que se puedan añadir a la cadena (Preukschat, 2017). La existencia del consenso es una de las partes más importantes en una *blockchain*, ya que impide problemas como el doble gasto y cualquier cambio en el consenso debe estar aprobado por la mayoría para poder llevarse a cabo (en el caso de *blockchain*s públicas) (Preukschat, 2017).

Ahora los generales ya tienen definidas las características del canal de comunicación y uno de ellos manda el plan de ataque. ¿Cómo saben los otros generales qué ese es el plan a seguir? En "Bitcoin: A Peer-to-Peer Electronic Cash System", Satoshi Nakamoto[5] soluciona este problema mediante el *Proof-of-Work (PoW)* o Prueba de Trabajo. En Bitcoin, el *PoW*

[4] Técnicamente una *blockchain* es un registro, no una base de datos.
[5] Nakamoto, S (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System". Bitcoin.org. Disponible en: https://bitcoin.org/bitcoin.pdf [Consultado: 23/07/2018].

consiste en encontrar una función *hash* (Bonneau *et al*; 2015), que es una secuencia alfanumérica que comprime siempre igual una información. En nuestro ejemplo, cuando uno de los generales "logre enviar un plan con su *hash* correcto, ése será el primer voto válido y el primer eslabón de esa cadena" (Preukschat, 2017: 216). El resto de los generales se pondrán a buscar el segundo *hash*, y el general que lo encuentre se lo enviará al resto de generales, y así sucesivamente, como se puede ver en el Gráfico 1.1.

GRÁFICO 2.1: FUNCIONAMIENTO DE LA CADENA DE BLOQUES




Fuente: Preukschat, 2017: 217

Pero puede ocurrir que dos generales envíen dos planes de forma simultánea y existan dos cadenas temporalmente (Preukschat, 2017). Nakamoto soluciona este problema mediante el consenso de la *blockchain*, por el cual la cadena más larga será la válida. Por este motivo, normalmente solo se considera como definitiva una transacción de bitcoin después de una hora ya que, si se tarda de media 10 minutos en encontrar un nuevo bloque, esto quiere decir que se habrán añadido otros 5 bloques a la *blockchain*, siendo ésta la más larga (Dwyer, 2015). De acuerdo con Bonneau *et al*. (2015) esta es la principal innovación de Bitcoin, que explica en gran parte el éxito de la criptomoneda.

La *PoW* de Bitcoin establece la proporción "una dirección IP-un voto", de esta forma la cadena de bloques se mantiene "honesta", siempre y cuando el 51%

de la red siga las normas[6]. Para que la red se mantenga "honesta", Satoshi Nakamoto[7], basándose en la teoría de juegos y en ideas de John Nash (Preukschat, 2017), estableció un sistema de incentivos para los mineros de la cadena de bloques. Este sistema de incentivos consiste en dos partes: el *Block Reward* y las comisiones. El *Block Reward* se basa en que cuando los mineros encuentran un nuevo bloque son recompensados con nuevos bloques. Este *Block Reward* sigue un proceso fijo por el cual cada 210.000 bloques la recompensa se reduce a la mitad, produciéndose esta disminución más o menos cada 4 años (Bonneau, *et al*. 2015). Esto será así hasta 2140, cuando se alcance el límite de los 21 millones de Bitcoins (Dwyer, 2015). Los mineros también son recompensados mediante las comisiones de cada transacción y, según Dwyer (2015), estas tasas de interés proporcionan un incentivo a los mineros para que incluyan las últimas transacciones a la cadena de datos. Estas comisiones son opcionales, aunque en 2014 el 97% de las transacciones incluían una (Böhme, *et al*; 2015).

Por último, la *PoW* soluciona el problema del doble gasto[8]. Antes de que apareciera Bitcoin la única manera de solucionar este problema era con un tercero de confianza. Sin embargo, con Bitcoin este intermediario no es necesario, ya que será la primera orden la que tendrá más "votos" y que el sistema finalmente considerará como válida (Preukschat, 2017).

## 3. LA CRISIS FINANCIERA DEL 2008

La crisis financiera del 2008 es considerada la peor crisis económica desde la Gran Depresión. De acuerdo con Bernanke (2010), el detonante de la crisis fueron las potenciales pérdidas de hipotecas de prestatarios no preferenciales o *subprime*. Estas pérdidas en un principio solo afectaban a una pequeña parte del sistema financiero estadounidense (BIS, 2009) y, comparadas con el conjunto global de los mercados financieros, no tenían la capacidad de provocar una

[6] Nakamoto, S (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System". Bitcoin.org. Disponible en: https://bitcoin.org/bitcoin.pdf [Consultado: 23/07/2018].
[7] Ibid.
[8] El problema del doble gasto es el riesgo por el que una moneda digital pueda gastarse dos veces.

recesión económica tan importante (Bernanke, 2010). Sin embargo, la inestabilidad que provocaron, unidas a las debilidades sistémicas que se daban en aquel momento en la economía, dieron lugar a la profunda recesión económica (Bernanke, 2010).

El 30 de julio de 2007, el banco alemán IKB anunció que recibiría apoyo del gobierno alemán. El problema de IKB eran sus instrumentos de deuda a corto plazo, concretamente de *Asset-Backed Commercial Paper* (*ABCP),* que había estado emitiendo en EE.UU. (Bernanke, 2010). Inversores de todo el mundo retiraron sus fondos y se produjo un efecto similar al "pánico financiero" (Bernanke, 2010). De acuerdo con Reinhart y Rogoff (2011) una crisis bancaria se puede definir por dos tipos de sucesos. El primero de ellos sería un "pánico bancario" que conlleva que el sector público tenga que adquirir o cerrar una entidad bancaria (Reinhart y Rogoff, 2011). Pero también puede darse una crisis bancaria sin que se produzca dicho "pánico financiero", debido al cierre, fusión o adquisición de una entidad financiera que tenga las mismas consecuencias para otras entidades (Reinhart y Rogoff, 2011). En el caso de la crisis financiera del 2008 se dio el primer escenario produciéndose un "pánico bancario" en el mercado de deuda a corto plazo, principalmente *ABCP* y los acuerdos *repo*.

Los mercados de *ABCP* y *repos* antes de la crisis se consideraban como seguros y fiables. Sin embargo, fueron todo lo contrario (IMF, 2010), principalmente debido a los problemas para valorar adecuadamente los productos titularizados a causa de la complejidad y opacidad del sistema (IMF, 2010). Todo esto provocó que las inversiones se redujeran y los fondos se retiraran (Bernanke, 2010). Esta presión sobre la financiación acabó finalmente trasladándose a los principales bancos (Bernanke, 2010), que se vieron obligados a pasar sus *ABCP* de fuera de balance a la hoja contable con la consiguiente pérdida de liquidez (IMF, 2010). Además, la desconfianza que había sobre los mercados dificultó aún más el acceso a la financiación de los bancos, que acabó afectando al mercado global (IMF, 2010). Los bancos comenzaron a acumular liquidez, provocando que el dólar estadounidense estuviese muy demandado, y que varios bancos centrales tuvieran que establecer líneas de permuta financiera o *swaps* con la Reserva Federal (IMF, 2010).

Por otra parte, el mercado de *repos* empezaba a mostrar también signos de estrés, lo que puso en peligro el modelo de financiación de los bancos de inversión (IMF, 2010). De acuerdo con el IMF (2010), el mercado de acuerdos *repo* llegó a representar entre el 20% y 30% del PIB de EE.UU. entre 2002 y 2007. Las tensiones en el mercado de *repos* no disminuyeron y, en 2008, el banco de inversión Bear Stearns es absorbido por JPMorgan Chase, una operación apoyada por las autoridades estadounidenses (BIS, 2009). Durante el 2008, las preocupaciones sobre las pérdidas de valor de títulos garantizados por empresas de seguros *monoline* aumentaron especialmente en junio, afectando profundamente las tensiones del sector a dos empresas, Fannie Mae y Freddic Mac (BIS, 2009). El gobierno estadounidense anunció paquetes de ayuda para estas dos empresas, sin embargo, las tensiones en el mercado solo desaparecieron brevemente (BIS, 2009). Finalmente, el 15 de septiembre de 2008, el banco de inversión Lehman Brothers se declaró en bancarrota.

La bancarrota de Lehman Brothers y Bear Stearns provocó que las condiciones en el mercado de *repos* se deterioraran aún más, ya que se vio que los riesgos del mercado no habían sido valorados adecuadamente (IMF, 2011). Además, los Fondos de Inversión del Mercado Monetario (FMM) amplificaron la inestabilidad existente (Bis, 2009), ya que muchos inversores se retiraron de los FMM, provocando un “pánico bancario” (Bernanke, 2010), al estar muy expuestos al mercado de *ABCP*. Estas retiradas de dinero tan solo se vieron atenuadas por las acciones llevadas a cabo por el Tesoro y la Reserva Federal de EE.UU. (Gorton y Mettric, 2012). A pesar de estas medidas, el valor liquidativo del fondo de inversión Reserve Primary cayó por debajo de 1USD, debido a su exposición a la quiebra de Lehman Brothers y a la incertidumbre existente (Gorton y Mettric, 2012). Los FMM ayudaron también a la expansión de la crisis a un nivel global, ya que muchos de ellos evolucionaron en entidades que eran intermediarios entre cuentas mancomunadas de EE.UU. y bancos de Europa (Pozsar, 2011).

La crisis económica, por tanto, estuvo relacionada con la demanda de instrumentos de deuda triple A (*ABCP* y *repos)* de alta solvencia que, sin embargo, se titularizaron con las hipotecas *subprime* (Pozsar, 2011). La demanda de este tipo de instrumentos financieros alternativos se debió a la continua entrada de capital extranjero que adquiría bonos del Tesoro (Bernanke,

2005) y que, por lo tanto, dio lugar a un sobreexceso de demanda. Esto provocó un vacío en el mercado siendo ocupado por un sistema bancario en la sombra o *shadow banking*, que actuaba como intermediario y no estaba casi regulado (Pozsar, 2011). Todo ello originó un sistema complejo y poco transparente que favoreció el que se produjeran dos "pánicos financieros", el primero de ellos con la primera contracción en el mercado de *ABCP*, y el segundo de ellos tras la caída de Lehman Brothers.

### 3.1. FALLOS DEL MERCADO:

La recesión económica nunca habría llegado a ser tan pronunciada de no ser por los fallos existentes en el mercado, que dieron lugar a las posteriores vulnerabilidades y que se pueden resumir en los siguientes:

- Fondos a corto plazo inestables:

  La utilización de instrumentos de deuda no asegurada por parte del sistema *shadow banking* les exponía a "pánicos bancarios" (Bernanke, 2010). Además, los modelos de estos instrumentos de deuda no reflejaban adecuadamente el riesgo que podían representar las liquidaciones.

- Los FMM:

  Ante los primeros síntomas de estrés en los mercados, las firmas y los bancos acumularon liquidez (Bernanke, 2010). Los FMM demostraron estar muy expuestos a déficits de liquidez en el mercado (Bernanke, 2010), ya que según el IMF (2010: 68) "el papel crucial de los FMM en el mercado de deuda a corto plazo no fue bien entendido", incrementando la vulnerabilidad de los mercados de financiación a retiradas de liquidez. Todo esto llevó a la gran demanda de dólares, que acabó con la Reserva Federal estableciendo líneas de *swaps* con varios bancos centrales (Bernanke, 2010), creando un problema similar al Dilema de Triffin[9] (Pozsar, 2011).

- Deficiencias en la gestión del riesgo:

[9] Paradoja a la que se enfrenta el emisor de la divisa internacional por excelencia, ya que debe proporcionar liquidez global para estimular la economía, pero esto provoca dudas sobre su solvencia. Durante el periodo Bretton Woods es lo que le ocurrió a EE.UU, llevando al abandono del patrón oro.

Los modelos utilizados no reflejaban adecuadamente el riesgo de los instrumentos de deuda a corto plazo (IMF, 2010). Además, se dio una gestión deficiente del riesgo, existiendo una confianza excesiva en los ratings crediticios, que llevó a una incorrecta diversificación del riesgo (Bernanke, 2010). En parte, de acuerdo con el IMF (2010), esto fue debido a las condiciones del mercado existentes en ese momento con bajos intereses nominales y el bajo nivel de las primas de riesgo. Además, los proveedores de *repos* optaron por pequeños recortes de valoración o *haircuts* (IMF, 2010). Estos *haircuts* sumados al entorno existente llevaron a un excesivo apalancamiento (IMF,2010). Por último, hay que añadir el mal uso del modelo *originate-to-distribute* (Bernanke, 2010)[10].

- <u>El mal uso de algunos derivados financieros:</u>

  Algunas empresas, como AIG, usaron los derivados de crédito para contraer un mayor riesgo, sin tener el capital suficiente para protegerse frente a los potenciales riesgos (Bernanke, 2010). Además, su complejidad no ayudó a las empresas a determinar adecuadamente su exposición al mercado (Bernanke, 2010).

- <u>El Sector Público:</u>

  La existencia de vacíos legales, especialmente en el caso del *shadow banking*, que se encontraba sin regulación ya que, por ejemplo, no tenía que aportar informes que mostrarán sus posiciones y exposición al riesgo del mercado (Bernanke, 2010). En el caso de las empresas, Fannie Mac y Freddic Mac, se las permitió operar con capital de baja calidad (Bernanke, 2010). Por último, los *stress tests* llevados a cabo por agencias gubernamentales demostraron la existencia de deficiencias de las empresas (Bernanke, 2010). Sin embargo, las medidas tomadas por las agencias reguladores se pueden considerar como pasivas (Bernanke, 2010).

A todos estos fallos habría que añadir el "efecto humano", que en muchos casos es muy difícil de evitar. Reinhart y Rogoff (2011) lo definen cómo el síndrome

[10] Aquellos casos en los que los acreedores no tienen el objetivo de mantener el préstamo hasta su vencimiento, si no que los venden a otras instituciones o inversores (Nasdaq. "Originate-to-Distribute". Nasdaq. Disponible en: https://bit.ly/2Dwbybc [Consultado: 23/09/2018]).

"*This-Time-Is-Different"*, por el cual la gente cree que una crisis financiera "es algo que pasa a otra gente en otros países y en otros tiempos". Además, habría que añadir, como dice Bernanke (2010), la creencia de los inversores respecto a las instituciones "*Too Big To Fail",* por la que un gobierno nunca va a dejar que quiebre, distorsionando de esta forma la competencia y los riesgos del mercado.

Para concluir, los fallos anteriormente enunciados llevaron a que el mercado tuviera unas debilidades sistémicas que le hicieron vulnerable ante la crisis de las hipotecas *subprime*, un sector del mercado financiero relativamente pequeño. Todo ello, sumado a la compleja estructura existente en el mercado, especialmente el de *repos* (IMF, 2010), llevó a una crisis de dimensiones desconocidas desde la Gran Depresión.

## 4. BITCOIN: ORÍGENES Y EVOLUCIÓN

El 31 de octubre de 2008, tan solo 2 meses después de la caída de Lehman Brothers, el usuario Satoshi Nakamoto publicó "Bitcoin: A Peer-to-Peer Electronic Cash System". El artículo fue publicado en metzdown.com, un sitio web de criptografía relacionado con el movimiento *cyberpunk* (Márquez, 2015). El movimiento *cyberpunk*, de acuerdo con Márquez (2015: 118), tiene su origen en los años 90 en las corrientes de pensamiento contrarias a "las prohibiciones del Gobierno de EE.UU. de publicar ideas o investigaciones relacionadas con la criptografía". Los *cyberpunks* consideraban la criptografía como algo necesario y sus ideas vienen recogidas en el "Manifiesto Criptoanarquista", y el "Manifiesto Cyberpunk" (Márquez, 2015).

De acuerdo con Márquez (2015: 118), en "Bitcoin: A Peer-to-Peer Electronic Cash System" muchas de las ideas que se presentan ya habían sido desarrollados por otros autores, "aunque se da una vuelta de tuerca al concepto de dinero electrónico y a los problemas de anonimato y descentralización". A la hora de analizar los precedentes de Bitcoin se suelen tener en cuenta los siguientes (Márquez, 2015):

- <u>eCash:</u>

  En 1981, David Chaum (1981) presentó un sistema basado en la criptografía de llave pública que permitía una comunicación electrónica

anónima. Los participantes podían comunicarse de forma secreta sin conocer quiénes eran ni el contenido de sus mensajes. Unos años más tarde, David Chaum fundó la empresa DigiCash y creó el protocolo eCash, que era un sistema de pagos no rastreable mediante el uso de firmas ciegas[11], aunque necesitaba de una autoridad central (Márquez, 2015).

- Hashcash:

En 1997 apareció Hashcash, creada por el criptógrafo Adam Back, cuyo objetivo era limitar el correo basura del email (Márquez, 2015). Adam Back quería conseguir esto mediante la imposición de un coste no monetario al envío de cada correo con la utilización de funciones hash[12]. La idea era "hacer el *hashing* del mensaje una y otra vez (variando cada vez un pequeño dato llamado "Nonce") hasta encontrar un hash que reuniera unas determinadas condiciones" a modo de testigo en la cabecera[13]. De esta manera, para una persona que enviará unos pocos de correos al día, el coste de cifrar el mensaje sería ínfimo. Sin embargo, para una persona que enviara millones de correos al día supondría una carga, ya que la búsqueda de la función hash requería el uso de cierto coste computacional[14]. El utilizar la función hash sería como añadir, por tanto, un sello de correos fabricado por el propio ordenador [15] .En *Hashcash* existen conceptos que más tarde fueron utilizados en Bitcoin como la *PoW*, y el uso de funciones hash (Márquez, 2015).

- Bitgold:

Bitgold fue una propuesta teórica de Nick Szabo que consistía en un sistema de creación de dinero, donde la existencia de una tercera parte de confianza no era necesaria (Márquez, 2015). Para muchos, el artículo "Bitgold" es considerado como el manifiesto fundacional de Bitcoin

[11] Las firmas ciegas permiten a una persona recibir un mensaje de otra entidad, sin necesidad de revelar el contenido del mensaje.
[12] - Preuskschat, A (2019). "Hashcash". Libro *Blockchain*. Disponible en: http://libro*blockchain*.com/hashcash/ [Consultado: 22/12/2018].
[13] Ibid
[14] Ibid
[15] Ibid

(Márquez, 2015: 124). La producción del dinero se llevaría a cabo mediante *PoW,* y Nick Szabo[16] resumía el proceso de la siguiente manera:

1. Creación de una cadena pública de bits o "Cadena-reto".
2. Alicia en su ordenador genera la cadena *PoW* para esta "cadena-reto" usando una función de referencia.
3. La *PoW* recibe un sello de tiempo seguro. Con la existencia de varios servicios de sellado funcionando de manera distribuida, para así no depender de ninguno.
4. Alicia añade la "cadena-reto" y la *PoW* a un registro distribuido de títulos de propiedad Bitgold, sin la existencia de un servidor predominante.
5. La última cadena de Bitgold proporciona los bits de la "cadena-reto" para la próxima cadena.
6. Para comprobar que Alicia es la propietaria de dichos Bitgolds, Bob comprueba la cadena infalsificable de títulos en el registro de propiedad de Bitgold.
7. Para evaluar el valor de una cadena de Bitgold, Bob comprueba y verifica las "cadenas-reto", la cadena de *PoW*, y el sello de tiempo.

Además de Bitgold en 1997, Nick Szabo publicó el artículo "The God Protocols", en el que "reflexionaba sobre la creación del protocolo tecnológico más importante, uno designado por Dios que sería la tercera parte de confianza en las transacciones" (Tapscott & Tapscott, 2016). En este artículo, Nick Szabo estableció la importancia de la confianza en Internet, ya que "hacer negocios online requiere un salto de fe" (Tapscott & Tapscott, 2016). Años más tarde, Bitcoin solucionaría este problema.

- <u>B-Money:</u>

Por último, B-Money fue una propuesta teórica realizada por Wei Dai, que fue publicada también en una lista *cyberpunk* (Márquez, 2015). Wei Dai[17] establece que "una comunidad es definida por la cooperación de sus

[16] Szabo, N (2008). "Bit gold". Unumerated. Disponible en: https://bit.ly/1cdYwoL [Consultado: 20/11/2018].
[17] Dai, W (1998). "B-Money". Disponible en: http://www.weidai.com/bmoney.txt [Consultado: 3/3/2019]

participantes, y una cooperación eficiente requiere de un medio de intercambio (dinero) y un modo de hacer cumplir los contratos". En B-Money describe dos protocolos que pueden ayudar a conseguir estos objetivos (Márquez, 2015). Para ello "asume la existencia de una red no rastreable, donde los receptores y emisores solamente están identificados por pseudónimos […] y donde cada mensaje se firma por el emisor (con su clave privada) y se encripta hacia el receptor (con su clave pública)" (Márquez, 2015: 125).

En el primer protocolo, cada participante mantiene una base datos separada de cuánto corresponde a cada pseudónimo[18]. De acuerdo a Wei Dai[19], este primer protocolo es poco práctico, pero es necesario para saber quién es el propietario del dinero, y es la causa del segundo protocolo. La creación de dinero se realizaría a través de la *PoW*, siendo la cantidad de dinero proporcional a la dificultad del problema (Márquez, 2015). La dificultad del problema sería determinada por toda la red mediante un sistema de votación (Márquez, 2015). Además, el primer protocolo también explica cómo se produciría el envío de dinero entre dos usuarios anónimos y la gestión de los contratos entre dichos usuarios (Márquez, 2015).

Wei Dai[20] establece que el segundo protocolo consistiría en que un subconjunto de participantes (servidores) se encargaría de guardar una copia del dinero que pertenece a cada pseudónimo. Para asegurarse que los servidores se mantienen "honestos", se requiere que cada servidor mantenga una cantidad de dinero en una cuenta especial a modo de depósito para ser utilizado como recompensa o penalización[21].

Como ya se ha dicho anteriormente, en el año 2008 se publica el artículo de Bitcoin, si bien no fue hasta enero de 2009 cuando aparece la versión 0.1[22]. Unos días antes de ser publicada dicha versión el bloque génesis de Bitcoin había sido

[18] Dai, W (1998). "B-Money". Disponible en: http://www.weidai.com/bmoney.txt [Consultado: 3/3/2019]
[19] Ibid
[20] Ibid
[21] Ibid
[22] History of Bitcoin. Disponible en: HistoryofBitcoin.org [Consultado: 13/08/2018]

minado, e incluía el siguiente texto “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”, sobre la posibilidad de un segundo rescate a los bancos[23]. El 12 de enero se produjo la primera transacción de bitcoin entre Satoshi Nakamoto y Hal Finney[24]. Los primeros adoptantes de bitcoin fueron en muchas ocasiones gente que veía en la criptomoneda una revolución que les recordaba a la de la *World Wide Web*, y no estaban interesados en hacer nada con ellos más que ver la evolución de la criptomoneda. De acuerdo con Cheah & Fry (2015), el 70% de los bitcoins existentes se encuentran en cuentas durmientes. En octubre de 2009, casi un año después de ser publicado el artículo de bitcoin, el operador *New Liberty Standards* establece el primer cambio de bitcoin por dólares[25]. El cambio que se fija es el de 1USD por 1.309,03 bitcoin, y para calcularlo *New Liberty Standards* usó una ecuación que incluía el coste de la electricidad para minar bitcoin[26]. Poco antes de acabar el 2009, debido al creciente interés en bitcoin, la red sufre el primer incremento de la dificultad en la minería de bitcoin[27].

Durante el año 2010 se producen varias fechas clave en la historia de Bitcoin. El primer hito clave se produce en mayo de 2010, cuando ocurre la primera transacción real, es decir, por primera vez se acepta bitcoins para pagar un bien. Esta transacción se produce en Florida y la realiza Laszlo Hanyecz, quien paga 10.000 bitcoins por dos pizzas (cuyo valor estaría en torno a 25USD)[28]. Desde ese día, el 22 de mayo en el mundo de las criptomonedas se conoce como el “Bitcoin Pizza Day”[29]. En julio, se crea Mt. Gox que llegará a ser la mayor plataforma de intercambio de criptomonedas mundial[30]. El 15 de agosto de 2010 se detecta la primera vulnerabilidad del protocolo Bitcoin como consecuencia “de la no verificación de las transacciones antes de ser incluidas en la cadena de bloques, lo que permitía crear un número indefinido de Bitcoines” (Márquez,

[23] Lee, T (2014). “Five years of Bitcoin in one post”. The Washington Post. Disponible en: https://wapo.st/2FurQl3 [Consultado: 22/12/2018].
[24] History of Bitcoin. Disponible en: HistoryofBitcoin.org [Consultado: 13/08/2018].
[25] Ibid.
[26] Ibid.
[27] Lee, T (2014). “Five years of Bitcoin in one post”. The Washington Post. Disponible en: https://wapo.st/2FurQl3 [Consultado: 22/12/2018].
[28] History of Bitcoin. Disponible en: HistoryofBitcoin.org [Consultado: 13/08/2018].
[29] Puigvert, M (2016). “Conozca la historia del bitcoin pizza day y… ¡buen provecho!”. Criptonoticias. Disponible en: https://bit.ly/2s4w21V [Consultado: 23/12/2018].
[30] History of Bitcoin. Disponible en: HistoryofBitcoin.org [Consultado: 13/08/2018].

2015: 119). En total debido a esta vulnerabilidad se emitieron 184 mil millones de bitcoins, que posteriormente fueron borrados, y la vulnerabilidad corregida. De acuerdo con Márquez (2015:119), esta vulnerabilidad "junto con la maleabilidad de las transacciones[31] son las únicas vulnerabilidades que se le han detectado al protocolo Bitcoin hasta la fecha". A pesar de este hecho, bitcoin finalizó el año con una cotización de 0.3USD, lo que supone una revalorización del casi el 100% respecto a cómo empezó el año.

En el año 2011, bitcoin se revaloriza alcanzando cotizaciones récord de paridad con el dólar (1USD=1bitcoin) (Márquez, 2015). A principios de ese año, el mercado negro *Silk Road* abre sus puertas y *WikiLeaks* empieza a aceptar donaciones en bitcoins (Márquez, 2015). Además, Mt. Gox sufriría su primer gran ataque, donde fueron robados 60.000 datos[32]. También en 2011, bitcoin sufre su primera burbuja durante el mes de junio, alcanzando nuevas cotizaciones récord[33]. La burbuja "estalla" durante el mismo mes, y la cotización desciende, aunque se mantiene en niveles superiores a los "pre-burbuja". Por último, aparece la criptomoneda Litecoin, creada por Charles Lee. De acuerdo con Márquez (2015), esta criptomoneda es la hermana pequeña de bitcoin y cuenta con muchas similitudes con ella. Entre las diferencias que podemos encontrar, las más importantes son que el procesamiento de un bloque se realiza más rápidamente (2,5 minutos), el límite de Litecoins es de 4 millones y, por último, su proceso de minería es más democrático ya que no requiere de un equipo especial para ello (Márquez, 2015). Actualmente, Litecoin, de acuerdo con CoinMarketcap, es la séptima criptomoneda más importante y la cuarta en cuanto a precio.

El año 2012 está considerado como el año de consolidación de bitcoin. Muchas webs comienzan a aceptarla, entre ellas *WordPress* (Márquez, 2015). La casa de apuestas *SatoshiDice* inicia operaciones[34] y se acabará convirtiendo en una de las más populares. De acuerdo con Böhme *et al*. (2015), durante varios meses

[31] Cuando se modifica el *hash* de una transacción, sin que las claves privadas lo sepan.
[32] History of Bitcoin. Disponible en: HistoryofBitcoin.org [Consultado: 13/08/2018].
[33] Jiménez, J (2017). "Las tres veces que hubo una "burbuja" de Bitcoin para luego hacer crack". Xataka. Disponible en: https://www.xataka.com/empresas-y-economia/las-tres-veces-que-hubo-una-burbuja-de-bitcoin-para-luego-hacer-crack [Consultado: 23/12/2018].
[34] Ibid.

el 80% de las transacciones totales de bitcoin fueron realizadas en la casa de apuestas. En 2012 Brian Armstrong funda Coinbase y aparece la criptomoneda Ripple[35]. Actualmente, Ripple es la segunda criptomoneda más importante del mundo por capitalización de mercado de acuerdo con Coinbase.

A finales de 2012, bitcoin comienza su segunda burbuja, tras la cual la criptomoneda se mantiene en torno a los 100USD[36]. Esta burbuja alcanzó su punto más alto con el corralito de Chipre en marzo de 2013[37]. Los días previos al anuncio del corralito el precio de bitcoin aumentó un 87%[38]. En 2013 se produce uno de los mayores hitos en la historia de bitcoin, que es la desaparición de la web *Silk Road*. Esta web se había convertido en el mayor mercado negro de drogas online, llegando a facturar más de mil millones en ventas[39]. Para poder acceder a la tienda era necesario un software especial criptográfico, llamado "The Onion Router" (TOR), que Bearman[40] define como una capa de invisibilidad que ocultaba a los usuarios y los sitios que visitaban. A través del software TOR, los clientes accedían a la tienda, pagaban con bitcoins y, posteriormente, la droga se enviaba muchas veces simplemente a través del correo postal. El 1 de octubre de 2013 el administrador de la web, Ross Ulbricht que se escondía bajo el alias "Temible Pirata Roberts" fue detenido en San Francisco, y *Silk Road* desapareció[41]. Sin embargo, esto no hizo más que aumentar la popularidad de bitcoin y confirmar que era una divisa increíblemente segura[42]. En 2013 bitcoin sufre su tercera burbuja, superando el precio por primera vez la cota de los 1000 USD. Esta burbuja vino marcada por las noticias de que el Banco Popular de China consideraba que la gente era libre de participar en el mercado de Bitcoin[43].

---

[35] Ibid.
[36] Jiménez, J (2017). "Las tres veces que hubo una "burbuja" de Bitcoin para luego hacer crack". Xataka. Disponible en: https://www.xataka.com/empresas-y-economia/las-tres-veces-que-hubo-una-burbuja-de-bitcoin-para-luego-hacer-crack [Consultado: 23/12/2018].
[37] Ibid
[38] Farrell, M (2013). "Bitcoin prices surge post-Cyprus bailout". CNN. Disponible en: https://cnnmon.ie/2AXBBnW [Consultado: 22/01/2019].
[39] Bearman, J (2015). "The Untold Story of Silk Road, Part 1". Wired. Disponible en: https://bit.ly/2atZpjE [Consultado: 3/01/2019].
[40] Ibid.
[41] Bearman, J (2015). "The Untold Story of Silk Road, Part 2". Wired. Disponible en: https://bit.ly/2osABUh . [Consultado: 3/01/2019].
[42] Villarejo, M (2017). "El Bitcoin y sus límites". Expansión. Disponible en: https://bit.ly/2j5vqp0 [Consultado: 1/07/2018].
[43] Jiménez, J (2017). "Las tres veces que hubo una "burbuja" de Bitcoin para luego hacer crack". Xataka. Disponible en: https://www.xataka.com/empresas-y-economia/las-tres-veces-que-hubo-una-burbuja-de-bitcoin-para-luego-hacer-crack [Consultado: 23/12/2018].

Después, el país asiático adoptaría una postura más crítica respecto a la criptomoneda prohibiendo operaciones con bitcoins. Por último, en 2013 se funda el proyecto Ethereum por Vitalik Buterin (Márquez, 2015). Actualmente, Ether es la segunda criptodivisa más importante del mundo en cuanto a precio y la tercera respecto a capitalización de mercado[44]. De acuerdo con Márquez (2015: 413), "el objetivo de Ethereum es crear un protocolo alternativo para construir aplicaciones descentralizadas" permitiendo a cualquiera escribir contratos inteligentes, entre otras muchas cosas.

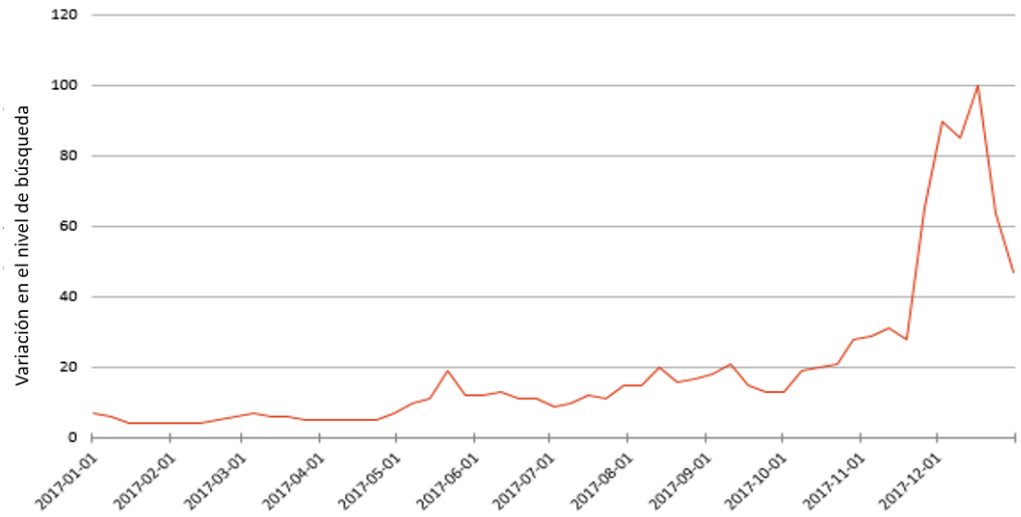
El 24 de febrero de 2014, *Mt. Gox*, la mayor casa de cambio (manejaba el 80% de todas las transacciones de Bitcoin en 2013), entró en bancarrota y solicitó la protección por quiebra en Tokio[45]. El cierre de *Mt. Gox* fue debido a los continuos ataques de hackers, el mayor de ellos consiguió robar 750.000 bitcoin, lo que equivalía en aquel momento a 350 millones de USD[46]. La cotización de bitcoin cayó un 36% desde febrero hasta finales de marzo[47], y esta tendencia bajista se mantuvo a lo largo del año[48].

El año 2015 comenzó con la mayor ronda de financiación de una casa de cambio: Coinbase consiguió 75 millones de USD[49]. Además, Barclays se convierte en el primer banco británico en aceptar bitcoins, aunque solo para donaciones a organizaciones benéficas[50]. En octubre de 2015, el tribunal de la UE equipara el bitcoin a las monedas fíat y un mes más tarde, en España se declaran exentas de IVA las operaciones con criptodivisas (Márquez, 2015). La cotización de bitcoin acaba el 2015 en 426,62 USD, lo que supone una revaloración del 35%[51].

[44] CoinMarketCap. Disponible en: https://coinmarketcap.com/es / [Consultado: 1/12/2018].
[45] Pollock, D (2018). "El lío que era Mt.Gox: cuatro años después". Cointelegraph. Disponible en: https://bit.ly/2RMG4nm [Consultado: 23/12/2018].
[46] Criptotendencia (2018). "Hackers al ataque: los golpes más grandes dados a los intercambios de criptos". Criptotendencia. Disponible en: https://bit.ly/2ALvLWE [Consultado: 20/12/2018].
[47] Pollock, D (2018). "El lío que era Mt.Gox: cuatro años después". Cointelegraph. Disponible en: https://bit.ly/2RMG4nm [Consultado: 23/12/2018].
[48] CoinMarketCap. Disponible en: https://coinmarketcap.com/es / [Consultado: 1/12/2018].
[49]Esparragoza, L (2018). "Un repaso por la historia de Bitcoin tras nueve años de minarse el bloque génesis". Criptonoticias. Disponible en: https://bit.ly/2m9IN8v [Consultado: 20/12/2018].
[50] Kar, I (2015). "Barclays just became the first UK bank to support bitcoin". Quartz. Disponible en: https://bit.ly/2FyHmM1 [Consultado: 21/12/2018].
[51] CoinMarketCap. Disponible en: https://coinmarketcap.com/es / [Consultado: 1/12/2018].

Durante el año 2016, distintas empresas empiezan a aceptar bitcoin, como UBER o Steam[52]. En Suiza, el sistema ferroviario federal acepta bitcoins en las máquinas automáticas de venta de billetes[53]. También es un año marcado por los ataques hackers, en concreto de *Ramsonware,* que secuestraban el ordenador del usuario para pedir un rescate en bitcoins[54]. Además, ese año se produce la segunda reducción a la mitad de la recompensa que reciben los mineros[55]. Después de la tercera burbuja en 2013, el precio de la criptomoneda mantuvo una tendencia alcista, sin embargo, esta revalorización parecía más o menos controlada hasta que, a finales de 2016, la cotización de bitcoin comienza una subida sin precedentes bitcoin comienza el año en 430,72 USD para acabar en 961,24 USD[56], si bien esta escalada en el precio no será nada comparada con la de 2017.

GRÁFICO 4.1: TENDENCIA BITCOIN 2017 (BÚSQUEDA WEB)




Fuente: *Google Trends*

En 2017 se produce la cuarta burbuja de bitcoin, alcanzando nuevas cotizaciones récord. La criptomoneda llego a alcanzar los 20.000 USD, acaparando durante meses la atención mediática debido a su revalorización y a la entrada en el

[52] Esparragoza, L (2018). "Un repaso por la historia de Bitcoin tras nueve años de minarse el bloque génesis". Criptonoticias. Disponible en: https://bit.ly/2m9IN8v [Consultado: 20/12/2018].
[53] Ibid.
[54] Ibid.
[55] Ibid.
[56] CoinMarketCap. Disponible en: https://coinmarketcap.com/es / [Consultado: 1/12/2018].

mercado de empresas profesionales dedicadas a la inversión. En 2017 acabó en torno a los 15.000 USD. Esta revalorización y volatilidad llevó a una amplia difusión en los medios generalistas, y con un rápido vistazo a Google Trends se puede observar cómo el interés en Bitcoin aumenta en aquellos meses con registros récord.

## 5. LA CRISIS FINANCIERA Y BITCOIN

Satoshi Nakamoto dejó escrito en el bloque génesis de Bitcoin este texto: “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”, haciendo referencia a una noticia de *The Times* sobre un posible segundo rescate a los bancos. Si se tienen en cuenta los lazos de Bitcoin con el movimiento *cyberpunk,* mucha gente ve en la crisis financiera el detonante para la aparición de la criptomoneda.

El sistema financiero actual es opaco (BIS, 2009) y de acuerdo con Ito *et al*. (2017), un nuevo sistema financiero descentralizado sería mucho más transparente, ya solo por el hecho de que existirían menos intermediarios. Bitcoin podría hacer el sistema más estable proporcionando formas de monitorizar y rastrear transacciones (Knight, 2017). Una de las causas de la crisis financiera fue la falta de transparencia en los mercados y, como consecuencia, el desconocimiento a la exposición de ciertas firmas a los activos. También la opacidad del mercado llevó a acumular liquidez a las empresas al no saber la exposición de otras empresas y el riesgo existente en el mercado. Con las criptomonedas esto podría mejorar, ya que aportarían transparencia, reducirían intermediarios y las personas fuera del sistema podrían entrar a formar parte de él (Knight, 2017). La tecnología *blockchain* es un registro descentralizado y distribuido, que se podría utilizar perfectamente para aumentar la transparencia en el mercado, si se registraran en dicha *blockchain* las transacciones realizadas. Teniendo en cuenta, además, que a la hora de realizar cualquier transacción en la *blockchain* de Bitcoin se puede añadir cualquier texto o incluso documentos, imágenes, etc.

De acuerdo con Simon Johnson, casi un 20% de la población en EE.UU. no usa servicios bancarios convencionales y, por el contrario, utiliza otros servicios que favorecen la pobreza (Knight, 2017). El uso de criptomonedas podría acercar a

dichas personas al sistema, ya que rebajarían los costes (Knight, 2017). Esto es lo que ha ocurrido en los envíos de remesas internacionales. De acuerdo con White (2017), *Western Union* y *Money Gram* cobran más de un 10% en comisiones. Por el contrario, los remitentes de bitcoin solo cobran un 1%. Otras criptomonedas podrían ayudar a agilizar los pagos internacionales, aunque no bitcoin, ya que no es lo suficiente rápido. El Banco Santander fue uno de los primeros en lanzar un sistema de pagos internacionales con tecnología *blockchain*[57]. Normalmente una transferencia internacional tarda varios días en llegar, sin embargo, con *One Pay* la transferencia llega como tarde al día siguiente[58].

Por último, uno de los usos más comentados y debatidos es su utilización como patrón monetario. Weber (2010) realizó un análisis sobre la hipotética existencia de un patrón bitcoin desde la experiencia del patrón oro. En su artículo, Weber (2010) establece dos claras mejoras respecto al estándar de moneda *fiat*: la primera de ellas es una predicción sobre la evolución de los precios más precisa, ya que el tiempo de minado de nuevos bitcoins está predeterminado; la segunda es que los recursos que actualmente se utilizan como cobertura para fluctuaciones en los tipos de cambio estarían disponibles. Sin embargo, Weber (2010) considera que un patrón bitcoin no se mantendría a lo largo del tiempo, por el riesgo de que bitcoin deje de ser apreciado. Esto puede suceder porque bitcoin sea reemplazado por otra criptomoneda, o por miedos a ataques o fallos en la red (Weber, 2010). El oro, además de tener una demanda monetaria, tiene una demanda no monetaria muy potente ya que es utilizado en muchas industrias, y esto hace que el valor del oro sea más o menos estable (Saifedean, 2018). En el caso de bitcoin, su demanda no monetaria está intrínsecamente relacionada con su demanda como reserva de valor (Saifedean, 2018), lo que conlleva una gran volatilidad en su precio.

[57] Suberg, W. (2018). "Santander, Ripple lanza el primer servicio internacional de pago *blockchain* para clientes minoristas". Cointelegraph. Disponible en: https://bit.ly/2DbBsis [Consultado: 5/01/2019].
[58] Banco Santander (2018). "One Pay: Transferencias internacionales Inmediatas". Banco Santander. Disponible en: https://bit.ly/2DbBAhW [Consultado: 5/01/2019].

## 6. EL FUTURO DE BITCOIN: ¿DINERO O ACTIVO ESPECULATIVO?

De acuerdo con Cheah & Fry (2015), el valor fundamental de bitcoin es cero y se comporta más como un activo que como una moneda. Actualmente, una persona si quiere puede hacer una vida perfectamente normal pagando solo con bitcoins (ya en 2013 una persona era capaz de vivir solo con bitcoins (Hill, 2013)), aunque con limitaciones. Desde entonces el uso y aceptación de bitcoin se ha generalizado. Sin embargo, la elevada y continua volatilidad que experimenta bitcoin complica su uso exclusivo como moneda. Esta elevada volatilidad puede responder a la utilización de bitcoin como un activo especulativo o como un activo refugio. En este último apartado, analizamos la evolución reciente de los precios y rentabilidades de bitcoin para intentar arrojar algo de luz sobre los posibles usos que rigen su comportamiento.

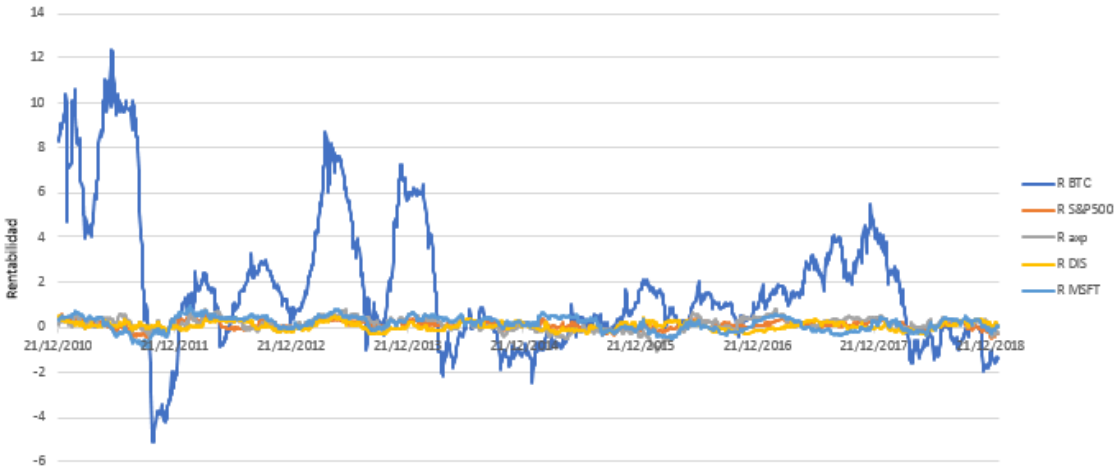
Para el análisis se han estimado la rentabilidad de sus cotizaciones diarias[59] y se ha calculado su media y desviación típica (como medida de la volatilidad total) de las rentabilidades diarias en cada trimestre. Con estos mismos datos, se han obtenido los coeficientes beta según el modelo CAPM, tomando como cartera de mercado el S&P500, como medida de la sensibilidad de las rentabilidades del Bitcoin frente a los cambios del mercado o riesgo sistemático. Dichos estadísticos se han comparado con los correspondientes de empresas cotizadas incluidas en este mismo índice: American Express (AXP), Coca-Cola (Co), Walt Disney (DIS), y Microsoft (MSFT)[60]. Las empresas elegidas pertenecen a distintos sectores para que su comparación con la de bitcoin muestre una evolución de la economía general, y no esté sesgada por la evolución de un sector en concreto.

Los gráficos 6.1, 6.2 y 6.3 muestran la evolución de cada una de estas tres variables (rentabilidad media, volatilidad y coeficientes beta) para los activos señalados. Primeramente, en el gráfico 6.1 se muestra la evolución de las rentabilidades medias anualizadas. Destaca la alta rentabilidad de bitcoin, al igual que sus caídas en comparación con los otros activos. En este gráfico

[59] Los datos han sido obtenidos de Quandl, y las observaciones comienzan el 17/08/2010, que es cuando se dan los primeros datos sobre el precio de Bitcoin.
[60] Los datos han sido obtenidos de Invertia, y las observaciones comienzan el 17/08/2010, que es cuando se dan los primeros datos sobre el precio de Bitcoin.

quedan patentes las grandes fluctuaciones que tiene la criptomoneda, aunque la amplitud de sus “picos” va disminuyendo. Esto se debe al desconocimiento, además del aumento del valor de bitcoin. Por ejemplo, no es lo mismo una revalorización de 1 euro a 2 euros, que supone una rentabilidad del 100%, que una revalorización de 3500 euros a 3700 euros, que es una rentabilidad en torno al 5%. En el primer caso, la variación del precio en Euros es menor, sin embargo, su rentabilidad resulta muy superior.

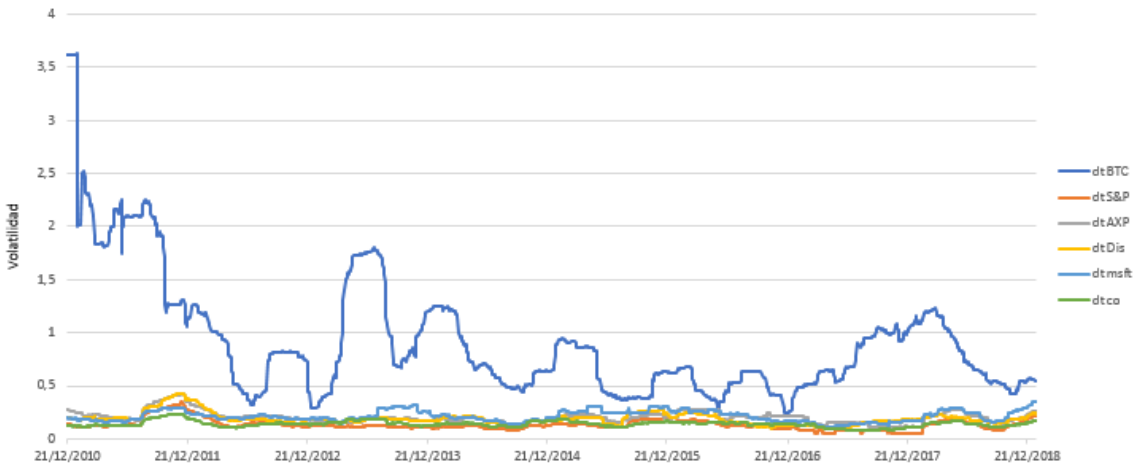
GRÁFICO 6.1: EVOLUCIÓN DE LA RENTABILIDAD




Fuente: Elaboración propia

En el gráfico 6.2 se puede observar cómo la volatilidad de Bitcoin es mucho mayor que la del resto de activos (incluido lógicamente el propio S&P500). La volatilidad de Bitcoin sigue una tendencia histórica a la baja que encuentra su justificación en el desconocimiento inicial (al ser Bitcoin la primera criptomoneda que apareció) y posterior familiarización de los inversores con su naturaleza y características. Sin embargo, con estos datos tampoco podemos inferir que esta tendencia histórica continúe, o por el contrario se estanque en torno a los valores actuales

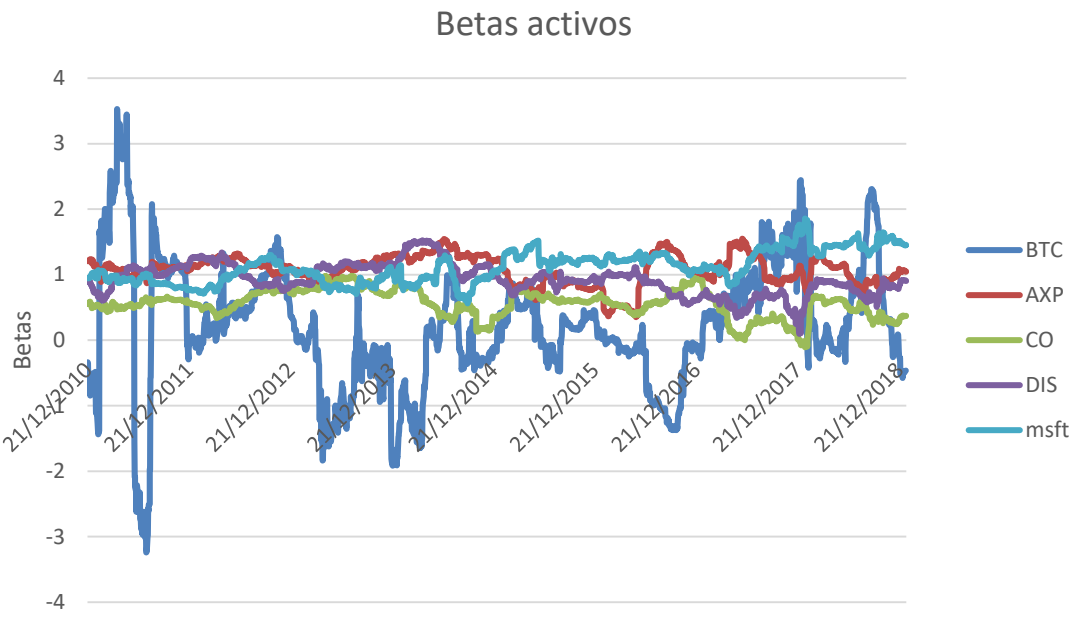
GRÁFICO 6.2: EVOLUCIÓN DE LA VOLATILIDAD DE LA RENTABILIDAD




Fuente: Elaboración propia

El gráfico 6.3 muestra la evolución de las betas. La beta de la cartera de mercado por definición es igual a 1 y aquellos valores por encima de ella son considerados activos especulativos mientras que cuando se encuentran por debajo son activos refugios. En el caso de bitcoin lo más destacable es la elevada volatilidad de su coeficiente beta fluctuando desde elevados valores positivos, que indicarían su carácter de activo especulativo, a valores muy negativos, que serían indicio de su utilización como un activo refugio. Además, a primera vista no parece existir un patrón explicable por las etapas del ciclo del mercado, como se verá más adelante.

GRÁFICO 6.3: EVOLUCIÓN DE LAS BETAS DE LOS ACTIVOS




Fuente: Elaboración propia

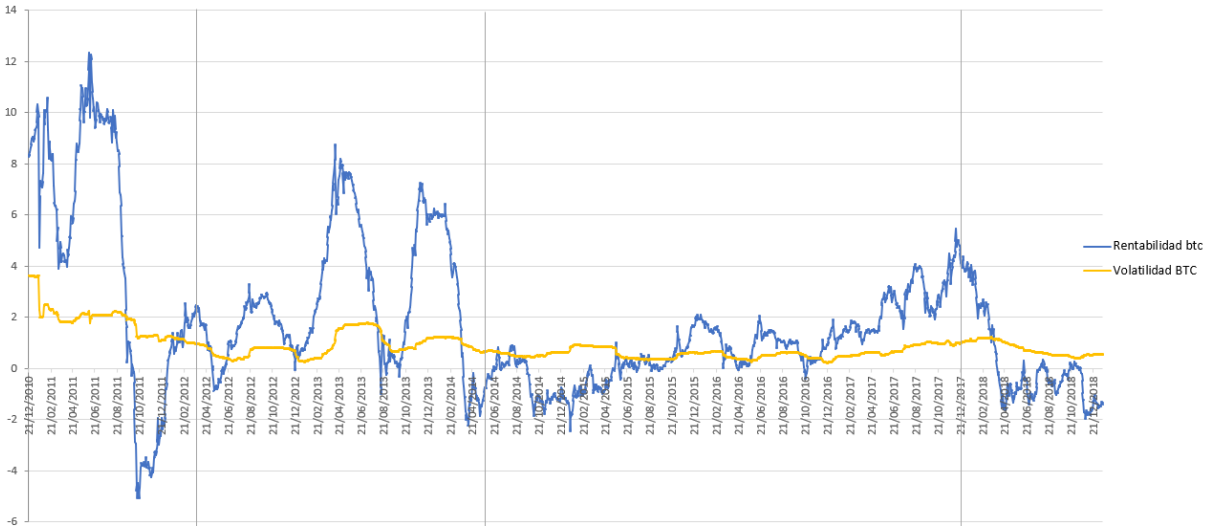
Los gráficos 6.4 y 6.5 muestran la relación entre la volatilidad y la rentabilidad de bitcoin y el S&P500 respectivamente.[61] Para el análisis se ha dividido la serie histórica en cuatro períodos.

El primer periodo viene marcado por la mayor caída en la rentabilidad de toda la serie de bitcoin. Por su parte, la cartera de mercado tiene también una caída muy pronunciada en su rentabilidad, y es anterior a la de la criptomoneda. El segundo periodo viene caracterizado por ser el único donde se puede decir que existe cierta "simetría" entre bitcoin y el S&P500. Esta simetría consiste en cuatro caídas de la rentabilidad, que son mucho más claras en la criptomoneda que en la cartera de mercado. En el tercer periodo, bitcoin comienza con rentabilidades muy bajas. No obstante, durante todo el periodo mantendrá una tendencia al alza que solo desaparecerá al final del mismo. Por su parte, la cartera de mercado tiene un par de caídas de su rentabilidad y, en general, se puede decir que su tendencia es más o menos "estable". Por último, el cuarto periodo viene marcado por una fuerte caída tanto de la rentabilidad de bitcoin como de la cartera de mercado.

[61] Se ha decidido separarlos en dos gráficos, pues la elevada amplitud de los valores de Bitcoin impide la comparación adecuada en un único gráfico..

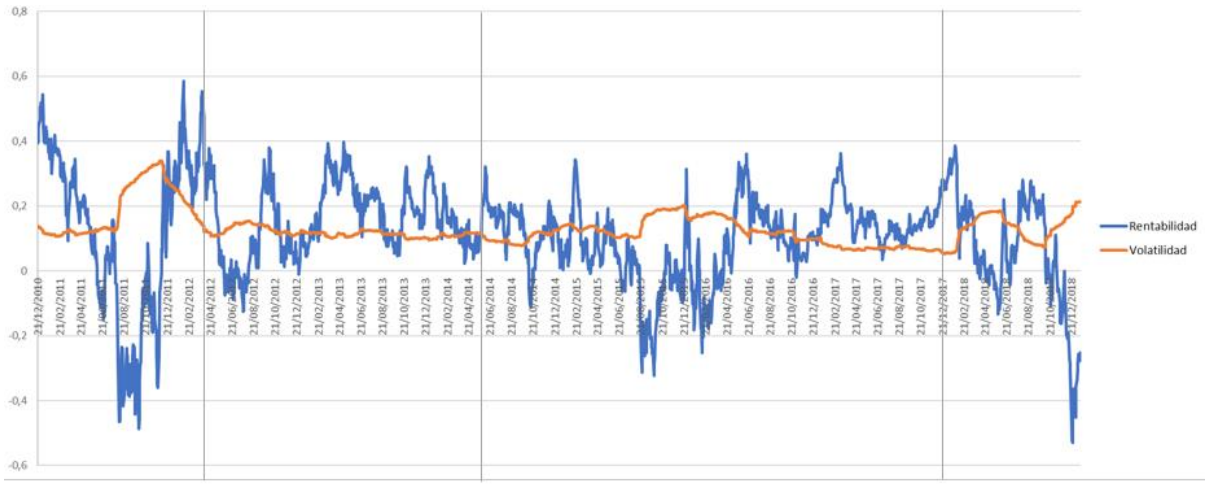
Como se puede ver, bitcoin no guarda relación con S&P500 y no se comporta como un activo refugio. Por ejemplo, en el tercer periodo la beta de bitcoin se comporta como refugio cuando el mercado está al alza y no al revés. Además, a la hora de analizar bitcoin es importante tener en cuenta que fue la primera criptomoneda que existió y abrió las puertas a un mercado totalmente nuevo dando lugar a la "criptoeconomía", influyendo en la evolución de su rentabilidad y riesgo. En cualquier caso, bitcoin no se comporta como ningún activo que haya existido, tampoco muestra características propias de un activo refugio, pero sí evidencia saltos en la rentabilidad y volatilidad típicos de un activo especulativo. Además, Lischke & Fabian (2016) constataron diferencias entre países respecto a su uso, por lo que sería interesante la realización de un estudio en mayor profundidad al respecto. Por último, Bitcoin también es muy sensible a la legislación, ya que actualmente no existe un estándar, y en algunos países cambia continuamente o no existe.

GRÁFICO 6.4: EVOLUCIÓN RENTABILIDAD Y VOLATILIDAD DE BITCOIN




Fuente: Elaboración propia

GRÁFICO 6.5: EVOLUCIÓN RENTABILIDAD Y VOLATILIDAD DE S&P500




Fuente: Elaboración propia

## 7. CONCLUSIÓN

La tecnología *blockchain* ha abierto un nuevo abanico de posibilidades para su aplicación en muchos sectores, desde el comercio internacional hasta los sistemas de votación actuales. Pero una de sus mayores aplicaciones se encuentra en el ámbito financiero. La crisis de 2008 mostró las debilidades del sistema financiero actual y cómo había margen de mejora. Bitcoin parece ser consecuencia de dicha crisis dado que surge para dar solución a ciertos problemas existentes en el mercado financiero.

Bitcoin facilita la desintermediación en el sistema financiero y, por tanto, mejora la competitividad en el mercado, aunque también está creando nuevos agentes intermedios como pueden ser los *exchanges*, los servicios de carteras online o las *mining pools*. Por lo tanto, Bitcoin puede sustituir a ciertos agentes tradicionales del sistema financiero, pero también estimula la aparición de otros nuevos.

Uno de los usos de bitcoin más comentados es el de medio de pago o patrón monetario, sin embargo, la continua volatilidad que sufre bitcoin complica esta utilidad. Bitcoin como patrón monetario tendría ciertas ventajas respecto al actual sistema como apuntaba Weber (2014). No obstante, que la criptomoneda se

convierta en patrón monetario en un futuro cercano se antoja complicado por cómo está diseñada la propia criptomoneda.

Desde su aparición, bitcoin ha sufrido en total cuatro burbujas y registra elevadas volatilidades. A través del estudio realizado se ha podido comprobar como bitcoin actualmente es un activo especulativo, y está lejos de poder ser considerado un activo refugio o un método de pago. Un estudio más profundo de la criptomoneda se podría realizar a través de técnicas econométricas más avanzadas aplicadas a información detallada por zonas geográficas.

Para concluir es importante destacar que estamos ante un activo completamente desconocido y, por lo tanto, tampoco se puede afirmar con rotundidad que en el futuro siga siendo un activo con fines especulativos. La criptomoneda abrió un mercado totalmente nuevo que solo el tiempo dirá como acabará.

## 8. CONCEPTOS

- Aseguradoras *monoline:* otorgan una garantía financiera a cambio de una prima, abaratando de esta forma la financiación privada[62].
- *Asset-Backed Comercial Paper (ABCP):* Deuda a corto plazo asegurada con activos físicos.
- *Blockchain:* registro distribuido de datos que de forma cronológica se va agrupando en bloques de forma descentralizada.
- Bloque Génesis: El primer bloque que se genera en una *blockchain*.
- Criptomoneda: aquella moneda digital que mediante la tecnología *blockchain*, permite realizar transacciones seguras y sin necesidad de un intermediario.
- Cuentas mancomunadas institucionales (Institutional Cash Pools): grandes cuentas centralizadas pertenecientes a empresas no financieras y a inversores institucionales como gestores de activos, prestamistas de valores y fondos de pensiones. (Pozsar, 2011).

[62] Invertir con éxito (2008). “Monoline: Una palabra en el desencadenamiento de la crisis bursátil”. Cinco Días. Disponible en: https://bit.ly/2OezzYs [Consultado: 25/07/2018].

- *Haircuts* o recortes de valoración*:* "reducción que se aplica al valor de un activo"[63].
- Hash: secuencia alfanumérica que comprime siempre igual una información. En el caso de *blockchain*, los hash sirven para unir los bloques.
- Hipotecas *Subprime*: préstamos que se concedían para la adquisición de bienes a clientes de escasa solvencia, es decir, con un alto riesgo de impago [64].
- NONCE: número arbitrario que sirve para la autenticación de datos y solo se puede usar una vez.
- Modelo *Origin-to-distribute:* aquellos casos en los que los acreedores no tienen el objetivo de mantener el préstamo hasta su vencimiento, si no que los venden a otras instituciones o inversores [65].
- *Monetary Market Mutual Funds (MMMFs):* "aquellas Instituciones de Inversión Colectiva cuyas participaciones son, en cuanto a su liquidez, sustitutos próximos de los depósitos". (Villanueva Fresán, 2009).
- *Repos:* "operación de recompra en la que una entidad financiera vende a un inversor un activo con el compromiso de comprarlo en una fecha determinada a un precio determinado"[66].
- *Shadow Banking:* forma de intermediación crediticia, formada por entidades que se encuentran fuera del sistema bancario tradicional. (FSB, 2011).
- *Swaps:* acuerdo financiero por el que una parte se compromete a hacer unos pagos periódicos a cambio de recibir una serie de cobros de la otra parte.[67]

[63] BCE (2016). "¿Qué son los recortes de valoración?" Disponible en: https://bit.ly/2N2ygaC [Consultado: 26/09/2018].
[64] López Domínguez, I. "Crisis Subprime". Expansión. Disponible en: https://bit.ly/2Qao16b [Consultado: 4/09/2018].
[65] Nasdaq. "Originate-to-Distribute". Nasdaq. Disponible en: https://bit.ly/2Dwbybc [Consultado: 23/09/2018].
[66] BBVA (2015). ¿Qué es un repo?. Disponible en: https://bbva.info/2xDrEup [Consultado:26/07/2018].
[67] BBVA (2017). "Swaps. Qué son y cómo funciona". Disponible en: https://bbva.info/2OUAf2A [Consultado: 23/07/2018].

- "*Too Big To Fail":* aquellas instituciones que, por su tamaño y complejidad, si se declarara en bancarrota, su quiebra tendría importantes repercusiones para la economía y el sistema financiero. (Bernanke, 2010).
- Valor liquidativo: Precio de las participaciones del fondo de inversión. Su valor se calcula dividiendo el patrimonio del fondo entre el número de participaciones[68].

## 9. BIBLIOGRAFÍA


- Bank for International Settlements (BIS) (2009). "The Global Financial Crisis". En: Bank for International Settlements. 79TH Annual Report. Basel: BIS, pp 16-39.
- Bernanke, B (2010). "Testimony in front of the Financial Crisis Inquiry Commision". Disponible en: https://bit.ly/2xQrejp [Consultado: 26/07/2018].
- Böhme, R *et al*. (2015). "Bitcoin: Economics, technology and governance". *Journal of Economics Perspectives,*29 (2), pp. 213-238.
- Bonneau, J; Miller, A; Clark, J; Narayanan, A; Kroll, J.A., Felten, E.W (2015). "SoK: Research perspectives and challenges for bitcoin and cryptocurrencies". *IEEE Symposium on Security and Privacy*, art. No. 7163021, pp. 104-121.
- Chaum, D (1981). "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms". Disponible en: https://bit.ly/2HdJSKg [Consultado: 23/12/2018].
- Cheah, E.-T. and Fry, J. (2015) "Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin", Economics Letters, 130, pp. 32–36. doi: 10.1016/j.econlet.2015.02.029.
- Dwyer, G.P. (2015). "The economics of Bitcoin and similar private digital currencies" Journal of Financial Stability, 17, pp. 81-91.
- Financial Stability Board (FSB) (2011). "Shadow Banking: Scoping the issues". Disponible en: https://bit.ly/2QUO7uR [Consultado: 5/09/2018]


[68] BBVA. "¿Qué es el valor liquidativo de un fondo de inversión". Disponible en: https://bit.ly/2zsrK9u [Consultado: 26/07/2018].

- Gorton, G; Mettrick, A (2012) “Getting up to speed on the Financial Crisis: A One-Weekend-Reader’s Guide”. Journal of Economic Literature, American Economic Association, vol. 50(1), pages 128-50, March.
- International Monetary Fund (IMF) (2010). “Systemic Liquidity Risk: Improving the Resilience of Financial Institutions and Markets”. En: International Monetary Fund. *World Economic Outlook, October 2010: Recovery, Risk and Rebalancing.* IMF, pp 58-83.
- Ito, J *et al*. (2017). “The *Blockchain* Will Do to the Financial System What the Internet Did to Media”. *Harvard Business Review*. Disponible en: https://bit.ly/2n6PqZ0 [Consultado: 3/01/2019].
- Knight, W (2017). “Can Bitcoin Be the Foundation of a Fairer Financial System?”. *MIT Technolog Review*. Disponible en: https://bit.ly/2oK4LzU [Consultado: 3/01/2019].
- Kristoufek, L. (2015). “What are the main drivers of the bitcoin price? Evidence from wavelet coherence analysis”. PLoS ONE, 10 (4) art. No. e0123923.
- Lischke, M. Fabian, B. (2016). “Analyzing the bitcoin network: The First Four Years”. *Future Internet*, 8 (1), art. No. 7.
- Márquez Solís, S (2016). *Bitcoin. Guía completa de la moneda del futuro.* Madrid: RA-MA Editorial.
- Pozsar, Z (2011). “Institutional Cash Pools and the Triffin Dilemma of the U.S. Banking System”. *International Monetary Fund.*
- Preuckschat, A. (2017): “Los fundamentos de la tecnología Blockchain”. En Preuckschat, A. (Coord) (2017). *Blockchain: La Revolución Industrial de Internet.* Barcelona: Grupo Planeta.
- Reinhart, C; Rogoff, K (2011). “From Financial Crash to Debt Crisis”. *American Economic Review,* 101 pp. 1676-1706.
- Saifedean, A (2018). *El patrón Bitcoin. La alternativa descentralizada a los bancos centrales.* Barcelona: Grupo Planeta.
- Tapscott, D; Tapscott, A (2016). *Blockchain Revolution. How the technology behind Bitcoin is changing money, business, and the world.* Nueva York: Penguin Random House LLC.
- Villanueva Fresán, M.Victoria (2009). “Las características de los fondos de inversión monetarios en distintas jurisdicciones”. *Monografía nº 36:*

*Julio, 2009.* CNMV. Disponible en: https://bit.ly/2NHYPXX [Consultado: 22/07/2018]

- Weber, W. (2010). “A Bitcoin Standard: Lessons from the Gold Standard”. *Bank of Canada*. Disponible en: https://bit.ly/2RHvBtp [Consultado: 4/01/2019].
- White, L (2017). “The market for cryptocurrencies”. *GMU Working Paper in Economics.* No. 14-45. Disponible en: https://bit.ly/2CmoMn7 [Consultado: 3/01/2019].