



**LA NUEVA MONEDA VIRTUAL QUE ESTÁ REVOLUCIONANDO
EL MUNDO DE LAS DIVISAS DIGITALES**

Proyecto Fin de Máster (SGR031)

Máster en Gestión Financiera y Contabilidad Avanzada

Universidad Jaume I, Castellón

AUTORA: YASMINA ASENSIO GRAU

TUTORA: LUISA NIETO SORIA

ÍNDICE

I.	Introducción.....	pág. 4
II.	¿Qué es un Bitcoin?.....	pág.5
III.	¿Cómo funciona el sistema Bitcoin?.....	pág.7
IV.	¿Cómo conseguirlos?.....	pág.17
V.	Historia del Bitcoin.....	pág.20
VI.	Ventajas y Desventajas.....	pág.27
VII.	Cotización BITCOIN/DÓLAR/EURO.....	pág.31
VIII.	Conclusión.....	pág.37
IX.	Bibliografía.....	pág.39

Resumen

Bitcoin es una moneda que en los últimos años ha tomado mucha importancia, aunque aún se considera una moneda digital en desarrollo. Por dicha importancia, mi objetivo en el presente trabajo ha sido explicar qué es el Bitcoin en su totalidad, analizar su evolución y comprobar si entre el Bitcoin y otras dos divisas existe arbitraje.

Asimismo, podemos considerar que el Bitcoin es una moneda virtual que, por diferenciarse en determinados aspectos de las demás ha conseguido una enorme popularidad, ya que presenta aspectos que otras monedas no tienen. Y como todas las monedas presenta sus ventajas, como su capacidad de divisibilidad, bajos costes de transacción, anonimato, etc. Pero también tiene inconvenientes, como son su valor volátil, su falta de aceptación, etc.

Durante sus 5 años de existencia, su progreso no ha sido constante, sino que ha tenido momentos de auge, como cuando a finales del 2013 llegó a su precio máximo, y de crisis, ya que ha habido momentos en los que alguno de sus intermediarios financieros ha tenido problemas y ha hecho caer el precio en picado, como en el 2011. Además, al realizar la comparación entre precios de mercado y precios cruzados, se observa que, con los datos con los que trabajo, puede existir posibilidad de arbitraje entre Bitcoin, Dólar y Euro.

Códigos JEL

G15, G23, G10, F31

Palabras clave

Bitcoin, bróker, wallet/monedero, Bloque, Criptomoneda, Hash, Minería, Nodo, P2P,

I. Introducción

La ciencia evoluciona y con ella, las tecnologías, esta evolución se debe a la necesidad de mejorar el bienestar de las personas. Un claro ejemplo de esta mejora se puede ver en las prestaciones de servicios que cada vez resultan más cómodas para las personas.

Uno de los temas con mayor importancia en la actualidad, son las diferentes formas de pago, ya que las transferencias por internet han aumentado y la gente intenta buscar la manera más fácil y económica para realizarlas. Por esta misma razón, hace años ya empezaron a surgir las primeras monedas virtuales, aunque ninguna con gran notoriedad. En cambio, en los últimos años una nueva moneda está revolucionando el sistema virtual, el Bitcoin, palabra que a pesar de estar teniendo mucha importancia actualmente, aún hay muchas personas que desconocen para que se utiliza, sus beneficios, sus inconvenientes...

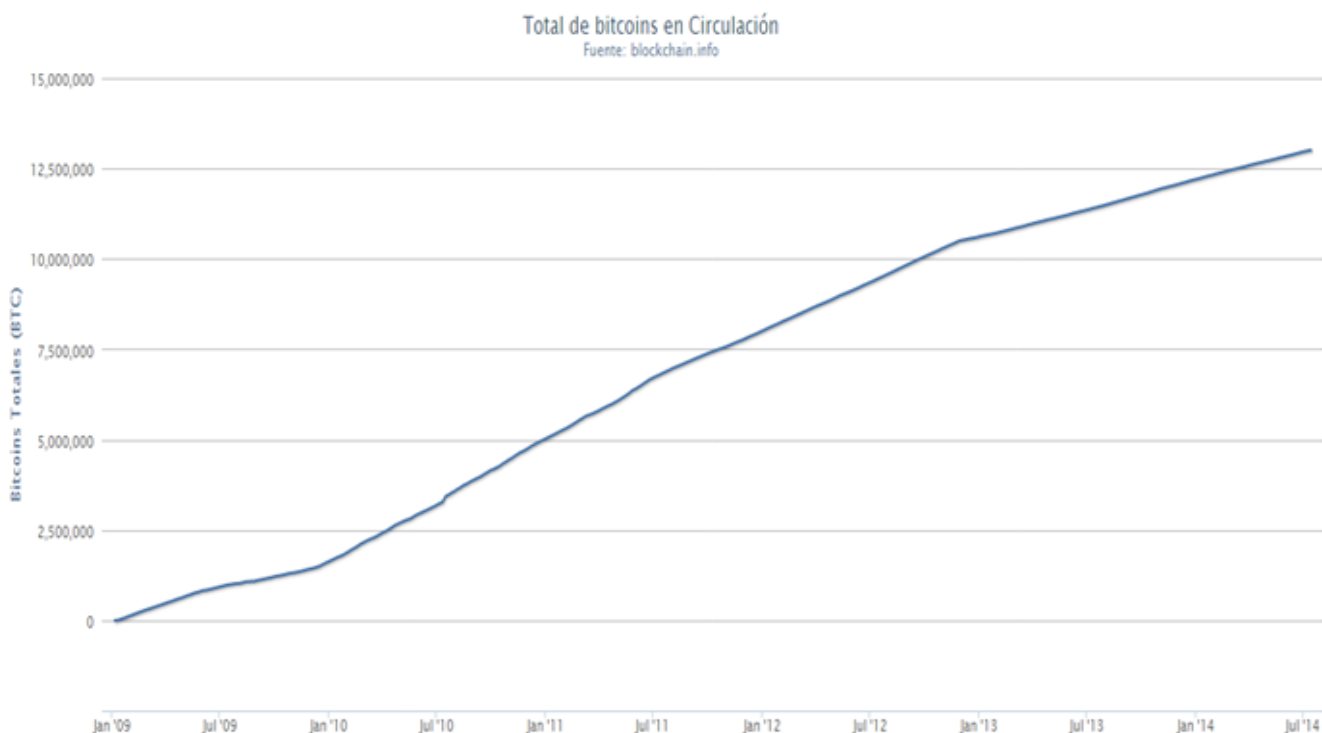
Por lo tanto, en el presente trabajo pretendo explicar de forma sencilla los principales aspectos del sistema Bitcoin, ¿qué es exactamente Bitcoin? Definirlo de forma que todo el mundo lo pueda entender, ¿Qué le hace tan especial? Bitcoin tiene alguna característica que le ha diferenciado del resto de monedas virtuales, ¿Cómo funciona? Mecanismos que se utilizan para poder manejarlo y cómo hacerlo, ¿Cómo ha sido su evolución desde su creación? Desde su creación el Bitcoin ha pasado por diferentes fases, auges y crisis ¿Ventajas? ¿Desventajas? Una vez explicado el mecanismo de esta nueva moneda virtual aportaré mis puntos de vista negativos y positivos respecto al Bitcoin.

Además, para concluir el trabajo realizaré un análisis económico para comprobar si entre el Bitcoin y otras dos divisas (euro, dólar) puede existir arbitraje. Para realizar este estudio utilizaré el precio de mercado del dólar frente al euro y su precio cruzado, es decir el cociente entre el dólar frente al Bitcoin y el euro frente al Bitcoin. Si no coinciden ambos precios podríamos decir que existe arbitraje. Asimismo para poder comprobarlo más específicamente lo formalizaremos con un análisis estadístico para comprobar si los dos tipos de cambio (mercado y cruzado) son iguales.

II. ¿Qué es un Bitcoin?

Bitcoin es una moneda virtual nacida en 2008 que, como cualquier otra moneda virtual, se utiliza para comprar y vender online, también se puede realizar cambio de moneda con otras divisas como Dolares, Euros, o Yens.

Esta nueva moneda virtual no está controlada por a gobiernos, bancos centrales y entidades financieras ya que no pertenece a ningún Estado o país, nadie controla la emisión de dinero en el mercado, la cual es limitada, es decir, cuando la cantidad de Bitcoins llegue a los 21 millones se dejará de producir dicha moneda. Su creador, el cual posteriormente nombraré, impuso este límite para evitar la saturación del mercado y así, la pérdida de valor. Actualmente, a fecha de 15/07/2014 sabemos que hay en circulación 13.0170.800 bitcoins, cifra que según vemos en el gráfico ha ido aumentando de manera continuada.



Fuente: blockchain.info

En un principio parece una moneda virtual como las que se han creado en otras ocasiones, pero tiene algo que lo diferencia de las demás y es que tiene un sofisticado sistema criptográfico que hace imposible su falsificación.

- ¿Cómo se fija el valor del Bitcoin?

El valor del Bitcoin depende de la aceptación del mismo, se basa en la confianza que la sociedad deposita sobre él, es decir, cuantos más usuarios acepten pagos con Bitcoins el valor de este aumentará con respecto a cualquier otra divisa, si fuese al contrario su valor respecto a otra divisa, disminuiría. En definitiva, cuanto más se conozca el Bitcoin y más gente confíe en esta moneda virtual, más aumentará su demanda en los mercados de intercambio, con lo cual incrementará su valor. Actualmente, a fecha 17/07/2014 está en 614 \$ y 455.40 €.

- ¿Quién lo creó?

Es la pregunta que se han hecho todos los interesados en el Bitcoin desde su creación. Hasta hace unos meses, es decir, hasta marzo de este mismo año, solo se conocía que su creador estaba escondido bajo un seudónimo, Satoshi Nakamoto, pero nadie sabía a quién correspondía este nombre hasta meses atrás.

La revista Newsweek afirmó haber encontrado al verdadero creador del Bitcoin, un estadounidense de 64 años llamado Dorian S. Nakamoto, ya que todas las pruebas que aportaba el artículo les llevaba hasta él. Pero horas más tarde, esa misma persona negó ser el creador del Bitcoin, afirmando que hasta hace poco tiempo atrás no sabía de la existencia de esta nueva moneda virtual.

Además, el “en teoría” creador del Bitcoin rompió su silencio escribiendo, en el mismo foro donde lo dio a conocer como una moneda abierta, negando que Dorian sea el verdadero Satoshi Nakamoto, aunque aún se está investigando si ese mensaje lo escribió el verdadero creador del Bitcoin, o alguien que ha conseguido un acceso no autorizado a su cuenta.

Por consiguiente, se sigue sin conocer la verdadera identidad del creador de la moneda virtual que está dando mucho que hablar en los últimos años.

III. ¿Cómo funciona el sistema Bitcoin?

Bitcoin es un sistema bastante sencillo de utilizar, esta nueva moneda virtual es creada por un proceso, considerado competitivo y descentralizado llamado “minería”, a las personas que participan en este proceso se llama “mineros”. Los mineros, resuelven las transacciones y se aseguran de su veracidad utilizando equipos informáticos especializados.

. En el apartado IV del trabajo podemos encontrar la operación de minería mejor definida y de manera más extensa.

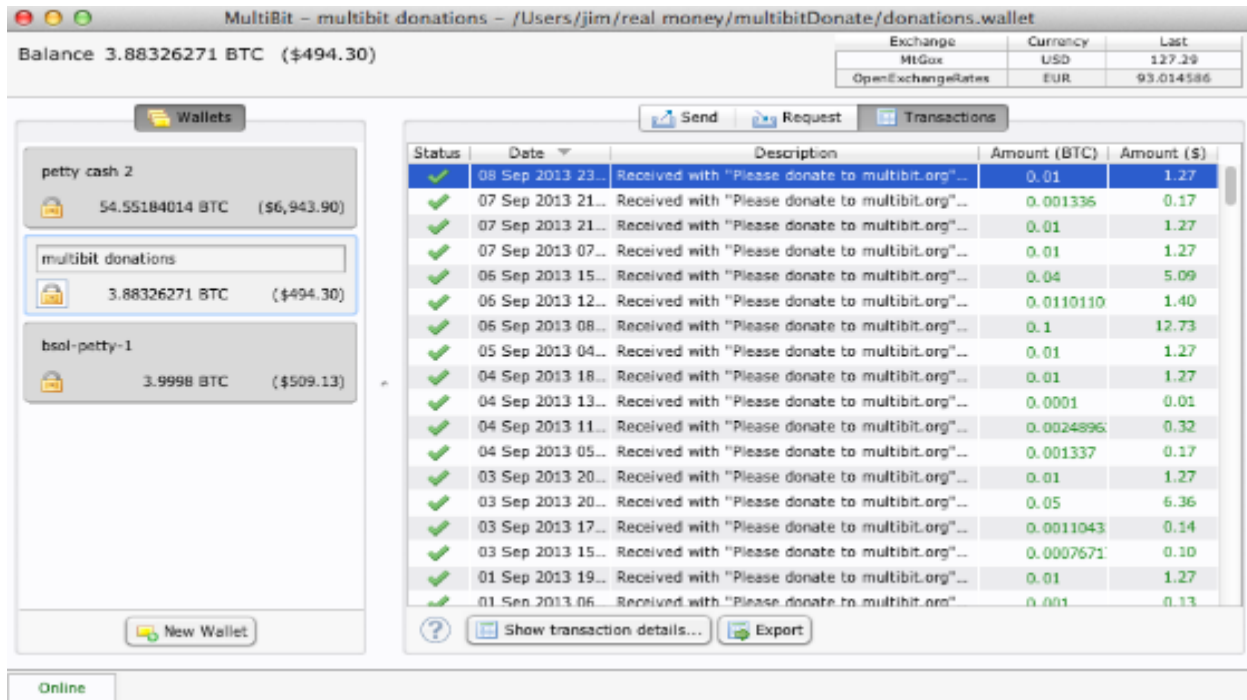
Como cualquier moneda, los bitcoins tienen un lugar donde guardarse, a diferencia de las monedas no virtuales, que son los bancos quien las almacena, el sistema bitcoin tiene unas aplicaciones, llamados monederos que son programas que guarda los bitcoins que una persona posee y permiten, transferir y recibir Bitcoins sin intermediarios mediante sus claves privadas.

Antes de empezar a explicar cómo funciona el sistema de transacciones de bitcoins se debe saber desde dónde operar, si de manera online o desde el propio ordenador, móvil o Tablet. Si decidimos que queremos operar desde nuestros propios dispositivos se ha de descargar el monedero para tenerlo en nuestro ordenador y así operar desde ahí. No sólo existe un monedero disponible, hemos de buscar los distintos monederos, ver sus características y decidir cuál es el que más nos interese.

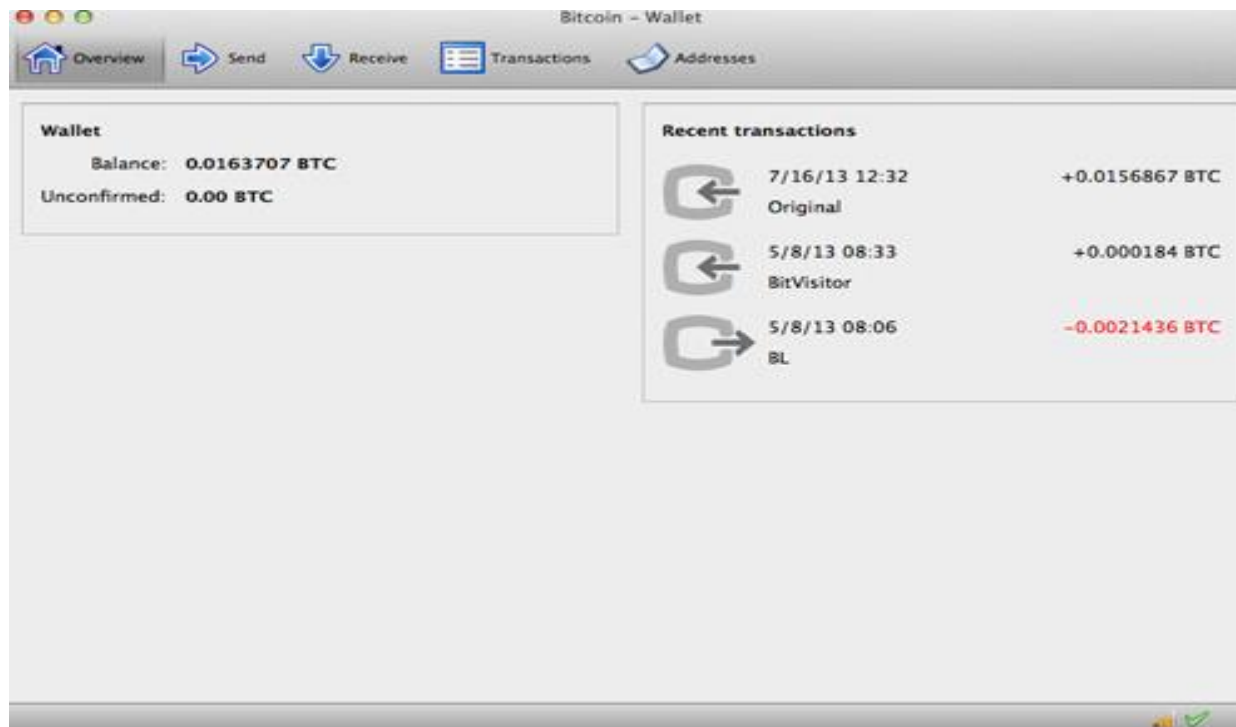
En primero lugar tenemos que saber que hay monederos distintos según queramos descargarlo a un móvil, a una Tablet o a un ordenador.

Los monederos más utilizados para ordenadores son:

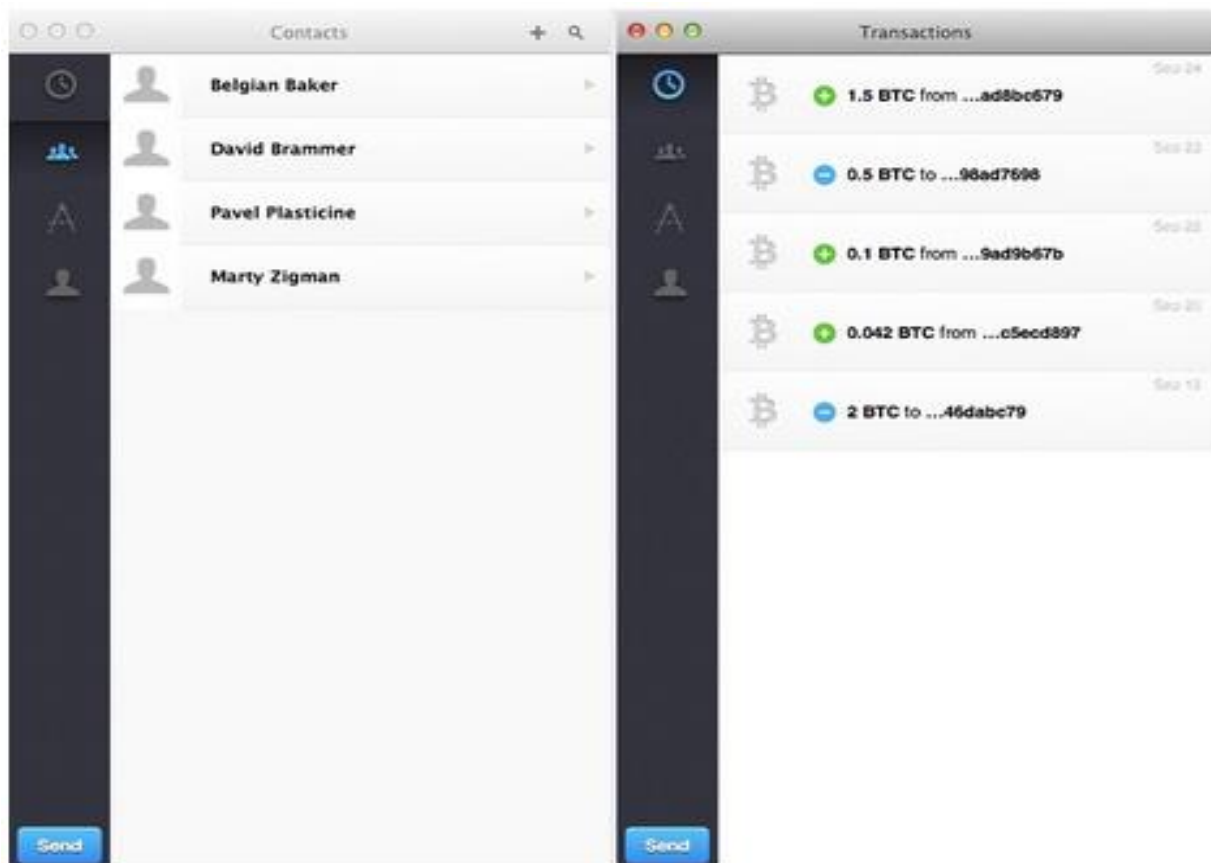
MultiBit → MultiBit es un programa rápido y fácil de usar. No necesita descargar toda la cadena de bloques para poder empezar a operar, por lo tanto, está listo para poder usarse en pocos minutos. MultiBit está traducido en más de 35 idiomas, característica que hace que sea tan utilizado en todo el mundo. Es una buena opción para los usuarios que no son técnicos, ya que está hecho para usuarios principiantes. Está disponible para Windows, Mac y Linux.



Bitcoin Core → Es un monedero creado por Satoshi Nakamoto y se considera uno de los más importantes de la red Bitcoin. Ofrece alta seguridad, privacidad y estabilidad, pero tiene una gran desventaja frente a otros monederos ya que necesita mucho espacio en el disco y memoria porque necesita descargar toda la información de la cadena de bloques. Se encuentra disponible para Windows, Linux, Mac y Ubuntu PPA.



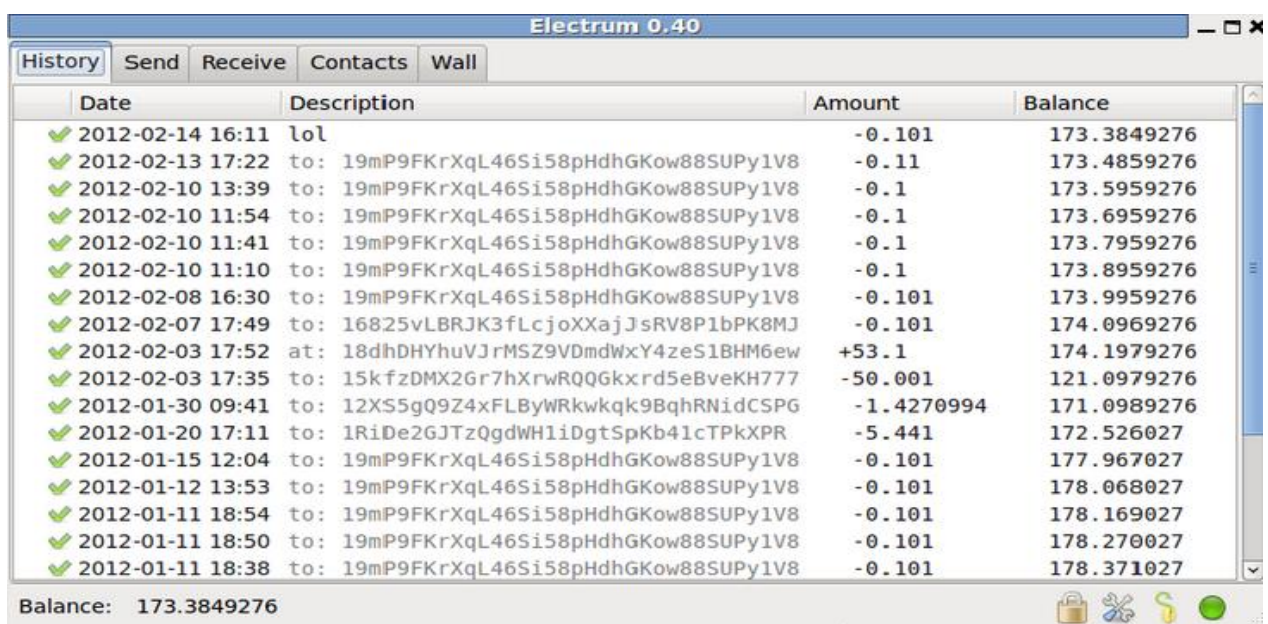
Hive OS X → Monedero fácil de usar y rápido ya que incorpora un sistema para acelerar el tiempo de arranque. Contiene un servicio de mensajería instantánea entre los contactos que lo utilizan y también está traducido en varios idiomas. Una característica muy positiva que tiene este monedero es que tiene el apoyo de la red Tor, red que permite mayor anonimato porque no desvela las direcciones IP. Está disponible en Mac OS X, pero también llegará para Android.



Armory → Es uno de los monederos con más características disponibles actualmente, muy popular entre los usuarios avanzados, pero además ofrece también otros modos de usuario más básicos. Una de sus características es que incluye un teclado gráfico para poder protegerse contra los keyloggers, personas que con la pulsación del teclado memorizan contraseñas. Además, ofrece diferentes opciones para poder almacenar el monedero en ordenadores sin conexión a internet, ya que las transacciones fuera de línea aportan más seguridad a la cartera. Armory está disponible en Windows, Mac y Linux y para poder utilizarlo se necesita tener descargado una de estas dos aplicaciones, Bitcoin-qt o Bitcoind.

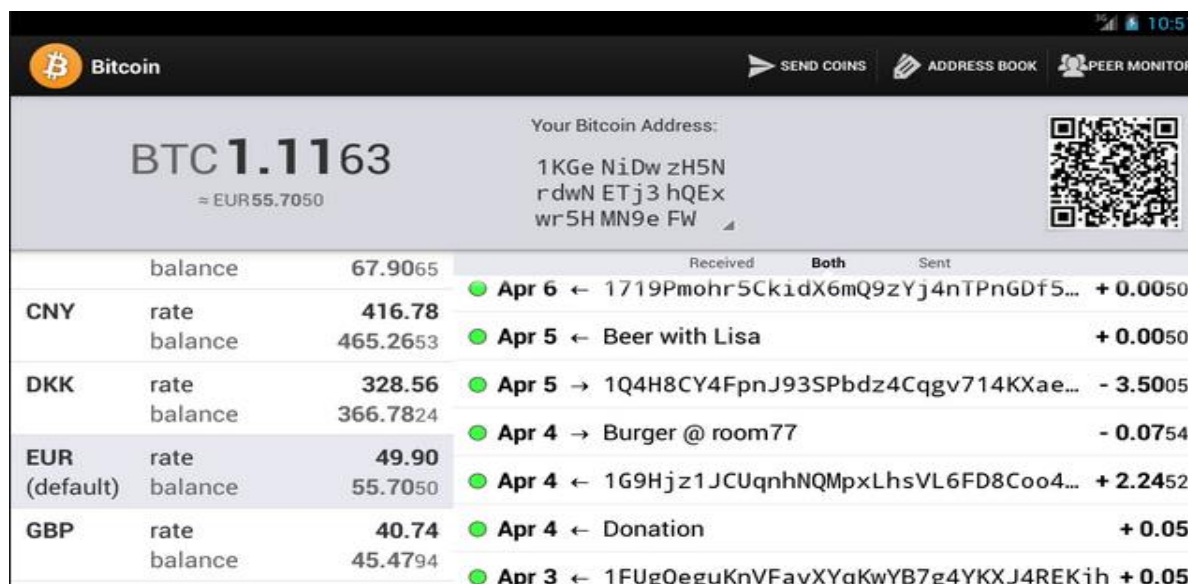


Electrum → Monedero fácil de utilizar y rápido, se caracteriza por su sencillez. Además, como Multibit, Electrum permite realizar transacciones sin tener que descargar toda la cadena de bloques. Utiliza servidores que se encargan de las partes más complejas del sistema, como por ejemplo, la creación de un código llamado “semilla” con el cual se podría recuperar el monedero en caso de pérdida de la clave privada. La semilla permite restaurar y hacer copias de seguridad sin necesidad de ninguna otra información. Electrum está disponible para Windows, Mac, Linux y Android.



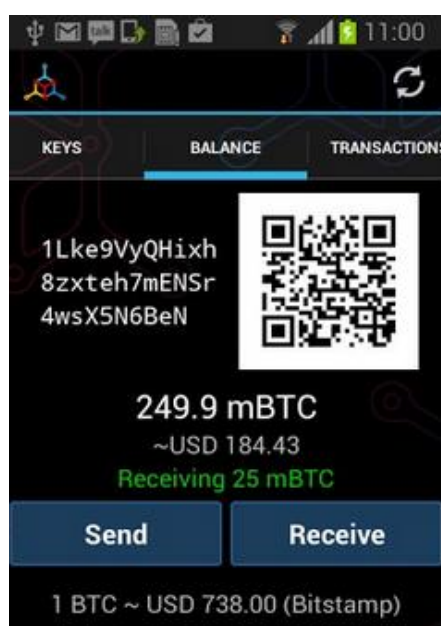
Los monederos más utilizados para tablets o móviles son:

Bitcoinwallet → Monedero más conocido para estos dispositivos, sencillo, seguro y rápido. Es el mejor monedero para principiantes en el sistema Bitcoin. Está disponible para Android y Blackberry.

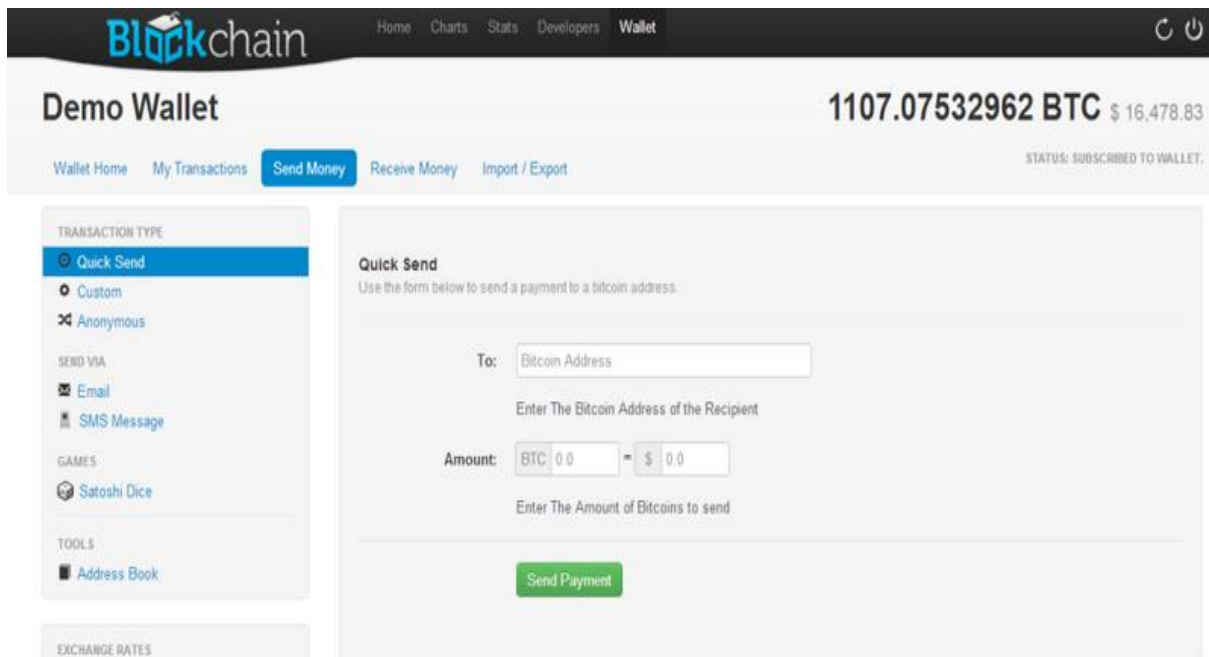


	balance	67.9065		Received	Both	Sent
CNY	rate	416.78		Apr 6 ←	1719Pmohr5CkidX6mQ9zYj4nTPnGDf5...	+ 0.0050
	balance	465.2653		Apr 5 ←	Beer with Lisa	+ 0.0050
DKK	rate	328.56		Apr 5 →	1Q4H8CY4FpnJ93SPbdz4Cqgv714KXae...	- 3.5005
	balance	366.7824		Apr 4 →	Burger @ room77	- 0.0754
EUR (default)	rate	49.90		Apr 4 ←	1G9Hjz1JCUqnhNQmpxLhsVL6FD8Coo4...	+ 2.2452
	balance	55.7050		Apr 4 ←	Donation	+ 0.05
GBP	rate	40.74		Apr 3 ←	1FUgQeguKnVFavXYqKwYB7g4YKXJ4REKjh	+ 0.05
	balance	45.4794				

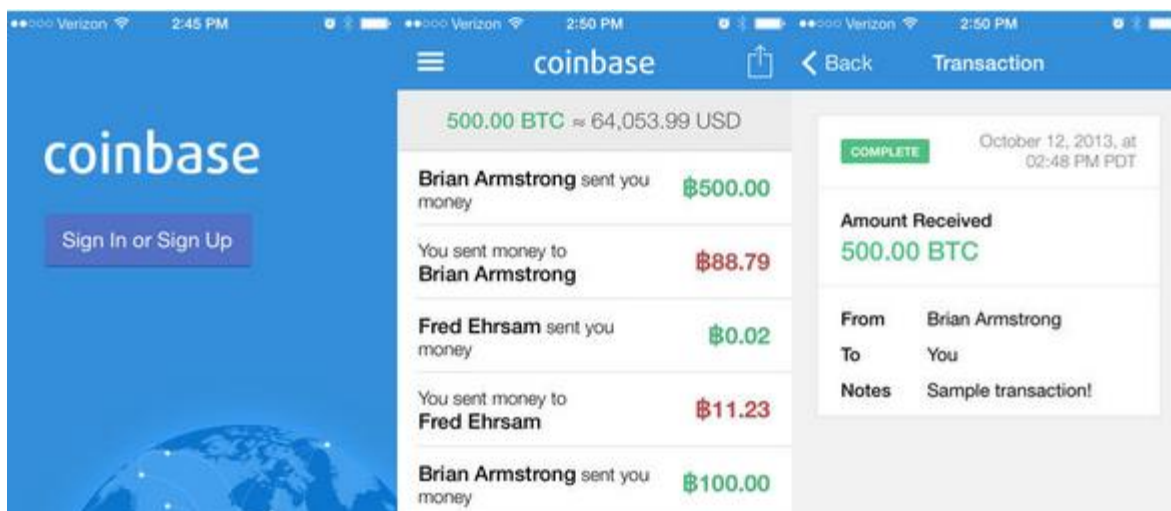
Mycelium → Monedero en auge actualmente siendo uno de los que realiza las transmisiones de Bitcoins de manera más rápida. Posee dos características que atraen a los usuarios ya que permite el contacto entre dos personas para comprar y vender bitcoins con un sistema de mensajería cifrado y además a los usuarios pueden conocer qué negocios aceptan Bitcoin y conocer las ubicaciones de cajeros automáticos cercanos.



Blockchain.info → monedero para móviles basado en un servicio web, incluye muchas características de la página como las copias de seguridad, encripta las claves privadas en el móvil y hace una copia de seguridad en sus servidores. Además tiene la opción de recibir las notificaciones de pago a través de sms o correo electrónico. Monedero disponibles para Android y para Iphone en un modo restringido por la políticas que sigue Apple.



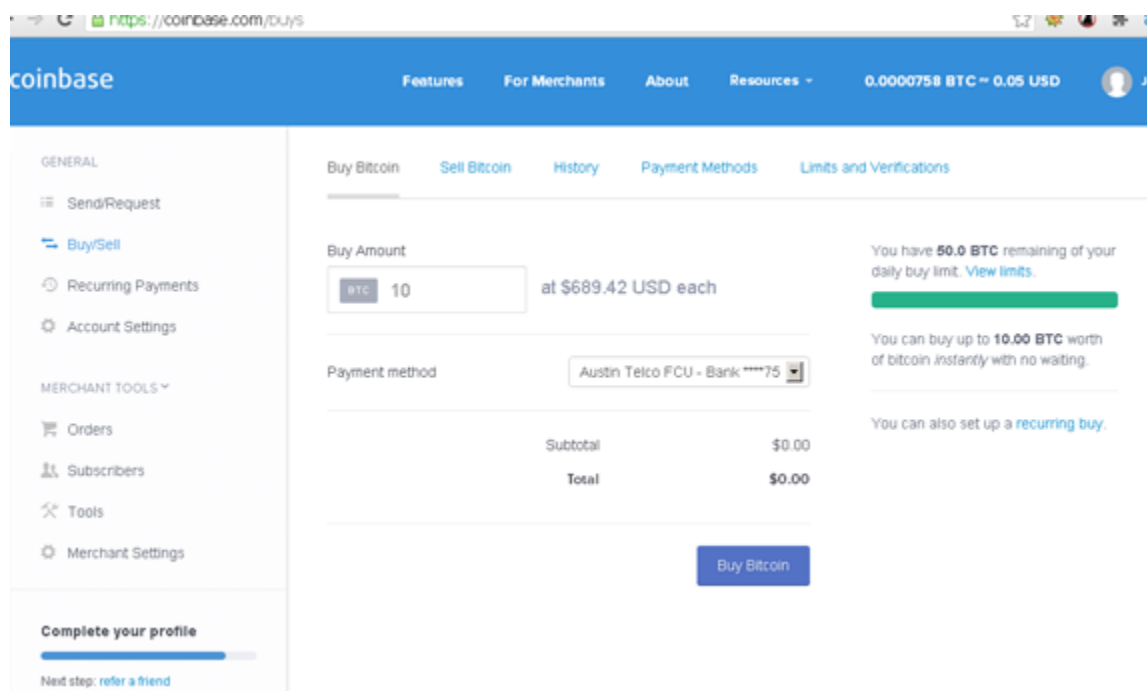
Coinbase → Monedero donde los usuarios pueden verificarse con una cuenta bancaria y un número de teléfono, luego ya es posible mover dinero a bitcoins o viceversa, pudiendo tener el dinero en su cuenta bancaria en pocos días. Lanzó la App para los servicios de Bitcoin en Appel y este retiró su monedero sin previo aviso y sin dar explicaciones.



Por otra parte, si decidimos que queremos trabajar de manera online debemos abrirnos una cuenta en uno de los distintos brokers que existen. En el mundo Bitcoin, una cuenta online es comparable con una cuenta en un Banco ya que una empresa privada es la que se encarga de almacenar y proteger las claves privadas de sus clientes. Por lo tanto, al existir una empresa intermediaria, al realizar una transferencia se cobra una mínima comisión. El control de los datos y el pago de la comisión son dos inconvenientes de abrir una cuenta online de Bitcoins, no se diferencia en nada con las monedas normales, pero también tiene ventajas como, poder realizar una transacción mediante un dispositivo con internet (móvil, Tablet...) en cualquier momento del día, realizar las transferencias instantáneas a un nombre en vez de a la dirección Bitcoin larguísima que se utiliza si uno mismo se descarga el software al ordenador y se encarga la persona de proteger sus Bitcoins. En este caso, es el intermediario el que ayuda a realizar las transacciones de Bitcoins.

Los monederos on-line más utilizados son:

Coinbase → Es un monedero online aunque también comercia con Bitcoins al mismo tiempo, pero solo en Estados Unidos. Tiene precio único para comprar Bitcoins y como se ha visto en el apartado anterior, también ofrece monedero para móviles.



The screenshot shows the Coinbase website interface for buying Bitcoin. The top navigation bar includes 'Features', 'For Merchants', 'About', 'Resources', and a user profile icon. The main content area is titled 'Buy Bitcoin' and includes a 'Buy Amount' field set to 10 BTC at \$689.42 USD each. A 'Payment method' dropdown is set to 'Austin Telco FCU - Bank ****75'. A 'Buy Bitcoin' button is visible at the bottom right. A progress bar indicates the user's profile completion status, with the next step being 'refer a friend'.

Blockchain.info → Es uno de los brokers más populares Ofrece un monedero online junto a su monedero para móviles. Blockchain.info se conserva la propiedad completa de los Bitcoins, Blockchain.info no puede ver el saldo de la cuenta, transacciones o realizar pagos en nombre del propietario.

Strongcoin → Monedero online que permite encriptar las claves privadas antes de enviarlas a los servidores de Strongcoin. Éste, no tiene acceso a las claves encriptadas, por lo tanto no puede acceder a las billeteras de los usuarios.

CarbonWallet.com → Ofrece un servicio similar a Blockchain.info aunque no sea tan conocido, es un monedero Bitcoin determinista, lo que quiere decir que puede generar una copia de seguridad, es decir, una copia de la información del monedero, esto se hace por seguridad, de esta manera si se produce algún fallo o entra un virus se puede recuperar la información.

Ambas opciones, tanto la descarga de un monedero personal en el ordenador como la creación de un monedero on-line, llevan al mismo resultado, obtención de un monedero de Bitcoins para poder realizar operaciones utilizando una contraseña privada.

Una vez tengamos nuestro monedero, lo primero que se debe hacer es encriptar la cuenta, es decir, cifrarla de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios, simplemente es una medida básica de seguridad por si el ordenador estuviese infectado por algún virus evitar que pudiesen entrar en la cuenta Bitcoin. El problema es que si esa contraseña se olvida se pierde el acceso a la cuenta, por eso se debe guardar bien.

Después de encriptar el monedero ya podemos empezar a operar con bitcoins con más seguridad. El intercambio de bitcoins o porciones de bitcoin se puede realizar directamente entre dos usuarios sin ninguna necesidad de tener un bróker como intermediario.

- Para poder empezar a recibir Bitcoins debemos agregar una dirección poniéndole un nombre para poder identificar la transacción, esta dirección es la clave pública. Una vez agregada la dirección, se la enviamos a la persona que nos va a enviar el dinero,

vía e-mail, móvil...como se quiera, simplemente es copiarle la dirección diciéndole la cantidad de dinero que tiene que enviar.

- Por otra parte, para enviar Bitcoins, lo que necesitamos saber es la dirección de la persona a la que le vamos a pagar y la cantidad de Bitcoins que le hemos de transferir.

Cuando la transacción se realiza pasa a la red, es decir, al conjunto de mineros, personas que se encargan de verificar si las transacciones de Bitcoins son válidas o no teniendo en cuenta dos claves:

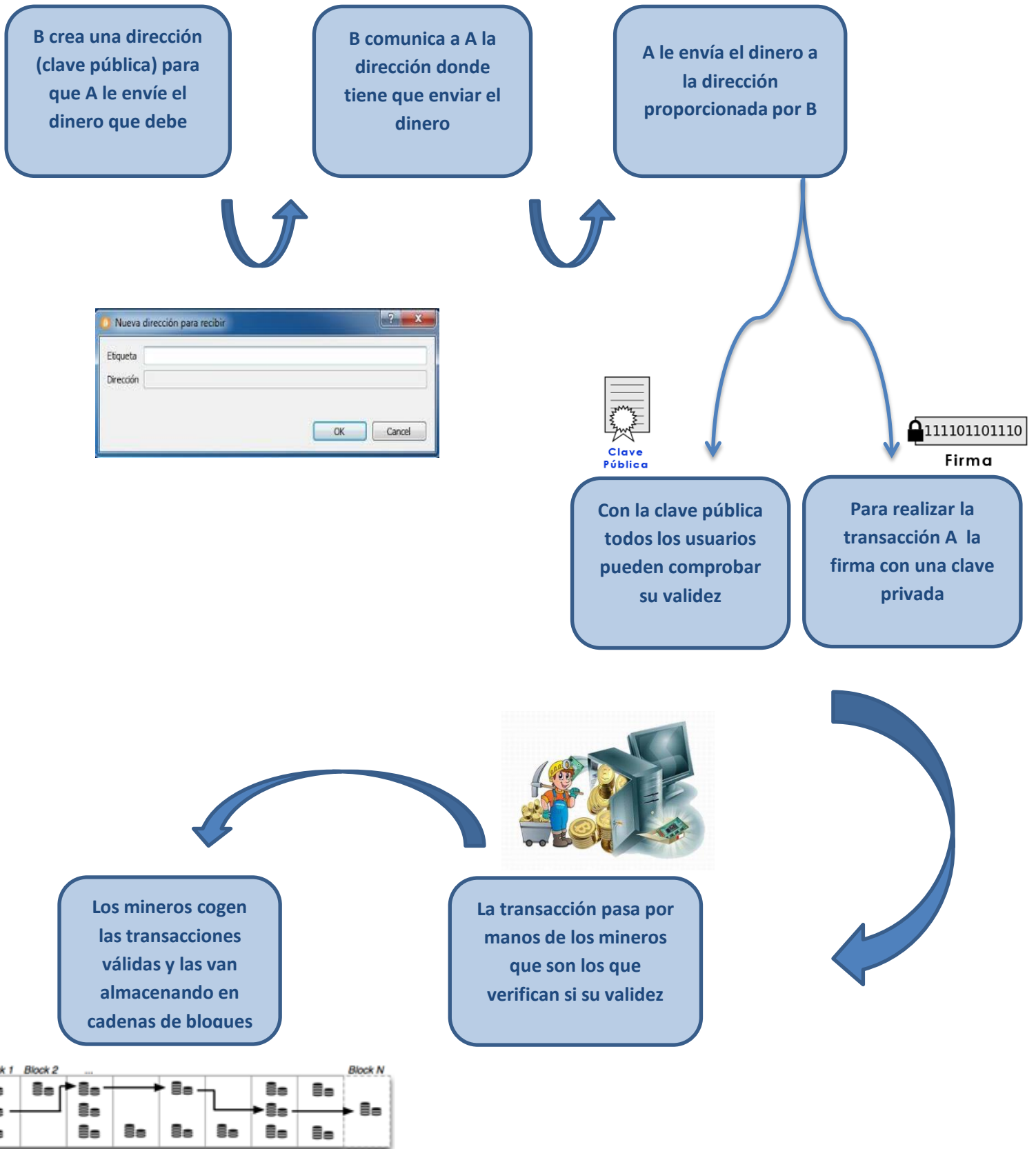
- La clave pública que es la dirección generada por el que cobra para que le puedan enviar los bitcoins, puede tener una clave pública para cada cobro.
- La clave privada que es la contraseña del que envía el dinero cuando firma la transacción.

Con ambas claves los mineros comprueban, por una parte, que el que paga es quien dice ser y por otra parte, que el que paga tiene suficientes Bitcoins para enviar.

Cuando se confirma que la transacción es correcta, ésta se almacena junto con otras transacciones hasta que sean confirmadas, a este conjunto de transacciones se le denomina bloque. Una vez se verifica el bloque se agrega al anterior bloque verificado y así sucesivamente, creando lo que actualmente se denomina cadena de bloques, aproximadamente cada 10 minutos se añaden a la cadena. La cadena de bloques es conocida como un tipo de libro contable mundial, donde se encuentran todas las transacciones de Bitcoins realizadas hasta la última de una manera ordenada, con integridad garantizada mediante la criptografía. Estas operaciones quedan registradas en la red, la transparencia es una de las características del sistema Bitcoin, pero nadie puede saber quién es el creador de cada dirección pública, todo se realiza de una manera anónima.

Por lo tanto, podría ser una red segura, ya que para intentar pasar una operación falsa, es decir, hacer una doble compra o venta, se tendría que engañar a más de la mitad de mineros.

ESQUEMA DE UNA TRANSFERENCIA DE BITCOINS



IV. ¿Cómo conseguirlos?

Actualmente, para obtener Bitcoins, de manera general, existen cuatro formas:

- Comprar:

Los mineros, las personas que crean Bitcoin, después de crearla se dedican a venderlos a grandes páginas web (brokers) dónde la gente puede acceder y comprar Bitcoins mediante su cuenta corriente. En estas páginas web es donde se fija el precio del Bitcoin dependiendo la oferta y la demanda.

El proceso de compra es sencillo, se crea un monedero online en la página donde se vaya a realizar la compra, se paga mediante tarjeta y se reciben directamente los Bitcoins al monedero online creado. Una vez los Bitcoins estén en el monedero por seguridad, la mayoría de las personas se transfieren esos Bitcoins a su monedero personal descargado en su propio ordenador. A partir de aquí ya se puede realizar cualquier tipo de operación.

- A cambio de prestar un bien o servicio.

Otra forma de obtener Bitcoins es a cambio de prestar un servicio o vender un producto y cobrar en Bitcoins, para ello puedes fijar un precio en cualquier moneda y pasarlo al valor del Bitcoin dependiendo del momento.

- Obtenerlos de forma gratuita:

Hay muchos lugares de Internet que ofrecen Bitcoins de manera gratuita, pero no resulta fácil el ingreso de esos Bitcoins. Las páginas web que ofrecen Bitcoins gratis obtienen dinero de la publicidad, como la mayoría, y para recompensar a las personas que la visitan o que hacen clic sobre sus anuncios regalan Bitcoins, pero como ya he comentado no es algo fácil de conseguir, ya que muchas veces es imposible debido a la cantidad de veces que se ha de entrar en la página o a la cantidad de anuncios que se deben ver.

- Minando Bitcoins:

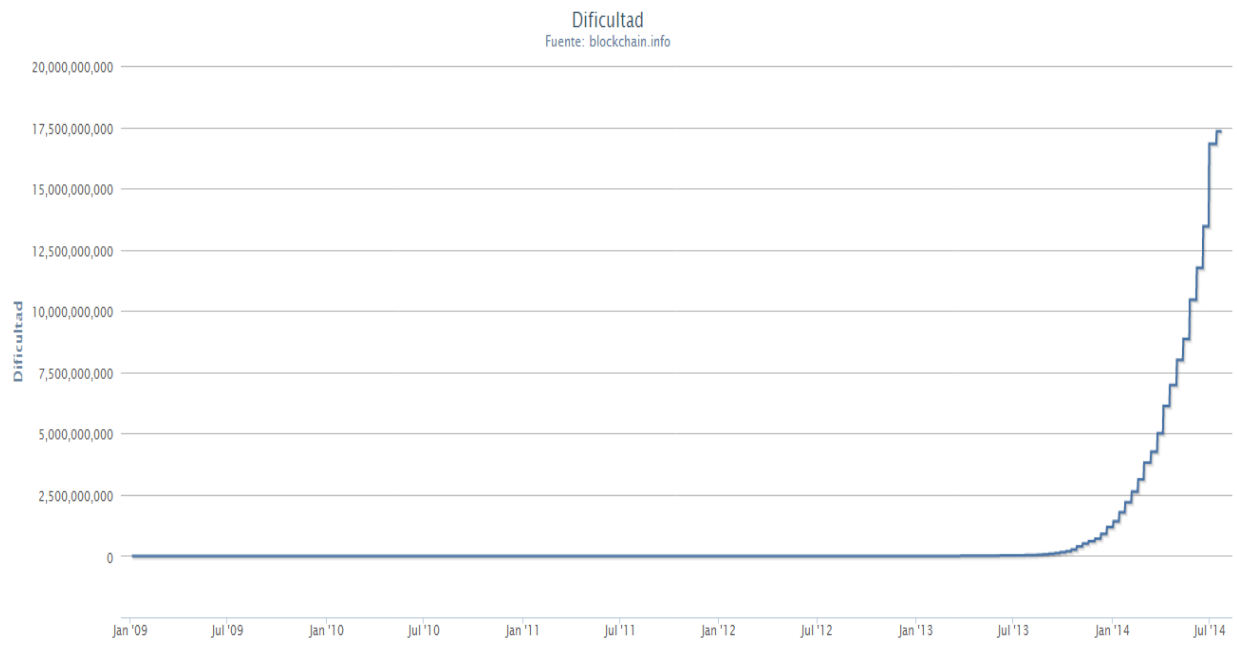
La minería en Bitcoin consiste en la verificación de las transacciones de Bitcoins mediante cálculos matemáticos realizados por diversos equipos informáticos. Así se aumenta la seguridad, evitando fraudes. Estas operaciones de confirmación son realizadas por unas personas a las cuales se les llama mineros.

Los mineros utilizan unos softwares especiales para encontrar los cálculos matemáticos que verifiquen los bloques, los cuales se denominan **hash**, y debido a la dificultad de encontrar estos cálculos, se recompensa de alguna forma a esa gente que está ofreciendo sus recursos informáticos para realizar dichas operaciones. Este problema criptográfico consiste en encontrar el hash del bloque anterior verificado más un número aleatorio, que se denomina **nonce**. Para resolver el problema, el minero irá cambiando el valor del nonce hasta encontrar la solución, ya que no existe nada que permita encontrar la solución de manera sencilla. Estos cálculos matemáticos se realizan a partir de datos de las transferencias (que cambian continuamente) y de un número secuencial. El resultado, es decir, el cálculo matemático obtenido debe ser inferior o igual a un número de 256 bits (muy grande) denominado target, número marcado por la red Bitcoin. El primer minero que encuentra el cálculo matemático (hash) que verifica la transacción se lleva la recompensa económica, actualmente consiste en 25 Bitcoins por bloque además de llevarse cantidades adicionales de usuarios que ingresan dinero por priorizar la verificación de sus transacciones.

Una vez confirmado que la transacción es correcta, ésta se almacena junto con otras transacciones, este conjunto de transacciones se denomina bloque. Cuando todas las transacciones de un bloque estén confirmadas, este se une al final de la cadena de bloques existentes hasta el momento. Dichos bloques están unidos de manera que cada bloque demuestra que el anterior era válido, podemos decir que están encadenados entre sí.

Como los mineros son los que confirman las transacciones, cuanto más mineros, mayor seguridad de la red. La red de Bitcoin cambia la dificultad de los problemas matemáticos automáticamente cada 2016 bloques.

A continuación presento un gráfico con la evolución de la dificultad a la que se han enfrentado y se enfrentan los mineros a la hora de encontrar los cálculos matemáticos que verifican cada bloque.



Fuente: blockchain.info

Como podemos ver en el gráfico la evolución en la dificultad de la resolución de bloques ha sido constante durante los primeros años de creación del Bitcoin, en cambio desde finales del 2013 hasta la actualidad está aumentando considerablemente debido a la gran competencia entre mineros.

Cuando empezó el sistema, al conocerlo muy poca gente, había muy pocos mineros, con lo cual, la dificultad era muy baja. Poco a poco la cantidad de mineros ha ido creciendo por el hecho de que es una moneda con una forma de producirse curiosa y que además, hay incentivos monetarios, la minería de Bitcoins. Al aumentar la cantidad de mineros, la dificultad de descifrar un bloque es mucho mayor cada vez. Con la nueva dificultad la probabilidad de que un ordenador de sobremesa, el típico de cualquier casa, con buena gráfica y un buen procesador, encuentre un bloque nuevo es muy baja, ya que hay demasiada competencia.

A partir del 2010, la dificultad aumentó 10.000 veces en un año (en el gráfico no se puede ver bien éste efecto), lo que hizo que surgiese la necesidad de que los mineros se ayudasen entre sí para acelerar el proceso de verificación. Muchos mineros decidieron juntarse y hacer grupos para trabajar juntos en la resolución del problema y luego repartirse

los beneficios, así aparecieron los “mining pools” (grupos de minería). El hecho de que la dificultad vaya creciendo cada vez más no sólo se hace para mantener la producción bajo control, también evita el fraude. Como cada Bloque referencia al anterior, haría falta reescribir todos los Bloques desde los que vas a usar hasta el actual para que todos sean válidos y poder usar Bitcoins falsas. El sistema está diseñado para que la producción se pare al llegar a 21 millones de Bitcoins.

V. Historia del Bitcoin

Muchas monedas virtuales han aparecido desde que empezó a existir todo el mundo virtual (Internet), como por ejemplo, en 1994, se creó CyberCash llegó, caracterizada por el anonimato, pero en 2001 se declaró en quiebra; otra moneda Beenz, que surgió en 1998, se podía conseguir entrando en sitios web y luego se podía comprar con ella en determinadas webs, pero tampoco tuvo un buen futuro y en 2001 quebró; en 1999 nació Flooz, moneda que tal como nació terminó. Éstas son monedas virtuales que, entre otras, no han tenido el recorrido que ha tenido y está teniendo el Bitcoin.

A diferencia de las divisas virtuales anteriores, el Bitcoin si ha tenido su éxito, no se sabe, si por la época en la que se creó, empezando la crisis, donde mucha gente no confiaba en la economía o porque presenta características que las demás divisas virtuales no poseían como la cadena de bloques, dónde todas las transacciones quedan registradas y comprobadas por una descentralizada red de ordenadores evita que un identificador sea utilizado más de una vez, impidiendo la duplicación.

Actualmente, visto el éxito que tuvo el Bitcoin desde sus inicios muchos han querido hacer surgir nuevas monedas virtuales con características similares a las del Bitcoin, como por ejemplo, el Litecoin (2011), muy parecida al Bitcoin pero con mayor rapidez en la confirmación de las transacciones y con menor necesidad de equipos informáticos potentes para poder minar. Aunque de momento, ninguna moneda ha podido desbancar al Bitcoin como principal moneda virtual, aun teniendo ésta durante su trayectoria momentos de crisis.

¿Cómo ha evolucionado el Bitcoin?

2008→ La crisis económica mundial de 2008 hace que la resistencia de las divisas se ponga en duda, lo que fue aprovechado para que surgiera esta nueva divisa virtual, el Bitcoin. En agosto de este mismo año se registra el dominio Bitcoin.org y en octubre se publica el primer documento que explica el diseño del Bitcoin.

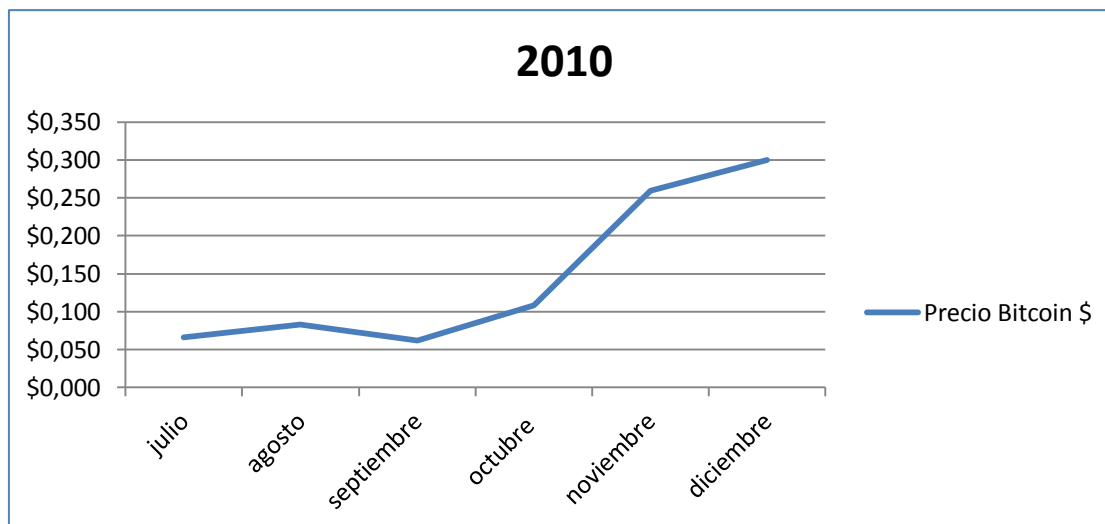
2009→ Nace la red Bitcoin, en enero Nakamoto mina el primer bloque de Bitcoins, a cambio del cual recibe 50 Bitcoins y realiza la primera transacción en Bitcoins a Hal Finney. A final del año, en octubre, se realiza el primer cambio de dólares por Bitcoins. El precio de esta primera transacción es **de 1.309,03 BTC por un 1\$,** es decir este fue el primer tipo de cambio de dólar/ bitcoin.

2010→ Por primera vez todo el mundo puede comprar Bitcoins por dólares, la primera compra se realiza en mayo de 2010, se realiza la primera compra, 10 mil Bitcoins en comprar dos pizzas.

En julio de 2010, surge la primera billetera para comprar Bitcoins, Mt Gox. Además, ese mismo mes la página Slashdot.org (una influyente página sobre proyectos de código abierto) publicó un comentario positivo sobre Bitcoin, lo que hizo que se provocara una subida del valor de la nueva moneda virtual, desde menos de un centavo de dólar hasta los 7 céntimos en unos pocos días. El precio de Bitcoin se multiplica por 10 en un periodo de 5 días **desde 0.008 a 0.08 dólares** por Bitcoin.

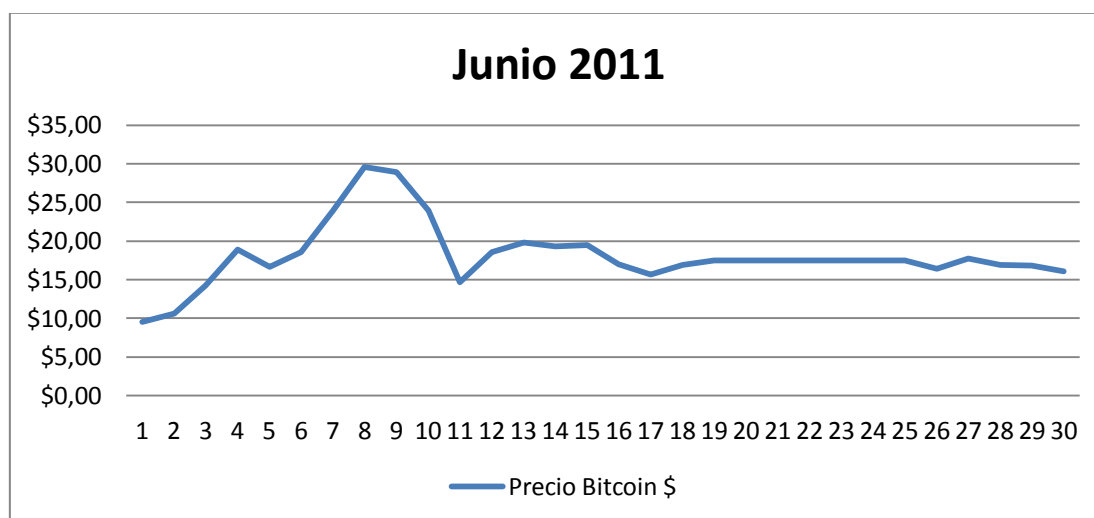
Pero todo no podía ser tan positivo, en agosto surge el primer gran error en el servicio Bitcoin ya que hasta ese momento las transacciones no eran verificadas antes de ser incluidas en la cadena de bloques. En poco tiempo, el problema fue detectado y solucionado.

En diciembre, el Bitcoin cierra el año valorándose a **0,30\$.**



Fuente: <http://www.coindesk.com/price/>

2011 → La nueva moneda virtual, Bitcoin, empieza a ser nombrada por los medios de comunicación, se empieza a dar a conocer, ya en febrero, el Bitcoin consigue la paridad con el Dólar. En cambio, en junio de 2011, tuvo una fuerte bajada ya que Mt Gox, uno de los brokers más conocidos hasta ese momento en la red Bitcoin, sufre su primer ataque de robo, muchos de sus clientes ven como sus cuentas son robadas. Al ocurrir esto, los clientes empiezan a realizar órdenes de venta para impedir que sus Bitcoins sean robados, con lo cual esto produce que el precio del Bitcoin en Mt. Gox pase de \$17,1 a \$0,01. Mt Gox bloquea las operaciones durante 7 días. A raíz de este problema, los precios del Bitcoin en otros sitios de intercambio también cayeron hasta los 13 dólares en el mismo día.

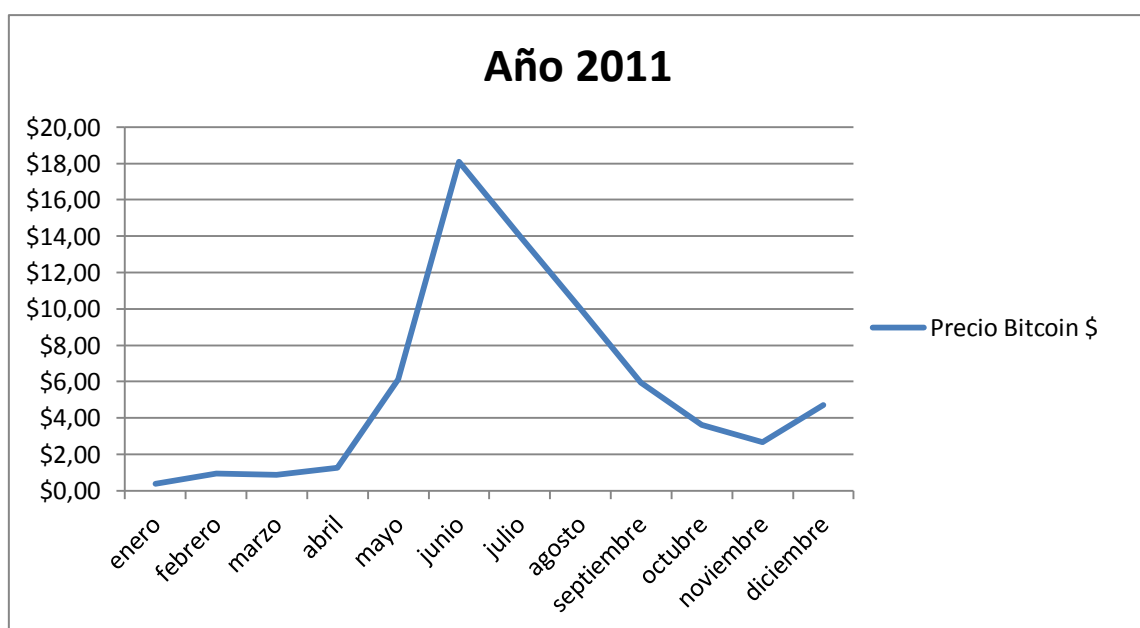


Fuente: <http://www.coindesk.com/price/>

En julio MyBitcoin.com, otro de los brokers más grandes deja de estar accesible para sus usuarios, los cuales no pueden disponer de sus bitcoins. Pasan unos días hasta que los que se encargan del control de este sitio web anuncian mediante un comunicado que MyBitcoin ha sido hackeado y que solo puede devolver el 49% de los Bitcoins a sus usuarios.

Los sucesos producidos, todos en el mismo año, provocan que los usuarios dejen de confiar en tener sus Bitcoins controlados por terceros.

Finalmente el Bitcoin cierra el 2011 a un precio de \$4.72



Fuente: <http://www.coindesk.com/price/>

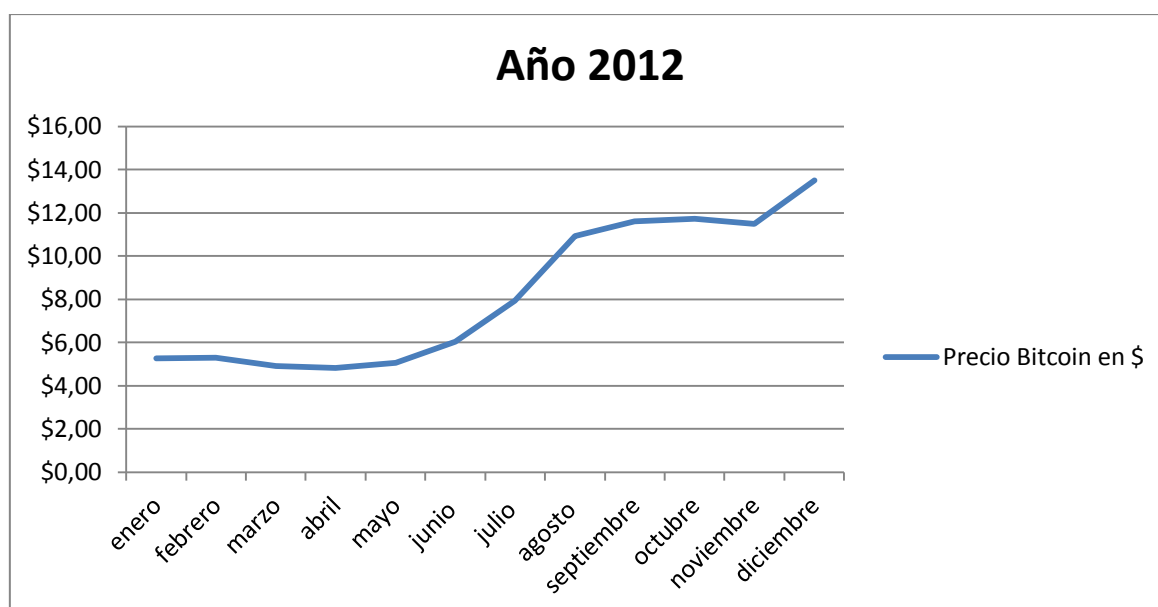
2012 → Aún no está depositada del todo la confianza en el Bitcoin después de lo que pasó en junio del 2011, el Bitcoin tarda un año en recuperar la confianza de sus usuarios. Durante el 2012 la moneda virtual se va consolidando, los primeros meses tuvieron subidas y bajadas del precio pero de una manera estable.

En noviembre, WordPress (importante y avanzada plataforma de publicación personal orientada a la estética, los estándares web y la usabilidad) acepta el pago con Bitcoin para sus servicios, lo cual fue un evento muy positivo para el desarrollo del Bitcoin. También en el mismo mes, la recompensa por minar Bitcoins se redujo, pasó de 50 Bitcoins por minería a

25, aproximadamente cada 4 años se divide por dos la cantidad de Bitcoins que se obtienen como recompensa

Según el informe del Banco Central Europeo de este mismo año, este afirma no estar preocupado porque monedas virtuales puedan afectar a la estabilidad financiera, ya que cree que no tienen suficiente volumen de negocio y de aceptación para poder suponer un problema en este ámbito. La verdadera preocupación del BCE es que, tanto el Bitcoin como demás monedas virtuales empiecen a ser utilizadas con fines ilegales.

El Bitcoin cierra el año a un precio de **\$13,51**.



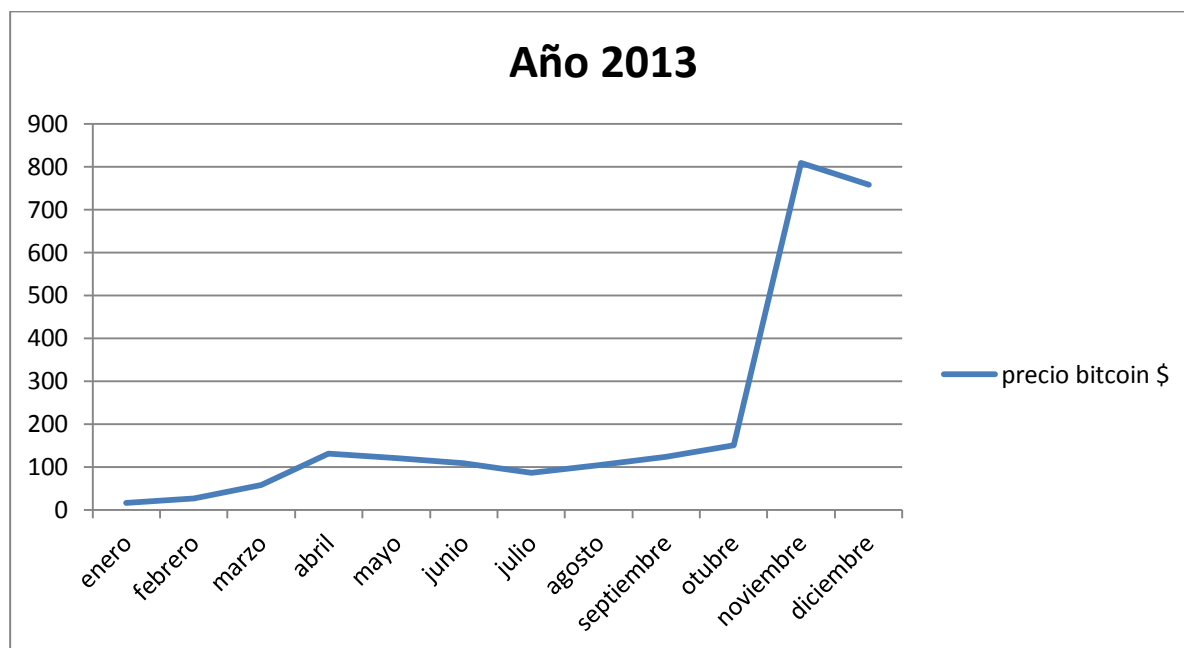
Fuente: <http://www.coindesk.com/price/>

2013 → El año 2013 se considera un año de aceleración en la evolución del precio del Bitcoin. Aun habiéndose producido fallos en alguno de los clientes Bitcoins, esto no impidió que en el mes de marzo el precio del Bitcoin aumentase estrepitosamente. A final de este mes el valor del Bitcoin estaba a 93\$.

En abril, Chipre anuncia un corralito bancario (imponen un impuesto a sus ahorros bancarios) y el precio del Bitcoin se duplica. Al mes siguiente, MtGox recibe ataques DDos, es decir, el servidor es atacado desde muchos ordenadores con lo cual, deja de funcionar. Este tipo de ataques se realizan para que, al dejar de funcionar el sistema, el precio de los

Bitcoins baja, momento en el cual aprovechan para comprar Bitcoins y luego cuando se soluciona el problema y empieza a subir el precio otra vez, venden los Bitcoins a un precio más alto de lo que lo han comprado. En ese momento, las autoridades de los EEUU congelaron varias veces las cuentas de Mt Gox en el país. Actualmente los servidores de Bitcoin ya tienen protección para que estos ataques no ocurran.

En octubre se crea el primer cajero de Bitcoins en Vancouver, Canadá y en meses posteriores, en diciembre, el Banco de China prohíbe la administración de transacciones en Bitcoins, lo que significa que las instituciones financieras no podrán comprar o vender la moneda virtual, ni asegurar productos relacionados con Bitcoin, lo que produjo la caída del Bitcoin en unas semanas.



Fuente: <http://www.coindesk.com/price/>

2014 → En Febrero, Mt Gox, una de las mayores plataformas de cotización de bitcoins, fue hackeada robándole 744.408 Bitcoins y tuvo que anunciar su quiebra. Momento en el cual se vuelve a poner en duda la seguridad de los sistemas de esta moneda virtual. Aunque no solo Mt Gox anunció su quiebra, sino que, Flexcoin, otro bróker muy importante, también

se vio obligado a cerrar después de que sufriese el robo de todas los Bitcoins que tenía en sus cuentas a la vista.

Además, Apple retiraba Blockchain, aplicación compatible con Bitcoin y Rusia prohibía el uso de esta moneda en su territorio, siguiendo así los pasos de China, que hizo lo propio a finales del año anterior.

En mayo, El Banco Central de Bolivia emite una resolución prohibiendo el uso de todas las monedas virtuales, entre ellas el Bitcoin, ya que según éste asegura la estabilidad del poder adquisitivo interno del país y evita dar facilidades al negocio de la droga con las monedas virtuales.

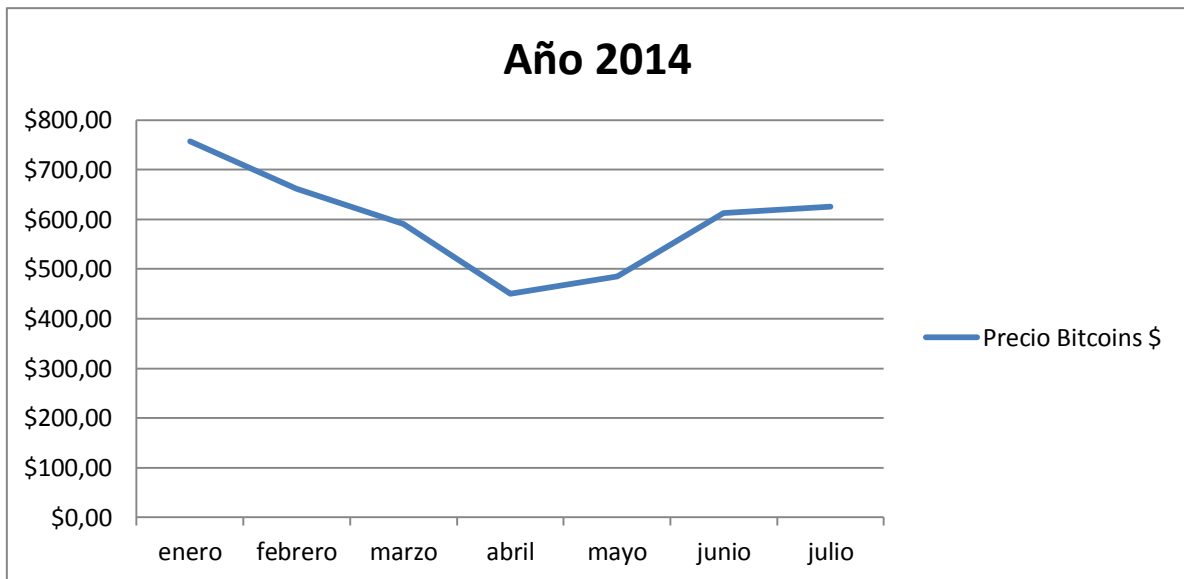
La última noticia importante sobre el Bitcoin hasta el momento, Julio 2014, sucede en Francia donde se desmanteló una plataforma ilegal de intercambio de Bitcoins, dónde se ha incautado 388 Bitcoins (200.000 euros). La investigación anuncia que era una plataforma web en proyecto de casino digital, todo construido de manera ilegal ya que no tenían ningún permiso de la Autoridad de Control Prudencial y de Resolución (órgano francés de supervisión de banca y seguros).

A raíz de este problema, el pasado 7 de julio, el ministro francés de Finanzas, Michel Sapin, anunció que:

“Su Gobierno ha decidido limitar el anonimato en la compra Bitcoins, al imponer que el dueño de una cuenta sea identificado y que se compruebe su identidad en la retirada y entrega de monedas”

También quiere proponer que las transferencias de Bitcoins tengan una cantidad limitada, según el “justificado por el carácter anónimo de ese tipo de pago y en coherencia con la reglamentación actual que afecta a los pagos en efectivo”

Actualmente, a 23 de Julio la cotización del Bitcoin está a 621.79\$.



Fuente: <http://www.coindesk.com/price/>

VI. Ventajas y Desventajas

▪ Ventajas

La nueva moneda electrónica que ha estado revolucionando el mundo en los últimos años, en mi opinión, presenta algunas ventajas respecto al resto de monedas.

- La **descentralización**, naturaleza de Bitcoin y demás monedas virtuales, es lo que la hace especial ya que su valor no está sujeto a ninguna decisión política con interés gubernamental, esta característica es lo que llama la atención del usuario para empezar a utilizar monedas virtuales.

La descentralización presenta otra característica positiva, que a su vez también puede tener aspectos negativos, los cuales comentaré posteriormente. La parte positiva es que el sistema descentralizado del Bitcoin hace imposible que cualquier persona que no sepa las contraseñas de la cuenta, acceda a ella, los Bitcoins son de la persona que los compró no pueden ser congelados ni embargados.

Además, se podría pensar que su creador podría ejercer el control si el así lo quisiera, pero eso no es así, en el momento que el primer minero empezó a minar el creador del Bitcoin ya perdió su control. Por lo tanto, la descentralización del Bitcoin asegura que no

haya manipulaciones arbitrarias del valor de la moneda, lo cual pasa con los Bancos Centrales.

- Otra de las grandes ventajas del Bitcoin es que al no tener intermediarios, es decir el mismo usuario se encarga de hacerlo todo y como el dinero pasa directamente de persona a persona, **abaratando los costes**, no hay ninguna comisión. Con lo cual aunque el comprador esté en una parte del mundo y el vendedor en la otra el costo de la transferencia es cero. Esta característica del Bitcoin es una gran ventaja ya que con el sistema bancario estamos acostumbrados a pagar comisiones con cualquier operación: por una transferencia a diferente banco, transferencias a otros países, por poseer tarjetas de crédito/débito, por mantenimiento de la cuenta... por eso, que el sistema Bitcoin permita realizar operaciones sin costo capta la atención del posible usuario.
- **El anonimato** es una de las características que desde mi punto de vista puede presentar el sistema Bitcoin posee ventajas y desventajas. Mediante las transacciones no hace falta revelar la identidad de la persona, ya que las direcciones son un conjunto de letras y números; y aunque con esto no se consigue el anonimato total y lo hace más seguro, ya que pueden ser rastreadas las direcciones y saber el dinero que recibe y envía una persona, hay maneras para evitar que esto pase, como por ejemplo, cada vez que se haga una transacción cambiar de dirección para que así no puedan ser rastreadas. Además también existen programas destinados para proteger el anonimato.
- Una de las características del Bitcoin es su **divisibilidad**, a medida que pasa el tiempo el Bitcoin es más divisible, puede ser infinitamente divisible. Desde mi punto de vista es una característica positiva porque no todo el mundo puede disponer de un Bitcoin, ya que cada vez su valor es mayor. Por lo tanto, cualquier persona puede llegar a disponer aunque sea de una mínima parte de un bitcoin. Con esta medida se evita el estancamiento del sistema Bitcoin porque siempre habrá bitcoins para comprar o vender, ya que hasta una milésima parte de un bitcoin es divisible.

▪ Desventajas

- El límite de emisión del Bitcoin son 21 millones, lo cual desde mi punto de vista es una gran desventaja, ya que esto provoca que la gente quiera conseguir Bitcoins antes de que lleguen a su límite, con lo cual el valor de estos sube. Por eso, creo que el Bitcoin es **una monera deflacionaria**, porque con el afán de conseguir Bitcoins, suele haber más demanda que oferta. Por lo tanto, es una moneda que aumenta el valor a medida que pasa el tiempo, ya que el valor de la moneda se aprecia. El hecho de ser deflacionaria incentiva el ahorro extremo y no al consumo y, por tanto, termina por deprimir el sistema Bitcoin porque no incentiva el gasto de Bitcoins.

Pero por otra parte, no podemos descartar la posibilidad de que pueda ocurrir lo contrario, que la oferta evolucione más rápido que su demanda, entonces hablaríamos de una moneda inflacionista.

- En el apartado anterior he comentado las ventajas que tiene que el Bitcoin sea una **moneda descentralizada**, pero no solo veo ventajas en esto, sino que también veo inconvenientes. Cuando compramos alguna moneda tenemos la confianza que hay alguien que está regulándola y encargándose de ella, pero ¿y cuando compramos Bitcoins? ¿tenemos la suficiente confianza en los usuarios de Bitcoin para dejar su control en la oferta y la demanda, que son realmente lo que controlan los Bitcoins? Es muy importante el desarrollo de la autogestión que nos permite el Bitcoin, pero no todos los usuarios tienen suficientes conocimientos como para depositar la confianza en su control. Con respecto a la otra característica positiva que he comentado de la descentralización, que nadie pueda congelar ni embargar las cuentas de bitcoins que posee una persona, creo que el aspecto negativo es que si una persona está haciendo alguna actividad ilegal y almacenándolo en Bitcoins, ese dinero nunca podrá ser confiscado ni devuelto.
- Bitcoin es una moneda volátil, como he comentado anteriormente, su **valor depende de la oferta y la demanda** y nadie lo regula, por lo tanto su precio fluctúa fuertemente, un día puede valer 800 euros y al día siguiente pasar a 900 euros. La fortaleza del Bitcoin depende en gran parte del número de usuarios que tenga, cuantos más, menos posibilidades de manipulación.

La mayoría de personas que compran Bitcoins no son para cambiarlos por un bien o servicio, aunque cada vez haya más sitios que acepten el pago con Bitcoins, sino que para especular. El problema vendría si países como China o Estados Unidos prohibiesen su utilización, el precio bajaría en picado porque, evidentemente la demanda caería.

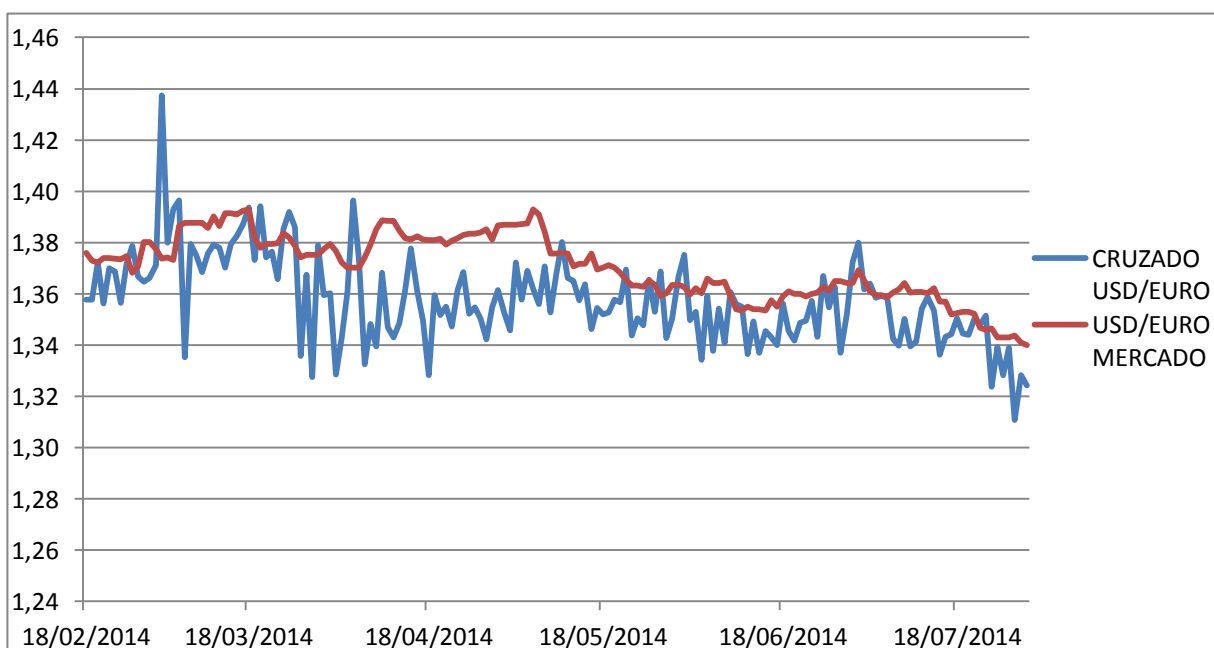
- El **anonimato**, en mi opinión también se puede presentar como una desventaja, ya que al no poner los datos personales en las transacciones hace que realizar asuntos ilegales o blanquear dinero sea más fácil y sobretodo en movimientos internacionales, ya que se puede comprar cualquier bien, ya sea legal o ilegal, y solo el comprador y el vendedor saben lo que se compra y a cuanto se compré.
- Otro de los grandes inconvenientes que particularmente le veo yo al Bitcoin, es que **si se pierde la contraseña (criptografía) no hay manera de recuperarla**, aunque se hagan muchas copias, hay que tener cuidado con no perderlas. He podido leer muchos artículos de usuarios de Bitcoin contando sus experiencias de pérdidas de discos duros dónde tenían guardado la criptografía y les ha sido imposible recuperar su dinero.
- Al principio, cuando el Bitcoin salió a la luz, tuvo un boom y parecía que iba a tener una buena **aceptación**, pero ha ido pasando el tiempo y parece que, sea por problemas que han surgido en algunos brokers o por otros temas, la gente ha perdido la confianza en este sistema o, otras personas que no la tenían y estaban viendo su evolución, ni siquiera quieren tener esa confianza. Por lo tanto, la viabilidad como moneda es muy dudosa.

VII. Cotización Bitcoin, Dólar, Euro

Una vez expuesta la teoría de la nueva moneda virtual incluyendo mi valoración personal respecto a los aspectos positivos y negativos que ésta moneda, realizaré un análisis para saber si entre las tres divisas puede haber posibilidad de arbitraje. Aunque antes de empezar dicho análisis he de indicar que no he tenido acceso al precio de comprador y del precio del vendedor exacto, probablemente los datos sean un punto medio entre ambos, por lo tanto la conclusión del análisis no es fiable.

Para el análisis he utilizado tablas Excel, gráficos, ejemplos y un análisis estadístico para comprobar si los dos tipos de cambio (mercado y cruzado). En primer lugar, he buscado unos datos imprescindibles para el inicio del análisis, cuyas fechas son desde el 18 de Febrero hasta el 30 de Julio del 2014, ¿Cuántos Dólares son un Bitcoin? (USD/BTC), ¿Cuántos Euros son un Bitcoin? (EUR/BTC), ¿Cuántos Euros son un Dólar? (USD/EUR)

Una vez obtenidos estos datos he calculado el precio cruzado del USD/EUR $\frac{\text{USD/BTC}}{\text{EUR/BTC}}$ para comparar si era el mismo que el precio de mercado, ya que en teoría tienen que coincidir. Cuando no coincide puede ser porque existe la posibilidad de arbitraje, que es exactamente lo que ocurre en este caso, que precio de mercado y precio cruzado son diferentes, tal y como podemos ver reflejado en el gráfico siguiente.



Para poder entender mejor estas pequeñas diferencias, voy a realizar dos ejemplos:

Cuando el Precio de Mercado está por encima del Precio Cruzado

Cuando el precio de mercado está por encima del precio cruzado como ocurre el día 11 de Marzo, dónde el precio cruzado está en 1.375824176 USD/EUR y el precio de mercado está a 1.3857 USD/EUR, tal y como nos muestra la siguiente tabla:

2014	USD/BTC	EUR/BTC	CRUZADO USD/EURO	USD/EURO MERCADO
18/02/2014	615	453	1,357615894	1,376
19/02/2014	611	450	1,357777778	1,3729
20/02/2014	542	395	1,372151899	1,3721
21/02/2014	555,5	409,57	1,35630051	1,3739
22/02/2014	597,56	436,15	1,370079101	1,3739
23/02/2014	598	436,87	1,368828256	1,3738
24/02/2014	555,76	409,74	1,356372334	1,3735
25/02/2014	535	390	1,371794872	1,3746
26/02/2014	568	412	1,378640777	1,3681
27/02/2014	569,88	417	1,366618705	1,3707
28/02/2014	536,3	393	1,364631043	1,3802
01/03/2014	562,3	411,58	1,366198552	1,3802
02/03/2014	554	404	1,371287129	1,3774
03/03/2014	644,03	448,03	1,437470705	1,3736
04/03/2014	656,56	475,8	1,379907524	1,3742
05/03/2014	653,15	468,9	1,392940926	1,3732
06/03/2014	648	464,08	1,396310981	1,3864
07/03/2014	619,72	464,08	1,335373212	1,3878
08/03/2014	609,97	442,15	1,37955445	1,3878
09/03/2014	627	456	1,375	1,3878
10/03/2014	622,6	454,99	1,368381723	1,3876
11/03/2014	626	455	1,375824176	1,3857

▪ **Cambio de DÓLAR→EURO→BITCOIN**

Tengo 100\$ y voy a cambiarlo por euros teniendo en cuenta que la cotización a día 11/03/2014 está a precio de mercado a 1.3857 USD/EUR (precio superior al cruzado 1.3758 USD/EUR)

$$100/1.3857= 72.1656 \text{ EUROS}$$

A continuación para llegar a los Bitcoins hemos de tener en cuenta que la cotización está a 455 EUR/BTC:

$$72.1656/455= 0.16042918 \text{ BITCOINS}$$

Y si ahora quisiéramos volver a dólares nos encontraríamos con que:

$$626*0.1586= 99.2873 \$, \text{ es decir, perderíamos dinero.}$$

En cambio si lo hacemos en otro orden:

- **Cambio de DÓLAR→ BITCOIN→ EURO**

Tengo 100\$ y voy a cambiarlo por Bitcoins teniendo en cuenta que la cotización a 11/03/2014 está a 626 USD/BTC

$$100/626=0.1597$$

Seguidamente para llegar a los Euros hemos de tener en cuenta que la cotización está a 453 EUR/BTC:

$$455 \times 0.1597 = 72.6837 \text{ €}$$

Y ahora si quisiéramos volver a dólares nos encontraríamos con que:

$$1.3857*72.6837=100.7178 \$, \text{ es decir, ganaríamos dinero.}$$

Como podemos ver el orden en el que hagamos los cambios de divisa nos influye en la cantidad final monetaria que vamos a poseer, en el caso de que el precio de mercado esté por encima del precio cruzado obtendremos beneficio cambiando dólares por Bitcoins y por último por euros, ya que si lo hacemos de la otra manera perdemos dinero.

Cuando el precio de Mercado está por debajo del Precio Cruzado

A continuación mostraré el mismo ejemplo pero cuando el precio de mercado está por debajo del precio cruzado, por ejemplo, en el día 01/07/2014, dónde el precio de mercado está a 1.3692 USD/EUR y el precio cruzado a 1.38 USD/EUR, tal y como nos muestra la siguiente tabla:

2014	USD/BTC	EUR/BTC	CRUZADO USD/EUR	USD/EUR MERCADO
01/07/2014	629	455,78	1,380051779	1,3692
02/07/2014	641,11	470,8	1,361745964	1,3653
03/07/2014	636,92	466,99	1,363883595	1,3609
04/07/2014	626,24	461	1,358438178	1,3595
05/07/2014	627,99	462	1,359285714	1,3595
06/07/2014	630,31	464	1,358426724	1,3588
07/07/2014	617,58	460	1,342565217	1,3606
08/07/2014	615,78	459,6	1,339817232	1,3617
09/07/2014	615,78	456,02	1,350335512	1,3643
10/07/2014	609,66	455,1	1,339617666	1,3604

▪ **DÓLAR→EURO→BITCOIN**

Tengo 100\$ y voy a cambiarlo por euros

$$100/1.3692= 73.0353 \text{ EUROS}$$

A continuación para llegar a los Bitcoins hemos de tener en cuenta que la cotización está a 455.78 EUR/BTC

$$72.1656/455.78= 0.1602 \text{ BTC}$$

Y si ahora quisiéramos volver a dólares nos encontraríamos con que:

$$629*0.1602= 100.7925 \$, \text{ es decir, ganaríamos dinero.}$$

En cambio si lo hacemos en otro orden:

▪ **DÓLAR → BITCOIN → EURO**

Tengo 100\$ y voy a cambiarlo por Bitcoins

$$100/629=0.1589 \text{ BTC}$$

A continuación para llegar a los Euros hemos de tener en cuenta que la cotización está a 455.78 EUR/BTC:

$$455.78 \times 0.1589 = 72.4610 \text{ €}$$

Y ahora si quisiéramos volver a dólares nos encontraríamos con que:

$$1.3692 * 72.4610 = 99.2136 \text{ \$, es decir, perderíamos dinero.}$$

Como se ve en los ejemplos, cuando el precio de mercado esté por debajo del precio cruzado obtendríamos beneficio si intercambiamos las divisas de la manera DÓLAR → BITCOIN → EURO. En cambio, si el precio de mercado está por encima del precio cruzado obtendríamos beneficio si intercambiamos las divisas de la manera DÓLAR → EURO → BITCOIN.

Además de los dos ejemplos anteriores, para una mayor demostración de la existencia de arbitraje con los datos que poseo, he realizado un análisis T de STUDENT para la diferencia entre ambos precios (p. mercado, p. cruzado), el cual proporciona el siguiente resultado:

	N	Media	Desviación típ.	Error típ. de la media
resta	163	-,0128550	,01571793	,00123112

En este primer cuadro encontramos algunos estadísticos descriptivos, como la media de la muestra da -0.128550 y su desviación típica de 0.01571793.

Prueba para una muestra

	Valor de prueba = 0					
	t	gl	Sig. (bilateral)	Diferencia de medias	95% Intervalo de confianza para la diferencia	
					Inferior	Superior
resta	-10,442	162	,000	-,01285496	-,0152861	-,0104238

En este segundo cuadro observamos el valor de nuestra prueba, que es la hipótesis nula que estamos contrastando es 0 a un nivel de confianza del 95%, es decir, que la diferencia entre el precio de mercado y el precio cruzado debería ser 0.

El nivel de significación es cero, con lo cual la probabilidad que la hipótesis nula sea cierta tiende a 0, y al ser menos al 0,05 rechazo la hipótesis nula. Por lo tanto, con este análisis podemos afirmar que la diferencia entre ambos precios no es 0, entre ambos existe una diferencia significativamente importante.

Por lo tanto, según todo el análisis diríamos que existe arbitraje entre las tres divisas, pero como he comentado al principio del apartado, no podemos afirmarlo ya que no estoy utilizando los datos exactos al precio del comprador y del vendedor, posiblemente si tuviéramos los precios exactos esa diferencia sería nula.

VIII. Conclusiones

Bitcoin cuenta con una compleja tecnología a sus espaldas que puede avalar el uso de ésta como moneda, ya que evita que se creen Bitcoins falsos, que se utilice el dinero más de una vez y además nos asegura un anonimato en las transacciones y sin comisiones. En resumen, desde el punto de vista técnico, el sistema Bitcoin ha llevado a cabo unos mecanismos, los cuales parecían difíciles de formar.

En cambio, desde el punto de vista económico y social, crea un espacio totalmente nuevo, donde es difícil pronosticar qué efectos tendrá y si será totalmente aceptado. El principal problema que le puedo encontrar a que el Bitcoin siga evolucionando, es su aceptación, ya que hay muchas personas que desconocen su existencia, o que no se fían de utilizarlo bien por no tener a alguien que lo regule, o por los problemas que ha tenido a lo largo de estos años con sus intermediarios financieros. Además, aún en la actualidad, no todo el mundo utiliza internet para las transacciones bancarias por falta de confianza. Si no confían en este uso común y conocido, ¿cómo se van a fiar de algo nuevo, casi desconocido por muchos?

Si se quiere que el Bitcoin tenga éxito se debería empezar a admitir en todas las empresas como forma de pago, es decir, poder utilizarlo en un día a día en cualquier lugar, lo cual aumentaría la confianza al ser utilizada.

Ahora bien, como la moneda presentase una evolución positiva, los Estados la verían como algo peligroso que podría poner en desequilibrio sus estructuras político-económicas. Con lo cual, ellos podrían poner barreras a este desarrollo declarándola moneda ilegal para no perder el control de sus economías.

Por lo tanto, parece complicado que tenga éxito, no sólo porque sea difícil su aceptación en nuestra sociedad, sino que aunque tuviera éxito, los Estados no dejarían que llegara a tener una gran importancia. Pero, a pesar de lo poco probable que es, que veamos al Bitcoin como moneda, como intento y como forma de ver cómo puede evolucionar una moneda en un futuro donde internet es cada vez más importante, me parece experimento muy interesante. Además, ¿quién sabe si las entidades financieras han visto en el Bitcoin, el futuro de una criptomoneda creada por ellas?

Para finalizar la conclusión del proyecto y respecto al análisis realizado al final del mismo, insistiré en que los datos utilizados no son exactos, probablemente sean un punto medio entre precio de comprador y vendedor, ya que, en mi opinión si existiera la posibilidad de arbitraje todo el mundo compraría Bitcoins para intercambiarlos y sacar así su propio beneficio, por lo tanto, no podemos afirmar la existencia de arbitraje entre las 3 divisas.

IX. Bibliografía

- Ballota, D. (2012, 10). El BCE preocupado por las "monedas virtuales" que no controla y pueden utilizar los delincuentes. *Genbeta*. Recuperado 03, 2013, de <http://www.genbeta.com/activismo-online/el-bce-preocupado-por-las-monedas-virtuales-que-no-controla-y-pueden-utilizar-los-delincuentes>
- *Bitcoin*. Recuperado 11, 2013, de <http://elbitcoin.org/>
- Bitcoins. Mecambio. Recuperado 01,2014, de <http://mecambio.net/bitcoin/>
- Datos de cambio de divisas. *Coindesk*. Recuperado 11, 2013, de <http://www.coindesk.com/>
- Desmantelan en Francia plataforma ilegal de Bitcoins. *Ámbito.com*. Recuperado 07, 2014, de <http://www.ambito.com/noticia.asp?id=748458>
- *Bitcoin Noticias*. Recuperado 01, 2014, de <http://www.bitcoinnoticias.com/>
- Bitcoin.org, (2011, 05). ¿Qué es Bitcoin?. *Bitcoin.org*. Recuperado 12, 2013, de <http://elbitcoin.org/que-es-un-bitcoin/>
- Chevi, (2013, 04). Guia completa sobre Bitcoins. *Chevismo*. Recuperado 11, 2013, de <http://blog.chevismo.com/2013/04/guia-completa-sobre-bitcoins/>
- ¿Cómo minar Bitcoins? *.El BitcoinGratis.es*. Recuperado el 11,2013, de <http://www.elbitcoingratis.es/minar.php>
- Gomez, A. (2013, 12). Bitoin, ¿moneda futura?. *El mundo laboral*. Recuperado 02, 2014, de <http://www.elmundo.com.ve/noticias/tecnologia/internet/bitcoin---moneda-futura-.aspx>

- Gráficos de últimos datos de Bitcoin. *Blockchain*. Recuperado 03, 2013 , de <https://blockchain.info/es/charts/>
- Hoctro, (2014, 03). ¿Que es Bitcoin? Entendiendo su funcionamiento y uso. *Fraterneo GNU/LINUX*. Recuperado 05, 2014, de <http://fraterneo.blogspot.com.es/2014/03/que-es-bitcoin-entendiendo-su.html>
- Huky, G. (2013, 12). La historia del Bitcoin. De 2008 a 2013. *Gurus Blog*. Recuperado 01, 2014, de <http://www.gurusblog.com/archives/historia-bitcoin/14/12/2013/4/>
- Huky, G. (2013, 03). Bitcoin supera los mil millones de dólares. *GurusBlog*. Recuperado 01, 2014, de <http://www.gurusblog.com/archives/bitcoin-mil-millones/31/03/2013/>
- Jimenez, J. (2014,01). ¿Cómo conseguir Bitcoins gratis? .Blog oficial internet, *3Cero*. Recuperado 11,2013, de <http://3cero.com/bitcoins-gratis/>
- Majamalu, (2011, 07). Como obtener Bitcoins. *Bitcoin.org*. Recuperado 12, 2013, de <http://elbitcoin.org/bitcoin-para-principiantes-como-obtener-bitcoins/>
- Monedas Virtuales que han fracasado. *Oro en las nubes*. Recuperado 05, 2014, de <http://oroenlasnubes.com/2014/03/24/monedas-virtuales-que-han-fracasado/>
- Mercado Moneda, (2013, 11). ¿Cómo puedo comprar Bitcoins?. *Mercado Moneda*. Recuperado 12, 2013, de <http://mercadomoneda.com/como-puedo-comprar-bitcoins/>
- Muñoz, I. (2014, 02). ¿Qué es Bitcoin? ¿Cómo funciona? ¿Dónde se compran?. *ComputerHoy.com*. Recuperado 04, 2014, de <http://computerhoy.com/noticias/internet/que-es-bitcoin-como-functiona-donde-compran-5389>

- Newsweek, (2013, 03). Desvelada la identidad del creador de Bitcoin. *La Vanguardia*. Recuperado 12, 2013, de <http://www.lavanguardia.com/economia/20140306/54402864090/identidad-creador-bitcoin.html>
- Pascual, A. (2013, 04). Desafío a las grandes divisas: los Bitcoins en circulación ya valen más de 1.000\$ millones. *El confidencial*. Recuperado 10, 2013, de <http://www.elconfidencial.com/tecnologia/2013/04/02/desafio-a-las-grandes-divisas-los-bitcoins-en-circulacion-ya-valen-mas-de-1000-millones-4590/>
- Pérez, D. (2013, 04). Guía rápida para 'minar' Bitcoins desde el ordenador de tu casa. *El confidencial*. Recuperado 10, 2013, de <http://www.elconfidencial.com/tecnologia/2013/04/13/guia-rapida-para-minar-bitcoins-desde-el-ordenador-de-tu-casa-4667/>
- Preukschat, A. (2013, 11). Precio del Bitcoin 2010 a 2011: los años de rebeldía. *Oro y finanzas*. Recuperado 05, 2014, de <http://www.oroymasfinanzas.com/2013/11/precio-bitcoin-cotizacion-2010-2011/>
- Preukschat, A. (2014, 02). Seguridad de las carteras Bitcoin: Medidas de seguridad para un monedero o wallet Bitcoin (II). *Oroyfinanzas.com*. Recuperado 06,2014, de <http://www.oroymasfinanzas.com/2014/02/seguridad-carteras-bitcoin-medidas-monedero-wallet/>
- ¿Qué es Bitcoin? Video tutorial. *Youtube*. Recuperado 11,2013 de <http://www.youtube.com/watch?v=Um63OQz3bjo>
- ¿Qué es el Bitcoin?. ¿Qué es el Bitcoin? Una sencilla introduccion. *Que es Bitcoin*. Recuperado 04, 2014, de <http://www.quesbitcoin.info/el-valor-del-bitcoin.html>
- ¿Qué es Bitcoin? Una sencilla introducción. *ComputerHoy.com*. Recuperado 04, 2014, de <http://www.quesbitcoin.info/el-valor-del-bitcoin.html>

- Riesgo, A. (2011, 08). Bitcoin. ¿El dinero del futuro? *Nubaria*. Recuperado 01, 2014, de <http://www.nubaria.com/es/blog/?p=43>
- Senserrich, R. (2014, 01). Del valor de una moneda y el problema con bitcoin. *Politikon*. Recuperado 05, 2014, de <http://politikon.es/2014/01/07/del-valor-de-una-moneda-y-el-problema-con-bitcoin/>
- Sharecast, (2013, 12). Especial Bitcoin: la divisa digital que quiere parecerse al Oro y acapara portadas. *Bolsa Manía*. Recuperado 03, 2014, de <http://www.bolsamania.com/noticias/mercados/especial-bitcoin-la-divisa-digital-que-quiere-parecerse-al-oro-y-acapara-portadas--155691.html>
- Sisternes, A. (2013, 12). La historia del Bitcoin: ¿cómo ha evolucionado estos años? . *Rankia*. Recuperado 12, 2014, de <http://www.rankia.com/blog/divisas-y-forex/2082787-historia-bitcoin-como-evolucionado-estos-anos>
- Skeo, A. (2014,01). Bitcoins; ICB te cuenta que son y como operarlos. *Infobae*. Recuperado 02,2014, de <http://www.infobae.com/2014/01/17/1537800-bitcoins-icb-te-cuenta-que-son-y-como-operarlos>
- Vocabulario Bitcoin. *Bitcoin*. Recuperado 12, 2013, de <https://bitcoin.org/es/vocabulario>
- Wayer, F. (2014, 07). Francia cierra por primera vez un sitio de intercambio de Bitcoins. *Que pasa en Venezuela*. Recuperado 07, 2014, de <http://quepasaenvenezuela.com/2014/07/07/francia-cierra-por-primera-vez-un-sitio-de-intercambio-de-bitcoins/>
- Zoomboomcrach, (2014, 04). La mejor explicación sobre qué es Bitcoin, la moneda virtual. *La información*. Recuperado 05, 2014, de <http://blogs.lainformacion.com/zoomboomcrash/2014/04/10/la-mejor-explicacion-sobre-que-es-bitcoin-la-moneda-virtual/>

Anexo

VOCABULARIO SOBRE TECNICISMOS DEL BITCOIN

- **BTC:** Es el símbolo del bitcoin.
- **Monedero/Wallet:** Programa que guarda los Bitcoins que una persona posee y permite transferir i recibir Bitcoins sin intermediarios mediante las claves privadas, es más o menos como un monedero físico pero en la red Bitcoin.
El monedero puede utilizarse online o se puede descargar mediante una aplicación y se queda guardado en el propio ordenador.
- **Monedero de papel:** Forma de guardar bitcoins que consiste en escribir las direcciones y sus claves privadas en un papel.
- **Bloque:** Conjunto de transacciones de bitcoins agrupadas para ser verificadas y unir las a la cadena de bloques.
- **Bloque génesis:** Nombre que recibe el primer bloque de la cadena de bloques.
- **Cadena de bloques:** Es un registro histórico de todas las transacciones válidas de Bitcoin realizadas y, de manera cronológica y pública, la podemos considerar como la contabilidad de la red Bitcoin.
- **Clave privada:** Es un número secreto que permite gastar los bitcoins. Cada dirección Bitcoin tiene asociada una clave privada. La clave privada está relacionada matemáticamente con la dirección Bitcoin, de tal modo que la dirección Bitcoin se deriva de la clave privada siguiendo unas reglas fijas, mientras que la operación inversa, deducir una clave privada a partir de la dirección Bitcoin, es imposible.
- **Clave pública:** Un texto alfanumérico del cual se obtiene trivialmente una dirección y que es conocido por todos. Al ser conocido por todos, cualquiera puede enviarle bitcoins a la dirección asociada. Pero solo quien tenga la clave privada asociada podrá disponer de ellos. La clave pública es generada fácilmente a partir de la clave privada.

- **Comisión:** Una pequeña suma de bitcoins que se entrega al minero que resuelve el bloque como recompensa
- **Confirmación:** Es el hecho de resolver un bloque e incluirlo en la cadena de bloques, estableciendo así la validez de las transacciones incluidas en él y afianzando más aún la confianza de los bloques anteriores.
- **Criptomoneda:** Monedas digitales que funcionan en redes descentralizadas, donde las partes actúan directamente entre sí. El bitcoin es la más conocida de estas monedas, pero no la única.
- **Criptografía:** Utilización de las matemáticas para crear mensajes de forma tal que solo el destinatario pueda comprender su significado. Si un tercero interceptara el mensaje, no podría comprenderlo.
- **Deflación:** La revalorización de una moneda con el paso del tiempo. Esto trae como consecuencia la disminución de los precios y el aumento del poder de compra.
- **Dificultad:** Número que determina cuántos hashes en promedio se necesitan crear hasta encontrar aquel que resuelve el bloque. La propia red ajusta la dificultad para asegurar que en promedio se resuelva 1 bloque cada 10 minutos, de manera si más gente pone su ordenador a buscar Bitcoins esa dificultad se ajusta automáticamente para mantener esa velocidad.
- **Dirección:** Es un identificador que tiene entre 27 y 34 caracteres alfanuméricos, comenzando por el número 1 o el 3, que representa un destino de Bitcoins, es decir, se utiliza para enviar y recibir Bitcoins.
- **Firma digital:** Proceso matemático que comprueba la autenticidad del remitente de un mensaje de forma tal que el receptor puede verificar que el mensaje fue escrito por este y por nadie más, y que el éste no fue alterado o modificado por otra persona.
- **Hash:** Un hash de un objeto es el equivalente de nuestra huella dactilar. Es una identificación única y constante. Dos objetos distintos tienen (teóricamente) hashes

distintos. Además, tiene la peculiaridad de que, si tienes el objeto es muy fácil obtener su hash. Sin embargo, si tienes el hash es extremadamente difícil obtener el objeto original del que proviene. En el caso de Bitcoin, el algoritmo es SHA256.

- **Inflación:** La desvalorización de una moneda con el paso del tiempo. Esto trae como consecuencia el aumento de los precios y la disminución del poder de compra.
- **Minería:** Resolución de un bloque, certificando todas las transacciones que contiene. A cambio, el minero recibe una recompensa en Bitcoins nuevos Bitcoins. De esta forma se generan nuevas monedas en la red.
- **Nonce:** Un número que se añade al hash del bloque anterior para intentar resolverlo. Si el hash encontrado no resuelve el bloque, se incrementa el nonce y se vuelve a intentarlo.
- **Pool de minería:** Es la agrupación de un conjunto de mineros que se unen para generar hashes de manera más rápida y así aumentar la probabilidad de resolver el bloque y obtener la recompensa, la cual se divide de forma proporcional entre los mineros.
- **Satoshi Nakamoto:** Es el pseudónimo de la persona o grupo de personas que inventaron el Bitcoin. Nadie conoce su verdadera identidad.
- **Volatilidad:** La medida en que fluctúa una divisa a lo largo del tiempo.