



# Trabajo Fin de Grado

## **Bitcoin, la nueva moneda digital global**

Autor

Rodolfo Artigas Villuendas

Directora

Dra. Nieves García Casarejos

Facultad de Economía y Empresa

Curso 2012/2013

# CONTENIDO

CAPITULO I: INTRODUCCION .....	1
1.1.    Presentacion y justificacion del estudio .....	1
1.2.    Objetivos .....	2
CAPITULO II: SISTEMA FINANCIERO Y MONETARIO ACTUAL .....	3
2.1.    Dinero fiduciario .....	3
2.1.1    Historia .....	3
2.1.2    Características .....	5
2.2.    Instituciones y regulación monetaria en Europa .....	5
2.3.    Oferta de dinero .....	6
2.4.    Estrategia monetaria .....	6
2.5.    Proceso de creación del dinero .....	7
2.6.    Consecuencias de la emisión de dinero fiduciario .....	9
CAPITULO III: CONDICIONES PARA EL CAMBIO DE MODELO .....	12
3.1.    Crisis económica actual .....	12
3.2.    Despegue tecnológico .....	14
3.3.    Viabilidad del cambio de modelo .....	16
CAPITULO IV: LA NUEVA ECONOMÍA DIGITAL .....	18
4.1.    Qué es Bitcoin .....	18
4.2.    Origen .....	19
4.3.    Funcionamiento del Bitcoin .....	20
4.3.1    Monederos .....	20
4.3.2    Transacciones .....	21
4.3.3    Generación .....	23
4.3.4    Compra y venta .....	24
4.4.    Bitcoin en cifras .....	26
4.5.    Alternativas Digitales a Bitcoin .....	31

4.6. Regulación Internacional .....	32
4.7. España frente al Bitcoin .....	34
CAPITULO V: EL FUTURO DE LA MONEDA DIGITAL .....	38
5.1. Ventajas y limitaciones del modelo digital.....	38
5.2. Futuro.....	40
CAPITULO VI: CONCLUSIÓN .....	43
BIBLIOGRAFIA .....	45

## **Resumen**

El desarrollo tecnológico está provocando una serie de cambios en la sociedad mundial impensables hace apenas dos décadas. Internet ha supuesto la eliminación de barreras físicas y culturales, permitiendo comunicar distintos puntos del planeta de manera prácticamente instantánea y, al amparo del avance de la red, están surgiendo nuevos proyectos que se han despertado el interés general por su carácter innovador. Uno de ellos es el proyecto Bitcoin.

Bitcoin es el nombre de una nueva moneda virtual que está revolucionando la red. La popularidad y difusión de la nueva moneda se ha incrementado de manera exponencial desde su creación en el año 2009.

Como cualquier moneda, sirve para intercambiar bienes y servicios, trasladando valor de unas personas a otras. Sin embargo, cuenta con una serie de características que la hacen destacar por encima de otras divisas.

El uso de Bitcoins se ha disparado sobre todo a raíz de la crisis económica actual, la cual ha hecho tambalear las estructuras bancarias de algunos países cuyos ciudadanos han visto en la moneda digital un valor refugio para mantener sus ahorros a salvo.

Dado el carácter innovador de la nueva moneda digital, no existe bibliografía acerca del tema, y la única información disponible se encuentra diseminada principalmente en páginas web tecnológicas, foros, blogs y portales de medios de comunicación.

Mediante este estudio se va a analizar el presente y futuro de la nueva moneda digital, y la repercusión que puede llegar a tener en el entorno económico globalizado actual.

## **Palabras Clave**

Bitcoin, moneda digital, dinero digital, dinero fiduciario, globalización, criptomoneda, inflación, deflación

# CAPITULO I: INTRODUCCION

## 1.1. PRESENTACION Y JUSTIFICACION DEL ESTUDIO

Bitcoin es el resultado de un proyecto de innovación tecnológica y financiera que poco a poco se está haciendo un hueco en el panorama económico mundial.

La nueva moneda digital cuenta con unas características que representan una clara evolución con respecto al dinero fiduciario.

- No está emitida ni respaldada por ningún estado ni organismo supranacional, por lo que escapa del control de gobiernos, bancos centrales, etc.
- Es intangible. No cuenta con el respaldo físico del papel moneda.
- Cuenta con un elevado nivel de seguridad.
- Puede ser utilizada a nivel global, sin necesidad de conversión a moneda local.
- Permite a sus usuarios permanecer en el anonimato si lo desean.
- Es posible realizar transacciones seguras a miles de kilómetros de distancia en cuestión de segundos, con un coste infinitamente menor al de la banca tradicional, llegando incluso a ser nulo.
- Esta moneda puede ser fácilmente almacenada sin necesidad de contar con una cuenta bancaria o una caja de seguridad. Una simple cadena de caracteres escrita en un papel puede representar el valor equivalente a varios millones de euros.

Quizá parte de su éxito radica en que ha llegado en un momento en el que la confianza por parte de la ciudadanía en el sistema financiero se encuentra bajo mínimos, y ven en la nueva moneda digital un recurso valioso para resguardar sus ahorros de espaldas al sistema financiero tradicional.

Aunque no todo van a ser ventajas, ya que existe una corriente crítica que desconfía de la nueva moneda, y no ven en ella más que un nuevo tipo de tulipán digital en manos de especuladores que antes o después estallará como una gran burbuja.

Una vez más los avances tecnológicos superan a la legislación, por lo que Bitcoin se encuentra en una situación de alegalidad en la mayoría de los países, quizás por el desconocimiento de las autoridades económicas acerca de la magnitud del proyecto y su potencial.

## **1.2. OBJETIVOS**

El presente trabajo se ha desarrollado con la intención de arrojar luz sobre el Proyecto Bitcoin, ya que dado el carácter innovador del tema, no se tiene conocimiento de ningún estudio académico que, hasta la fecha, haya analizado la nueva moneda digital y la repercusión que puede tener en una economía globalizada. Para ello, este documento se va estructurar de la siguiente manera.

En primer lugar se realizará un estudio de la situación actual, es decir, las características del dinero fiduciario, cómo se genera y porqué, y las implicaciones que para la economía tiene el uso de este tipo de moneda.

Seguidamente analizaremos el contexto económico, social y tecnológico actual para ver si se cumplen las condiciones necesarias para que la moneda digital pueda despertar el interés de la población y tener éxito.

A continuación se explicará en qué consiste el Proyecto Bitcoin, sus aspectos técnicos, cuál es el grado de uso y aceptación a día de hoy de la criptomoneda, y la postura de las autoridades monetarias ante este fenómeno.

Por último, se tendrá en consideración las ventajas y limitaciones de este nuevo modelo, así como una previsión del futuro del Bitcoin.

## CAPITULO II: SISTEMA FINANCIERO Y MONETARIO ACTUAL

### 2.1. DINERO FIDUCIARIO

Antes de profundizar acerca de las características de la nueva moneda digital, es conveniente hacer una breve introducción acerca del dinero fiduciario, su historia, regulación y funcionamiento.

#### 2.1.1 Historia

El trueque fue en la antigüedad el medio habitual empleado por la humanidad para hacerse con los bienes que debían cubrir sus necesidades. Sin embargo, este sistema presentaba varias dificultades. La principal era encontrar una contraparte que poseyera el bien que se precisaba y que a su vez, demandara el producto con el que se contaba. En segundo lugar, había que establecer qué cantidad del bien A y del bien B eran equivalentes de tal manera que ambas partes quedasen satisfechas con el trato<sup>1</sup>.

Estas limitaciones llevaron a la sociedad a buscar un sistema que les permitiese llevar a cabo transacciones evitando el trueque, mediante el empleo de un bien intermedio de aceptación general. A lo largo de la historia, muchos han sido los bienes que han sido empleados con ese fin. En algunos lugares de la India se hacía uso de las conchas de cauri<sup>2</sup>, en Chica el arroz o los discos de piedra caliza de la isla de Yap en el Pacífico.

Los primeros billetes surgen en China hacia el siglo VII D.C. Según las anotaciones del propio Marco Polo a mediados del siglo XII, en los territorios de la China del Imperio Mongol, era frecuente el uso de los llamados “billetes de seda”, cuyo contravalor no venía fijado en ningún metal precioso sino en madejas de seda.

Su uso era muy extendido y se conservan documentos de aquella época donde se relata la lucha de las autoridades contra la falsificación del papel moneda, delito que era castigado con la pena de muerte.

---

<sup>1</sup> Zevallos Avilés, Günter. Fundamentos de Economía Política. 1<sup>a</sup> edición, 2.007. Prensas Universitarias de Zaragoza. ISBN 978-84-7733-950-2

<sup>2</sup> <http://www.bolsaone.net/manuales/dinero/introduccion/0>

La falsificación es un problema recurrente a lo largo de la historia que ha generado ingeniosas maneras de luchar contra ella, como los *Tally Sticks*<sup>3</sup> del Rey Enrique I de Inglaterra. El sistema consistía en dar valor a palos de madera que se cortaban en dos partes y con los que los ciudadanos pagaban sus impuestos. La Corona guardaba un trozo de cada palo para poder verificar la autenticidad de cada *Tally Stick* posteriormente.

Sin embargo, fueron los metales preciosos los que acabaron imponiéndose de manera global como forma de dinero debido a su amplia aceptación.

El acuñado de moneda en estos metales surge como una solución a los problemas de valoración y fraccionamiento que se generaban al utilizar trozos de metales en bruto.

Las autoridades fueron las encargadas de la fabricación de las primeras monedas en metales preciosos con cierto grado de pureza, pero debido a los problemas de falsificación, surgieron los primeros bancos que se dedicaron a custodiar oro de usuarios que a cambio recibían un documento de pago convertible de nuevo en una cantidad determinada delpreciado metal. Con el tiempo, pocas personas convertían de nuevo esos documentos llamados “billetes de banco” en oro, y comenzó su libre circulación.

Es entonces cuando nace el negocio bancario tal y como lo conocemos hoy en día, facilitando créditos y captando depósitos de sus clientes. Sin embargo, debido a los problemas surgidos al emitir billetes sin el suficiente respaldo, o a la concesión de préstamos sin requerir las suficientes garantías, con frecuencia estos bancos se veían con dificultades para devolver los depósitos a sus clientes. Es entonces cuando la mayoría de los países se hacen con el control del sistema bancario, creando sus propios bancos centrales, e introduciendo normas para regular el funcionamiento de las prácticas bancarias. Estos bancos centrales adquieren en exclusiva la capacidad de emisión de papel moneda.

La convertibilidad con el oro pronto desaparecería ya que era un impedimento a la hora de llevar a cabo sus políticas económicas, por lo que debían asegurarse de que la población aceptase este nuevo dinero no convertible. Los Gobiernos de los países introdujeron entonces la obligación de que las transacciones se realizasen en billetes y

---

<sup>3</sup> <http://audrilcobroi.blogspot.com.es/2009/06/el-tally.html>

monedas de curso legal, es decir, las que ellos mismos emitían, dando lugar así a la creación del dinero fiduciario.

### 2.1.2 Características

Las principales características o funciones del dinero pueden resumirse en tres:

- El dinero debe facilitar el intercambio y ser ampliamente aceptado por la sociedad como medio válido para realizar transacciones.
- Función de depósito de valor. El dinero es un elemento que permite almacenar riqueza a quien lo posee, sin deteriorarse con el tiempo ni perder valor. En la actualidad no es posible utilizar el dinero en sí mismo como reserva de valor a largo plazo, ya que el propio transcurso del tiempo provoca la pérdida de poder adquisitivo debido al efecto de la inflación, pero sí que reporta ventajas en cuanto al deterioro si lo comparamos por ejemplo con el uso de productos perecederos.
- Medida de valor. El dinero debe poder usarse como referencia para establecer el valor de diversos bienes. Ha de tener, además, la capacidad de poder subdividirse en unidades de cuenta más pequeñas, de manera que se pueda realizar cualquier transacción sin que ello origine pérdida de valor.

## 2.2. INSTITUCIONES Y REGULACIÓN MONETARIA EN EUROPA

El Sistema Europeo de Bancos Centrales (SEBC) está compuesto por el Banco Central Europeo (BCE) y todos los bancos centrales de los países miembros con independencia de si han adoptado el Euro como moneda o no.

*Ilustración 2.2.1 Consejo de Gobierno del BCE, enero 2013*



*Fuente: europa.eu*

De acuerdo con el Tratado de la Unión Europea<sup>4</sup>, al SEBC le corresponde la tarea de definir y ejecutar la política económica de la Unión Europea, entre otras funciones. El Consejo de Gobierno<sup>5</sup> del BCE se compone de los miembros del Comité Ejecutivo y de los responsables de los Bancos Centrales de cada país miembro.

Este Consejo de Gobierno es el único responsable de autorizar la emisión de billetes dentro de la UE.

### **2.3. OFERTA DE DINERO**

El Eurosistema (compuesto por el BCE y los Bancos Centrales de países miembros que han adoptado la moneda única), distingue tres agregados monetarios para definir la oferta de dinero en la economía europea.

- M1. Efectivo en papel moneda que posee la población y depósitos a la vista del sistema bancario.
- M2. Compuesto por M1 más los depósitos a corto plazo.
- M3. Compuesto por M2 más las cesiones temporales de activos, las participaciones en fondos del mercado monetario e instrumentos del mercado monetario, más los valores de renta fija. A este agregado se le conoce también como “M”, y viene a representar la cantidad total de dinero de la economía europea.

### **2.4. ESTRATEGIA MONETARIA**

El objetivo principal del BCE es que haya estabilidad en los precios, y estos no superen un incremento anual superior al 2%.

En caso de que se produzca alguna desviación de sus previsiones, la Autoridad Monetaria intervendrá, aunque siempre con prudencia. Regularmente efectúa evaluaciones de los agregados monetarios contenidos en “M3”, y en función de su evolución, los precios y el PIB, el Consejo de Gobierno del BCE puede tomar la decisión

---

<sup>4</sup> [http://noticias.juridicas.com/base\\_datos/Admin/tue.html](http://noticias.juridicas.com/base_datos/Admin/tue.html)

<sup>5</sup> <http://www.ecb.europa.eu/ecb/orga/decisions/govc/html/index.es.html>

de modificar la oferta de dinero, e incrementar o disminuir los tipos de interés para tratar de ajustar el crecimiento económico a sus objetivos.

## 2.5. PROCESO DE CREACIÓN DEL DINERO

A las entidades financieras la normativa les exige que sean capaces de hacer frente a sus obligaciones a corto plazo, también llamada *liquidez bancaria*, estableciendo para ello unos niveles mínimos de reservas. Además, deben mantener otro tipo de reservas denominadas de *solvencia bancaria*, cuya cuantía debe ser suficiente para cubrir el resto de sus obligaciones mediante la posesión de activos a medio y largo plazo.

A la fracción de los depósitos que los bancos están obligados a guardar en el Banco de España, se le denomina *Encaje legal*, siendo la cuantía resultante de ese encaje los denominados *Activos de caja*, no constituyendo estos activos, por lo tanto, parte de la oferta monetaria del mercado. La tasa de encaje varía en función de los objetivos de la Autoridad Monetaria, de tal manera que cuando la tasa de encaje disminuye, la liquidez del sistema aumenta al incrementarse la oferta monetaria del mercado y viceversa.

De acuerdo a este sistema, el dinero que realmente se pone en circulación por parte de las instituciones financieras cuando disminuye la tasa de encaje no se corresponde exactamente con el importe de masa monetaria liberada, ya que existe un efecto multiplicativo de esa cantidad que hace que la oferta monetaria se incremente varias veces el importe inicial.

Este es el efecto que, por ejemplo, se puede producir al ingresar en una entidad bancaria 8.000 euros.

El banco X al recibir el depósito, se verá obligado de acuerdo a la normativa del Banco de España a guardar el 5% como reservas, es decir 400 euros, y dispondrá de 7.600 euros para realizar préstamos con los que obtener un beneficio.

Por tanto el balance de esa entidad bancaria de manera simplificada quedaría:

*Tabla 2.5.1 Balance inicial Banco X*

Posición inicial Banco X			
ACTIVO		PASIVO	
Reservas requeridas	400	Depósitos	8.000
Reservas excedentarias	7.600		
<b>Total</b>	<b>8.000</b>	<b>Total</b>	<b>8.000</b>

*Fuente: Zeballos, 2007*

*Tabla 2.5.2 Balance final Banco X*

Posición final Banco X			
ACTIVO		PASIVO	
Reservas requeridas	400	Depósitos	8.000
Préstamos	7.600		
<b>Total</b>	<b>8.000</b>	<b>Total</b>	<b>8.000</b>

*Fuente: Zeballos, 2007*

Esos 7.600 euros son prestados a un individuo A que salda una deuda pendiente con otro individuo B, quien a su vez ingresa el montante en otra entidad bancaria.

El balance resultante de esta entidad sería:

*Tabla 2.5.3 Balance inicial Banco Y*

Posición inicial Banco Y			
ACTIVO		PASIVO	
Reservas requeridas	380	Depósitos	7.600
Reservas excedentarias	7.220		
<b>Total</b>	<b>7.600</b>	<b>Total</b>	<b>7.600</b>

*Fuente: Zeballos, 2007*

*Tabla 2.5.4 Balance final Banco Y*

Posición final Banco Y			
ACTIVO		PASIVO	
Reservas requeridas	380	Depósitos	7.600
Préstamos	7.220		
<b>Total</b>	<b>7.600</b>	<b>Total</b>	<b>7.600</b>

*Fuente: Zeballos, 2007*

De nuevo, esos 7.220 euros que el Banco Y dispone, son empleados para conceder un préstamos a un tercer individuo C, que a su vez, liquida una deuda con un cuarto, efectuando este un ingreso en otra entidad bancaria. El balance del nuevo Banco Z quedará de la siguiente manera:

Tabla 2.5.5 Balance inicial Banco Z

Posición inicial Banco Z			
ACTIVO		PASIVO	
Reservas requeridas	361	Depósitos	7.220
Reservas excedentarias	6.859		
<b>Total</b>	<b>7.220</b>	<b>Total</b>	<b>7.220</b>

Fuente: Zeballos, 2007

Tabla 2.5.6 Balance final Banco Z

Posición final Banco Z			
ACTIVO		PASIVO	
Reservas requeridas	361	Depósitos	7.220
Préstamos	6.859		
<b>Total</b>	<b>7.220</b>	<b>Total</b>	<b>7.220</b>

Fuente: Zeballos, 2007

En este momento, los 8.000 euros iniciales se han transformado en 22.820 euros ( $8.000 + 7.600 + 7.220$ ) en forma de depósitos, además de 6.859 euros en forma de líquido disponible.

Esta misma secuencia de préstamos / ingresos puede repetirse varias veces mientras las entidades cumplan con el requisito de garantizar el 5% de sus depósitos, por lo que si continuáramos hasta agotar las garantías, esos 8.000 euros se convertirían en depósitos por valor de 160.000 euros, es decir, 20 veces el montante inicial.

Esta es la manera mediante la cual las entidades bancarias, gracias al efecto de expansión del crédito, crean dinero fiduciario cumpliendo con la normativa vigente.

## 2.6. CONSECUENCIAS DE LA EMISIÓN DE DINERO FIDUCIARIO

Historicamente el dinero *commodities*<sup>6</sup>, es decir, el que está respaldado por un activo como el oro, se ha sustituido por dinero fiduciario en ocasiones excepcionales en las que la deuda pública se había disparado, como ocurre en las grandes guerras.

En EEUU, el uso de dinero fiduciario se implantó durante siete años con el fin de poder asumir el coste de la Guerra Civil. Hasta esa fecha, la Constitución Norteamericana castigaba con la pena de muerte a aquellos que degradaran el valor del dinero.

---

<sup>6</sup> <http://www.gurusblog.com/archives/dinero-fiduciario/15/09/2010/>

Thomas Jefferson<sup>7</sup>, el tercer presidente de la historia de los Estados Unidos entre 1801 y 1809, mostraba una fuerte oposición a la emisión de dinero sin respaldo y al Banco Central de los EEUU.

En una carta<sup>8</sup> que el Presidente envía al Senador John Taylor<sup>9</sup> en 1812, deja clara su postura hacia el sistema bancario de la época.

*«Pienso que las instituciones bancarias son más peligrosas para nuestras libertades que ejércitos enteros listos para el combate. Si el pueblo americano permite un día que los bancos privados controlen su moneda, los bancos y todas las instituciones que florecerán en torno a los bancos, privarán a la gente de toda posesión, primero por medio de la inflación, enseguida por la recesión, hasta el día en que sus hijos se despertarán sin casa y sin techo, sobre la tierra que sus padres conquistaron».*

Parece ser que los temores del Presidente se han ido confirmando a lo largo de la historia, y la aparición del dinero fiduciario ha generado una economía inflacionaria global.

La inflación provoca anomalías en el sistema económico debido a su carácter imprevisible<sup>10</sup>. Esta imprevisibilidad provoca que no todos los precios de bienes y servicios incrementen su valor en el mismo momento y proporción, además de que cuanto mayor sea el incremento inflacionario, más se distorsionan las expectativas de los agentes económicos.

El precio de los productos es el medio para que, por medio de la oferta y la demanda, las empresas puedan calcular qué deben producir y en qué cantidad. Si la variación de los precios es constante, va a repercutir sobre los hábitos de compra de los consumidores, por lo que va a dejar de cumplir con su función informativa creando incertidumbre sobre las necesidades del mercado a los proveedores, desalentando además la inversión.

---

<sup>7</sup> <http://www.whitehouse.gov/about/presidents/thomasjefferson>

<sup>8</sup> Testimonio de Charles C. Mayer, Hearings Before the Committee on Banking and Currency, House of Representatives, Seventy-fourth Congress, First Session, on H.R. 5357, p. 799

<sup>9</sup> <http://www.co.caroline.va.us/taylor.html>

<sup>10</sup> <http://www.eumed.net/cursecon/13/13-2.htm>

Por otra parte, la inflación va a provocar que los ahorradores sean castigados con la pérdida de valor de sus fondos, lo que desincentivará también el ahorro.

Una etapa continuada de inflación sostenida es causada cuando la emisión de moneda crece más rápidamente que la tasa de crecimiento económico.

La mayoría de corrientes económicas de la actualidad, sin embargo, ven favorable una tasa reducida y estable de inflación ya que puede ayudar a suavizar el efecto de la recesión. Una inflación moderada de entre un 1% y 3%, incentiva a las familias a consumir hoy y no dilatar a largo plazo sus decisiones de compra. Por esta misma razón, a las empresas les será atractivo realizar inversiones productivas por su mayor rentabilidad frente a las inversiones financieras. Estos dos, son los ingredientes fundamentales de un crecimiento económico sostenido.

## CAPITULO III: CONDICIONES PARA EL CAMBIO DE MODELO

### 3.1. CRISIS ECONÓMICA ACTUAL

La mayoría de los países del mundo están sufriendo una profunda crisis económica llamada la Gran Recesión iniciada en 2008, que devastó en primer lugar la economía americana para extenderse poco después a prácticamente el resto de países. Las razones que originaron este derrumbe económico se atribuye a la gran burbuja inmobiliaria que se produjo en EEUU y a un valor del dólar excesivamente bajo frente a otras divisas.

Los brokers de hipotecas flexibilizaron las condiciones de las conocidas como hipotecas *subprime*<sup>11</sup> con el único propósito de captar nuevos clientes, sin dar demasiada importancia a la calidad crediticia de los demandantes.

La crisis americana azotó también a Europa, cebándose especialmente en países como España, Irlanda, Italia, Francia y Grecia.

Es precisamente en este último país, uno de los más castigados, donde la autoridad monetaria europea tiene que acudir a su rescate en mayo de 2010, ante el temor de un *default* de su sistema bancario, y las nefastas consecuencias que se preveía podía tener una situación así para el resto de países de la Zona Euro.

La desconfianza en el sistema bancario es total. En octubre de 2011 los ciudadanos acuden en masa<sup>12</sup> para retirar sus fondos ante el temor de que el sistema monetario quede fuera del euro. Desde comienzos de años, ya habían disminuido los depósitos bancarios en más de un 10%, y alrededor del 20% desde enero de 2010, en busca de nuevas localizaciones que ofrecieran mayor confianza a los ahorradores helenos.

A pesar de los rumores, los depósitos griegos corrieron mejor suerte que los de sus vecinos chipriotas.

Chipre se vio sumida en marzo de 2013 mediante decreto a una quita del 37,5% en sus depósitos bancarios de más de 100.000 euros, siendo finalmente<sup>13</sup> del 47,5% y

---

<sup>11</sup> <http://analisisfundamental.es/hipotecas-subprime%C2%BFque-son/>

<sup>12</sup> <http://www.libremercado.com/2011-10-26/los-griegos-acuden-a-sus-bancos-para-retirar-en-masa-sus-depositos-1276439465/>

<sup>13</sup> [http://economia.elpais.com/economia/2013/07/29/actualidad/1375111894\\_245705.html](http://economia.elpais.com/economia/2013/07/29/actualidad/1375111894_245705.html)

quedando bloqueado un 22,5% más en previsión de nuevos ajustes, según el acuerdo acordado entre el Gobierno chipriota y la *Troika* formada por el BCE, CE y FMI.

No fue el único país europeo cuyos ciudadanos vieron mermados sus depósitos en cuestión de horas. En febrero del mismo año, Amagerbanken, el décimo banco de Dinamarca, cerró sus puertas ante la incapacidad de cumplir con los requerimientos legales de solvencia y tras alcanzar un acuerdo de transferencia de activos con Finansiel Stabilitet. La bancarrota de la entidad supuso una quita del 41% a los depósitos de más de 100.000€ que sus clientes les habían confiado.

*Ilustración 3.1.1 Cacerolada Argentina.*



*Fuente actibva.com*

Una situación así no tenía antecedentes en la historia reciente europea, sin embargo, en otras zonas del mundo ya habían sufrido situaciones similares como el famoso “corralito<sup>14</sup>” argentino impuesto bajo el gobierno de De La Rúa, y que consistía en que cada ciudadano no podía retirar del banco más de 250 pesos, equivalente a la misma cantidad de dólares, a la semana. Esta medida fue impuesta para evitar la fuga de capitales de la maltrecha economía argentina tras el segundo mandato de Carlos Saúl Menem, pero supuso poner a la población en una situación límite, ya que en esa época era muy frecuente que el pago de facturas de la luz, gas, etc, no se domiciliaran, por lo que los argentinos durante un año pasaron auténticas penurias para llegar a fin de mes.

---

<sup>14</sup> <http://www.eitb.com/es/noticias/economia/detalle/886007/que-es-corralito--el-corralito-argentina-de-rua/>

Debido a esta situación, la población perdió toda confianza en el sistema bancario, y adquirió la costumbre de guardar parte de sus ahorros en cajas de seguridad o en otros lugares ajenos a los bancos.

### 3.2. DESPEGUE TECNOLÓGICO

Por otro lado, la humanidad está viviendo desde hace apenas dos décadas una revolución tecnológica cuyo mayor exponente se encuentra en la red de redes.

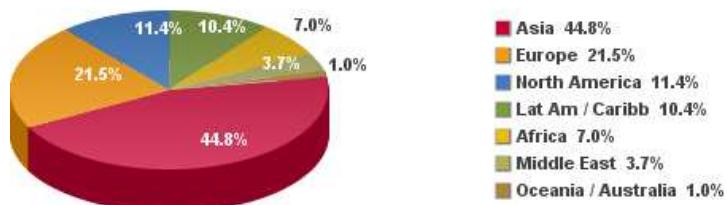
Internet ha supuesto un impacto en la humanidad comparable con la capacidad de hacer fuego o el empleo de los metales.

La expansión de Internet continúa en un vertiginoso ascenso<sup>15</sup>.

A nivel mundial desde el año 2000 hasta el 2009, sus usuarios han aumentado de 394 a 1.858 millones. Ya en el año 2010, un 22% de la población mundial tenía acceso a un ordenador personal. El número de búsquedas que Google realizaba eran más de 30 millones por minuto, dos mil millones de vídeos diarios eran visionados en Youtube, y 300 millones de usuarios leían blogs<sup>16</sup>.

*Ilustración 3.2.1 Usuarios de Internet junio 2012*

#### Internet Users in the World Distribution by World Regions - 2012 Q2



Source: Internet World Stats - [www.internetworldstats.com/stats.htm](http://www.internetworldstats.com/stats.htm)  
Basis: 2,405,518,376 Internet users on June 30, 2012  
Copyright © 2012, Miniwatts Marketing Group

*Fuente: Internet Word Stats*

En cuanto a la distribución de los internautas, la zona de mundo que contaba con más usuarios de la Red hacia mediados de 2012 era Asia, con 1.076 millones, seguida de

<sup>15</sup> <http://www.internetworldstats.com/stats.htm>

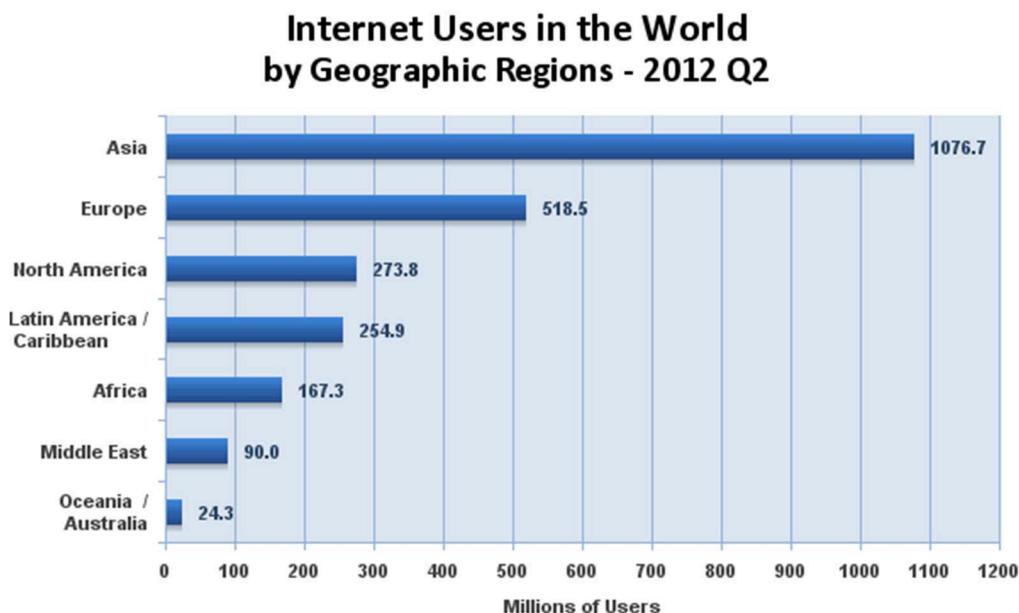
<sup>16</sup> <http://www.antaranews.com/en/news/71940/google-earth-demonstrates-how-technology-benefits-ris-civil-society-govt>

Europa con 518 millones, y en tercer lugar Norte América con casi 274 millones de usuarios conectados.

Estos datos sirven para hacerse una idea del tamaño actual de La Red, aunque las previsiones de diversos expertos<sup>17</sup>, auguran un crecimiento para el año 2016 hasta alcanzar un tamaño cuatro veces el actual, con más de 3.400 millones de personas conectadas, o lo que es lo mismo, un 45% de la población mundial prevista para entonces.

China es uno de los países de mayor crecimiento y en los que la moneda virtual ha causado más expectación.

*Ilustración 3.2.2 Distribución de usuarios de Internet Q2 2012*



Source: Internet World Stats - [www.internetworldstats.com/stats.htm](http://www.internetworldstats.com/stats.htm)  
2,405,518,376 Internet users estimated for June 30, 2012  
Copyright © 2012, Miniwatts Marketing Group

Fuente: Internet Word Stats

<sup>17</sup> <http://www.cisco.com/web/ES/about/press/2012/2012-05-30-internet-sera-cuatro-veces-mas-grande-en-2016--informe-vini-de-cisco.html>

Las razones<sup>18</sup> que pueden ayudar a adoptar al pueblo chino la moneda virtual son variadas:

- Ya han impulsado con éxito una nueva moneda virtual, el Q Coin<sup>19</sup>
- Bitcoin puede ayudar a evitar los estrictos controles de capital a los que están sometidos.
- Es una cultura propensa al riesgo en las inversiones, y se sienten atraídos por la alta volatilidad de la moneda y sus posibles beneficios.
- Hay un creciente uso de los ordenadores personales, por encima de los dispositivos móviles como en otros países emergentes.
- El Gobierno no tiene capacidad para bloquear el uso de Bitcoin ni para identificar a sus usuarios.

Aunque sea una pequeña proporción la de ciudadanos chinos que se interesen por la moneda digital, dada la cantidad de habitantes que suponen con respecto a la población mundial, puede suponer un empuje decisivo para ayudar a despegar al Bitcoin.

Según una encuesta realizada a expertos e inversionistas tecnológicos por el proyecto Internet & American Life del Pew Research Centre junto con la Elon University, el 65% de los encuestados opinaron que hacia el año 2020, la mayoría de la población empleará sus dispositivos móviles tipo Smartphone para realizar pagos online y en establecimientos. A través del uso de la tecnología NFC, es posible establecer comunicaciones en un radio de sólo 4 cm, lo que puede ayudar a que un dispositivo móvil se emplee como medio de pago con las mayores garantías.

### 3.3. VIABILIDAD DEL CAMBIO DE MODELO

Los sucesos generados como consecuencia de la crisis económica global han creado un ambiente de desconfianza entre los usuarios de la banca que han visto como en las épocas de mayor inestabilidad financiera, sus depósitos bancarios eran mermados o congelados.

Otro problema con el que tienen que lidiar los ciudadanos de otros países, es la hiperinflación. Uno de los casos más dramáticos se dio en Zimbabue en la década del

---

<sup>18</sup> <http://mashable.com/2013/04/13/bitcoin-boom-chinese/>

<sup>19</sup> [http://cincodias.com/cincodias/2007/01/12/economia/1168741406\\_850215.html](http://cincodias.com/cincodias/2007/01/12/economia/1168741406_850215.html)

2000, poco después de que el Gobierno confiscara las tierras agrícolas que estaban en manos de la minoría blanca, y dejara de pagar la deuda contraída con el FMI. En noviembre de 2008, se estimaba que la tasa de inflación era de 89.700 trillones por ciento<sup>20</sup>, es decir, los precios se duplicaban cada 24 horas.

*Ilustración 3.3.1 Billete 500 millones Zimbabwe*



*Fuente: Libertad Digital*

Ante circunstancias así, la confianza en el dinero fiduciario cae en picado, y la tendencia de la población es la de buscar valores refugio como el oro, que ve como, en situaciones de crisis o ante sucesos políticos importantes, su cotización se dispara.

Lamentablemente, en todas las partes del mundo no es posible adquirir otras divisas o metales preciosos con la misma facilidad y en las mismas condiciones económicas, por lo que Bitcoin es el medio ideal para que la población pueda acceder a un valor refugio de aceptación global, sin importar la nacionalidad y ubicación de sus demandantes.

<sup>20</sup> <http://www.libertaddigital.com/economia/zimbabwe-la-segunda-mayor-hiperinflacion-de-la-historia-1276368268/>

## CAPITULO IV: LA NUEVA ECONOMÍA DIGITAL

### 4.1. QUÉ ES BITCOIN

Bitcoin es el nombre de la moneda electrónica descentralizada pero, además, el mismo término se emplea también para referirse al software libre<sup>21</sup> diseñado inicialmente por Satoshi Nakamoto para su gestión y a la red P2P<sup>22</sup> necesaria para el funcionamiento de todo el sistema.

Ilustración 4.1.1 Moneda Bitcoin



Fuente: [image.excite.es](http://image.excite.es)

Lasse Birk Olesen, fundador del portal BitcoinNordic.com ha sabido sintetizar con un sencillo ejemplo qué es Bitcoin y cómo funciona.

*“¿Cómo funciona Bitcoin?. Imagine un tipo especial de email que no puede ser copiado. Esto significa que cuando usted lo envía a otra persona, éste email automáticamente se borra de su propia casilla de correo electrónico, es decir, el destinatario pasa a tener el email que usted ya no tiene. Ahora también imagine que sólo existe una cantidad finita de estos emails especiales, y que nadie puede crear más de los que ya existen. Debido a estas propiedades, la gente ha comenzado a considerar a estos emails como algo valioso. Estos emails especiales, por supuesto, se llaman Bitcoins.”*

Detrás de Bitcoin se encuentra un ingenioso sistema muy complejo y seguro que permite a sus usuarios realizar transacciones económicas en esta divisa de manera casi

---

<sup>21</sup> <http://www.fsf.org/about/what-is-free-software>

<sup>22</sup> <http://ingeniatic.euitt.upm.es/index.php/tecnologias/item/574-redes-p2p>

instantánea por medio de Internet, prescindiendo de la intermediación de cualquier entidad financiera y con un coste muy reducido o incluso nulo.

#### 4.2. ORIGEN

El concepto de Bitcoin surge a raíz de un mensaje publicado por un criptógrafo llamado Wei Dai en la lista de correo Cypherpunk en el año 1998. Sobre una base de criptografía de clave pública Wei describe el concepto de B-money<sup>23</sup>, un sistema descentralizado que permite a sus usuarios el intercambio de valor por medio de una moneda electrónica, y que les asegura, si así lo desean las partes involucradas, mantener el anonimato en una transacción. Además, esta nueva moneda virtual estaría fuera del control de los gobiernos y demás instituciones reguladoras. Este trabajo es completado posteriormente por otros expertos en criptografía como Nick Szabo y Hal Finney.

El mensaje de Wei Dai llamó la atención de otro usuario de la lista de correo quien unos años más tarde, en noviembre de 2008, anunciaría<sup>24</sup> en el foro de la P2P Foundation el nacimiento del Bitcoin, publicando un documento titulado “Bitcoin: A Peer-to-Peer Electronic Cash System”<sup>25</sup>, en donde se establecen las bases del proyecto.

La identidad de ese usuario es un misterio desde entonces.

Se hace llamar Satoshi Nakamoto<sup>26</sup>, pero diversas investigaciones han concluido que no se trata de un nombre real. Las pocas personas que han tenido contacto con él lo han hecho a través de mensajes de correo electrónico. Se sospecha que es de origen japonés por los datos de su perfil de la P2P Foundation<sup>27</sup> y por las declaraciones del propio Hal Finney quien intercambió varios mensajes con Satoshi a raíz de la publicación de la primera versión del software de Bitcoin<sup>28</sup>.

Es muy celoso con su identidad, hasta el punto de utilizar exclusivamente cuentas de correo de servidores públicos a través de redes seguras, de tal manera que no se pueda rastrear su localización y comprometer su anonimato.

---

<sup>23</sup> <http://www.weidai.com/bmoney.txt>

<sup>24</sup> <http://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html>

<sup>25</sup> <http://Bitcoin.org/Bitcoin.pdf>

<sup>26</sup> [https://es.Bitcoin.it/wiki/Satoshi\\_Nakamoto](https://es.Bitcoin.it/wiki/Satoshi_Nakamoto)

<sup>27</sup> [http://p2pfoundation.ning.com/profile/SatoshiNakamoto?xg\\_source=activity](http://p2pfoundation.ning.com/profile/SatoshiNakamoto?xg_source=activity)

<sup>28</sup> <http://elBitcoin.org/Bitcoin-y-yo-por-hal-finney/>

En abril de 2011 le comentó a un desarrollador del proyecto que “se iba a dedicar a otras cosas” y desde entonces no contesta a sus cuentas de correos ni nadie tiene noticias de él.

En la actualidad el proyecto está liderado por Gavin Andresen<sup>29</sup> y desarrollado a través de la Bitcoin Foundation<sup>30</sup>, cuyos principios fundamentales abogan por “*una economía que no dependa de la política, abierta e independiente*”.

Su uso a día de hoy está extendido por todo el planeta y cada día son más los comercios que admiten Bitcoin como una moneda válida para el pago de sus productos y servicios.

### 4.3. FUNCIONAMIENTO DEL BITCOIN

#### 4.3.1 Monederos

Para empezar a emplear Bitcoin, primero se debe contar con un sistema para almacenarlos y poder operar con ellos.

Un usuario de la red Bitcoin debe poseer un monedero electrónico<sup>31</sup>, el cual contiene pares de llaves criptográficas, es decir, una clave pública y otra privada propias de la criptografía asimétrica<sup>32</sup>. Aunque no la conoczamos por su nombre, la criptografía asimétrica forma parte de nuestras vidas desde hace tiempo, y es el sistema en el que se basa la seguridad del nuevo DNI electrónico o de los certificados digitales que instalamos en nuestro navegador para verificar nuestra identidad frente a organismos de la Administración.

Una dirección Bitcoin pública se asemeja al número de una cuenta bancaria. Es un identificador de entre 27 y 34 caracteres alfanuméricos que comienzan por el número 1 ó 3. Si el poseedor de un monedero electrónico desea recibir un pago, deberá facilitar esta cadena de caracteres al igual que un usuario de la banca tradicional debe comunicar su número de cuenta si desea recibir una transferencia.

---

<sup>29</sup> <https://Bitcoinfoundation.org/about/board>

<sup>30</sup> <https://Bitcoinfoundation.org/>

<sup>31</sup> <http://Bitcoin.org/es/elige-tu-monedero>

<sup>32</sup> <http://www.genbeta.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida>

Una dirección Bitcoin válida tiene este aspecto:

*1P6VtQhPBJ4qF3gMAXJH2UwErvhfwdFkJv*

La clave privada, por el contrario, debe permanecer a buen recaudo ya que, al igual que por ejemplo la clave de firma de la banca virtual, se va a emplear para firmar operaciones de transferencia de fondos a los monederos de otros usuarios.

Un usuario puede tener tantas direcciones Bitcoin como desee. Se generan de manera instantánea de una manera muy sencilla y por supuesto gratuita a través del propio software monedero o por medio de portales como bitaddress.org.

*Ilustración 4.3.1.1 Generador monedero Bitcoin*



Fuente: [bitaddress.org](http://bitaddress.org)

Hay usuarios que, incluso para preservar por completo su anonimato, generan una dirección en cada transacción que realizan.

Los monederos electrónicos también reciben el nombre de carteras electrónicas o billeteras electrónicas. Existen diversos tipos de monederos<sup>33</sup>, desde aplicaciones para ordenadores personales, tablets y smartphones, o portales web donde se permite almacenar carteras Bitcoins de manera segura y operar con ellas, como BlockChain.info o MtGox.com. Incluso un trozo de papel puede servir para almacenar millones de euros en Bitcoins simplemente apuntando la clave privada asociada<sup>34</sup> a una cartera.

### 4.3.2 Transacciones

Cuando un usuario A desea transferir una cantidad de Bitcoins a un usuario B, A renuncia a su posesión agregándole la clave pública de B y firmando la operación con

<sup>33</sup> <http://www.coinrevolution.com/elige-tu-cartera-Bitcoin>

<sup>34</sup> [https://es.Bitcoin.it/wiki/Monedero\\_de\\_papel](https://es.Bitcoin.it/wiki/Monedero_de_papel)

su clave privada, verificando así la propiedad de esos Bitcoins. Esta información se propaga a través de la red P2P como una nueva transacción. Es entonces cuando el resto de los nodos comprueban que realmente el usuario A posee esa cantidad de Bitcoins en su monedero y que la operación está correctamente firmada. Si es así, esa transacción pasa a formar parte de la Cadena de bloques, es decir, de una base de datos que es replicada en tiempo real en cada nodo que forma la red Bitcoin, por lo que existen millones de copias de ella repartidas por equipos de todo el mundo.

La Cadena de bloques es un registro público por lo que todas las transacciones en Bitcoins registradas hasta la fecha pueden ser consultadas sin problemas incluso en tiempo real. Esto dota al sistema de una transparencia sin precedentes si se compara con el sistema bancario actual.

Existen varias utilidades y portales web que ayudan en la labor de interrogar a la Cadena de bloques como blockchain.info.

No todas las transacciones que se propagan a través de la red son válidas ya que pueden producirse errores, intencionados o no, como el “doble gasto”<sup>35</sup>, lo que hace necesario que se verifique cuidadosamente cada transacción. Este trabajo corresponde a los nodos generadores, comúnmente llamados equipos mineros.

Cada nodo generador o equipo minero incluye en un archivo todas esas transacciones que son necesarias verificar, junto con el último bloque válido de la cadena de bloques del que tiene constancia.

Es entonces cuando los mineros compiten entre sí para ver cuál es el primero que encuentra el código aleatorio que representa ese bloque (Hash<sup>36</sup>) por el método de prueba y error. Cuando un minero finalmente encuentra la solución, lo propaga a la red Bitcoin donde es verificado por el resto de mineros y añadido a la cadena de bloques.

El dar con la solución supone un esfuerzo computacional muy elevado que tiene como recompensa un lote de nuevos Bitcoins para el primer minero que obtiene el hash.

---

<sup>35</sup> <http://Bitcoin.org/es/vocabulario#doble-gasto>

<sup>36</sup> <https://es.Bitcoin.it/wiki/Hash>

La labor de los mineros es fundamental para el sostenimiento de todo el sistema, ya que se encargan de validar las transacciones y mantener actualizada la base de datos distribuida.

#### 4.3.3 Generación

El proceso de generar nuevos Bitcoins se conoce como minar. Es una manera de equiparar la obtención de nuevas criptomonedas con la acción de extraer oro u otros metales preciosos de una mina.

La red crea y distribuye un nuevo lote de Bitcoins con una frecuencia aproximada de diez minutos, que se reparten en forma de premios a los mineros. El tamaño de los lotes varía con el tiempo y en la actualidad está compuesto por 25 btcs<sup>37</sup>. El propio sistema está concebido para generar un número limitado de Bitcoins, por lo que el grado de dificultad para su obtención y tamaño del lote va a ir variando con el tiempo hasta alcanzar la cifra de 20.999.999 Bitcoins previsiblemente en el año 2140. La generación de Bitcoins sigue una progresión geométrica, de tal manera que en la actualidad ya han sido generadas la mitad del total de criptomonedas que se pondrán en circulación, y en el año 2017 las tres cuartas partes de las mismas.

Para realizar este proceso de minado se precisan equipos cada vez más potentes puesto que debido a lo rentable que es descubrir el hash de los nuevos bloques (un lote en la actualidad tiene un valor al cambio de 2.500€), muchos usuarios se han interesado por la minería y el nivel de competencia es muy elevado. En el origen del proyecto, un PC de sobremesa era suficiente para poder hacerse con un lote de Bitcoins en pocas horas. A día de hoy, ha habido una auténtica revolución en cuanto al desarrollo de equipos específicos para la minería de Bitcoin, con potencias de hasta 500 Giga Hash/s en un solo equipo, es decir, con capacidad de realizar 500.000.000.000 de comprobaciones del hash del bloque por segundo por un precio superior a los 22.000\$, y ni siquiera con equipos de esa potencia se puede tener la certeza de obtener un solo lote de Bitcoins en varios meses. Por esta razón, los mineros suelen adherirse a grupos denominados “pools” para sumar la potencia de cálculo de cada uno de ellos y evitar realizar comprobaciones por duplicado,

---

<sup>37</sup> Abreviatura de Bitcoins

repartiendo posteriormente las ganancias proporcionalmente a la potencia de cálculo aportada por cada uno de ellos.

Otra manera de premiar la labor de los mineros en el sostenimiento de la red, es mediante el abono voluntario de una comisión al realizar una transacción en Bitcoins. De esta manera, el minero que incluye la transacción en el bloque a verificar se lleva una pequeña gratificación generalmente de unos pocos céntimos de Bitcoin. Además, las transacciones que incorporan una gratificación suelen ser procesadas más rápidamente por los mineros.

La capacidad de la red Bitcoin es inmensa. En la actualidad<sup>38</sup>, la mayor supercomputadora<sup>39</sup> existente en el mundo es la Tianhe-2<sup>40</sup> ubicada en Guangzhou, China. La construcción de esta máquina supuso un coste al Gobierno chino de más de 390 millones de dólares, y su potencia es de 33,86 PetaFLOPS. La actual red Bitcoin cuenta con una potencia de cálculo<sup>41</sup> de 11.878,24 PetaFLOPS, lo que equivale a más de 350 veces la potencia de la supercomputadora china, o más de 186.000 veces la de MareNostrum<sup>42</sup>, el mayor supercomputador de España, que cuenta con 0,0638 PetaFLOPS.

#### 4.3.4 Compra y venta

Como hemos visto, una manera de obtener Bitcoins es mediante el proceso de minería. En el pasado, sí que era relativamente sencillo obtener monedas mediante este sistema, pero a día de hoy, debido al elevado número de mineros y al coste que supone hacerse con un equipo competitivo, esta opción ha dejado de ser rentable. Por supuesto, otra opción para obtener Bitcoins es mediante la venta de bienes y prestación de servicios como veremos más adelante.

El método más rápido y sencillo para poder adquirir Bitcoins, es abrir una cuenta en una casa de cambio de las que abundan por Internet, y comprar Bitcoins empleando

---

<sup>38</sup> Septiembre 2013

<sup>39</sup> <http://www.top500.org/lists/2013/06/>

<sup>40</sup> <http://www.top500.org/system/177999>

<sup>41</sup> <http://Bitcoinwatch.com/>

<sup>42</sup> <http://www.top500.org/system/8242>

nuestra moneda doméstica. Existe un número elevado de cambistas aunque en la actualidad entre los cinco principales acaparan más del 92% del Market Share.

*Ilustración 4.3.4.1 Principales casas de cambio*

## Exchanges

Currency: [\[ALL\]](#) [AUD](#) [CAD](#) [CHF](#) [CNY](#) [DKK](#) [EUR](#) [GBP](#) [HKD](#) [ILS](#) [JPY](#) [NOK](#) [NZD](#) [PLN](#)  
[RUB](#) [RUR](#) [SEK](#) [SGD](#) [THB](#) [USD](#)

Time span: [24h](#) [3d](#) [7d](#) [30d](#) [6m](#)

Total volume in selected timespan: **29,591 BTC**

Name	Total volume [BTC]	Market share	Currencies
<b>mtgox</b>	10,491	35.46 %	<a href="#">AUD</a> <a href="#">CAD</a> <a href="#">CHF</a> <a href="#">DKK</a> <a href="#">EUR</a> <a href="#">GBP</a> <a href="#">HKD</a> <a href="#">ILS</a> <a href="#">JPY</a> <a href="#">NOK</a> <a href="#">NZD</a> <a href="#">PLN</a> <a href="#">RUB</a> <a href="#">RUR</a> <a href="#">SEK</a> <a href="#">SGD</a> <a href="#">THB</a> <a href="#">USD</a>
<b>bitstamp</b>	8,718	29.46 %	<a href="#">USD</a>
<b>btce</b>	3,687	12.46 %	<a href="#">USD</a> <a href="#">RUR</a> <a href="#">EUR</a>
<b>localbitcoins</b>	2,733	9.24 %	<a href="#">USD</a> <a href="#">EUR</a> <a href="#">GBP</a> <a href="#">AUD</a> <a href="#">CAD</a> <a href="#">JPY</a> <a href="#">PLN</a>
<b>btcchina</b>	1,643	5.55 %	<a href="#">CNY</a>
<b>campbx</b>	878	2.97 %	<a href="#">USD</a>
<b>rmbtb</b>	707	2.39 %	<a href="#">CNY</a>
<b>cavirtex</b>	361	1.22 %	<a href="#">CAD</a>
<b>bitcurex</b>	354	1.20 %	<a href="#">PLN</a> <a href="#">EUR</a>
<b>justcoin</b>	13	0.05 %	<a href="#">EUR</a> <a href="#">NOK</a>
<b>bit2c</b>	2	0.01 %	<a href="#">ILS</a>

(c) 2011-2013 Bitcoinity.org, created by Kacper Cieśla (comboy) | [contact](#)

Fuente: Bitcoinity.org

Para abrir una cuenta en una de estas casas de cambio y poder realizar ingresos o retirar fondos, es necesario previamente verificar la identidad de los usuarios, por lo que es necesario enviar copia del documento de identidad, facturas de suministros recientes, etc<sup>43</sup>. De no ser verificada una cuenta, únicamente se le permitirá operar con Bitcoins.

Esta medida se está llevando a cabo en todos los exchanges para prevenir el blanqueo de capitales y evitar problemas con las autoridades que puedan llegar a paralizar la actividad como fue el caso de Bitcoin24<sup>44</sup>. En abril de 2013, las autoridades alemanas y polacas bloquearon las cuentas bancarias con saldos millonarios desde las que esta empresa operaba al no contar con ningún tipo de licencia bancaria ni verificar la identidad de sus usuarios.

<sup>43</sup> <https://support.mtgox.com/entries/21651045-AML-Account-Statuses>

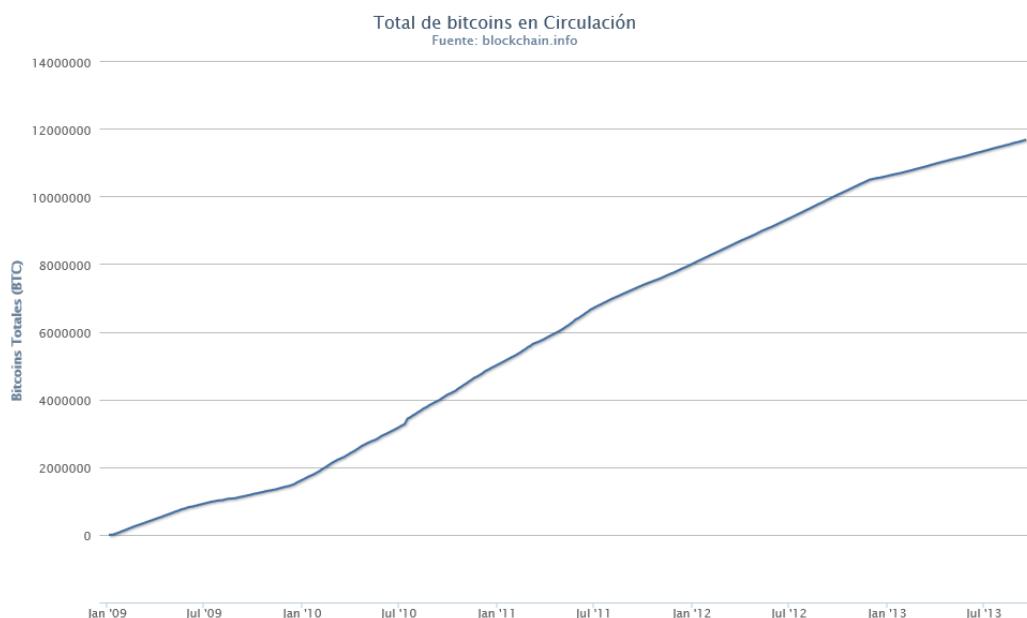
<sup>44</sup> <https://Bitcoin-24.com/>

#### 4.4. BITCOIN EN CIFRAS

Para que se pueda tener una idea de la magnitud del proyecto y el creciente interés que está despertando entre usuarios de todo el mundo, vamos a analizar la evolución desde el origen de algunos parámetros significativos<sup>45</sup>

A día de hoy<sup>46</sup>, el número total de Bitcoins que hay en circulación es de más de 11.675.000, si bien es verdad que parte de esas monedas se han perdido para siempre debido a errores por parte de los usuarios que las custodiaban, como por ejemplo el no hacer copias de seguridad de las billeteras electrónicas, o a la falta de interés de los primeros mineros en conservar las monedas debido al escaso valor de las mismas en los primeros meses del proyecto.

*Gráfica 4.4.1 Cantidad total de Bitcoins emitidos*



*Fuente: blockchain.info*

Hasta la fecha, se han generado una cantidad de Bitcoins por un importe superior a 1.623.000.000\$, aunque como hemos mencionado anteriormente, no toda esa cantidad se encuentra en circulación.

<sup>45</sup> <http://blockchain.info/es/charts>

<sup>46</sup> Septiembre 2013

*Gráfica 4.4.2 Capitalización del mercado de Bitcoins*



Fuente: blockchain.info

El precio de cotización del Bitcoin se mantuvo sin apenas variación durante los primeros tres años, sin embargo desde comienzos de 2013 ha sufrido un fuerte incremento en su cotización unido a una altísima volatilidad.

Como ha sucedido con otros activos, no ha estado exenta de movimientos especulativos y grandes caídas en su cotización.

La moneda ha sufrido movimientos adversos en varias ocasiones<sup>47</sup>, siendo las más importantes:

<sup>47</sup> <http://www.forbes.com/sites/timothylee/2013/04/11/an-illustrated-history-of-bitcoin-crashes/>

- 8 al 12 de junio de 2.012. Precio máximo 32\$. Caída de precio 68%.

*Gráfica 4.4.3 Cotización junio 2012*



Fuente: MtGox.com

- 17 de enero de 2012. Precio máximo 7,20\$. Caída de precio 36%.

*Gráfica 4.4.3 Cotización enero 2012*



Fuente: MtGox.com

- 17 a 19 de agosto de 2012. Precio máximo 15,25\$. Caída de precio 51%.

*Gráfica 4.4.4 Cotización agosto 2012*



Fuente: MtGox.com

- 6 y 11 de marzo de 2013. Precio máximo 49\$. Caída de precio 33%.

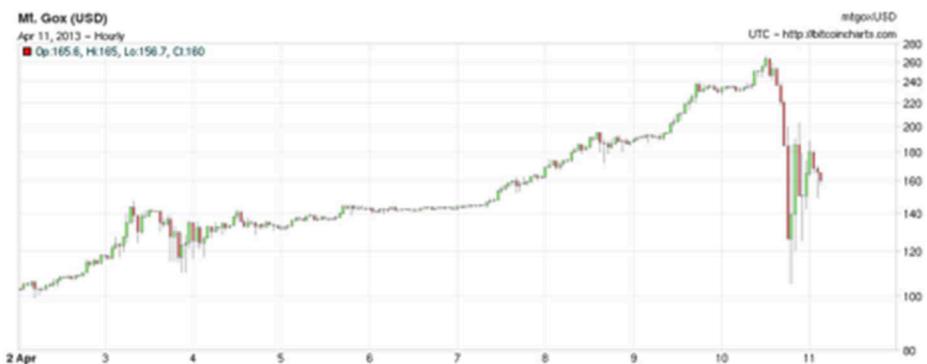
*Gráfica 4.4.5 Cotización marzo 2013*



Fuente: MtGox.com

- 10 de abril de 2013. Precio máximo 266\$. Caída de precio 61%

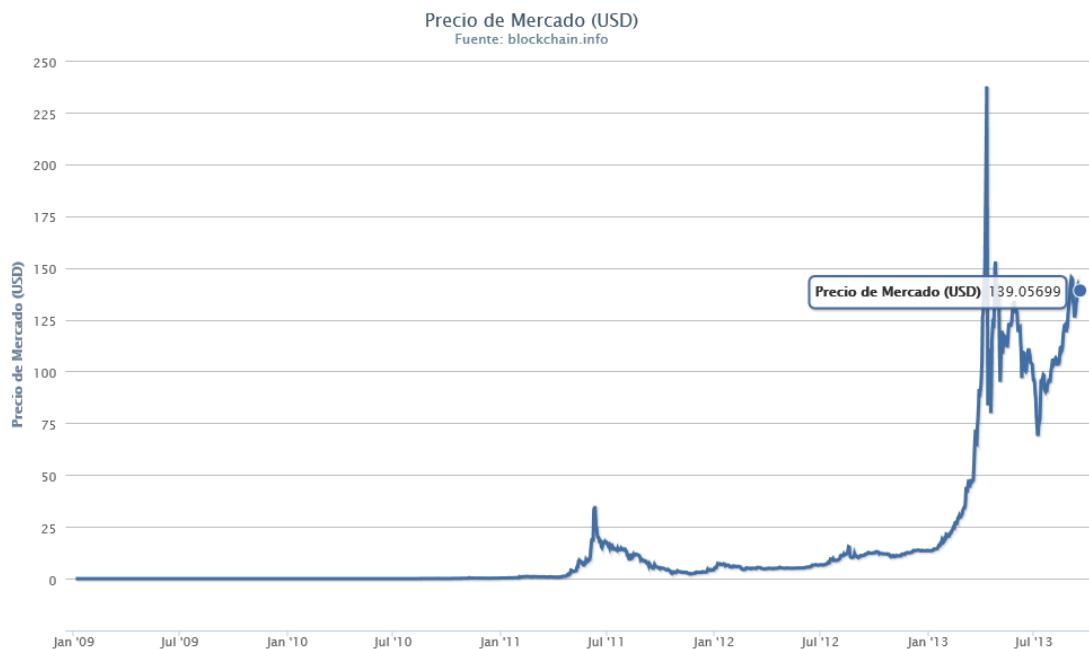
*Gráfica 4.4.6 Cotización abril 2013*



Fuente: MtGox.com

En cuanto al futuro del precio, de continuar despertando este interés, las previsiones más pesimistas calculan que se va a incrementar vertiginosamente. Si únicamente el 1% de la masa monetaria actual (alrededor de 60 billones de dólares) fuesen bitcoins, en el año 2.017 cuando se hayan extraído el 75% del total de bitcoins, el valor futuro de cada Bitcoin debería ser de 38.095\$. Por supuesto la masa monetaria mundial va a seguir incrementándose, por lo que la cotización prevista sería mayor.

*Gráfica 4.4.7 Evolución cotización hasta la actualidad*



Fuente: blockchain.info

#### 4.5. ALTERNATIVAS DIGITALES A BITCOIN

Bitcoin es el principal proyecto de desarrollo de criptomonedas, pero no el único.

Litecoin<sup>48</sup> es una moneda electrónica distribuida basada en el protocolo de Bitcoin, cuya principal diferencia es la confirmación de las transacciones de manera más rápida (2,5 minutos de media frente a 10 minutos de Bitcoin) y que utiliza un algoritmo de prueba de trabajo optimizado para el uso con CPU<sup>49</sup> y GPU<sup>50</sup> de equipos domésticos, sin ser necesario el uso de hardware especializado como en el proyecto original.

Freicoind<sup>51</sup> es otra moneda que a diferencia de Bitcoin, será repartida en su totalidad en un corto periodo de tres años, en su mayoría a instituciones benéficas y otros proyectos altruistas. Incorpora un concepto un tanto peculiar, el de *demurrage* u oxidación<sup>52</sup> del teórico económico Silvio Gesell (1862-1930), de tal manera que las carteras de los usuarios se irán depreciando un 5% anualmente en un intento de que la moneda circule y no se tienda a acaparar grandes cantidades. Ese porcentaje de depreciación irá a caer en manos de los mineros que dan soporte al proyecto.

Otro proyecto que despierta cierto interés es Ripple<sup>53</sup>. No está basando en ninguna criptomoneda aunque su funcionamiento se sustenta en redes de confianza P2P. No es en realidad la alternativa a Bitcoin ni a ninguna otra moneda electrónica, incluso de prosperar puede ayudar a complementar e impulsar otros proyectos de monedas digitales. La red de Ripple es parecida a un servicio de red social basado en la confianza mutua de sus participantes, es decir, es un sistema de emisión y gestión de crédito basado en una red punto a punto.

El funcionamiento es el siguiente. Cada nodo de Ripple actúa como un sistema de cambio local de tal manera que el conjunto de todos los nodos forman un banco mutualista descentralizado. JP Koning<sup>54</sup> compara el funcionamiento de Ripple con el sistema de

---

<sup>48</sup> <https://litecoin.org/es>

<sup>49</sup> Central Processing Unit o Unidad Central de Procesamiento

<sup>50</sup> Graphics Processing Unit o Unidad de Procesamiento Gráfico

<sup>51</sup> <http://freico.in/>

<sup>52</sup> El proceso de oxidar la moneda fue llamado, por R. Steiner “envejecimiento del dinero”, y por I. Fisher “stamp scrip”, también en los años de la Gran Depresión, según lo refiere el mismo autor (Schuldt, 1997). Por su parte Keynes (1936) lo denominó “dinero estampillado”

<sup>53</sup> <https://ripple.com/>

<sup>54</sup> <http://jpkoning.blogspot.com.ar/2013/02/ripple-or-bills-of-exchange-20.html?sref=tw>

letras de cambio que prosperó en los siglos XVII y XVIII. Estos documentos se emitían como un compromiso de pago en contraprestación de algún producto o servicio, y después eran sucesivamente endosados entre comerciantes antes de alcanzar la madurez, momento en el que el emisor se hacía cargo del pago en oro del valor nominal.

#### **4.6. REGULACIÓN INTERNACIONAL**

Ante la nueva realidad del dinero digital, son muchos los países que se están planteado regular o aceptar Bitcoin como una moneda válida.

Alemania, en respuesta a una pregunta del diputado liberal Frank Schaeffler, a través de su Ministro Federal de Hacienda reconoció<sup>55</sup> recientemente a la moneda digital como “unidad de cuenta legal”, o lo que es lo mismo, “dinero privado” mediante el cual es posible expresar valores o definir deudas. Este movimiento del Estado Alemán puede verse como una manera de ejercer un control jurídico y legal para evitar la evasión fiscal o un uso indebido de la nueva moneda.

Berlín está estudiando ahora de qué manera han de tributar las transacciones realizadas entre particulares, aunque se encuentran ante el serio problema de poder identificar a los usuarios que hagan uso de la moneda por las especiales características de la misma.

Poco después del reconocimiento alemán, ha sido Bélgica a través de su Ministro de Finanzas la que se ha posicionado<sup>56</sup> con respecto a la divisa digital.

El Ministro declaró en el Parlamento belga que a pesar de que su uso actual de es residual, el Banco Nacional de Bélgica no se opone al uso del Bitcoin. También aseguró que de momento no se ha detectado un uso indebido de la moneda para realizar operaciones de lavado de dinero, y que en caso de que esto ocurriese, sería fácil identificar a los infractores a través de las casas de cambio.

Más allá de las fronteras europeas, la Administración Tributaria de Israel ha declarado<sup>57</sup> “no podemos ignorar este fenómeno que de una manera u otra implica

---

<sup>55</sup> <http://coinrevolution.com/Bitcoin-aceptado-legalmente-en-alemania#.UkFSAiSbthE>

<sup>56</sup> <http://coinrevolution.com/se-suma-belgica-la-fiesta#.UkFYFCSbthE>

<sup>57</sup> <http://coinrevolution.com/israel-estudia-la-regulacion-Bitcoin#.UkFa1SSbthE>

transacciones financieras y por lo tanto estamos atendiendo a su importancia". De momento no es posible el uso de la moneda de un modo generalizado, pero la Asociación de Abogacía israelí sí que permite<sup>58</sup> que sus asociados puedan cobrar sus honorarios en moneda digital, lo cual es un primer paso para su uso se extienda a otros gremios.

EEUU busca desde hace tiempo regular el uso del Bitcoin. En marzo de 2013, un comunicado del FinCEN (Financial Crimes Enforcement Network) un órgano ejecutivo dependiente del Tesoro Americano, emitió una nota informativa<sup>59</sup> en la que advertía a los exchanges de moneda virtual que debían cumplir la misma normativa que los cambistas de moneda fiduciaria. En agosto, un juez norteamericano determinó<sup>60</sup> en un juicio relacionado una estafa piramidal siguiendo un esquema del tipo "Ponzi" con la moneda virtual que "Está claro que Bitcoin se puede utilizar como dinero. Se puede usar para comprar bienes y servicios, e incluso para pagar gastos corrientes individuales". Esta declaración tuvo una gran repercusión porque fue la primera vez que un órgano judicial de los EEUU equiparaba al Bitcoin con el dinero de curso legal.

El interés de las autoridades norteamericanas por la moneda ha ido en aumento desde entonces. El pasado 28 de agosto de 2013 se celebró una reunión<sup>61</sup> convocada por la Bitcoin Foundation en el edificio del Tesoro de Washington a la que asistieron representantes de los principales organismos de la Administración Norteamericana como la Reserva Federal, FBI, Financial Crimes Enforcement Network (FinCEN), Federal Deposit Insurance Corporation (FDIC), Internal Revenue Service (IRS), Drug Enforcement Administration (DEA), Department of Homeland Security (DHS), Office of the Comptroller of the Currency (OCC) o el Servicio Secreto. El objetivo de ese encuentro según un responsable del Tesoro<sup>62</sup> era conversar ampliamente sobre la moneda virtual y establecer pautas para prevenir el blanqueo de capitales y el uso de la moneda con fines delictivos. En propio FBI denunció en 2012 que el Bitcoin era utilizado por redes de delincuentes para mover dinero por todo el mundo.

Canadá ha sido uno de los países que más entusiasmo ha mostrado por el proyecto, ya que debido a una filtración, parece ser que ha demostrado incluso interés en recibir

---

<sup>58</sup> <http://www.forexminute.com/Bitcoin/now-israeli-attorneys-can-accept-payment-in-Bitcoin-for-their-legal-services-9056>

<sup>59</sup> [http://www.fincen.gov/statutes\\_regs/guidance/html/FIN-2013-G001.html](http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html)

<sup>60</sup> <http://rt.com/usa/Bitcoin-sec-shavers-texas-231/>

<sup>61</sup> <http://coinrevolution.com/eeuu-da-un-paso-gigante-en-la-regulacion-Bitcoin#.UkFmwCSbthE>

<sup>62</sup> <http://www.itespresso.es/eeuu-fundacion-Bitcoin-contra-blanqueo-dinero-115318.html>

depósitos de ciudadanos norteamericanos<sup>63</sup>. En una carta del Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) dirigida a las principales casas de cambio canadienses, se les aseguraba que en la actualidad no tenían la consideración de empresas de servicios de dinero (money service business) y por tanto estaban exentas de las restrictivas leyes que regulan ese tipo de servicios. Si la postura de las autoridades canadienses no varía, es posible que Canadá se convierta en un refugio para la operativa en Bitcoin de los ciudadanos norteamericanos.

Tailandia ha sido el único país hasta el momento que ha declarado ilegal<sup>64</sup> tanto la venta como el uso de la moneda. Miembros de la Administración de Cambio de Moneda y el Departamento de Políticas aseguraron que las actividades con Bitcoins son ilegales debido a “la falta de leyes aplicables, control de capital y el hecho de que los Bitcoins se extiendan en múltiples facetas financieras<sup>65</sup>”.

#### **4.7. ESPAÑA FRENTE AL BITCOIN**

Según Concha Martín, directora de Comunicación del Ministerio de Economía, en España de momento no hay planes para regular el uso del Bitcoin. Desde el Banco de España recuerdan que según la Ley 46/1998 de Introducción al Euro, “La única moneda de curso legal en España es el euro, al ser la única que goza de poder liberatorio y que, por tanto, debe ser aceptada obligatoriamente por un ciudadano como medio de pago de una deuda”.

De acuerdo a este artículo, un ciudadano no está obligado a aceptar como medio de pago Bitcoins si no quiere, pero tampoco se desprende que el uso de los mismos sea ilegal mientras las partes estén de acuerdo.

La falta de interés de la Administración Tributaria por ajustarse a la realidad económica del momento, puede provocar un efecto perverso mediante el cual un consumidor final puede no abonar el IVA al adquirir productos y servicios sujetos y no exentos, y todo ello dentro del marco de legalidad vigente, tal como se detalla a continuación.

---

<sup>63</sup> [http://www.theregister.co.uk/2013/05/20/canada\\_welcomes\\_Bitcoin\\_traders\\_fintrac\\_letter/](http://www.theregister.co.uk/2013/05/20/canada_welcomes_Bitcoin_traders_fintrac_letter/)

<sup>64</sup> [http://tecnologia.elpais.com/tecnologia/2013/07/31/actualidad/1375259283\\_419129.html](http://tecnologia.elpais.com/tecnologia/2013/07/31/actualidad/1375259283_419129.html)

<sup>65</sup> <http://www.elmundo.es/elmundo/2013/07/30/navegante/1375162539.html>

El Bitcoin no tiene la consideración de moneda, divisa o valor para la legislación española. El elemento que mejor definiría la realidad del Bitcoin podría ser el de “Sistema de Intercambio Comercial” (SIC) al que se accedería mediante la compra a un proveedor de Bitcoins (por ejemplo, en una casa de cambio) de un derecho de crédito canjeable en aquellos establecimientos adheridos a este sistema de pagos. El valor del Bitcoin vendrá determinado en función de su oferta y demanda, y podrá ser reintegrado en moneda de curso legal de nuevo en las casas de cambio.

Dentro de este sistema se pueden definir varios sujetos:

- Proveedor de Bitcoins es toda aquella persona física o jurídica que actúa como mediadora entre el comprador de Bitcoins y el comercio adherido al sistema, receptor final del dinero fiduciario.
- Comprador del Bitcoins es quien abona una cantidad pactada por acceder a este sistema y comprar derechos de crédito en forma de Bitcoins.
- Los Comercios adheridos aceptan los Bitcoins como forma de pago válida y podrán hacerlos efectivos de nuevo en moneda de curso legal en los proveedores de Bitcoins.

A raíz del despegue del comercio virtual tanto de bienes tangibles como intangibles, se han producido cambios significativos en los principios impositivos que deben regir la fiscalidad. La legislación se ha enfrentado a un doble reto: en primer lugar, definir como se han de gravar los bienes intangibles cuyo comercio se lleva a cabo a través de la red, y en segundo lugar, superar el concepto de ámbito de aplicación nacional que fijan las jurisdicciones fiscales existentes<sup>66</sup>.

Aunque inicialmente puede parecer evidente que las transacciones realizadas en Bitcoins dentro del territorio de aplicación deben estar sujetas a los impuestos aplicables, especialmente el IVA, un análisis más en profundidad puede demostrar lo contrario.

Según la Agencia Tributaria<sup>67</sup>, “El IVA es un tributo de naturaleza indirecta que recae sobre el consumo y grava: las entregas de bienes y prestaciones de servicios

---

<sup>66</sup> OCDE. (2000) Attribution of Profit to a permanent Establishment Involved in Electronic Commerce Transactions.

<sup>67</sup> [http://www.agenciatributaria.es/AEAT.internet/Inicio\\_es\\_ES/\\_Segmentos\\_/Empresas\\_y\\_profesionales/Empresas/IVA/Funcionamiento\\_general\\_del\\_Impuesto.shtml](http://www.agenciatributaria.es/AEAT.internet/Inicio_es_ES/_Segmentos_/Empresas_y_profesionales/Empresas/IVA/Funcionamiento_general_del_Impuesto.shtml)

efectuadas por empresarios y profesionales, las adquisiciones intracomunitarias y las importaciones de bienes”. Al aplicar el impuesto se deberán tener en cuenta los Convenios Internacionales y Tratados suscritos por España. Por medio de los Bitcoins se pueden adquirir bienes y servicios en los comercios adheridos al sistema, por lo que de acuerdo con el artículo 1 de la Ley del Impuesto sobre el Valor Añadido<sup>68</sup>, debería estar gravado por el impuesto, por lo que el proveedor del bien o servicio tendrá la obligación de retener el importe del porcentaje aplicable de IVA.

Sin embargo, suele ser habitual que la adquisición de Bitcoins se realice en países extracomunitarios, cuyo régimen fiscal no tiene porqué ser de aplicación en España.

Según el artículo 7.2 de la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico, aplicable a los proveedores de servicios establecidos fuera del ámbito de la Unión Europea y del Espacio Económico Europeo, dichas adquisiciones deberán atenerse a lo dispuesto en Tratados y Convenios suscritos por España, por lo que pagaremos el IVA si el proveedor está obligado según las leyes de su país o de los posibles acuerdos bilaterales.

Una vez adquirido ese derecho de adquisición en forma de Bitcoins, no debería existir ninguna disposición que nos obligase a pagar de nuevo el tributo al hacer uso de la moneda digital, debido a que o bien ya se ha pagado o por Ley se ha estado exento de hacerlo. En caso contrario se encontraría en un caso de “doble imposición fiscal internacional”, supuesto que suele contemplarse en la mayoría de Tratados internacionales.

El artículo 69 de la citada Ley indica que “cuando el destinatario del producto no es un empresario o profesional actuando como tal, los servicios se entenderán, a efectos de aplicación del impuesto, prestados en el territorio donde tenga la sede el prestador de los servicios, o desde el territorio donde se localice el establecimiento permanente desde el que preste los servicios, o en su defecto en el lugar donde se localice su domicilio o residencia habitual”.

A pesar de que existen criterios dispares, la doctrina de la Agencia Tributaria tiende a establecer que el IVA deberá ser cobrado en el momento de compra de ese derecho de

---

<sup>68</sup> [http://noticias.juridicas.com/base\\_datos/Fiscal/I37-1992.tp.html#a1](http://noticias.juridicas.com/base_datos/Fiscal/I37-1992.tp.html#a1)

acceso a bienes y servicios, y que debe existir una relación de comercios y establecimientos que acepten este medio de pago<sup>69</sup>.

En la actualidad existen en España varias webs donde se establece un registro de entidades donde poder emplear la moneda digital, aunque para el perfeccionamiento de este sistema en su aspecto tributario debería que confeccionarse un registro único de referencia.

A modo de resumen, mientras la Administración Tributaria no tome cartas en el asunto y de acuerdo con la legalidad vigente, se puede establecer que el usuario final que emplee Bitcoin como sistema de intercambio, no deberá abonar el IVA en el momento del pago de bienes y servicios, ya que se debe presumir que le ha sido cobrado al adquirir los Bitcoins<sup>70</sup>.

---

<sup>69</sup> Resoluciones V0053-2011 y V1858-2003 de la Dirección General de Tributos.

<sup>70</sup> Resolución V1160-11 de la Dirección General de Tributos

## CAPITULO V: EL FUTURO DE LA MONEDA DIGITAL

### 5.1. VENTAJAS Y LIMITACIONES DEL MODELO DIGITAL

El carácter innovador de la nueva moneda presenta importantes ventajas con respecto a la moneda fiduciaria tradicional, aunque también cuenta con una serie de aspectos negativos a tener en cuenta.

Al ser una moneda que no está emitida ni cuenta con el respaldo de ningún gobierno o entidad, el Bitcoin escapa a cualquier control acerca de su convertibilidad. No es posible devaluarla ni establecer ningún tipo de control sobre su uso ni sobre su cotización, que fluctuará libremente dependiendo de la oferta y demanda del mercado.

Cualquier intento de un gobierno por acabar con ella resultaría técnicamente imposible al igual que ha sido imposible restringir el intercambio de archivos por redes tipo Torrent o Emule. Las autoridades norteamericanas consiguieron clausurar el portal de Napster o Megaupload debido a que la información residía en un único punto, pero gracias al carácter distribuido de Bitcoin, copias de la misma base de datos que sustenta el sistema se encuentran en millones de ordenadores de todo el mundo, por lo que es imposible acabar con el proyecto.

Una de las principales ventajas es la facilidad con la que se pueden realizar transacciones económicas verificables en pocos minutos y con un coste prácticamente nulo o nulo a miles de kilómetros de distancia y sin que la normativa de cada país pueda suponer un obstáculo. Sin embargo la velocidad de verificación de una transacción está todavía lejos de la de una operación con tarjeta de crédito de apenas un minuto, por lo que puede suponer un problema en aquellas transacciones que necesitan immediatez en la verificación de un pago como puede ser en un comercio.

Por su carácter intangible, es una moneda muy fácil de transportar y de almacenar, sin necesidad de tener que contar con medidas de seguridad excepcionales. Una alternativa muy simple a la hora de guardar Bitcoins están en los monederos papel. Este tipo de almacenamiento está recomendado especialmente para protegerse frente a robos, virus informáticos o fallos en el hardware de los equipos que los almacenan. Consiste simplemente en apuntar en un trozo de papel la clave privada de una billetera Bitcoin. A

partir de esa clave privada es posible obtener la clave pública o dirección de una cartera Bitcoin y acceder al saldo que en ella se almacena. El caso más extremo de simplicidad a la hora de almacenar Bitcoins están en los denominados “Brain Wallets”, en los que no se requiere más que el usuario recuerde una frase a partir de la cual se podrá generar la clave privada de su monedero y por ende la clave pública que dará acceso al saldo de Bitcoins.

Su carácter intangible la hace perfecta para un uso común por medio de dispositivos electrónicos, sin embargo puede dificultar su uso entre sectores de la población con déficit tecnológico a los que les cuesta usar medios de pago electrónico, o simplemente no cuentan con los medios tecnológicos necesarios y acceso a Internet como ocurre en determinadas zonas subdesarrolladas del planeta. No obstante sí que están surgiendo compañías como Casascius<sup>71</sup> que han puesto en circulación monedas físicas de Bitcoin, por lo que siempre existe la opción de hacer uso del papel moneda.

Bitcoin es intrínsecamente una moneda segura. Desde el comienzo del proyecto no se ha producido ninguna situación donde se haya visto comprometida la integridad del mismo. Los recursos necesarios para intentar, por ejemplo, duplicar una única transacción requeriría tomar el control de más del 50% de la red Bitcoin, por lo que sería más rentable para alguien que contase con semejante capacidad de cálculo hacer un uso legítimo de los equipos obteniendo Bitcoins mediante minado.

Sin embargo sí es habitual los robos de las claves de los monederos de Bitcoins por parte de crackers que acceden tanto a ordenadores de uso personal como a los sistemas de las casas de cambio, haciéndose con sustanciosos botines que dado el carácter anónimo de las transacciones, hacen prácticamente imposible que se puedan recuperar.

Las transacciones en Bitcoins son irreversibles, por lo que hay que prestar especial atención a la hora de realizar un envío de monedas a un desconocido por ejemplo en una compra online, ya que en caso de estafa no puede retrocederse la operación realizada.

También es frecuente la pérdida de Bitcoins de usuarios que no han realizado copias de seguridad de sus monederos y sufren un robo de sus equipos o un fallo de hardware como por ejemplo la avería de un disco duro.

---

<sup>71</sup> <https://www.casascius.com/>

Como estas situaciones se dan con relativa frecuencia, han surgido empresas forenses de servicios digitales<sup>72</sup> que se encargan tanto de intentar recuperar los Bitcoins de dispositivos de almacenamiento dañados, como de seguir el rastro a las monedas robadas a través de la cadena de bloques con el fin de detectar cuándo se intentan cambiar por dinero fiduciario y tratar de identificar a los implicados.

Esta nueva moneda puede ser utilizada a nivel global, incluso para realizar transacciones con aquellos países que por razones políticas se encuentran sometidos a un bloqueo económico por la Comunidad Internacional como puede ser el caso de Irán<sup>73</sup>. Recientemente la criptomoneda adquirió un papel protagonista en el caso WikiLeaks ya que el Gobierno de los EEUU consiguió que los principales medios de pago como VISA, Mastercard o PayPal no permitiesen realizar donaciones al proyecto ni a su fundador Julian Assange a través de sus pasarelas, por lo que el único medio para colaborar en su financiación era mediante donaciones en Bitcoins.

Existen países en los que Bitcoin está siendo adoptado como reserva de valor para luchar contra las fuertes tasas inflacionistas como es el caso de Argentina (30%) o Venezuela (45%), donde además la compra de otras divisas refugio como el dólar está muy restringida.

El carácter anónimo de las transacciones realizadas en esta moneda también tiene su lado oscuro ya que permite el comercio ilegal de sustancias prohibidas, armas o cualquier otro producto o servicio a espaldas de las autoridades. Existen sitios dentro de la llamada Internet Profunda como SilkRoad donde es posible adquirir cualquier tipo de droga realizando el pago en Bitcoins.

## 5.2. FUTURO

A lo largo de este estudio se ha ido demostrando que Bitcoin está sustentado por un sólido proyecto, y que la comunidad internacional está demostrando un creciente interés, aunque de momento casi únicamente por su carácter especulativo.

---

<sup>72</sup> <http://www.sytech-consultants.com>

<sup>73</sup> <http://www.businessweek.com/articles/2012-11-29/dollar-less-iranians-discover-virtual-currency>

La moneda no solo ha despertado el interés del pequeño inversor. Incluso grandes inversionistas como los hermanos Tyler y Cameron Winklevoss, supuestos ideólogos de Facebook, cuentan con aproximadamente el 1% de los bitcoins en circulación, lo que equivale en la actualidad a más de 15 millones de dólares.

Existen además compañías como Exante Ltd con sede en Malta que permite a las instituciones y grandes patrimonios acceder al mercado Bitcoin mediante un fondo de inversión, para lo que se exige desembolsar un mínimo de 100.000 euros.

Otro aspecto que preocupa a los expertos es el carácter deflacionario de Bitcoin. A medida que la cantidad de monedas se aproxime a su límite prefijado de 21.000.000, la economía Bitcoin entrará en deflación<sup>74</sup>. Este incremento de valor no implicará un problema fraccionario, ya que en estos momentos se puede operar utilizando hasta ocho decimales, lo que equivale a contar con 2,1 cuatrillones ( $2,1 \times 10^{15}$ ) de unidades totales. Llegado el caso, se podría extender el número de decimales ilimitadamente.

El objetivo deflacionista del proyecto busca evitar la inflación monetaria que se produce debido a que al haber abundancia de moneda en manos de los consumidores, estos estarán dispuestos a pagar más por adquirir bienes y servicios por lo que de acuerdo al principio de oferta y demanda los precios se incrementarán.

La deflación intrínseca del Bitcoin está provocando movimientos especulativos importantes. Ante un escenario de unidades monetarias limitadas y debido al creciente interés por la moneda digital, se han producido situaciones de gran volatilidad duplicando y triplicando su valor en pocos días. El pico más importante en su cotización se produjo el 10 de abril de 2013, alcanzando un valor máximo al cambio de 266\$/btc cuando justo un mes antes su cotización era de 47,95\$/btc.

Los expertos advierten que si la moneda alcanzase un peso específico considerable dentro de la economía global, podía tener consecuencias negativas dado su carácter inflacionario.

La deflación consiste en una caída generalizada y constante de los precios en una economía. A pesar de que en principio puede parecer algo positivo, no es así. Ante un escenario en el que los precios bajan día a día, o lo que es lo mismo, la moneda se

---

<sup>74</sup> <http://elBitcoin.org/Bitcoin-y-deflacion/>

revaloriza constantemente, el consumo se frenará debido a que la gente esperará a que los precios bajen aún más para realizar sus compras. Al disminuir la demanda, el dinero no circula y el precio de los bienes baja en un intento de reactivar el consumo. Esta bajada generalizada es interpretada por los consumidores como que no merece la pena comprar hoy porque posiblemente mañana los precios sean todavía menores, y se entra en un círculo vicioso de consecuencias fatales.

Por lo tanto el carácter inflacionista de la moneda digital es un arma de doble filo que puede hacer peligrar su futuro. Por un lado, es evidente que despierta el interés del inversor y de la población que ve en ella un medio de atesoramiento de riqueza, lo cual no es el fin último de la existencia del Bitcoin.

Para que la moneda alcance el éxito pleno debe de ser empleada como medio de circulación, e ir sustituyendo de manera parcial o total al dinero fiduciario. Sólo cuando la población pueda elegir con qué moneda quiere realizar el pago de los bienes que adquieren en el día a día, se podrá asegurar que Bitcoin es un éxito.

## CAPITULO VI: CONCLUSIÓN

Todavía es pronto para valorar si Bitcoin es la moneda del futuro o no es más que un nuevo tipo de tulipán digital que algún día estallará en una gran burbuja especulativa, haciendo pedazos a más de una economía doméstica, pero sí que es verdad que ha llegado en un momento muy adecuado.

Por un lado estamos inmersos en una etapa de despegue tecnológico sin precedentes, gracias en su mayor parte a Internet. Además, el uso de tecnología por parte de la población está muy generalizado e interiorizado, de tal manera que cada vez estamos más receptivos a nuevos sistemas que ya forman parte de nuestra vida, como por ejemplo, los pagos online con PayPal, o aquellos que están por venir, como el uso generalizado de la tecnología NFC<sup>75</sup>.

Además, la confianza de la población en el sistema bancario está bajo mínimos. Ciudadanos de países como Chipre o Argentina, donde de la noche a la mañana han visto sus depósitos mermados o congelados, ven en la moneda digital un medio para preservar su patrimonio, lejos de un nuevo colapso del sistema bancario.

Es un sistema de intercambio de valor que aporta muchas ventajas sobre el dinero convencional, pero uno de los mayores retos a los que ahora se enfrenta, es ganarse la confianza de la gente, al igual que lo ha logrado, aunque quizás por imposición legal, el dinero fiduciario.

Detrás de Bitcoin no se encuentra ningún banco central ni organización que respalde su valor, aspecto que hay quien lo considera positivo. La confianza en esta divisa la genera la propia tecnología y el conocimiento en profundidad de su funcionamiento, al igual que la moneda de un país se basa en la confianza que los ciudadanos tienen en su sistema financiero.

La divisa digital se sustenta por un sólido proyecto en constante evolución sin que se haya detectado ni un solo agujero de seguridad que haya podido comprometer la seguridad del sistema en los cuatro años que lleva en funcionamiento. Bitcoin viene a ser a la moneda tradicional lo que el correo electrónico al correo postal.

---

<sup>75</sup> <http://www.xataka.com/moviles/nfc-que-es-y-para-que-sirve>

De hecho, el proceso de creación de Bitcoin tiene una base matemática detrás de la que carece el dinero fiduciario, que es creado de la nada en función de las expectativas de crecimiento económico de un grupo de personas, y multiplicado por el efecto de los depósitos bancarios.

Una vez más la regulación administrativa va por detrás de la realidad de los mercados, y en el caso de Bitcoin, es posible que los gobiernos de todo el mundo estén subestimando el potencial de la moneda electrónica. Unicamente Alemania y Canadá parecen ser conscientes de que el Bitcoin es el equivalente a una cuenta bancaria en Suiza para el común de los ciudadanos, y que lo deben tener en consideración desde esta etapa inicial legislando para regular su uso, o puede convertirse en el motor de una economía sumergida a escala global que escape a su control en poco tiempo.

El éxito de Bitcoin radica en que sepa mantener la misma expectación que ha causado hasta ahora y que sus usuarios dejen de atesorarlos a la espera de que se produzca una nueva subida en su cotización con el fin de especular, y se comiencen a utilizar como cualquier otra moneda de uso común en las compras del día a día.

Si el Bitcoin va a ser un rotundo éxito o un estrepitoso fracaso, sólo el tiempo lo dirá.

## BIBLIOGRAFIA

- [Libros](#)
  - Zevallos Avilés, Günter. *Fundamentos de Economía Política*. 1<sup>a</sup> edición, 2.007. Prensas Universitarias de Zaragoza. ISBN 978-84-7733-950-2
  - *Plan General de Contabilidad y de PYMES* 2008. 2<sup>a</sup> edición corregida, 2.008. Ediciones Pirámide (Grupo Anaya, S.A.). ISBN 978-84-368-2177-2
- [Papers](#)
  - Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2.008
  - Dai, Wei. *B-Money*. 1998
- [Webpages](#)
  - <https://www.casascius.com>
  - <http://www.bolsaone.net>
  - <http://www.fsf.org>
  - <http://ingeniatic.euitt.upm.es>
  - <http://www.weidai.com>
  - <http://www.mail-archive.com>
  - <http://bitcoin.org>
  - <https://es.bitcoin.it>
  - <http://p2pfoundation.ning.com>
  - <http://elbitcoin.org>
  - <https://bitcoinfoundation.org>
  - <http://www.genbetadev.com>

- <http://bitaddress.org>
- <http://www.coinrevolution.com>
- <http://elblogdeltoguero.blogspot.com>
- <http://www.blockchain.info>
- <http://www.top500.org>
- <http://bitcoinwatch.com>
- <https://www.mtgox.com>
- <http://www.bitcoinity.org>
- <https://bitcoin-24.com>
- <https://litecoin.org>
- <http://freico.in>
- <https://ripple.com>
- <http://jpkoning.blogspot.com.ar>
- <http://www.whitehouse.gov/about/presidents/thomasjefferson>
- <http://www.forbes.com>
- <http://www.sytech-consultants.com>
- <http://www.businessweek.com>
- <https://exante.eu>
- <http://www.forexminute.com>
- <http://www.fincen.gov>
- <http://rt.com>

- <http://www.itespresso.es>
- <http://www.theregister.co.uk>
- <http://tecnologia.elpais.com>
- <http://www.elmundo.es>
- <http://www.agenciatributaria.es>
- <http://noticias.juridicas.com>