



FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES
(ICAIDE)

BITCOIN: UNA ALTERNATIVA FALLIDA AL SISTEMA MONETARIO CENTRALIZADO

Autor: Pablo Cánovas Vaca
Director: Amparo Merino de Diego

Madrid
Junio, 2014

A mis padres: Antonio Fco. y M^a del Carmen

Índice de contenido	2
Resumen y palabras clave	3
Glosario	4
Listado de gráficos y figuras	5
Introducción	6
Objetivos	7
Metodología empleada	8
Estructura de trabajo	9
Capítulo I. Antecedentes económicos, políticos y sociales	11
1.1) Estados Unidos, el inicio del final	11
1.2) Europa	13
1.3) Japón, la cuna del Bitcoin	14
1.4) Corrupción global, casos y teorías	15
Capítulo II. El Bitcoin	18
2.1) Bitcoin y las monedas privadas	18
2.2) Orígenes, definición y funcionamiento	19
2.2.1) <i>Procesamiento – minería</i>	20
2.2.2) <i>Balances – cadena de bloques</i>	21
2.2.3) <i>Transacciones - llaves privadas</i>	21
2.3) Volatilidad	22
2.4) Popularidad, robos y controversias	25
2.4.1) <i>Aceptación comercial</i>	25
2.4.2) <i>Bitcoin y Silk Road 2.0</i>	26
2.4.3) <i>Continúan los robos: MtGox, Flexcoin y Poloniex</i>	28
2.5) El proceso legislador	29
Capítulo III. Razones a favor del Bitcoin, concepto teórico	34
3.1) Bitcoin como moneda. Latinoamérica	34
3.2) Moneda humanitaria	36
3.3) Bitcoin sustitutivo del oro y mejor que el dinero fiduciario	37
Capítulo IV. Razones en contra del Bitcoin, evidencia empírica	40
4.1) Medio de cambio	40
4.2) Unidad de cuenta y de valor	43
4.3) Otras objeciones	45
4.4) ¿Mejor que el oro?	47
Conclusiones y futuras líneas de investigación	51
Bibliografía	55
Anexos	59

Resumen

El presente trabajo de investigación presenta un tema muy actual: el Bitcoin. Recoge información básica sobre la situación de la moneda criptográfica, de sus orígenes y de su evolución. Asimismo, se intenta dar una respuesta clara a la viabilidad de dicha moneda como sistema alternativo a un supuesto sistema monetario fallido. Para ello se presentarán diversos puntos de vista académicos y se somete a examen al Bitcoin para llegar a una serie de conclusiones finales. .

Palabras clave

Bitcoin, sistema monetario, centralización, volatilidad, fraude, transacciones, nodos, crisis institucional, legislación, commodity, criptomoneda, moneda virtual, digital

Abstract

This argumentative paper aims to present a very popular topic nowadays: the Bitcoin. Basic information about the origins and evolution of the cryptographic currency is given. Moreover, it tries to answer to a decisive question formulated since the Bitcoin very beginning: Could this currency be an alternative to the current monetary system and its disappointments? Therefore, several and different academic researches and opinions will be stated in order to achieve the final conclusions.

Key words

Bitcoin, monetary system, centralization, volatility, fraud, transactions, nodes, institutional crisis, legislation, commodity, cryptocurrency, virtual money, digital

Glosario

BCE: Banco Central Europeo

Bn: Billones americanos (1000,000,000)

BTC: Bitcoin

CEI:

EEUU: Estados Unidos de América

EUR: Euros

FED: Reserva Federal Norteamericana

GBP: Libras esterlinas

GS: Goldman Sachs

IRS: Internal Revenue Service

MM: Millones (1,000,000)

PIB: Producto Interior Bruto

Q1: Primer cuatrimestre

UE: Unión Europea

\$/USD: Dólar norteamericano

Listado de gráficos, figuras y anexos

Gráfico 1: Cotización Bitcoin (Septiembre 2010-Noviembre 2011) en USD	23
Gráfico 2: Cotización Bitcoin	23
Gráfico 3: Cotización Bitcoin	24
Gráfico 4: Capitalización de mercado BTCs (2013-2014)	26
Gráfico 5: Postura de los diferentes países de cara al fenómeno Bitcoin	32
Gráfico 6: Activos de los Bancos Centrales del G4 (EEUU, Zona Euro, Reino Unido y Japón). Índices con base en 2006.	38
Gráfico 7: Número de transacciones por día (BTC)	41
Gráfico 8: “Algunas monedas son usadas internacionalmente debido al poder de algunos gobiernos”, John Normand (2014).	42
Gráfico 9: Histórico del Nasdaq	44
Gráfico 10: Volatilidad del Bitcoin vs. otra divisas e inflación (últimos 60 años)	45
Gráfico 11: Volumen medio de negociación diario de las diferentes divisas en el Chicago Mercantile Exchange (en USD Bn)	46
Anexo 1: Funcionamiento del Bitcoin, ejemplificado	59
Anexo 1.1: Traducción Anexo 1	60
Anexo 2: Histórico del Bitcoin	61
Anexo 3: Relación inversa entre el valor del Bitcoin y el volumen de transacciones llevadas a cabo. La excesiva volatilidad lo compromete como instrumento de cambio	62

Introducción

Las sucesivas políticas monetarias llevadas a cabo antes y después de la crisis financiera de las hipotecas “*subprime*” (2007), Russo y Katzel (2010), han demostrado una serie de debilidades y flaquezas del sistema centralizado (corrupción institucional, fallo del “inflation targeting”, brechas entre la economía nominal y la real...), donde las políticas monetarias se han visto cuestionadas por los acontecimientos sucedidos y donde los costes de transacción se ven inflados por la excesiva presencia de agentes intermediarios. Las brechas surgidas en la confianza de la población han dado lugar a la creación e idealización de alternativas al dinero fiduciario y centralizado, controlado, al fin y al cabo, por una institución intervencionista, Lew Rockwell (2013).

El interés general demostrado en los últimos años por una moneda criptográfica singular: el Bitcoin, ha despertado la necesidad de desarrollar en este trabajo sus fortalezas y debilidades, además de oportunidades y peligros, J.P Morgan (2014), David Yermack (2014). Es importante mantener la objetividad en todo momento y limitarse a describir una situación real de la que frecuentemente se tiene noticia por los diversos medios de comunicación. Además, todo suceso tiene un origen y unas consecuencias, en este caso sociales y económicas, las cuales se han plasmado a lo largo de toda la obra. Se procura, así dar una visión clara del tema y acercar al lector a uno de los campos con mayor auge de la informática: las monedas criptográficas, y en especial, el caso del Bitcoin, Reuben Grinberg (2011).

Se presenta el entorno macroeconómico mundial que da lugar a la moneda mencionada, y cómo la misma es producto de una sociedad defraudada y alertada por los casos de corrupción y mala gestión monetaria. Se revisa, así, la situación Estadunidense, Europea y Japonesa, además de las consecuencias de la corrupción en el ánimo y la confianza de los ciudadanos. Posteriormente, se da una visión clara del Bitcoin, su nacimiento (2009), funcionamiento y significado, eliminando el lenguaje técnico y desarrollando un texto claro y preciso.

Asimismo, el lector podrá contrastar diferentes posturas con respecto a la moneda criptográfica, enmarcadas en dos bandos diferentes: a favor o en contra de su viabilidad

como alternativa al sistema fiduciario actual. Así, se someterá a examen dicha moneda, aplicando cada una de las características propias del dinero a su realidad: 1) Medida de valor y cuenta; 2) Medio de pago e intercambio (con la connotación de aceptación mundial).

Una serie de preguntas serán planteadas a lo largo del trabajo, con el objetivo de que el lector reflexione y pueda llegar a sus propias conclusiones, las cuales se verán corregidas y perfeccionadas conforme continúe con la lectura, llegando así a la parte más importante del ensayo: publicaciones y estudios contrapuestos, evidencias y demostraciones empíricas, que ayudará a formular una conclusión global que podremos usar para referirnos al Bitcoin y su realidad actual, y posiblemente futura.

Objetivos

Los objetivos perseguidos por este ensayo son:

- Determinar y describir los factores determinantes del nacimiento y desarrollo del Bitcoin. Identificar las variables tanto cualitativas como cuantitativas que definen su funcionamiento. Y ofrecer una clara imagen del movimiento social que lo promueve.
- Dar una respuesta a la viabilidad del Bitcoin como moneda descentralizada en el modelo económico vigente. Se pretende estudiar cada una de las ventajas e inconvenientes de la moneda, su introducción en el mundo de las transacciones financieras y las consecuencias que tendría la aceptación y regulación por parte de cada uno de los Gobiernos.
- Avanzar en el conocimiento sobre la moneda criptográfica, intentando transmitir un trazo conceptual capaz de identificar cada uno de los diferentes dimensiones de este fenómeno, para así poder contractarlas con las que configuran la percepción pública.

- Examinar las atribuciones más conceptuales e ideológicas atribuidas al Bitcoin, contractarlas y fijar posibles vías de desarrollo y aplicación.

Metodología empleada

La metodología empleada en este trabajo consiste en la comparación y análisis de las diversas opiniones y estudios publicados acerca de la nueva moneda: el Bitcoin. Se parte de un análisis macroeconómico y de las políticas monetarias realizadas en tres áreas fundamentales de nuestra economía mundial (EEUU, Europa y Japón), para adentrarse poco a poco en una evaluación sistemática de las condiciones de la moneda criptográfica. Posteriormente, y usando publicaciones recientes, tratados económicos y estudios cualificados, se compraran las diversas posturas acerca del Bitcoin.

Cabe resaltar que se han utilizado diferentes fuentes secundarias de información acerca del tema tratado: Informes bancarios, comunicados de prensa, foros especializados y artículos varios, publicados por instituciones como Bloomberg, Financial Times o Forbes. Un tema muy actual que está en continuo desarrollo y cuya incesante actualización es necesaria. Por lo que se trata de una exposición que ha tenido como objetivo mostrar al lector la realidad y funcionamiento de una nueva moneda, en un campo prometedor y con altas perspectivas de futuro, como son los métodos de pago virtuales.

Para la confección de esta obra, se ha seguido parcialmente un enfoque argumentativo y que constituye una simbiosis entre un texto explicativo y delineador (en este caso explicar el Bitcoin y todo lo que abarca) y un texto destinado al debate (con matiz de rechazo), según la clasificación de MacInnis (2011) sobre tipos de aportación de una investigación conceptual. De esta manera la metodología empleada se desarrollaría en torno a:

- a) Una introducción en la que se presentan el porqué del tema tratado, la popularidad del mismo y el impacto que se pretende alcanzar en el lector tras su estudio y asimilación.

- b) Un apartado dedicado a presentar el “*background*” macroeconómico y social en el que nace el Bitcoin. Sus antecedentes y realidad en el momento de su creación.
- c) La presentación de la moneda criptográfica. Al ser un tema complejo ha sido necesario la explicación de su funcionamiento y utilidad, además de mostrar algunas de sus debilidades y fortalezas más claras mediante casos reales sucedidos recientemente. Hasta aquí, el texto alcanza una función explicativa y delineadora, ofreciendo al lector un desglose de la intención del texto, de la realidad político-económica, y de las características propias del Bitcoin. Se va dibujando un mapa conceptual similar al realizado por un cartógrafo que proporciona una clara imagen de lo que estudiamos y del porqué de su estudio,
- d) La contraposición de opiniones y evidencias empíricas. Puesta en duda la teoría y concepto que sigue el “movimiento” Bitcoin, se proponen una serie de datos empíricos que “acusan” a la moneda de irreal e inviable, como lo haría un fiscal en un juicio civil o penal, mostrando evidencias que rechacen la “inocencia” del acusado, siendo en este caso el Bitcoin.
- e) Una conclusión final, donde se intentará poner fin a las dudas del lector sobre el susodicho tema y donde se recogerán las respuestas a las preguntas formuladas a lo largo del trabajo.

Por último, mencionar que las variables utilizadas han sido tanto cualitativas como cuantitativas, teniendo las primeras una mayor incidencia. Se han utilizado variables cuantitativas a la hora de la presentación del tema y con el objetivo de proporcionar al lector una mayor claridad y capacidad de comprensión. Las variables cualitativas han constituido la esencia del trabajo, al proporcionar un debate empírico acerca del tema tratado y ayudar a confeccionar un final concluyente.

Estructura del trabajo

El trabajo realizado cuenta con cuatro capítulos y un apartado dedicado a las conclusiones.

En el primer capítulo se ha realizado un análisis del entorno económico y político social en el que ha “nacido” el Bitcoin, con el objetivo de una mejor comprensión de la realidad que engloba a la moneda virtual. Así, se ha llevado a cabo un detallado análisis sobre tres de las potencias mundiales donde más se ha notado su actividad (Estados Unidos, Europa y Japón). Además, se ha añadido un apartado dedicado a la corrupción política y social, fomentada en gran parte por las políticas económicas llevadas a cabo en el mundo occidental. Conocer estos hechos es necesario para llegar a entender el aspecto más social de la moneda virtual.

En el segundo capítulo se ha presentado al Bitcoin en su totalidad. Partiendo de su nacimiento, se ha descrito su funcionamiento y proceso de creación (además el lector cuenta con un esquema explicativo de dichos procesos en Anexos 1 y 1.1, para su mejor comprensión). Asimismo se ha analizado la reciente realidad de la moneda virtual, viendo su importancia en el mundo de las transacciones comerciales y en de los robos informáticos. Analizaremos su volatilidad como aspecto introductorio y de gran importancia para continuar con el tercer capítulo. Además, se hará mención a los numerosos procesos legislativos que han empezado a aparecer como consecuencia a los desajustes legales que supone esta nueva moneda virtual.

El tercer capítulo desglosará las opiniones de todos aquellos que siguen y apoyan esta nueva corriente monetaria y virtual. Veremos como es ensalzada por encima del oro o de monedas fiduciarias como el dólar o el euro.

El cuarto capítulo, por su parte, recoge un listado de diferentes evidencias que tienden a desacreditar al Bitcoin como moneda o como mejor refugio de valor.

Por último, las conclusiones finales resumirán el trabajo, determinando el grado de cumplimiento de los objetivos preestablecidos y abrirán la posibilidad de futuras fuentes de investigación o aplicación del Bitcoin.

Capítulo I

Antecedentes económicos, políticos y sociales

En este capítulo se describe la situación macroeconómica, política y social de las tres potencias mundiales donde la moneda criptográfica ha alcanzado su mayor auge (EEUU, Europa y Japón), además de una sección que engloba un problema global de la sociedad: la corrupción. Su presentación y estudio tiene el objetivo de presentar la realidad en la que se concibe y desarrolla el Bitcoin, para poder entender el movimiento social que en primer lugar lo promueve.

1.1) EEUU

Todo comienza con la crisis de las hipotecas “*subprime*” (EEUU, 2007) y su posterior contagio al sistema financiero internacional (crisis financiera 2008). El excesivo endeudamiento de las entidades financieras estadounidenses, el mantenimiento de los ratios de interés a niveles de mínimos históricos por un periodo de tiempo superior al que se debía, junto con la política de “*laissez faire, laissez passer*”, que la Reserva Federal Americana de Alan Greenspan¹ desarrolló desde 2002, había generado un sentimiento de bonanza que se extendía por todos los extractos de la sociedad, John Taylor (2009). De acuerdo con el CEI (en base al Bureau of Economic Analysis²), el ahorro neto de las familias como porcentaje del PIB en \$US, había descendido en más de un 62% del 8% en 1992 a un 3% a comienzos del 2007. El ahorro neto de la economía había caído en un 83% desde 1998, y en 2008 era de cifra negativa: \$ -100Bn americanos.

Por otro lado, de acuerdo a The Federal Reserve Board, el grado de endeudamiento hipotecario del país, se había incrementado en un 53% (USD9,3Bn en Q4 2003-USD14.3Bn en Q4 2007). Su déficit había aumentado en un 34%, llegando a constituir el 64.3% del PIB del país en 2007 y el 110.81% en 2010³. Y los tipos de interés no

¹ Alan Greenspan (1926), presidente de la Reserva Federal de EE.UU. (1987-2006).

² US Bureau of Economic Analysis, Institución oficial dedicada a la acumulación de datos estadísticos sobre diversos aspectos económicos de EEUU

³ Treasury Direct, página oficial de servicios financieros en EEUU. Consultada el 4 de Febrero de 2014. https://www.treasurydirect.gov/govt/reports/ir/ir_expense.htm US Government Spending, consultada el 4

dejaron de bajar hasta llegar a mínimos históricos (1% anual) en 2003, alimentando la especulación financiera y la creación de la burbuja inmobiliaria que no tardaría en “explotar”, Russo y Katzel (2010).

La situación descrita, no es más que un claro reflejo de la teoría de los ciclos económicos neo-keynesiana: Un shock monetario (incremento de la oferta en este caso), como el que la Reserva Federal provoca con la bajada de los tipos de interés a corto y a largo plazo, afectará a la economía de manera escalonada. En un primer momento, el incremento de liquidez se traducirá en un incremento del volumen de negociación en los mercados financieros. Aumentará la demanda y con ello los precios de dichos productos, hasta que los inversores hayan conseguido todos los beneficios posibles. Los inversores decidirán diversificar sus portafolios, invirtiendo en activos no financieros (inmuebles). La demanda excederá la oferta, aumentando el precio de los mismos y fomentando su construcción y especulación, Lindbeck (1998).

Las familias y entidades se endeudan, ya que los tipos de interés son inferiores a la rentabilidad que puede conseguir en el mercado. La inflación se dispara, pero debido a un fallo en la coordinación y los llamados “*lags*”⁴ en materia de reconocimiento, toma de decisión y efectividad; las políticas monetarias y fiscales no actúan en consonancia, por lo que se produce un desajuste en el sistema: los tipos de interés aumentan ante el temor inflacionario. Las hipotecas y demás deudas comienzan a vencer, los impagos se incrementan desestabilizando a las entidades que poseen dichas carteras. El excesivo endeudamiento bancario solo empeora la situación, multiplicando los efectos del impago, Lindbeck (1998). Además, el efecto no es aislado. Con la globalización, el sistema financiero y bancario está interconectado internacionalmente, la caída de una compañía con activos de un valor razonable, tendría repercusiones en todo el mundo. El caso de la quiebra de Lehman Brothers Inc. el 15 de septiembre de 2008 (compañía con activos valorados en \$ 691,063Bn, finales de 2007), ejemplifica esta teoría. El suceso tuvo réplicas nocivas por el sistema bancario e hipotecario mundial, considerándose como “el inicio del fin” del mundo financiero hasta entonces conocido.

de Febrero de 2014.
http://www.usgovernmentspending.com/spending_chart_2007_2017USd_10s11i111mcn__US_Real_GDP_Chart

⁴ Retrasos

La teoría y la lógica nos dicen que la política monetaria de un país o conjunto de países con una misma moneda, debe ir ligada a la evolución económica de la misma. Sin embargo, en un discurso el 16 de julio de 2002 Alan Greenspan, Chairman de la Reserva Federal, sostuvo que tan solo se incrementarían los tipos de interés en caso de depresión económica (y entiéndase con ello, en el momento en el que la economía perdiese potencia) y que no estaba en su labor frenar la “burbuja” inmobiliaria que se estaba creando, Russo y Katzel (2010). Al mismo tiempo el Economista Jefe del Fondo Monetario Internacional, Raghuram Rajan (2003-2007), sostenía que la lógica del Chairman de la FED no era solo asimétrica, sino gravemente peligrosa. Greenspan estaba alimentando la inflación del precio de los activos, diciendo a Wall Street y a los bancos de todo el mundo que no aumentaría los tipos de interés:

IMF Chief Economist Raghuram Rajan, this “...logic was not only strangely asymmetrical – why is the bottom easier to recognize than the top? – but also positively dangerous[, in that it] fueled the flames of asset-price inflation by telling Wall Street and banks across the country that the Fed would not raise interest rates to curb asset prices, and that if matters went terribly wrong, it would step in to prop prices up.” Gunn Dwyer (2010) y Russo and Katzel (2010: 26).

Siguiendo la predicción Neo-Keynesiana, en 2004, la FED aumentó progresivamente los tipos de interés del 1% al 5,25%, ante el miedo inflacionario, con el consecuente resultado en 2007: impago de hipotecas, venta de inmuebles, con la consecuente caída de precios y deterioro de las carteras bancarias.

1.2) Europa

Al otro lado del “Charco”, la Europa de los 12⁵ se había unido monetariamente mediante el Euro (introducción de monedas y billetes: 1 de enero de 2002). Una moneda centralizada, gestionada por el BCE⁶ y con grandes perspectivas de futuro.

⁵ Países de la UE que adoptaron el Euro como moneda común cuando se adoptó oficialmente el 16 de diciembre de 1995: Bélgica, Alemania, Francia, Italia, Luxemburgo, Países Bajos, Irlanda, Grecia, España Portugal, Austria, Finlandia.

Ante la crisis del Petróleo y la caída de las “Telecom”, el Banco Central Europeo adoptará tipos de interés muy bajos desde 2002, potenciando el crédito, el crecimiento del PIB (de 0.5% en 2002 a 3% en 2008⁷) y reduciendo el desempleo medio hasta un 7% de la masa laboral. Sin embargo, estos son datos medios. El problema se generó ante las diferencias estructurales y económicas de los diferentes países integrantes de la Unión, los cuales compartían una política monetaria común, pero con estructuras productivas, financieras, políticas y poblacionales muy diferentes.

Los diferentes grados de exposición financiera al sistema Americano determinaron la manera en la que les afectó el deterioro económico. Numerosos Bancos Europeos se vieron afectados (los Sparkassen Alemanes, las cajas de ahorro españolas, los bancos Griegos...). Además, el BCE aumentó los tipos de interés llegando al 4%⁸, 2009, sin tener en cuenta la situación de los diferentes Países. Como era de esperar, la población de algunos miembros de la UE no pudieron hacer frente a esta subida (los “PIGS”), aumentando los impagos y la tasa de morosidad, colapsando el sistema financiero y necesitando, muchos de ellos, un “rescate” centralizado.

Las ayudas no vinieron sin condiciones, debiendo los Gobiernos, tomar medidas de austeridad y restructuración interna, que causaron un malestar social que aún perdura, y que sin duda ha ayudado a alentar tendencias sociales de cambio, como podríamos referirnos al movimiento que engloba el Bitcoin, OECD (2014).

1.3) Japón, la cuna del Bitcoin

Japón, por su parte, sufría de un período deflacionario y de problemas estructurales. La política monetaria del Banco Central nipón de mínimos (0,5%) no conseguía aumentar la liquidez de la economía. El Sistema Bancario japonés, uno de los más opacos del mundo, no ayudó a la labor del Gobierno. Basado en los “Keiretsu”, es un sistema piramidal en cuyo vértice se encuentra un banco, el cual podía tener hasta un 5% de las

⁶ El BCE es el banco central de la moneda única europea, el euro. Su función principal consiste en mantener el poder adquisitivo del euro y, con ello, la estabilidad de precios en la zona del euro. La zona del euro comprende los 18 países de la Unión Europea que han adoptado el euro desde 1999.

⁷ Fuente: BCE, <http://www.ecb.europa.eu/ecb/10ann/figures/html/index.es.html>

⁸ <http://es.euribor-rates.eu/tipo-de-interes-del-BCE.asp>

empresas clientes. Lo que se tradujo en la continuación de préstamos de dudoso cobro con las empresas de interés y una restricción al crédito a pequeñas y medianas compañías ajenas al “Keiretsu”.

La población, envejecida, entró en una “trampa de liquidez”⁹, de acuerdo a Paul Krugman. No hay incentivos para ahorrar pero tampoco para consumir debido a la esperanza de la bajada de los precios, lo cual se cumple ante la reducción del consumo (expectativas autocumplidas), Álvaro Espina (2004).

Las diversas medidas llevadas a cabo para frenar esta situación deflacionaria (aumentar la transparencia bancaria y reducir la dependencia de las exportaciones) no parecían haber funcionado de manera correcta, ya que la subida de los tipos de interés ante la crisis de 2007, generaron una masiva cantidad de impagos y una caída del PIB del 1%. Además el desempleo aumentó hasta situarse en 5,5% a finales de 2009, Bank of Japan (2014), resultando, como en los casos anteriores, en una pérdida de confianza y desmotivación social, que podía palparse: manifestaciones, comentarios en la red y movilización juvenil entre otros.

1.4) Corrupción global, casos y teorías

Como cabe esperar, tras los acontecimientos descritos los grandes agentes públicos y privados del sistema monetario comenzaron a perder credibilidad. La etapa de bonanza económica había acabado y una nueva depresión se desataba por todo el Globo, afectando de diferente manera a la mayoría de los países de la comunidad internacional. Aparte de lo ya mencionado, surge otro factor que supondrá la pérdida de confianza definitiva en el sistema: la corrupción política y financiera, pública y privada.

“In virtually all transactions we rely on the word of those with whom we do business.”, Alan Greenspan, 1999.

⁹ **Trampa de liquidez:** término utilizado en la teoría económica para describir una situación en la que los tipos de interés se encuentran en mínimos, próximos a cero. De esta manera no hay incentivo para invertirlo y se prefiere conservar todo el dinero: la preferencia por la liquidez es absoluta. Las políticas monetarias tiene poco efecto (o nulo) y se aboca por medidas fiscales e intervencionistas del Estado en materia de empleo.

La confianza es algo primordial y necesario para el funcionamiento del sistema financiero que conocemos, sin ella el mercado no podría funcionar, no existirían bancos ni dinero fiduciario, ya que nadie creería ni adoptaría una unidad de cambio centralizada como método de pago. No existiría el mundo en el que vivimos y conocemos.

Los escándalos de corrupción, tráfico de influencias y la caída del sistema financiero han minado este elemento vital que sostiene la estructura monetaria y comercial de nuestras economías. Así, se ha podido comprobar cómo el periodo inflacionario, con políticas monetarias de mínimos ha favorecido a una serie de escándalos financieros y públicos que se han ido destapando tras la explosión de la “burbuja económica”.

Tras analizar la inconsistencia temporal de la realidad social con la política monetaria aplicada, el señoreaje y los ciclos político-económicos que se suceden a lo largo del tiempo, existe y es empíricamente demostrable la relación entre el nivel de inflación y el grado de corrupción de un determinado país, Rahmani y Yousefi (2009). Entre 2002-2007, más de 800 funcionarios fueron acusados por corrupción pública en Florida (referente de la expansión inmobiliaria americana de la época), 704 en el estado de Nueva York, y más de 500 en Texas, Pennsylvania, California y Ohio (protagonistas de la extracción petrolífera del país y del desarrollo tecnológico mundial. Casos como la manipulación del LIBOR en Gran Bretaña, malversación de fondos públicos en España, o tráfico de influencias en China no han ayudado a desmentir esta teoría, Financial Trust Index (2014).

Como resultado, el número de partidarios de una reforma monetaria y financiera ha aumentado considerablemente, destacando la importancia de opciones planteadas por las Escuelas de economía, alternativas a la vigente. Los estudios publicados que resaltan la posibilidad de volver a la utilización de monedas locales, dinero libre de deuda o al patrón oro aumentaron notoriamente junto con las críticas al sistema vigente.

En este ambiente de críticas, desconfianza y “decepción” surge el Bitcoin, dando esperanzas a aquellos que sostenían y sostienen la necesidad de algo “nuevo” capaz de sustituir al sistema centralista actual, a sus monedas politizadas y a sus agentes imperfectos. Constituye una solución creativa y que responde a esta cita:

“Los miles de jóvenes que hoy en día descubren por primera vez las ideas de la libertad deben permanecer fuera de la máquina del Estado y de todo su encanto y fascinación letal. En lugar de tratar de infiltrarse en el Estado, deben perseguir sus ideales a través del comercio, la educación, el espíritu empresarial, las artes, la difusión de ideas, el debate, etc. Liderar y ejercer influencia a través del respeto alcanzado por sus logros. Estas son áreas que ofrecen promesas reales y altos rendimientos.” — Lew Rockwell¹⁰, (2013).

¹⁰ **Lew Rockwell**, fundador del Mises Institute, dedicado a defender el movimiento de libre mercado. Principal promotor del resurgimiento de la economía austriaca en EEUU. Editor de Ludwig von Mises y jefe de personal del congresista Ron Paul (1979-1985).

Capítulo II

El Bitcoin

Tras haber dado una clara imagen sobre la realidad en la que el Bitcoin fue creado, el presente capítulo pretende realizar un estudio exhaustivo de la moneda virtual: Clasificarlo y definirlo, describir su nacimiento y funcionamiento, introducir un concepto clave en su actividad, la volatilidad en la que está sumido, estudiar los principales problemas que ha tenido (robos y relación con el crimen organizado) e introducir la iniciativa legislativa que ha avivado en la mayoría de los países del mundo.

2.1) Bitcoin y las monedas privadas

El Bitcoin entra dentro de la definición de monedas criptográficas, las cuales son consideradas como dinero que solo puede intercambiarse de manera electrónica y virtual, utilizando para ello un sistema de valor almacenado digitalmente. Sin embargo, esto no supone ninguna novedad a nuestro sistema fiduciario actual. El Bitcoin no destaca por su carácter virtual, ya que mucho antes de su creación (2009), ya existía el dinero digital, el cual podemos dividir en dos clases, Gans y Halaburda (2014):

- 1) Digitalización de las monedas Estatales (USD, Yen...) o Comunitarias (EUR). Las cuales representan más del 90% de la masa monetaria mundial y fueron creadas para reducir coste de transacción y facilitar la protección y almacenamiento de ese dinero.
- 2) Monedas privadas¹¹ digitalizadas, como los “Facebook Credits”¹², monedas de videojuegos o puntos viaje de compañías aéreas. Las cuales puede ser usadas como “dinero” en un ámbito privado y predeterminado. No existe una conversión generalizada.

¹¹ **Monedas privadas:** dinero emitido por una organización privada, ya sea con fines comerciales o altruistas. Muchos países restringen la emisión de este tipo de dinero.

¹² **Facebook Credits:** Dinero propio de Facebook, usado hasta 2012, mediante el que se podía comprar extras para juegos y otras aplicaciones de la plataforma. \$1 equivalía a 10 Facebook Credits, y estaban disponibles en 15 diferentes monedas.

Es en la segunda categoría donde nacen ciertas “ambiciones” de competir y sustituir a la primera, el dinero fiduciario. En 2012, Matthew Yglesias (economista y periodista estadounidense), planteó la posibilidad de que un “gigante” no gubernamental como Facebook pudiese lanzar, algún día, una divisa capaz de competir con las monedas fiduciarias. Ese mismo año, David S. Evans sostuvo la posibilidad de esta “utopía”, manteniendo que desarrolladores o pequeñas y medianas empresas podrían aceptar Facebook Credits, ya que los usarían para comprar cosas que necesitasen (entre ellos) y para premiar a clientes, Joshua y Hanna (2014). Posteriormente esto quedaría probado como imposible, y es en esta línea donde este ensayo se desarrollará: la evidencia empírica y argumentativa de la imposibilidad del Bitcoin como sustitutivo del dinero en curso legal.

Ambas clases (monedas estatales y privadas) comparten el hecho de que existe una institución (pública o privada) que los soporta, controla y de alguna manera asegura su continuidad. Una entidad (BCE, VISA, la FED...) que mantiene la contabilidad de las transacciones y que asegura el correcto funcionamiento del sistema: cuando una persona, compañía o Banco realiza un pago o ingreso, una entidad “mayor” y común a todos, realiza dicha anotación en cuenta (disminuye la cantidad pagada de una cuenta para aumentar la cantidad correspondiente de la cuenta/s de destino). El Bitcoin, sin embargo rompe con esta concepción y elimina cualquier vestigio de “centralización”. Es aquí, donde radica su carácter novedoso y “esperanzador”.

2.2) Orígenes, definición y funcionamiento

El Bitcoin, creado en Japón el 2009 por un agente bajo el pseudónimo de Satoshi Nakamoto¹³, es una moneda digital, descentralizada, que crea unidades electrónicas no duplicadas y únicas, a partir de un algoritmo diseñado con un límite máximo. De acuerdo con el tratado original publicado por “*Satoshi*”: “Una bitcoin es una unidad de moneda virtual no material, también llamada criptomoneda. Estas son almacenadas en “billeteras electrónicas” anónimas, descritas por una serie de 33 letras y números. La Bitcoin puede viajar de una billetera a otra, por medio de una red de transacción online

¹³ **Satoshi Nakamoto**, persona o grupo de ellas a las que se le atribuye el desarrollo y creación de Bitcoin. Este pseudónimo publicó en 2008 un ensayo en el que explicaba la esencia y funcionamiento de su creación. El manifiesto original podemos encontrarlo en: <https://bitcoin.org/bitcoin.pdf>

“peer-to-peer” (P2P= entre iguales). Cualquier transferencia entre billeteras es registrada en el Código de Bitcoin, así el registro histórico de transacciones claramente identifica a su dueño en cualquier momento, previniendo así conflictos potenciales de propiedad. Los Bitcoins pueden ser divididos en partes tan pequeñas como 100 millonésima de unidad. El sobresaliente volumen actual de Bitcoins está por encima de 10 millones y se proyecta que alcanzará los 21 millones en el año 2140”, The Bitcoin Foundation (2014).

Su creación se lleva a cabo mediante un proceso llamado “mining” y consiste en la resolución de una serie de problemas matemáticos creados de manera aleatoria y resueltos mediante ordenadores de gran capacidad. El algoritmo está definido de tal forma que la producción de Bitcoin sea regresiva y se reduzca a la mitad cada 4 años. Si ahora, por cada proceso se obtienen 25 Bitcoins, en 4 años tan solo se obtendrán 12,5 unidades. Por lo que la oferta de esta “moneda” sería limitada, ocasionando una serie de problemas macroeconómicos que se explicarán en lo sucesivo.

El Bitcoin, sin embargo, y como se ha mencionado con anterioridad, es una moneda que elimina cualquier tipo de control o centralismo. Basándose en un sistema de peer-to-peer (usuario a usuario, de igual a igual), consigue eliminar cualquier tipo de intermediación, lo que implica que a emisión y la gestión de las transacciones, es llevada a cabo de forma colectiva por la red.

A continuación se explican cada una de las operaciones Bitcoin, de acuerdo a la web oficial: Bitcoin.org. Su comprensión es necesaria para poder seguir con el trabajo de investigación. Para más información sobre el funcionamiento de una operación Bitcoin, diríjase al Anexo 1.

2.2.1) Procesamiento - minería

La minería es un sistema de consenso distribuido que se utiliza para confirmar las transacciones pendientes a ser incluidas en la cadena de bloques. Hace cumplir un orden cronológico en la cadena de bloques, protege la neutralidad de la red y permite un acuerdo entre todos los equipos sobre el estado del sistema. Para confirmar las transacciones, deberán ser empacadas en un bloque (registro en la cadena de bloques que contiene confirmaciones de transacciones

pendientes) que se ajuste a estrictas normas de cifrado y que será verificado por la red. Estas normas impiden que cualquier bloque anterior se modifique, ya que hacerlo invalidaría todos los bloques siguientes. La minería también crea el equivalente a una lotería competitiva que impide que cualquier persona pueda fácilmente añadir nuevos bloques consecutivamente en la cadena de bloques. De esta manera, ninguna persona puede controlar lo que está incluido en la cadena de bloques o reemplazar partes de la cadena de bloques para revertir sus propios gastos.

2.2.2) *Balances – cadena de bloques*

Una cadena de bloques o "block chain" es una contabilidad pública compartida en la que se basa toda la red Bitcoin. Todas las transacciones confirmadas se incluyen en la cadena de bloques. De esta manera los monederos Bitcoin pueden calcular su saldo gastable y las nuevas transacciones pueden ser verificadas, asegurando que el cobro se está haciendo al que realiza el pago. La integridad y el orden cronológico de la cadena de bloques se hacen cumplir con la criptografía.

2.2.3) *Transacciones - llaves privadas*

Una transacción es una transferencia de valores entre monederos Bitcoin que será incluida en la cadena de bloques. Los monederos Bitcoin disponen de un fragmento secreto llamado “clave privada”, utilizada para firmar las operaciones, proporcionando una prueba matemática de que la transacción está hecha por el propietario del monedero. La firma también evita que la transacción no sea alterada por alguien una vez ésta ha sido emitida. Todas las transacciones son difundidas entre los usuarios y por lo general empiezan a ser confirmadas por la red en los 10 minutos siguientes a través de la “minería”. Lo único que tiene que hacer un usuario nuevo es descargar en su ordenador o móvil el monedero de Bitcoins. En ese momento se generará su primera dirección, la cual se usará para hacer pagos y demás transacciones futuras, The Bitcoin Foundation (2014).

Resumiendo, el Bitcoin es creado con el fin de rentabilizar las transacciones comerciales, eliminando a los intermediarios. Surge como sistema de pago

basado en pruebas criptográficas que permite suprimir la necesidad de confianza¹⁴, Satoshi Nakamoto (2009).

La crisis financiera y económica de 2007-8 ha provocado un gran escepticismo social ante la capacidad de las autoridades públicas (Gobiernos, Bancos Centrales...) de mantener políticas eficientes y acordes a la realidad económica. El excesivo endeudamiento de los agentes públicos y privados ha resaltado el poder bancario, derivando en un sentimiento de malestar y protesta. El Bitcoin naciendo con un objetivo: rentabilizar el sistema de transacciones y pagos, eliminando a terceros (bancos, instituciones públicas...), constituye la herramienta perfecta y esperanzadora que albergan algunos sectores de la sociedad molestos con la situación social actual, ensalzándolo posible solución a un supuesto corrupto sistema financiero.

Algunos economistas como miran con cierto desprecio a esta idea. "Es bastante lógico que muchos sueñen con una moneda que los políticos, banqueros y bancos centrales no puedan manipular; una moneda de la gente, por la gente y para la gente. Con Bitcoin aflora la esperanza de conseguir algo así. Desgraciadamente, las esperanzas que Bitcoin infunde en tantos corazones y mentes son falsas", Yanis Varoufakis (2013).

2.3) Volatilidad

Al constituir la alternativa más “famosa” al sistema fiduciario actual, el Bitcoin ha captado la atención de economistas, medios de comunicación y gobiernos del todo el mundo. Desde su creación, el Bitcoin ha sufrido una gran volatilidad. Manteniéndose en un valor cercano a \$1, hasta mayo de 2011, cuando sufrió un incremento importante hasta situarse cerca de \$30 en Junio de ese mismo año para luego desplomarse progresivamente hasta los \$2 en octubre. Como podemos ver el Gráfico 1 de Mt. Gox,

¹⁴ Introducción del manifiesto inicial de Bitcoin: El comercio en el Internet ha venido a depender exclusivamente de instituciones financieras las cuales sirven como terceros confiables para el procesamiento de pagos electrónicos (...), el costo de la mediación incrementa costos de transacción (...) Lo que se necesita es un sistema de pagos electrónicos basado en pruebas criptográficas en vez de confianza, permitiéndole a dos partes interesadas en realizar transacciones directamente sin la necesidad de un tercero confiable.

Gráfico 1: Valor Bitcoin (Septiembre 2010-Noviembre 2011), en USD



Fuente: MtGox (2014)

plataforma de intercambio de Bitcoins más usada (70% de las transacciones), que solicitó la quiebra en febrero de 2014 debido a una serie de incidentes los cuales desarrollaremos más adelante.

Posteriormente, y con el incremento de su popularidad, Bitcoin ha llegado a valer más de \$1100 (diciembre de 2013). Sin embargo este valor, lejos de mantenerse, cayó por

Gráfico 2: Cotización histórica Bitcoin (BitStamp) en USD



Fuente: BitStamp (2014)

debajo de los \$500 a final de ese mismo mes, para llegar a estar alrededor de los \$600 en marzo del 2014¹⁵. (Nota: los valores son aproximados y las referencias usadas son BitiStamp y Bitifinex, las plataforma de intercambio de Bitcoins con mayor volumen de negociación, 35% y 26%, respectivamente).

Gráfico 3: Cotización histórica Bitcoin (Bitifinex) en USD



Fuente: Bitifinex (2014)

Una gran volatilidad que alterna cambios de hasta el 600% en tan solo un mes, afectando directamente a “holders”, mineros y demás beneficiarios de esta moneda criptográfica, lo que nos lleva a plantear una serie de cuestiones: ¿No es posible que esta gran volatilidad pueda ser aprovechada en una labor especulativa, o peor aún, que sea generada por la misma?, ¿daña las cuentas de los negocios que aceptan esta moneda como método de pago?, ¿puede compensar su uso? Una cosa está clara: una gran volatilidad conlleva una gran inseguridad en el valor de cualquier activo. Y la inseguridad no ayuda a crear confianza, elemento clave y constitutivo de las monedas fiduciarias.

Nota: para más información acerca de la volatilidad de la moneda criptográfica visitar Anexo 2.

¹⁵ Nota: los valores son aproximados, y la referencias usadas son BitiStamp (<https://www.bitstamp.net>) y Bitifinex (<https://www.bitfinex.com>), las plataforma de intercambio de Bitcoins con mayor volumen de negociación a la fecha de 4 de Marzo de 2014, 35% y 26% respectivamente.

2.4) Popularidad, robos y controversias

2.4.1) *Aceptación comercial*

A pesar de lo mencionado, la moneda criptográfica, ha generado una serie de simpatizantes entre comerciantes de todo el mundo¹⁶. El número de comercios que aceptan la moneda criptográfica asciende de manera vertiginosa: inmobiliarias, diseñadores gráficos, consultorías, artesanos, joyeros... Principalmente pequeños negocios que luchan por sobrevivir y encuentran en el Bitcoin una oportunidad creativa e innovadora de diferenciarse frente a sus competidores. Alternativa que se ha extendido también a las grandes multinacionales que quieren aumentar el rango de clientes¹⁷ online. Así, desde pequeñas cafeterías en Amsterdam o Vancouver¹⁸, hasta compañías tan conocidas como Wordpress (compañía que engloba marcas líderes en la información: The New York Times, CNN, Reuters, NBC...), Domino's Pizza (a través de un servidor que verifica las transacciones llamado Pizza For Coins), The Pirate Bay, y hasta la famosa marca de ropa juvenil: Forever 21 (mediante Bitfas, servidor que gestiona y controla los pagos de diversos "retailers"). Además, Tesla y Virgin Galactic han realizado ya alguna transacción en Bitcoins, y eBay y su subsidiaria PayPal están planteándose aceptar a la moneda como método de pago, Nasdaq (2014).

El auge comercio electrónico es una realidad. Cada vez más tiendas abren espacios en la web que permitan a los consumidores adquirir sus productos. El comercio electrónico mundial superó el \$1BN en 2012, creciendo un 21.1% con respecto al año anterior. Esta cifra no ha dejado de aumentar, y se espera que en 2016 se alcance el trillón de dólares americanos (\$1,000,000,000,000) sólo en el sector del "retail", contando con claros líderes mundiales como Amazon, Alibaba o eBay, Scott Devitt (2013).

¹⁶ Lista de los comercios más importantes de la Web que aceptan Bitcoins (Nasdaq): <http://www.nasdaq.com/article/what-companies-accept-bitcoin-cm323438>

¹⁷ Lista publicada por Morgan Stanley. Fuente utilizada: <http://www.businessinsider.com/morgan-stanley-best-ecommerce-companies-2013-1#amazon-1>

¹⁸ Waves Coffe Shop, en Vancouver, posee el primer ATM que permite intercambiar moneda fiduciaria por Bitcoins y viceversa. \$100,000CAD fueron operados la primera semana (29 Octubre 2013-9 Noviembre 2013).

Gráfico 4: Capitalización de mercado BTCs (2013-2014)



Fuente: J.P. Morgan (2014)

Como se puede observar en el gráfico anterior (Gráfico 4), el volumen de capitalización de Bitcoin, ascendió a finales del 2013, en torno a los \$14,000,000,000, estando en torno a los \$6,000,000,000 en abril de 2014, constituyendo, a pesar de esta enorme bajada (dependiente de la volatilidad de su cotización), una importante oportunidad de negocio para todas aquellas empresas que participan o pretenden entrar en “el negocio de internet”. Además, el mismo estudio destaca que el e-commerce realizado mediante dispositivos móviles es, aún, una oportunidad por explotar y con altas perspectivas de beneficio. El pago de Bitcoins ya puede llevarse a cabo mediante un “app” ya desarrollado por Android.¹⁹. Por lo que puede decirse que la moneda criptográfica, supondría, en circunstancias de estabilidad de valor, una oportunidad inigualable para facilitar la captación de clientes en la web, por parte de comercios de todo tipo.

2.4.2) Bitcoin y Silk Road 2.0

Hasta ahora se ha hecho referencia a empresas y negocios aceptados por las diferentes legislaciones mundiales. Sin embargo, es momento de hacer mención

¹⁹ <https://play.google.com/store/apps/details?id=de.schildbach.wallet&hl=es>

a la “cara oscura” de lo que conlleva la privacidad absoluta y el no intervencionismo en la Web.

Silk Road original, fue un mercado negro virtual cerrado por el FBI el 2 de octubre de 2013. En este sitio Web, operado mediante el servidor Tor²⁰, se comerciaba todo tipo de productos y servicios fuera de la legalidad perteneciente al “mundo real”: desde drogas hasta falsificaciones. Una realidad paralela en la que la privacidad era el elemento más importante. El Bitcoin, no solo garantiza ésta, sino que al eliminar la presencia de intermediarios, las operaciones no serían rastreadas ni localizadas, constituyendo el método de pago ideal para este tipo de negocios.

Tras la acusar a Ross William Ulbricht como fundador y administrador de la página y cerrar la misma, el 6 de noviembre de 2013, Silk Road 2.0 aparece, para sustituir a su predecesora. Sin embargo, el 13 de febrero de 2014, Forbes publica que la Web ilegal, había sido “*hackeada*” y acumulaba una pérdida de \$2.6 MM, según predicciones de Nicholas Weaver, investigador del *International Computer Science Institute*. El administrador de la Web, declaraba en un “*Post*” que el robo se había producido debido a un fallo en el protocolo de Bitcoin llamado “*transaction malleability*”²¹.

El 15 de Abril de 2014, Charlie Shrem, Vicepresidente de Bitcoin Foundation²² era acusado por blanqueo de dinero (desde 2011) a través de la página ilegal Silk Road. La necesidad de una regulación clara y detallada de la moneda se hace notar.

²⁰ **Tor**: Servidor que garantiza el anonimato en la red. Mantiene el IP de usuario en constante cambio para mantener la privacidad y confidencialidad de sus usuarios: <https://www.torproject.org>

²¹ **Transaction malleability**: Ataque que permite a alguien cambiar el ID de una transacción de Bitcoin, antes de que sea confirmada por la red. Este cambio permite al que lo realiza, pretender que la transacción nunca ocurrió. Para más explicaciones visitar: <http://www.coindesk.com/bitcoin-bug-guide-transaction-malleability/>

²² Organización con base en EEUU, cuya actividad se basa en estandarizar el Bitcoin, protegerlo y promoverlo por todo el mundo. <https://bitcoinfoundation.org>

2.4.3) Continúan los robos: MtGox, Flexcoin y Poloniex

MtGox Exchange, constituía la mayor plataforma de intercambio de moneda criptográfica por volumen de negocio hasta el 26 de febrero de 2014, fecha en la que anunciaba su cierre indefinido y declaración de quiebra. La plataforma había sufrido una serie de “irregularidades” las semanas anteriores, que le llevaron a parar todo tipo de transacciones e impedir que sus usuarios pudiesen recuperar sus fondos. Se encontró un fallo en el sistema, que podía haber sido usado para el robo de Bitcoins y ralentizar la velocidad de compra/venta de Bitcoins en la web.

Ese mismo lunes (25 de febrero de 2014), se probó que la web se había convertido en insolvente, tras haber perdido más de \$350MM en Bitcoins, 744,408 para ser exactos. Con el fin de no agravar la situación, el CEO de MtGox, Mark Karpeles, declaró la bancarrota, acogiéndose al sistema legal japonés. Los perjudicados, en lugar de ver la situación mejorar, tuvieron que observar desde sus respectivos países (más del 90% de los mismos no eran residentes del país nipón), como el ministro de finanzas del país, Taro Aso, y su gabinete, no se decidían a determinar si era un caso constitutivo de delito o de quiebra, Peston (2014).

Fuera de cualquier resolución, el caso MtGox sigue abierto, esperando a ser solucionado. Sin embargo, el 7 de marzo de 2014 Mark Karpeles declaró que habían encontrado un monedero olvidado que contenía unos 200,000 BTCs, lo cual reduce la cantidad denunciada (como robada) por la compañía y aumenta las dudas sobre la inocencia y diligencia de la misma. Pero la cosa no acaba aquí, el 4 de marzo de 2014, semanas después del ataque y cierre de MtGox, Flexcoin, una pequeña plataforma de intercambio de Bitcoins de Alberta, Canadá, declaraba su cierre tras haber sido víctima de un ataque informático y perdido \$600,000 en Bitcoins. La imposibilidad de mantener la plataforma con suficiente liquidez les llevó a cerrar dos días después del ataque,

Joe Weisenthal (2014). Ese mismo día, al otro lado del “Charco”, Poloniex, una plataforma polaca de intercambios de la moneda criptográfica publicaba el robo de \$50,000 en BTC (un 12.3% de su volumen de negocio). En este caso, el dueño, Tristan D’Agosta, se comprometió a devolver cada uno de las unidades

robadas, pero tomando como medida de precaución la reducción del 12.3% de cada una de las cuentas que Poloniex posee, con el fin de que los usuarios no retirasen todos los fondos existentes, ocasionando la quiebra de la plataforma, Pablo Pardo (2014).

Como cabe esperar, estos sucesos ponen en “jaque” la seguridad de las carteras de Bitcoins y la confianza en el imbatible protocolo de la moneda criptográfica. Además, provoca, especialmente en el caso de MtGox, una serie de preguntas y preocupaciones en relación a su regulación y protección legal. ¿Tienen los mismos derechos aquellos que sufren un timo, engaño o robo en materia de Bitcoins, que aquellos que lo sufren en cualquier moneda fiduciaria?, ¿Serán indemnizados los perjudicados alguna vez? ¿Existe dicho fallo en el protocolo de la moneda, o fueron los administradores de Silk Road o MtGox los que se beneficiaron de los robos?

2.5) El proceso legislador

Tras lo expuesto, parece que cada vez son más los que intentan aprovecharse de este vacío legal y desarrollar actividades ilícitas a la sombra de la ley. Como era de esperar, los Países de todo el Mundo han ido cambiando y adaptando sus posturas de cara al Bitcoin. Tras los sucesivos escándalos de robos o de “blanqueo” de dinero, las autoridades mundiales han decidido clasificar a la moneda criptográfica dentro de sus regulaciones, además de recoger los delitos relacionados con la misma en sus respectivos códigos penales y civiles.

Tras el escándalo de MtGox, Japón decidió (7 marzo 2014²³) clasificar el Bitcoin dentro de la lista de “commodities” de metales preciosos, El País (2014). No podrá ser manejado por bancos nipones ni casas de valores. Su transacción y rentabilidad obtenida serán objeto de tasación y toda actividad ilícita relacionada con la moneda (lavado de dinero, evasión de impuestos...) será considerada delito, de acuerdo a la ley nipona.

²³El País http://economia.elpais.com/economia/2014/03/07/agencias/1394187181_008696.html

Se limita así la capacidad transaccional de la moneda (o en este caso commodity) y se aumenta el control sobre los fondos obtenidos por la misma. Además de adoptar este tipo de regulación, el vice ministro de finanzas del país nipón, Jiro Aichi, declaró el 27 de Febrero de 2014 (Reuters) que la regulación de la moneda virtual no debía ser aislada, sino internacional, con el objetivo de impedir lagunas legales en casos que afectases a diversos países (como el de MtGox).

Sin embargo, Estados Unidos no se ha pronunciado por una regulación clara y firme, como lo ha hecho Japón. Más cautelosos, los americanos se mantienen a la espera de la elaboración de un texto que se adapte mejor a la realidad del Bitcoin. Benjamin Lawsky, Superintendente de los Servicios Financieros de la ciudad de Nueva York plantea (12 febrero 2014) en una entrevista para CNN Money la emisión de licencias (BitLicenses) a los negocios que trabajen con Bitcoins, ofreciendo un mejor control de sus movimientos y resultados. Lawsky, cree que así aumentará la confianza a largo plazo en la moneda virtual²⁴. Incluso pioneros del Bitcoin como Barry E. Silbert, fundador de Bitcoin Investment Trust, apoyan la decisión de Lawsky, quien afirmaba a principios de ese mismo mes, que sería apropiado regular las transacciones de Bitcoin cuando estuviese involucrada alguna organización no regulada²⁵, New York State Department of Financial Services (2014). Asimismo, es conveniente tener en cuenta que la IRS emitió el 25/3/2014 un informe²⁶, que merece la pena leer, acerca del deber impositivo de cara a operaciones en Bitcoins.

En la misma línea que Japón, China declaró mediante un informe elaborado por el People's Bank of China (PBOC), que no tratarán al Bitcoin como moneda (Diciembre 3, 2013). De esta manera tanto bancos como instituciones de pago quedaban imposibilitados a operar con Bitcoins. Sin embargo, el 27 de marzo, esta prohibición era retirada, permitiendo las transacciones de la moneda criptográfica, previo registro en el Ministerio de Industria y Tecnología. Asimismo, se han publicado diversas leyes que limitan estas transacciones y que han provocado que diversas casas de trading cierren bajo amenaza de grandes multas.

²⁴ "We've found in other areas of the financial world that strong, clear, concise disclosures are critical to earning the long-term trust and confidence of consumers, and virtual currency is no exception."

²⁵ "It may be appropriate to regulate any transaction that involves an unregulated intermediary converting Bitcoin to dollars on behalf of a third party".

²⁶ Informe del Internal Revenue Service (IRS): <http://www.irs.gov/pub/irs-drop/n-14-21.pdf>

Está claro que medidas como las mencionadas, que limiten las actividades de especulación con la moneda criptográfica, pero que protejan a los consumidores, conseguirán que un mayor número de personas confíen en el Bitcoin. Pero a la vez, limita las esperanzas de aquellos que desearan una respuesta positiva a la pregunta central de este trabajo: ¿puede el Bitcoin sustituir a las monedas centralizadas y convertirse en dinero fiduciario?

Siguiendo con el aspecto legal al que se refiere este apartado, la Unión Europea sigue sin presentar legislación alguna con respecto a la moneda virtual. En octubre del 2012, el Banco Central Europeo emitió un breve estudio sobre la moneda, clasificada por algunos dentro de la Directiva 2009/110/EC²⁷. Más tarde, el 13 de diciembre de 2013 la Autoridad Bancaria Europea (ABE) destacó los problemas y peligros asociados con las operaciones de compra/venta, trading o mantenimiento de Bitcoins. De esta manera, y lejos de regular la moneda virtual, la ABE destacó que los consumidores quedan fuera de la protección legal, pero cuyas operaciones aún podrían constituir hechos impositivos, lo cual demuestra una total incertidumbre y falta de coordinación entre los países miembros.

Al mismo tiempo, algunos países como el Reino Unido o Alemania, consideran por ahora, que se trata de una moneda privada, beneficiándose de las exenciones impositivas aplicadas a este tipo de activos. Sin embargo, instituciones de ambos países demandan una regulación más exacta, que permita controlar y clasificar (tanto a nivel impositivo como penal) todas las actividades llevadas a cabo en Bitcoins.

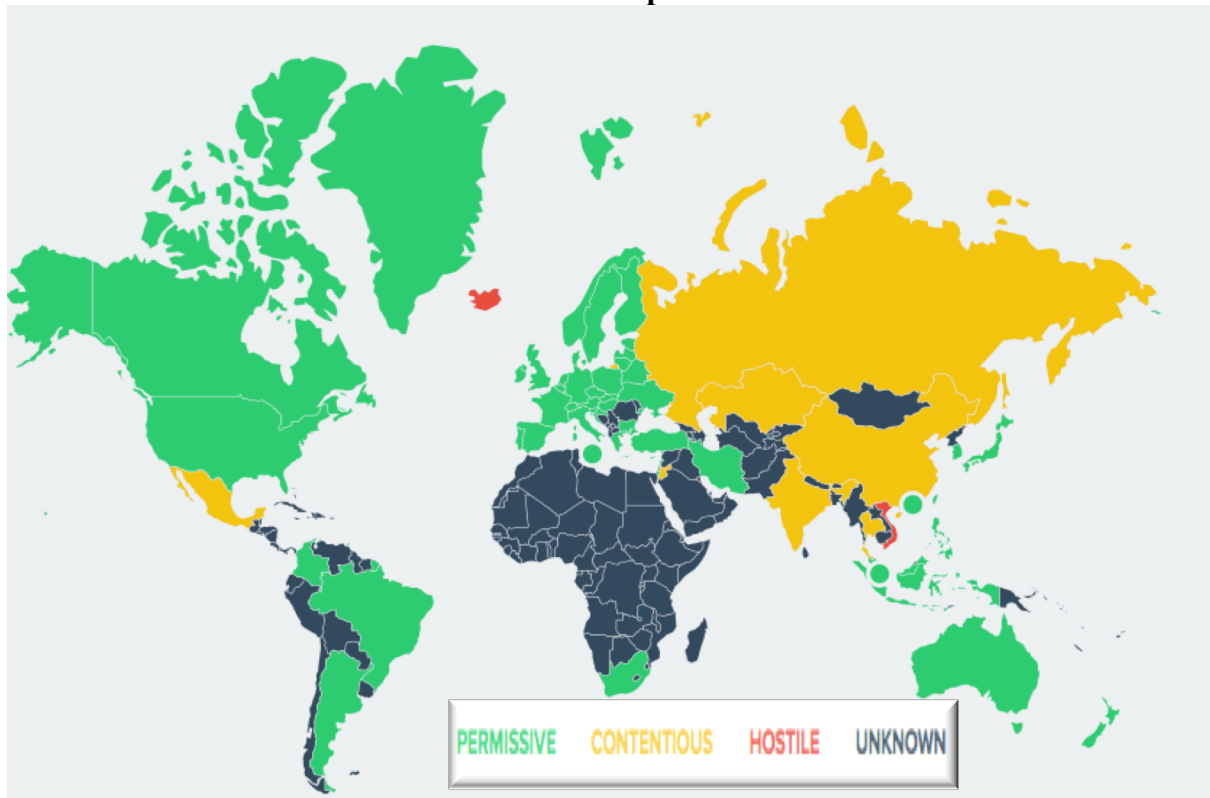
A continuación se muestra un mapa (proporcionado por BitLegal²⁸, Gráfico número 5) con todos los países del mundo y su actitud de cara al Bitcoin, con el fin de clarificar al lector sobre la situación mundial.

²⁷ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:0036:EN:PDF>

²⁸ <http://bitlegal.net> Página en continua actualización sobre los avances legales respecto al Bitcoin

A pesar de que las legislaciones mundiales estén aún algo “verdes” en el campo de la moneda virtual, la gran mayoría adoptan una clara aptitud positiva. Lo que nos indica que en un futuro el marco legal de los respectivos países irá adaptándose a este nuevo

Gráfico 5: Postura de los diferentes países de cara al fenómeno Bitcoin



Fuente: Bitlegal.net (2014)

fenómeno, clasificándolo, eso sí, como moneda privada o como commodity. Nunca como moneda fiduciaria, ya que aunque no se ha mencionado con anterioridad, la mayoría de los países europeos, asiáticos y americanos niegan la posibilidad de que el Bitcoin se convierta en una moneda como el Dólar americano o el Euro, debido a su gran volatilidad y a su falta de centralización. Así, las novedades que incorpora el Bitcoin se convierten en sus debilidades a la hora de una aceptación soberana²⁹.

Esto sostiene la opinión de Posner (2014), profesor distinguido de derecho de la Universidad de Chicago: *“The internet empowered the government rather than*

²⁹ El caso de Islandia, que restringe el Bitcoin en todo caso, se debe a un marco legal de control del capital, derivado del colapso Bancario que sufrió el país, y el Mundo en 2008.

citizens...I am therefore skeptical about the idea that bitcoin is liberating and allows people to evade government control”³⁰.

De manera que a pesar de la popularidad que está obteniendo la moneda en las redes sociales y páginas de “market places”, existen una serie de elementos legales y de seguridad que deben ser tratados antes de comenzar a considerar al Bitcoin como método de pago generalizado.

³⁰ Entrevista realizada para Goldman Sachs el 11 de marzo de 2014, en la que explica el por qué el Bitcoin nunca podrá reemplazar al dinero fiduciario como tal.

Capítulo III

Razones a favor del Bitcoin, concepto teórico

Tras haber presentado los antecedentes, el funcionamiento y la realidad del “movimiento” Bitcoin, el presente capítulo pretende exponer los argumentos y opiniones a favor de que el Bitcoin sea un sustitutivo del dinero fiduciario, y constituye un “logro” para la sociedad. Se puede apreciar que la gran mayoría de opiniones recogidas en este capítulo no tiene base científica y se basan en un concepto teórico de carácter utópico propio de revolucionarios de nuestra época, idealistas y otros simpatizantes. Sin embargo, muchas de ellas se ven respaldadas por matizaciones realizadas por instituciones de gran prestigio en el mundo financiero, como Goldman Sachs o JP Morgan Chase & Co.

A continuación se pretende en realizar una exposición progresiva, desde los argumentos fundamentados en la pasión y esperanza, a los más racionales:

3.1) Bitcoin como moneda. Latinoamérica

Numerosas han sido las voces que han abocado por la sustitución de las monedas convencionales por el Bitcoin. *“Los ciudadanos están frustrados con los políticos corruptos, un creciente estado de inseguridad y futuros económicos inciertos para la mayoría de los jóvenes”*, Ossowski (2014). Tenemos el ejemplo de Venezuela, y la continua pérdida de poder adquisitivo protagonizada por el Bolívar.

Desde 2003, la Comisión de Administración de Divisas (CADIVI) controla y limita la cantidad de dólares estadounidenses usados o intercambiados legalmente en Venezuela. Al mismo tiempo, un mercado negro paralelo permite la obtención de USD de manera ilimitada pero a un precio 14 veces mayor del legalmente establecido. *“El uso de Bitcoin como moneda podría facilitar enormemente las cosas dentro del país ya que no estaría regulado por entes estatales, y permite a sus usuarios funcionar como cajeros haciendo negociaciones de persona a persona (P2P), excluyendo a las instituciones bancarias (pago de comisiones) y los pesados trámites burocráticos a través de organismos responsables de la asignación de divisas”*. Diario Bitcoin (2014).

Al mismo tiempo, diversos países mantienen el dólar americano como moneda principal. Es el caso de Ecuador, El Salvador y Panamá en Latinoamérica. *“Estos países han entregado su soberanía monetaria a los Estados Unidos para mantener la inflación a raya, mantener precios estables e impulsar sus economías”*, Ossowski (2014), y al mismo tiempo sostiene que las criptomonedas descentralizadas (y en especial el Bitcoin) pueden devolver la integridad monetaria de estas regiones. Así mismo, la adopción del Bitcoin por estos países ratificaría la separación entre moneda y estado, descentralizando el sistema financiero y anulando todo tipo de repercusión de las políticas monetarias orquestadas por Bancos Centrales de todo el mundo: *“El dinero sería increíblemente fungible, encriptado y por siempre seguro de cualquier intromisión de burócratas gubernamentales bien intencionados”*. Además, *“Esta medida empoderaría a los más rezagados de la sociedad, dándoles mayor acceso a la tecnología que progresivamente incrementaría sus propias habilidades y su atractivo hacia futuros empleadores”*, Ossowski (2014). Aspecto que rebatiremos en el siguiente capítulo.

Para concluir, Yaël Ossowski pretende eliminar el problema de la volatilidad con la confianza general que ocasionaría que un Estado-nación adopte al Bitcoin como moneda principal. Y en parte no le falta razón. Pero, ¿quién será lo bastante “osado” para adoptar un proyecto de moneda/commodity como base de su economía? Más adelante discutiremos los problemas que arroja el hecho de considerar al Bitcoin como moneda.

Al mismo tiempo, la economista y profesora asociada Robin Tieglund (especialidad en Estrategia y Marketing) del prestigioso Stockholm School of Economics sostiene que el Bitcoin puede constituir una alternativa real al dinero convencional (en la línea del periodista Yaël Ossowski): *“Creo que ya lo es, pues las personas ya hacen negocios y transacciones cada día en todo el mundo en esta moneda. Hay al menos 60.000 transacciones en Bitcoins cada día. Yo diría que algunas comunidades la están utilizando como una forma alternativa de pago. Sé que los empresarios que lo utilizan todos los días, prefieren comerciar, comprar y vender servicios utilizando la moneda virtual. Así que cuando la gente comienza a usar y operar con esta moneda, se*

convierte ya en una alternativa diaria al dinero”³¹ Tiegländ (2014). Y es este uso y confianza en una moneda lo que le convierte en instrumento válido de intercambio, desde la caída del sistema del patrón oro o patrón dólar³². Además, “creo que una de las razones por las que Bitcoin se ha vuelto tan popular es el interés y la voluntad de las personas por desconectar el dinero de los Gobiernos. En el caso de esta divisa, el dinero es algo no controlado por ninguna autoridad central o banco. Además, los Bitcoins se pueden enviar a cualquier persona, en cualquier parte del mundo o efectuar micro pagos al instante. Así que puedo enviar un dólar a un programador en Pakistán en menos de dos minutos, mientras que una transferencia bancaria tarda un par de días y su envío puede costar unos 30 o 50 dólares más que la cantidad que me gustaría enviar”, Tiegländ (2014).

Sintetizando lo expuesto, podemos resaltar de estas dos opiniones: 1) La descentralización y faceta apolítica del Bitcoin; 2) el poder economizar transacciones y procesamiento de pago y cambio de divisa; y 3) el beneficio que ocasionaría a los “desdichados” de la sociedad.

3.2) Moneda humanitaria

Es la tercera de las ideas expuestas con anterioridad donde queremos basar este apartado. La crisis política, social y económica en la que se ve sumida Ucrania³³, ha alentado a la población a buscar medidas alternativas para financiar su subsistencia. Enviar fondos al país no es cosa fácil. Las transferencias internacionales pueden tardar días en llegar y los cambios de divisas, han albergado costes en comisiones de hasta un 7-8% (PayPal).

³¹ Texto completo en: <http://actualidad.rt.com/economia/view/116344-economista-explicacion-bitcoin>

³² Patrón oro: sistema monetario que fija el valor de la unidad monetaria en términos de una determinada cantidad de oro. El emisor de la divisa garantiza que pueda dar al poseedor de sus billetes la cantidad de oro consignada en ellos. Una alternativa es el patrón bimetálico, en el que la moneda está respaldada por una parte de oro y otra de plata. Patrón dólar, (Bretton Woods, 1944): sustitución del oro por el dólar como garantía de pago.

³³ Crisis Ucraniana: tras la negativa del gobierno de Yanukóvich de firmar el Acuerdo de Asociación con el UE (21/11/2013), más de un millón de personas tomaron el Barrio Gubernamental y derribaron una estatua de Lenin (8/12/2013). Las protestas se radicalizaron, y el país se sumió en un caos, hasta la huida de Yanukóvich (22/2/2014). La región de Crimea se separa de Ucrania y anexiona a Rusia (21/3/2014). Para más información, visitar: <http://www.rtve.es/noticias/20140414/cronologia-tesis-ucrania/881602.shtml>

Natasia Pustova y Viktor Kiyashko³⁴, quienes son voluntarios en tareas de coordinación y financiación de campañas en Kiev, comenzaron a pensar en la posibilidad de aceptar Bitcoins. Es verdad que no hay muchas comunidades donde el uso del Bitcoin esté generalizado, sin embargo, una vez en manos (o en carteras virtuales) de los ucranianos, podrán ser convertidos en la moneda local, la Grivna, RT (2014). *“La revolución viene representada por gente que está buscando nuevas ideas. Esto, y una caída del 20% en el valor de la Grivna en el último par de días podría aumentar el interés en otras alternativas monetarias”*, Roman Skaskiw (2014)³⁵.

Así, sostienen, una moneda como el Bitcoin, capaz de llegar a la región en cuestión de minutos y con un costo transaccional mínimo, podría beneficiar a todas las actividades de financiación, una vez convertidos en Grivnas. La cuestión radica en que esta medida podría usarse en cualquier situación de calamidad o crisis, aumentando la capacidad de recuperación de una región o país.

3.3) Bitcoin sustitutivo del oro y mejor que el dinero fiduciario

Hay quienes piensan en el oro como mejor moneda, que el dinero convencional emitido por el gobierno es tan solo papel al servicio de los intereses del poder político y económico.. *“It is always the government paper fiat money that gets corrupted throughout history. Bitcoin is not just a new digital currency. It is actually about liberty.”* Ken Shishido³⁶ (2014). Este apasionado de la moneda virtual, sostiene junto a los demás miembros del Tokyo Bitcoin Group, que el Bitcoin supera al oro y a la plata al constituir un activo digital, con infinitas posibilidades (no existe una autoridad central que lo controle y la oferta se encuentra limitada en 21 MM de unidades). *“Everyone here believes in bitcoin, but there are so many reasons for believing”*, dice. Wired (2013).

Resalta la independencia del Bitcoin ante instituciones Federales, la inexistencia de comisiones intermediarias de bancos y compañías crediticias; la posibilidad de conocer

³⁴ Nastasia Pustova: Directora de la campaña en Kiev, formada por 900 voluntarios. Publicista, estratega y gestora de marketing. Viktor Kiyashko: Expatriado ucraniano encargado de la recaudación de fondos y su canalización a coordinadores locales.

³⁵ Estadounidense residente en Ucrania y director de un grupo de Bitcoin en la ciudad de Lviv.

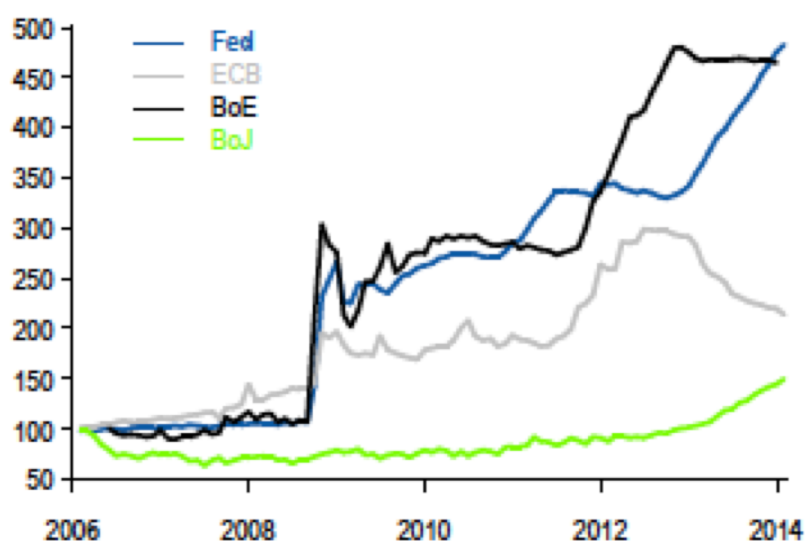
³⁶ Ken Shishido: Organizador y coordinador del Tokyo Bitcoin Meetup Group

quién gasta y en qué (los Bitcoins contienen la dirección pública de su dueño, de manera que se puede comprobar qué dirección ha estado involucrada en cada una de las transacciones realizadas con la moneda virtual. Lo que no se desvela es la identidad detrás de la cuenta). Resulta útil esta aclaración, ya que una vez regulado, el blanqueo de dinero o su uso en actividades delictivas como las descritas en capítulos anteriores, podrán verse controlados y penados, al mismo tiempo que los usuarios conservan su privacidad de cara a la actividad controladora de gobiernos o agencias internacionales. De hecho, Marco Crispini, un desarrollador británico viviendo en Tokyo, está desarrollando un programa que permitirá seguir el flujo de gasto en la red, proporcionando protección a los fondos y seguridad contra el blanqueo de dinero.

En la línea de Shishido, los miembros del Tokyo Bitcoin Group destacan la oferta limitada de Bitcoins y descontrol gubernamental, lo cual hace imposible su devaluación o reducción artificial de su valor. Además de eliminar posibles “burbujas” financieras. Esto es, los mercados no estarían pendientes de la actividad de la FED ni mantendrían expectativas sobre las políticas de la misma (*quantitative easing* o *tapering*). No se crearían subidas artificiales, y la economía se desarrollaría en un entorno más acorde con la realidad social.

Siguiendo la línea de los diferentes simpatizantes del Bitocin, un informe publicado por

Gráfico 6: Activos de los Bancos Centrales del G4 (EEUU, Zona Euro, Reino Unido y Japón). Índices con base en 2006.



Fuente: J.P. Morgan (2014)

JP Morgan Chase & Co., destaca que el Bitcoin impide el gran riesgo del problema inflacionario creado por la rápida expansión del balance de los grandes bancos mundiales (Gráfico 6), además de prevenir la imposición de controles de capital por instituciones internacionales a países soberanos, JP Morgan (2014).

Asimismo, el informe destaca, la habilidad de la moneda para mantener un constante y predecible crecimiento de su oferta³⁷; la verificación instantánea del balance de fondos (para reducir fraudes); y su reducido coste transaccional.

Por lo tanto, y tras lo dicho, Bitcoin (partiendo de la opinión de sus defensores) contiene una serie de ventajas:

- No está sujeto a una institución gubernamental o privada. Carece de carácter político, y su creación no depende de intereses económicos o financieros. Se impiden los controles de capital impuestos a países soberanos, por organismos internacionales.
- Transacciones baratas y rápidas: más baratas que el 3-5% que cobraría una gestora de tarjetas de crédito. Y en minutos (50 min. son necesarios como máximo para que se verifiquen todos los bloques de la transacción y se impida el doble gasto).
- No existe burocracia a la hora de trabajar con este tipo de moneda, no requiere unas pruebas de identidad, residencia o bienes como para abrir una cuenta en un banco. Es fácil de transportar, a diferencia del oro o el papel moneda, el dinero virtual puede llevarse en cualquier dispositivo electrónico³⁸.
- Su valor no deja de aumentar (al poseer una oferta limitada a 21 MM de unidades), por lo que elimina el riesgo inflacionario, generado por políticas como el “*quantitative easing*”.

³⁷ La oferta de Bitcoins se encuentra determinada por el protocolo inicial. Actualmente existen unos 12 millones de Bitcoins y el ratio de creación por cada 10 minutos es de 25 unidades. Cada cuatro años la creación es reducida a la mitad, por lo que se espera que se alcance los 21 MM en el 2040

³⁸ Nota: el dinero convencional también es usado virtualmente, por lo que el Bitcoin no supondría ninguna ventaja ni novedad.

Capítulo IV

Razones en contra del Bitcoin, evidencia empírica

En este capítulo el lector dispondrá de una serie de opiniones publicadas por expertos en los mercados y el sector económico/financiero (miembros de GS, JP Morgan, Bank of America, New York University y el National Bureau of Economics Research) acerca de la moneda virtual. El Bitcoin es atacado como sustitutivo de la moneda convencional o fiduciaria, pero ensalzado, a su vez, como alternativa innovadora en método de pago.

Se ha mencionado con anterioridad que algunos países han clasificado al Bitcoin dentro del apartado “commodity”, quitándole su esencia monetaria inicial. A continuación se muestran las desventajas de la moneda virtual como dinero fiduciario, justificando la precavida decisión de los mismos. El dinero es considerado como tal gracias a unas cualidades intrínsecas que le hacen único y diferenciable frente a otros activos.

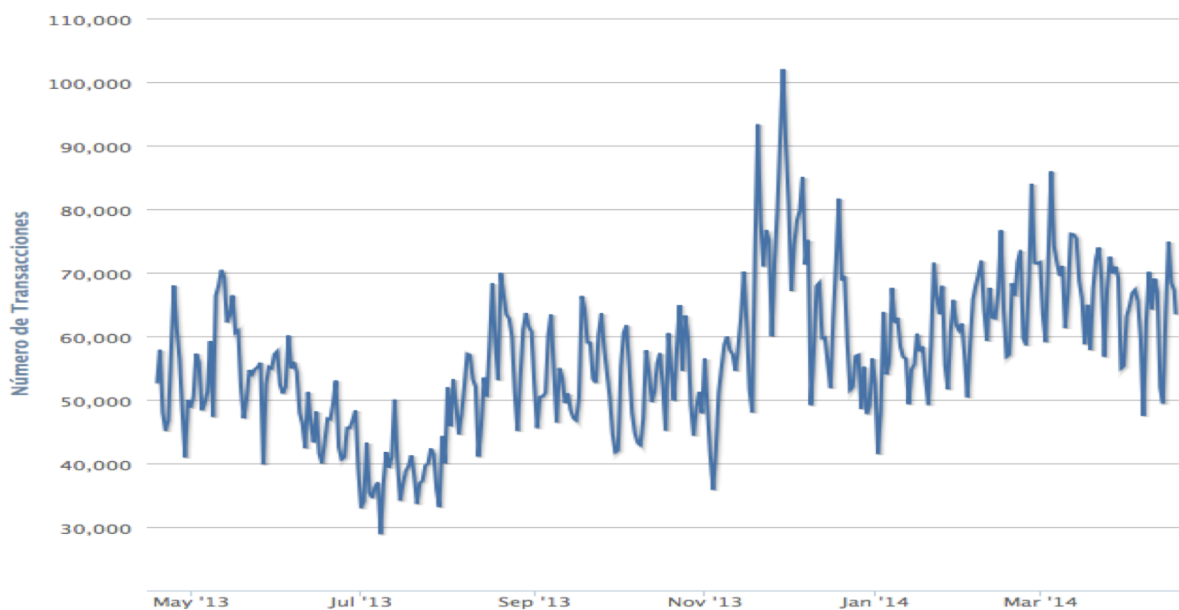
4.1) Medio de cambio

En primer lugar, a pesar de la creciente oferta de comercios que aceptan el pago mediante Bitcoins, la gran mayoría consisten en compañías enfocadas a la venta software o hardware; suministro de productos relacionado con la moneda criptográfica y plataformas de cambio y gestión de Bitcoins. No hay una cantidad significativa de comercios (diferenciados) que los acepten como medio de pago (por ahora), David Yermack (2014)³⁹.

Además, resaltando la actividad de las plataformas de cambio y gestión de Bitcoins, la especulación de la moneda es algo preocupante. De las aproximadas 65,000 transacciones (Gráfico 7) ocurridas a lo largo del mes de abril de 2014, el 80% corresponde a especulación, mientras que el 20% restante a pagos reales

³⁹ Profesor de Finanzas y Transformación de Negocios del New York University Stern School of Business, desde 1994. Sus obras han sido publicadas en diferentes revistas académicas como *Journal of Financial Economics*, *Journal of Finance*, and *Journal of Law, Economics, and Organizations*.

Gráfico 7: Número de transacciones por día (BTC)



Fuente: Blockchain.info (2014)

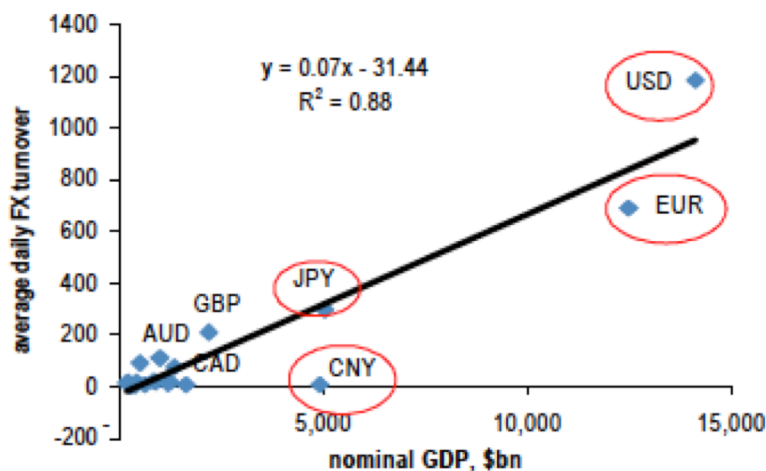
Conjuntamente, de acuerdo con Fred Ehrsam, Cofundador de Coinbase⁴⁰, se calcula que en años anteriores la cifra especulativa habría rondado al 95% de las transacciones totales. Es frecuente observar como hasta los más “apasionados” y defensores de la moneda virtual desarrollar sus propias estrategias para especular en el mercado de Bitcoins⁴¹, Goldman Sachs (2014).

Asimismo, Bitcoin no presenta, en este campo, ventaja alguna con respecto a las monedas convencionales. Cualquier cosa portable (monedas, billetes, carteras electrónicas, tarjetas de crédito...) puede ser utilizada como método de pago si comúnmente está aceptado por la sociedad. El Bitcoin carece de una autoridad gubernamental o supranacional capaz de promover el uso de esta moneda, o de establecerlo legalmente. Por ejemplo, el dólar y el euro se encuentran en una situación de primacía debido a que son respaldados por las economías y mandatos legales de dos potencias mundiales como EEUU y la Eurozona (Gráfico 8), Bank of America (2013) y JP Morgan (2014).

⁴⁰ Cartera y plataforma de Bitcoins donde comerciantes y consumidores pueden negociar y realizar transacciones con la moneda virtual

⁴¹ <https://bitcointalk.org/index.php?board=57.0> / <http://blogs.marketwatch.com/cody/2013/11/20/some-bitcoin-trading-and-investing-strategies-as-prices-swing/> / <http://www.reddit.com/r/BitcoinMarkets>

Gráfico 8: “Algunas monedas son usadas internacionalmente debido al poder de algunos gobiernos”, John Normand (2014)



PIB Nominal (**eje de X**) frente a la media intradía del volumen de negociación del mercado de FX, por moneda en comparación con todas las demás (**eje de Y**).

Fuente: JP Morgan, BIS (2014)

Con el fin de fortalecer el argumento anterior supongamos que todos decidimos operar con Bitcoins, aceptando la moneda como unidad de cambio internacional. Surgiría un problema de disposición de Bitcoins. Aquellos que no posean (porque no tengan acceso o no puedan costearlo) las capacidades tecnológicas requeridas para minar Bitcoins, deberán de obtener los mismos mediante plataformas online. Así, 7 Bn de personas desearían obtener Bitcoins, aumentando su demanda online, e inflando su valor de manera exorbitante (además de sumar el efecto negativo producido por la baja liquidez al no existir un mercado de productos derivados y de los altos *spreads*), sin que ninguna institución pudiese poner freno aumentando la oferta monetaria, y devaluando su valor. Y aunque la hubiese, y suponiendo que los gobiernos de todo el mundo pusiesen su capacidad tecnológica a disposición de la minería de Bitcoins, la cantidad límite es de 21 MM de unidades, insuficiente para abastecer una demanda mundial (aquellos con más recursos serían capaces de mantener su posición, mediante la compra o producción de un mayor número de unidades⁴², mientras que los desfavorecidos, quedaría atrapados en su situación para siempre).

⁴² Según un artículo publicado por Bloomberg el 16 de Abril de 2014, en los 5 años desde que Bitcoin fue creado, se ha consumido suficiente electricidad en los procesos de creación (“mining”), como para mantener encendida 260 años la Torre Eiffel. Un coste desorbitado para la producción de 12MM de unidades.

Finalmente, el Bitcoin no permite la compra a crédito. En la sociedad de la deuda en la que vivimos, es difícil imaginar la inexistencia de pago aplazado, o de financiación mediante apalancamiento (financiero). Siempre nos han enseñado que la financiación más barata es la que se hace mediante deuda, y que si obtenemos una rentabilidad mayor que el coste de esa deuda, todo son ventajas. Con el Bitcoin, este sistema no tiene sentido. Los pagos serán inmediatos y las ventajas de financiación: inexistentes, David Yermack (2014).

4.2) Unidad de cuenta y de valor

A menos que la moneda virtual cumpla estas dos funciones (a falta de la anterior), su uso se vería limitado considerablemente. Sin embargo, el Bitcoin no cumple con estos dos requisitos propios del dinero convencional.

La excesiva volatilidad en la que hacíamos hincapié en el Capítulo II, se convierte en un problema a estas alturas del estudio. Bitcoin ha tenido una volatilidad media del 120% los pasados 3 años (con rasgos que van desde 50% al 400%). Comparado con el 8% (rangos de 7-16%) experimentado por las divisas propias del G10 o el 9% de los mercados emergentes (rangos de 7-20%), constituye una cifra desorbitada, JP Morgan (2014).

Incluso, comparándolo con la volatilidad de compañías “start-up”, la cifra resulta mucho mayor. Como se pudo observar en el Gráfico 9, el Nasdaq (con la burbuja de las puntocom) quintuplicó su valor en 3 años (1997-2000), mientras que el Bitcoin ha doblado más de 50 veces el suyo en tan solo 12 meses (Gráficos 2 y 3).

Así, la volatilidad se convierte en un problema para la población al no saber lo que podrán comprar en un futuro cercano con Bitcoins. Como apuntan Dominic Wilson y Jose Ursua de GS Markets Research, la volatilidad impide la estabilidad de la moneda, y aunque, como se resaltaba en la primera parte de este capítulo, el Bitcoin limita el efecto negativo de la inflación; en la mayoría de las economías, mencionado problema ha dejado de ser común y lo que los consumidores buscan es cierta estabilidad en el valor de las divisas con las que operan, Goldman Sachs (2014).

Gráfico 9: Histórico del Nasdaq

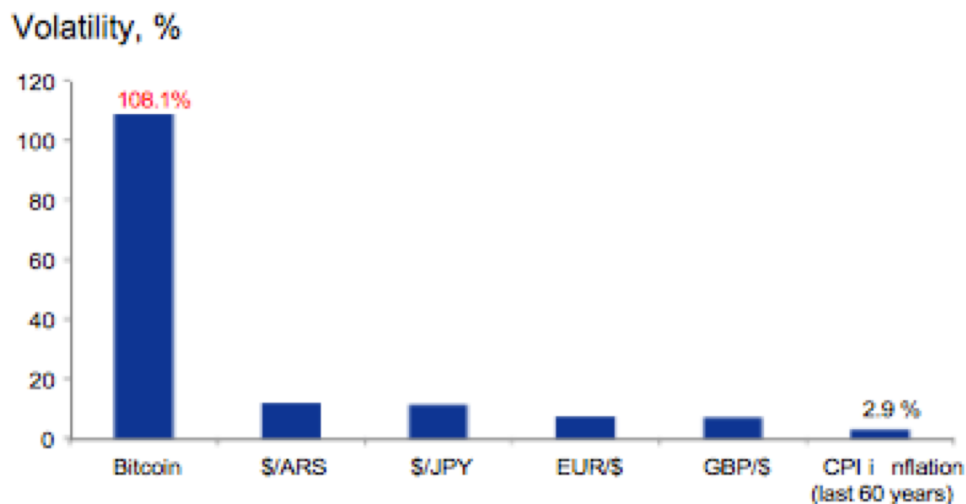


Fuente: Yahoo Finance (2014)

Haciendo referencia a la moneda como unidad de valor: Alguien que posea dólares o euros hoy mismo, estima y espera poder obtener el mismo valor económico (o parecido) una vez gaste dichas unidades monetarias. Además, espera tenerlas en un seguro hasta su consumo (Banco, caja fuerte, o debajo de un colchón). Sin embargo, esto no es posible con Bitcoin. En primer lugar, debido a su alta volatilidad (Gráfico 10), a que su oferta no puede ser controlada y no existe organización capaz de mantener su valor estable. En segundo lugar, los Bitcoin deben de ser almacenados en carteras virtuales, las cuales carecer de plena seguridad (revisar capítulo II, apartado de MtGox y otros robos).

De la misma manera, los comerciantes de un país en el que el Bitcoin fuese aceptado como moneda de pago, deberían recalcular el precio de sus productos a cada momento (de acuerdo a los cambios de mercado), lo cual resultaría costoso para el comerciante y confuso para los clientes. Este no es el caso, ya que ningún país acepta de manera amplia el Bitcoin como método de pago, sin embargo la volatilidad también ha tenido efectos negativos en la integración de la moneda en transacciones comerciales.

Gráfico 10: Volatilidad del Bitcoin vs. otra divisas e inflación (últimos 60 años)



Fuente: Goldman Sachs Global Investment research (2014)

Un informe publicado por Merrill Lynch en diciembre de 2013 demostraba la relación inversa entre la volatilidad del valor de Bitcoin y el número de transacciones comerciales realizadas con el mismo (visitar Anexo 3).

4.3) Otras objeciones

Se destaca la falta de liquidez del mercado de Bitcoin. Actualmente existen 12 MM de Bitcoins. En un rango de valor de \$500-\$1300⁴³, la capitalización del mercado se encontraría entre los \$6Bn y los \$156Bn⁴⁴ (con un valor de \$20MM en transacciones diarias). Frente a los \$1.2 trillones, EUR950 billones y GBP360 billones (con valores de \$34Bn para los Euros y \$10Bn para las Libras⁴⁵); el mercado de Bitcoins es relativamente pequeño y poco líquido (Gráfico 11), con todos los problemas que ello acarrea, Merrill Lynch (2013).

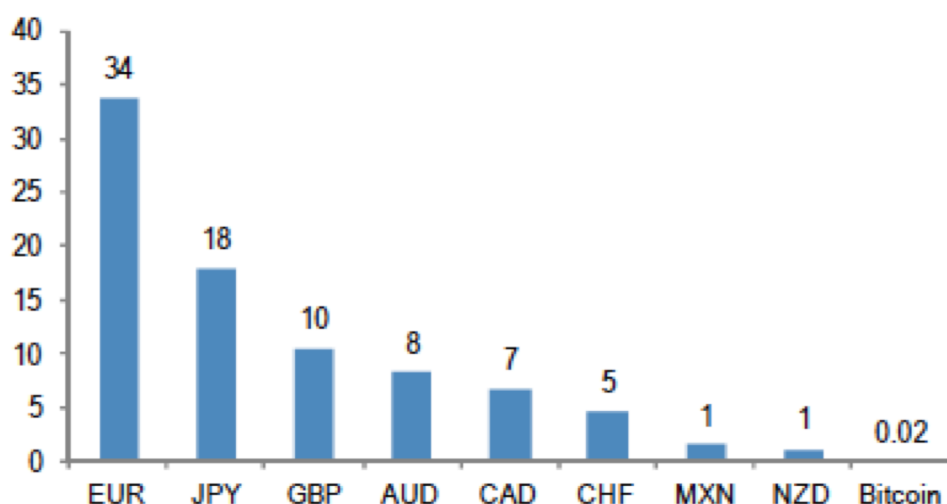
⁴³ Rango de valor, cuyo mínimo corresponde al valor inferior teórico no superado desde Enero del 2014, y cuyo máximo corresponde al valor real asignado por Merrill Lynch el 5 de Diciembre de 2013.

⁴⁴ La cifra real sería mucho inferior, ya que parte de los 12 MM de unidades se han perdido y otra gran cantidad se encuentra parada.

⁴⁵ Volúmenes correspondientes al Chicago Mercantile Exchange

Es más, muchos de los que tiene Bitcoins, pretenden mantener los mismos hasta que la moneda alcance un mayor valor: al haber una oferta limitada, es sistemático que la demanda de la misma se vea incrementada (si todo va bien, y la población no pierde el interés en la misma), aumentando su valor considerablemente.

Gráfico 11: Volumen medio de negociación diario de las diferentes divisas en el Chicago Mercantile Exchange (en USD Bn).



Fuente: J.P. Morgan (2014)

Además, las sucesivas medidas e intenciones regulatorias por parte de los países para con la moneda virtual puede evolucionar a un incremento de los costes transaccionales. Hemos visto que los gobiernos están tomando precauciones ante la posibilidad de que la moneda sea usada para financiar actividades ilegales o para evadir impuestos. De esta manera, la inclusión de la moneda, dentro del marco impositivo (como Japón o EEUU), aumentaría los costes de usarlo, anulando la gran ventaja de la moneda virtual: su economía transaccional de bajo costo. Lo cual limitaría aún más su utilidad como medio de cambio.

Por otro lado, surgen los incentivos gubernamentales de eliminar al Bitcoin, en caso de extenderse demasiado. El señoreaje (o ingresos que obtiene el gobierno al “producir” dinero) constituye, en el caso de Estados Unidos, una considerable fuente de ingresos, la cual se vería reducida por la producción de Bitcoins. El incremento de beneficios iría dirigido a los mineros encargados de producir Bitcoins, y por tanto, en caso de una expansión desorbitada de la moneda virtual, constituiría un mayor problema para los entes gubernamentales, que probablemente encontrarían la manera de controlarlo.

El último de los problemas que se destacará en esta sección será el de seguridad. El recibo de confirmación de pago, en una operación de Bitcoins, tarda 50 min. En este tiempo, diferentes bloques son añadidos a la cadena, para proteger la transacción de un doble gasto. Ninguna tercera parte se encarga de controlar la transacción y por tanto de garantizar la seguridad de su consecución, lo cual ya genera algo de riesgo. Pero tras conocer los casos expuestos en el segundo capítulo acerca de los robos llevados a cabo en organizaciones especializadas como Mt Gox o Fexcoin, no cabe duda de que el fenómeno llamado “*transaction malleability*” se repita frecuentemente.

Así, el Bitcoin supone: a) Un riesgo para comerciantes, ya que a pesar del ahorro en comisiones, su excesiva volatilidad, y falta de liquidez, constituyen un mayor problema que no proporciona flexibilidad financiera alguna (como el dinero convencional líquido) al negocio; b) Un riesgo para consumidores; c) Y que los inversores intenten no invertir en productos relacionados con dicha moneda electrónica, debido a su incertidumbre de futuro y a la imposibilidad de calcular la tendencia de su valor, John Normand 2014)⁴⁶.

4.4) ¿Mejor que el oro?

Hasta aquí hemos mencionado algunos de los argumentos que descalifican al Bitcoin como moneda, sin embargo, ante la clasificación del mismo dentro del rango de metales preciosos (Japón), y la concepción de algunos (Ken Shishido) como mejor “commodity” que el oro, se van a presentar una serie de argumentos que ponen en entredicho a esta idea.

Una “commodity” o mercancía, es cualquier producto destinado al uso comercial. Productos que satisfacen parte de nuestras necesidades y deseos, como la necesidad de protección o depósito de una reserva de valor. A lo largo de la historia, los humanos han utilizado todo tipo de materiales y productos agrícolas como reserva de valor (desde las especias, pasando por el café hasta el oro). Buscando siempre, cual satisfacía mejor sus necesidades y pudiese reemplazar a la anterior “mejor commodity”. Así, el carbón

⁴⁶ Director de Global FX Strategy en JPMorgan.

reemplazó a la madera, el petróleo al carbón, y el oro a todos ellos considerándose el valor refugio y reserva de valor por excelencia.

Una vez planteado a lo que nos referimos con el término “commodity”, debemos preguntarnos si el Bitcoin supera o reemplaza de manera decisiva al oro como tal, de manera que podamos confirmarlo como la nueva reserva de valor del siglo XXI. Para ello, y siguiendo con el argumento de Jeff Currie (2014) (Director de GS Commodities Research), hay que estudiar los atributos que deben de poseer:

- a) Estabilidad y carencia de sustitutos:* El oro, considerado como uno de los metales menos reactivos en su forma sólida, superó hace tiempo a otros metales como la plata o el platino, en objeto de inversión. El Bitcoin, sin embargo, carece de una gran estabilidad (el hecho de ser una moneda electrónica y virtual, le hace depender de los software usados para su verificación (en transacciones) por la mayoría de sus productores (mineros). Un cambio en el mismo podría alterar su codificación, rechazando antiguas versiones del mismo. Además, a pesar de que sus competidores (Litecoin o Dogecoin⁴⁷) no estén tan popularizados, podría surgir una nueva versión de la moneda virtual que mejorase y perfeccionase las debilidades propias del Bitcoin.
- b) Facilidad de almacenamiento:* Como cabe esperar, la facilidad de almacenamiento del Bitcoin supera a la del oro, debido a su carácter virtual. La densidad de oro, que ha hecho que gane ventaja sobre otros metales en este aspecto, no puede competir con el bajo coste que supone el mantenimiento y almacenamiento de los Bitcoins.
- c) Garantía frente a conflictos/catástrofes:* El oro se mantendría como líder, ya que el Bitcoin radica en la existencia de Internet. En el caso del peor escenario (Tercera Guerra Mundial, desastre natural mundial...) es probable que la red cayese y que a la energía disponible se le diese otro uso (coste de oportunidad).

⁴⁷ BBC (22/1/2014)

http://www.bbc.co.uk/mundo/noticias/2014/01/140122_tecnologia_monedas_digitales.shtml

d) Volatilidad: Por último, la volatilidad propia de la moneda virtual vuelve a ser causa de discordia. La variación excesiva de la demanda del Bitcoin, con su respectiva alternancia en su valor, hace que los beneficios de invertir en esta “commodity” se vean reducidos. El oro, por otro lado, mantiene una demanda previsible y parcialmente estable.

Por lo tanto, encontramos, que a pesar de la facilidad de uso y almacenamiento del Bitcoin; la estabilidad, predictibilidad y la carencia de substitutivos, hacen que el oro mantenga su carácter de reserva de valor más fiable.

Asimismo, y tras haber analizado numerosos argumentos correctores del uso como moneda o valor refugio del Bitcoin, podemos concluir:

- La alta volatilidad del Bitcoin perjudica a comerciantes y consumidores, al suponer un alto riesgo en el mantenimiento del valor pagado o recibido. Además, imposibilita al Bitcoin como unidad de cambio o de valor.
- Su carácter apolítico y liberal (no sujeto a ninguna institución que lo respalde) imposibilita la compra a crédito (apalancamiento financiero), reduce la seguridad de las transacciones e impide la reclamación ante robo o pérdida.
- El bajo costo de sus transacciones puede aumentar en el momento en el que se regulen por Gobiernos u otras instituciones supranacionales. Incentivados por los casos de financiación de actividades ilegales, blanqueo de dinero y la reducción del señoreaje.
- El pequeño número de transacciones comerciales frente al gran movimiento especulativo, impiden la estabilidad de la moneda e inducen a la desconfianza sobre la moneda. Además, el alto coste tecnológico y energético de producción limita el acceso al mercado a la mayoría de personas.

- Las carencias de estabilidad y predictibilidad, además de la emersión de posibles substitutos hacen que el Bitcoin reduzca su impulso en el mercado de “commodities”, no pudiendo reemplazar al oro como valor refugio.

Conclusiones y futuras líneas de investigación

El objetivo fundamental de este trabajo ha sido el de estudiar la situación del Bitcoin en nuestro entorno y el de determinar su viabilidad como moneda alternativa al dinero fiduciario, propio del sistema monetario actual. A lo largo de la investigación se ha ido dibujando un mapa conceptual que sitúa en un punto central al fenómeno estudiado: el Bitcoin. En torno al mismo, se han trazado una serie de circunstancias, características, conceptos e ideas que lo envuelven, formando, lo que se ha querido denominar como “la realidad del Bitcoin”. Siguiendo con la metodología empleada, se ha sometido a examen esta realidad, cuestionando mediante la evidencia empírica, que la moneda criptográfica pudiese llegar a ser considerada como dinero (fiduciario).

Tras ofrecer una breve introducción histórica y social, se ha podido comprobar como el Bitcoin tiene un importante matiz ideológico y conceptual, cuya creación está fuertemente ligada a los movimientos anti sistema surgidos como consecuencia del deterioro institucional y pérdida de credibilidad que sufren las organizaciones gubernamentales e internacionales a lo largo del Globo. La idea generalizada que abarca esta “realidad” a la que antes se hace referencia, no es otra que la separación de los sistemas financiero y económico del centralismo que actualmente rige en el Mundo. La sustitución de las monedas fiduciarias vigentes por una moneda capaz de eliminar del sistema monetario cualquier vestigio político, institucional o centralista.

No obstante, detrás de los ideales propios de este movimiento existe una complejidad técnica que se ha tratado de explicar y delinear a lo largo de la obra. Esta complejidad ofrece una serie de ventajas con respecto al diseño transaccional de las operaciones de pago y cobro del sistema actual, repletas de intermediarios. Así, el Bitcoin ofrece la posibilidad de eliminar estas instituciones en las transacciones de pago o transferencia, por lo que reduce el coste y aumenta la velocidad de las mismas (hasta 216 veces más rápido). Además, su carácter descentralizado permite eliminar los controles de capital impuestos por instituciones supranacionales o nacionales. Los casos de Venezuela y Ucrania ejemplifican estos puntos.

Su carácter independiente y su limitada oferta (21MM de unidades) permiten eliminar la posibilidad de devaluación de la moneda y frenar el problema inflacionario. Lo que en teoría, ayudaría a mantener constantes las expectativas del mercado, descartando la formación de burbujas especulativas y el problema de las expectativas fallidas. Además, su almacenamiento y capacidad de uso superarían al oro como activo refugio.

Sin embargo, y tras haber sometido a la moneda virtual a examen, descubrimos que muchas de sus ventajas se pueden convertir en argumentos en contra de la misma. El hecho de no estar respaldado por ninguna organización pública o privada, conlleva un descontrol que puede perjudicar a los usuarios del Bitcoin, ya que nadie verificará que las transacciones realizadas no son intervenidas por un tercero (hacker) o malversadas. Casos como los de MtGox o Poliniex lo justifican. Tampoco se podría controlar la oferta de la misma, ocasionando una revalorización de la moneda que imposibilitaría el acceso al sistema monetario a los menos favorecidos. Las mayores fortunas invertirían en la moneda o en su creación, mientras que los realmente necesitados se hundirían en una espiral de pobreza mayor que la que sufren actualmente. De esta manera los ideales iniciales se podrían ver corrompidos, o más bien descartados de “la realidad del Bitcoin”.

Esta limitada oferta es, además, causante de una liquidez escasa y de fomentar el ahorro, limitando la inversión. Ya que si esperamos que una cartera de Bitcoins se revalorice indefinidamente, se tenderá a no gastar ninguna unidad, esperando un mayor valor en el futuro. Se reduciría la inversión, el consumo y aumentaría el ahorro, con todo lo que ello conlleva para las economías del planeta.

Además, a lo largo del trabajo se ha comprobado que la moneda criptográfica no supone una mejora en lo que a medio de cambio o método de pago se refiere. El número de comercios que la aceptan como tal, aunque en aumento, es muy pequeño, y queda limitado a actividades de compra y venta de software o hardware (mayoritariamente). El 80% de sus transacciones constituyen actividad especulativa, y tan solo un 20% está destinado a la compra o venta de los servicios antes mencionados. No existe, por ahora, una conciencia generalizada que adopte al Bitcoin como medio de intercambio.

La excesiva volatilidad de la moneda (acrecentada por la alta actividad especulativa) perjudica a comerciantes y consumidores: Eleva los costes comerciales de actualización de precios de productos y da lugar a una confusión generalizada y a una pérdida de credibilidad hacia el “nuevo sistema” por parte de los consumidores (ya que no es lo mismo que un producto o servicio cueste 40 Bitcoins, cuando la cotización de la moneda sea de USD 1,000 a que lo sea de USD 600). Por todo esto, tampoco puede considerarse unidad de valor o de cuenta, requisitos indispensables para configurarse como dinero fiduciario.

Otro de los inconvenientes que nos lleva a rechazar la moneda como tal es que su popularización haría que las instituciones gubernamentales de todos los países tendiesen a regular y legislar cualquier actividad que ocasione un vacío legal en el sistema. Este ha sido el caso del Bitcoin, dónde su regulación tiende a aumentar los bajos costes transaccionales del mismo (y que en un principio constituían una clara ventaja frente a la participación de intermediarios). Además, el hecho de que la creación de dinero constituya una de las principales fuentes de ingresos para economías como la de EEUU, incrementa las posibilidades de que su regulación se convierta en una prohibición o “*boicot*”.

Por lo tanto, y después de lo expuesto, podemos concluir que habiendo cumplido con la finalidad del trabajo: se rechaza al Bitcoin como posible moneda fiduciaria y se desmienten las concepciones más ideológicas que engloba la moneda. Es incompatible con la realidad social, económica y política en la que vivimos, y tampoco ofrece una perspectiva de mejora real.

Futuras líneas de investigación

Sin embargo, como se ha expuesto, el Bitcoin ofrece la posibilidad de incrementar la velocidad en las transacciones, constituye una mejora con respecto al oro en el uso y almacenamiento y su situación privilegiada frente a sus competidores (muy lejos de igualar su popularidad y características) dejan una puerta abierta a futuras investigaciones y aplicaciones.

En este trabajo se quiere hacer constar que el Bitcoin constituye un fenómeno novedoso y creativo, y cuyo campo de aplicación puede estar dirigido a su uso como “commodity” refugio o como medio de ayuda ante posibles catástrofes (por su gran velocidad de transacción), ayudado siempre por una fuerte regulación que reduzca su volatilidad, asegurando una estabilidad y predictibilidad confiables.

Bibliografía

Arancón, Fernando (2013), *Los Bitcoin, la moneda de la interneteconomy*, elOrdenMundial, 14 de Diciembre de 2013, <http://elordenmundial.com/economia/los-bitcoin/> [1 de Mayo 2014]

Bank of America Merrill Lynch (2013), *Bitcoin a first assessment*, FX and Rates Global, 5 de Diciembre de 2013 <https://ciphrex.com/archive/bofa-bitcoin.pdf> [30 de Mayo 2014]

Bank of Japan (2014), “Main Time-series Statistics”. Disponible en <http://www.stat-search.boj.or.jp/ssi/mtshtml/fy_en.html>. [1 de Mayo 2014]

Bitstamp (2014) <https://www.bitstamp.net> visitado el 30 de Marzo de 2014

Bitfinex (2014) <https://www.bitfinex.com/pages/stats> visitado el 30 de Marzo de 2014

Cosgrove-Sacks, Carol y Dembinski, Paul H. (2012), “Trust and Ethics in Finance: Innovative ideas from the Robin Cosgrove Prize”, Globethics.net pp. 257-259

Deborah J. MacInnis (2011), “A Framework for Conceptual Contributions in Marketing”, Journal of Marketing Vol. 75, pp. 136-141

Diario Bitcoin (2014), *Manifestantes en Ucrania se manifiestan a favor de Bitcoin para contrarrestar la crisis económica*, disponible en <http://www.diariobitcoin.com/index.php/tag/otestas/> [4 de Mayo, 2014]

Espina, Álvaro (2004), *Sobre estabilidad de precios, deflación y trampas de liquidez en el G-3* Real Instituto Elcano de Estudios Internacionales y Estratégicos No.3, pp. 20-28

Financial Trust Index (2014) *Chicago Booth Kellogg School*, <http://www.financialtrustindex.org/> [24 de Mayo 2014]

- Gans, Joshua S. y Halaburda, Hanna** (2013), "Some Economics of Private Digital Currency". Rotman School of Management Working paper No. 2297296. 23 de Julio del 2013.
- Goldman Sachs** (2014), *Top of Mind*, Global Macro Research, No.21 <http://www.paymentlawadvisor.com/files/2014/01/GoldmanSachs-Bit-Coin.pdf> [30 de Mayo 2014]
- Grinberg, Reuben** (2011), "Bitcoin: An Innovative Alternative Digital Currency", Grinberg 110.docx Vol. 4:1
- Gunn, Dwyer** (2010), "Predicting the Financial Crisis: A Q&A With Fault Lines Author Raghuram Rajan", The New York Times, June 17.
- Ian Kar, Bezinga** (2014), "What Companies Accept Bitcoin?", Nasdaq. Disponible en <http://www.nasdaq.com/article/what-companies-accept-bitcoin-cm323438>. [20 de Mayo 2014]
- J.P. Morgan** (2014), *The audacity of Bitcoin, Risks and opportunities for corporates and investors*, Global Rates & FX Research
- Kar, Dev y LeBlanc, Brian** (2013), "Illicit Financial Flows from Developing Countries: 2002-2011", Global Financial Integrity <http://www.gfintegrity.org/press-release/study-finds-crime-corruption-tax-evasion-drained-946-7bn-from-developing-countries-in-2011/> [4 de Mayo, 2014]
- Lindbeck** (1998), "A. New keynesianism and aggregate economic activity", Economic Journal, Royal Economic Society, Londres 1998
- Metz, Cade** (2013), "For Bitcoin's Biggest Believers, Digital Currency Is Better Than Gold", Wired. Disponible en <http://www.wired.com/2013/10/bitcoin-in-japan/>. [22 de Mayo 2014]
- Morgan Stanley** (2013), "eCommerce Disruption: A Global Theme. Transforming Traditional Retail". Disponible en http://www.rundlemall.com/bm.doc/ecommerce_bp0106131.pdf. [20 de Mayo 2014]
- MtGox** (2014), *Bitcoin prices* <https://www.mtgox.com> visitado el 20 de Febrero de 2014.

New York State Department of Financial Services (2014), *Written Testimony of Barry E. Silbert Founder and CEO, SecondMarket; Founder, Bitcoin Investment Trust*, 28 De Enero del 2014 http://www.dfs.ny.gov/about/hearings/vc_01282014/silbert.pdf, [30 de Mayo 2014]

OECD (2014), *Economic challenges and policy recommendations for the euro area*, Better Policies Series, pp. 5-18

Ossowski, Yaël (2014), “Latin-American Countries Should Ditch the Dollar for Bitcoin”, PanAm Post, 25 de Febrero. Disponible en < <http://panampost.com/yael-ossowski/2014/02/25/latin-american-countries-ditch-dollar-bitcoin/>>. [21 de Mayo 2014]

Pardo, Pablo (2014), “Nuevos robos de mercados de bitcoin”, 4 de Marzo de 2014, <http://www.elmundo.es/economia/2014/03/04/53162e8022601d3e638b4586.html> [1 de Mayo 2014]

Peston, Robert (2014), “Top Bitcoin exchange MtGox goes offline” BBC news, 25 de Febrero del 2014, <http://www.bbc.com/news/technology-26333661> [1 de Mayo 2014]

Rahmani, Teymur y Yousefi, Hana (2009) “Corruption, Monetary Policy, and Inflation: A cross-Country Examination”, pp. 10-15 accedido en <http://dmk.ir/Dorsapax/userfiles/file/Corruption,%20Monetary%20Policy,%20and%20Inflation%20A%20Cross-Country%20E.pdfm> [21 de Mayo 2014]

RT (2014), “Una economista explica todo lo que tiene que saber sobre el bitcóin”, 7 de Enero de 2014, <http://actualidad.rt.com/economia/view/116344-economista-explicacion-bitcoin> [3 de Mayo 2014]

Russo, Thomas A. and Katzel, Aaron J. (2010), “The 2008 Financial Crisis and Its Aftermath: Addressing the Next Debt Challenge”, Group of Thirty, Wahsintong, DC, No.82 pp. 21-62

Surowiecki, James (2012), "Bankers gone wild", The New Yorker Julio 30. Disponible en http://www.newyorker.com/talk/financial/2012/07/30/120730ta_talk_surowiecki. [20 Mayo 2014]

Yermack, David 2014, "Is bitcoin a real currency? An economic appraisal", New York University Stern School of Business and National Bureau of Economic Research

Taylor, John B. (2009), "Getting Off Track: How Government Actions and Interventions Caused, Prolonged, and Worsened the Financial Crisis", Hoover Institution Press

The Foundatio of Bitcoin <https://bitcoin.org/es/> visitado el 4 de Junio 2014

Treasury Direct (USA), http://www.treasurydirect.gov/govt/reports/pd/histdebt/histdebt_histo5.htm, accedido el 5 de Marzo de 2014

U.S. Department of the Treasury (2014). Disponible en <http://www.treasury.gov/resource-center/data-chart-center/Pages/index.aspx>. [20 de Febrero 2014]

US Government Spending: http://www.usgovernmentspending.com/us_gdp_history, accedido el 5 de Marzo de 2014

Weisenthal, Joe (2014), "How A 'Bitcoin Bank' Was Robbed Of Every Single Coin It", 5 de Marzo del 2014, <http://www.businessinsider.com/flexcoin-robbery-2014-3> [1 de Mayo 2014]

Wilson, Red (2014), "The most corrupt state(s) in America", The Washington Post Enero 22. Disponible en <http://www.washingtonpost.com/blogs/govbeat/wp/2014/01/22/the-most-corrupt-states-in-america/> [21 de Mayo 2014]

Yahoo Finance (2014), *NASDAQ* <https://es.finance.yahoo.com/echarts?s=%5ENDX>, visitado el 30 de Marzo de 2014

How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES



Bob and Alice both have Bitcoin "wallets" on their computers.



Wallets are files that provide access to multiple Bitcoin addresses.



An address is a string of letters and numbers, such as 1HULMwZEPkjEPeCh43BeKJLJybLCWrfDpN.

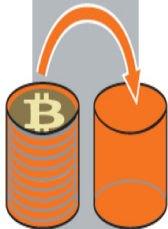
CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.



Each address has its own balance of bitcoins.

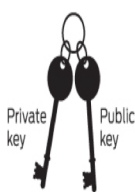
SUBMITTING A PAYMENT



Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.

Public Key Cryptography 101

When Bob creates a new address, what he's really doing is generating a "cryptographic key pair" composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.



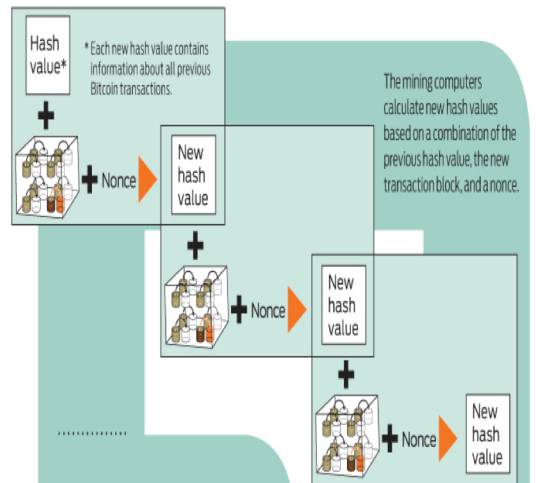
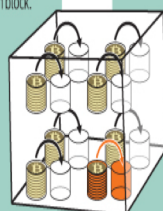
Gary, Garth, and Glenn are Bitcoin miners.

VERIFYING THE TRANSACTION

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."



The miners' computers are set up to calculate cryptographic hash functions.



Cryptographic Hashes

Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

The root of all evil → 6d0a1899 086a... (56 more characters)

The root of all evil → 486c 6be4 6dde...

The root of all evil → b8db 7ee9 8392...

The root of all evil ??? → 0000 0000 0000...

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

Nonces

To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.



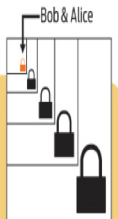
The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.



TRANSACTION VERIFIED

As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.



Como funciona una transacción Bitcoin

Pablo, un comerciante en línea, decide empezar a aceptar bitcoins como forma de pago. Alicia, una compradora, tiene bitcoins y quiere comprar mercancía de Pablo.

CARTERAS Y DIRECCIONES



Pablo y Alicia tienen ambos "carteras" de Bitcoins en sus ordenadores



Las carteras son archivos que permiten el acceso a las direcciones de los Bitcoins



Una dirección es una cadena de texto de letras y números como: IH8PJ34R J18F201B ...

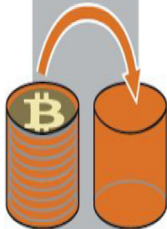
CREANDO UNA NUEVA DIRECCIÓN

Pablo crea una nueva dirección de Bitcoin para Alicia y así ella pueda recibir el



Cada dirección tiene su propio balance de bitcoins

ENVIANDO UN PAGO



Alicia le dice a su cartera que quiere transferir la cantidad de la compra a la cartera de Pablo



Criptografía Pública 101

Cuando Pablo crea una nueva dirección, lo que realmente hace es un "par de llaves criptográficas", compuesto de una clave privada y otra clave pública. Si se firma un mensaje con una clave privada (solo la sabes tú), puede ser verificada con su clave pública (conocida por todos). La nueva dirección de Pablo representa una clave pública única, con su correspondiente clave privada que es almacenada en su cartera. Gracias a la clave única, a uno le permite verificar que el mensaje firmado con su clave privada es válida.

Se puede pensar que una dirección es como una cuenta bancaria, pero en verdad difieren un poco. Un usuario puede crear tantas direcciones como quiera, de hecho, se recomienda crear una nueva dirección para cada transacción para aumentar la privacidad. Mientras nadie sepa las direcciones que le pertenecen a Alicia, su anonimato estará protegido.



Héctor, Sergio y Ricardo con minadores de Bitcoin

VERIFICANDO LA TRANSACCIÓN

Sus ordenadores agrupan las transacciones de los últimos 10 minutos en un "nuevo bloque de transacción"



Clave Privada

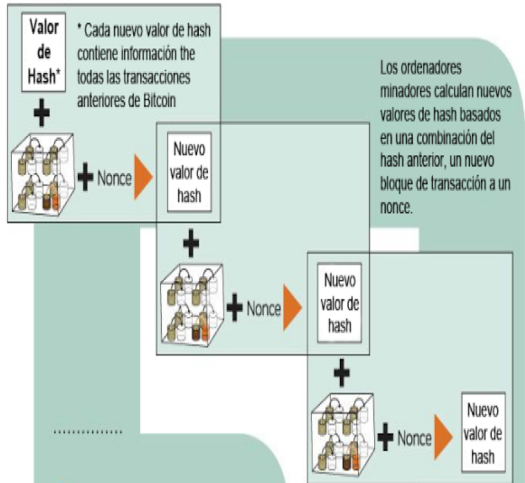


La cartera de Alicia contiene la clave privada de SUS direcciones. La cartera firma su petición de transacción con la clave privada de la dirección con la que está pagando

Clave Pública



Cualquier persona en la red puede usar la clave pública para verificar la petición de transacción viene realmente de la persona legítima



Hashes Criptográficos

Los hashes de las funciones criptográficas transforman un bloque de datos en una cadena alfanumérica con una longitud fija, llamada valor de hash. Incluso un pequeño cambio en el bloque de datos produce un gran cambio en el valor del hash, y es prácticamente imposible predecir que bloque de datos crearía un valor de hash específico.

The root of all evil	6d0a1899 086a... (56 caracteres más)
The root of all evil	486c 6be4 6dde...
The root of all evil	b8db 7ee9 8392...

Nonces

Para crear distintos valores de hash del mismo dato, Bitcoin emplea "nonces". Un nonce es solo un número aleatorio que es añadido a un dato antes de ser hashado. Cambiando el valor del nonce, varía bruscamente el valor del hash.

The root of all evil ??? → 0000 0000 0000 ...

La creación de hashes es computacionalmente bastante trivial, pero el sistema de Bitcoin requiere que el nuevo valor del hash tenga una estructura particular, debe de empezar con un número determinado de ceros.

Los mineadores no tienen forma de predecir que nonce producirá el valor de



hash con el número requiendo de ceros. Por lo que se deberán de crear muchos hashes con diferentes nonces hasta dar con el correcto.

Cada bloque tiene un "coinbase", al que se paga con 50 bitcoins al minador que lo haya obtenido, en este caso Sergio al que se le ha creado una nueva dirección en su cartera con la cantidad de los Bitcoins minados.



TRANSACCIÓN VERIFICADA

A la medida que pasa el tiempo, la transacción de Alicia hacia Pablo se queda detrás de las transacciones más recientes. Si cualquiera quisiera modificar los detalles, debería de rehacer el trabajo que hizo Sergio, ya que para efectuar un cambio hará falta de un nonce totalmente diferente que sea válido, y luego rehacer el trabajo de todos los minadores involucrados. Una tarea así es prácticamente imposible.

