



UNIVERSIDAD NACIONAL DE RÍO
CUARTO



FACULTAD DE CIENCIAS ECONÓMICAS

Bitcoin, ¿la moneda del futuro? Un análisis de sus características e implicancias

AUTOR: González, Gabriel Franco.

DIRECTOR: Polinori, Héctor.

CODIRECTOR: Milanesio, Javier.

LICENCIATURA EN ECONOMÍA. AÑO 2018.

ÍNDICE GENERAL

Índice general	3
Lista de figuras	6
Resumen – Abstract	7
Capítulo 1: Planteamiento metodológico	9
1.1. Introducción	9
1.2. Planteamiento del problema	10
1.3. Objetivos de investigación	10
1.3.1. Objetivos generales	10
1.3.2. Objetivos específicos	10
1.4. Metodología de trabajo	11
1.5. Justificación teórica y práctica de la investigación	11
1.6. Viabilidad de la investigación	12
1.7. Resultados de la investigación	12
Capítulo 2: Historia y evolución del dinero	13
2.1. Dinero: concepto, funciones y propiedades	13
2.2. El dinero y su evolución a lo largo de la historia del hombre	17
2.2.1. El valor del intercambio: el trueque	17
2.2.2. El dinero mercancía	18
2.2.3. Oro y plata: dos metales especiales	19
2.2.4. La acuñación de las primeras monedas	19
2.2.5. Sobre el origen del papel moneda	20
2.2.6. El patrón oro y el paso al dinero fiduciario	21
2.3. Avances recientes en la evolución del dinero: dinero electrónico, monedas virtuales y criptomonedas	23

Capítulo 3: Antecedentes y nacimiento de Bitcoin	29
3.1. Los cimientos de Bitcoin: La comunidad Cypherpunk	29
3.2. Nacimiento de Bitcoin	30
3.3. Acerca de Satoshi Nakamoto	35
Capítulo 4: ¿Qué es realmente Bitcoin? Un análisis de sus propiedades	37
4.1. ¿Qué es Bitcoin?	37
4.2. Participantes del sistema Bitcoin	38
4.3. ¿Cómo funciona Bitcoin?	39
4.4. Transacciones de Bitcoins	40
4.5. ¿Es Bitcoin o su tecnología Blockchain?	42
4.6. Obtención de Bitcoins.	47
4.7. ¿Dónde se almacenan los Bitcoins?	48
4.8. Fundamentos económicos de Bitcoin	49
4.9. ¿Cómo se crean los Bitcoins? El proceso de minería.	50
4.10. Ventajas y desventajas de Bitcoin. Fortalezas y debilidades.	53
4.10.1. Ventajas de Bitcoin	53
4.10.2. Desventajas de Bitcoin	56
Capítulo 5: Bitcoin en números	60
5.1. Cotizaciones	60
5.2. ¿El precio de Bitcoin ha sido manipulado por Bots?	67
5.3. Capitalización de mercado	69
5.4. Número de transacciones diarias	71
5.5. Número de Bitcoins en circulación	72
5.6. Tiempo medio de espera para la confirmación de una transacción	72
5.7. Cuota de mercado de los principales pools mineros	73
Capítulo 6: Análisis de la verdadera naturaleza de Bitcoin	75
6.1. Bitcoin como dinero	75
6.2. Bitcoin como activo	80
6.3. ¿Bitcoin es una burbuja?	82

6.4. Bitcoin como esquema Ponzi	86
6.5. Bitcoin como facilitador de actividades ilegales	87
Capítulo 7: Análisis de la regulación emergente de Bitcoin	90
7.1. Actitudes permisivas	92
7.2. Actitudes en disputa y hostiles	97
7.3. Bitcoin en Argentina	100
7.3.1. ¿Cómo ha sido la recepción de Bitcoin por parte de las autoridades en Argentina?	101
Conclusiones	104
Bibliografía	106

LISTA DE FIGURAS

Figura 2.1: Diferentes modalidades de dinero.	24
Figura 2.2: Esquemas de monedas virtuales.	25
Figura 4.1: Red basada en un único servidor vs. Red P2P.	38
Figura 4.2: Ejemplo de billetera virtual.	48
Figura 4.3: Diferentes denominaciones de Bitcoin.	49
Figura 4.4: Evolución del stock de BTCs en el mercado.	51
Figura 4.5: Recompensas por minería (Número de BTCs por bloque).	52
Figura 4.6: Captura de la web “ <i>Silkroad Marketplace</i> ” antes de su cierre.	58
Figura 5.1: Cotización de BTC (en USD). Período Mayo 2009 a Enero 2013.	61
Figura 5.2: Cotización de BTC (en USD). Período Febrero 2013 a Febrero 2014.	62
Figura 5.3: Cotización de BTC (en USD). Período Enero 2014 a Enero 2015.	64
Figura 5.4: Cotización de BTC (en USD). Período Enero 2015 a Enero 2016.	64
Figura 5.5: Cotización de BTC (en USD). Período Enero 2016 a Enero 2017.	65
Figura 5.6: Cotización de BTC (en USD). Período Enero 2017 a Enero 2018.	66
Figura 5.7: Cotización de BTC (en USD). Período Enero 2018 a Febrero 2018.	67
Figura 5.8: Capitalización de mercado de BTC (en USD). Período Enero 2011 a Febrero 2018.	69
Figura 5.9: Capitalización de mercado de BTC (en USD). Período Enero 2017 a Febrero 2018.	70
Figura 5.10: Capitalización de BTC vs. Empresas más valiosas del mundo.	71
Figura 5.11: Número de transacciones diarias de Bitcoin. Enero 2009 a Enero 2018.	71
Figura 5.12: Total de Bitcoins en circulación. Enero 2009 a Enero 2018.	72
Figura 5.13: Tiempo medio de confirmación de una transacción.	73
Figura 5.14: Cuota de mercado de los principales pools mineros.	74
Figura 6.1: Comparación entre instrumentos bancarios vs. Efectivo vs. Bitcoin.	79
Figura 6.2: Tulipmanía y Burbuja de la Compañía del Mar del Sur.	83
Figura 6.3: Estallido de la burbuja de las “ <i>punto com</i> ”.	83
Figura 6.4: Etapas de una burbuja de acuerdo a Jean Paul Rodrigue.	84
Figura 6.5: Evolución en la cotización de BTC. Julio 2011 a Enero 2018.	85
Figura 7.1: Actitudes de los diferentes países frente a Bitcoin.	92

RESUMEN - ABSTRACT

RESUMEN

Las criptomonedas, más conocidas como monedas virtuales, están ganando notoriedad gracias a la difusión que los medios de comunicación les están proporcionando con las frecuentes noticias sobre el tema. Las ventajas de su anonimato y los crecientes intereses financieros que comienzan a rondar a este tipo de activos están dando lugar a un incremento considerable del número de usuarios que las utilizan así como de su cotización. En este trabajo se realiza un análisis de los fundamentos de funcionamiento en los que se basa la más popular de estas monedas virtuales: Bitcoin.

El desarrollo del trabajo se estructura de la siguiente manera: en el primer capítulo se realiza el planteamiento metodológico de la investigación, señalando el problema que la motivó, los objetivos generales y específicos, la metodología de trabajo empleada, como así también las consecuencias que se pretende que surjan de la misma. A continuación, en el segundo capítulo se analizan los atributos que debe poseer un bien para ser utilizado eficientemente como dinero, como así también las funciones que éste debe cumplir, y, además, se realiza una síntesis de su evolución a lo largo de la historia de la humanidad, para llegar a una mejor comprensión del mismo y de sus distintas formas. En el tercer capítulo se indaga acerca de los antecedentes históricos, el nacimiento y la identidad del fundador de Bitcoin. En el cuarto capítulo se estudia a Bitcoin, la moneda virtual más popular del momento, y se profundiza acerca de su funcionamiento, la ideología que lo respalda, como así también sus ventajas y desventajas. En el quinto capítulo se abordan los datos relacionados a Bitcoin, tanto en lo que respecta a sus cotizaciones históricas, como así también el número de transacciones diarias, el stock de unidades de esta moneda, entre muchas otras estadísticas. En el capítulo sexto se analiza la verdadera naturaleza de Bitcoin, tratando de revelar qué es en realidad Bitcoin desde el punto de vista económico. En el séptimo capítulo se realiza una exploración acerca de las reacciones que han tenido las autoridades de los distintos países con respecto a la regulación de las criptomonedas. Finalmente, se presentan las conclusiones más importantes de la investigación y la bibliografía utilizada.

ABSTRACT

Cryptocurrencies, better known as virtual currencies, are gaining notoriety thanks to the publicity

that the media are providing them with the frequent news on the subject. The benefits of their anonymity and the growing financial interests that are beginning to surround these types of assets are leading to a considerable increase in the number of users who use them as well as their prices. This document analyzes the fundamentals of performance on which the most popular of these virtual currencies is based: Bitcoin.

The development of the work is structured in the following way: in the first chapter the methodological approach of the research is made, indicating the problem that motivated it, the general and specific objectives, the methodology of work employed, as well as the consequences that pretend that they arise from it. Then, the second chapter analyzes the attributes that a good must possess to be used efficiently as money, as well as the functions that it must fulfill, and, in addition, a synthesis of its evolution is made throughout history of humanity, to reach a better understanding of it and its different forms. In the third chapter it is inquired about the historical background, the birth and the identity of the founder of Bitcoin. In the fourth chapter, Bitcoin, the most popular virtual currency of the moment, is studied, and its operation, the ideology that supports it, as well as its advantages and disadvantages are studied. The fifth chapter deals with data related to Bitcoin, both in terms of its historical prices, as well as the number of daily transactions, the stock of units of this currency, among many other statistics. In the sixth chapter, the true nature of Bitcoin is analyzed, trying to reveal what Bitcoin is really from the economic point of view. In the seventh chapter an exploration is made about the reactions that the authorities of the different countries have had with respect to the regulation of cryptocurrencies. Finally, the most important conclusions of the research and the bibliography used are presented.

CAPÍTULO 1: PLANTEAMIENTO METODOLÓGICO

1.1. Introducción

La historia de los medios de pago está marcada por el éxito del dinero en efectivo. Desde que se acuñaron las primeras monedas, en el siglo VII antes de Cristo, el efectivo ha vertebrado el intercambio de bienes y servicios y aún hoy es el medio de pago claramente predominante en el mundo. Sin embargo, la revolución tecnológica ha acelerado el proceso de sustitución del dinero por otros medios de pago. Con la explosión del uso de internet y de las redes sociales, la utilización de medios virtuales de pago también se ha generalizado para facilitar las operaciones y obtener una mayor seguridad en las transacciones. De esta manera, servicios como *PayPal* o *Google Wallet*, entre muchos otros, proporcionan un monedero virtual con el que se pueden realizar pagos en infinidad de servicios de todo tipo prestados en la red.

Sin embargo, en ciertos entornos se ha hecho necesario ir un paso más allá con objeto de alcanzar el anonimato total en las transacciones. En este contexto, donde el anonimato resulta imprescindible para los artífices de ciertas actividades en la red, surgen las denominadas monedas virtuales. Se trata de activos equivalentes al dinero en metálico, dado que no identifican al poseedor y no queda constancia de las operaciones que éste lleva a cabo.

A pesar de su proliferación, la atención del mercado se concentra en unas pocas iniciativas de gran éxito a nivel mundial, entre las que destaca, por su creciente popularidad en los medios de comunicación y por las cotizaciones que ha llegado a alcanzar en los últimos meses, el caso de Bitcoin.

La moneda virtual “Bitcoin” nació con la idea de descentralizar los pagos entre usuarios, eliminando la necesidad de instituciones financieras que actúen como intermediarios en las transacciones. Aunque no exenta de polémica, esta solución ha demostrado en la práctica ser funcional y válida para la realización de transacciones y su adopción está creciendo en todo el mundo.

Por otra parte, desde una perspectiva teórica, Bitcoin refleja la puesta en práctica de ideas donde los medios de pago se independizan de los sistemas bancarios y gubernamentales, lo cual coincide en los tiempos actuales con crisis importantes en el funcionamiento de tales sistemas que se desencadenaron a partir de la explosión de la burbuja “*subprime*”.

Esta criptomoneda es una innovación financiera que ha acaparado elogios y críticas. Se cree que

tiene el potencial de promover un comercio global más eficiente. Brinda ciertas ventajas frente a los sistemas de pago tradicionales, pero también representa, como cualquier otra moneda, desventajas que han provocado que en Tailandia, China y Ecuador se hayan prohibido las transacciones con este medio dentro de su territorio. Esta situación es algo que quizá puedan llegar a imitar otros países, por los riesgos de pérdida de valor que conllevan las transacciones con esta moneda virtual, el anonimato de los participantes y la dependencia tecnológica. El Parlamento Europeo, en su resolución de Mayo de 2016 destacó el potencial de las monedas virtuales para mejorar y abaratar transacciones financieras y mecanismos de pago, aunque también advirtió de algunos riesgos relacionados con la incertidumbre y la falta de control.

1.2. Planteamiento del problema

Bajo estas condiciones y términos expresados, surge el siguiente problema de investigación:

¿De qué se trata esta moneda virtual, denominada Bitcoin, ¿de qué manera surge y cuál es su naturaleza y su modo de funcionamiento?

1.3. Objetivos de investigación

1.3.1. Objetivo general

El objetivo general de la investigación es estudiar una moneda virtual, descentralizada y pseudoanónima conocida como “Bitcoin”, que ha surgido en nuestra sociedad en el transcurso de la última década. Concretamente, se pretende echar luz acerca del surgimiento de esta criptomoneda, su naturaleza y su modo de funcionamiento, y además analizar cuáles han sido las reacciones de los diferentes países frente al surgimiento y proliferación de esta moneda.

1.3.2. Objetivos específicos

- a) Realizar una revisión de la evolución del dinero a lo largo de la historia del hombre.
- b) Destacar las diferentes características que debe reunir un bien para poder ser utilizado como dinero, como así también las principales funciones que éste debe cumplir satisfactoriamente para utilizarse ampliamente.
- c) Analizar los avances recientes en cuanto a medios de pago: dinero electrónico, billeteras virtuales, criptomonedas; además, examinar la tecnología, la operatoria y los conceptos básicos detrás de las criptomonedas.
- d) Explorar de qué manera surge la criptomoneda denominada “Bitcoin” y su evolución en los últimos años.

- e) Examinar las características del Bitcoin, su funcionamiento y las condiciones del mercado de Bitcoin. Indagar acerca de sus fortalezas y debilidades.
- f) Analizar el estado de situación de Bitcoin en Argentina.
- g) Sintetizar las principales regulaciones a nivel internacional de la moneda Bitcoin. Plantear las respuestas de las autoridades argentinas en cuanto a la regulación de las criptomonedas y, en particular, de Bitcoin.

1.4. Metodología de trabajo

El desarrollo del presente trabajo sigue una metodología exploratoria. Pretende recoger, identificar y documentar acerca de una cuestión poco abordada hasta el momento, como son los medios de pago virtuales y las criptomonedas, buscando aumentar el grado de familiaridad con el fenómeno de las monedas virtuales, e identificar conceptos y variables promisorios, así como sus implicancias potenciales.

Se recurre a diversos métodos de análisis en el presente trabajo de investigación, a fin de lograr el cumplimiento de los objetivos planteados. En primer lugar, se acude al método histórico a fin de realizar una síntesis de la amplia literatura acerca de la evolución del dinero a lo largo de la historia de la humanidad y de las características de cada uno de los bienes que han sido utilizados como dinero por el hombre.

Posteriormente, se efectúa una revisión y contrastación de estas características teóricas con la situación actual del Bitcoin, analizando la tecnología detrás de esta moneda virtual y los factores que inciden tanto en su oferta como en su demanda. Para el logro de este objetivo se apela a numerosas fuentes bibliográficas como libros, informes académicos y de organismos internacionales.

Por otra parte, también se realiza un estudio de aplicación de las características del Bitcoin para concretar las potenciales implicaciones para las autoridades económicas mundiales, enfrentadas al desafío de la prohibición o la regulación de este tipo de monedas virtuales. Además, se desarrolla en último lugar una investigación sobre las principales tendencias regulatorias alrededor del Bitcoin. Para ello se ha recurrido principalmente a actas de los gobiernos de varios países, informes académicos y a numerosos artículos periodísticos.

1.5. Justificación teórica y práctica

A través del uso de un programa público, Bitcoin permite la transmisión de fondos de una moneda inexistente en un formato físico entre usuarios anónimos. Por primera vez en la historia

contemporánea existe una forma de transmisión de valor monetario fuera del área de control de los gobiernos, bancos o autoridad central de cualquier tipo. Por lo tanto, un tema de gran interés y relevancia es si realmente su comportamiento en la sociedad es el de una moneda como las que actualmente circulan y son de curso legal en los países.

Políticos, inversores y el resto de la sociedad están tratando de comprender la naturaleza de esta innovación financiera y las implicaciones que tendrá en la sociedad. Debido a esto, constituye un tema de gran relevancia el análisis del concepto de Bitcoin, su funcionamiento, y la tecnología detrás de esta innovación, aspectos que motivaron el planteamiento de esta investigación.

Se considera que la presente investigación contribuirá a formar una base para profundizar más en el tema y de esta manera enriquecer la discusión sobre el papel que cumplen en la actualidad las criptomonedas y en cuanto a las perspectivas que existen en torno a ellas en un futuro no tan lejano, tanto desde el punto de vista de sus posibles usuarios como también de las autoridades económicas encargadas de su regulación.

1.6. Viabilidad de la investigación

La investigación resulta viable, ya que se cuenta con los recursos necesarios para efectuarla. En primer lugar, se cuenta con una amplia bibliografía necesaria para documentar la evolución del dinero a lo largo de la historia del hombre. Por otra parte, se ha detectado la existencia de numerosos estudios, informes y publicaciones académicas y de organismos internacionales, acerca de las criptomonedas y, en particular, de Bitcoin. Además, existe gran cantidad de portales, páginas web y blogs que publican datos estadísticos acerca de las cotizaciones, la capitalización de mercado de Bitcoin, el número de transacciones efectuadas, entre otras estadísticas.

Finalmente, se cuenta con publicaciones periódicas y notificaciones de los distintos países referidos a las medidas regulatorias relacionadas a Bitcoin.

1.7. Resultados de la investigación

Se pretende echar luz acerca del fenómeno de las criptomonedas, como último paso en la evolución del dinero, estudiando acerca de las características y propiedades de las mismas, las regulaciones más adecuadas para su uso, intentando contribuir en futuras investigaciones relacionadas a las innovaciones en los medios de pago.

CAPÍTULO 2: HISTORIA Y EVOLUCIÓN DEL DINERO: DESDE EL DINERO MERCANCÍA A LAS CRIPTOMONEDAS

El dinero es una mercancía que ha surgido, al igual que el resto, como consecuencia de una demanda para satisfacer ciertas necesidades. Estas necesidades son las de facilitar los intercambios de los demás bienes y servicios que existen en la economía. A lo largo de la historia del dinero, desde la utilización de semillas de cacao hasta las formas actuales del mismo, se puede observar una constante evolución para mejorar la eficiencia y la eficacia en la satisfacción de la necesidad de realizar transacciones.

El primer objetivo de esta sección es comprender qué atributos debe poseer una mercancía para poder ser utilizada eficientemente como dinero, como así también analizar cuáles son las funciones que ésta debe cumplir. El segundo objetivo es examinar su evolución a lo largo de la historia de la humanidad para llegar a una mejor comprensión del mismo y de sus distintas formas.

2.1. Dinero: Concepto, funciones y propiedades

La palabra dinero procede del vocablo latín *denarius*, derivado del adjetivo distributivo *deni*, que significa ‘cada vez’, y que deriva del decimal diez.¹

El “denario” era una pequeña moneda romana de plata muy popular en su época. Originariamente valía diez ases; de ahí su nombre, ya que *denarius* significa en latín “que contiene diez”; y en éste se reconoce la misma raíz que en *decem* “diez”.²

Es frecuente encontrar en la literatura económica que se considera que el dinero es aquello que realiza las funciones del dinero (*money is what money does*), esta definición traslada el problema del concepto del dinero a las funciones que éste cumple.

De esta manera, se definirá al dinero como “cualquier objeto al que por consenso general se le atribuye el papel de medio de cambio, en cuyos términos se expresa el valor de cambio de todas las mercancías” (Ortiz Soto, 2001, p. 25). En palabras de Lord Robbins (1935, p.56) “...el dinero es evidentemente un medio para una compra final... es claro que el dinero es en sí mismo tan solo un medio: un medio de cambio, un instrumento de cálculo”. Tres décadas más tarde, a la pregunta

¹ Ruiz Calleja, A.: *Blog Numismático*. Acceso web: www.blognumismatico.com

² Corominas, J. (1987). *Breve diccionario etimológico de la lengua española*. Ed. Gredos. Madrid

de ¿Qué es el dinero? Newlyn (1962) respondió expresando que “...*la función primordial, cuyo desempeño nos permite identificar al dinero, es muy simple, la de fungir como medio de cambio*” (p. 11).

En tal sentido, las formas precisas que adopta el dinero pueden cambiar de acuerdo a las sociedades o el momento histórico considerado, pero lo importante es que todas cumplen las mismas funciones. Entonces, para comprender el concepto de dinero debemos estudiar sus funciones, es decir, para qué se utiliza.

Si bien en la actualidad el uso del dinero se ha extendido, las principales funciones que ha tenido y tiene el dinero son las siguientes:³

- a) Medio de cambio.
- b) Unidad de cuenta.
- c) Depósito de valor.

a) **El dinero como medio de intercambio:** La primera y principal función del dinero es la de servir como un medio de cambio. El funcionamiento eficiente de una economía requiere de un medio que elimine los inconvenientes derivados del trueque directo o indirecto, cuyas condiciones imponen un serio obstáculo al intercambio de bienes y servicios y, por ende, al desarrollo. Es condición necesaria para que el dinero sea un eficaz medio de intercambio, que la sociedad lo acepte como medio generalizado de pago. Dicha aceptación o consenso general a favor del dinero depende de la estabilidad de su poder adquisitivo. Fluctuaciones imprevistas o de importante magnitud en el poder adquisitivo del dinero socavan su aceptación general. La utilización del dinero como medio de cambio incentiva la especialización y la división del trabajo y promueve la eficiencia económica, ya que elimina muchos de los costos involucrados en el intercambio de bienes y servicios, los costos de transacción.⁴

b) **El dinero como unidad de cuenta:** La segunda función que el dinero cumple en una sociedad económica es la de proveer una medida estándar de valor de cambio, o precio, a todos los bienes y servicios que se ofrecen en el mercado. Esto implica que todas las mercancías adoptan un precio expresado en unidades monetarias. El valor monetario es la unidad de medida más importante para un sistema económico. De esta función del dinero

³ Ortiz Soto, O. (2001). *El dinero. La teoría, la política y las instituciones*, p. 26. Facultad de Economía UNAM. México.

⁴ Jimenez, F. (2012). *Elementos de teoría y política macroeconómica para una economía abierta*. Fondo Editorial – Pontificia Universidad Católica del Perú. Perú.

se deriva lo que se conoce como poder de compra o poder adquisitivo de la moneda, que refleja la cantidad de bienes y servicios que pueden obtenerse, a través del tiempo, con una cantidad determinada de dinero y que puede variar debido a numerosos factores.

- c) **El dinero como medio para depositar valor:** La inversión en medios de producción resulta imprescindible para la supervivencia y expansión de una sociedad económica. Una economía debe ser capaz de generar un excedente que permita a algunos de sus agentes dedicarse a la producción de bienes de inversión, es decir, bienes para mejorar y ampliar la capacidad de producción de bienes de consumo. Para que lo anterior sea posible, la sociedad debe abstenerse de consumir la totalidad del ingreso generado en el proceso productivo, y de esta manera ahorrar los recursos no empleados en el consumo. Sin embargo, para que esta acumulación sea posible, la moneda debe conservar su poder adquisitivo con el transcurso del tiempo, ya que, si esta se deprecia, la sociedad pierde el incentivo al ahorro, que hace imposible la inversión y la consecuente expansión de la producción. De esta manera, el dinero, en su función de depósito o reserva de valor, es utilizado para almacenar poder adquisitivo o capacidad de compra a lo largo del tiempo.

Una vez conocidas las funciones del dinero, se pasa a exponer las características que debe reunir un bien para ser considerado como un buen medio de intercambio (Ortiz Soto, 2001, p. 27):

En primer lugar, para que un objeto se utilice como medio de pago, debe gozar de **identificabilidad**, es decir, tiene que ser fácilmente reconocible. En las economías que utilizaban sal o granos de chocolate como medio de pago la identificación del dinero no planteaba muchos problemas. En cambio, los metales son más difíciles de identificar ya que su peso y la composición de las aleaciones pueden modificarse con relativa facilidad. El papel moneda es otro ejemplo de la importancia de la identificabilidad del dinero. La razón de ser de las filigranas y de los papeles y de las tintas especiales que se utilizan en el diseño de los billetes es facilitar su identificación y dificultar las falsificaciones.

En segundo lugar, el dinero debe tener **valor intrínseco**, característica que se explica por la necesidad del consenso general que debe existir en una sociedad con respecto a las mercancías que son utilizadas como tales, principalmente en la fase de formación del sistema de pagos. Por valor intrínseco se entiende que dicha mercancía debe tener un valor de uso, además del valor de cambio que la sociedad le otorga, lo cual implica que debe ser una mercancía escasa y apreciada por la sociedad.

La **durabilidad** es otra característica muy importante, tanto por el natural desfase que produce el propio proceso de intercambio, al considerar el carácter indirecto de las transacciones, como por el dinero concebido como un medio para atesorar valor. En este sentido, los bienes perecederos, como los alimentos, no son un buen medio de intercambio por no ser durables, al estar sujetos a un proceso natural de descomposición que los hace perder sus propiedades físicas.

Asociado al uso del dinero como medio para atesorar, es también primordial que esté sujeto a **condiciones estables en su oferta**. Grandes fluctuaciones en la disponibilidad del medio de intercambio tenderán a depreciar o apreciar su valor en términos del resto de las mercancías. Fluctuaciones drásticas en su demanda también provocarán los efectos indicados, que necesariamente tienden a minar la eficiencia del sistema monetario, dado que el valor del dinero se vuelve prácticamente impredecible.

Otro atributo deseable de la mercancía vehículo es la **homogeneidad**, es decir, que cada unidad de la misma debe ser lo más parecida posible a la otra. El dinero concebido como unidad de cuenta y medio de intercambio pierde efectividad cuando las unidades monetarias son diferentes entre sí, al dar origen a problemas entre los sujetos que participan en una transacción, que deben ponerse de acuerdo en cuanto a las características de su dinero, lo cual constituye un gran retraso.

La **divisibilidad** es otra característica muy deseable en un medio de intercambio, dado que cuando una unidad monetaria tiene un valor muy alto, y no es divisible, es inoperable para la realización de transacciones más pequeñas. En sistemas monetarios primitivos era habitual encontrar algún medio de intercambio para realizar transacciones de escaso valor, y otros medios para transacciones de mayor monto, mecanismo que fue utilizado en los sistemas metálicos, en donde las aleaciones de metales baratos servían para transacciones pequeñas. Fernand Braudel en “*Las estructuras de lo cotidiano*” relata que los mercaderes chinos en la Baja Edad Media iban a las ferias con unas tijeras para cortar las láminas de plata y de oro, y con una balanza de precisión para pesarlas.⁵

La última propiedad deseable en un medio de cambio consiste en la **portabilidad**, que implica la facilidad de poder transportarse de un lado a otro. La importancia de este atributo reside en el hecho de que las transacciones se llevan a cabo en el mercado, localizado en lugares distintos a la

⁵ Braudel, F. (1984). *Las estructuras de lo cotidiano*. Ed. Alianza, Madrid.

residencia de los sujetos que intervienen en las transacciones (aunque esto en las sociedades actuales ha ido cambiando).

2.2. El dinero y su evolución a lo largo de la historia del hombre

Si se analiza la evolución del dinero a lo largo de la historia del hombre, es posible observar que éste ha ido progresando acorde con la sociedad. La naturaleza de los bienes utilizados como dinero ha ido cambiando. De esta manera, la evolución del dinero ha estado impulsada por diversos factores como la importancia relativa de los intercambios comerciales y el estado de la evolución de la economía.

Es importante remarcar que el dinero no tuvo un único origen, sino que se desarrolló de manera simultánea e independiente en muchas áreas del mundo, remotas entre sí, y en distintas épocas. Surgió, además, por razones que no sólo fueron económicas y comerciales, sino también políticas, religiosas y sociales.

2.2.1. El valor del intercambio: El trueque

¿Cuál es el motivo de que se introduzca el intercambio entre los hombres? Tal como lo expresa Rothbard (1979, p. 17), el intercambio es la base principal de nuestra vida económica. Sin intercambio no existiría economía verdadera y prácticamente tampoco habría sociedad. El intercambio voluntario se produce a causa de que ambas partes esperan beneficiarse, ya que cada una de éstas atribuye más valor a lo que recibe que a lo que entrega.

¿Por qué el intercambio es algo tan universal en la especie humana? Principalmente debido a la enorme diversidad que existe en la naturaleza: la variedad en el hombre, y la diversidad en la ubicación de los recursos naturales. Todo hombre posee un conjunto diferente de destrezas y aptitudes, y todo lote de terreno está dotado de características distintivas, que son únicas. De este hecho natural y eterno de la diversidad surgen los intercambios (Rothbard, 1979, p. 19).

De acuerdo a lo que exponen Morales y Galindo (2009, p. 7) el comercio se inició hace unos 2.500 años a.C., en la Mesopotamia, Persia, China, Egipto, India y algunos otros lugares. Sucedió cuando el ser humano, necesitado de adquirir mercancías que lo alimentaran, vistieran y le proporcionaran herramientas para trabajar la tierra, recurrió al intercambio de sus excedentes por otros recursos. A este proceso se le denominó “trueque”, un método de intercambio directo en el cual los bienes se intercambiaban por otros bienes.

Por supuesto, el intercambio directo de bienes y servicios alcanzaría apenas para mantener a una

economía por encima del nivel primitivo. Los tres problemas fundamentales a los que se enfrentaban los individuos que practicaban el trueque eran la falta de coincidencia en cuanto a las necesidades, la falta de coincidencia en cuanto a las cantidades y las indivisibilidades de los bienes sujetos a intercambio.⁶ Además, una consecuencia de este método de intercambio directo era la falta de estímulos a la especialización y la producción a gran escala.

2.2.2. El dinero mercancía⁷

Con el transcurso del tiempo, el hombre descubrió el camino que posibilitaba alcanzar una economía más desarrollada: el intercambio indirecto. Mediante el intercambio indirecto, un individuo vendía su producto, no a cambio de una mercancía que precisa directamente, sino a cambio de otro bien que, a su vez, es vendido a cambio del bien que uno requiere.

Ahora bien, así como en la naturaleza existe gran variedad de recursos, se presenta también mucha diversidad en la comerciabilidad de los bienes. Algunos son más fácilmente fraccionables, otros son más durables en períodos prolongados de tiempo, o más adecuados para su transporte hacia lugares alejados. Todas esas ventajas se traducen en lo que se llama mayor “comerciabilidad”. En toda sociedad, como es natural, son los bienes más comerciables los que se eligen para desempeñar el papel de medio de intercambio. A estos bienes utilizados para el intercambio de otros bienes se les ha denominado “dinero mercancía” (Weatherford, 1997, p. 43).

Históricamente se registró la utilización de numerosas mercancías como medio de intercambio. Por ejemplo, los Aztecas empleaban las semillas del cacao como dinero, para los pueblos de Filipinas, Japón y otras regiones del sudeste asiático, tradicionalmente el arroz en medidas estandarizadas ha servido como dinero (Weatherford, 1997, p. 44). En China y el norte de África se utilizaba la sal como dinero. Los pueblos pastores empleaban regularmente animales vivos como forma de pago, con los que se estimaba el valor de todo lo demás. Las tribus siberianas utilizaban el reno, los antiguos hititas estimaban el valor de algo en ovejas y los griegos de la época de Homero se valían de los bueyes. Los pueblos pastores calculaban y pagaban prácticamente todo, desde los esclavos y las esposas hasta las multas por adulterio y asesinato, en reses (Weatherford, 1997, p. 45).

⁶Abramovich, A. y Vazquez G. (2003). *La experiencia del trueque en Argentina: otro mercado es posible*. Universidad Nacional de General Sarmiento. Buenos Aires

⁷ Este apartado está basado en Weatherford (1997). *La historia del dinero: de la piedra arenisca al ciberespacio*, p. 37 a 75. Editorial Andrés Bello Chile

2.2.3. Oro y plata: dos metales especiales

Después del alimento, una de las mercancías más apreciadas y populares entre los seres humanos es el metal. De todos los materiales que pueden utilizarse para fabricar dinero, el metal tiene más aplicaciones prácticas que otros y conserva su valor por más tiempo. Además, como se lo puede reducir a piezas más o menos pequeñas, resulta un buen medio de cambio (Ortiz Soto, 2001).

De todos los metales, el oro ha sido el más valorado en todo el mundo. Este metal tiene relativamente pocos usos prácticos fuera del decorativo, sin embargo, el hombre se ha sentido siempre atraído por él. La gente de todo el mundo ha asociado al oro y la plata con la magia y la divinidad. En la mayoría de las culturas, los dioses valoraban las ofrendas en metales preciosos más que las flores, los alimentos, los animales o incluso los seres humanos (Weatherford, 1997, p. 51). Los pueblos advertían la semejanza de su colorido con el sol, una coincidencia a la que adjudicaban un significado profundo. Los antiguos egipcios creían que el oro era sagrado para Ra, el dios sol, y entregaban grandes cantidades de metal con los cadáveres de los faraones. Entre los Incas, el oro y la plata representaban el sudor del sol y la luna, y recubrían las paredes de sus templos con estos metales preciosos.⁸

2.2.4. La acuñación de las primeras monedas

La introducción de la moneda metálica constituyó un medio por el que las antiguas sociedades intentaron superar los problemas asociados al uso de bienes perecederos como dinero (Banco Central Europeo, 2011).

En Mesopotamia, China, Egipto y otros muchos lugares del mundo antiguo pueden hallarse elementos parecidos al dinero e instancias parecidas al mercado, pero, en rigor, en ninguno de ellos se utilizó verdaderamente la moneda hasta el surgimiento del reino de Lidia y el subsiguiente acuñamiento de las primeras monedas, ocurrido entre el 640 y el 620 a.C.⁹

Las primeras monedas que se confeccionaron fueron fichas ovaladas de electro, una aleación de oro y plata de color ámbar que se da naturalmente. Para garantizar su autenticidad, el rey hacía estampar en cada una de ellas su emblema, una cabeza de león. El divulgador científico e histórico Isaac Asimov escribió:

“El reino lidio emitió entonces monedas, es decir, piezas de oro, plata o una aleación de ambos metales, en las que estaban estampados su peso y valor, y que llevaban un retrato del rey o algún

⁸ Bodega Barahona, F. (1991). *Notas sobre la antigua historia del oro*. Cuaderno Lab. Xeológico de Laxe. Coruña

⁹ Carbonell, S. (2016). *La moneda en el mundo antiguo: Grecia, Roma e Hispania*. Ies Cotes Baixes Alcoi. España

otro dibujo que indicara su carácter oficial y garantizara su pureza”¹⁰

La aparición de la moneda fue una gran bendición para la raza humana. Careciendo de moneda no podía haber verdadera especialización, no podía avanzar la economía más allá de un simple nivel primitivo. Con la moneda, todos los problemas de la indivisibilidad y de la coincidencia de necesidades, que afligían a la sociedad de trueque, desaparecieron por completo (Rothbard, 1979). Muchos pueblos circundantes adoptaron la práctica lidia de acuñar monedas y el mundo mediterráneo asistió a una revolución comercial que se extendió por todo su ámbito, y particularmente hacia el vecino inmediato de Lidia: Grecia (Weatherford, 1997, p. 61).

Atenas (575 a.C.) y Corinto (570 a.C.) fueron las primeras ciudades-estado griegas en acuñar sus propias monedas. Las monedas griegas eran utilizadas en un entorno muy vasto, que fue ampliado por Alejandro Magno. Por su parte, los romanos adoptaron la innovación griega consistente en el uso de monedas oficiales y fueron los primeros en introducir el sistema bimetálico utilizando el *denarius* de plata y el *aureus* de oro.¹¹

Los griegos y los romanos habían propagado la costumbre del uso de las monedas, así como los conocimientos técnicos necesarios para su acuñación en una amplia zona geográfica. Durante casi toda la Edad Media, las monedas de oro y plata acuñadas localmente constituyeron el principal medio de pago, si bien el empleo de las monedas de cobre fue en aumento.

2.2.5. Sobre el origen del papel moneda

En la historia de la moneda como medio de intercambio, el uso del papel como soporte físico del dinero es relativamente reciente, ya que no se tiene constancia del mismo hasta el siglo IX de nuestra era, en la China de la Dinastía Tang.¹²

En China, entre los años 618 y 907 d.C., durante la dinastía Tang, aparecieron los primeros bancos en los que la gente depositaba sus monedas y a cambio se le extendía un certificado por el importe depositado que servía como medio de pago. Al principio fue emitido por particulares que así evitaban el transporte de las pesadas monedas en operaciones de comerciantes y mayoristas. Funcionaban como pagarés en los que se escribía la cantidad que se le debía a la persona, quedando el dinero en efectivo a cargo de una persona de confianza. Este tipo de dinero recibió en nombre de “papel moneda convertible”. El primer billete se creó en China en el siglo VII, con la

¹⁰ Asimov, I. (1989). *Historia y cronología del mundo*. Editorial Ariel. España

¹¹ Banco Central Europeo. (2011). “*La estabilidad de precios, por qué es importante para ti*”. Boletín Mensual, Enero.

¹² Cobo Huici, R. “*Primeros billetes impresos en China*”, en Blog numismático digital, 22 de Octubre de 2014. Recuperado de: <http://www.numismaticodigital.com/noticia/2407/articulos-notafilia/primeros-billetes-impresos-en-china.html>

finalidad de reducir la circulación de metales (monedas) por la escasez de cobre, pero lo que en principio se ideó como una medida temporal resultó, al acumular mucho más dinero en menos espacio, ser la gran solución en el transporte de grandes cantidades a lo largo y ancho del Gran Imperio. Los ejemplares de billetes más antiguos conocidos son los “kuan” chinos realizados con corteza de morera en el siglo XIV.¹³

En el siglo XIII, un ciudadano veneciano conocido como Marco Polo, emprendió una expedición a China. Las anotaciones que hizo durante este viaje contienen las primeras referencias que existen en Occidente acerca de la producción y uso del papel moneda, forma de pago incomprensible para las condiciones imperantes en Europa por entonces. Previamente se había generalizado la custodia del oro y las joyas de las familias adineradas por parte de los orfebres, quienes entregaban resguardos con su firma y sello a los depositantes. Al igual que los pagarés, tales resguardos acabarían siendo aceptados como medios de pago en las transacciones. El uso de ambos documentos hacía más rápidos y seguros los intercambios, al evitar tener que cargar con pesadas piezas de oro o plata en los largos y peligrosos viajes de la época.¹⁴

En Europa, aunque como se mencionó, Marco Polo ya había llevado noticias del novedoso sistema monetario chino, no fue hasta el siglo XVII cuando se crearon los primeros billetes. Los primeros billetes de los que hay constancia aparecieron en Suecia en el año 1661 (siglo XVII) de la mano del cambista Johan Palmstruch, quien los entregaba como "recibo" para quien depositaba oro u otro metal precioso en el Banco de Estocolmo, que había fundado él mismo.

En este sentido, durante varios siglos el billete no era más que un sustituto de la moneda metálica, un objeto que representaba su valor y que no tenía un valor en sí mismo, ya que debía estar respaldado por moneda metálica depositada en un banco, cuya circulación era legal, pero su aceptación voluntaria.¹⁵

2.2.6. El patrón oro y el paso al dinero fiduciario

Un hecho trascendental para la historia del dinero se puede situar en Inglaterra cuando un extranjero holandés ocupó el trono en 1689. El destituido Carlos II había entrado en bancarrota debido a sus deudas y este nuevo rey, *William of Orange* fue quien lo reemplazó. Es en este momento cuando a un grupo de burgueses y en especial a un comerciante escocés el rey propuso

¹³ Mendoza Martínez, D. (2009). *El nacimiento del billete: una revolución en el concepto del dinero*. OMNI N°1. Agosto 2009.

¹⁴ Huidobro Moya, J. (2015). *Numismática y heráldica en España*. Ed. Liber Factory. España.

¹⁵ Chacón Hidalgo, M. (2006). *Del real al colón: Historia de la moneda en Costa Rica*. BPR Publishers.

la idea de la creación de una nueva institución llamada *Bank of England*. Este Banco Central se comprometía a la financiación de los asuntos reales siempre y cuando se le proporcionara el derecho único de emisión de moneda papel.¹⁶ Este concepto novedoso rápidamente se difundió por otras naciones que reconocieron un gran potencial en su instauración. En un principio se mantuvo la representación del dinero en un estándar bimetálico de plata y oro. Pero con el paso del tiempo se vio que este doble soporte del dinero papel llevaba a problemas monetarios entre ambas “monedas”. Así es como en 1880 se instituyó el patrón oro, que significaba que todas las unidades monetarias estarían unidas a un cierto peso de oro. El valor de la moneda, por lo tanto, pasaba a depender de las reservas de oro del país.

Tras el comienzo de la Primera Guerra Mundial, muchos países comenzaron a imprimir cada vez más billetes con el objeto de financiar los costos de la guerra. A consecuencia del incremento del dinero en circulación, la mayoría de los países suspendieron la convertibilidad en oro de sus monedas, puesto que esta mayor cantidad de dinero ya no se correspondía con las reservas de oro nacionales. De esta manera, el patrón oro estuvo vigente un corto período, hasta el año 1913.

En un intento por mantener la moneda unida a una reserva física de oro se convocó a numerosas potencias aliadas a una convención en Bretton Woods (New Hampshire), en el año 1944. En ella se acordó un patrón oro revisado: los tipos de cambio de las monedas nacionales de las principales potencias económicas quedaron vinculados al dólar y el dólar podía convertirse en oro al precio fijo de 35 dólares por onza. El sistema monetario de Bretton Woods suele denominarse “patrón divisas oro”. Los bancos centrales daban dólares a cambio de sus respectivas monedas nacionales y viceversa.

No obstante lo anterior, el patrón divisas oro fue desplazado por una decisión política el 15 de Agosto de 1971, cuando el presidente Richard Nixon anunció la suspensión de la convertibilidad del oro y el dólar, lo que produjo serias fluctuaciones en los mercados. Esto acabó por romper el vínculo con las reservas de oro y todas las monedas pasaron a carecer de ningún tipo de respaldo salvo la confianza en el gobierno. Esto es lo que se conoce como “moneda fiduciaria” o moneda *fiat*, las monedas y billetes fiduciarios no basan su valor en la existencia de una contrapartida en oro, plata o cualquier otro metal, ni en su valor intrínseco, sino simplemente en su declaración como dinero por el Estado y también por la confianza (la fe en su aceptación) que inspira. Sin esta declaración, la moneda, simples papeles o metales circulares, no tendría ningún valor.

Este nuevo escenario permitió a los operadores políticos que dominan la banca central pasar del

¹⁶ Boudeguer, R. (2015). *El primer Banco Central de la historia y su máquina de imprimir dinero*. Informe mensual de estrategia (Noviembre), Banca March.

dinero-mercancía (con valor intrínseco como el oro) al dinero fiduciario (con el respaldo extrínseco de la legalidad).¹⁷ Esto fue fácil por la habituación que existía a los billetes (que eran títulos al portador respaldados por el oro del banco emisor), lo que permitió que la población siguiera valorando algo que ya carecía de dicho valor, tal como lo expresa Mankiw (2007, p.150): *“Si nadie se molesta en canjear los billetes por oro, a nadie le importa que se abandone esta opción. En la medida en que todo el mundo continúe aceptando los billetes de papel en los intercambios, éstos tendrán valor y servirán de dinero. El sistema de dinero mercancía se convierte, pues, en dinero fiduciario. Obsérvese que al final la utilización de dinero para realizar intercambios es en gran medida una convención social, en el sentido que todo el mundo valora el dinero fiduciario simplemente porque espera que los demás lo valoren. La moneda pasó de ser un instrumento de trueque a un sistema de representación con valor intrínseco de un metal precioso, luego a representarse en un billete relacionado con el metal precioso y, finalmente, a un billete fiduciario impreso por la banca central”*.

De esta manera, a partir de 1971 las monedas nacionales de las principales potencias económicas han sido dinero fiduciario en sentido estricto.

2.3. Avances recientes en la evolución del dinero: dinero electrónico, monedas virtuales y criptomonedas.

La evolución del dinero no se ha detenido. En las últimas décadas han surgido diversas formas de dinero intangible, entre las que cabe mencionar el dinero electrónico (*e-money*), las monedas virtuales y, entre ellas, las criptomonedas. Estas nuevas modalidades de dinero pueden utilizarse para pagar por bienes y servicios a través de la red.

Antes de entrar en el mundo de las criptomonedas, resulta necesario hacer una distinción entre los conceptos de “dinero electrónico”, “moneda virtual” y “criptomonedas”.

De acuerdo a la definición propuesta por el Banco Central Europeo (2012), una **moneda virtual** es “un tipo de dinero digital no regulado, emitido y generalmente controlado por sus desarrolladores, y utilizado y aceptado entre los miembros de una comunidad virtual específica”. Esto significa que una moneda virtual se refiere a una representación digital de valor denominada en su propia unidad de cuenta y susceptible de ser obtenida, guardada y transferida electrónicamente.

¹⁷ Montoya Vasquez, M. (2016). *Inversión en Bitcoins: modelo para Costa Rica*. Tecnológico de Costa Rica. Costa Rica.

Las monedas virtuales se diferencian de lo que se denomina **dinero electrónico** (*e-money*), el cual es una representación digital de la moneda de curso legal de una jurisdicción, es decir, del dinero fiduciario. En consecuencia, las monedas virtuales no tienen el estatus de ser de curso legal, no hay un emisor que esté obligado a canjearlas (por ejemplo, a moneda fiduciaria), y no son emitidas por ningún gobierno soberano. El dinero electrónico, en cambio, sí cumple con todas estas características.

Figura 2.1. Diferentes modalidades de dinero.

Fuente: Banco Central Europeo (2012).

<i>Estatus legal</i>	<i>Formato</i>	
	<i>Físico</i>	<i>Digital</i>
<i>Sin regular</i>	Ciertos tipos de monedas locales	Monedas virtuales
<i>Regulado</i>	Billetes y monedas (de curso legal)	Dinero electrónico (e-money)
		Dinero bancario (depósitos)

El dinero electrónico es definido por el Comité de Pagos y Liquidación de Valores de Basilea (CPSS) como un “valor monetario derivado de una obligación de parte de un emisor y que se encuentra almacenado en un medio electrónico (tarjetas, computadoras o teléfonos celulares) y que puede ser empleado para fines de pago, transferirse entre usuarios y convertirse de nuevo en efectivo”. En los sistemas de dinero electrónico, el vínculo entre el dinero electrónico y la moneda fiduciaria con la que se lo respalda permanece intacto, ya que los fondos se expresan en unidades de esa moneda (Dólares de los Estados Unidos, Euros, Pesos argentinos, etc.). Para mitigar riesgos sistémicos y de protección del consumidor, el efectivo que respalda el dinero electrónico habitualmente se deposita en instituciones financieras que cumplen con todas las regulaciones.

Esquemas de monedas virtuales

Existe una gran variedad de esquemas de monedas virtuales. Una forma de clasificarlos es en base a sus interacciones con el dinero real y la economía real. Esto ocurre a través de dos canales: a) el flujo monetario a través de los intercambios de divisas; y b) el flujo real en el sentido de la posibilidad de comprar bienes y servicios reales. Tomando esto como base, se pueden distinguir tres tipos:¹⁸

- 1) Esquemas cerrados o monedas virtuales no convertibles. Estos esquemas casi no tienen vínculos con la economía real y a veces se los llama esquemas de "sólo en el juego". Los

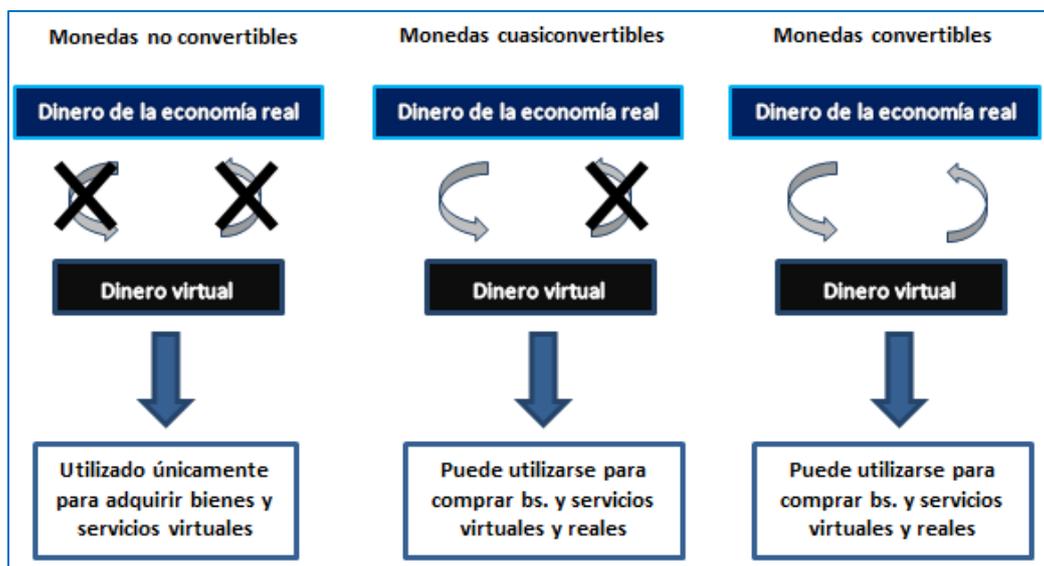
¹⁸ European Central Bank. (2012). *Virtual Currency Schemes*. Eurosystem. Germany.

usuarios generalmente pagan una tarifa de suscripción y luego ganan dinero virtual en función de su desempeño en línea. La moneda virtual solo se puede gastar comprando bienes y servicios virtuales ofrecidos dentro de la comunidad virtual y no se puede comerciar fuera de la comunidad virtual.

- 2) Esquemas con flujo unidireccional o monedas cuasiconvertibles. La moneda virtual se puede comprar directamente usando la moneda real a un tipo de cambio específico, pero no se puede cambiar a la moneda original. Las condiciones de conversión son establecidas por el propietario del esquema. Este tipo de esquema permite que la moneda se use para comprar bienes y servicios virtuales y reales.
- 3) Esquemas con flujo bidireccional o monedas virtuales convertibles. Los usuarios pueden comprar y vender dinero virtual de acuerdo a las tasas de cambio con su moneda. La moneda virtual es similar a cualquier otra moneda convertible con respecto a su interoperabilidad con el mundo real. Estos esquemas permiten la compra de bienes y servicios virtuales y reales.

Figura 2.2. Esquemas de monedas virtuales.

Fuente: Banco Central Europeo (2012).



Todas las monedas virtuales no convertibles (primer esquema) son centralizadas: por definición, son emitidas por una autoridad central que establece normas que las hacen no convertibles. Por el contrario, las monedas virtuales convertibles (tercer esquema) pueden ser cualquiera de los dos subtipos: centralizadas o descentralizadas (o entre pares: *peer-to-peer*).

- 1) En el caso de las **monedas virtuales centralizadas** existe una autoridad administrativa única, es decir, una tercera parte que controla el sistema. El administrador emite la moneda,

establece las normas para su utilización, mantiene un libro de contabilidad central de pago, y tiene autoridad para canjear la moneda (y retirarla de circulación).

La tasa de cambio de una moneda virtual convertible puede ser variable, es decir, determinada por la oferta y la demanda de la moneda virtual, o fija, es decir, fijada por el administrador según un valor establecido medido en dinero real.

2) Las **monedas virtuales descentralizadas** (también conocidas como criptomonedas) por su parte, no tienen una autoridad central que las administre y el mantenimiento del registro de saldos y operaciones en muchos de estos esquemas se hace de manera abierta y distribuida entre los participantes del sistema. Ejemplos de este tipo de monedas son Bitcoin, LiteCoin y Ripple.

Este tipo de monedas solo existen en la web y su valor está sostenido porque hay un comprador y un vendedor que la admiten para una transacción determinada, en cualquier parte del mundo. Para operar utilizan cifrados de alta seguridad, sin embargo, su uso no está exento de riesgos, ya que su valor no está sostenido por ninguna autoridad monetaria y puede sufrir profundas pérdidas de valor, como ya ocurrió hace unos años, cuando China prohibió su uso en el comercio online del país. A continuación se realiza un análisis de mayor profundidad acerca de este tipo particular de monedas virtuales.

El último avance en la evolución del dinero: Las Criptomonedas

Una criptomoneda (CM) se define como una moneda virtual convertible descentralizada, fundamentada matemáticamente y protegida por criptografía.¹⁹

Las criptomonedas se basan en llaves públicas y privadas para transferir el valor de un usuario a otro, dicha transacción debe ser criptográficamente firmada cada vez que se realiza. La seguridad y la integridad de los libros de contabilidad de la criptomoneda están garantizadas por una red de partes mutuamente desconfiadas (en Bitcoin se conocen como mineros) que protegen la red a cambio de la obtención de una remuneración (en Bitcoin, un pequeño número de nuevas unidades de Bitcoins llamado “recompensa de bloque” y en algunos casos, también las tasas transaccionales que pagan los usuarios como incentivo para que los mineros incluyan sus transacciones en el próximo bloque).

¹⁹ La *criptografía* es la rama de las matemáticas que permite crear pruebas matemáticas que proporcionan altos niveles de seguridad a documentos y datos. Implica la creación de códigos que permiten que la información se mantenga en secreto, convirtiendo los datos en un formato que es ilegible para un usuario no autorizado.

Es probable que la criptomoneda más conocida mundialmente sea Bitcoin, sin embargo, desde su lanzamiento en el año 2009, han surgido una enorme cantidad de monedas “derivadas” (“forks”)²⁰, que actualmente rondan las mil cuatrocientas. Entre ellas se destacan: Ethereum, Ripple, Bitcoin Cash, Litecoin, IOTA, Dash, Bitcoin Gold, Dogecoin, entre muchísimas otras.

El valor de las criptomonedas proviene de su posibilidad de ser aceptadas en el intercambio por bienes y servicios, otras monedas de curso legal o activos financieros, y de la estabilidad de su valor en el tiempo. En otras palabras, su valor depende de la confianza que los participantes tengan sobre la calidad presente y futura de sus atributos para ser ampliamente aceptadas como medio de pago, reserva de valor y unidad de cuenta frente a otras alternativas similares.

Para generar esta confianza, las CM deben garantizar la solución a tres de sus principales problemas: que su emisión esté de alguna forma controlada, que no puedan ser falsificadas y utilizadas por el mismo tenedor más de una vez (el problema del doble gasto). Finalmente, deben asegurar que su autenticidad sea fácilmente verificable al momento de hacer una transacción.

Estos problemas se resuelven mediante protocolos de criptografía de alta seguridad y protocolos descentralizados para la validación de saldos y transacciones. En particular, estos sistemas generan para cada usuario una llave pública y una llave privada para que, combinándolas, el usuario firme digitalmente sus transacciones.²¹

Los esquemas de CM utilizan la tecnología denominada de registro descentralizado encriptado o *Blockchain*, para llevar la historia transaccional completa del activo digital entre cuentas de distintos participantes sin la necesidad de que sea intermediada por un administrador centralizado. Estos esquemas se basan en la creación de una única cadena de registros públicos (cadena de bloques) disponible en línea y validable por cualquier participante del sistema. Cada vez que se genera un nuevo bloque de transacciones aquellos participantes con suficiente capacidad de procesamiento comienzan a competir por la solución de algoritmos de validación computacionalmente complejos para verificar la autenticidad de este código único a cambio de algún incentivo generado por el sistema (como por ejemplo nuevas unidades de la criptomoneda o tarifas transaccionales). Este protocolo de validación descentralizada de las transacciones es conocido como *proof-of-work*, y es el que soluciona los problemas de falsificación y robo de las criptomonedas.

²⁰ En el lenguaje de programación, un *fork* es un proyecto de software que parte de una copia de otro proyecto para desarrollarse de manera independiente del original.

La mayoría de las CM basadas en *proof-of-work* limitan la oferta de la CM en el sistema, haciendo cada vez más onerosa la minería computacional de una unidad adicional (costos marginales crecientes) y reduciendo las unidades minadas por bloque como premio para los mineros ganadores (incentivos decrecientes).

Participantes en los sistemas de Criptomonedas

Los esquemas de criptomonedas operan sobre una red de dispositivos electrónicos (computadoras y celulares, principalmente) conectados entre sí a través de internet. En el caso de las CM basadas en *proof-of-work*, los mineros, dedicados a la validación de las transacciones y del registro público del sistema, son parte central de estos esquemas.²¹

Cualquier individuo con un dispositivo conectado a internet puede abrir una billetera electrónica para operar como usuario de criptomonedas. Estos usuarios pueden adquirir las mismas para hacer pagos por bienes o servicios, pagar deudas o transferir fondos a otros integrantes de la comunidad, y mantenerlas como inversión.

Por otra parte, es habitual encontrar en los esquemas de CM operadores de plataformas de almacenamiento e intercambio de CM o *Exchanges*. Aunque algunos de los *exchanges* de criptomonedas solo ofrecen los servicios de cambio entre CM y otros activos (como divisas) a cambio de una comisión, la mayoría ofrece también los servicios de provisión de billeteras o cuentas virtuales para el almacenamiento y transferencia de CM.

²¹ Arango-Arango, C y Bernal Ramírez, J. (2017). *Criptomonedas*. Documentos técnicos de trabajo. Banco de la República de Colombia. Colombia.

CAPÍTULO 3: ANTECEDENTES Y NACIMIENTO DE BITCOIN

3.1. Los cimientos de Bitcoin: La Comunidad Cypherpunk

La idea de crear una moneda virtual no nació con Bitcoin, sino que se puede identificar al movimiento Cypherpunk, formado a finales de los años ochenta en Estados Unidos, como su precursor. Sus integrantes (programadores, ingenieros, apasionados por la tecnología y pensadores libertarios) buscaban aplicar los principios de la criptografía²² para proteger la privacidad de los individuos frente al poder de los Estados. Los integrantes más destacados de este movimiento son:

- **Eric Hughes:** matemático de la Universidad de California y autor de *“A Cypherpunk’s Manifesto”* (1993). En este texto afirmaba: *“La privacidad no es el secretismo. Un asunto privado es algo que uno no quiere que todo el mundo se entere, un asunto secreto es algo que uno no quiere que nadie se entere. La privacidad es el poder de revelarse selectivamente ante el mundo. Por lo tanto, la privacidad en una sociedad abierta requiere sistemas de transacciones anónimas.”*²³
- **Tim May:** ingeniero y científico de Intel. Fue autor de *“A Crypto Anarchist Manifesto”* (1992) en el que pronosticaba: *“Así como la tecnología de la imprenta cambió y redujo el poder de los gremios medievales y la estructura de poder en la sociedad, los métodos criptográficos alterarán fundamentalmente la naturaleza de las corporaciones y de la interferencia del gobierno en las transacciones económicas”*.²⁴
- **John Gilmore:** fundador de *Electronic Frontier Foundation*. Abogaba por una “verdadera privacidad financiera” y creía que sólo la física y la matemática serían capaces de garantizar una “verdadera privacidad en las comunicaciones personales”.²⁵

A fines de 1992, se creó *alt.cypherpunks*, una lista de emails encriptados en la que se realizaban intercambios de opiniones sobre diversas cuestiones relacionadas a la tecnología, la criptografía, la privacidad, las comunicaciones y las intersecciones entre todas estas áreas. Entre los suscriptores más conocidos se encuentran Julian Assange, fundador de Wikileaks; Bram Cohen, creador de BitTorrent; Adam Back, creador del sistema *proof-of-work* y Hal Finney, destinatario de la

²² En el caso de *Bitcoin*, la criptografía se utiliza para impedir que alguien pueda gastar los fondos del monedero de otro usuario o que se pueda corromper la cadena de bloques. También se utiliza para encriptar un monedero, de manera que no se pueda utilizar sin una contraseña.

²³ Hughes, E. (1993). *“A Cypherpunk’s Manifesto”*. Recuperado de: <http://www.activism.net/cypherpunk/manifesto.html>

²⁴ May, T. (1992). *“A Crypto Anarchist Manifesto”*. Recuperado de: <http://www.activism.net/cypherpunk/crypto-anarchy.html>

²⁵ Gilmore, J. (1991). *“Privacy, Technology, and the open society”*. Recuperado de: <http://www.toad.com/gnu/cfp.talk.txt>

primera operación de Bitcoin.

Una idea que despertaba un gran interés en el grupo era la posibilidad de inventar una moneda virtual que no dependiera de ningún gobierno para funcionar. Había un antecedente atractivo. A principios de 1980, el doctor en sistemas David Chaum había exhibido trabajos que sentaban las bases de una moneda digital y en 1989 había fundado DigiCash, una empresa de dinero electrónico basada en protocolos criptográficos (la cual quebró en 1998).²⁶

Entre los *cypherpunks*, los debates e investigaciones cobraron cada vez más energía. De ese clima intelectual surgieron muchas propuestas y experiencias, tales como E-gold, Bitgold y B-money (Wei Dai). Ninguna logró establecerse definitivamente, y algunas sólo fueron propuestas teóricas, pero las lecciones aprendidas a raíz de sus fracasos fueron clave como cimiento para el desarrollo de Bitcoin.

3.2. El nacimiento de Bitcoin

“Bitcoin is one of many attempts dating back to the 1980s to develop a decentralized payment network” (BBVA, 2013, pág. 1). Siguiendo las ideas del BBVA, la moneda virtual Bitcoin se creó como medio de pago en uno de los tantos intentos desde la década de 1980 para desarrollar un intercambio descentralizado, libre de cualquier autoridad estatal o compañía privada.

Cuando se produjo la crisis financiera del 2008, los Bancos Centrales de los principales países del mundo adoptaron una política monetaria fuertemente expansiva, de manera tal de inyectar liquidez en el sistema financiero. La recesión que se produjo a nivel mundial provocó que la solidez de las monedas tradicionales respaldadas por los gobiernos comience a ser cuestionada. Este escenario dio pie al surgimiento de una nueva moneda electrónica, independiente de cualquier Banco Central y de cualquier tipo de regulación estatal.

Poco después de la crisis financiera del año 2008, un grupo de personas (o una sola), utilizando el pseudónimo de *“Satoshi Nakamoto”* creó un protocolo para el intercambio de bienes y servicios denominado *“Bitcoin”*. Esta criptomoneda fue presentada primeramente en un foro de internet. El contenido del foro era científico, conformado por una comunidad académica principalmente relacionada a la matemática y a la informática, *metzdowd.com*, el lugar perfecto para introducir este tipo de moneda revolucionaria.

El 31 de Octubre de 2008 fue el día seleccionado por Nakamoto para publicar el documento titulado *“Bitcoin: A Peer-to-Peer Electronic Cash System”*, cuya traducción es *“Bitcoin: un*

²⁶ Mantilla, S. (2014). *Bitcoin: la otra cara de la moneda*. Instituto de Estrategia Internacional. CERA. Argentina

sistema de efectivo electrónico usuario-a-usuario". El contenido del mensaje era el siguiente: "*He estado trabajando en un nuevo medio de pago electrónico que es completamente peer to peer, sin necesidad de contar con una tercera parte como intermediario*"²⁷. El ensayo está disponible en: <http://www.bitcoin.org/bitcoin.pdf>.

Este documento de estilo académico describe todos los detalles de la nueva forma de moneda que Nakamoto había creado, el Bitcoin. No es un documento de fácil comprensión, ya que implica numerosas cuestiones técnicas de informática. Además de estas cuestiones técnicas, Nakamoto también expone su preocupación sobre la manera en que el desarrollo tecnológico había superado ampliamente al desarrollo financiero. Esta preocupación radica en la figura de los bancos como organizaciones que ya no facilitan las transacciones en el mercado, sino que se han transformado en un intermediario que las ralentizaba.

Después de la publicación del documento, se supo que el trabajo de Nakamoto había comenzado un año atrás, en el inicio de la explosión de la crisis financiera. En esta época ya se podían observar los primeros indicios de una parálisis del sistema financiero a nivel mundial. Las calificadoras de riesgo habían comenzado a advertir sobre el riesgo presente en un gran número de hipotecas y se empezaron a producir los primeros rescates de bancos y una colección de sucesos que llevaron a la población a un despertar amargo sobre la realidad financiera. En medio de este caos es cuando Nakamoto se propuso crear esta nueva moneda basada en un sistema despojado de la necesidad de la confianza y de terceros agentes.

Esta red diseñada por Nakamoto estaría regulada últimamente por los usuarios que participan en la misma. No contaría con un ente centralizado y regulador, como el Banco Central de cada país, por lo tanto, no podría ser manipulada por medio de medidas de política económica. Es posible relacionar este razonamiento con una forma de capitalismo liberal en la que el sistema no depende de un órgano regulador sino del interés personal de los usuarios. En uno de los intercambios de opiniones en los foros, Nakamoto expresaba el 14 de Noviembre de 2008: "*...Bitcoin es muy atractivo desde el punto de vista liberal si se puede explicar bien; sin embargo soy mejor con el código que con las palabras...*".

Después de unos meses, Nakamoto cumplió su promesa de poner en circulación una versión en funcionamiento. De esta forma, el 8 de Enero de 2009 se publicó en *metzdowd.com* una entrada titulada "*Bitcoin v0.1 released*". El mensaje que lo acompañaba era el siguiente: "*Anuncio el primer lanzamiento del Bitcoin, una moneda digital que utiliza un sistema completamente peer-to-*

²⁷ Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Recuperado de www.bitcoin.org

peer.... Es un sistema completamente descentralizado sin ningún organismo o autoridad central...". Este programa se encontraba aún en fase experimental y permitía modificaciones de usuarios según fueran necesarias. Además de cuestiones de informática, este primer lanzamiento se encontró con una cuestión decisiva para el despegue del Bitcoin. Uno de los integrantes de la comunidad mencionaba: "El verdadero problema será conseguir individuos para que realmente Bitcoin consiga valor y pueda convertirse en moneda". A este comentario, Nakamoto respondió: "Puede que simplemente tenga sentido conseguir unos cuantos Bitcoins en caso de que el concepto triunfe. Si suficiente gente piensa que esto es posible, por sí mismo se convertirá en un triunfo."

La siguiente aparición del Bitcoin fue el 11 de Febrero de 2009 cuando alguien, bajo el nombre de Satoshi Nakamoto, se registró en la página *P2Pfoundation.net*, una comunidad dedicada concretamente a proyectos *peer to peer*. El mismo día de registrarse publicó un link a una nueva versión del programa de Bitcoin. Este nuevo programa ya contaba con los primeros Bitcoins, minados por el propio Satoshi (el cual obtuvo una recompensa de 50 BTCs) y generados en el denominado "Bloque génesis", el primero de los bloques destinado a dar comienzo a la cadena de bloques. En este nuevo lanzamiento del Bitcoin el discurso técnico del primer foro es sustituido por un discurso más retórico centrado en la filosofía detrás de la moneda. Principalmente, se ataca a la "moneda fiat"²⁸ y al sistema de reserva fraccionaria para atraer a todos aquellos descontentos con la situación propiciada en la crisis financiera.

En palabras de Nakamoto en su comunicado sobre el estreno de la moneda, se pretende dar un empujón a las monedas virtuales por lo siguiente:

"La raíz del problema actual de las monedas convencionales y del sistema en general es toda la confianza que hay que depositar en ellas para que funcionen. Debemos confiar en el Banco Central en que no devaluará la moneda y en que ejercerá las políticas adecuadas en cada momento en beneficio de la sociedad. Pero la historia del dinero fiat está llena de antecedentes que minan de dicha confianza. Debemos confiar en depositar nuestro dinero en los bancos y de enviarlo electrónicamente, pero lo prestan en olas de burbuja de crédito con apenas fracciones de reservas. Tenemos que confiar en ellos nuestra privacidad para que los ladrones de identidades saqueen nuestras cuentas. Sus excesivos costos de personal hacen los micropagos imposibles. Por lo que, en definitiva, existen severos problemas inherentes al modelo." (Nakamoto, 2008).

²⁸ **Dinero fiat:** Se llama de esta manera al dinero fiduciario, que es el que se basa en la fe o la confianza de la comunidad, es decir, que no está respaldado por metales preciosos sino en una promesa de pago por parte de la entidad emisora. Es el papel moneda cuyo elemento esencial es su uso obligatorio en una jurisdicción por imposición de una ley que lo hace de curso forzoso, Como se analizó en el capítulo anterior, la utilización del dinero fiat comenzó a partir de 1971.

“Hace una generación, los sistemas de computación para usuarios múltiples tenían el mismo problema. Antes de la etapa en la que la encriptación se hizo fuerte, los usuarios tenían que proteger sus registros con claves, confiando en los administradores de los sistemas para mantener su información resguardada. Pero la privacidad se podía eliminar en cualquier momento por los administradores, basándose en su propio criterio o en el de sus superiores. Después llegó con firmeza la encriptación y ya no había que basarse en la confianza. Los datos podían ser asegurados de una forma que era imposible que fueran accesibles por otros. Es tiempo de que tengamos lo mismo para el dinero. Con la moneda digital basada en pruebas criptográficas, sin la necesidad de tener que confiar en un intermediario, el dinero puede estar seguro y se pueden hacer transacciones sin esfuerzo”. (Nakamoto, 2008).

“Lo que se necesita es una forma de pago electrónica basada en pruebas criptográficas y no en confianza, permitiendo de esta manera a las dos partes dispuestas, realizar transacciones directamente sin necesidad de un intermediario.” (Nakamoto, 2008).

Ante estos problemas presentados, Nakamoto situaba al Bitcoin como la posible solución. Este supondría la eliminación de los intermediarios, la no necesidad de la confianza en entidades reguladoras como los Bancos Centrales y la garantía de privacidad e independencia de los usuarios. En estos primeros meses el éxito de la segunda versión de *Bitcoin* fue limitado, llegando solamente a unas pocas decenas de descargas semanales. Sin embargo, una gran cantidad de expertos en distintas áreas acudieron a Nakamoto con la intención de colaborar en el proyecto con sus conocimientos.²⁹

Un poco más tarde de su puesta en marcha, el 11 de Julio de 2010 constituye otra fecha importante en el calendario de la moneda y es cuando se hace la primera compra utilizando Bitcoins, un usuario con el alias “*Laszlo*” compró una pizza, pagando por ella 10.000 Bitcoins en Estados Unidos, iniciando así una espiral de confianza depositada en el protocolo del Bitcoin (González Otero, 2013).

A pesar de sus problemas, Bitcoin continuó su camino de crecimiento exponencial llegando a la paridad con el dólar en Febrero de 2011. La comunidad financiera empezó a verlo como una inversión con el potencial de grandes rentabilidades en el corto y mediano plazo. Un hecho que favoreció la imagen del Bitcoin como alternativa viable fue la utilización de esta moneda para la

²⁹ Gutiérrez Hernández, P. (2015). *Bitcoin: ¿Presente y futuro del dinero?* Universidad Pontificia Comillas. Madrid, España.

financiación de WikiLeaks. Cuando se produjo el escándalo de Wikileaks, todas las grandes empresas de pago electrónico como PayPal, MasterCard o Visa negaron las donaciones realizadas hacia la organización. En este momento, el Bitcoin surgió como una alternativa confiable de transferencia de fondos, esto demostró a la comunidad que el sistema Bitcoin funcionaba correctamente.

Fueron muchos los intentos por averiguar más datos sobre el misterioso *Satoshi Nakamoto* del que aún no se conocía ningún tipo de detalle. Pero Nakamoto se rehusó a todo intento por reconocerle o saber cualquier tipo de detalle sobre él, solo se comunicaba con sus colaboradores por correo o en foros públicos. Con el tiempo, Nakamoto pasó de ser el líder del movimiento a ocupar un papel secundario. El código del programa original había sido completamente rediseñado y estaba siendo constantemente controlado por un equipo de desarrolladores altamente calificados. En Abril de 2011 Nakamoto en una nota a esos especialistas advertía: “*Me voy a ocupar de otras cosas*”. Luego de este mensaje de despedida no se supo nunca nada más de él. De todas formas, el proyecto continuaba vigente teniendo como figura visible a Gavin Andresen.

Un mes después de estos eventos se produjo una masiva explosión de popularidad del Bitcoin y las descargas experimentaron un crecimiento sin precedentes. En Mayo del año 2011 se produjeron casi doscientas mil descargas y en el mes siguiente unas trescientas mil. Bitcoin estaba despegando.

Alrededor de este despegue de Bitcoin surgieron plataformas online que facilitaban las transacciones. La primera en surgir fue *BitcoinMarket.com* en Febrero de 2010, seguido de *Mt.Gox*. En estas primeras fases la exposición fue limitada a ciertos círculos relacionados a la informática y las finanzas. Se producían reportes constantes de errores en el sistema, transacciones fallidas, entre otras dificultades que alejaban al público general del Bitcoin.

Con el tiempo la popularidad de esta moneda virtual llamó la atención de otro tipo de público que vio gran potencial en su privacidad y se empezó a utilizar con fines de encubrimiento de fondos de dudosa procedencia y transacciones de incierta legalidad. En aquel momento *Mt. Gox* ya había procesado transacciones de Bitcoin por valor de un millón de dólares. Además, una nueva página web llamada “*Silk Road*”, en la que se comerciaba todo tipo de drogas y demás productos ilegales, estaba comenzando a operar aceptando únicamente Bitcoin como forma de pago. Debido a que las transacciones de Bitcoin son pseudoanónimas, no se puede perseguir a quien hace o recibe el pago. Este lado oscuro del Bitcoin atrajo la atención de las entidades reguladoras de los distintos países y, como se analiza en la última sección de este trabajo, propició la regulación del mismo a través de distintos mecanismos.⁸

De esta forma, Bitcoin surgió inicialmente en un foro de matemáticos e informáticos hasta llegar a captar la atención de muchos otros sectores y de una gran parte del público. Primero acudieron a él programadores y libertarios de distinta clase para ser seguidos por negocios ilícitos y buscadores de riqueza. Finalmente ha logrado, y cada vez más, atraer a inversores y personas involucradas en el mundo de las finanzas. Este proyecto ha superado las barreras de su fundador y ya ha pasado a ser de propiedad general. Ya no solo Bitcoin en sí, sino también la ideología y tecnología que hay detrás puede representar un claro cambio en el funcionamiento de la sociedad.³⁰

3.3. Acerca de Satoshi Nakamoto

“Satoshi Nakamoto” fue el pseudónimo utilizado por la persona, o el grupo de personas que diseñaron y crearon el sistema Bitcoin, con el fin de mantener el anonimato y así protegerse a ellos mismos y a la red.

Lo único que se sabe de “Satoshi Nakamoto” son los datos publicados en su perfil de la comunidad *P2Pfoundation*: hombre de nacionalidad japonesa y 38 años de edad (en el momento de publicación del documento principal). Sin embargo, no es posible demostrar que estos datos sean reales. Además, dado el diseño de Bitcoin, se le pueden atribuir conocimientos avanzados en criptografía y algoritmos matemáticos.³¹

Hay numerosas especulaciones sobre la identidad real que se esconde detrás de este pseudónimo. Una de ellas apuntaría a que se trata de Shinichi Mochizuki, matemático especializado en teoría de números y profesor de la Universidad de Kyoto.³² Otras especulaciones enlazan la figura de Nakamoto con identidades relacionadas con mercados negros y negocios criminales.

Inicialmente Satoshi Nakamoto fue muy activo en el foro de Bitcoin, llamado *bitcointalk.com* donde participaba y respondía a e-mails, utilizando tanto inglés británico como americano, en horarios aleatorios sin ningún patrón que pudiera sugerir una zona horaria.

A pesar de que Bitcoin era un proyecto de código abierto (“*open source*”), la mayoría de las modificaciones del código fuente fueron hechas por Satoshi el primer año, pero muy pronto dejó de estar involucrado de una manera activa.

³⁰ Gutiérrez Hernández, P. (2015). *El Bitcoin, ¿presente y futuro del dinero?* Universidad Pontificia Comillas. Madrid, España.

³¹ Díaz Vico, J. y Sanchez Aragón, A. (2014). *Bitcoin, una moneda Criptográfica*. Instituto Nacional de Tecnología de la Comunicación.

³² Neyman, L. (19 de Mayo de 2013). *Did mathematician Shinichi Mochizuki invent Bitcoin?* Gizmodo. Recuperado de: <https://gizmodo.com/did-mathematician-shinichi-mochizuki-invent-bitcoin-508715535>

Su última contribución fue a mediados de 2010 y después supuestamente pasó el mando a Gavin Andresen, que es quien se hizo visible y se dio a conocer como el Jefe Científico de la “Fundación Bitcoin” hasta Abril de 2014, cuando fue reemplazado por Wladimir Van Der Lan.

En Abril de 2011 cuando Nakamoto fue preguntado sobre su bajo nivel de involucramiento pese a haber sido su mentor, explicó que se había ocupado de otros proyectos: “*moved on to other things*”, expresó. Tiempo después dejó de responder a emails incluidos los de Andresen. No se detectaron referencias a Satoshi Nakamoto fuera del contexto de Bitcoin.³³

Finalmente, en el año 2016 un empresario y científico computacional australiano, llamado Craig Wright, reveló su identidad a la BBC, las revistas The Economist y GQ, declarando que él era Satoshi Nakamoto y ofreciendo pruebas técnicas para respaldar su declaración. En su reunión con la BBC, Wright firmó mensajes digitalmente usando claves criptográficas que fueron creadas durante las primeras etapas de la creación del Bitcoin. Estas claves están inextricablemente vinculadas a bloques de Bitcoins que se sabe fueron minados por Satoshi Nakamoto, el nombre con que se identificaba el creador de la moneda.³⁴ Craig Wright afirmó que, al revelar públicamente su identidad, esperaba poner fin a toda la especulación sobre Satoshi Nakamoto.

Poco después de la revelación, Gavin Andresen, el jefe científico de la Fundación Bitcoin, publicó un blog respaldando la afirmación. “*Creo que Craig Steven Wright es la persona que inventó el Bitcoin*”, escribió. Sin embargo, la comunidad del Bitcoin mantiene sus reservas sobre si realmente Craig Wright es Satoshi Nakamoto.

³³ La revista *Newsweek* afirmó, el 7 de marzo de 2014, que un ingeniero de origen japonés, de 64 años, residente de California, era el misterioso creador de la moneda virtual, pero *Dorian Satoshi Nakamoto* negó tal versión, todo lo cual ocasionó una gran conmoción internacional que terminó con las acciones legales del señalado hacia la revista por utilización de su imagen en violación a su intimidad. Más recientemente, científicos británicos mediante análisis del estilo de escritura del artículo original han identificado al experto en criptografía y derecho *Nick Szabo*, dentro de las once personas o grupos considerados habitualmente como los principales sospechosos, descartando a otros, como *Dorian Satoshi Nakamoto*. Recuperado de: http://www.tendencias21.net/Encuentran-al-creador-del-sistema-monetario-virtual-Bitcoin_a33080.html

³⁴ “*Luego de años en las sombras, el creador de Bitcoin revela su identidad*”. 2 de Mayo de 2016. BBC Mundo. Recuperado de: http://www.bbc.com/mundo/noticias/2016/05/160502_bitcoin_creador_satoshi_nakamoto_craig_wright_revelacion_wbm

CAPÍTULO 4: ¿QUÉ ES REALMENTE BITCOIN? UN ANÁLISIS DE SUS PROPIEDADES

4.1. ¿Qué es Bitcoin?

Usualmente se suele reconocer a Bitcoin como una moneda virtual, un sistema electrónico de pagos, una red descentralizada P2P y un software de código abierto. La unión de estos componentes permite la realización de transacciones casi instantáneas entre pares (*peer-to-peer*) y, por consiguiente, pagos alrededor de todo el mundo con unos bajos costos, o incluso nulos, de procesamiento de dichas transacciones.

Bitcoin utiliza una tecnología *peer-to-peer*, esto implica que no depende de una autoridad central que asuma la responsabilidad ni de su emisión ni del registro de los movimientos que se produzcan con la misma. En su lugar, se apoya en una red de distribución “*persona-a-persona*”, a través de computadoras interconectadas que representan a la comunidad de usuarios de esta moneda.³⁵

De esta manera, no es posible manipular el valor de los Bitcoins o crear inflación imprimiendo más moneda. La propia red es la que gestiona las transacciones y la emisión de Bitcoins, que se generan a través de la actividad denominada “minería”, de forma controlada y descentralizada.

La utilización de criptografía garantiza la seguridad de las transacciones. Las figuras de control y supervisión presentes en los sistemas monetarios de los mercados actuales no existen en Bitcoin.

¿Qué es una red *peer-to-peer*?

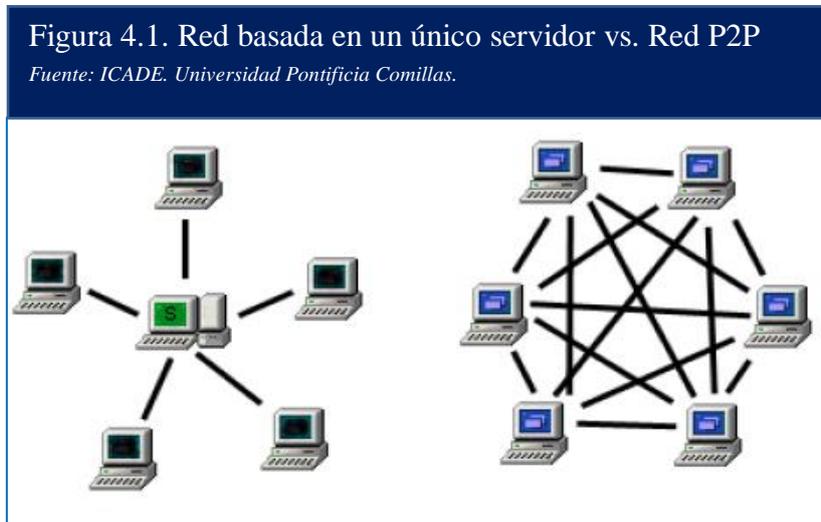
Una red “*peer-to-peer*”, red de pares o red punto a punto (P2P, por sus siglas en inglés) es una red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino mediante una serie de nodos o puntos de encuentro que se comportan como iguales entre sí.³⁶ Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red y, de esta forma, se produce el intercambio directo de información sin necesidad de un intermediario. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados.

Resumiendo, a diferencia de una red tradicional basada en servidores donde existe un administrador central que se encarga del control de la red, P2P conecta directamente dos

³⁵ Gorjón, S. (2014). *Divisas o Monedas Virtuales: el caso de Bitcoin*. Banco de España. España.

³⁶ Mariño, K. (sin fecha). Redes de Comunicación. Recuperado de: <http://es.calameo.com/read/002743183263406e7733a>

ordenadores permitiendo que interactúen sin necesidad de intermediación. Esta diferencia se puede observar en la Figura 4.1.



La red *peer-to-peer* tiene como gran ventaja la creación de grandes bases de datos de manera gratuita, ya que todos los ordenadores conectados pueden descargarse información de los diferentes integrantes de la red. Esta ventaja es la utilizada por el sistema Bitcoin. (Sánchez De Diego Martínez Cabrera, 2014).

4.2. Participantes del sistema Bitcoin

Pioneros en la adopción de Bitcoin: Los pioneros en la adopción de Bitcoin se sumaron al proyecto desde su etapa más temprana, dándole el impulso inicial para que sobreviva en los primeros años de su desarrollo.

Mineros: Son usuarios especiales que dedican capacidad de procesamiento para validar nuevas transacciones, creando lo que se conoce como cadena de bloques (*Blockchain*). Al verificar la legitimidad de las transacciones, los mineros proveen seguridad a la comunidad de Bitcoin. Para eso invierten su tiempo (en actualizar, mantener y ajustar sus equipos) y su dinero (en hardware y electricidad). Lo hacen, por supuesto, a cambio de una recompensa en Bitcoins.

Desarrolladores: Bitcoin es, en definitiva, un software y como tal, necesita un desarrollo y mantenimiento activos para lo cual es imprescindible un equipo de desarrolladores.³⁷

Ahorristas: Son aquellos que atesoran buena parte de los Bitcoins que han adquirido. De esta manera, mejoran el poder adquisitivo de todos los poseedores de Bitcoins (muchos de los cuales

³⁷ Se puede consultar un listado en <https://en.bitcoin.it/wiki/Clients>

invertirán ese capital en emprendimientos que, a larga, fortalecerán a Bitcoin), y así atraen a nuevos usuarios.

Comerciantes: Desde los emprendedores más arriesgados hasta los comerciantes más tradicionales, todos los que aceptan Bitcoins a cambio de sus productos están expandiendo el uso y difundiendo las ventajas de esta criptomoneda.

Consumidores: Son quienes guían, en gran medida, las decisiones de los empresarios. Usar Bitcoins para adquirir bienes y servicios es otra manera de fortalecer a la economía basada en Bitcoin.

4.3. ¿Cómo funciona Bitcoin?

Antes del surgimiento de Bitcoin, las transacciones realizadas a través de internet requerían de una institución intermediaria. Por ejemplo, si el individuo “A” quería enviar \$100 a otro individuo “B”, tenía que confiar en un intermediario, como por ejemplo *PayPal*. Este tipo de intermediarios conserva registros de todos los saldos de las cuentas de los titulares. Cuando “A” le envía \$100 a “B”, *PayPal* extrae dicho monto de la cuenta de “A” y lo acredita en la cuenta de “B”.

Sin estos intermediarios, existiría el riesgo de que el dinero digital se gaste dos veces. Un ejercicio práctico es imaginar que no existen intermediarios que lleven este tipo de contabilidad y que el dinero digital es un simple archivo, como lo son los documentos digitales. De esta manera, “A” podría enviarle \$100 a “B” adjuntando un archivo de dinero a un mensaje. Pero como sucede con el correo electrónico, enviar un documento adjunto no lo elimina de nuestra computadora. “A” conservaría una copia del archivo de dinero después de enviarlo y bien podría enviar los mismos \$100 a otro individuo “C”. En las Ciencias de la Computación, esto se conoce como el “problema del doble gasto”³⁸, hasta la llegada de Bitcoin solo se lo podía resolver empleando un intermediario de confianza que conservara un registro de cada cuenta.

La invención de Bitcoin es revolucionaria ya que, por primera vez, el problema del doble gasto se puede solucionar sin la necesidad de un intermediario. Bitcoin permite superar esto mediante la distribución de los registros entre todos los usuarios del sistema conectados a una red de transmisión de persona a persona. Cada transacción que se produce en la red de Bitcoin queda registrada en un libro digital público, distribuido, que se denomina ‘cadena de bloques’. Cada nueva transacción se verifica contra la cadena de bloques para asegurarse de que los mismos Bitcoins no hayan sido gastados previamente, eliminando así el problema del doble gasto. La red global de persona a persona, compuesta por miles de usuarios, adquiere así el lugar del

³⁸ Chaum, D. (1992). “Achieving Electronic Privacy,” *Scientific American*, p.96–101.

intermediario, lo que permite a “A” y “B” realizar transacciones sin utilizar *PayPal* u otros.³⁹

Es importante destacar, además, que las transacciones en la red de Bitcoin no están denominadas en Pesos o Dólares o Euros, como sí lo están en *PayPal*, sino que están denominadas en Bitcoin. Esto la convierte en una moneda virtual además de una red descentralizada de pagos. El valor de la moneda no está basado en el precio del oro ni determinado por ningún gobierno, sino que es el valor que la gente le asigna.⁴⁰

Criptografía de claves públicas

La manera en que se verifican las transacciones y se evita el problema del doble gasto es mediante la utilización de la criptografía de claves públicas. La criptografía de claves públicas requiere la asignación a cada usuario de dos claves: una privada, que debe mantenerse secreta (como una contraseña privada) y una pública, que puede compartirse con todo el mundo. Las llaves privadas correspondientes a cada llave pública sirven para que un determinado usuario autorice pagos (transfiera Bitcoins) desde su billetera.

Las direcciones públicas no tienen ninguna información sobre sus dueños; éstas aparecen como secuencias alfanuméricas de 33 caracteres de largo, como por ejemplo:

1rYK1YzEGa59pI314159KUF2Za4jAYYTd

Los usuarios de Bitcoin pueden tener múltiples direcciones; de hecho, pueden generar direcciones nuevas fácilmente y sin límites. Generar una nueva dirección equivale a generar un nuevo par de llaves (pública y privada), y no requiere ningún contacto con nodos de la red. Los usuarios que desean preservar el anonimato suelen crear una nueva dirección para cada transacción.

4.4. Transacciones de Bitcoins

Cuando un usuario A transfiere Bitcoins a un usuario B, el usuario A renuncia a su posesión de un determinado número de Bitcoins, agregándoles la llave pública de B y firmando la combinación resultante con su llave privada (gracias al empleo de la criptografía asimétrica, la llave privada no puede ser deducida de la firma que de ella deriva). Esta información se transmite a toda la red P2P como una nueva transacción. De esta manera, el resto de los nodos de la red verifican el número de Bitcoins involucrados y la autenticidad de las firmas criptográficas, antes de aceptar la transacción como válida. La transacción (y de esa manera la transferencia de la propiedad de los Bitcoin) queda registrada, timbrada con la fecha y la hora y visible en uno de los “bloques” de la

³⁹ Brito, J. y Castillo, A. (2014). *Bitcoin, manual básico (para legisladores y diseñadores de políticas)*. Research Gate. George Mason University.

⁴⁰ Markets.” BitcoinCharts”. Recuperado de: <http://bitcoincharts.com/markets/>

cadena de bloques.

Una vez que se efectúa la transacción, ésta es distribuida por todos los nodos de la red para su confirmación y colocación en un bloque. La firma permite que la operación no sea alterada durante este proceso y previene el doble gasto. Las transacciones empiezan a ser confirmadas en los diez minutos siguientes. Se considera que con seis confirmaciones (una hora) la transacción es irreversible y, por consiguiente, válida y segura.

La criptografía de claves públicas permite que todas las computadoras de la red tengan un registro constantemente actualizado y verificado de todas las transacciones que se realizan en la red, lo que evita el doble gasto.⁴¹

En síntesis, la operatoria con Bitcoins se resume de la siguiente manera:

- a. Las transferencias de BTCs se hacen exclusivamente de manera online, y todas las transacciones tienen lugar entre “direcciones” (serie de 33 caracteres, letras y números) en lugar de personas identificadas.
- b. Cada usuario utiliza una billetera o archivo que debe tener instalado en su computadora (también los hay online), antes de comenzar a operar en un sitio de Internet que opere con BTCs (conocidos normalmente como “*Bitcoin Exchanges*”).
- c. Quien ingresa por primera vez para adquirir Bitcoins debe registrarse, abrir una cuenta propia en el *Bitcoin Exchanges*, hacerle una orden de compra, y una transferencia bancaria desde su monedero (o billetera) a este sitio por la cantidad de BTCs que desee comprar.
- d. El *Bitcoin Exchanges* es el encargado de gestionar la oferta y la demanda de BTCs, y básicamente se ocupa de transferir BTCs de una dirección a otra, a cambio del pago de una comisión.
- e. Una vez aprobada la operación, se transfieren los BTCs desde el *Bitcoin Exchanges* a la billetera del comprador. Éste, retira los BTCs adquiridos con su clave privada, transfiriéndolos desde la web de la sociedad intermediadora a su billetera virtual, y al completarse la operación, pasa a tener en su billetera, 0 (cero) moneda de curso legal y la cantidad de BTCs adquiridos.
- f. Inversamente, para vender la persona transfiere los BTCs que desea vender, desde su billetera a la cuenta propia que tiene en el *Bitcoin Exchanges*, donde coloca una orden de venta por un precio determinado. Al completarse la operación, esta persona requiere un retiro de fondos al *Bitcoin Exchanges*, el que le haría una transferencia bancaria desde la

⁴¹ Brito, J. y Castillo, A. (2014). *Bitcoin, manual básico (para legisladores y diseñadores de políticas)*. Research Gate. George Mason University.

cuenta del sitio a su billetera, pasando a tener la moneda de curso legal en su balance en el sitio y 0 (cero) BTCs.⁴²

4.5. ¿Es Bitcoin o su tecnología *Blockchain*?⁴³

En los últimos tiempos ha aparecido una serie de economistas, expertos y especialistas en finanzas que afirman que lo revolucionario no ha sido el surgimiento de una moneda virtual completamente descentralizada, sino que la innovación que podría cambiar el futuro de los sistemas de pago es la tecnología en la que esta criptomoneda está basada, el *Blockchain* o la cadena de bloques.

El *Blockchain* o cadena de bloques es un registro público y descentralizado de transacciones que se mantiene mediante una red distribuida de computadoras, que no requiere respaldo de ninguna autoridad central o una tercera parte de confianza y que ofrece un esquema transaccional libre de intermediarios, gracias al uso de algoritmos.⁴⁴

Una red de computadoras mantiene este “libro contable común” vía Internet. Este libro contable común es público y es distribuido en su totalidad a través de una red de “nodos”, cada uno de los cuales tienen una copia completa del mismo o de la cadena de bloques.

En una cadena de bloques, todos los detalles de una nueva transacción son registrados y verificados por agentes denominados “mineros”, quienes compiten por ser los primeros en resolver problemas matemáticos complejos y poder publicar el siguiente bloque de transacciones en el libro contable (o la cadena del historial de transacciones). Los mineros son personas que utilizan complejos sistemas informáticos para resolver problemas matemáticos y reciben un tipo de remuneración por sus esfuerzos. Cuando el bloque de transacciones es subido por el minero que fue el primero en resolver el cálculo, todos los nodos de la red validan automáticamente el libro contable y todas las transacciones que se encuentren en él. Por lo general, la mayoría de los nodos (el 51% de los mismos) deben aceptar que el bloque es válido para que éste pase a formar parte de la cadena de bloques de transacciones o *Blockchain*. Los bloques de transacciones son usualmente publicados en el libro contable compartido en intervalos de diez minutos.

Esta tecnología permite dar solución a la principal barrera técnica de las últimas décadas para los desarrolladores tecnológicos, el problema del doble gasto.

⁴² Viegas, C. et al. (2014). *Bitcoin, un desafío para la ejecución de políticas de la Banca Central*. Banco Central de la República Argentina. Argentina

⁴³ Este apartado está basado en “*La cadena de bloques: Una tecnología disruptiva con el poder de revolucionar el sector financiero*”. Informe técnico de EquiSoft. Marzo de 2017

⁴⁴ Rodríguez, N. y García, A. (2017). *Blockchain: mirando más allá del Bitcoin*. Asobancaria

El problema del doble gasto

Es usual considerar a la capacidad de replicación de Internet como un atributo provechoso, ya que se puede copiar y enviar todo tipo de archivos sin que eso implique una pérdida de acceso al original. Sin embargo, este gran poder multiplicativo no pareciera conveniente para una moneda ya que, en una suerte de falsificación, se podría copiar y gastar varias veces. Esto es lo que se conoce como el ‘problema del doble gasto’.

La solución clásica a este problema es la existencia de una autoridad central, como una casa de la moneda, que lleve un registro de todas las transacciones para identificar un doble gasto. Sin embargo, esto es lo que justamente Satoshi Nakamoto quería evitar. Afirmaba que, con ese esquema, “*el destino de todo el sistema monetario depende de la compañía que gestiona la casa de moneda*”. ¿Cómo hacer, entonces, para verificar que el Bitcoin que uno adquiere no ha sido ya utilizado en otra transacción?

“*La única forma de confirmar la ausencia de una transacción es estando al tanto de todas las transacciones. Para lograr esto sin un tercero de confianza, las transacciones deben ser anunciadas públicamente; necesitamos un sistema de participantes que estén de acuerdo con una única historia del orden en que éstas fueron recibidas*”, alegaba Nakamoto.⁴⁵ Este razonamiento encontró su expresión técnica en el ‘*Blockchain*’ o cadena de bloques, una de las mayores singularidades de Bitcoin.

¿Qué tan segura es la cadena de bloques?

Considerando el carácter público y compartido de la cadena de bloques, es natural que surjan cuestionamientos respecto a la seguridad de las transacciones en este tipo de red. En realidad, la cadena de bloques es mucho más segura que las redes de transacción existentes.⁴⁶

En primer lugar, aunque el libro contable y todas sus transacciones son públicos, las personas que participan en la cadena de bloques mantienen el anonimato, por intermedio de claves cifradas públicas y privadas. Esto significa que incluso si todos conocen todas las transacciones y el saldo de todos los participantes en la cadena de bloques, no existe ninguna manera de relacionar las transacciones con las personas específicas.

En segundo lugar, debido a que cada nodo individual de la red posee un registro actualizado del libro contable, para modificar las transacciones en la cadena de bloques un *hacker* informático tendría que piratear por lo menos el 51% de los nodos a nivel mundial (porque si no hay consenso,

⁴⁵ Nakamoto, S. (2008). *Bitcoin: un sistema de efectivo electrónico usuario a usuario*. Extraído de: www.bitcoin.org

⁴⁶ *La cadena de bloques: una tecnología disruptiva con el poder de revolucionar el sector financiero*. Informe técnico de EquiSoft. Marzo de 2017

un bloque de transacciones no puede ser incluido en la cadena) en un tiempo de diez minutos (que es la frecuencia con que un nuevo bloque de transacciones es validado y agregado a la cadena). Esta situación se analiza a continuación.

Colapso por mayoría

El problema de la verificación descentralizada reside en encontrar un mecanismo que haga muy costoso que uno o varios verificadores manipulen el registro a su favor exitosamente. Esto es lo que se llama en el ámbito de seguridad digital *el problema de los generales bizantinos*.⁴⁷

El colapso por mayoría sería una situación en la cual exista un minero o un “pool” de mineros que tenga más del 50% del poder de procesamiento de la red. En ese caso, esa persona o grupo podría alterar todo el funcionamiento monetario pudiendo verificar transacciones que utilicen por segunda vez el mismo Bitcoin, ya que sólo con su mayoría gobernarían los movimientos de la moneda en todo el mundo. Esta realidad hipotética es muy difícil que llegue a darse en la realidad, debido al mecanismo de incentivos con que se maneja el protocolo de Bitcoin. En palabras del economista Paul Bhom:

“Para asegurarse de que le sea más caro a un atacante adquirir el poder computacional necesario para poder engañar al sistema, Bitcoin cuenta con una estructura de incentivos. Los usuarios que aportan poder computacional (los “mineros”) se ven recompensados por su trabajo; así, cuando el valor del Bitcoin aumenta y por lo tanto atacar al sistema se torna más rentable, también se torna más rentable para los usuarios honestos agregar recursos computacionales a la red.

En cualquier momento dado, los mineros invierten en equipos tanto como es rentable para cada uno de ellos. La “minería” no es en absoluto un desperdicio de energía, sino todo lo contrario: es una forma increíblemente eficiente de hacer que los ataques no sean rentables. Bitcoin incentiva a los mineros a fin de proteger el consenso que se da entre los nodos de la red, pero nunca utiliza más recursos computacionales de los que necesita para proteger su integridad y buen funcionamiento”. (Bohm, 2013, pág. 3)

Innovaciones financieras utilizando Blockchain

Las aplicaciones de la tecnología de cadena de bloques están centradas en el concepto de facilitar las operaciones de intercambio de dinero u otros activos y la actualización de los antiguos

⁴⁷ Este problema es ilustrado por un ejército bizantino que acampa en grupos dispersos a punto de tomarse una ciudad enemiga. Los generales involucrados solo puede comunicarse a través de mensajeros. Los generales deben llegar a un acuerdo sobre un plan de acción común (por ej. la hora del ataque); no obstante, puede haber generales traidores que emiten mensajes alterados. Por tanto, los generales deben tener un protocolo de comunicación que garantice que los generales leales seguirán el mismo curso de acción dictado por el protocolo, y que este curso de acción tiene altos chances para alcanzar la victoria, sin importar cuáles sean las acciones de los generales traidores

sistemas heredados de transacción y de liquidación. Sin embargo, la tecnología *Blockchain* ofrece a las firmas de servicios financieros y a las empresas de seguros otras e innumerables oportunidades para optimizar sus procesos y reducir los costos.¹⁴

Industria de medios de pago: La principal innovación que aporta el *Blockchain* es el registro público de transacciones sobre el que opera su sistema de pago, y en el que las transacciones son registradas en forma secuencial. Las redes de pago a través de tarjetas de crédito y los servicios que permiten hacer transferencias están diseñadas para resolver un problema de doble gasto, es decir, garantizan que no se duplique ninguna transacción y que el dinero fluya de una persona a otra. El *Blockchain* permitiría esta garantía no solo para el dinero, sino para cualquier activo financiero que se quisiera transferir.⁴⁸

Mercado de Capitales: En el caso de mercado de capitales, el *Blockchain* puede utilizarse para la simplificación de varios de los procesos asociados al intercambio de instrumentos financieros, como por ejemplo el pago, la compensación y la liquidación, que pueden ser automáticos y descentralizados, sin necesidad de un intermediario, como una cámara de compensación. A futuro, y en la medida que la tecnología evolucione, podrán desarrollarse soluciones que soporten el proceso de otros activos, como por ejemplo hipotecas.

¿A qué desafíos se enfrenta esta tecnología?

Si bien la tecnología de cadena de bloques tiene el potencial de impulsar un cambio de paradigma en la forma como se hacen los negocios en el mundo, ésta no deja de tener desafíos. A continuación se indican algunos de los principales retos asociados con la adopción de esta joven tecnología.⁴⁹

Aceptación: Debido a que la cadena de bloques es una tecnología sin precedentes, lograr su comprensión y aceptación por parte de los desarrolladores de sistemas, los usuarios y los operadores constituye todo un reto.

Costo: Pese a que la tecnología de cadena de bloques puede ofrecer a las organizaciones ahorros increíbles en los costos, los altos costos iniciales pueden representar un factor disuasivo. Pasar de un sistema centralizado a una red descentralizada requiere cambios significativos o el reemplazo completo de la estructura heredada.

⁴⁸ Rodríguez, N. y García, A. (2017). *Blockchain: mirando más allá del Bitcoin*. Asobancaria

⁴⁹ *La cadena de bloques: una tecnología disruptiva con el poder de revolucionar el sector financiero*. Informe técnico de EquiSoft. Marzo de 2017

Aspectos reglamentarios: Las divisas mundiales en la actualidad son por lo general creadas y reguladas por los gobiernos nacionales. Las criptomonedas, gestionadas por cadenas de bloques, pueden tener dificultades para lograr su adopción generalizada por las instituciones financieras existentes, si las preguntas acerca de su estatus normativo no son contestadas.

Consumo de energía: La tecnología de cadena de bloques necesita una cantidad importante de energía para mantenerse activa. A medida que se añaden nuevas cadenas de bloques, las exigencias en cuanto a la capacidad informática de procesamiento pueden crecer exponencialmente.

Normalización: Para que la cadena de bloques pueda acelerar eficazmente los procesos comerciales, mejorar el mantenimiento de registros, perfeccionar la detección de fraudes y mucho más, es necesario un cierto nivel de normalización global a través de las instituciones. Desafortunadamente, esto es algo más fácil de decir que de hacer. Las costumbres, los regímenes reglamentarios y los procesos políticos de los países pueden retrasar los esfuerzos de normalización.

En resumen, se podría entender esta tecnología con fundamento en sus tres características generales de la siguiente forma: i) Blockchain es una tecnología "sin confianza", lo que significa que por primera vez en la historia, intercambios de valor a través de una red de computadoras pueden ser verificados, monitoreados y asegurados sin la presencia de un tercero de confianza o de una institución central; ii) es una tecnología de autenticación y verificación, que permite de forma más eficiente las transferencias de títulos y la verificación de propiedad y iii) por ser una tecnología sin fronteras y sin fricción, puede proporcionar una más económica y rápida infraestructura para el intercambio de unidades de valor.⁵⁰

Tarifas transaccionales

Debido a que los mineros no tienen la obligación de incluir transacciones en los bloques que generan, los remitentes de Bitcoins pueden pagar voluntariamente una tarifa de transacción.

Al hacerlo, además de acelerar la transacción, proveen incentivos a los usuarios que mantienen nodos generadores (es decir, a los mineros). Los nodos generadores retienen el valor correspondiente a las tarifas de todas las transacciones incluidas en los bloques que han resuelto.

⁵⁰ Rodríguez. N. v García. A. (2017). *Blockchain: mirando más allá del Bitcoin*. Asobancaria

Dichas tarifas suelen ser una fracción muy pequeña del monto enviado, si se las compara con las de cualquier otro sistema de transferencia de valor.

Las tarifas de transacción irán cobrando más importancia cuanto más bajo sea el premio por bloque. En el futuro, los mineros se verán motivados a mantener los nodos generadores por la suma de pagos en concepto de tarifas que puedan acumular, más que por los Bitcoins que sean capaces de generar.

4.6. Obtención de Bitcoins

Existen varios mecanismos a través de los cuales se pueden obtener Bitcoins, los que se mencionan a continuación:

- Compra de Bitcoins en sitios de *Bitcoin Exchanges*.
- Intercambio entre particulares.
- Compensación por la venta de productos o servicios.
- Minería de Bitcoins.

En los últimos años han aparecido muchos sitios de *trading* que permiten que la oferta y la demanda de Bitcoins coincidan en un lugar común para poder hacer intercambios. Estos servicios son muy importantes ya que permiten adquirir Bitcoins a cambio de dinero y, lo más importante, permiten convertir los Bitcoins en dinero en efectivo. Estas operaciones pueden estar sujetas a una comisión para el prestador del servicio.

Un particular también puede hacer un intercambio sin necesidad de recurrir a un servicio concreto. Sólo requiere conocer el identificador del destinatario de la transacción y ordenarla mediante su monedero de Bitcoins. Como contraprestación puede recibir dinero, servicios o cualquier otro beneficio que hayan acordado las dos partes como si se tratara de dinero en metálico.

Son muchas las empresas que están comenzando a utilizar a Bitcoin como medio de pago de sus servicios. El tipo de negocio que empezó a aceptar el pago en Bitcoins estaba relacionado con actividades ilícitas como armas, drogas, etc. Sin embargo, la economía real también está empezando a tenerlo en cuenta como medio de pago.

Para incentivar a que los usuarios sostengan activamente el funcionamiento del sistema, la colaboración en el procesado de transacciones es una actividad remunerada que permite a la persona que proporciona sus recursos obtener un beneficio de las operaciones necesarias para incorporar transacciones a la cadena de bloques. Esta actividad, que se denomina minería, es un mecanismo relativamente complejo que se tratará con más detalle en el apartado 4.9. “¿Cómo se

crean los Bitcoins? El proceso de minería”.

4.7. ¿Dónde se almacenan los Bitcoins?

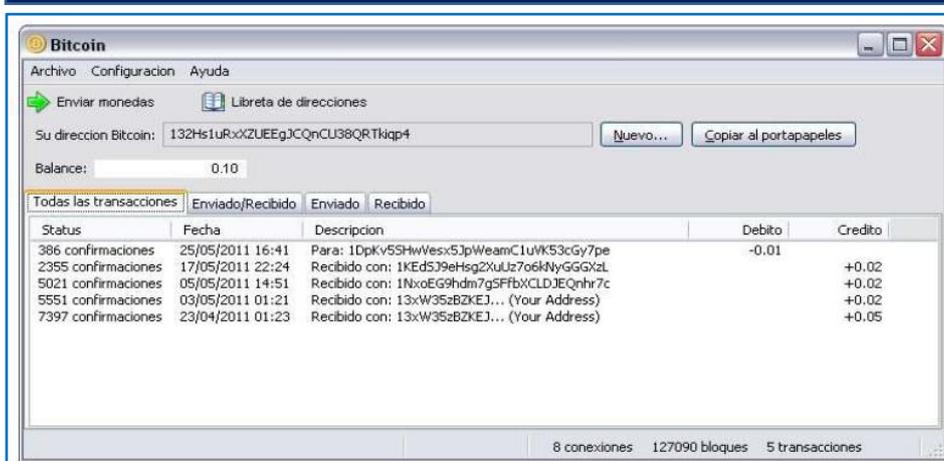
La página semioficial⁵¹ de Bitcoins (<https://bitcoin.org/en/choose-your-wallet>) ofrece distintas billeteras virtuales o monederos que pueden ser utilizados para almacenar y transferir Bitcoins entre los usuarios. Básicamente las billeteras son pequeños estados de cuenta que muestran el saldo (cantidad de Bitcoins disponibles), las últimas transacciones y que permiten al usuario realizar operaciones.

Estas billeteras son *softwares* de escritorio (carteras frías) que pueden funcionar en distintos tipos de plataformas como *Windows*, *Mac* o *Linux*, así como también en plataformas móviles como *Android* o *Blackberry*. Al descargar la aplicación, se proporciona un nombre de usuario y una contraseña, la cual permanecerá privada siempre cuando el usuario no comparta esta información. Al crearse un nuevo registro, se encripta la billetera y pasa a ser parte de la red global de Bitcoins en el mundo; su dirección es única y cada transacción que realice queda registrada en la red Bitcoin. Este método es bastante seguro, aunque resulta vulnerable ante robos físicos o simples pérdidas de las claves.

Además, existen muchas billeteras en forma de páginas web que proporcionan la opción de alojar el monedero de un usuario (carteras calientes). Esta es la forma más cómoda de almacenar los Bitcoins, pero implica un gran riesgo de ataque informático. En la Figura 4.2 se puede observar un ejemplo de una billetera virtual.

Figura 4.2. Ejemplo de billetera virtual.

Fuente: www.bitcoin.org.es



⁵¹ Bitcoin no tiene una página oficial, sin embargo www.bitcoin.org es un portal manejado por los mismos fundadores de la criptomoneda y se dedica a dar noticias, cotizaciones y temas varios relacionados a los Bitcoins.

De lo expuesto anteriormente se deduce que el almacenamiento de los Bitcoins se reduce al almacenamiento de las llaves que componen una cartera. La llave privada de la cartera, equivalente a una clave bancaria, es el elemento más importante de la misma ya que su pérdida inutiliza la cartera. La seguridad de cada usuario en el sistema del Bitcoin reside en gran medida en las formas utilizadas para el almacenamiento de las llaves.

En cuanto a las denominaciones de esta moneda virtual, un Bitcoin es denotado como 1 BTC y puede ser dividido hasta alcanzar hasta 8 cifras decimales. Esto significa que la mínima cantidad de BTCs que se puede poseer es 0.00000001 BTC, que como homenaje a su fundador se conoce como un *Satoshi*. De esta manera, las demás divisiones posibles también tienen su propia denominación:

Figura 4.3. Diferentes denominaciones de Bitcoin.
Fuente: www.bitcoin.org.es

1 BTC	A bitcoin
0.01 BTC	A bitcent
0.001 BTC	An mbit
0.000001 BTC	A ubit
0.00000001 BTC	A satoshi

4.8. Fundamentos económicos de Bitcoin⁵²

Las raíces teóricas de Bitcoin se pueden encontrar en la Escuela de Economía Austríaca y su crítica del actual sistema de dinero fiduciario y las intervenciones emprendidas por los gobiernos y otras agencias, que, en su opinión, resultan en ciclos económicos exacerbados y procesos inflacionarios.

Uno de los temas sobre los que se ha centrado la Escuela de Economía de Austria, dirigida por Eugen von Böhm-Bawerk, Ludwig von Mises y Friedrich A. Hayek, es el ciclo económico. En resumen, según la teoría austriaca, los ciclos económicos son la consecuencia inevitable de las intervenciones monetarias en el mercado, por lo que una expansión excesiva del crédito bancario provoca un aumento en la oferta de dinero mediante el proceso de creación de dinero en un sistema bancario de reserva fraccionaria, que a su vez conduce a tasas de interés artificialmente bajas. En esta situación, los empresarios, guiados por señales de tipos de interés distorsionadas, se embarcan en proyectos de inversión demasiado ambiciosos que no coinciden con las preferencias de los consumidores en ese momento en relación con el consumo intertemporal (es decir, sus decisiones sobre el consumo a corto plazo y futuro). Tarde o temprano, este desequilibrio

⁵² Apartado extraído de: European Central Bank. *Virtual Currency Schemes* (2012).

generalizado ya no puede sostenerse y conduce a una recesión, durante la cual las empresas necesitan liquidar cualquier proyecto de inversión fallido y readaptar sus estructuras de producción de acuerdo con las preferencias intertemporales de los consumidores. Como resultado, muchos economistas de la Escuela Austriaca piden que se abandone este proceso aboliendo el sistema bancario de reserva fraccionaria y volviendo al dinero basado en el patrón oro, que no puede ser fácilmente manipulado por ninguna autoridad.

Otra área relacionada en la que los economistas austríacos han sido muy activos es la teoría monetaria. Uno de los principales nombres en este campo es Friedrich A. Hayek. Este autor escribió algunas publicaciones muy influyentes, como *Denationalisation of Money* (1976), en las que plantea que los gobiernos no deberían tener el monopolio de la emisión de dinero. En cambio, sugiere que se permita a los bancos privados emitir certificados sin intereses basados en sus propias marcas registradas. Estos certificados (es decir, las monedas) deberían estar abiertos a la competencia y se negociarían a tipos de cambio variables. Cualquier moneda que pueda garantizar un poder de compra estable eliminaría otras monedas menos estables del mercado. El resultado de este proceso de competencia y maximización de utilidades sería un sistema monetario altamente eficiente donde solo coexistirían monedas estables.

4.9. ¿Cómo se crean los Bitcoins? El proceso de minería⁵³

El esquema de Bitcoin está diseñado como un sistema descentralizado donde no está involucrada una autoridad monetaria central. Por lo tanto, el suministro de dinero no depende de la política monetaria de ningún Banco Central, sino que se desarrolla en función de los usuarios interesados que realizan la actividad de la minería.

Como indica González Otero en su libro “Bitcoin: la moneda del futuro” (González Otero, 2013), dentro del sistema *peer-to-peer*, en el que cada usuario aporta su granito de arena, es donde se encuadra la actividad de la minería de Bitcoins. El nombre con el que se denominó a esta actividad proviene del método de extracción de metales preciosos, dado que la base teórica es similar, en el cual un individuo o un grupo de individuos, aplicando un trabajo pueden obtener una recompensa. Dicha minería es el mecanismo en el cual se agregan “bloques” a la “cadena” para verificar las últimas transacciones realizadas. Este es un proceso complejo y necesita un gran poder de procesamiento. El incentivo para las personas que aportan su tiempo y sus equipos informáticos es que al producir un bloque de esa “cadena de bloques” recibirán una cantidad estipulada de

⁵³ Este apartado se encuentra basado en Vidal, G. (2014). *Bitcoin: comportamiento como moneda e inversión*. Facultad de Economía y Empresa. Universidade da Coruña. España

Bitcoins recompensando su esfuerzo. Esta cantidad en los inicios de la moneda eran 50 BTCs, y va disminuyendo progresivamente a la mitad cada cuatro años.

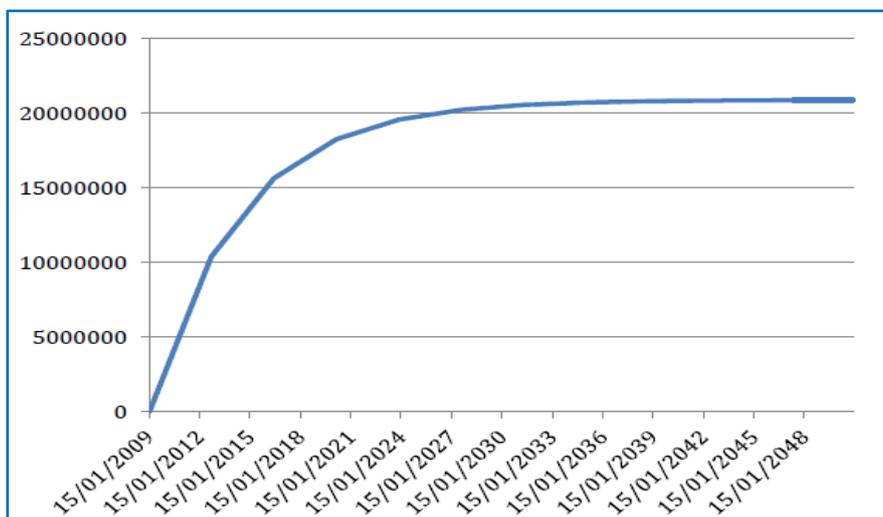
De esta manera, un minero de Bitcoins es aquel individuo que mediante un programa informático aporta la capacidad de procesamiento de su computadora personal para el funcionamiento de la red, a cambio de la obtención de una cierta cantidad de Bitcoins de nueva creación. La capacidad de procesamiento de esta computadora será utilizada para la resolución de algoritmos relacionados con la verificación de transacciones producidas en la red.

Los algoritmos a ser resueltos (es decir, los nuevos bloques por descubrir) para recibir los Bitcoins recién creados se vuelven cada vez más complejos (se necesitan más recursos informáticos). Como se explica en el sitio web www.bitcoin.org, la tasa de creación de bloques es aproximadamente constante a lo largo del tiempo: seis por hora, uno cada diez minutos. Sin embargo, el número de Bitcoins generados por bloque disminuye con el paso del tiempo, con una reducción del 50% cada cuatro años.

Este proceso de creación de nuevos Bitcoins está completamente regulado por el protocolo de Bitcoin publicado en 2008, siendo diseñado para que se alcance un stock total de 21 millones de Bitcoins en el mercado en el año 2141, fecha a partir de la cual no se generarán más. Sin embargo, la fecha realmente importante es la de 2033, en la que, según los cálculos, el aporte de Bitcoins por bloque descifrado se vería reducido hasta los 0.78 BTCs con lo que sería a grandes rasgos cuando se estabilizaría la inyección de Bitcoins en el mercado (González Otero, 2013).

En la Figura 4.4 se puede observar la evolución del stock de BTCs en el mercado, y lo anteriormente expuesto acerca de su comportamiento asintótico con máximo en los 21 millones de Bitcoins.

Figura 4.4. Evolución del stock de BTCs en el mercado.
Fuente: www.WebRankia.com



Por otro lado, como consecuencia de que la dificultad se va incrementando, llega un momento en la historia del Bitcoin en que comienza a salir muy costosa la minería, con lo que para combatir este inconveniente los usuarios, de manera de tener unas posibilidades razonables de ganancia de dinero, se unen en los denominados “*pools* de minería” agrupándose y sumando mayor nivel de procesamiento que individualmente, por lo que cada vez que el “*pool*” obtenga un lote repartirá el beneficio proporcionalmente al poder de procesamiento que suministre cada uno. En la Figura 4.5 se observa que el sistema del Bitcoin emplea un mecanismo de recompensas decrecientes para los mineros. Inicialmente la recompensa por bloque era de 50 BTCs, luego pasó a 25 BTCs, actualmente es de 12,5 BTCs y el monto se va reduciendo un 50% cada cuatro años o cada 210.000 bloques.

Es así como, por medio de la minería se retribuye a los agentes que hacen posible que el sistema funcione, y con ello dándose la inyección de moneda al mercado, hasta alcanzar los 21 millones de unidades.

Figura 4.5. Recompensas por minería (Número de BTCs por bloque).

Fuente: Elaboración propia en base a www.bitcoin.org.es

<i>Período</i>	<i>Años</i>	<i>Recompensa por bloque</i>
1	2009 - 2012	50 BTCs
2	2013 - 2016	25 BTCs
3	2017 - 2020	12,5 BTCs
4	2021 - 2024	6,25 BTCs
5	2025 - 2028	3,125 BTCs

Como se mencionó anteriormente, la dificultad para conseguir un Bitcoin con el tiempo se va acrecentando y el aporte por parte de los mineros tendrá que ser proporcionalmente mayor. Es fácil caer en la consideración de que estos mineros al prestar sus procesadores no incurren en costos para la obtención de los Bitcoins. El uso del procesador del dispositivo con la consecuente reducción de la vida útil y el costo de electricidad en la que se incurre son costos muy importantes. Esto implica que los mineros solo aportarán su colaboración si el valor del Bitcoin es superior a los gastos en los que tienen que incurrir. En el largo plazo esto irá desplazando a los particulares en favor de las empresas o “*pools*” que lo realicen a gran escala debido al decreciente margen obtenido con el tiempo.

El hecho de que la oferta de Bitcoins esté determinada de antemano implica que, en teoría, la emisión de dinero no puede ser alterada por ninguna autoridad central que desee "imprimir" dinero extra. De acuerdo con los adeptos a Bitcoin, se supone que el sistema debe evitar la inflación, así

como los ciclos económicos que se originan en torno a la emisión de dinero. Sin embargo, este sistema ha sido acusado de conducir a una espiral deflacionista. Si se espera que el suministro total de Bitcoins crezca hasta alcanzar un límite finito de 21 millones, y si el número de usuarios de Bitcoin comienza a crecer exponencialmente por cualquier motivo, y suponiendo que la velocidad del dinero no crece de manera proporcional, se puede esperar una apreciación a largo plazo de la moneda. Las personas tendrían un gran incentivo para atesorar esos Bitcoins y retrasar su consumo, lo que agravaría la espiral deflacionista.

Hasta qué punto esto podría ser un problema en la realidad no está claro. Dos comentarios deben hacerse. En primer lugar, como destacó *The Economist* (2011), la hipótesis de la deflación implica una suposición que no es realista en esta etapa, es decir, que mucha más gente querrá recibir Bitcoins a cambio de bienes o a cambio de papel moneda. Sin embargo, Bitcoin todavía es un instrumento bastante prematuro como medio de cambio generalizado, lo cual es un claro desincentivo para su uso. En segundo lugar, Bitcoin no es la moneda de un país o área monetaria y, por lo tanto, no está directamente vinculada a los bienes y servicios producidos en una economía específica, sino a los bienes y servicios proporcionados por los comerciantes que aceptan Bitcoins. Estos comerciantes también pueden aceptar otras monedas y, por lo tanto, el hecho de que la deflación se anticipe podría dar lugar a una situación en la que los comerciantes adapten los precios de sus bienes y servicios en Bitcoins.

4.10. Ventajas y desventajas de Bitcoin

4.10.1. Ventajas

Como se ha mencionado previamente, Bitcoin tiene ciertas ventajas frente a los otros medios de cambio. Entre las destacadas se encuentran la falta de un ente regulador que controle esa criptomoneda, los menores costos de transacción y la privacidad que confiere a aquellos que la utilizan para realizar transacciones. A continuación se destacan las principales virtudes de Bitcoin.

a) Se utiliza en todo el mundo: Bitcoin no es exclusivo de algún país en particular. No existen fronteras para el intercambio de BTCs. Además, no existen días inhábiles u horarios de cierre para hacer operaciones. Las transacciones se pueden recibir en cualquier momento y en cualquier parte del mundo.

b) Arquitectura descentralizada: la información es gestionada por los usuarios y no depende de la confianza y control de una autoridad central. Permite a Bitcoin funcionar como una plataforma de pago abierta e independiente. Además, tiene una estructura democrática, de manera que

siempre que el 51% de la red sea honesta, ningún usuario podrá saltarse las normas establecidas en el protocolo.

Su valor se determina por la oferta y la demanda de Bitcoins. De esta manera, Bitcoin también puede proporcionar asistencia a los habitantes de países que estén sujetos a estrictos controles de capital. No existe en Bitcoin una autoridad central que pueda revertir transacciones o impedir el intercambio de Bitcoin entre países. Por lo tanto, Bitcoin ofrece una vía de escape para quienes deseen una alternativa a la devaluación de la moneda o control del mercado de capitales de sus países. Quienes se encuentren en situaciones de opresión o emergencia también podrían beneficiarse de la privacidad financiera que Bitcoin ofrece.

c) Es difícil de falsificar: ya que está basada en un sofisticado sistema criptográfico. El sistema criptográfico en el que se sustenta es fuerte y su efectividad está probada, si las técnicas se utilizan correctamente el almacenamiento de Bitcoins es seguro. Si bien podría quedar obsoleto en el futuro con el avance de los algoritmos matemáticos. Sin embargo, el protocolo permite su modificación mediante el consenso entre sus usuarios. Siempre y cuando se mantenga actualizado, no debería suponer un problema.

d) Costos transaccionales más bajos: Al no requerir la existencia de intermediarios, las transacciones se realizan directamente entre pares en la red Bitcoin, por lo que son considerablemente menos costosas y más rápidas que en las redes tradicionales de pagos. Debido a los menores costos transaccionales, Bitcoin hace posible los micropagos.

e) Funciona como moneda de intercambio: es decir, se pueden cambiar Bitcoins por cualquier tipo de divisa. En este sentido, Bitcoin podría funcionar además como un sistema de transmisión de dinero a bajo costo. Una gran proporción de las remesas familiares (de individuos residentes en países desarrollados a sus familiares que residen en países en vías de desarrollo) se envían a través de empresas de envío de dinero tradicionales tales como Western Union o MoneyGram, quienes cobran altos aranceles por el servicio y pueden llegar a tardar varios días en entregar los fondos en el destino. Por el contrario, los aranceles en la red de Bitcoin ascienden a menos del 1 por ciento de la transacción. Bitcoin permite realizar remesas de manera instantánea y a bajo costo y la reducción del costo total de las remesas para los consumidores podría ser significativa.

f) Transparencia y privacidad: Como se afirma en el documento en el que se presentó

inicialmente esta moneda, Bitcoin es probablemente el sistema de pagos electrónicos más transparente que existe. Esto es así ya que, como se lleva un registro cronológico de las transacciones (conocido como “cadena de bloques”), cualquiera puede consultar el historial completo de transacciones, y saber de dónde viene o a dónde ha ido cualquier moneda en concreto.

Si bien las claves públicas de todas las transacciones, también conocidas como “direcciones de Bitcoin”, quedan registradas en la cadena de bloques, esas claves públicas no están vinculadas a ninguna identidad. El público puede ver que alguien está enviando una cantidad de BTCs a otra persona, pero sin información que relacione la transacción a ninguna persona en particular.⁵⁴

Es por eso que se suele considerar a Bitcoin como una moneda “pseudonónima”, en donde existe una combinación de transparencia (de las transacciones) y de privacidad (de la identidad) de los usuarios.

Por otro lado, cabe destacar que la identidad de una persona (o al menos algún dato como puede ser la dirección del protocolo de internet) queda generalmente registrada cuando una persona realiza una transacción por Bitcoin en un sitio web o cuando cambia moneda de curso legal por Bitcoins en una casa de cambio de Bitcoin. Para aumentar las probabilidades de permanecer anónimo, uno tendría que usar un software anonimizador como TOR y cuidarse de nunca realizar transacciones con direcciones que puedan ser vinculadas a su identidad.

g) El intercambio se produce entre usuarios vía P2P: las transacciones se transmiten en cuestión de segundos y son verificadas rápidamente. El plazo medio de verificación de las transacciones ronda entre los ocho y los veinte minutos.

h) Estímulo para las innovaciones financieras: Como se mencionó anteriormente, una de las más prometedoras posibilidades que Bitcoin ofrece es como plataforma para la innovación financiera. El protocolo de Bitcoin contiene el modelo digital para el desarrollo de una serie de servicios financieros y legales que los programadores pueden desarrollar con facilidad.

⁵⁴ Nakamoto, S. (2008). *Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario*. Extraído de www.bitcoin.org

4.10.2.Desventajas

A pesar de los muchos beneficios que presenta, Bitcoin también tiene aspectos negativos que sus interesados deben tomar en consideración. Por ejemplo, el valor del BTC ha exhibido una enorme volatilidad a lo largo de su existencia y los nuevos usuarios corren el riesgo de no proteger adecuadamente e incluso perder sus Bitcoins si no toman ciertas precauciones. Además, existen preocupaciones acerca de si la piratería informática puede poner en peligro la economía de Bitcoin. Cabe destacar, además, que muchos de los aspectos negativos potenciales de Bitcoin son los mismos que caracterizan al tradicional efectivo. El efectivo ha sido históricamente el vehículo preferido de los traficantes de drogas y lavadores de dinero, pero los legisladores nunca considerarían seriamente prohibir el efectivo.

a) Bitcoin no tiene su contraparte de riesgo: por ejemplo, el oro sí tiene su contraparte de riesgo, ya que se salvaguarda en una caja de seguridad de un banco.

b) Vulnerabilidad ante los piratas informáticos o *hackers*: Pese a que la moneda virtual en sí misma no puede ser vulnerada, los *hackers* sí han intervenido en las carteras digitales que guardan Bitcoins. El robo de carteras es otro problema de actualidad derivado de su uso. Las características esenciales del Bitcoin hacen que las monedas si se tienen en un monedero privado, se almacenen en nuestro ordenador a través de ficheros .dat, aunque con este fichero se puede hacer, como cualquier otro, una copia de seguridad tanto en otro ordenador como en una “nube”, cualquier usuario con acceso a ese archivo podría hacer transacciones con nuestro dinero. Derivado de lo anterior las medidas de seguridad adquieren una gran importancia, debido a que cada vez que el valor de los Bitcoins sube, también lo hace el número de hackeos, ya que sus robos son más importantes.

Por supuesto, muchos de los riesgos informáticos que enfrenta Bitcoin son similares a los que enfrentan las monedas tradicionales. Los billetes pueden ser destruidos o robados, la información financiera personal puede ser hurtada y utilizada por los delincuentes. Los usuarios de Bitcoin deben preocuparse por aprender acerca de los riesgos y tomar las precauciones necesarias de la misma manera que lo hacen hoy para proteger sus actividades financieras.

c) Las operaciones con Bitcoins pueden ser riesgosas: ya que no existe ninguna garantía por parte de algún país, Banco Central, institución financiera o empresa en particular.

d) Se pueden originar transacciones que provienen de operaciones ilícitas: Otro inconveniente de esta moneda es la mala imagen generada por el uso (gracias a su pseudoanonimato) en actividades ilegales como en el tráfico de drogas, blanqueo de capitales o la ciberdelincuencia.

Las transferencias hoy en día con esta moneda se pueden convertir en difíciles de rastrear y con ello la persona que se encuentra detrás de cada unidad monetaria. Esto es debido al uso de proxies que eliminan o hacen mucho más difícil seguir el rastro dejado por nuestros actos en internet. Junto con estos proxies⁵⁵ y con otras herramientas como la red TOR, se consigue el anonimato en internet, y como consecuencia de la invisibilidad usando esta moneda se generan los diversos problemas.⁵⁶

Gracias a esta “irrastreabilidad” existía hace unos años la web “*Silk Road*”, “La ruta de la seda”, cuyo nombre proviene de la antigua ruta comercial entre Asia y Europa. En esta web, creada en los primeros meses de la moneda, se permitía la compra y venta de productos utilizando Bitcoins. Los productos que eran vendidos en esta comunidad estaban calificados como contrabando en la mayoría de las jurisdicciones mundiales, teniendo la mayor parte de los vendedores su sede en el Reino Unido y los Estados Unidos, y ofrecían productos como Heroína, LSD, Cannabis y otras drogas o incluso armas (como se puede observar en la Figura 4.6, la cual refleja una captura de dicha web).

Para frenar esto, el senado de los EEUU empezó una investigación sobre la página y sus contenidos en Junio de 2011, siendo este proceso muy lento debido a la mencionada privacidad que otorgan las monedas virtuales. El entramado acabó con la actuación del FBI que llevó al administrador de esta web William Ulbricht, a acabar tras las rejas el 2 de Octubre de 2013, y debido a ello la página cerró derivando en una bajada del tipo de cambio de la moneda desde los USD 140 hasta los USD 110, evidenciando que los usos de la divisa y sus repercusiones generan cambios de valor muy importantes.^{57 58}

e) No es aceptada en todos los comercios: En la mayor parte de las transacciones cotidianas de bienes y servicios, los BTCs no son aceptados como medio de pago. Esto significa que, como moneda, Bitcoin tiene aún un largo camino por recorrer.

⁵⁵ Un *proxie* es un programa informático que enmascara la IP usada para la conexión de internet, por lo que al acceder a la web consta como que se ha efectuado la conexión desde otro emplazamiento.

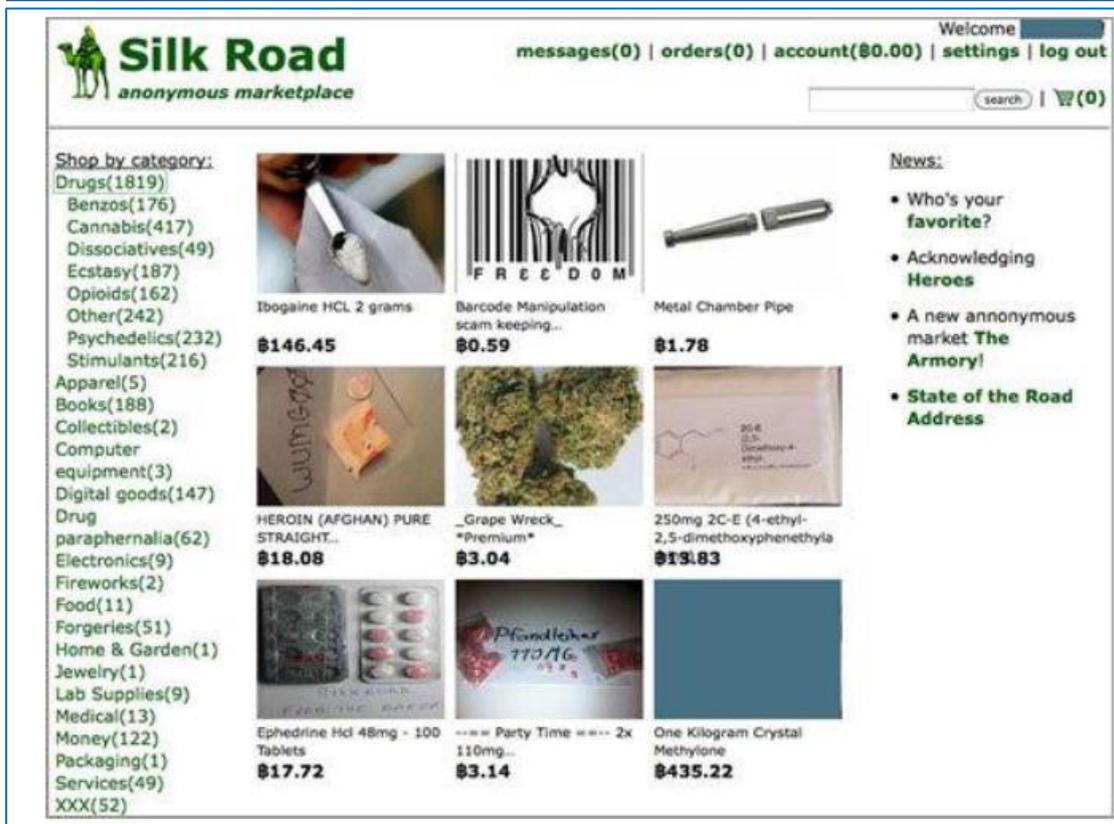
⁵⁶ Una red TOR es una red no indexada por los buscadores como *Google*, en la cual hay que acceder mediante la dirección específica sin poder buscarla por los métodos comunes o rastrearla.

⁵⁷ Análisis paso a paso del fin de la web “*Silk Road*”: <http://www.yorokobu.es/silk-road/>

⁵⁸ Vidal. G. (2014). *Bitcoin: comportamiento como moneda e inversión*. Facultad de Economía v Empresa. Universidade da Coruña.

Figura 4.6. Captura de la web “SilkRoad Marketplace” antes de su cierre.

Fuente: www.ShareLegal.com



f) Alta volatilidad en su valor: El problema principal del Bitcoin para ser tratado como moneda actualmente son sus constantes fluctuaciones de valor con respecto al dólar, cosa común en empresas o activos en procesos de capitalización y en etapas iniciales de vida, pero no en monedas, por lo que no puede atribuirse al mismo la función de reserva de valor como sí se da en el oro, el cual es el activo refugio universal. Al producirse tanta variación en la cotización de esta criptomoneda, los usuarios no tienen ninguna certeza de que en el corto plazo o en un futuro más lejano sus ahorros valgan una cantidad determinada de dólares. Por otro lado, al fluctuar tanto, los empresarios tendrían que estar actualizando los precios de sus productos de manera periódica.

g) Evasión fiscal y blanqueo de capitales: Ya que Bitcoin no está regulado en la mayor parte de los países, se ha dejado fuera de las declaraciones fiscales, lo que propicia la posibilidad de utilizarlo con fines de evasión fiscal. Esto propicia a que, por ejemplo, operando en un país determinado el usuario podría comprar Bitcoins y llevar su dinero conseguido de manera ilegal a otro país, en el que no tuviese que dar ninguna información haciendo perder su rastro del método de obtención o destino. Después de almacenar el dinero en cuentas de otros países, también se

podría aprovechar ciertas “amnistías fiscales” de los gobiernos, para legalizarlo pagando menos impuestos por ellos de los que deberían en un inicio.

h) Consumo de energía: La minería se realiza en base a operaciones computacionales, y para ello los equipos tienen que estar conectados y en funcionamiento, con el consumo de energía que eso representa. Teniendo en cuenta la dificultad creciente que la red introduce en la minería de Bitcoins, y el costo de la energía eléctrica, a la larga podría no resultar rentable dedicarse a la minería, por lo que las tasas aplicadas a las transacciones deberían crecer para mantener la sostenibilidad del sistema. Sin embargo, este mismo hecho podría hacer que los usuarios abandonasen la red por otras con menores costos.

i) Prohibición en muchos países: La mayoría de los países del mundo tienen legislación neutra o abiertamente favorable sobre Bitcoin. La tendencia es positiva, las leyes son cada vez más pro-Bitcoin. Las autoridades financieras de países como Reino Unido, Brasil, Japón y Nueva Zelanda han hecho afirmaciones muy favorables con respecto a Bitcoin y las criptodivisas. Sin embargo, en algunos países como Bangladesh, Ecuador y Bolivia, se prohíben las transacciones de Bitcoin y del resto de monedas virtuales.

CAPÍTULO 5: BITCOIN EN NÚMEROS

En este capítulo se realiza un análisis de los datos relacionados a Bitcoin, tanto en lo que respecta a su registro histórico de cotizaciones desde su surgimiento, como así también la capitalización de mercado, el número de transacciones diarias realizadas, el stock de unidades de esta moneda que actualmente circulan en el mercado, el tiempo medio de espera para la confirmación de una transacción y, finalmente, la cuota de mercado que actualmente conservan los principales pools mineros de la comunidad Bitcoin.

5.1. Cotizaciones

Bitcoin ha tenido un significativo crecimiento durante los últimos años y ha generado muchísima curiosidad e interés por parte de personas de diferentes ámbitos. No obstante, su naturaleza “libre de ataduras” hace que tenga variaciones extremadamente pronunciadas en su cotización. Ya desde sus inicios allá por el año 2009 tuvo siempre como característica principal la inestabilidad en su cotización con respecto al dólar, manteniéndose esto hasta el día de hoy. Las enormes oscilaciones en su valor se producen básicamente por la especulación de la gente y la transmisión de noticias acerca de esta criptomoneda.

Como se puede observar en la figura 5.1, hasta el año 2011 las cotizaciones de Bitcoin fueron insignificantes, siendo el valor de un Bitcoin menor a USD 1. En Febrero de 2011 se alcanza la paridad con el dólar (1 BTC = USD 1) por un corto período de tiempo y luego se mantiene en los niveles de cotización anteriores. Finalmente, se advierte un significativo crecimiento en el precio del BTC en Junio de 2011, conocido como “La Gran Burbuja de 2011”. El valor de Bitcoin alcanza un máximo de USD 35, el 09 de Junio de 2011 y, en los días siguientes, se desploma hasta los USD 10.

Figura 5.1. Cotización de BTC (en USD). Período Mayo 2009 a Enero 2013

Fuente: www.blockchain.info/charts



El aumento pronunciado del precio se relaciona con la exposición pública de Bitcoin en importantes medios de comunicación. Diversos artículos de reconocidos periódicos y revistas como *Forbes*, *The Economist* o *The Financial Times* comienzan a hablar de la criptomoneda. Este hecho atrae a inversores que especulan con el valor de Bitcoin. Como se puede recordar de la historia, ocurren los robos siendo Mt.Gox el principal protagonista, lo que provoca el crash de la “Gran burbuja” y la pérdida de valor de los BTCs. El resto del año se produce un descenso más estable llegando a una cotización de USD 2 y cerrándose con un valor aproximado de USD 4.

Durante el año 2012 se observa un aumento ligero y progresivo de la cotización llegando a un valor aproximado de USD 14 en Diciembre. En este mes se funda “*Bitcoin Central*” que recibe la licencia para operar como un banco, lo que le proporciona de confianza a la moneda. Este suceso se refleja en el próximo mes, momento en el cual la moneda comienza a aumentar más ligeramente que en el año 2012. (Ver Figura 5.1)

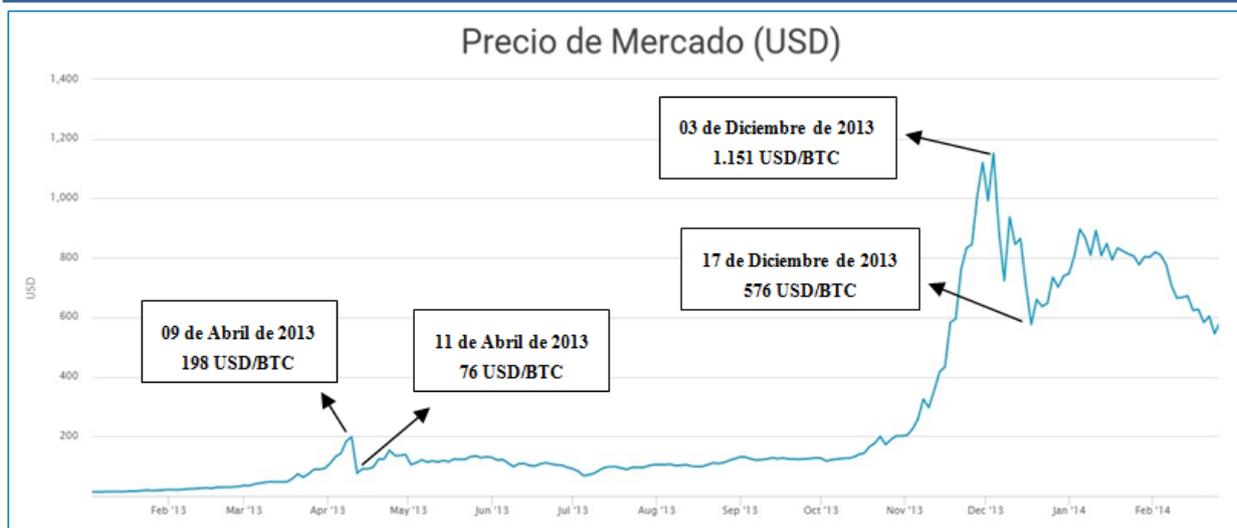
En el año 2013, el valor de Bitcoin empieza a incrementarse con velocidad alcanzando su mayor valor hasta entonces, de USD 198 en el mes de Abril. Se asocia a este crecimiento tres eventos: Primeramente, la regulación de Bitcoin por parte de FinCEN (Red de Control de Delitos Financieros de Estados Unidos) que aporta un marco legal para el funcionamiento de la moneda y, por consiguiente, mayor confianza para los inversores. Y finalmente, la caída económica española y la crisis bancaria de Chipre.

Por un lado, la crisis financiera provoca una caída general de la economía de España durante varios años, lo que supone una mayor desconfianza en el sistema bancario y en los gobiernos. En el mes de Marzo se observa un incremento considerable de las descargas del software de Bitcoin ya que supone una posible alternativa al sistema y el estrés financiero.

Por otro lado, el corralito en Chipre de Marzo 2013, se bloquea la libre disposición de fondos y se cierran las oficinas bancarias para evitar la retirada masiva de dinero ante un gravamen impuesto por la Unión Europea, este gravamen sería parte de un pacto para el rescate del país. Esta situación genera desconfianza de los ciudadanos en el sistema bancario y eleva el interés en Bitcoin.

Figura 5.2. Cotización de BTC (en USD). Período Febrero 2013 a Febrero 2014.

Fuente: www.blockchain.info/charts



Finalmente, dos días después se produce un derrumbe en la cotización del BTC de aproximadamente el 60%. La caída en las cotizaciones llega a los USD 76, tras conocerse noticias acerca de ataques de *hackers* sobre el principal portal de cambio de esta moneda, Mt.Gox. A través de un comunicado, Mt.Gox reconoce que estaba luchando contra un ataque de denegación de servicios, también conocido como ataque DDOS, que consiste en un ataque de bombardeo de datos a la página, que ésta no puede asumir y cae. A su vez, en su comunicado, las autoridades de Mt.Gox pidieron a los poseedores de esta moneda que estén tranquilos y que no traten de vender sus Bitcoins mientras fluctúa la moneda. Tras una serie de rebotes y la desaparición del pánico financiero el precio del BTC se estabiliza aproximadamente alrededor de los USD 100 Y USD 130.

Por otra parte, se produce un evento muy relevante que permite explicar la subida de la cotización ocurrida en Noviembre llegando al máximo valor de Bitcoin en toda su historia.

Baidu⁵⁹ empieza a aceptar Bitcoins, lo que supone un aumento de interés chino en la criptomoneda. El intercambiador “BTC China” releva a Mt.Gox como el mayor intercambiador de Bitcoins en volumen de transacciones.

El interés chino por Bitcoin junto con una audiencia del senado estadounidense sobre las divisas virtuales, potencia la publicidad sobre la moneda lo que supone un aumento de la demanda de Bitcoins y un crecimiento de la cotización acelerado hasta alcanzar el máximo de USD 1.151. El mayor conocimiento del concepto supone el aumento de fondos a *start-ups* y negocios emprendedores relacionados con Bitcoin.

Tras la atención mediática que eleva las cotizaciones hasta máximos históricos se produce el crash. En Diciembre del año 2013, el Banco Central Chino anuncia la prohibición de Bitcoin en transacciones financieras y Baidu deja de aceptar pagos en Bitcoin, lo que provoca el desplome de la cotización en un 50% llegando a los USD 576. La recuperación estabiliza la cotización durante un breve periodo alrededor de los USD 800.

Después de la estabilización en el precio se observan dos caídas más. En Enero de 2014 se produce el arresto de Charlie Shrem, CEO de BitInstant y Vice-presidente de *The Bitcoin Foundation*, bajo la acusación de lavado de dinero (venta de Bitcoins a Silk Road) y operar sin licencia de negocio transmisor de dinero. Charlie Shrem era una de las personalidades más conocidas en la comunidad Bitcoin y uno de sus líderes más destacados. El 28 de Enero de 2014, Charlie Shrem dimite de su puesto como vicepresidente de la Fundación Bitcoin.

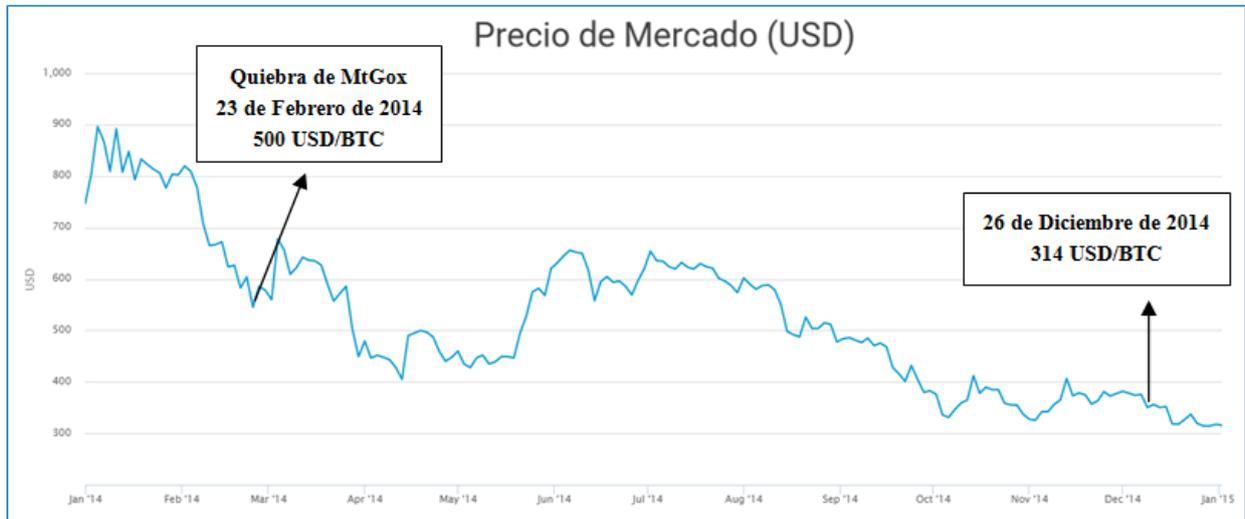
El valor de Bitcoin vuelve a aumentar hasta el mes de Febrero. Durante ese mes varios ataques informáticos a las compañías de intercambio suponen una detención en los retiros de fondos. Estos ataques derivan en el colapso de la mayor plataforma de intercambio de BTCs, Mt.Gox (la cual argumenta el robo de 744.000 BTCs) y su proceso de cierre y bancarrota. Estos eventos originan un derrumbamiento en la cotización de BTC, posicionándose en un valor de USD 500. Finalmente, tras la recuperación de esta caída se produce un incremento del valor de los BTC, siendo su valor aproximado a Junio de 2014 de USD 650.

Durante el resto del año 2014 se pronuncia la tendencia bajista, situándose la cotización en torno a los USD 300 en el mes de Diciembre (Ver Figura 5.3).

⁵⁹ Baidu es el motor de búsqueda más grande de China. El 14 de Octubre de 2013 se convirtió en el primer servicio de este tipo en aceptar Bitcoins.

Figura 5.3. Cotización de BTC (en USD). Período Enero 2014 a Enero 2015.

Fuente: www.blockchain.info/charts



El 13 de Enero del año 2015 se registra el menor valor de Bitcoin (177 USD/BTC) desde Abril de 2013, cuando había caído a los 76 USD/BTC. Durante el resto del año la cotización de la moneda se mantiene irregular en torno a los USD 200 y USD 300. Sin embargo, a partir del mes de Septiembre la cotización comienza una tendencia alcista, logrando un máximo de USD 459 el 17 de Diciembre (Ver Figura 5.4).

Figura 5.4. Cotización de BTC (en USD). Período Enero 2015 a Enero 2016.

Fuente: www.blockchain.info/charts



Durante el año 2016 continúa la escalada ascendente en el precio de Bitcoin, aún sin superar la barrera de los USD 1.000. De esta manera, al 31 de Diciembre de 2016 la moneda virtual estaba

cotizando en torno a los USD 998. (Ver Figura 5.5). Una de las principales noticias de este año es el “*Halving*”, que ocurre en el mes de Julio y eleva los precios de la criptomoneda. El *Halving* es una característica del protocolo Bitcoin, según la cual, cada 210.000 bloques minados se reduce exponencialmente el número de BTCs que obtienen los mineros. Este número era, en el año 2009, de 50 BTCs por bloque, en 2012 bajó a 25 por bloque y el 9 de Julio de este año, cuando se minó el bloque 420.000, se redujo aún más la ganancia: 12,5 por bloque.

Otra noticia que destacar es el ataque ocurrido al *exchange Bitfinex* en el mes de Agosto, cuando fueron robados casi 120.000 BTC.

Dos informaciones de carácter político y económico afectaron el precio de *Bitcoin*. El *Brexit*, o salida del Reino Unido de la Comunidad Económica Europea, y el triunfo de Donald Trump como presidente de Estados Unidos

Figura 5.5. Cotización de BTC (en USD). Período Enero 2016 a Enero 2017.

Fuente: www.blockchain.info/charts



Durante el año 2017 continúa la escalada ascendente en el precio del Bitcoin, comenzando el año en torno a los USD 1.000 (ya el 02 de Enero cotizaba en USD 1.023), pero superando ampliamente ese valor durante el resto del año. Para Mayo de 2017, Bitcoin circundaba los 1.800 Dólares, pero para el mes de Julio rondaba los USD 3.000, desencadenando una escalada en su precio que llegaría hasta el mes de Diciembre. Durante el mes de Septiembre alcanza los 4.000 USD y durante Noviembre la posibilidad de que instituciones como Cboe, CME, LedgerX y el

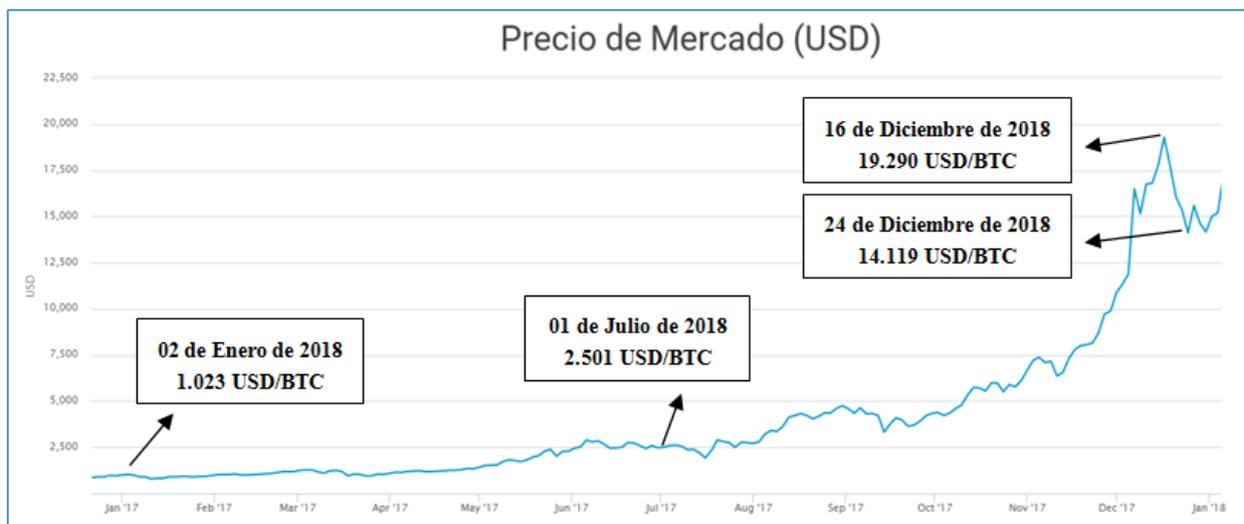
Credit Suisse Bank ofrecieran contratos de futuros basados en Bitcoin, hace que Bitcoin alcance por primera vez los USD 10.000.

Uno de los eventos que marcaron el 2017 más notablemente fue la activación del “Protocolo *SegWit*”. A mediados de Agosto este fue activado en el bloque 481.824 por el equipo de desarrolladores *Bitcoin Core*, con el propósito de permitir aumentar el número de transacciones por bloque a más de 2000 transacciones cada 1 MB, generando una disminución en las comisiones por su procesamiento y mayor velocidad para concretarlas.

En Diciembre fue particularmente especial la escalada de precios, ya que Bitcoin logra duplicar su precio al alcanzar los USD 19.290, su máximo histórico hasta el momento, para luego descender correctivamente hasta entre 12.000 y 15.000 dólares.

Figura 5.6. Cotización de BTC (en USD). Período Enero 2017 a Enero 2018.

Fuente: www.blockchain.info/charts



Durante el año 2018 las cotizaciones fueron un tanto más irregulares, con una tendencia bajista en los primeros meses. Entre los principales motivos de estas caídas en las cotizaciones se encuentran:

- La primera de ellas es la estacionalidad que afecta a las criptomonedas. De la misma manera que hubo una caída en Navidad, ahora la está empezando a haber por la proximidad del año nuevo chino en el que los inversores cambian sus criptomonedas por moneda fiat. Esta festividad tiene lugar el 16 de Febrero; sin embargo, en la preparación es donde la gente empieza a gastar su dinero. Y con la población china

fuertemente invirtiendo en Bitcoin, tiene un enorme papel que desempeñar en el movimiento del mercado.

- Por otro lado, se encuentran las noticias acerca de las intenciones del Gobierno de Corea del Sur de prohibir el comercio de criptomonedas, haciendo que los precios de Bitcoin caigan en picada y provocando que el mercado virtual de monedas se encuentre sumido en un estado de confusión. El ministro de Justicia, Park Sang-ki, afirmó que el gobierno estaba preparando un proyecto de ley para prohibir el comercio de la moneda virtual en los intercambios domésticos. En palabras de Sang-Ki *"Existen grandes preocupaciones con respecto a las monedas virtuales y el Ministerio de Justicia está básicamente preparando un proyecto de ley para prohibir el comercio de criptomonedas a través de intercambios."*

Figura 5.7. Cotización de BTC (en USD). Período Enero 2018 a Febrero 2018.

Fuente: www.blockchain.info/charts



5.2. ¿El precio de Bitcoin ha sido manipulado por Bots?

Neil Gandal, JT Hamrick, Tyler Moore y Tali Oberman, investigadores de la Universidad de Tel Aviv y la Universidad de Tulsa, y autores de "La manipulación del precio en el ecosistema Bitcoin" lograron comprobar que el precio de Bitcoin fue manipulado en más de una ocasión gracias al uso de programas informáticos conocidos como "bots", que efectuaron automáticamente tareas repetitivas de compra y venta de la criptomoneda para modificar su cotización.

El estudio, llamado "Manipulación de precios en el ecosistema Bitcoin", y publicado en la revista *Journal of Monetary Economics*, se centra en analizar el período entre los meses de

Febrero y Noviembre de 2013.⁶⁰ En aquel momento, la criptomoneda, por entonces desconocida para el gran público, empezó a causar interés por su gran incremento en la cotización. Los cuatro autores argumentan que todo fue producto del accionar de dos robots, que provocaron la subida de precio mediante operaciones inventadas, realizadas a través de la plataforma de intercambio de Bitcoins más popular durante esos años, Mt.Gox, hasta su quiebra a comienzos del año 2014.

Esta investigación pudo ser realizada gracias a la filtración de las transacciones en la plataforma Mt.Gox a principios del año 2014. Este volcado de datos de Mt.Gox dio acceso a aproximadamente 18 millones de transacciones de compra y venta coincidentes entre Abril de 2011 y Noviembre de 2013. Estos datos eran mucho más precisos que los que se podrían obtener a través de la consulta en el registro público de la cadena de bloques, ya que en esta filtración se incluían campos tales como ID de transacción, cantidad, tiempo, moneda y códigos de país y estado del usuario. También se incluía la identificación del usuario, que es el número interno asociado con los usuarios de Mt.Gox. La identificación del usuario era crucial, ya que les permitió a los investigadores vincular cada transacción por parte del mismo autor.

A principios de 2014, luego de la filtración de datos de Mt.Gox, varias personas que comerciaban en esta plataforma encontraron lo que se consideraba “actividad comercial sospechosa” y escribieron extensamente al respecto. A partir de esas conjeturas, los autores decidieron realizar su propio análisis de los datos, confirmando las sospechas de manipulación en las cotizaciones.

Los responsables de tales operaciones de manipulación fueron dos *bots*, bautizados bajo los nombres de “Markus” y “Willy”, este último con una actividad mucho más intensa y efectiva. En conjunto, estos comerciantes no autorizados “adquirieron” alrededor de 600.000 BTCs en Noviembre de 2013. Las transacciones efectuadas por estos dos actores produjeron efectos positivos significativos en las cotizaciones de Bitcoin. De hecho, los principales resultados de las investigaciones revelaron que:

- Los precios aumentaron en aproximadamente el 80% de los días en que se produjo la actividad comercial sospechosa. Por el contrario, los precios aumentaron en aproximadamente el 55% de los días en los que no se produjo ninguna actividad comercial sospechosa.

⁶⁰ Gandal, Hamrick, Moore y Oberman. (2018). *Price manipulation in the Bitcoin system*. Recuperado de: <https://www.sciencedirect.com/science/article/pii/S0304393217301666>

- Durante los días en los que los bots estuvieron activos (principalmente Willy), la tasa de cambio USD/BTC aumentó en más de USD 20 por día. Durante el mismo período, la tasa de cambio prácticamente no se modificó en los días en que el actor no estuvo activo.
- La actividad comercial sospechosa de un solo actor (Willy) fue la causa principal del aumento masivo en la cotización del Bitcoin, desde los USD 150 a más de USD 1.000 en solo dos meses a finales del año 2013.
- Luego de la quiebra de Mt.Gox a principios de 2014, Bitcoin tardó más de tres años en igualar el aumento provocado por las transacciones fraudulentas.

En su trabajo investigativo, los autores concluyen afirmando que, dado que el ecosistema de Bitcoin no está regulado actualmente, es esencial que los jugadores y las organizaciones clave se controlen a sí mismos. Además, aseveran que es posible que los reguladores deseen comenzar a asumir una función de supervisión activa a medida que el ecosistema de Bitcoin se integra más en las finanzas y los sistemas de pago internacionales.

5.3. Capitalización de mercado

Al igual que lo que ocurrió con la evolución de la cotización en USD del Bitcoin, y como resultado de ésta, se ha evidenciado un exponencial crecimiento en la capitalización total de mercado de esta criptomoneda. Como se muestra en la Figura 5.8, la capitalización total de Bitcoin ha pasado desde USD 1.508.165 (01 de Enero de 2011) a los USD 16.604.032.594, el 02 de Enero de 2017.

Figura 5.8. Capitalización de mercado de BTC (en USD). Período Enero 2011 a Febrero 2018.

Fuente: www.blockchain.info/charts



Durante el año 2017, en el que el precio del Bitcoin se incrementó desde los USD 1.000 hasta los USD 19.000 en el mes de Diciembre, la capitalización total de mercado de la criptomoneda tuvo un comportamiento similar, marcando su récord histórico y logrando ubicar al valor de capitalización al nivel de varias de las empresas más importantes del mundo.

Figura 5.9. Capitalización de mercado de BTC (en USD). Período Enero 2017 a Febrero 2018.

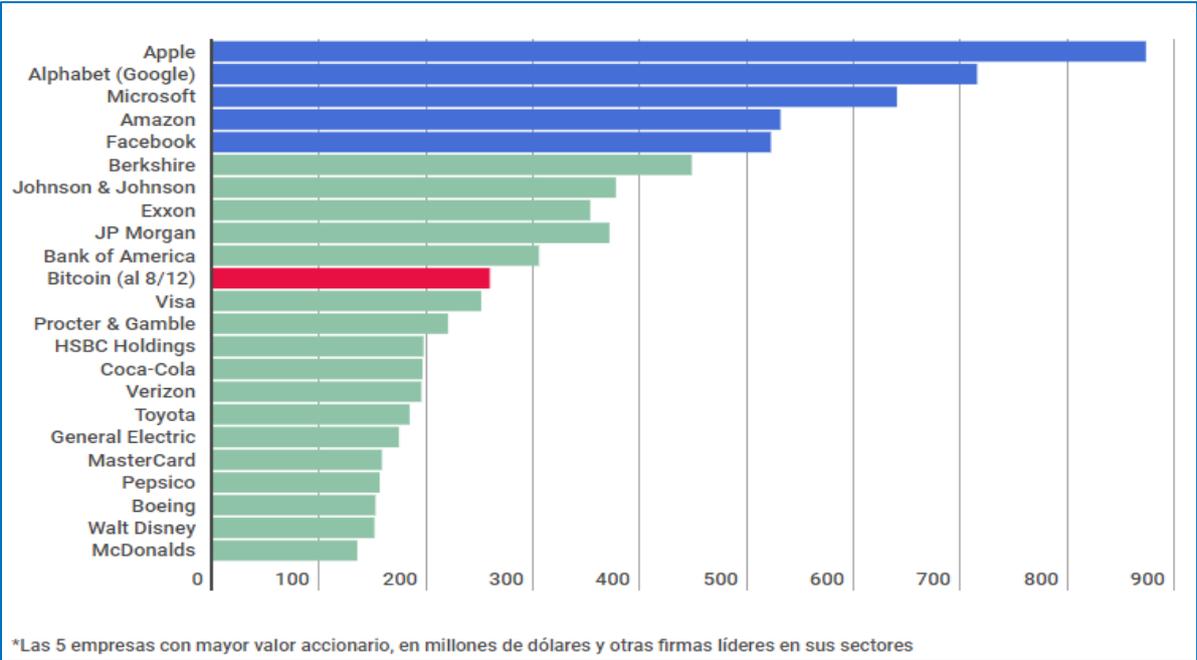
Fuente: www.blockchain.info/charts



De acuerdo al ranking de Global 2000 de la revista *Forbes*, si el Bitcoin fuese una empresa, estaría entre las 20 compañías más grandes del mundo, teniendo en cuenta su valor total de mercado. La criptomoneda se ubicaría por encima de firmas como *Walt Disney*, *Toyota*, *Boeing*, *Mastercard* o *Visa*, y en camino a alcanzar a *Bank of America* o *JP Morgan*, comparando el precio de todos los Bitcoins en circulación y el de todas las acciones públicas de estas compañías.⁶¹

⁶¹ Datos a Diciembre de 2017. Ver Figura 5.10.

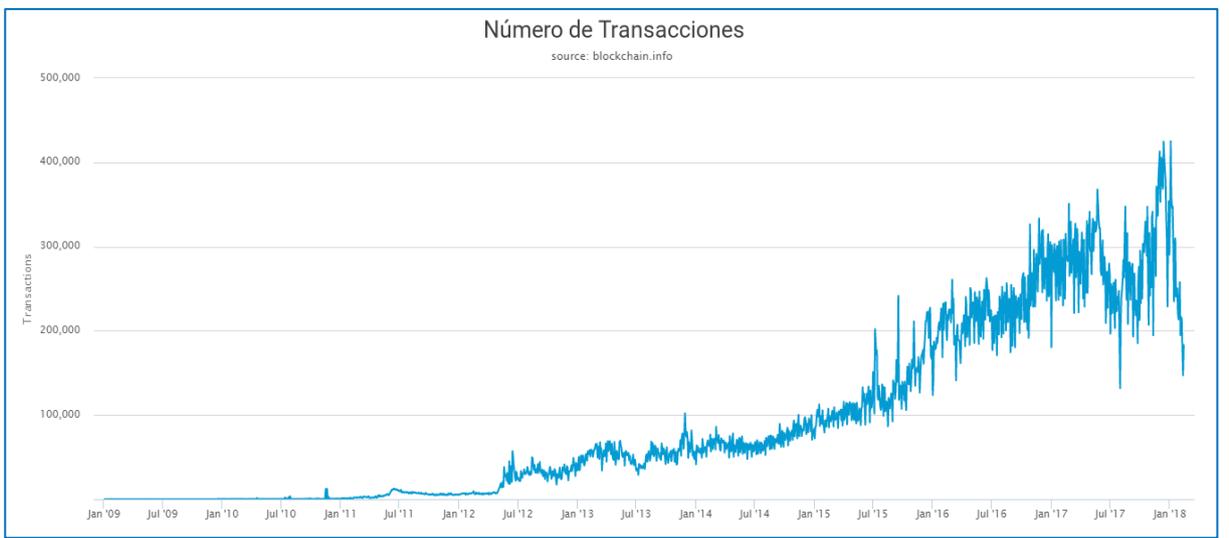
Figura 5.10. Capitalización de Bitcoin / Empresas más valiosas del mundo. Diciembre de 2017
 Fuente: Elaboración de Zegarra, Gonzalo. Recuperado de: <https://infogram.com/8a91ff4a-1d45-46c4-b5d5-6b7cefddddd43>



5.4. Número de transacciones diarias

En cuanto al número de transacciones que se realizan por día, si bien es cierto que se ha observado un gran crecimiento en la aceptación de Bitcoin y se ha incrementado el número de transacciones, de todas formas esta cifra es muy baja comparada con otros medios de pago como las tarjetas de crédito (principalmente VISA y Mastercard) y medios electrónicos como *Paypal*.

Figura 5.11. Número de transacciones diarias de Bitcoin. Enero 2009 a Enero 2018.
 Fuente: www.blockchain.info/charts



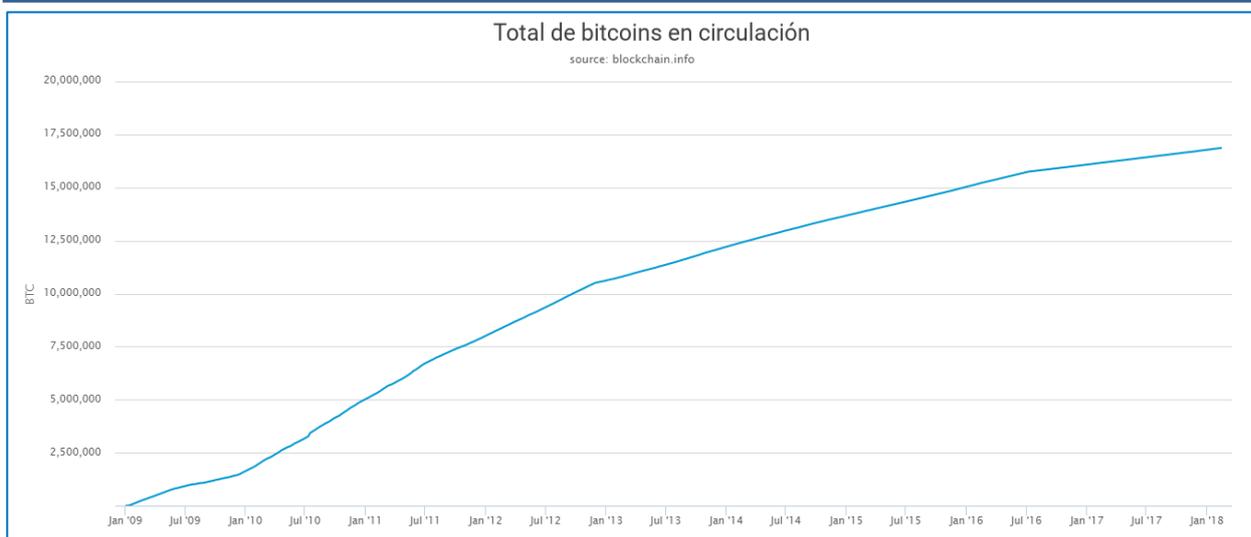
Como se observa en la Figura 5.11, durante el año 2017 el número de transacciones de BTC rondó en torno a las 200.000 y 350.000 transacciones diarias. A inicios del año 2018 se observa una caída importante en las mismas, llegando a las 150.000 transacciones por día.

5.5. Número de Bitcoins en circulación

Como ya se explicó en el apartado 4.9 del capítulo cuatro, “¿Qué es realmente Bitcoin? Un análisis de sus propiedades”, el proceso de creación de nuevos Bitcoins está completamente regulado por el protocolo de Bitcoin publicado en 2008, siendo diseñado para que se alcance un stock total de 21 millones de Bitcoins en el mercado en el año 2141, fecha a partir de la cual no se generarán más. Sin embargo, la fecha realmente importante es la de 2033, en la que, según los cálculos, el aporte de Bitcoins por bloque descifrado se vería reducido hasta los 0.78 BTCs con lo que sería a grandes rasgos cuando se estabilizaría la inyección de Bitcoins en el mercado. Actualmente la cantidad de Bitcoins en circulación, es decir, la cantidad de BTCs que se han minado hasta el momento alcanza la cifra de 16.863.313 (12 de Febrero de 2018). En la Figura 5.12 se observa la evolución en el stock total de Bitcoins en el mercado.

Figura 5.12. Total de Bitcoins en circulación. Enero 2009 a Enero 2018.

Fuente: www.blockchain.info/charts



5.6. Tiempo medio de espera para la confirmación de una transacción

Entre las ventajas con las que cuenta esta criptomoneda, se encuentra la inexistencia de agentes intermediarios que tengan la función de verificar y confirmar cada transacción. En este caso, las transacciones se realizan directamente entre los usuarios vía P2P, se transmiten en cuestión de

segundos y a partir de ese momento se verifican rápidamente, gracias a la labor de los mineros. El plazo medio de verificación de las transacciones ronda entre los ocho y los veinticinco minutos.

Figura 5.13. Tiempo medio de confirmación de una transacción.

Fuente: www.blockchain.info/charts



5.7. Cuota de mercado de los principales pools mineros

Como ya se ha explicado anteriormente, los pools mineros de Bitcoin son una manera de juntar recursos entre muchos nodos para compartir su poder de *hashing* (potencia de minado), al tiempo que se dividen las recompensas logradas de acuerdo con la cantidad de acciones que contribuyeron a resolver para cerrar un bloque.

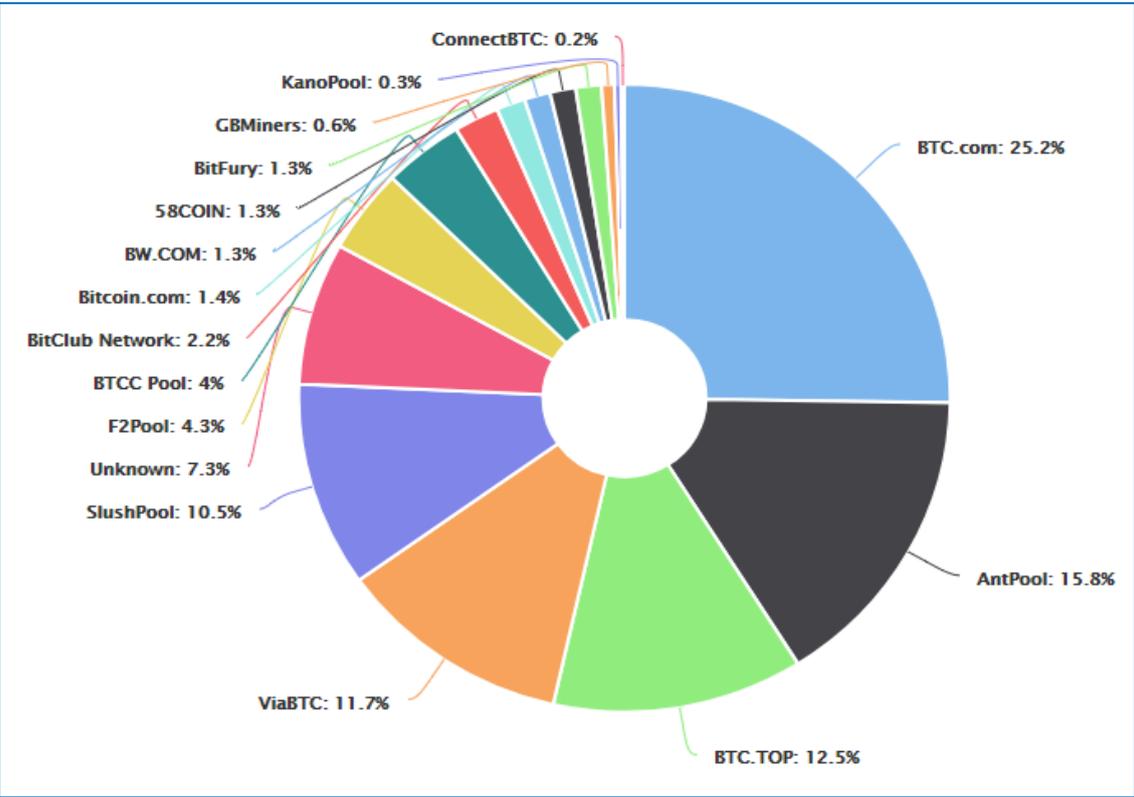
Se otorga una recompensa a los miembros mineros de Bitcoin del mismo pool que contribuyeron a cerrar el bloque y presentar una prueba válida de trabajo que uno de los mineros en el pool resolvió. La minería Bitcoin en los pools comenzó cuando la dificultad para la minería aumentó, hasta el punto en que un solo minero podría tardar años para generar un bloque.

La solución a este problema fue que los mineros pusieran en común sus recursos. Esto hizo que pudieran generar bloques más rápido y, por lo tanto, recibir una porción de la recompensa del bloque de Bitcoin de forma consistente, en lugar de aleatoriamente una vez cada pocos años.

El siguiente gráfico (Figura 5.14) muestra la cuota de mercado de los pools de minería más populares. Se debe considerar únicamente como estimación aproximada ya que por diversas razones no son 100% exactos. Una gran parte de bloques desconocidos no representan necesariamente un ataque sino simplemente que aún no han sido reconocidos.

Figura 5.14. Cuota de mercado de los principales pools mineros.

Fuente: www.blockchain.info/charts



CAPÍTULO 6: ANÁLISIS DE LA VERDADERA NATURALEZA DE BITCOIN

Uno de los objetivos de este trabajo es tratar de determinar si Bitcoin realmente representa una forma de dinero o si, por el contrario, ha de ser considerado como un activo de inversión. Aunque esta discusión puede parecer trivial, ya que no afectaría a su funcionamiento, resulta fundamental. Esta clasificación de Bitcoin como una forma de dinero o no, tiene un enorme impacto en los movimientos que se están produciendo por parte de los países en términos de regulación legal, la aplicación de impuestos, la supervisión de sus movimientos o el carácter que tendría en el patrimonio de una persona. Estos y otros muchos temas que determinarán en gran medida el futuro del Bitcoin están afectados por su identificación como dinero, activo de inversión, esquema Ponzi, entre otras consideraciones.

6.1. Bitcoin como dinero

Como ya se analizó en el segundo capítulo de este trabajo, las propiedades esenciales que debe presentar un bien para utilizarse como dinero son siete: debe ser un bien *escaso*, *duradero*, *homogéneo*, *divisible*, *transportable*, *almacenable* y *difícil de falsificar*. Tomando como base estas propiedades, se realiza un análisis de Bitcoin (Preukschat, 2013).

- **Escasez:** Bitcoin es un activo escaso, siendo el año 2033 cuando virtualmente se llegue a su stock final, basando su crecimiento en la “minería” con conceptos teóricos similares a la minería tradicional, eso quiere decir que este activo obtiene su valor por lo difícil y caro de minar que resulta y en esto se diferencia claramente de las monedas fiduciarias como el Euro o el Dólar, dado que el proceso en el que se incurre al crear estas divisas es muy barato e ilimitado por parte de los gobiernos y Bancos Centrales, los cuales para controlar la masa monetaria y los tipos de interés solamente tienen que decidir hacerlo, cosa que no hace más que aumentar la inestabilidad y disminuir la confianza, y que por otro lado es una herramienta óptima de combate para el control de los ciclos económicos y las turbulencias que estos provocan.

- **Durabilidad:** El Bitcoin en este sentido también es un activo muy duradero, capaz de ser utilizado como medio de pago sin perder propiedades, si es que se gestiona racionalmente, por ejemplo, haciendo copias de seguridad de nuestra cartera. Con el sistema de claves públicas y privadas el dinero en esta moneda se conserva inalterable con el paso del tiempo.

Como en el anterior punto de la escasez, el dinero fiduciario es diferente en esta cualidad, un billete de cualquier moneda del mundo se deteriora fácilmente con su uso y con el paso de los años, teniendo dichos billetes una vida relativamente corta ya que, sumado a los constantes cambios por el deterioro, existe la posibilidad de crear falsificaciones.

- **Homogeneidad:** Un Bitcoin es igual en cualquier parte del mundo, siendo incluso más homogéneo que el oro, por ejemplo. En este apartado las monedas fiduciarias se asemejan al oro y al Bitcoin; un dólar estadounidense, por ejemplo, es igual y tiene el mismo valor, dejando de lado la serigrafía de cada moneda o billete, en cualquier lugar del mundo.

- **Divisibilidad:** Las monedas fiduciarias son fácilmente divisibles con sus diferentes céntimos, diversas monedas y diferentes billetes de multitud de cantidades. Por otra parte, el Bitcoin se puede fraccionar hasta el octavo decimal y pudiéndose ampliar sin ningún tipo de costo, lo que representa una gran ventaja con respecto a cualquier otro tipo de moneda o medio de cambio.

- **Portabilidad:** El dinero fiduciario es relativamente fácil si se quiere mover de una cuenta a otra un saldo a través de un banco, aunque con ciertos costos de transacción. El Bitcoin es el mejor sistema de los estudiados, sin costos o muy pequeños en todo caso, y pudiéndose llevar a cabo en cualquier parte del mundo con una conexión de internet, con la capacidad de realizar pagos transfronterizos sin pasar por entidades bancarias ni intermediarios, y a cualquier hora del día.

- **Almacenamiento:** Desde este punto de vista, en el Bitcoin el almacenaje es más sencillo, físicamente no existe, por lo que no hay que guardarlo en algún lugar físico como indica el concepto, en cambio hay que mantener la cartera virtual. Sin embargo, hacerlo con un tercero no es todo lo seguro como cabría de esperar ya que se suelen dar casos de robos de hackers o cierres de plataformas de carteras, como el conocido caso de Mt.Gox.

El dinero fiduciario es almacenable fácilmente, con el problema del valor decreciente con el paso del tiempo por la inflación, y aunque los bancos sufren también intentos de hackeos informáticos o robos son muy seguros en su gran mayoría, aun pudiéndose dar casos como el “corralito” argentino o el chipriota en el que los reguladores prohibieron las retiradas de depósitos de dinero.

- **Dificultad en la falsificación:** El Bitcoin, debido a la cadena de bloques y control de transacciones, hace que sea virtualmente imposible falsificar o duplicar, ya que hay que contar con la mayoría de los usuarios de la red para certificar una transferencia. El dinero *fiat* es en esta

categoría el elemento menos fiable, está siendo falsificado continuamente por grupos de todo el mundo.

Es decir, se puede manifestar que cualquier tipo de instrumento utilizado para el intercambio tiene debilidades y fortalezas. La facilidad de movimiento, almacenamiento y dificultades en su falsificación puede poner un paso por delante al Bitcoin teóricamente, aunque más allá de este básico análisis la criptomoneda evidentemente es todavía un experimento con un futuro variable e incierto que se encuentra en sus primeros años de vida y es muy joven.

Funciones del dinero

En este apartado se analiza si Bitcoin cumple con las funciones económicas clásicas asociadas al dinero y, por tanto, puede ser considerado como tal. Para ello, se estudiará el comportamiento de Bitcoin como medio de intercambio, unidad de cuenta y depósito de valor.

En una economía de mercado desarrollada, se le atribuye al dinero tres funciones esenciales:

- **Medio de cambio:** El dinero debe poder utilizarse para intercambiar bienes y servicios con otras personas.
- **Depósito de valor:** El dinero tiene que ser capaz de transportar el poder adquisitivo del presente al futuro.
- **Unidad de medida:** Los bienes y servicios tienen que poder ser medidos en términos de unidades monetarias.

Las principales críticas sostienen que Bitcoin no cumple ninguna o alguna de estas tres condiciones que son necesarias para ser considerado dinero y por lo tanto debería considerarse como otro tipo de activo. A continuación se realiza una comparación del Bitcoin respecto a estas tres funciones fundamentales del dinero con el propósito de determinar su naturaleza.

Medio de cambio

Para que un medio de intercambio sea aceptado ampliamente, debe conservar su poder adquisitivo y debe evitar una gran volatilidad (cambios bruscos en su valor). Bitcoin presenta grandes variaciones en su cotización, lo que limita su utilización como medio de intercambio. Si existe incertidumbre constante acerca del valor que tendrá en el futuro, una persona no puede hacer previsiones respecto al costo de los productos que necesita.

No obstante, dado que Bitcoin es un concepto relativamente nuevo y experimental, es razonable que presente gran volatilidad en sus inicios y pueda tender a estabilizarse en los próximos años. Sin embargo, la oferta limitada de Bitcoins hace que el valor dependa de la demanda del mercado, cuanta más demanda, más valor y viceversa. Con lo que, al carecer de una autoridad que regule el

precio y dejarlo a las fuerzas del mercado, los Bitcoins son proclives a la volatilidad.

Además de este problema de volatilidad, Bitcoin presenta otra desventaja como medio de intercambio. Como cualquier moneda, los Bitcoins tienen valor siempre y cuando se acepte como medio de intercambio válido entre dos individuos. En este contexto, la aceptación de Bitcoins para realizar compras de bienes y servicios actualmente no es elevada, siendo la mayoría de las transacciones entre inversores con objetivos especulativos. Por consiguiente, si la mayoría de los comercios no acepta BTC, la oferta de productos a la que se puede acceder es limitada. En el futuro podría incrementarse la aceptación de Bitcoins con una regulación y conocimiento del protocolo. Sin embargo, el uso de Bitcoins requiere ciertos conocimientos informáticos o la confianza en un tercer agente que gestione la seguridad del monedero, lo que limita la amplitud de su uso (Sánchez de Diego Martínez Cabrera, 2014).

Por último, hay que tener en cuenta el poder de los gobiernos en la utilización del dinero. No pueden modificar el protocolo o afectarlo sin el 51% de la capacidad computacional de la red, pero pueden vetar su utilización en las instituciones dependientes del estado y, sobre todo, nunca podría ser una alternativa factible al sistema monetario, si el gobierno no acepta los Bitcoins para el pago de impuestos.

Depósito de valor

Con respecto a la capacidad para funcionar como depósito de valor es donde el Bitcoin recibe el mayor número de críticas y donde más dudosa se puede ver su condición como dinero.

La principal causa de estos defectos como depósito de valor es la volatilidad en su precio. La visión que se tiene del Bitcoin como inversión es el equivalente a la de una *Startup*. Se invierte en los inicios con un gran riesgo a cambio de una posibilidad de triunfo y crecimiento exponencial. El riesgo es que el valor del Bitcoin caiga a cero o sufra una gran caída. Hay ciertos escenarios bajo los cuales esto podría suceder y por lo tanto acabar con el Bitcoin también como moneda. Estos podrían ser un fallo en la seguridad del sistema, una pérdida de confianza por ataques de hackers que produzcan una migración masiva de usuarios y, entre otras, que surja otra moneda o cambio en las existentes que desbanque totalmente cualquier incorporación de nuevos usuarios en la red.

Si se comparan las características como depósito de valor del Bitcoin frente a otros activos se encuentra la siguiente situación:

Figura 6.1. Comparación entre instrumentos bancarios vs. Efectivo vs. Bitcoin.

Fuente: elaboración propia.

Instrumentos bancarios	<ul style="list-style-type: none"> • Pago de intereses • Riesgo de contrapartida • Riesgo impositivo • Riesgo político (devaluaciones monetarias)
Efectivo	<ul style="list-style-type: none"> • Coste de oportunidad de intereses no recibidos • Anónima • Riesgo de robo • Difícil de trasladar en grandes cantidades • Riesgo político (devaluaciones monetarias)
Bitcoin	<ul style="list-style-type: none"> • Sin intereses • Pseudo-anónima • Riesgo de pérdida o robo • Transporte y almacenamiento fácil y poco costoso • Alta volatilidad de precio • Sin reconocimiento legal como moneda en curso

Las principales ventajas del Bitcoin son la ausencia de costos de almacenamiento y la protección frente a devaluaciones monetarias impuestas por los bancos centrales. Como principales críticas y desventajas se puede observar la gran volatilidad en su cotización, el riesgo de no recuperación en caso de pérdida y por último su carencia de carácter de moneda de curso legal. Esta ausencia de legalidad y reconocimiento gubernamental genera su inutilidad para pagar por la mayoría de los bienes y servicios cotidianos, y crea incertidumbre sobre los riesgos impositivos y legales que recaen sobre la misma.

Unidad de cuenta

El Bitcoin tiene un gran potencial en términos de unidad de cuenta de los distintos bienes y servicios debido a su gran divisibilidad. Pero en la realidad la gran volatilidad del mismo no permite que los precios de una gran mayoría de los artículos se fijen basándose en el Bitcoin. Para un negocio marcar sus productos en unidades de Bitcoin supone un gran riesgo de cambio de moneda, de la misma forma que las empresas que operan en distintas monedas. La diferencia es que el riesgo en el caso del Bitcoin es exponencialmente mayor debido a su gran volatilidad.

Si la economía se guiara tomando como referencia al Bitcoin, debido a su volatilidad, los precios

de los bienes y servicios tendrían que ajustarse continuamente. Por otra parte, esto podría ser costoso para los comercios y confuso para los consumidores. Además, si se analiza la situación actual, podemos observar que el valor de un BTC es muy elevado, lo que haría que productos de bajo costo presentaran números difíciles de evaluar y comparar. Por ejemplo, una tira de pan podría costar 0.00047 BTC y un paquete de chicles 0.0000103 BTC. Claramente estos números ofrecen una dificultad de cálculo adicional a la hora de comparar alternativas y no suponen un punto de referencia para un consumidor medio (Sánchez de Diego Martínez Cabrera, 2014).

Conclusión

Habiendo analizado de qué manera Bitcoin se adapta tanto a las propiedades que debe cumplir para utilizarse como dinero, como también así a las funciones que debería desempeñar eficientemente, se concluye que Bitcoin, en este momento, no puede ser considerado como una moneda completamente funcional en todos los aspectos y no es una alternativa realista al sistema monetario, debido a los grandes inconvenientes que alberga. Si en el futuro se estabiliza su valor, podría estudiarse su factibilidad económica en concepto de moneda.

La gran volatilidad en su valor le impide una funcionalidad completa y afecta a las demás funciones que debería cumplir, lo que motiva a utilizarlo como un activo de inversión en lugar de una nueva forma de dinero para realizar transacciones. La falta de respaldo por parte de terceras partes de confianza y seguros de valor también minan su capacidad para representar un verdadero depósito de valor seguro. Además, el mismo hecho de que no sea una divisa reconocida legalmente implica un riesgo.

Si el Bitcoin no llega a ser reconocido como una moneda de curso legal las presiones impositivas que se ejercerán sobre el mismo serán las equivalentes a las acciones u otros activos financieros. Este hecho sería una barrera a sus aspiraciones de convertirse en una moneda como se explicará en un apartado posterior.

Esta valoración de la situación actual no es una negación de su potencial como moneda. El futuro del Bitcoin como moneda depende de las presiones de la sociedad, la concepción, aceptación y regulación del mismo. Sin embargo, actualmente no podría considerarse como dinero y se asemeja más a un activo de inversión. En el siguiente apartado se razona acerca de este asunto.

6.2. Bitcoin como activo

Ante la gran volatilidad mostrada en la cotización del Bitcoin desde su surgimiento, y tras lo visto

en la sección anterior respecto a sus propiedades necesarias para ser considerada una moneda, aparece ahora un nuevo interrogante, ¿Es posible que, en lugar de un medio de cambio utilizado extensamente, Bitcoin pueda convertirse en un activo de cara a invertir en él?, ¿es seguro o puede tratarse de una burbuja especulativa como la de las *puntocom*?

Para analizar a Bitcoin como activo primero se consideran las principales características que ha de tener toda inversión en general. Estas características son principalmente la rentabilidad, el riesgo, la liquidez, y la fiscalidad del activo en cuestión. Estos aspectos también pueden ser importantes a la hora de generar los incentivos necesarios para una demanda de Bitcoins dirigida a contribuir a una diversificación óptima de carteras de inversión.

Los datos de la evolución en la cotización del BTC, expuestos en el capítulo 5 “Bitcoin en números – Cotizaciones” evidenciaron la enorme e incomparable tasa de rentabilidad que se pudo obtener si hubiésemos comprado esta moneda en sus momentos iniciales, e incluso años después. Sin embargo, esas tasas de rentabilidad no son ni cercanas a las de los demás activos de inversión, aunque toda rentabilidad se debe comparar con su riesgo y volatilidad para poder obtener unos datos más objetivos y con una visión más global. Del mismo modo la maduración o plazo de recuperación de la inversión está siendo muy bajo si se considera la revalorización de su precio como beneficio al no tener dividendos que mirar.

Asociado a esa rentabilidad tan grande hay que realizar un estudio del riesgo. En este caso el riesgo es igualmente muy grande ya que existe una probabilidad de pérdida de la cantidad invertida muy alta, debido a las grandes variaciones que tiene el activo en su cotización, siendo éste un aspecto negativo para incentivar la demanda; en los gráficos del capítulo anterior se dejó en evidencia que, aunque existen períodos de intenso crecimiento sostenido en el precio del BTC, también existen períodos de fuerte caídas. Ante tal incertidumbre sobre el valor futuro, resulta muy difícil depositar la confianza en el Bitcoin como activo de inversión para inversores con cierta aversión al riesgo. [*“Why go through the laborious process of buying Bitcoins in order to buy goods and maintain liquid asset balances in Bitcoins that might lose 99 percent of their value overnight?”*] (Grinberg, 2011, pág. 31).

Por otra parte, se debe tener en cuenta que todavía el mercado de Bitcoins es un mercado aún muy poco líquido, con una base de seguridad alta se tarda mucho en liquidar la inversión, por lo que resulta un aspecto negativo a tener en cuenta.

En definitiva, los datos de la evolución de la cotización de Bitcoin demuestran que se trata de **activo de un muy alto riesgo**, con lo que la demanda como activo estaría sólo indicada, en todo caso, hacia inversores muy agresivos y sin aversión al riesgo.

6.3. ¿Bitcoin es una burbuja?

En los últimos años ha aparecido una serie de expertos y especialistas en finanzas que afirman que Bitcoin en realidad no es dinero, sino un activo alrededor del cual se ha formado una enorme burbuja especulativa. Algunos personajes que se han pronunciado en este sentido fueron Alan Greenspan⁶², Warren Buffet⁶³, Xavier Sala-i-Martín⁶⁴, Nouriel Roubini⁶⁵, Kenneth Rogoff⁶⁶ y los premios Nobel Jean Tirole⁶⁷, Joseph Stiglitz⁶⁸, Paul Krugman⁶⁹ y Robert Shiller⁷⁰,

En primer lugar, se definirá a una burbuja especulativa como un incremento desproporcionado en el precio corriente de un activo, sobrepasando sustancialmente el valor teórico del mismo o su “fundamental económico”. Por lo tanto, este fenómeno se produce cuando existe la creencia colectiva de que el precio del activo siempre subirá y se podrá vender mucho más caro de lo que se ha comprado, esto atrae aún más compradores, genera un aumento en la demanda y produce una espiral alcista en su cotización. Lo anterior permite la obtención de grandes beneficios a través de la especulación, esto lleva a realizar acciones mucho más temerarias (como el endeudamiento excesivo) por el clima de euforia que se respira gracias a la burbuja.

Las burbujas suelen formarse en torno a activos con una tipología concreta, con un almacenamiento fácil y poco costoso (algo que se da en el caso de Bitcoin), una velocidad de producción que haga frente al fuerte incremento de la demanda, cierta escasez inicial y sin aparentes bienes sustitutivos. Básicamente se tiende a mantener un apalancamiento excesivo para realizar acciones de inversión en la compraventa o para aumentar la producción. Este pensamiento se extiende cada vez más, atrayendo a más inversores hasta que llega un punto en que los precios alcanzan valores máximos. Conforme las cotizaciones van aumentando, los compradores

⁶² Kearns, J. (4 de Diciembre de 2013). “Greenspan Says Bitcoin a Bubble Without Intrinsic Currency Value”, en Bloomberg. Recuperado de: <http://www.bloomberg.com/news/2013-12-04/greenspan-says-bitcoin-a-bubble-without-intrinsic-currencyvalue.html>

⁶³ Crippen, A. (14 de Marzo de 2014). “Buffett blasts Bitcoin as ‘mirage’: ‘Stay away!’”, en CNBC. Recuperado de: <http://www.cnbc.com/id/101494937>

⁶⁴ Sala-i-Martín, X. (13 de Abril de 2013). “La burbuja del Bitcoin”. Recuperado de: <http://www.salaimartin.com/randomthoughts/item/589-la-burbuja-del-bitcoin.html>

⁶⁵ Roubini, N. (26 de Enero de 2018). “Las promesas rotas de Blockchain”, en Project Syndicate. Recuperado de: <https://www.project-syndicate.org/commentary/why-bitcoin-is-a-bubble-by-nouriel-roubini-2018-01/spanish>

⁶⁶ Rogoff, K. (9 de Octubre de 2017). “¿Oro falso encriptado?”, en Project Syndicate. Recuperado de: <https://www.project-syndicate.org/commentary/bitcoin-long-term-price-collapse-by-kenneth-rogoff-2017-10/spanish?barrier=accessreg>

⁶⁷ Tirole, J. (30 de Noviembre de 2017). “There are many reasons to be cautious about Bitcoin”, en Financial Times. Recuperado de: <https://www.ft.com/content/1c034898-d50f-11e7-a303-9060cb1e5f44>

⁶⁸ Stiglitz, J. (1 de Diciembre de 2017). “Por qué el premio nobel de Economía Joseph Stiglitz cree que se deberían prohibir los Bitcoins”, en BBC Mundo. Recuperado de: <http://www.bbc.com/mundo/noticias-42196322>

⁶⁹ Krugman, P. (31 de Enero de 2018). “Los fraudes y problemas que habrá cuando estalle la burbuja de Bitcoin”, en The New York Times. Recuperado de: <https://www.nytimes.com/es/2018/01/31/burbuja-bitcoin-inversion-criptomonedas/>

⁷⁰ Weisenthal, J. (24 de Enero de 2014). Robert Shiller: “El Bitcoin es un ejemplo asombroso de una burbuja, de eso no hay duda”, en El economista. Recuperado de: <http://www.economista.es/mercados-cotizaciones/noticias/5485736/01/14/Robert-Shiller-El-bitcoin-es-un-ejemplo-asombroso-de-una-burbuja.html>

disminuyen, lo que acaba por una desaceleración del mismo. A partir de ahí, empieza una etapa crítica donde los inversores toman conciencia y el mercado se vuelve muy sensible a cualquier noticia negativa. Los especuladores se retiran del mercado, venden todos sus activos y se produce un cambio de expectativas provocando una caída en la demanda que hunde los precios.

La cotización de Bitcoin podría asemejarse a la de otras conocidas burbujas, como la “Tulipmanía” del siglo XVII, la “South Sea Bubble” del siglo XVIII (Burbuja de la Compañía del Mar del Sur) o la burbuja de las “punto com” a finales de la década de 1990 (Ver Figuras 6.2 y 6.3). A continuación se analiza esta cuestión.

Figura 6.2. Tulipmanía y Burbuja de la Compañía del Mar del Sur.

Fuente: www.BigTrends.com

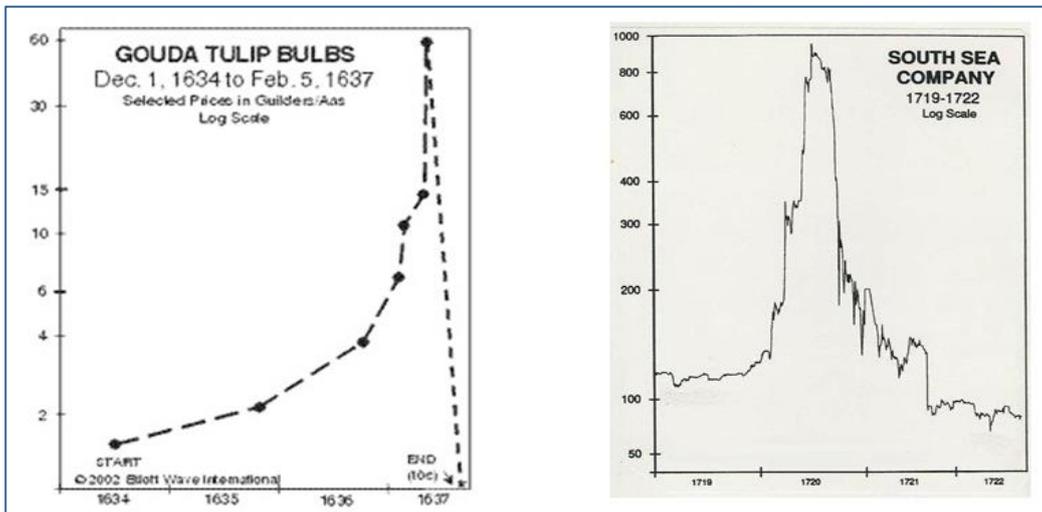
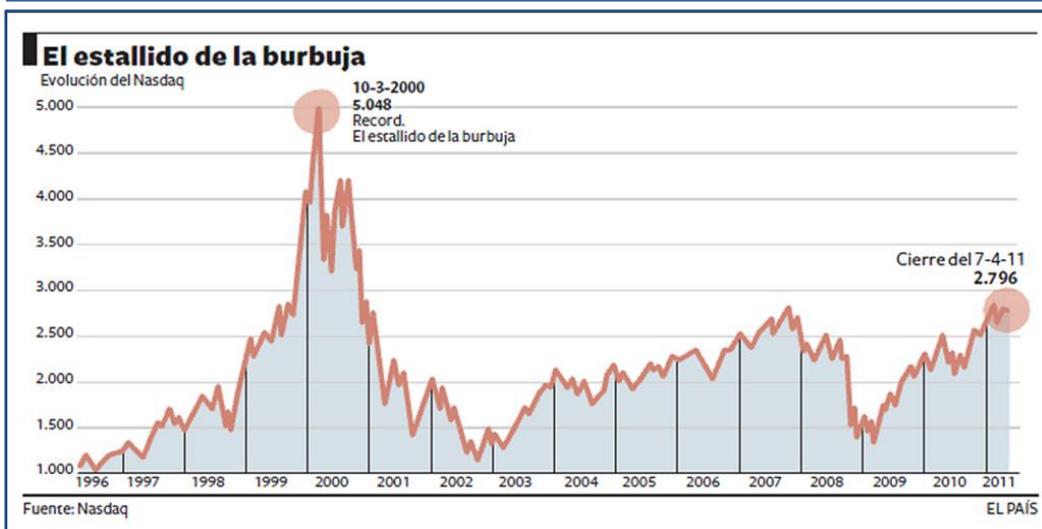


Figura 6.3. Estallido de la burbuja de las “punto com”.

Fuente: www.ElPaís.com



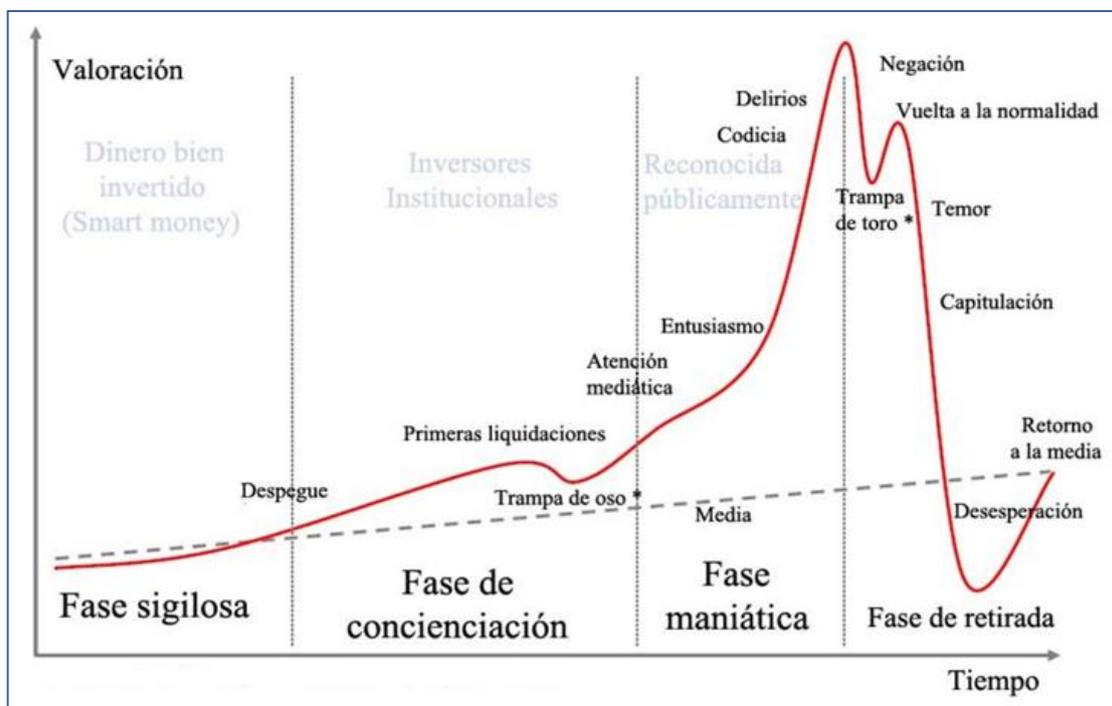
Existen ciertos aspectos de la burbuja de las empresas “*punto com*” que se pueden aplicar al comportamiento de los Bitcoin. Por un lado, los indicios de que el precio está movido por ansias especulativas son considerables, ya que no existe ningún activo que por naturaleza pueda variar tanto de precio (en el capítulo 5 se observó que durante el año 2017 el precio de un BTC se incrementó un más de 1.800%).

Otro aspecto a considerar en la similitud son las expectativas que crearon en sus inicios; tanto las “*puntocom*” como el Bitcoin prometen un gran cambio económico y social que puede modificar completamente los escenarios económicos precedentes: medios de pagos y poder de los Estados, medios de información, lobbies, gobiernos, entre otras cuestiones.

La mejor forma de analizar el comportamiento de lo que se cree que constituye una burbuja es mediante el gráfico elaborado por Jean-Paul Rodrigue de la Universidad de Hofstra, el cual ilustra el comportamiento y las emociones de los participantes en el mercado durante los ciclos de auge y caída (Figura 6.4).

Figura 6.4. Etapas de una burbuja de acuerdo a Jean Paul Rodrigue.

Fuente: Dr. Jean Paul Rodrigue, Dept. Of Economics & Geography, Hofstra University.



En este modelo se pueden apreciar las cuatro etapas que se dan en toda burbuja. La primera, “la fase invisible”, donde el valor del activo es muy pequeño y su popularidad poco extendida entre la comunidad. Un buen proyecto con ideas revolucionarias que poco a poco va llegando a un público más general.

Más adelante después del “despegue” se va tomando conciencia del producto y lo que puede llegar a ser, atrayendo a inversores institucionales que confían en el activo y su desenvolvimiento futuro. En esta etapa, ya cuando el valor sube por la entrada de inversores, se da la primera liquidación donde muchos que invirtieron en la primera fase al ver cómo el valor sube venden para obtener ganancias sencillas, pero el activo sigue fuerte y cada vez más mediático.

En la tercera etapa, donde se gesta principalmente la burbuja, es donde el activo y su incremento de valor llega a oídos menos especializados y a pequeños inversores, que verán la oportunidad de lucrar en el corto tiempo debido a su espiral alcista en su valor y a la avaricia de los agentes. Se acoge con gran entusiasmo esta subida, teniendo gran repercusión en medios como la prensa y el precio sigue incrementándose.

El cuarto período es donde la burbuja pincha, en principio moderadamente debido a la negación de dicho pinchazo donde parece que se da una vuelta a la normalidad, para luego más tarde precipitar el precio del activo.⁷¹

Figura 6.5. Evolución en la cotización de BTC. Julio 2011 a Enero 2018

Fuente: www.blockchain.info/charts



En la gráfica anterior (Figura 6.5) se observa cómo las etapas dispuestas por el profesor Rodrigue se podrían aplicar al caso de la cotización del Bitcoin. Las cuatro fases descritas se encadenan hasta el día de hoy, en donde el precio está sufriendo muchas variaciones en su cotización, pero se observa una recuperación a partir de la caída sufrida durante los primeros días del mes de Febrero de 2018.

⁷¹ Vasile, D. y Ciprian, T. (2012). “*Speculative Bubbles – A behavioral approach*”. Estudio para la Universidad de Bucarest. Rumania.

Sin embargo, a diferencia de las burbujas mencionadas anteriormente, como la TulipManía y la burbuja “dotcom”, que crecieron hasta pincharse, Bitcoin es sorprendentemente resistente. De hecho, hubo varias instancias que podrían catalogarse como burbujas –durante el año 2011 pasó de USD 0,8 a USD 35 y luego a USD 10, en Marzo y Abril de 2013 pasó de USD 35 a USD 266, y luego a USD 50, y en Octubre y Noviembre de 2013 pasó de USD 130 a más de USD 1.000, y luego se redujo a USD 500, finalmente se encuentra el caso del 2017, durante el cual Bitcoin inició con una cotización cercana a los USD 1.000 (Enero), alcanzó su máximo histórico de USD 19.290 y luego cayó a niveles cercanos a los USD 7.000 en el mes de Febrero de 2018– y ninguna ha marcado el fin de Bitcoin. Los defensores de Bitcoin creen que, en el fondo, el pinchamiento de las sucesivas burbujas es positivo para el sistema en su conjunto, porque deja a los ‘verdaderos creyentes’ como participantes y, además, contribuye a solidificar la madurez de la comunidad. En definitiva, a priori, es muy complicado decir a ciencia cierta si se trata de una burbuja o no. Por otra parte, es verdad que Bitcoin tiene unas buenas bases con un sistema muy lógico, basado en la cooperación y el premio a la minería, que sin trabas en su transacción y facilidad de uso pudiera convertirse en la moneda de uso significativo en el futuro, o al menos, un complemento a las convencionales en el ámbito tecnológico como puede ser en las compras por internet y en los sistemas de transferencias de remesas internacionales.

6.4. Bitcoin como esquema Ponzi

Otro problema recurrente es si Bitcoin funciona como un esquema Ponzi o no. Los usuarios ingresan al sistema comprando Bitcoins contra monedas reales, pero solo pueden salir y recuperar sus fondos si otros usuarios desean comprar sus Bitcoins, es decir, si los nuevos participantes desean unirse al sistema. Para muchas personas, esto es característico de un esquema Ponzi. La Comisión de Bolsa y Valores de Estados Unidos (SEC) define a un esquema Ponzi en los siguientes términos: “*un esquema Ponzi es un esquema de inversión fraudulenta que implica el pago de supuestos rendimientos a los inversores existentes de fondos aportados por nuevos inversores*”. Es decir, en estos sistemas, se genera un ciclo en el que se les paga a los inversores viejos con el dinero de los inversores nuevos, y no con las ganancias de algún negocio concreto. Estas estafas siempre sufren un colapso final a expensas de los últimos participantes. El nombre deriva de Carlo Ponzi, un inmigrante italiano a Estados Unidos que, en 1920, cometió un engaño de este tipo que les generó enormes pérdidas a las víctimas.⁷²

Cabe la pena destacar que Bitcoin no parece representar un Esquema Ponzi porque no hay una

⁷² Frankel, T. (2012). “*The Ponzi Scheme Puzzle: A History and Analysis of Con Artists and Victims*”. Oxford University Press. Nueva York.

autoridad centralizada u organizadora que diseña el sistema y que pueda desaparecer con los fondos de los usuarios y, lo más importante, no hay ninguna promesa o garantía de obtener una ganancia.⁷³ Cada persona que compra Bitcoin lo hace a sabiendas de su riesgo, y la volatilidad de la cotización no es precisamente un secreto. Desde luego, esto no impide que ciertos estafadores organicen Esquemas Ponzi utilizando Bitcoin, aprovechándose del deseo de ganar dinero y de la relativa ignorancia de algunos inversores sobre la cuestión de las monedas virtuales.⁷⁴

La diferencia es clara. Entonces, ¿por qué hay quienes dicen que Bitcoin es un Esquema Ponzi? Quizás la confusión tenga que ver con los beneficios de los primeros usuarios de Bitcoin:

- Los primeros mineros se beneficiaron más que los actuales porque, en un principio, cada bloque ofrecía 50 Bitcoins como recompensa, cifra que se va reduciendo a la mitad cada cuatro años.
- Quienes compraron Bitcoins en los primeros años se vieron beneficiados por la enorme suba en el precio del BTC.

Sin embargo, podría argumentarse que, al igual que los primeros inversores en nuevas empresas, se trata de evaluar la relación entre riesgo y rentabilidad. Los primeros mineros y compradores de Bitcoin de algún modo asumieron un gran riesgo al comprometerse en una inversión cargada de incertidumbre. Podría haberles ido muy bien, pero también muy mal.

6.5. Bitcoin como facilitador de actividades ilegales

Por las características particulares de Bitcoin, algunos aseveran que es una herramienta ideal para llevar a cabo todo tipo de actividades ilegales: lavado de dinero, compra y venta de bienes y servicios ilegales (drogas, armas, asesinatos por encargo y pornografía infantil), y financiamiento de actividades ilícitas (terrorismo y trata de personas).⁷⁵

El caso más importante que involucró a Bitcoin con el mundo de la criminalidad fue el de “*Silk Road*”, una página conocida como “el Amazon de las drogas”. Allí se podía comprar y vender todo tipo de sustancias utilizando Bitcoins como medio de pago. La página, que formaba parte de

⁷³ Un reciente estudio de Kaushik Basu, economista del Banco Mundial, afirma que Bitcoin es un Esquema de Ponzi “natural”, lo que significa que, en su visión, es una burbuja de activos. Ver: Basu, Kaushik. “*Ponzis. The Science and Mystique of a Class of Financial Frauds*”. Policy Research Working Paper WPS6967, Banco Mundial, Julio de 2014. Recuperado de: http://www.wds.worldbank.org/external/default/WDSCContentServer/WDSP/IB/2014/07/16/000112742_20140716115536/Rendered/PDF/WPS6967.pdf

⁷⁴ “*SEC Charges Texas Man with Running Bitcoin-Denominated Ponzi Scheme*”, en Securities and Exchange Commission. Acceso online: https://www.sec.gov/News/PressRelease/Detail/PressRelease/1370539730583#.U0mLP_mSzHQ “*Ponzi Schemes Using Virtual Currencies*”. Acceso online: http://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf

⁷⁵ Segal, D. (18 de Enero de 2014). “*Eagle. Scout. Idealist. Drug Trafficker?*”, en The New York Times. Recuperado de: <https://www.nytimes.com/2014/01/19/business/eagle-scout-idealist-drug-trafficker.html>

Christin, N. (2012). “*Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace*”. Recuperado de: <https://www.andrew.cmu.edu/user/.../TR-CMU-CyLab-12-018.pdf>

la “*Deep web*”, fue lanzada en febrero de 2011 y cerrada por el FBI en Octubre de 2013, aunque después hubo un relanzamiento (con otros operadores) y diversos imitadores.

Se estima que, entre Febrero de 2011 y Julio de 2013, *Silk Road* tuvo un total de ventas por 9,5 millones de BTCs, por las que cobró comisiones de 614.000 BTCs.⁷⁶ A partir de la clausura de la página, por un tiempo el gobierno estadounidense se convirtió en uno de los mayores tenedores de Bitcoins. El FBI requisó unos 144.000 BTCs del supuesto líder de *Silk Road*, Ross Ulbricht, y otros 30.000 BTCs de *Silk Road* que fueron subastados a fin de junio de 2014.⁷⁷ El ganador de la subasta, el capitalista de riesgo Tim Draper, afirmó que trabajaría junto a la startup Vaurum para llevar Bitcoin a los países emergentes: “*Esperamos crear nuevos servicios que provean liquidez y confianza a mercados que han sido paralizados por monedas débiles*”.⁷⁸

Tras el cierre de *Silk Road*, muchos se preguntaban si sería el fin de Bitcoin. Lo cierto es que, si bien hubo una reducción en el precio, logró sobrevivir a esta prueba. Según los defensores de la criptomoneda, el episodio fue positivo porque ayudó a sanear su imagen.⁷⁹ En realidad, la expansión y consolidación de Bitcoin, con una estabilización de su valor, y el refinamiento de las técnicas de anonimato, proveería mayor incentivo para usarlo con fines ilícitos, por su facilidad para realizar transacciones internacionales. Sin embargo, por el momento, la moneda más usada para fines ilegales sigue siendo el dólar estadounidense, en efectivo.

Por otra parte, sería miope reducir a Bitcoin a una mera herramienta del crimen. Sin negar que se utilice para realizar actividades ilegales, conviene enmarcar este aspecto en una caracterización más amplia: la de Bitcoin como un sistema alternativo de pagos que permite operar por fuera de los controles de gobiernos e instituciones financieras. La capacidad que tiene Bitcoin de operar por fuera de los canales tradicionales no debe ser subestimada.⁸⁰ Es así que se vuelve deseable por motivos ideológicos, por conveniencia o para eludir normativas perjudiciales.

Hay quienes se ven atraídos hacia Bitcoin por motivos ideológicos. Los usuarios de Bitcoin tienen todo tipo de pensamientos políticos, pero la criptomoneda tiene especial popularidad entre los libertarios. Éstos se entusiasman con el relativo anonimato de las transacciones, la posibilidad de

⁷⁶ “*United States of America v. Ross William Ulbricht*”. Pág. 15. Recuperado de:

<https://www.documentcloud.org/documents/801103-172770276-ulbricht-criminal-complaint.html>

⁷⁷ “*Silkroad Seized Coins*”, en www.blockchain.info. Recuperado de:

<https://blockchain.info/address/1F1tAaz5x1HUXrCNLbtMDqCW6o5GNn4xqX>

⁷⁸ Tim Draper Wins Gov’t Auction, Partners With Vaurum to Provide Bitcoin Liquidity in Emerging Markets”, Comunicado de Vaurum, en *Medium*, 2 de Julio de 2014. Acceso online:

<https://medium.com/@vaurum/timdraper-wins-govt-auction-partners-with-vaurum-to-provide-bitcoin-liquidity-in-emerging-markets-88f04a1d8598>

⁷⁹ Ver, por ejemplo: Eha, B. (5 de Octubre de 2014). “*Could the Silk Road closure be good for Bitcoin?*”, en *The New Yorker*. Acceso online:

<http://www.newyorker.com/online/blogs/currency/2013/10/could-the-silk-roadclosure-be-good-for-bitcoin.html>

⁸⁰ Matonis, J. (20 de Agosto de 2012). “*WikiLeaks Bypasses Financial Blockade With Bitcoin*”, en *Forbes*. Recuperado de: <http://www.forbes.com/sites/jonmatonis/2012/08/20/wikileaks-bypasses-financial-blockade-with-bitcoin>

generar una alternativa a las monedas de curso legal y la posibilidad de quitarles poder a los gobiernos y Bancos Centrales. Como ya se ha analizado, en el plano económico, se basan en las ideas de la Escuela Austríaca.⁸¹

Otro atractivo es que, con Bitcoin, se podría eludir a los gobiernos, esquivando leyes impositivas o normas que regulan el flujo de capitales a través de las fronteras. Evitar los controles de capital es un claro ejemplo.⁸² Es más, dos de los episodios de alza de valor de Bitcoin en 2013 tuvieron que ver con la elusión de ciudadanos de controles de capital: el corralito impuesto en Chipre y el crecimiento de la demanda en China.

La virtud de Bitcoin como circuito alternativo se topa con la pregunta del anonimato. ¿Qué tan anónimo es? Aquí hay que considerar varios factores. El sistema pseudoanónimo (publicidad de las transacciones/ocultamiento de las identidades) hace teóricamente imposible ligar las direcciones con sus dueños, pero existen técnicas que tienen como objetivo rastrear patrones y tendencias en las transacciones.⁸³ Sumado a esto, la propia comunidad Bitcoin puede interesarse en monitorear las transacciones de alguna billetera considerada sospechosa, en una suerte de ‘vigilantismo’ que impone la moral de la propia comunidad.

Pese a esto, las técnicas de protección del anonimato evolucionan día a día, tal como se evidencia con los servicios de ‘lavandería’ que, a cambio de una pequeña comisión, mezclan los Bitcoins provenientes de distintas direcciones para imposibilitar su asociación al verdadero origen. Además, hay algunas criptomonedas que buscan avanzar sobre Bitcoin en temas de privacidad, como *Zerocoin*.⁸⁴

Por eso, los reguladores y agentes judiciales suelen concentrar sus esfuerzos en las fronteras del mundo Bitcoin, aquellos lugares de entrada y salida, donde hay vínculos más sólidos con las identidades reales de los usuarios (por ejemplo, cuentas bancarias).⁸⁵

⁸¹ Ver, por ejemplo: Von Hayek, F. (1976). *Denationalisation of money: the argument refined*. Institute of Economic Affairs. Londres.

⁸² Worstall, T. (21 de Noviembre de 2013). “*Finally, A Proper Use for Bitcoin, Avoiding Capital Controls*”, en Forbes. Recuperado de: <http://www.forbes.com/sites/timworstall/2013/11/21/finally-a-proper-use-for-bitcoinavoiding-capital-controls/>

⁸³ Ver: Reid, F. y Harrigan, M. (2011). “*An Analysis of Anonymity in the Bitcoin System*”. Recuperado de: http://arxiv.org/pdf/1107.4524.pdf?origin=publication_detail

⁸⁴ Zerocoin Project. Acceso online: <http://zerocoin.org/>

⁸⁵ “Bitcoin Virtual Currency: Intelligence Unique Features Present. Distinct Challenges for Deterring Illicit Activity”. Recuperado de: <http://crvptome.org/2012/05/fbi-bitcoin.pdf>

CAPÍTULO 7: ANÁLISIS DE LA REGULACIÓN EMERGENTE DE BITCOIN

Para el futuro cercano y no tan cercano de esta criptomoneda, es muy importante el marco legal que le otorguen los países, ya que esto supondrá un avance o un freno en el desarrollo del Bitcoin. En el siguiente apartado se analizan las diferentes posturas que han adoptado los países del mundo con respecto a esta moneda virtual.

MEDIDAS REGULATORIAS VINCULADAS A BITCOIN

En amplios términos, se pueden considerar dos tipos de regulación, o dos motivaciones de la misma, la primera es la regulación de las actividades ilegales asociadas a Bitcoin y la segunda es la relacionada con el aspecto económico e impositivo.

En primer lugar, se encuentran aquellas regulaciones cuyo propósito radica en la eliminación de las actividades ilegales que han prosperado gracias a la utilización de Bitcoin. En 1999 Milton Friedman ya afirmaba que *“en un futuro cercano se desarrollará la posibilidad de intercambiar fondos por internet. Por supuesto esto tendrá un lado negativo, significará que los mafiosos y personas ligadas a actividades ilegales tendrán un medio rápido de hacer prosperar su negocio”*⁸⁶

El primer acontecimiento que alarmó a las entidades reguladoras de Estados Unidos fue la creación de *Silk Road*, una página web ilegal en la que se podía comprar todo tipo de drogas imaginables. Solo dos semanas después el Senador Chuck Schumer reclamó a las autoridades federales de EE.UU. el cierre de *Silk Road* y de la “moneda *peer to peer* anónima conocida como Bitcoin que alimenta a la página”.⁸⁷

Por otra parte, la división de crimen digital del FBI expresaba en Enero del 2012 que el *“Bitcoin seguirá interesando a criminales con intención de robo de fondos o financiamiento de actividades ilegales... Ya que el Bitcoin no cuenta con una autoridad central, la aplicación de la ley se encuentra con dificultades de detección de actividades ilícitas e identificación de los usuarios.”*. Además, el FBI destacaba que el momento en el que se podría aplicar la regulación es cuando se transforman esos Bitcoins en la moneda de curso legal, todos los sitios que realicen esta actividad tendrían que estar registrados en la Red de Persecución de Crímenes Financieros (FinCEN) e implementar un programa de persecución del lavado de dinero.

⁸⁶ Hanke, S. (2014). *Friedman and hanke on Bitcoin*. Abstract. CATO Institute.

⁸⁷ Greenberg, A. (26 de Febrero de 2014). *Senator Calls for Bitcoin Ban in Letter to Financial Regulators*, en Forbes. Recuperado de: <https://www.forbes.com/sites/andygreenberg/2014/02/26/senator-calls-for-bitcoin-ban-in-letter-to-financialregulators/#742704021140>

Posteriormente, un conjunto de críticas se produjo en el momento del quiebre de Mt.Gox. Ante esta situación se produjo un intento de prohibición total del Bitcoin en Estados Unidos por parte del Senador Joe Manchin. Algunas de las razones eran “*su inestabilidad y disrupción de la economía*” y “*su papel en el desarrollo de actividades ilícitas*”.⁸⁸

Una segunda cuestión radica en la problemática reguladora por los aspectos tributarios y de reconocimiento del patrimonio. Esta discusión se basa en el reconocimiento del Bitcoin como un activo financiero o como una moneda de curso legal. Dependiendo de su identificación estará sujeto a diferentes obligaciones tributarias.

Ante la novedad del fenómeno Bitcoin, los gobiernos y Bancos Centrales alrededor del mundo se vieron obligados a improvisar sobre la marcha. A nivel internacional, los gobiernos no han logrado formular una estrategia común o estándares uniformes para tratar a Bitcoin. Sus reacciones han ido desde una observación despreocupada hasta la prohibición absoluta, pasando por advertencias al público y regulaciones específicas.

Hasta la fecha de elaboración de este trabajo (Febrero de 2018), los países más restrictivos en materia regulatoria han sido Ecuador, Bolivia y China. Países como Rusia e India se han mostrado adversos, finalmente, Japón, Alemania y Canadá han aceptado mayormente el fenómeno.

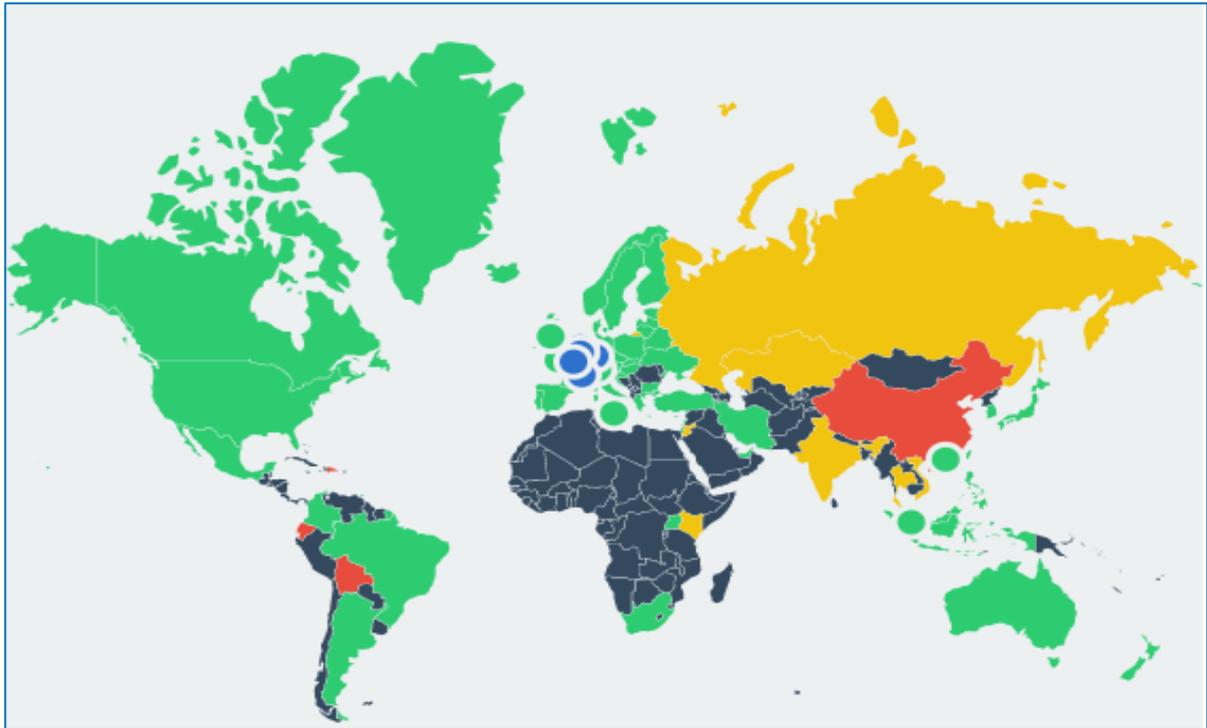
El sitio web *Bitlegal*⁸⁹ se encarga de realizar un seguimiento de las posturas regulatorias de los distintos países y de clasificarlas en “permisivas” (**verde**), “en disputa” (**amarillo**) y “hostiles” (**rojo**). Hasta la fecha, se observa lo siguiente:

⁸⁸ Fung, B. (26 de Febrero de 2014). *Sen. Joe Manchin calls for a Bitcoin ban as regulators seek 'accelerated push'*, en The Washington Post. Recuperado de: https://www.washingtonpost.com/news/the-switch/wp/2014/02/26/sen-joe-manchin-calls-for-a-bitcoin-ban-as-regulators-seek-accelerated-push/?utm_term=.ddc925723345

⁸⁹ BitLegal, Tracking Blockchain Technology and Regulation around the World. Acceso online: <http://bitlegal.io>

Figura 7.1. Actitudes de los diferentes países frente a Bitcoin.

Fuente: www.BitLegal.com



7.1. Actitudes permisivas

Japón

Japón se ha consolidado como el principal motor de la expansión de las criptomonedas. La Agencia de Servicios Financieros de Japón (FSA) se dedicó a trabajar redactando una nueva legislación. El 1 de Abril de 2017 una nueva ley monetaria entró en vigor, en la que se reconoce a las criptomonedas como un método legal de pago. De esta manera Japón se convirtió en el primer país en reconocer las monedas digitales como medio de pago.

Según la regulación aprobada en Abril de 2017, no se podrá comprar ni vender aquellas monedas no registradas ante la FSA. Las normas buscan proteger a los consumidores asegurándose de que las plataformas de intercambio cumplan con los estándares de gestión de riesgo, entreguen información y administren los fondos apropiadamente. Al mismo tiempo, evitan el blanqueo de dinero y el terrorismo, al requerir certificaciones de identidad de los operadores.⁹⁰

La nueva ley define a Bitcoin y a otras monedas virtuales como un método de pagos, no como una moneda propiamente dicha. Bitcoin seguirá siendo tratada como activo. Los Bitcoins son

⁹⁰ Fernandez, M. (01 de Octubre de 2017). *Japón da alas al uso del Bitcoin tras el carpetazo de China*, en El Boletín. Recuperado de: <http://www.elboletin.com/noticia/154021/economia/japon-da-alas-al-uso-del-bitcoin-tras-el-carpetazo-de-china.html>

“utilizables como pago a partes indefinidas por el coste de compra o alquiler de artículos o recepción de servicios y que pueden ser transferidos por medio de sistemas electrónicos de procesamiento de datos “, describe la ley.⁹¹

El país se está preparando también para crear su propia moneda electrónica, el “*JCoin*”, que será convertible en yenes. El proyecto está liderado por dos de los principales bancos del país, el grupo Mizuho y el Japan Post Bank, que ya se han reunido con el regulador financiero japonés para estudiar la viabilidad.⁹²

Se pretende reducir la dependencia con respecto al dinero en efectivo en Japón, donde el 70% de las transacciones se realizan bajo este modo de pago, dejando a la nación en el primer lugar entre los países desarrollados.

Estados Unidos

En el caso estadounidense, cada Estado tiene su propia actitud frente a Bitcoin. A nivel nacional se observa lo siguiente:

El mes de Marzo de 2014 el *Servicio de Rentas Internas Estadounidense (IRS)* se pronunció señalando que la Administración de Estados Unidos tratará al BTC como una propiedad a los efectos fiscales, aplicándole las mismas reglas que emplea para regular las acciones y las operaciones de intercambio. Por otra parte, el gasto o venta de Bitcoins debe considerarse como ganancia de capital, tomando la diferencia entre el valor de mercado de la fecha de adquisición de los Bitcoins y la fecha en que se gastan.⁹³

La Red contra los Delitos Financieros (*Financial Crimes Enforcement Network, FinCEN*) decidió pronunciarse sobre la operatoria con monedas virtuales emitiendo el 18 de Marzo de 2013 la Directriz FIN-2013-G001 sobre la “Aplicación de la normativa de la FinCEN a personas que administren, intercambien o usen monedas virtuales”, y que se encuentra disponible en su sitio oficial.⁹⁴

En esta directriz se define a la moneda virtual como “*un medio de cambio que no es de curso legal en ninguna jurisdicción y que funciona como una moneda en ciertos contextos, pero que carece de la totalidad de los atributos de la moneda real, como para ser consideradas como tal*”. A continuación, se realiza la aclaración de que la actividad de los usuarios de monedas virtuales

⁹¹ Para una revisión de la “Ley de negocios de préstamos de dinero” ver: <http://www.fsa.go.jp/news/28/ginkou/20170324-1.html>

⁹² “Bitcoin: Japón se convierte en el primer país en permitir sus operaciones”, en La República. 30 de Septiembre de 2017. Recuperado de: <http://larepublica.pe/economia/1104616-bitcoin-japon-se-convierte-en-el-primer-pais-en-permitir-sus-operaciones>

⁹³ “Anuncio impositivo de la IRS sobre Bitcoin (explicado)”, en ElBitcoin.org, 26 de marzo de 2014. Recuperado de: <http://elbitcoin.org/anuncio-impositivo-de-la-irs-sobre-bitcoin-explicado/>

⁹⁴ La directriz FIN-2013-G001 se encuentra disponible en www.fincen.gov

(aquellos que obtienen monedas virtuales para comprar bienes o servicios) no se encuentra alcanzada por regulación alguna. Sin embargo, los administradores (aquellos que se dedican a la emisión de una moneda virtual y que gozan de facultades para retirar de circulación una moneda virtual en forma habitual) y los agentes cambiarios (aquellos que se dedican a la intermediación cambiaria de moneda virtual por moneda real, fondos u otra moneda virtual en forma habitual) sí constituyen una Empresa de Servicios Monetarios (MSB, por sus siglas en inglés) conforme a las reglas de la FinCEN, y por lo tanto están sujetos a las normas en materia de inscripción, informes y registro aplicables a las MSB.

Canadá

Este país ha identificado al BTC como “dinero privado”. En el año 2013 se implementó en este país por primera vez en el mundo, la instalación de “cajeros” (o “Robocoins”), estos aparatos permiten cambiar Bitcoins por dólares canadienses en efectivo y viceversa.⁹⁵ Por otra parte, la Agencia del Consumidor Financiero de Canadá (*Financial Consumer Agency of Canada*) en su página web emitió en Abril de 2014 un comunicado aclarando las características y riesgos asociados al BTC a fin de advertir y educar a los consumidores financieros.⁹⁶

Alemania

El gobierno alemán considera que Bitcoin no es una moneda de curso legal ni un tipo de divisa, si no que (según declaró en Junio del año 2013) recibiría un tratamiento similar al de otros activos como el oro y los bonos. Alemania clasificó literalmente a BTC como “unidad de cuenta” en el 2014, similar a las monedas extranjeras, pero sin ser de curso legal.⁹⁷

No obstante, el Bundesbank, en Enero de 2014, advirtió que por su constitución y volatilidad, los Bitcoins son altamente especulativos.⁹⁸ Además, bajo el título “*Bitcoins: Reseña en materia de supervisión y riesgos para los usuarios*”, el BAFIN (Autoridad Federal de Supervisión Financiera en Alemania) decidió pronunciarse sobre la operatoria de Bitcoins, publicando el 19 de Diciembre

⁹⁵ “Canadá tiene el primer cajero de Bitcoins”, en ABC tecnología, 30 de Octubre de 2013. Recuperado de:

<http://www.abc.es/tecnologia/informatica-hardware/20131030/abci-cajero-bitcoin-canada-prox-201310292201.html>

⁹⁶ Para una revisión del comunicado de la *Financial Consumer Agency of Canada* acerca de los Bitcoins ver: <https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html>

⁹⁷ “Alemania reconoce el Bitcoin”, en El País, 20 de Agosto de 2013. Recuperado de:

https://elpais.com/economia/2013/08/20/actualidad/1376988282_349327.html

⁹⁸ “From Bitcoin to digital central bank money: still a long way to go”, en Deutsche Bundesbank. 20 de Septiembre de 2017. Recuperado de:

https://www.bundesbank.de/Redaktion/EN/Reden/2017/2017_09_20_thiele.html

de 2013 un artículo en el que expuso su evaluación sobre esta moneda virtual.⁹⁹

La regla general es que la compra y venta de BTCs por parte de los usuarios no se encuentra sujeta a autorización alguna. En efecto, el simple uso (compra y venta) de Bitcoins como sustituto de la moneda de curso legal para poder participar en el ciclo económico y en el mercado cambiario, no es una actividad que requiera autorización. Sin embargo, operar con Bitcoins con fines comerciales, se encuentra alcanzado por el requisito de autorización previsto en la Ley Bancaria Alemana. Operar sin permiso puede acarrear consecuencias penales, de acuerdo a la ley.

En cuanto a la actividad conocida como “minería de Bitcoin”, la regla general es que no se encuentre alcanzada por el requisito de autorización previa.

En su parte final, el documento termina por aclarar que los bancos y los proveedores de servicios financieros que ya cuentan con una autorización para operar con instrumentos financieros pueden realizar operaciones con Bitcoins.

Francia

El Banco de Francia, mediante un artículo publicado en su sitio oficial¹⁰⁰ el 5 de Diciembre de 2013 titulado “*Riesgos asociados al surgimiento de las monedas virtuales: el ejemplo de los BTC*”, definió al Bitcoin como una moneda virtual no regulada y sin garantía de reembolso, pensada como una alternativa a las monedas oficiales de curso legal.

El documento señala que “*los BTCs pueden clasificarse como un esquema monetario virtual de flujo bidireccional, tal como lo describe el informe del Banco Central Europeo de Octubre de 2012 sobre monedas virtuales*”. En virtud de ello, se concluye que la circulación de los BTCs no violaría el monopolio de los bancos centrales en lo que respecta a la emisión monetaria.

A lo largo del documento se describen a las plataformas de intercambio como las encargadas de convertir las monedas virtuales en moneda de curso legal. Las plataformas de intercambio deben clasificarse como proveedores de servicios que requieren una autorización para funcionar. Para obtener la licencia, las plataformas de intercambio deben cumplir con todas las normas de prevención de lavado de activos y financiamiento del terrorismo. En Francia, en virtud del Artículo L522-6 del Código Monetario y Financiero Francés, la autoridad de supervisión francesa (*Autorité de contrôle prudentiel et de résolution, ACPR*) es la responsable del otorgamiento de

⁹⁹ Ver “Bitcoins: reseña en materia de supervisión y riesgos para los usuarios”, en BAFIN. 19 de Diciembre de 2013

http://www.bafin.de/EN/Homepage/homepage_node.html;jsessionid=FE4E6A4B6237291760BB5BC3677FEA79.1_cid372

¹⁰⁰ “*Riesgos asociados al surgimiento de las monedas virtuales, el ejemplo de los Bitcoin*”. Banco de Francia, 5 de Diciembre de 2013.

Recuperado de:

https://www.banquefrance.fr/fileadmin/user_upload/banque_de_france/publications/Focus10the_dangers_linked_to_the_emergence_of_virtual_currencies_the_example_of_bitcoins-GB.pdf

licencias y de la supervisión de las plataformas.

Por otra parte, el Banco de Francia tiene a su cargo el control de la seguridad operativa de todas las plataformas que cuentan con licencia, a fin de limitar el riesgo de fraude en la compra y venta de Bitcoins.

Brasil

Brasil adoptó una actitud favorable frente a Bitcoin, sin embargo, a fines tributarios se considera a Bitcoin como un activo financiero.¹⁰¹ En Febrero de 2014 el Banco Central de Brasil (BCB) emitió un comunicado en el que advertía al público sobre los riesgos de usar monedas virtuales y lo diferenció del dinero electrónico.¹⁰²

Rusia

El ministro ruso de Finanzas, Anton Siluanov, ha recalcado la necesidad de regular este mercado (el de las criptomonedas). Siluanov ha señalado que *"el Estado ruso entiende que las criptodivisas son reales. No tiene sentido prohibirlas, pero sí hay una necesidad de regularlas"*.¹⁰³

El ministerio de Finanzas ruso trabaja en una ley que situará el marco legal a este mercado de divisas digitales. Se prevé que incluya un procedimiento para la compra de criptodivisas en el que se registra a aquellas personas que quieran comprar este tipo de dinero virtual.¹⁰⁴

Mientras el Estado trabaja en la legislación, el viceministro de Finanzas, Aleksey Moiseev, enfatizó que la compra y venta de Bitcoin y otras criptomonedas serían legalizadas. Esto es todo un cambio de rumbo para el país, ya que el presidente Vladimir Putin prácticamente había condenado a Bitcoin y las criptomonedas en Octubre de 2017.

Por otra parte, el gobierno de Rusia confirmó la creación de su propia criptomoneda, la cual se llamará *"Criptorublo"*, una moneda virtual controlada por el Estado, que no se podrá minar y que podrá cambiarse por rublos para agilizar y simplificar el pago de impuestos.

¹⁰¹ Banco Central Do Brasil, comunicado N° 25.306. 19 de Febrero de 2014. Recuperado de: <https://www3.bcb.gov.br/normativo/detalharNormativo.do?method=detalharNormativo&N=114009277>

¹⁰² Moreno, F. (20 de Febrero de 2014). *"Banco Central de Brasil emite notas sobre problemas del Bitcoin"*, en InfoMoney. Recuperado de: <http://www.infomoney.com.br/mercados/cambio/noticia/3203295/incomodado-com-competicao-banco-central-emite-nota-sobre-problemas-bitcoin>

¹⁰³ Iglesias Fraga, A. (08 de Septiembre de 2017). *"Rusia se plantea regular el Bitcoin y otras criptomonedas"*, en TICBeat. Recuperado de: <http://www.ticbeat.com/innovacion/rusia-se-plantea-regular-el-bitcoin-y-otras-criptomonedas/>

¹⁰⁴ *"Cercos al Bitcoin: Rusia anuncia que regulará el mercado de las divisas digitales"*, en El Economista, 08 de Septiembre de 2017. Recuperado de: <http://www.economistas/divisas/noticias/8596283/09/17/Cercos-al-bitcoin-Rusia-regulara-el-mercado-de-las-divisas-digitales.html>

7.2. Actitudes en disputa y hostiles

Tailandia

En Tailandia se ha prohibido el desarrollo y la comercialización de las monedas virtuales, cuyo exponente resulta ser Bitcoin. Tras la negativa de las autoridades tailandesas a registrar una empresa proveedora de servidores para operar con los mismos, su Banco Central ha sido el primero en pronunciarse negando la calidad de moneda al BTC.¹⁰⁵

Sin embargo, actualmente existen rumores, de acuerdo a diarios locales, de que el Banco de Tailandia ha sido ordenado por el Viceprimer Ministro de Tailandia para mirar más de cerca a Bitcoin y relajar sus estrictas normas que dificultan la innovación *fintech*.¹⁰⁶

China

El Banco Central de China, a principios de Diciembre del 2013, decidió que los Bitcoins no cumplen con los requisitos para ser considerados una moneda de curso legal, y a partir de ello, prohibió a sus entidades financieras hacer operaciones con BTCs a fin de “*proteger los derechos de propiedad y los intereses del público para proteger la situación jurídica del yuan, evitar riesgos de lavado de dinero y mantener la estabilidad financiera*”.¹⁰⁷ Las instituciones financieras y de pagos tienen prohibido usar Bitcoin como unidad de cuenta, operar en Bitcoins, ofrecer cualquier producto (seguros, hipotecas, productos financieros, servicios) en Bitcoins, realizar intercambios con el yuan u otras monedas, etcétera.¹⁰⁸

Este documento numerado bajo la sigla “YIN FA 2013–N° 289”, y que puede encontrarse en el sitio oficial del Banco Popular de China¹⁰⁹, se complementa con un segundo documento en el cual el BPC brinda una serie de respuestas a interrogantes que frecuentemente se plantean con relación a los Bitcoins.

En Marzo de 2014 el *People's Bank of China* envió documentación a las entidades para que cerraran 15 cuentas *online* que negociaban con BTCs, lo que provocó otro fuerte descenso en la cotización y en Abril de ese mismo año, el gobierno chino comenzó a planear la introducción de

¹⁰⁵ “Tailandia, el primer país que prohíbe la moneda virtual Bitcoin”, en BBC, 30 de Julio de 2013. Recuperado de:

http://www.bbc.com/mundo/ultimas_noticias/2013/07/130730_ultnot_bitcoin_tailandia_vp

¹⁰⁶ Cedeño, A. (03 de Julio de 2017). “Banco central de Tailandia encargado de estudiar Bitcoin”, en InfoCoin. Recuperado de:

<http://infocoin.net/2017/07/03/banco-central-de-tailandia-encargado-de-estudiar-bitcoin/>

¹⁰⁷ Situación legal de China, en Bitlegal. Recuperado de: <http://bitlegal.net/nation/CN.php>

¹⁰⁸ “Bitcoin: China prohíbe las colocaciones con criptodivisas”, en CincoDías, 07 de Septiembre de 2017. Recuperado de:

https://cincodias.elpais.com/cincodias/2017/09/04/mercados/1504518523_957352.html

¹⁰⁹ Ver <http://www.pbc.gov.cn:8080/dig/ENDefault.jsp?Q=BITCOIN>

nuevas leyes para penalizar a los bancos que operen con BTCs.¹¹⁰ Además de paralizarse todos los servicios comerciales con criptodivisas para clientes locales, también se ilegalizaron las ICO (Oferta Inicial de Monedas, por sus siglas en inglés), un mecanismo de financiación cada vez más popular que permite a un proyecto crear su propia criptomoneda (los llamados “Tokens”) para recaudar en poco tiempo grandes cantidades de dinero.

Finalmente, la potencia asiática analiza imponer restricciones al consumo energético, lo que cambiaría de manera radical la producción o minado de Bitcoins, con el traslado a otros territorios de los principales pools mineros radicados en China.¹¹¹

Corea del Sur

El ministro de Justicia de Corea del Sur, Park Sang-ki, anunció el 11 de Enero de 2018 en una conferencia de prensa que las divisas virtuales plantean "grandes preocupaciones" para las autoridades y dijo que están preparando *"un proyecto de ley para prohibir el comercio de las criptomonedas a través de intercambios"*.

"Las monedas virtuales son actualmente incapaces de funcionar como un medio de pago y están siendo utilizadas para finalidades ilegales, como el lavado de dinero, estafas y operaciones de inversión fraudulentas", afirmó el director de la Comisión de Servicios Financieros (FSC), Choi Jong-ku.¹¹²

India

Bajo la petición del Banco de la Reserva de la India (RBI), a fines del 2013 el gobierno de India ha ordenado suspender las plataformas de comercio que operaban con BTCa raíz de la advertencia sobre los riesgos que conlleva la moneda virtual acerca de su posible uso para el lavado de activos y la financiación del terrorismo.¹¹³ Así, *BuySellBitCo.in*, la mayor plataforma de comercio de BTCs de la India ha cesado sus operaciones. Actualmente existen rumores de que el RBI está trabajando para crear su propia criptomoneda.¹¹⁴

¹¹⁰ “Bancos chinos cerrarán cuentas en Bitcoins”, en Forbes México, 11 de Abril de 2014. Recuperado de: <https://www.forbes.com.mx/bancos-chinos-cerraran-cuentas-de-bitcoin/>

¹¹¹ “China libra una guerra sin cuartel contra Bitcoin que amenaza con hacerla añicos”, en eldiario.es, 11 de Enero de 2018. Recuperado de: http://www.eldiario.es/hojaderouter/tecnologia/China-guerra-Bitcoin-anicos-cuestion_0_727927522.html

¹¹² “Por qué Corea del Sur quiere prohibir el uso del Bitcoin (y en qué otros 8 países no se puede utilizar)”, en BBC Mundo, 12 de Enero de 2018. Recuperado de: <http://www.bbc.com/mundo/noticias-42648703>

¹¹³ “RBI cautions users of Virtual Currencies against Risks”, Reserve Bank of India, 24 de Diciembre de 2013. Recuperado de: <http://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/IEPR1261VC1213.pdf>

¹¹⁴ Solé, R. (15 de Septiembre de 2017). “India, pese a no estar cómoda con el Bitcoin, estaría trabajando en su propia criptomoneda”, en HardwardEsfera. Recuperado de: <https://hardwaresfera.com/india-pese-no-estar-comoda-bitcoin-estaria-trabajando-criptomoneda/>

Vietnam

El gobierno de Vietnam anunció en Febrero de 2014 que comerciar utilizando Bitcoin y otras criptodivisas similares es ilegal en su país, y ha instado a sus ciudadanos a dejar de hacerlo inmediatamente.

El Banco Central vietnamita indica que las divisas virtuales suelen estar vinculadas a lavado de activos y demás actividades ilegales, probablemente debido al carácter anónimo intrínseco a su funcionamiento. Aunque, por otra parte, tampoco ha indicado posibles sanciones a quienes realicen transacciones utilizando Bitcoin en territorio vietnamita.¹¹⁵

Bolivia

El Banco Central de Bolivia (BCB) emitió el 6 de Mayo de 2014 una resolución que prohíbe expresamente el uso de monedas no emitidas o reguladas por los Estados, entre las que figuran Bitcoin y otras criptomonedas. De esta manera, Bolivia se convirtió en el primer país de América Latina en institucionalizar la ilegalidad de las monedas virtuales. El Artículo 1 del documento resuelve que *“A partir de la fecha queda prohibido el uso de monedas no emitidas o reguladas por Estados, países o zonas económicas, y de órdenes de pago electrónicas en monedas y denominaciones monetarias no autorizadas por el Banco Central de Bolivia en el ámbito del sistema de pagos nacional”*.¹¹⁶¹¹⁷

En el escrito se detallan monedas virtuales como *“Bitcoin, Namecoin, Tonal Bitcoin, IxCoin, Devcoin, Freicoín, 10coin, Liquidcoin, Peercoin, Quark, Primecoin, Feathercoin y otras que no pertenecen a ningún Estado, país o zona económica”*, y que por no estar regulado su uso y emisión, se considera que pueden *“ocasionar pérdidas a sus tenedores”*.¹¹⁸

¹¹⁵ “Vietnam declara ilegales todas las transacciones con Bitcoin”, en Eju!, 28 de Febrero de 2014. Recuperado de: <http://eju.tv/2014/02/vietnam-declara-ilegales-todas-las-transacciones-con-bitcoin/>

¹¹⁶ Marty, B. (19 de Junio de 2014). “Bolivia, el primer país americano en prohibir Bitcoin”, en PanamPost. Recuperado de: <https://es.panampost.com/belen-marty/2014/06/19/bolivia-el-primer-pais-americano-en-prohibir-bitcoin/>

¹¹⁷ Banco Central de Bolivia, nota de prensa 062/2017. “BCB recuerda que está prohibido el uso de monedas virtuales”, 29 de Junio de 2017. Recuperado de: https://www.bcb.gob.bo/webdocs/files_noticias/NP%2062%20Uso%20de%20Monedas%20Virtuales.pdf

¹¹⁸ Gerencia de entidades financieras. Resolución de Directorio N° 044/2014. “Prohibición del uso de monedas y denominaciones monetarias no reguladas en el ámbito del sistema de pagos nacional”, Banco Central de Bolivia. Recuperado de: <http://www.bcb.gob.bo/webdocs/2014/Normativa/Resoluciones/044%202014.PDF>

Ecuador

A través de un comunicado de prensa emitido en Julio de 2014, el Banco Central del Ecuador (BCE), aclaró que el Bitcoin no es un medio de pago autorizado para su uso en el país. Es importante señalar que no está prohibida la compra y venta de criptomonedas, como el Bitcoin, a través de Internet; sin embargo, se recalca que Bitcoin no es una moneda de curso legal y no está autorizada como un medio de pago de bienes y servicios en el Ecuador, conforme lo establece el artículo 94 del Código Orgánico Monetario y Financiero. La entidad llamó a la ciudadanía a estar alerta y a rechazar actividades promovidas por *“organizaciones inescrupulosas que buscan estafar bajo la oferta de altos rendimientos y bonificaciones, producto de sistemas piramidales que utilizan Bitcoins”*.¹¹⁹

Por otra parte, se establecieron las directrices para la creación de una moneda digital estatal, dependiente del Banco Central del Ecuador.¹²⁰

7.3. El Bitcoin en Argentina

Al igual que en todo el mundo, el Bitcoin está teniendo un considerable auge en América Latina, cada vez son más las personas que han escuchado de las monedas virtuales e incluso, países como Ecuador, Venezuela o Argentina están interesados en agregar las divisas virtuales a su marco monetario e institucionalizarlas como parte de su economía.

Argentina no es ajena a Bitcoin, y hasta ahora reuniría a la comunidad más grande de *“bitcoiners”* en Latinoamérica, con alrededor de unos 10.000 usuarios, según datos extraoficiales.¹²¹

De acuerdo a los datos provistos por la ONG Bitcoin Argentina en la actualidad existen unas 15 empresas que operan con Bitcoin en territorio argentino, entre desarrollos locales y compañías del exterior con presencia en el país. La gran mayoría trabaja sobre los usos financieros de la moneda: desde casas de cambio especializadas hasta servicios de billetera digital, préstamos colaborativos en Bitcoins o bien compañías de procesamiento, intermediarios entre una persona que quiere pagar en esta moneda y un comercio que desea cobrar en pesos. También hay espacio para inversores muy arriesgados, con fondos a medida. Una compañía, incluso, vende cajeros automáticos para

¹¹⁹ “Comunicado oficial sobre el uso de Bitcoin”, Banco Central de Ecuador (BCE), 8 de Enero de 2018. Recuperado de: <https://www.bce.fin.ec/index.php/boletines-de-prensa-archivo/item/1028-comunicado-oficial-sobre-el-uso-del-bitcoin>

¹²⁰ “Ecuador prohíbe Bitcoin y aprueba creación de moneda digital estatal dependiente del Banco Central”, en OroYFinanzas, 28 de Julio de 2014. Recuperado de: <https://www.oroymasfinanzas.com/2014/07/ecuador-prohibe-bitcoin-aprueba-creacion-de-moneda-digital-estatal-dependiente-banco-central/>

¹²¹ Fundación Bitcoin Argentina. Acceso online: <http://www.bitcoinargentina.org>

que alguien con Bitcoins pueda salir del paso en moneda local.¹²²

También los Bitcoins demostraron su presencia en el interior del país, cuando un empresario cordobés publicó la venta de sus lotes de 485 metros cuadrados en la localidad de Santa Rosa de Calamuchita, a 93 kilómetros de Córdoba capital. El dato hubiera pasado desapercibido si no fuera por un detalle: la valuación del terreno estaba en Bitcoins.¹²³

Otros dos hechos que demuestran la importancia creciente que están adquiriendo las criptomonedas, y particularmente Bitcoin, en nuestro país son, en primer lugar, la instalación a partir de Octubre de 2017, de 200 cajeros que permiten realizar operaciones tanto con dinero común y físico, como con criptoactivos. Este hecho generó que Argentina se convierta así en una de las primeras naciones del mundo en tener cajeros bidireccionales. El sistema bidireccional se refiere a que estos cajeros pueden dar y recibir billetes de curso legal en Argentina, como también dar y recibir criptoactivos. Entre las criptomonedas que se manejan se encuentran Bitcoin, Ethereum y Litecoin y se añadirán otras criptomonedas según su relevancia.¹²⁴

El segundo hecho significativo relacionado a Bitcoin en Argentina es el lanzamiento en Agosto de 2017 del primer fondo de inversión en Bitcoins en la región. “Crypto Assets Fund” (CAF) nace como el primer fondo de inversión privado exclusivamente enfocado en Bitcoins y criptomonedas de América latina, uno de los primeros del mundo con esas características.

Crypto Assets Fund se constituye como un fondo que invierte USD 50 millones en Bitcoins y otros criptoactivos digitales como Ethereum, Litecoin, Zcash, Ripple y Dash. La cartera está compuesta en un 50% por Bitcoins y en un 50% por otros activos derivados como Ethereum, Litecoin, Zcash, Dash y Ripple, tecnologías similares a los Bitcoins.¹²⁵

7.3.1. ¿Cómo ha sido la recepción de Bitcoin por parte de las autoridades en Argentina?

Hasta el momento, sólo el Banco Central de la República Argentina (BCRA) y Unidad de Información Financiera (UIF) realizaron declaraciones oficiales.

En el año 2014, el Banco Central de la República Argentina (BCRA) emitió un comunicado con el

¹²² Feliba, D. (30 de Noviembre de 2016). “Bitcoins: la moneda virtual crece en la Argentina y apunta a los clientes no bancarizados”, en La Nación. Recuperado de: <http://www.lanacion.com.ar/1960718-bitcoins-la-moneda-virtual-crece-en-la-argentina-y-apunta-a-los-clientes-no-bancarizados>

¹²³ “Los Bitcoins encienden la ilusión también en el interior del país”, en El Cronista, 14 de Marzo de 2014. Recuperado de: <https://www.cronista.com/itbusiness/-Los-bitcoins-encienden-la-ilusion-tambien-en-el-interior-del-pais-20140114-0014.html>

¹²⁴ “En octubre se instalarán 200 cajeros de criptomonedas en Argentina”, en iProfesional, 15 de Septiembre de 2017. Recuperado de: <http://www.iprofesional.com/notas/255910-euro-banco-moneda-mercado-divisas-bitcoin-fintech-transferencias-letes-En-octubre-se-instalaran-200-cajeros-de-criptomonedas-en-Argentina>

¹²⁵ Bustamante, S. (14 de Julio de 2017). “Lanzan en Argentina el primer fondo de inversión en Bitcoins de la región”, en El Cronista. Recuperado de: <https://www.cronista.com/finanzasmercados/Lanzan-en-Argentina-el-primero-fondo-de-inversion-de-Bitcoins-de-la-region-20170714-0060.html>

objetivo de alertar a los usuarios en general sobre los riesgos de operar con monedas virtuales, al afirmar que, al no ser emitidas por el BCRA ni por otras autoridades monetarias internacionales, no tienen curso legal ni poseen respaldo alguno. Mientras tanto, en cuanto al valor que puedan llegar a tener, destacaron que *"no existen mecanismos gubernamentales que garanticen su valor oficial"*. Este comunicado además agrega *"Las llamadas monedas virtuales han revelado una gran volatilidad hasta el momento, experimentado veloces y sustanciales variaciones de precios"*.

En el mismo sentido, el BCRA destacó que, en el ámbito internacional, *"aún no hay consenso sobre la naturaleza de estos activos (las monedas virtuales)"* y remarcó que *"diversas autoridades han advertido acerca de su eventual uso en operaciones de lavado de dinero y diversos tipos de fraude"* y que *"se encuentra actualmente analizando diversos escenarios para verificar que las operaciones con estos activos no se constituyan en un riesgo para aquellos aspectos cuya vigilancia está expresamente establecida en su Carta Orgánica"*. Finalmente, afirmó que *"los riesgos asociados a las operaciones que involucran la compra o uso de monedas virtuales como medio de pago, son soportados exclusivamente por sus usuarios"*.^{126 127}

De acuerdo al artículo 30 de la Carta Orgánica del BCRA:

El Banco es el encargado exclusivo de la emisión de billetes y monedas de la Nación Argentina y ningún otro órgano del gobierno nacional, ni los gobiernos provinciales, ni las municipalidades, bancos u otras autoridades cualesquiera, podrán emitir billetes ni monedas metálicas ni otros instrumentos que fuesen susceptibles de circular como moneda. Se entenderá que son susceptibles de circular como moneda, cualesquiera fueran las condiciones y características de los instrumentos, cuando:

- i) El emisor imponga o induzca en forma directa o indirecta, su aceptación forzosa para la cancelación de cualquier tipo de obligación; o*
- ii) Se emitan por valores nominales inferiores o iguales a 10 veces el valor del billete de moneda nacional de máxima nominación que se encuentre en circulación.*¹²⁸

Por lo tanto, Bitcoin no entra en la definición del BCRA de moneda: no es emitido por una autoridad, su uso y aceptación es puramente opcional (no es forzosa), y no mantiene una relación definida con la moneda nacional.

¹²⁶ *"El Banco Central informó que los Bitcoins no son legales, ni tienen respaldo"*, en iProfesional, 29 de Mayo de 2014. Recuperado de: <http://www.iprofesional.com/notas/187955-banco-central-riesgos-bitcoin-El-Banco-Central-informo-que-los-bitcoins-no-son-legales-ni-tienen-respaldo>

¹²⁷ *"Monedas virtuales. Comunicación al público en general"*. Banco Central de la República Argentina. Recuperado de: www.bcra.gov.ar/bilmon/bm023000.asp

¹²⁸ Carta Orgánica del BCRA, Ley 24.144. Pág. 16. Recuperado de: <http://www.bcra.gov.ar/pdfs/marco/CartaOrganica2012.pdf>

Además, en nuestro país la Unidad de Información Financiera (UIF) dictó una resolución en Julio de 2014 (resolución 300/2014) en la cual advirtió que los ‘sujetos obligados’ por la Ley 25.246 (por ejemplo, entidades financieras, casas de cambio, agentes de bolsa, sociedades que exploten juegos de azar, empresas aseguradoras, corredores inmobiliarios, etc.) a informar sobre posibles operaciones sospechosas de sus clientes *“deberán prestar especial atención al riesgo que implican las operaciones efectuadas con monedas virtuales y establecer un seguimiento reforzado respecto de estas operaciones evaluando que se ajusten al perfil del cliente que las realiza, de conformidad con la política de conocimiento del cliente que hayan implementado”*. Para ello, a partir de Agosto de 2014 deben informar mensualmente sobre todas las operaciones que se realicen con monedas virtuales. De esta manera, las operaciones con Bitcoin recibirían el mismo tratamiento que el resto.¹²⁹

La UIF aclaró que, tal como especifica el Grupo de Acción Financiera Internacional (GAFI) ²⁴, entiende por “monedas virtuales” la *“representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción”*. Reconoció que, en los últimos tiempos, estas monedas han cobrado “relevancia económica” y que *“involucran una serie de riesgos para el sistema de prevención de los delitos de Lavado de Activos y de la Financiación del Terrorismo”*. Señaló como riesgos principales el “anonimato” que *“impide la trazabilidad nominativa de las operaciones”* y la facilidad para el *“movimiento transfronterizo de activos, pudiendo participar de las mismas jurisdicciones que no tienen controles de prevención del lavado de dinero y la financiación del terrorismo”*.¹³⁰

¹²⁹ “Resolución 300/2014. *Monedas Virtuales*. Resolución N° 70/2011. Modificación (Resolución 300/2014)”, Unidad de Información Financiera, 4 de julio de 2014. Recuperado de: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/230000-234999/231930/norma.htm>

¹³⁰ “*Virtual Currencies. Key Definitions and Potential AML/CFT Risks*”, FATF Report, Junio de 2014. Recuperado de: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft risks.pdf>

CONCLUSIONES

El esquema basado en la moneda virtual Bitcoin se ha desarrollado con el objetivo de convertirse en una plataforma de pagos alternativa frente a las monedas nacionales de curso legal, y frente a los sistemas de pago basados en cuentas de depósito con intermediarios financieros. Es una alternativa frente al dinero en efectivo, ya que subsana muchos de los inconvenientes de portabilidad, divisibilidad y transferibilidad de este medio de pago, puede ser operada a un bajo costo de forma electrónica, puede almacenarse de manera ilimitada en cualquier dispositivo electrónico y, una vez creada una billetera virtual, los fondos pueden ser transferidos entre cuentas en cuestión de minutos. No obstante, tiene características que se le asemejan al dinero, ya que puede ser transferida sin la intermediación de un tercero, es pseudoanónima, y no tiene ningún valor intrínseco. Más aun, su carácter global hace que potencialmente compita con todas las monedas nacionales.

Como se ha analizado a lo largo de este trabajo, Bitcoin tiene todos los elementos necesarios para convertirse en una moneda independiente de bancos centrales y entidades reguladoras. Sin embargo, actualmente consta de grandes obstáculos a su funcionalidad como moneda. El principal es la volatilidad en su cotización debido a los movimientos especulativos que ha sufrido a lo largo de su historia. Esa gran variabilidad en su valor le impide una funcionalidad completa y afecta a las demás funciones que debería cumplir para actuar como una alternativa frente al dinero de curso legal, lo que motiva a utilizarlo como un activo de inversión de riesgo, en lugar de una nueva forma de dinero para realizar transacciones.

Muchos de los otros obstáculos que relegan el éxito de Bitcoin como medio de pago alternativo, tienen que ver con la gran cantidad de riesgos asociados a la operatoria con esta criptomoneda. En cuanto a los riesgos operativos de Bitcoin, las tecnologías criptográficas avanzadas para su emisión, validación y registro han mostrado hasta el momento ser bastante robustas. No obstante, la tecnología basada en el protocolo *proof-of-work* es vulnerable a ataques en aquellos casos en los que un pool minero alcance más del 50% de la capacidad de procesamiento de la red. Sin embargo, lo más crítico en materia de riesgos en la historia de Bitcoin ha sido los grandes robos y actos fraudulentos que han ocurrido en varios de los *exchanges* más grandes del mundo.

Por otra parte, los usuarios de esta criptomoneda enfrentan riesgos legales, dado el cambiante marco regulatorio sobre monedas virtuales en numerosos países. Finalmente, las criptomonedas

como Bitcoin se prestan para que agentes oportunistas estafen a los usuarios no especializados con negocios y servicios prometedores, como los esquemas Ponzi y otros tipos de estafas. Incluso, en ausencia de una actividad fraudulenta, las operaciones en las plataformas de intercambio de Bitcoin son irreversibles e irrevocables y los usuarios podrían enfrentarse a la pérdida de recursos debido a errores al realizar una operación.

Con estos inconvenientes relacionados a Bitcoin, lo que se impide es una popularización del mismo entre círculos no formados de la sociedad que no están dispuestos a asumir tales riesgos.

En síntesis, Bitcoin puede ser una alternativa eficaz en nichos tales como los servicios de remesas internacionales y como activo de riesgo con ciertas propiedades de cobertura financiera. No obstante, esta criptomoneda aún presenta muchas limitaciones, debido a la alta volatilidad de su precio como medio de pago, los riesgos asociados con su tenencia frente al crimen cibernético y el fraude financiero, a la opacidad de sus protocolos de emisión y verificación, a los costos transaccionales en el cambio por otros activos y a la inexistencia de un responsable que dé cuenta de cualquier falla o fraude en estos esquemas. En consecuencia, el grado de aceptación y utilización de Bitcoin es aún muy bajo, comparado con los sistemas de pago atados a monedas de curso legal. Todas estas desventajas hacen de Bitcoin un activo cuyos estándares para servir como medio de pago, depósito de valor y unidad de cuenta aún sean muy cuestionables.

A partir de lo anterior, se concluye que Bitcoin, en este momento, no puede ser considerado como una moneda completamente funcional en todos los aspectos y no es una alternativa realista al sistema monetario, debido a los grandes inconvenientes que alberga. Si en el futuro se estabiliza su valor y se limitan todos los riesgos asociados a su operatoria, podría estudiarse su factibilidad económica en concepto de moneda. Esta valoración de la situación actual no es una negación de su potencial como moneda y como esquema alternativo al basado en el dinero fiduciario. El futuro del Bitcoin como moneda depende de las presiones de la sociedad, la concepción, aceptación y regulación del mismo. Sin embargo, actualmente no podría considerárselo como dinero y se asemeja más a un activo de inversión.

En todo caso, más allá del escenario de corto plazo que actualmente se describe, el posicionamiento de Bitcoin en el ámbito comercial y financiero dependerá del grado en que se vaya implementando su uso, el cual a su vez está vinculado a la confianza de los usuarios y el apoyo gubernamental que reciba, por lo que hacer previsiones al respecto a largo plazo es extremadamente complicado.

BIBLIOGRAFÍA

- Abramovich, A. y Vazquez G. (2003). *La experiencia del trueque en Argentina: otro mercado es posible*. Universidad Nacional de General Sarmiento. Buenos Aires.
- Arango-Arango, C y Bernal Ramírez, J. (2017). *Criptomonedas*. Documentos técnicos de trabajo. Banco de la República de Colombia. Colombia.
- Asimov, I. (1989). *Historia y cronología del mundo*. Editorial Ariel. España.
- Banco Central Europeo. (2011). “*La estabilidad de precios, por qué es importante para ti*”. Boletín Mensual, Enero.
- BBVA. (2013). “*Bitcoin, a chapter in Digital Currency Adoption*”. Department of Economic Analysis. Recuperado de: https://www.bbvaesearch.com/KETD/fbin/mult/130731_EconomicWatchEEUU_Bitcoin_tcm348-398292.pdf+&cd=1&hl=es&ct=clnk&gl=ar
- Bodega Barahona, F. (1991). *Notas sobre la antigua historia del oro*. Cuaderno Lab. Xeolóxico de Laxe. Coruña.
- Boudeguer, R. (2015). *El primer Banco Central de la historia y su máquina de imprimir dinero*. Informe mensual de estrategia (Noviembre), Banca March.
- Braudel, F. (1984). *Las estructuras de lo cotidiano*. Ed. Alianza, Madrid.
- Brito, J. y Castillo, A. (2014). *Bitcoin, manual básico (para legisladores y diseñadores de políticas)*. Research Gate. George Mason University.
- Carbonell, S. (2016). *La moneda en el mundo antiguo: Grecia, Roma e Hispania*. Ies Cotes Baixes Alcoi. España.
- Chacón Hidalgo, M. (2006). *Del real al colón: Historia de la moneda en Costa Rica*. BPR Publishers.
- Chaum, D. (1992). “*Achieving Electronic Privacy*,” *Scientific American*, p.96–101.
- Corominas, J. (1987). *Breve diccionario etimológico de la lengua española*. Ed. Gredos. Madrid.
- Díaz Vico, J. y Sanchez Aragón, A. (2014). *Bitcoin, una moneda Criptográfica*. Instituto Nacional de Tecnología de la Comunicación.
- Eagleton, C. y Williams, J. (2009). *Historia del dinero*. Ediciones Paidós Ibérica. Barcelona, España.
- European Central Bank. (2012). *Virtual Currency Schemes*. Eurosystem. Germany.

- Gandal, Hamrick, Moore y Oberman. (2018). *Price manipulation in the Bitcoin system*. Economics of Information Security. WEIS.
- García Soto, R. (1984). *Introducción a la teoría monetaria*. Editorial Universidad Estatal a distancia. San José, Costa Rica.
- Gilmore, J. (1991). “*Privacy, Technology, and the Open Society*”. Recuperado de: <http://www.toad.com/gnu/cfp.talk.txt>
- González Otero, J.M. (2013). *Bitcoin: La moneda del futuro. Qué es, cómo funciona y por qué cambiará el mundo*. Unión Editorial; España.
- Gorjón, S. (2014). *Divisas o Monedas Virtuales: el caso de Bitcoin*. Banco de España. España.
- Gringberg, R. (2011). *Bitcoin: An innovative Alternative Digital Currency*. Estudio para la Universidad de Austin. USA.
- Gutierrez Hernández, P. (2015). *Bitcoin: ¿Presente y futuro del dinero?* Universidad Pontificia Comillas. Madrid, España.
- Hanke, S. (2014). *Friedman and hanke on Bitcoin*. Abstract. CATO Institute.
- Hughes, E. (1993). “*A Cypherpunk’s Manifesto*”. Recuperado de: <http://www.activism.net/cypherpunk/manifesto.html>.
- Huidobro Moya, J. (2015). *Numismática y Heráldica en España*. Ed. Liber Factory. España.
- Informe del Centro del Sector Financiero de PwC e IE Business School, “*Los medios de pago, un paisaje en movimiento*”. Junio de 2015. Madrid.
- Jimenez, F. (2012). *Elementos de teoría y política macroeconómica para una economía abierta*. Fondo Editorial – Pontificia Universidad Católica del Perú. Perú.
- Jevons, W. (1876). *Money and the Mechanism of Exchange*. D. Appleton and Co. New York.
- Mankiw, Gregory. (2007). *Macroeconomía (6ª edición)*. Ed. Antoni Bosch. Barcelona.
- Mantilla, S. (2014). *Bitcoin: La otra cara de la moneda*. Instituto de Estrategia Internacional. CERA. Argentina.
- Mariño, K. (sin fecha). *Redes de comunicación*. Recuperado de: <http://es.calameo.com/read/002743183263406e7733a>
- May, T. (1992). *A Crypto Anarchist Manifesto*. Recuperado de: <http://www.activism.net/cypherpunk/crypto-anarchy.html>

- Mendoza Martinez, D. (2009). *El nacimiento del billete: una revolución en el concepto del dinero*. OMNI N°1.
- Montoya Vasquez, M. (2016). *Inversión en Bitcoins: Modelo para Costa Rica*. Tecnológico de Costa Rica. Costa Rica.
- Morales, A. y Galindo, E. (2009). *Dinero, la autodestrucción del ser humano*. Editorial Académica Española. Edición electrónica gratuita. Texto completo en www.eumed.net/libros/2009a/505
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Recuperado de www.bitcoin.org
- Ortiz Soto, O. (2001). *El dinero. La teoría, la política y las instituciones*. Facultad de Economía UNAM. México.
- Preukschat, A. (2013). *Diferencias y similitudes en las funciones del dinero*. Artículo para el diario digital Oro y Finanzas. España.
- Robbins, L. (1935). *An essay on the nature and significance of economic science*. Ed. Macmillan and Co. Toronto, Canadá.
- Rodriguez, N. y García A. (2017). *Blockchain: mirando más allá de Bitcoin*. Asobancaria.
- Rothbard, M. (1979) *Moneda, libre y controlada*. Edición Fundación Bolsa de Comercio de Buenos Aires. Bs. As.
- Vasile, D. y Ciprian, T. (2012). “*Speculative Bubbles – A behavioral approach*”. Estudio para la Universidad de Bucarest. Rumanía.
- Vidal, G. (2014). *Bitcoin: comportamiento como moneda e inversión*. Facultad de Economía y Empresa. Universidade da Coruña. España.
- Viegas, C. (2014). *Bitcoin: Un desafío para la ejecución de políticas de la Banca Central. Algunas consideraciones jurídicas frente al creciente fenómeno de las llamadas “criptomonedas”*. Banco Central de la República Argentina. Argentina.
- Von Hayek, F. (1976). *Denationalisation of money: the argument refined*. Institute of Economic Affairs. Londres.
- Weatherford, J. (1997). *La historia del dinero, de la piedra arenisca al ciberespacio*. Editorial Andrés Bello. Chile.

Sitios de internet

- “Anuncio impositivo de la IRS sobre Bitcoin (explicado)”, en ElBitcoin.org, 26 de marzo de 2014. Recuperado de: <http://elbitcoin.org/anuncio-impositivo-de-la-irs-sobre-bitcoin-explicado/>
- Banco Central de Bolivia, nota de prensa 062/2017. “BCB recuerda que está prohibido el uso de monedas virtuales”, 29 de Junio de 2017. Recuperado de: https://www.bcb.gob.bo/webdocs/files_noticias/NP%2062%20Uso%20de%20Monedas%20Virtuales.pdf
- Banco Central Do Brasil, comunicado N° 25.306. 19 de Febrero de 2014. Recuperado de: <https://www3.bcb.gov.br/normativo/detalharNormativo.do?method=detalharNormativo&N=114009277>
- “Bancos chinos cerrarán cuentas en Bitcoins”, en Forbes México, 11 de Abril de 2014. Recuperado de: <https://www.forbes.com.mx/bancos-chinos-cerraran-cuentas-de-bitcoin/>
- “Bitcoin: China prohíbe las colocaciones con criptodivisas”, en CincoDías, 07 de Septiembre de 2017. Recuperado de: https://cincodias.elpais.com/cincodias/2017/09/04/mercados/1504518523_957352.html
- “Bitcoin: Japón se convierte en el primer país en permitir sus operaciones”, en La República. 30 de Septiembre de 2017. Recuperado de: <http://larepublica.pe/economia/1104616-bitcoin-japon-se-convierte-en-el-primer-pais-en-permitir-sus-operaciones>
- “Bitcoin Virtual Currency: Intelligence Unique Features Present. Distinct Challenges for Deterring Illicit Activity”. Recuperado de: <http://cryptome.org/2012/05/fbi-bitcoin.pdf>
- “Bitcoins: reseña en materia de supervisión y riesgos para los usuarios”, en BAFIN. 19 de Diciembre de 2013. Recuperado de: https://www.bafin.de/EN/Homepage/homepage_node.html
- BitLegal, *Tracking Blockchain Technology and Regulation around the World*. Acceso online: <http://bitlegal.io>
- Bustamante, S. (14 de Julio de 2017). “Lanzan en Argentina el primer fondo de inversión en Bitcoins de la región”, en El Cronista. Recuperado de: <https://www.cronista.com/finanzasmercados/Lanzan-en-Argentina-el-primer-fondo-de-inversion-de-Bitcoins-de-la-region-20170714-0060.html>

- “*Canadá tiene el primer cajero de Bitcoins*”, en ABC tecnología, 30 de Octubre de 2013. Recuperado de: <http://www.abc.es/tecnologia/informatica-hardware/20131030/abci-cajero-bitcoin-canada-prox-201310292201.html>
- Carta Orgánica del BCRA, Ley 24.144. Pág. 16. Recuperado de: <http://www.bcr.gov.ar/pdfs/marco/CartaOrganica2012.pdf>
- Cedeño, A. (03 de Julio de 2017). “*Banco central de Tailandia encargado de estudiar Bitcoin*”, en InfoCoin. Recuperado de: <http://infocoin.net/2017/07/03/banco-central-de-tailandia-encargado-de-estudiar-bitcoin/>
- “*Cerco al Bitcoin: Rusia anuncia que regulará el mercado de las divisas digitales*”, en El Economista, 08 de Septiembre de 2017. Recuperado de: <http://www.eleconomista.es/divisas/noticias/8596283/09/17/Cerco-al-bitcoin-Rusia-regulara-el-mercado-de-las-divisas-digitales.html>
- “*China libra una guerra sin cuartel contra Bitcoin que amenaza con hacerla añicos*”, en eldiario.es, 11 de Enero de 2018. Recuperado de: http://www.eldiario.es/hojaderouter/tecnologia/China-guerra-Bitcoin-anicos-cuestion_0_727927522.html
- Christin, N. (2012). “*Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace*”. Recuperado de: <https://www.andrew.cmu.edu/user/.../TR-CMU-CyLab-12-018.pdf>
- Cobo Huici, R. “*Primeros billetes impresos en China*”, en Blog numismático digital, 22 de Octubre de 2014. Recuperado de: <http://www.numismaticodigital.com/noticia/2407/articulos-notafilia/primeros-billetes-impresos-en-china.html>
- “*Comunicado oficial sobre el uso de Bitcoin*”, Banco Central de Ecuador (BCE), 8 de Enero de 2018. Recuperado de: <https://www.bce.fin.ec/index.php/boletines-de-prensa-archivo/item/1028-comunicado-oficial-sobre-el-uso-del-bitcoin>
- Crippen, A. (14 de Marzo de 2014). “*Buffett blasts Bitcoin as 'mirage': 'Stay away!'*”, en CNBC. Recuperado de: <http://www.cnbc.com/id/101494937>
- Digital Currency, en Financial Consumer Agency of Canada. Recuperado de: <https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html>
- Directiva sobre dinero electrónico de la Comisión Europea (2009/110/EC). Recuperado de: http://ec.europa.eu/internal_market/payments/emoney/text/index_en.htm

- “Ecuador prohíbe Bitcoin y aprueba creación de moneda digital estatal dependiente del Banco Central”, en OroYFinanzas, 28 de Julio de 2014. Recuperado de: <https://www.oroymasfinanzas.com/2014/07/ecuador-prohibe-bitcoin-aprueba-creacion-de-moneda-digital-estatal-dependiente-banco-central/>
- “El Banco Central informó que los Bitcoins no son legales, ni tienen respaldo”, en iProfesional, 29 de Mayo de 2014. Recuperado de: <http://www.iprofesional.com/notas/187955-banco-central-riesgos-bitcoin-El-Banco-Central-informo-que-los-bitcoins-no-son-legales-ni-tienen-respaldo>
- “En octubre se instalarán 200 cajeros de criptomonedas en Argentina”, en iProfesional, 15 de Septiembre de 2017. Recuperado de: <http://www.iprofesional.com/notas/255910-euro-banco-moneda-mercado-divisas-bitcoin-fintech-transferencias-letes-En-octubre-se-instalaran-200-cajeros-de-criptomonedas-en-Argentina>
- Feliba, D. (30 de Noviembre de 2016). “Bitcoins: la moneda virtual crece en la Argentina y apunta a los clientes no bancarizados”, en La Nación. Recuperado de: <http://www.lanacion.com.ar/1960718-bitcoins-la-moneda-virtual-crece-en-la-argentina-y-apunta-a-los-clientes-no-bancarizados>
- Fernandez, M. (01 de Octubre de 2017). “Japón da alas al uso del Bitcoin tras el carpetazo de China”, en El Boletín. Recuperado de: <http://www.elboletin.com/noticia/154021/economia/japon-da-alas-al-uso-del-bitcoin-tras-el-carpetazo-de-china.html>
- Frankel, T. (2012). “The Ponzi Scheme Puzzle. A History and Analysis of Con Artists and Victims”. Oxford University Press. Nueva York.
- “From Bitcoin to digital central bank money: still a long way to go”, en Deutsche Bundesbank. 20 de Septiembre de 2017. Recuperado de: https://www.bundesbank.de/Redaktion/EN/Reden/2017/2017_09_20_thiele.html
- Fundación Bitcoin Argentina. Acceso online: <http://www.bitcoinargentina.org>
- Fung, B. (26 de Febrero de 2014). “Sen. Joe Manchin calls for a Bitcoin ban as regulators seek ‘accelerated push’”, en The Washington Post. Recuperado de: https://www.washingtonpost.com/news/the-switch/wp/2014/02/26/sen-joe-manchin-calls-for-a-bitcoin-ban-as-regulators-seek-accelerated-push/?utm_term=.ddc925723345
- Gerencia de entidades financieras. Resolución de Directorio N° 044/2014. “Prohibición del uso de monedas y denominaciones monetarias no reguladas en el ámbito del sistema

- de pagos nacional*”, Banco Central de Bolivia. Recuperado de: <http://www.bcb.gob.bo/webdocs/2014/Normativa/Resoluciones/044%202014.PDF>
- Greenberg, A. (26 de Febrero de 2014). “*Senator Calls For Bitcoin Ban In Letter To Financial Regulators*”, en Forbes. Recuperado de: <https://www.forbes.com/sites/andygreenberg/2014/02/26/senator-calls-for-bitcoin-ban-in-letter-to-financial-regulators/#742704021140>
 - Iglesias Fraga, A. (08 de Septiembre de 2017). “*Rusia se plantea regular el Bitcoin y otras criptomonedas*”, en TICBeat. Recuperado de: <http://www.ticbeat.com/innovacion/rusia-se-plantea-regular-el-bitcoin-y-otras-criptomonedas/>
 - Kearns, J. (4 de Diciembre de 2013). “*Greenspan Says Bitcoin a Bubble Without Intrinsic Currency Value*”, en Bloomberg. Recuperado de: <http://www.bloomberg.com/news/2013-12-04/greenspan-says-bitcoin-a-bubble-without-intrinsic-currencyvalue.Html>
 - Krugman, P. (31 de Enero de 2018). “*Los fraudes y problemas que habrá cuando estalle la burbuja de Bitcoin*”, en The New York Times. Recuperado de: <https://www.nytimes.com/es/2018/01/31/burbuja-bitcoin-inversion-criptomonedas/>
 - “*Los Bitcoins encienden la ilusión también en el interior del país*”, en El Cronista, 14 de Marzo de 2014. Recuperado de: <https://www.cronista.com/itbusiness/-Los-bitcoins-encienden-la-ilusion-tambien-en-el-interior-del-pais-20140114-0014.html>
 - “*Luego de años en las sombras, el creador de Bitcoin revela su identidad*”. 2 de Mayo de 2016. BBC Mundo. Recuperado de: http://www.bbc.com/mundo/noticias/2016/05/160502_bitcoin_creador_satoshi_nakamoto_craig_wright_revelacion_wbm
 - *Markets*,” *Bitcoincharts*”. Recuperado de: <http://bitcoincharts.com/markets/>
 - Marty, B. (19 de Junio de 2014). “*Bolivia, el primer país americano en prohibir Bitcoin*”, en PanamPost. Recuperado de: <https://es.panampost.com/belen-marty/2014/06/19/bolivia-el-primer-pais-americano-en-prohibir-bitcoin/>
 - Matonis, J. (20 de Agosto de 2012). “*WikiLeaks Bypasses Financial Blockade With Bitcoin*”, en Forbes. Recuperado de: <http://www.forbes.com/sites/jonmatonis/2012/08/20/wikileaks-bypasses-financial-blockade-with-bitcoin>

- “*Monedas virtuales. Comunicación al público en general*”. Banco Central de la República Argentina. Recuperado de: www.bcra.gov.ar/bilmon/bm023000.asp
- Moreno, F. (20 de Febrero de 2014). “*Banco Central de Brasil emite notas sobre problemas del Bitcoin*”, en InfoMoney. Recuperado de: <http://www.infomoney.com.br/mercados/cambio/noticia/3203295/incomodado-com-competicao-banco-central-emite-nota-sobre-problemas-bitcoin>
- Neyman, L. (19 de Mayo de 2013). “*Did mathematician Shinichi Mochizuki invent Bitcoin?*”, en Gizmodo. Recuperado de: <https://gizmodo.com/did-mathematician-shinichi-mochizuki-invent-bitcoin-508715535>
- “*Ponzi Schemes Using Virtual Currencies*”. Acceso online: http://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf
- “*Por qué Corea del Sur quiere prohibir el uso del Bitcoin (y en qué otros 8 países no se puede utilizar)*”, en BBC Mundo, 12 de Enero de 2018. Recuperado de: <http://www.bbc.com/mundo/noticias-42648703>
- “*RBI cautions users of Virtual Currencies against Risks*”, Reserve Bank of India, 24 de Diciembre de 2013. Recuperado de: <http://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/IEPR1261VC1213.pdf>
- Reid, F. y Harrigan, M. (Julio de 2011). “*An Analysis of Anonymity in the Bitcoin System*”. Recuperado de: http://arxiv.org/pdf/1107.4524.pdf?origin=publication_detail
- “*Resolución 300/2014. Monedas Virtuales. Resolución N° 70/2011. Modificación (Resolución 300/2014)*”, Unidad de Información Financiera, 4 de julio de 2014. Recuperado de: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/230000-234999/231930/norma.htm>
- “*Riesgos asociados al surgimiento de las monedas virtuales, el ejemplo de los Bitcoin*”. Banco de Francia, 5 de Diciembre de 2013. Recuperado de: https://www.banquefrance.fr/fileadmin/user_upload/banque_de_france/publications/Focus_10the_dangers_linked_to_the_emergence_of_virtual_currencies_the_example_of_bitcoins-GB.pdf
- Rogoff, K. (9 de Octubre de 2017). “*¿Oro falso encriptado?*”, en Project Syndicate. Recuperado de: <https://www.project-syndicate.org/commentary/bitcoin-long-term-price-collapse-by-kenneth-rogooff-2017-10/spanish?barrier=accessreg>

- Roubini, N. (26 de Enero de 2018). “*Las promesas rotas de Blockchain*”, en Project Syndicate. Recuperado de: <https://www.project-syndicate.org/commentary/why-bitcoin-is-a-bubble-by-nouriel-roubini-2018-01/spanish>
- Ruiz Calleja, A.: *Blog Numismático*. Recuperado de: www.blognumismatico.com
- Sala-i-Martín, J. (13 de Abril de 2013). *La burbuja del Bitcoin*. Recuperado de: <http://www.salaimartin.com/randomthoughts/item/589-la-burbuja-del-bitcoin.html>
- “*SEC Charges Texas Man With Running Bitcoin-Denominated Ponzi Scheme*”, en Securities and Exchange Commission. Acceso online: https://www.sec.gov/News/PressRelease/Detail/PressRelease/1370539730583#.U0mLP_mSzHQ
- Segal, D. (18 de Enero de 2014). “*Eagle. Scout. Idealist. Drug Trafficker?*”, en The New York Times. Recuperado de: <https://www.nytimes.com/2014/01/19/business/eagle-scout-idealist-drug-trafficker.html>
- Solé, R. (15 de Septiembre de 2017). “*India, pese a no estar cómoda con el Bitcoin, estaría trabajando en su propia criptomoneda*”, en HardwarEsfera. Recuperado de: <https://hardwaresfera.com/india-pese-no-estar-comoda-bitcoin-estaria-trabajando-criptomoneda/>
- Stiglitz, J. (1 de Diciembre de 2017). “*Por qué el premio nobel de Economía Joseph Stiglitz cree que se deberían prohibir los Bitcoins*”, en BBC Mundo. Recuperado de: <http://www.bbc.com/mundo/noticias-42196322>
- “*Tailandia, el primer país que prohíbe la moneda virtual Bitcoin*”, en BBC, 30 de Julio de 2013. Recuperado de: http://www.bbc.com/mundo/ultimas_noticias/2013/07/130730_ultnot_bitcoin_tailandia_vp
- “*Tim Draper Wins Gov’t Auction, Partners With Vaurum to Provide Bitcoin Liquidity in Emerging Markets*”, Comunicado de Vaurum, en Medium, 2 de julio de 2014. Acceso online: <https://medium.com/@vaurum/timdraper-wins-govt-auction-partners-with-vaurum-to-provide-bitcoin-liquidity-in-emerging-markets-88f04a1d8598>
- Tirole, J. (30 de Noviembre de 2017). “*There are many reasons to be cautious about Bitcoin*”, en Financial Times. Recuperado de: <https://www.ft.com/content/1c034898-d50f-11e7-a303-9060cb1e5f44>

- *Vietnam declara ilegales todas las transacciones con Bitcoin*”, en Eju!, 28 de Febrero de 2014. Recuperado de: <http://eju.tv/2014/02/vietnam-declara-ilegales-todas-las-transacciones-con-bitcoin/>
- *“Virtual Currencies. Key Definitions and Potential AML/CFT Risks”*, FATF Report, Junio de 2014. Recuperado de: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cftrisks.pdf>
- Weisenthal, J. (24 de Enero de 2014). *Robert Shiller: “El Bitcoin es un ejemplo asombroso de una burbuja, de eso no hay duda”*, en El economista. Recuperado de: <http://www.eleconomista.es/mercados-cotizaciones/noticias/5485736/01/14/Robert-Shiller-El-bitcoin-es-un-ejemplo-asombroso-de-una-burbuja.html>
- Worstall, T. (21 de Noviembre de 2013). *“Finally, A Proper Use for Bitcoin, Avoiding Capital Controls”*, en Forbes. Recuperado de: <http://www.forbes.com/sites/timworstall/2013/11/21/finally-a-proper-use-for-bitcoinavoiding-capital-controls/>

