Bitcoin

Guía completa de la moneda del futuro

ra-ma empresa

Santiago
MÁRQUEZ SOLÍS

Bitcoin

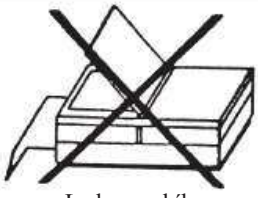
Guía completa de la moneda del futuro

Bitcoin

Guía completa de la moneda del futuro

Santiago Márquez Solís

Ra-Ma®



La ley prohíbe
fotocopiar este libro

Bitcoin. Guía completa de la moneda del futuro

Editado por:
RA-MA Editorial
Calle Jarama, 3A, Polígono Industrial Igarsa
28860 PARACUELLOS DE JARAMA, Madrid
Teléfono: 91 658 42 80
Fax: 91 662 81 39
Correo electrónico: *editorial@ra-ma.com*
Internet: *www.ra-ma.es* y *www.ra-ma.com*
ISBN: 978-84-9964-627-5
Depósito legal: M-4831-2016
Maquetación: Antonio García Tomé
Diseño de portada: Antonio García Tomé
Filmación e impresión: Copias Centro
Impreso en España en marzo de 2016

A Sofía y Jesús...

...por un mundo mejor para vosotros,
porque lo imposible solo tarda un poco más.

ÍNDICE

PRÓLOGO

Las cosas cambian. Todo está sujeto a esta ley. Da igual donde miremos, todo es cambio y nada permanece inalterado para siempre. ¿Todo? Bueno, al menos casi todo, porque el funcionamiento del dinero y cómo la sociedad se articula en torno a él no ha variado mucho en los últimos siglos.

Sin embargo, la llegada de Bitcoin parece que va a cambiar esta situación. Parece que el poder democratizador de la Red también va a llegar a tocar el instrumento que hace que estados y gobiernos puedan ejercer su manipulación sobre los ciudadanos.

Nos guste o no, el dinero es una institución social y es el mecanismo inventado para organizar las actividades económicas de una sociedad, pero como todos los inventos creados por el hombre, tiene sus cosas buenas pero también sus defectos, y aunque estamos acostumbrados a tener mejores coches, mejores casas, mejores comunicaciones, mejores ropas y alimentos de mejor calidad, pocas veces nos hemos planteado que esto mismo debería ser aplicable al dinero. **¿Es no solo posible, sino además deseable, tener una moneda de calidad?**

Creo que Bitcoin puede ser también la respuesta a todos los que nos hemos hecho alguna vez esta pregunta, y a pesar de sus lados oscuros y de la incertidumbre que aún existe, puede que nos encontremos ante una revolución comparable solo a la propia Internet, y esta revolución viene de la mano de dos ideas principales: una, la separación entre el Estado y la moneda, y otra la tecnología de la cadena de bloques (blockchain).

Y dado que muchos tratan de criminalizarlo y obstaculizar su imparable éxito, otros queremos darlo a conocer, porque estamos seguros de que a la larga seremos capaces de crear una sociedad mejor para nuestros hijos.

Antes de comenzar, te doy las gracias de antemano por tu tiempo y por el interés demostrado por este libro.

Madrid, 2016.

www.santiagomarquezsolis.com

ACERCA DE ESTE LIBRO Y A MODO DE BIENVENIDA

Hace casi algo más de tres años, comencé a leer artículos en algunos foros de Internet, en donde Bitcoin auguraba ser una auténtica revolución (con r minúscula), incluso reconozco que comencé a leer el artículo original de Nakamoto y me llegué a interesar por la minería, pero acabé dejándolo de lado; la idea fundamental de moneda electrónica y de criptomoneda no eran conceptos nuevos, y los principios cuasi filosóficos sobre **criptoanarquía**, aunque muy interesantes sobre el papel, siempre pensé que llegar a ponerlos en práctica en la realidad era muy complicado. La barrera de entrada era demasiado elevada, y ni bancos ni gobiernos, por no decir en general todo el mundo financiero, poseían unos intereses tan grandes en dejar las cosas como estaban, que permitir que una moneda como Bitcoin pudiera ponerse en marcha; era simplemente algo inconcebible, máxime después de ver como otras iniciativas, aunque diferentes en su ejecución, similares en su concepción, y que perseguían la utilización de monedas de uso voluntario, como el Liberty Dollar, por poner un ejemplo rápido, acababan con su fundador en la cárcel.

Sin embargo, me equivoqué y demostré tener poca visión de futuro, subestimé el poder de la Red y de las personas que trabajan en ella, y que Bitcoin no es sino una respuesta, que tarde o temprano y tal y como están las cosas, tenía que acabar sucediendo; era la respuesta a la pregunta que en muchas ocasiones estoy seguro que te habrás hecho, **¿cómo podemos cambiar las cosas y hacer un mundo más justo y mejor?** Hoy casi cuatro años más tarde, la revolución no solo se ha puesto en marcha, sino que da muestras de llegar a producir un auténtico cambio en el orden de las cosas.

Si los augurios se confirman, estaríamos ante el principio del cambio del sistema económico mundial y de la sociedad en su conjunto, y nos estaríamos

enfrentando a algo sin precedentes, ni más ni menos que a la división entre Estado y moneda. Sé que quizás es aún pronto para verlo, y quizás alguien pueda pensar que exagero, que Bitcoin no es más que un experimento fallido que no llegará a nada, y que el convulso año 2014 que tuvo no es más que la muestra de que no va a ningún lado.

Según el portal **Sputnik**, hay cinco razones básicas que harían que Bitcoin acabase desapareciendo a lo largo del año 2015: el precio, la cada vez menos rentable labor de los mineros, la falta de protección de los consumidores, su bajo ritmo de adopción y que Bitcoin no es más que una moda pasajera.

¿Llevaban razón en sus argumentaciones y pésimos augurios? ¿Desaparecerá Bitcoin este año? Pienso que no, y espero que las razones que vamos a dar a lo largo de este libro sean suficientes para que veas por qué están equivocados.

Aquellos que dan por muerto a Bitcoin lo hacen demasiado pronto, se centran y justifican sus argumentos basándose solo en el precio y dejan de lado otras muchas cuestiones. Por eso, y al igual que sucede con la función exponencial, cuando se mira un rango acotado de sus valores sin tener en cuenta toda la función, parece que la variación y el aumento entre puntos es lineal y poco importante; solo cuando se produce el salto y se mira desde mucho más lejos se ve que el punto de inflexión es tan dramáticamente fuerte y veloz, que una vez se produce, nadie puede escapar de su influencia.

Si la idea de separar Estado y moneda nos resulta atractiva a muchos, hay otra que aún es mucho más sutil para el recién llegado a este panorama, me refiero al poder de la cadena de bloques, y a sus enormes posibilidades para permitirnos crear una nueva gama de aplicaciones que van a complicar mucho a los Estados el control y vigilancia continua a la que quieren someternos.

Pero, ¡ojo!, todo esto no es fácil de entender, pagar con Bitcoines no es aún cómodo y es previsible que siga sin serlo durante algún tiempo; entender sus entresijos no es trivial, lidiar con conceptos criptográficos nos asusta, y el panorama, al menos al principio, puede echarnos para atrás.

A pesar de tantos inconvenientes y tantas voces hablando en contra, así es como veo a Bitcoin y a las criptomonedas en general, como algo arrollador que acabará formando parte de tu vida, del mismo modo que ahora mismo no puedes entender vivir sin Internet, sin estar completamente conectado en cada momento, sin tener tu móvil al alcance de la mano (¿recuerdas cuando hablar por móvil en la calle era considerado algo solo de altos ejecutivos y de lo más extravagante? Y ¿cuánto hace de ello? Se puede decir que fue ayer); llegará un día (y no muy lejano) en donde no podrás vivir sin Bitcoines y su tecnología subyacente.

Si quieres formar parte de la Revolución (y ahora con r mayúscula) y tu objetivo es comprender cómo funciona esta moneda, qué la hace tan especial, por qué te interesa entenderla y adoptarla cuanto antes, y el porqué de sus bondades, entonces, todo lo que cuento es para ti.

A lo largo de este libro, conocerás todos los conceptos que hay detrás de Bitcoin, aprenderás a usarlo y a encajarlo en el complicado entramado monetario digital en el que nos movemos.

Te aseguro que no quedarás defraudado.

MOTIVACIÓN

El universo de las criptomonedas es un universo muy vivo y muy, muy amplio, en donde los cambios y las noticias se producen, aunque sea una obviedad decirlo, a una velocidad de vértigo. Debido a ello, hay quien no logra entender el verdadero significado de lo que es Bitcoin y prefiere esperar a ver qué sucede; no resulta fácil de entender a primera vista y eso que estamos hablando de algo *a priori* sencillo, ni más ni menos que de dinero, algo que usamos todos los días.

Tampoco contribuye mucho cuando en los medios de comunicación parecen haberse empeñado en asociar la palabra Bitcoin con otras tan poco amigables como drogas, prostitución, delincuencia… como si el euro o los dólares pudieran estar ajenos a esta realidad, que nos guste o no nos guste está ahí, pero que es independiente del mecanismo monetario que se utilice para su acceso y financiación.

¿Qué podría hacer yo para contribuir a su difusión y ayudar a que la gente que no lo conoce se acercara a Bitcoin y viera su verdadero potencial? Pues una de las cosas que creo que mejor se me da hacer: explicar lo difícil de manera fácil, utilizar la experiencia que tengo a lo largo de los años formando en tecnología a mucha gente y mostrar que, si tal vez se intenta que Bitcoin no resulte inteligible o se le persigue, puede ser precisamente por su elevado poder para cambiar y revolucionar.

REQUISITOS PREVIOS

La pregunta que puede surgirte es ¿necesito yo, simple mortal, tener algún conocimiento particular para poder entender lo que vas a explicar o podré entenderlo sin demasiados problemas? La respuesta a esta pregunta varía un poco en función de donde te encuentres, pero en general puedo responderte que **no**, no es necesario que tengas ningún requisito previo para poder entender la mayor parte de lo que vamos a ver en este libro, está pensado para una persona que no conoce nada de criptomonedas, aunque para ser justos vamos a hacer unos matices.

Los **dos primeros capítulos**, dedicados a explicar mi justificación de la necesidad de Bitcoin en la sociedad y el concepto de dinero electrónico y los conceptos básicos como doble gasto, P2P, Internet oculta, etc., no requieren de ningún conocimiento previo, solo tener la mente abierta y creer que es posible cambiar las cosas y entender unos conceptos básicos muy sencillos. Además la historia del origen de Bitcoin y de quién es Satoshi Nakamoto resulta digna de un guión de Hollywood.

En el **capítulo 3**, comenzaremos a trabajar con Bitcoin, y puede resultarnos un poco más complicado tal vez al principio; rápidamente veremos que si estamos acostumbrados a instalar aplicaciones en nuestro ordenador, con seguir los asistentes de configuración habremos hecho la parte más complicada del trabajo. Hay algunos conceptos un poco más novedosos que igual pueden sonarte raros al principio, como puede ser la idea del determinismo de una billetera o las ideas en las que se basa la multifirma, pero nada que tenga un nivel de complejidad que resulte insalvable.

El **capítulo 4**, dedicado a la criptografía, es un poco más complicado, pero del mismo modo, tampoco se requiere ser un gurú en el tema, siguiendo el avance natural del libro, veréis que todo es más sencillo de lo que parece; me he esforzado en que las matemáticas no sean un problema para comprenderlo, y lo he articulado de modo que si alguien quiere saltárselo, pueda hacerlo sin que se penalice el no

haberlo leído. Sin embargo, personalmente yo no me saltaría este tema a pesar de que más de uno pensará que menudo rollo.

No somos conscientes de la sociedad en la que actualmente vivimos y de la cantidad de información que cedemos de nuestras vidas de manera completamente gratuita y sin control ninguno. Es común que la gente diga "no tengo nada que ocultar" o "no me importa", pero realmente lo que está diciendo es no me importa ceder el derecho a controlar lo que hay en Internet de mí, algo que es muy peligroso. Comprender la criptografía debería ser algo que desde ya tiene que estar incluido en nuestra operativa diaria, y que no debemos relegar a terceros. Es como cuando coges el coche y te tienes que poner el cinturón de seguridad, al principio resulta un poco incómodo, e incluso puedes a veces olvidarlo, pero una vez se hace costumbre, quién saldría de viaje sin ponérselo. En este capítulo también se explica hasta dónde llega la anonimidad de Bitcoin y hasta qué punto las transacciones que dejamos en la *blockchain* pueden llevarnos a nosotros.

El **capítulo 5** es un monográfico sobre los aspectos técnicos de Bitcoin en toda regla, la mayor parte de los aspectos que se te puedan pasar por la cabeza sobre su funcionamiento están explicados y recogidos aquí. Todas las piezas que falten del puzle y que no hayan sido explicadas en los capítulos anteriores lo serán en este y se profundizará en las definiciones previas que se dieron. Veremos en más detalle el funcionamiento de las transacciones y como estas se integran en los bloques para formar la cadena de bloques, el libro contable público donde está registrado todo lo que ha sucedido desde que se puso en marcha Bitcoin. A lo largo de este capítulo también entraremos en más detalle en la minería, el éxito o fracaso a futuro de Bitcoin radica en gran medida en la existencia de mineros que sean capaces de soportar el proceso de la red, tanto en la generación de nuevas monedas, como en el mantenimiento de la cadena de bloques.

Finalmente, en el **capítulo 6** se intenta abordar y explicar el futuro de Bitcoin, los proyectos que se están realizando con él sobre base, las nuevas alianzas que han surgido para defenderlo, la evolución de las inversiones de capital riesgo y las mejoras que se quieren implementar. El desarrollo de aplicaciones nativas o la creación de contratos digitales son algunos ejemplos, y plataformas como Coinbase o Ethereum están proporcionando herramientas y API de programación para facilitar la expansión de este tipo de desarrollos. Este capítulo es quizás el más arduo de entender, y estar familiarizado con algunos conceptos de programación puede ayudarnos, aunque no se entra en detalles de codificación ni se abordan cuestiones de implementación.

ACERCA DEL AUTOR

Probablemente llegados a este punto, alguien pueda preguntarse quién soy yo (cosa por otro lado del todo lógica y comprensible) y cuál es mi interés y motivación por el mundo de Bitcoin. Para satisfacer esta curiosidad, aquí presento esta pequeña carta de presentación y dejo en manos del lector la valoración que de este libro y de los siguientes quiera realizar.

En primer lugar, me llamo Santiago Márquez Solís y nací en Madrid, y la informática ha sido mi pasión desde que mis padres me regalaron, cuando era chiquitín, un ZX Spectrum. Desde el momento en que aquel ordenador cayó en mis manos, supe que dedicaría mi vida a trabajar con ellos y ahora mismo, llevo casi 20 años de carrera profesional, que se dice pronto. Probablemente si alguien me pidiera que usara una palabra para definirme profesionalmente usaría la palabra polifacético, porque a pesar de tener un trabajo "oficial" durante estos años, siempre me las he ingeniado para realizar labores paralelas que me enriquecieran profesionalmente aunque no fueran mi trabajo principal; fundamentalmente estas labores paralelas han sido tres: el desarrollo de proyectos *freelance*, la formación técnica y el desarrollo de videojuegos.

Mi actividad profesional oficial no es ningún secreto, y está disponible para cualquiera que quiera consultarla en mi perfil de LinkedIn, aunque por resumirla un poco, en los últimos años trabajo en la gestión de aplicaciones económicas de un importante organismo público, como consultor de proyectos en carácter de personal externo. El tema del dinero, por ese lado, me toca muy de cerca.

El desarrollo de proyectos *freelance* y la formación técnica es algo que de vez en cuando surge, uno ya tiene sus años y conoce a mucha gente en el sector, y a veces te ofrecen oportunidades de hacer algo diferente, porque seamos sinceros, el trabajo normal, y aunque trabajes en Google creo que acaba por pasar, termina

por ser monótono. Estos proyectos son bocanadas de aire fresco, que ayudan a no dejar de lado la evolución tecnológica, algo que como ingeniero que soy, creo que es indispensable nunca olvidar.

Aunque lo que a mí más me apasiona, además de Bitcoin, son los videojuegos. Supongo que como a muchos otros jóvenes de mi generación, casi pioneros porque fuimos de los primeros en disponer de un ordenador en casa, una de las posibilidades que más me fascinaron era la creación de juegos; de hecho con él hice mis primeros pinitos en este mundo, creando un pequeño juego del tipo *Arkanoid* en Basic, aunque el juego realmente serio que creé fue una aventura conversacional llamada *Diatmar*, que se publicó en la ya extinta revista *Microhobby*, en la sección *Mundo de la Aventura* comandada por el inolvidable Andrés Samudio.

ENTONCES…

Con un emulador de **Spectrum** todavía se puede jugar a **Diatmar** y descargártelo desde World of Spectrum.

A posteriori creé un pequeño juego llamado *House* con la herramienta **3D Construction Kit 2**, que resultó ganador de la segunda edición que la revista *Micromanía* realizó de aplicaciones construidas con este programa allá por el año 1993 (gané un fantástico ordenador **Amiga 1200** que aún conservo); desgraciadamente perdí el código del juego y no he sido capaz de recuperarlo nunca, y ahora me encuentro reescribiéndolo para Android.

Unos cuantos años más tarde creé un sitio web llamado **goodForYourMind.com**, donde durante el año 2002 tuve alojados una serie de tutoriales de programación de juegos en C++, sin embargo, el tener montados los servidores en casa no resultó ser una buena idea y cuando me mudé, aquel proyecto quedó definitivamente abandonado. Después de aquello y de manera esporádica he publicado artículos relacionados con el tema en diferentes medios, los últimos de ellos fueron en la revista *Todo Programación* en 2006, sobre la creación de juegos para móviles con J2ME.

Mi andadura por el mundo de los videojuegos continúa en 2012, cuando fundé la empresa **z-games.es ltd**, dedicada al desarrollo de juegos de tipo independiente para dispositivos móviles. A través de esta empresa llevo publicados tres juegos: los *remakes* de *La Aventura Original* y de *La Guerra de las Vajillas* y un juego original y de cosecha propia llamado *Talking with God*.

La Aventura Original

Sin olvidar **#CalleBitcoin**, un juego del que hablaré un poco más adelante. Por cierto, en *La Guerra de las Vajillas* la moneda que usa el Imperio, en sus intentos por acabar con los Rebeldes sin Causa, es ni más ni menos que Bitcoin, un guiño simpático que quise incluir y que sustituye a los créditos iniciales que se utilizaban en la versión Spectrum.

Pero es que también me gusta escribir, y tengo publicado otro libro, *La Web Semántica*; lo escribí cuando creé el sitio web **laWebSemantica.com**, que es el resultado del emocionante viaje que comenzó cuando inicié mis estudios de ingeniería.

La Guerra de las Vajillas

Durante todo este tiempo, la tecnología en general (incluidos los videojuegos) ha sido para mí un mundo completamente fascinante, la revolución que ha supuesto para la sociedad el uso de Internet (aún recuerdo con cierta nostalgia cuando estando en los primeros cursos en la universidad, conocí Internet gracias al navegador de

texto lynks) y las herramientas que se han forjado gracias a ella me han permitido ampliar mi espectro de conocimientos y experiencias.

ENTONCES…

La Web Semántica estaba accesible originalmente en: *www.lawebsemantica.com*. Ahora ya no está en funcionamiento. Aunque si tienes mucha curiosidad puedes usar el buscador **archive.org** y por allí queda algún registro de lo que publiqué en su momento.

¿Cómo llega un fanático de los videojuegos a Bitcoin? Pues por casualidad, así de simple. Las teorías económicas siempre me han gustado, y me gusta leer todo lo que cae en mis manos sobre estos temas. Un día en un foro, encontré una referencia al *paper* de Nakamato y me pareció brillante, aunque de difícil implementación práctica; desde entonces, con mayor o menor grado de atención, nunca he perdido de vista a Bitcoin, hasta que llegados a este punto creo que es necesario darlo a conocer más que nunca, sobre todo por el empeño que hay en que no triunfe.

Lógico, cuando acabes de leer este libro entenderás el porqué.

Actualmente todos mis avances y logros profesionales los dejo reflejados en la web: *http://www.santiagomarquezsolis.com*

LOS PROYECTOS #CALLEBITCOIN Y MEETBMADRID

Tal es mi empeño en que Bitcoin sea conocido que hace unos meses, en colaboración con otro buen puñado de entusiastas que compartimos grupo en Facebook y en donde se encuentra mucha gente que "reparte el bacalao" del mundo Bitcoin hispano, resulta que a uno de ellos, **Félix Moreno**, se le ocurrió que sería una buena idea intentar montar en Madrid algo similar a lo que ya sucede en Alemania, Estados Unidos u Holanda y que consiste en tener un grupo de comercios agrupados físicamente y donde es posible comprar usando Bitcoines. En nuestro caso el objetivo era ni más ni menos que convencer a los comercios de la milla de oro madrileña, la famosa calle Serrano, una de las calles más importantes y lujosas, ya no de Madrid sino de todo el mundo.

Así que respondí a la petición que se hizo en el grupo pidiendo voluntarios que quisieran colaborar con el proyecto y me presenté en la primera reunión de la iniciativa **#CalleBitcoin**, que tuvo lugar en el restaurante doEat, uno de los primeros que tenían instalado un cajero Lamassu (ahora salvo error por mi parte está ubicado en el centro comercial ABC Serrano) y que permite operar con Bitcoines. Total, que nos propusimos recorrer la calle Serrano y ver qué podíamos sacar de todo esto, con un objetivo claro en mente, convencer al mayor número de comercios posible para que aceptaran Bitcoines y tener un día Bitcoin, al que llamamos **Día B**.

Dejo aquí una foto del grupo en su primera reunión:

Primera reunión de los voluntarios de #CalleBitcoin

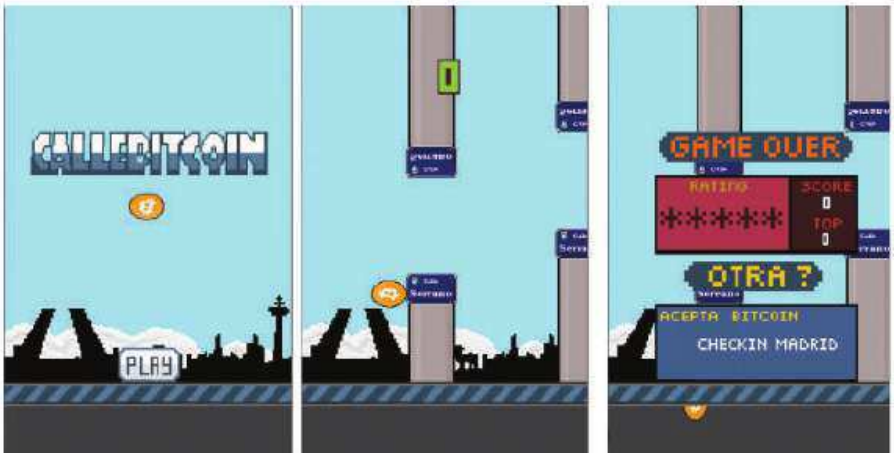
Y del material promocional que fuimos entregando durante el verano a cada uno de los comercios que visitamos.

Material promocional de #CalleBitcoin

Los días 3 y 4 de octubre de 2014 fueron finalmente los días elegidos para que la iniciativa #CalleBitcoin diera sus frutos. Algo de lo que tenemos que sentirnos muy orgullosos.

Pero, ¿os he dicho que el tema de los videojuegos es algo que me apasiona, verdad? Uniendo mi pasión por Bitcoin y por los videojuegos, para ayudar a promocionar el evento de **#CalleBitcoin**, puse en Google Play el juego *#CalleBitcoin*. Este juego sigue el mecanismo popularizado por el famosísimo *Flappy Bird*, aunque en vez de utilizar un pajarito e ir pasando entre tuberías, lo que tendremos que hacer

es que un valiente y aguerrido Bitcoin pase entre las señales de la calle Serrano, con un fondo madrileño muy castizo, que junto a la típica música de chotis madrileño, amenizarán nuestro viaje por el juego. Cuando nos maten tendremos información sobre alguno de los muchos comercios que en la calle Serrano permiten pagar con Bitcoines.



El juego para #CalleBitcoin

También después del verano, decidimos como un medio para dar continuidad a lo iniciado en el proyecto #CalleBitcoin, crear un punto de encuentro para que todo aquel que vive en Madrid y le apetezca charlar sobre Bitcoin, aprender un poco más y compartir sus experiencias con nosotros pueda hacerlo, por ese motivo comenzamos una serie de reuniones y encuentros presenciales. Inicialmente organizados en el **MediaLab de Madrid**, donde realizamos los tres primeros, luego pasamos a realizarlos en el **Broker Café** junto al estadio de futbol Santiago Bernabéu, y ahora mismo y desde el pasado 24 de abril de 2015, el lugar de las quedadas es el **Geographic** en la calle Alcalá. Después de un tiempo en el Broker, vimos la necesidad de tener un lugar en donde, a parte de tomarnos algo y hacer *networking*, poder dar pequeñas charlas sobre temas específicos. Recomiendo revisar la página de la convocatoria por si hubiese cambios más adelante que no estén reflejados en este libro.

Estas quedadas las organizamos a través de la página meetup.com, y desde aquí os invito, no os dé vergüenza ir, si vives en Madrid no tienes excusa para no hacerlo. Pasamos un rato muy divertido hablando sobre Bitcoin y conociendo gente que siempre resulta de lo más interesante e inspiradora. Ah, que se me olvida poneros la dirección para que estemos en contacto:

http://www.meetup.com/Encuentro-Semanal-Bitcoin-Madrid

Página del Meetup

¡Espero veros pronto en alguno!

Creo que con esta pequeña carta de presentación, sabrás un poco mejor quién soy y cuáles han sido mis motivaciones.

AGRADECIMIENTOS

En primer lugar **a mi abuela**, por haberme criado, y a mi **madre** por haber trabajado para sacarnos a mi hermano y a mí adelante, e inculcarnos una cultura del esfuerzo y del trabajo que hace que veas el mundo de un modo muy diferente.

También a mis dos hijos, **Sofía y Jesús**, sin ellos nada de lo que hago tendría el mismo sentido. Y a mi mujer **Encarna**, que se ocupa de todo lo demás y deja que yo pueda cacharrear y aprender; sin ella, nada sería igual.

Tengo que darle las gracias a mi amigo **Alberto Gómez Toribio**, una de las personas técnicamente más competentes que he tenido el placer de conocer, y que actualmente está detrás de una *startup*, **Coinffeine**, que revolucionará la forma de intercambiar dinero dentro de la red y los activos financieros. De momento ha conseguido ser la primera empresa del mundo constituida íntegramente en Bitcoines y que una entidad de la talla de Bankinter haya invertido en ella. Muchas gracias por tus sabios consejos.

Sin duda a quien quiera que sea **Satoshi Nakamoto**, por habernos hecho ver la luz.

A **Rocío Mogollón** de la Editorial RA-MA por haberme dado la oportunidad de que este libro pueda ver la luz y fijarse en mi trabajo previo en Amazon.

A todos los que trabajan por que Bitcoin siga adelante, incluidos aquellos a los que he tenido el placer de conocer durante la puesta en marcha de la iniciativa #CalleBitcoin y que siguen trabajando para que los *meetups* de Madrid sean un éxito, a Jaime, a los dos Álex, Félix, Eva, Antonio, Fernando… y a alguno que otro seguro que me dejo en el tintero, que sepa disculparme y no se enfade conmigo (o mejor que me mande un *email* y me lo diga y actualizo el texto).

Y cómo no, a todos los que de un modo u otro influyen en mi vida, y hacen que yo sea quien soy.

Y sí, también a Él y a Bit por los secretos que compartimos.

A todos ellos muchas gracias por su paciencia conmigo.

Para finalizar, espero que este libro resulte tan interesante y entretenido de leer, como para mí ha sido el escribirlo. Igualmente, a través de mi dirección de correo electrónico (*smarquezsolis@gmail.com*) o (*librobitcoin@gmail.com*) se me puede enviar cualquier comentario, crítica o sugerencia que se me quiera hacer, y estaré sumamente interesado en recibirlos, leerlos y por supuesto contestarlos.

Sin más preámbulos comencemos pues con nuestro viaje por el mundo de Bitcoin y las criptomonedas.

1

¿POR QUÉ BITCOIN?

Aunque todos estamos acostumbrados a manipular el dinero, por regla general, si nos ponemos a hablar con cualquier persona sobre él, además de sentirse bastante incómoda, resultará paradójico que algo de vital importancia para el desarrollo de nuestra vida diaria sea tan desconocido. Y no me refiero solo a sus orígenes, sino fundamentalmente a su funcionamiento, al papel que juegan los bancos centrales, el porqué de que la inflación y su control resulten tan importantes, qué es el precio del dinero, por qué liquidez y rentabilidad influyen de manera diferente, por qué devaluar una moneda es un acto que debería de preocuparnos y en definitiva a conocer las reglas del juego, del juego del dinero, valga la redundancia.

ENTONCES…

Un pequeño apunte antes de ir más lejos, más que nada por los puristas. Generalmente se utiliza la palabra Bitcoin, con **B mayúscula** para indicar que nos estamos refiriendo al protocolo Bitcoin, mientras que cuando se usa Bitcoin (con **b minúscula**), se habla de unidad de medida. A lo largo del libro yo utilizo Bitcoin con B mayúscula en ambos casos por simplificar y no enzarzarnos en debates que nos alejen del objetivo principal, comprender lo que Bitcoin (con B/b) realmente es. Cuando hayas acabado de leer el libro, podrás poner la B/b donde corresponda sin problemas. Por cierto, esto es aplicable a todas las criptomonedas, Dogecoin (protocolo) vs. dogecoin (moneda), Litecoin (protocolo) vs. litecoin (moneda), etc.

El desconocimiento de estas reglas es, en mi modesta opinión, la principal razón por la que gran parte de la población nunca llega a fin de mes, y pasa la mayor parte de su vida endeudada, viendo el dinero como un problema, más que como lo que realmente es, un medio de intercambio de bienes y servicios. Tal vez Bitcoin se

convierta en una de las llaves que permita que podamos liberarnos y llegar a obtener la tan ansiada libertad financiera que todos buscamos o al menos deberíamos intentar buscar y más ahora, donde las palabras crisis y recesión económica están a la orden del día.

Y es que, nos guste o no nos guste, el dinero es una institución social, y es el mecanismo inventado para organizar las actividades económicas de una sociedad, y como todos los inventos creados por el hombre, tiene sus cosas buenas pero también sus defectos, y aunque estamos acostumbrados a tener mejores coches, mejores casas, mejores comunicaciones, mejores ropas, y alimentos de mejor calidad, pocas veces nos hemos planteado que esto mismo debería ser aplicable al dinero. ¿Es no solo posible sino además deseable, tener una moneda de calidad? Creo que Bitcoin puede ser también la respuesta a todos los que nos hemos hecho alguna vez esta pregunta, y a pesar de sus lados oscuros y de la incertidumbre que aún existe, puede que nos encontremos ante una revolución comparable solo a la propia Internet, y esta revolución no es otra que la separación entre el Estado y la moneda.

Es muy fácil decir que la culpa de todos los males la tiene el dinero, personalmente yo no comparto esa opinión, creo sencillamente que es un problema de entender cómo funciona el sistema y comprender como la economía, nos guste o no, es algo que nos afecta a todos, y si no somos capaces de entenderla/o, ¿cómo vamos ni tan siquiera a intentar cambiarla/o de un modo inteligente y efectivo?

He intentado, siempre que he podido, añadir cuestiones y preguntas que debemos hacernos referentes a qué sucedería con tal o cual cosa si el uso de Bitcoin llega a generalizarse, y fijaos en que digo preguntas, no respuestas, yo carezco de muchas de ellas, tengo mi opinión personal al respecto forjada por mi experiencia y te lo hago saber desde este mismo momento. Creo que cada uno de vosotros debéis llegar a crear vuestra propia opinión, por tanto vuestro aporte personal será tan importante como puede serlo el mío, considerarme si queréis como un *sherpa*, alguien que ha recorrido la montaña antes y sabe dónde está, si no el mejor camino, al menos uno de los más seguros para llegar a la cima, pero sin presumir de conocer todos los entresijos y recovecos, la gracia es que juntos lleguemos (como decía el poeta) no a mi verdad ni a la tuya, sino a la verdad, o al menos a lo más parecido que esta pueda ser y como quiera que sea, creo que podemos conseguirlo o al menos acercarnos bastante.

Probablemente este primer capítulo pueda ser el más controvertido, porque mis opiniones sobre cómo funcionan los Estados, por qué considero que la deuda es algo perjudicial, bancos centrales y por qué justifico que Bitcoin será un éxito, pueden no coincidir con las tuyas, o incluso puede que alguna explicación en un intento por simplificar lo haya hecho tanto que resulte demasiado obvia, pero no olvides una cosa: todo el que llega a Bitcoin o cualquier otra criptomoneda, debe

verse como un pionero en territorio inexplorado, y los escenarios posibles que pueden aparecer en los años próximos no están para nada claros, aunque los indicios parecen apuntar a que Bitcoin será algo muy importante; hay quien dice que es una burbuja y que acabará por estallar, otros que es una moda pasajera, otros que la propia base de su modelo deflacionista lo hará caer y colapsar, o que otras criptomonedas como Litecoin son mejores.

Sin embargo, hay otros que opinan que es el medio necesario que hacía falta para reestructurar el sistema económico mundial y dar el siguiente paso evolutivo. ¿Quién lleva razón? Si he decidido escribir todas estas páginas y dedicar muchas horas a ello, es porque firmemente no creo que estemos ante una moda pasajera. El tiempo nos dirá hasta qué punto estaba en lo cierto, en cualquier caso, lo que sí vas a lograr es hacerte una opinión sólida sobre la situación que se vive en estos momentos y poner tu granito de arena. Si entidades financieras españolas como Bankinter (en la *startup* española Coinffeine), BBVA (en la *startup* americana Coinbase) o más recientemente Santander (en Ripple) han decidido meter capital riesgo en empresas que trabajan con Bitcoines, debe ser sinónimo de que algo al menos les inquieta, ¿no os parece? Por no decir que 2014, a pesar de haber sido el peor año de Bitcoin (si solo nos fijamos en el precio, claro), ha sido el año en donde se han invertido más de 500 millones de dólares en startups involucradas con el desarrollo de la criptomoneda, superando incluso los mejores momentos de inversión en la naciente Internet hace ya varias décadas.

Da que pensar, sobre todo si tenemos en cuenta que Bitcoin está aún en sus inicios y que sus posibilidades están comenzando a dibujarse en el horizonte y que todavía sigue siendo un software experimental, no olvidarlo, pero que ha logrado movilizar a muchísima gente con ganas de hacer las cosas de un modo diferente.

¿Qué espero conseguir con lo que voy a contarte? Lo más importante es explicar por qué creo que Bitcoin es revolucionario (a pesar de su juventud o de ese estado inicial experimental en donde aún se encuentra); parto del funcionamiento básico del dinero y de lo que significa su uso en la economía, y trato de poner en contexto, en un momento como el que actualmente vivimos, la llegada de las criptomonedas en general y de Bitcoin en particular. Estoy seguro de que entonces entenderás mucho mejor las diferencias que presenta con el dinero tradicional y por qué es tan especial, y serás capaz de diferenciarlo de sus competidores.

Además, los acontecimientos que sucedieron a lo largo de 2014, como el cierre de Mt. Gox, el robo en Bitstamp o Bter y las prohibiciones por parte de algunos países, que intentan por todos los medios criminalizar el uso de Bitcoin, hacen más que necesaria la existencia de libros como este que expliquen de un modo sencillo por qué es necesario que Bitcoin triunfe, es necesario acercar Bitcoin a la gente y que se entienda cómo funciona si queremos que llegue a imponerse y a generalizarse

como moneda de masas. Pero, incluso en el caso de que esto no llegue a suceder y quede como un mero experimento monetario, aún queda otra parte si cabe más importante, y es como la tecnología de la cadena de bloques puede ayudarnos a crear una nueva generación de aplicaciones que pueden reordenar la sociedad.

A modo de conclusión de esta introducción, me quedo con una frase, aparecida en enero de 2015 en el *Wall Street Journal*, sobre el potencial de Bitcoin y donde los autores Michael J. Casey y Paul Vigna dicen:

"Bitcoin es radicalmente nuevo, un sistema descentralizado de la manera que la sociedad gestiona el intercambio de valor. Es, sencillamente, una de las innovaciones más potentes en las finanzas de los últimos 500 años".

Para abrir boca, no está nada mal el comentario.

1.1 EL ORIGEN DEL DINERO

Pero empecemos por el principio…

El origen del dinero es casi tan antiguo como la propia civilización, y apareció a lo largo del período Neolítico, de un modo gradual y paulatino, que avanza a medida que las relaciones entre los seres humanos y las transacciones que se realizan entre ellos se vuelven más complejas. Aunque la frase pueda resultar escandalizadora a más de uno, el dinero surgió para facilitarnos la vida y mejorar nuestras relaciones.

Durante el período Neolítico, al principio, no existía el dinero, la forma en la que unos humanos "hacían negocios" con otros era a través del intercambio o trueque. Este sistema era más que suficiente al principio, aunque implicaba que se diera la doble coincidencia de necesidades, o dicho de otro modo, que lo que yo tengo para cambiar y lo que necesito coincidiera con las necesidades de otra persona.

Puede que yo sea un cazador y tenga pieles y quiera zanahorias, pero el agricultor que tiene las zanahorias en ese momento no está interesado en las pieles, sino que necesita vasijas de barro, luego o encuentro a un agricultor con zanahorias y necesidad de pieles, o no tendré zanahorias. Como se ve por este ejemplo tan tonto, hay una serie de problemas que se resumen en:

- Los intercambios dependían de la demanda de cada individuo en cada momento, por tanto no se pueden adaptar a las urgencias inmediatas de estos (¡yo quiero zanahorias ya!).

- Hay un problema relacionado con el valor de los productos y las **equivalencias** entre ellos, sería algo así a responder a la siguiente pregunta: ¿a cuántas zanahorias equivale una piel?

- También tenemos el problema de que no todos los bienes son igualmente fáciles de intercambiar, las zanahorias se pueden llevar en una cesta, las pieles pueden requerir un transporte más complicado.

- Como hay que buscar a alguien para hacer casar los intereses de los participantes en el intercambio, el proceso puede ser muy lento y difícil, igual el agricultor que quiere pieles y tiene las zanahorias está a dos días de viaje de mi casa.

Con el paso a una sociedad cada vez más necesitada de bienes y servicios, el trueque no podía funcionar debido a estos problemas; obviamente no desapareció de la noche a la mañana, sino que fue sustituido progresivamente por el uso del dinero, lo más probable es que cada pequeña comunidad desarrollara su propio tipo de dinero (cocos, piedras o lo que fuera) hasta que acabó extendiéndose y generalizándose su uso.

Veamos cómo se pudo producir este proceso…

Volvamos a nuestro cazador y sus pieles, resulta que el agricultor no necesita las pieles, pero sí vasijas de barro, y da la casualidad de que el cazador ha encontrado un alfarero que necesita las pieles pero no tiene zanahorias. Una posibilidad es que el alfarero intercambiara con el cazador las pieles por las vasijas y luego este fuera al agricultor e intercambiara las vasijas por las zanahorias, o incluso que agricultor y alfarero hubieran coincidido y hubieran solucionado el intercambio entre ellos solos, para perjuicio del pobre cazador que se queda sin zanahorias.

Pero también pudo suceder, y es aquí donde aparece algo parecido al concepto del dinero, que el cazador y el alfarero llegaran a un acuerdo. Es decir, el cazador no se llevó las vasijas, al fin y a la postre, hemos dicho que uno de los problemas del trueque es precisamente la dificultad en el intercambio de algunos bienes, aparte de que el cazador no estaba interesado en las vasijas más que para realizar un intercambio *a posteriori*. ¿Y si para llevar las vasijas hubiese necesitado un burro? ¿O si en el transporte una se cae y se rompe? En este caso, el alfarero le pudo dar un papel, un trozo de madera o "algo" (y fácilmente transportable) que equivaliese al valor de las pieles por las vasijas y al reconocimiento por parte del alfarero de que ese "algo" valía las vasijas que hubiera negociado con el cazador. Ahora nuestro cazador puede llevar este "algo" al agricultor. El cazador cambia el

"algo" por las zanahorias, y el agricultor puede ir al alfarero, en otro momento, llevar el "algo" e intercambiarlo por las vasijas por el valor previamente acordado.

Parece claro que será este "algo" lo que acabará por convertirse posteriormente en el dinero, pero sigamos viendo la sociedad de entonces y cambiemos "algo", que es un término muy abstracto, y supongamos que se usó un trozo de madera.

Y es que el agricultor pudo volver hasta el alfarero y cambiar su trozo de madera por las vasijas, pero también pudo suceder, que antes de cambiarlo, le surgiera otra necesidad, y se encontrase con otra persona (que también tenía necesidad de vasijas), a la que se lo dio, por lo que es probable que algunos de estos trozos de madera no llegaran nunca a su emisor original, es decir, al alfarero que los emitió, sino que se quedaran circulando en el circuito de intercambios, gracias a que eran demandados por otras personas, debido a su liquidez.

Y en esta situación se mantenían, hasta que llegaban a desaparecer, por regla general por dos motivos: su destrucción o su pérdida de valor.

La destrucción

Puede deberse a muchas causas, el simple paso del tiempo hace que la madera se descomponga, pero también se pudo perder y no encontrarse nunca. Hoy en día es algo común, que cada poco tiempo los billetes cambien y se tengan que imprimir nuevos y retirar los que están deteriorados (para ser sinceros, también porque aparecen nuevos mecanismos para evitar la falsificación, como ha sucedido recientemente con los billetes de 5 y 10 euros).

Incluso Bitcoin no ha sido ajeno a esta situación, como veremos, al principio de ponerse en marcha, algunos de los primeros mineros encargados de producirlos perdían sus billeteras cargadas de Bitcoines por la simple pérdida de su clave privada. Es probable que aquellos gustosos de especular, cuando Bitcoin superó los 1.000 euros al cambio en noviembre de 2013, se tiraran de los pelos.

La pérdida de valor (devaluación)

Se refiere a que el trozo de madera, en donde se dijo que valía por ejemplo 5 vasijas, ya no tenga sentido, porque 5 vasijas es demasiado poco para hacer un intercambio razonable por nada.

Tampoco debemos olvidar, que no solamente en este sistema están operando agricultores, cazadores, o alfareros, también se encuentran en él metidas otras personas dentro de la sociedad, como pudieran ser los reyes o monarcas, los cuales en vez de utilizar un trozo de madera como nota, pudieron usar otros elementos de

mayor valor como metales preciosos, siendo estos, y más concretamente el oro y la plata, por su aceptación universal, los que primeramente fueron utilizados como dinero y se acuñaron como monedas. De este modo, pasaremos de usar la tabla de madera y cuyo valor se expresa en vasijas, a usar monedas que valdrán una cierta cantidad de oro o de plata.

De toda esta historia que acabamos de leer, si nos tuviéramos que quedar con algo en la cabeza, sin lugar a dudas, yo me quedaría con el acuerdo al que llegaron el alfarero y el agricultor para usar el trozo de madera como mecanismo de intercambio, porque ahí reside la clave de lo que es el dinero y si alguien nos preguntase una definición rápida de lo que este es, probablemente una de las mejores que podríamos dar sería esta:

"Cualquier cosa que los miembros de una comunidad están dispuestos a aceptar como pago de bienes o de deudas dentro de una economía".

Y casi sin darnos cuenta hemos llegado a otra palabra clave: **economía**.

Si no hubiera economía no habría necesidad de dinero.

1.1.1 ¿Qué pasa con la economía?

Me imagino que coincidiremos cuando digo que tanto agricultor, como alfarero, como cazador o incluso los monarcas (y tú mismo por supuesto), parten de un hecho común, y es que sus recursos son limitados y que todos ellos tienen necesidades que cubrir y que esas necesidades no pueden ser cubiertas por ellos mismos y necesitan de la relación con otras personas. Ni el cazador tiene todas las pieles que quiere ni produce zanahorias, ni el alfarero todas las vasijas, etc., sin embargo, todos intentan conseguir sus objetivos, ¿cierto?

Pues ni más ni menos que esto es la economía, o mejor dicho, de lo que trata la economía, de entender cómo las personas consiguen obtener el máximo beneficio a partir de sus recursos limitados y por tanto, para conseguirlo, no queda otra que administrar de un modo eficaz y eficiente los bienes de los que disponemos, utilizando para ello y mayormente, el dinero como mecanismo de intercambio. Y esto es independiente de si somos un monarca, un Estado o un simple ciudadano de a pie, la economía nos afecta a todos y cada uno de nosotros.

Es más, cuando digo todos, es **TODOS**, en mayor o menor medida en la sociedad, actuamos como **productores** (¿yo productor?, sí, sí, tú, o qué crees que haces cuando estás trabajando si no es otra cosa que producir) o **consumidores** de bienes y servicios, y en función de nuestras necesidades y de la demanda y oferta de

los bienes disponibles, los precios de los mismos se fijan, dando lugar a la economía de mercado. Los productores y los consumidores, cada uno en su papel, son el motor de la economía, y esta necesita de ambos para funcionar.

Cuando no administramos de una manera eficaz y eficiente nuestros bienes para conseguir lo que queremos, lo único que conseguimos es ir al desastre, por el simple hecho de que no conseguimos maximizar lo que obtenemos a partir de nuestros recursos limitados, y esto es una máxima de la vida que deberían enseñarnos en la escuela. Aunque claro, algunos dirán que siempre podemos endeudarnos y comprar a plazos, pero eso es otra historia de la que ya hablaremos. Simple sentido común.

Ahora bien, el mundo se ha convertido en algo muy complicado, y para poder explicar lo que sucede en la economía, esta se divide en dos partes, la microeconomía y la macroeconomía.

La microeconomía está pensada para estudiar el comportamiento de los individuos, de las familias y de las empresas grandes o pequeñas, su objetivo es tratar de entender por qué producimos o vendemos tal o cual cosa, y por qué gastamos o invertimos de tal o cual manera. En nuestro ejemplo del cazador, sería preguntarnos ¿por qué quiere zanahorias y no lechugas? ¿Compra siempre zanahorias? ¿Qué hace con las zanahorias, se las come o las cambia por otra cosa?

ENTONCES…

Hay quien argumenta que **la economía surge por nuestro deseo de ser felices y conseguir aquello que queremos**. Razón, desde luego, no les falta. ¿Pero qué pasa con la moral? ¿Y si lo que a mí me hace feliz hace desgraciado a otro? ¿No debería la economía estar sustentada en unos valores? ¿Y si son los Estados, los políticos, banqueros y entidades financieras las que no respetan esos valores?

La macroeconomía es más o menos lo mismo, pero el objeto de estudio solo es un poco más grande. En macroeconomía se suma el efecto de todas las actividades económicas de todas las familias, empresas y también del sector público, con el objetivo de ver qué se ha producido o consumido en conjunto, en qué se ha invertido, qué se ha exportado o importado, etc. Como resultado, nos devuelve un indicador llamado **Producto Interior Bruto (o PIB)** que nos ayuda a saber cómo vamos de riqueza a nivel nacional y a establecer comparaciones con el resto de países, y como además se mira también cómo afecta la inflación, los tipos de interés y el desempleo, tenemos un termómetro bastante bueno.

ENTONCES…

Andreas Antonopoulus, una de las personas que más saben de Bitcoin en el mundo, y que te recomiendo desde ya que sigas, habla de como la llegada de las criptomonedas traerá consigo dos nuevas ciencias: la **macroeconomía computacional** y la **microeconomía computacional**, ambas se basarán en el estudio de los datos almacenados en la cadena de bloques para explicar los hechos económicos de la sociedad futura.

Pero darme un par de páginas, que cuento algunas cosas adicionales y luego volvemos sobre el PIB y las implicaciones que una moneda como Bitcoin puede tener con él.

1.1.2 La aparición de la moneda

¡Vale!, nos ha quedado claro qué es eso de la economía y como es algo que va de la mano de la misma sociedad y que si no estuviéramos en un mundo limitado y con necesidades que satisfacer, para poco nos serviría el dinero. Como el trueque no es, como ya hemos visto, un elemento que permita dinamizarla y hacerla más ágil, es necesario algo que facilite la realización de los intercambios, y es aquí donde vamos a detenernos ahora un poquito para ver cómo aparecieron las monedas y las ventajas que trajeron consigo.

La aparición de las monedas supuso un paso adelante en la utilización del dinero por parte de la sociedad; tenían unas ventajas intrínsecas como eran la facilidad de transporte o su durabilidad. Las monedas se creaban a partir de un metal base (como el cobre, no se solía utilizar el hierro porque a pesar de su dureza tiene el problema de que se oxida) al que se le añadía cierta cantidad de oro o plata, aunque también era común encontrarse con monedas hechas únicamente de uno de estos dos materiales.

Para garantizar que una moneda contenía cierta cantidad de metal precioso, apareció la acuñación, algo así como una garantía o certificación, realizada por una entidad reconocida y respetada (como podía ser un reino) que avalaba el peso y calidad de los metales que las monedas contenían.

Esta acuñación consistía en poner un distintivo o una señal sobre la moneda (por ejemplo hacer un agujero de un determinado tamaño en su superficie o poner una imagen de un animal o del monarca), que era fácilmente reconocible por todo el mundo, no olvidemos además que estamos en sociedades en donde el grado de

analfabetismo era muy grande, era necesario que el dinero fuera suficientemente reconocible y fácil de entender por todos para generalizar su uso.

ENTONCES…

¿El mundo al revés? Paradójicamente, la historia se repite y la mayor parte de **la población mundial es analfabeta referente al dinero y a cuestiones económicas**. Si antiguamente eran los propios monarcas los interesados en que su utilización fuera comprendida y aceptada, ahora parece que aquellos que deberían velar por su buen funcionamiento, lo manejan en una nebulosa oscura en donde no queda muy claro qué es lo que sucede en su interior.

En algunas monedas griegas se veían espigas de trigo o las cabezas de sus dioses, y las monedas romanas más antiguas llevaban estampados dibujos de cabezas de ganado, aunque luego se utilizaron los bustos de sus césares.

Tampoco debemos olvidar que ya entonces aparecería un problema que dura hasta nuestros días, la **falsificación**. En el mundo de Bitcoin, veremos que este problema recibe el nombre de doble gasto, y como mediante una cosa que llamaremos **prueba de trabajo** conseguiremos que no pueda darse o que en caso de que alguien pueda plantearse hacerlo, no le resulte rentable llevarlo a cabo (ni tan siquiera si es un gobierno el que lo intentase hacer, y el porqué de meter a los gobiernos en esta saca de falsificadores lo entenderemos cuando hablemos de la Operación Bernhard al final).

Las primeras monedas que se conocen se acuñaron en **Lidea** (Turquía) en el siglo VII a. C., siendo los primeros que introdujeron las monedas de oro y plata y las primeras tiendas de cambio (¿a qué os recuerda esto?). Utilizaban para hacerlas una aleación de oro y plata, que se conoce con el nombre de **electro**, y creaban a base de ella una moneda que se conocía con el nombre de **estatero**, y para garantizar su autenticidad se estampaba en cada una de ellas la cabeza de un león, proceso que hacía que la moneda quedara aplanada y le daba una forma característica y única.

Durante el reinado de **Creso** (595 a. C.), rey al que se le atribuye el origen de la acuñación, se crearon nuevas monedas de puro oro o de pura plata, que se utilizaron como medio estandarizado de intercambio.

A esto se llama **dinero material**, donde el valor de la moneda es equivalente al valor de su materia (de lo que está hecho), o dicho de otro modo su valor intrínseco era igual al valor nominal como veremos más adelante, de momento nos basta con esto. Y si Bitcoin está hecho de bits (0 y 1), ¿cómo se aplica esto? Luego lo vemos.

Otras monedas primitivas famosas han sido la moneda de China, el **denario** romano y la **lechuza** griega. Es a partir de una derivación de la palabra denario de la que surge la palabra dinero.

1.1.3 La aparición del papel moneda

El origen del papel moneda lo tenemos que buscar en la civilización china, durante la **dinastía Tang** en el año 845 a. C. El uso de la moneda implicaba llevar consigo algo pesado, por lo que se decidió crear algo más liviano y manejable, aunque estuviese construido en un material que tuviera menos valor (menor valor intrínseco) como es el caso del papel, pero que por decreto gubernamental valía una cantidad específica de oro o plata. Los encargados de emitir este papel moneda eran los bancos privados por orden de los monarcas.

En Europa el uso del papel moneda no se extendió hasta el año 1250 por Jaime de Aragón. Pero el valor que poseía dependía de los depósitos de oro que poseyera el país. Fue en Suecia en 1661 cuando se imprimen los primeros billetes de banco, y en España es el **Banco de San Carlos**, el antecedente al Banco de España, el que en 1783 realiza la primera emisión.

A finales del siglo XVIII se produce el reemplazo de los bancos privados como emisores de papel moneda por los bancos centrales, y es en el siglo XIX cuando se establece un patrón internacional del valor del oro y del valor del dinero en papel a paridad, **el patrón oro** que contaremos luego.

Con esto acabamos nuestra pequeña historia sobre el origen del dinero, seguro que algún que otro detalle habré pasado por alto, pero más o menos las cosas sucedieron como os he contado.

1.2 ALGUNOS CONCEPTOS BÁSICOS

Ya sabemos cuál es el origen del dinero, y cómo su invención ayudó a crear una sociedad más dinámica y con relaciones más ricas y complejas y a tejer un universo en donde existen relaciones económicas que deben satisfacerse. Veamos a continuación unos conceptos que van a acompañarnos en el resto del libro y que en muchas ocasiones se utilizan como arma para atacar a Bitcoin y proclamar su fracaso. Cuando esto sucede, he explicado la manera en la cual dichas predicciones catastrofistas se equivocan argumentando el porqué de ello.

1.2.1 Una reflexión: la utilidad marginal decreciente

Paremos a refrescarnos y mientras bebemos un sorbito de agua (solo agua, el whisky aún no), veamos si somos capaces de responder a esta simple pregunta: ¿por qué consideramos algo como valioso o por qué no lo consideramos como tal?, o ¿por qué deberíamos considerar a Bitcoin como algo valioso? Esta es una pregunta que yo muchas veces me he hecho personalmente, y siempre que alguien me dice que tal o cual cosa vale mucho, me paro y lo miro bajo la perspectiva siguiente para ver si lleva o no razón (y os recomiendo que vosotros también lo hagáis). Pero vayamos al meollo del asunto…

Para que un bien sea económicamente valioso, se tienen que dar dos coincidencias simultáneas en el tiempo: utilidad y escasez. El motivo por el cual el oro tiene valor para nosotros es precisamente por esos dos motivos, es útil y es escaso.

Con la escasez no creo que haya muchas dudas, se refiere a que hay poco de algo, el oro es valioso porque en la naturaleza no lo encontramos por todas partes. La utilidad puede presentarnos alguna duda más, pero es también fácil de entender, ya que es una medida del grado de felicidad o de satisfacción que obtengo cuando consigo una determinada cosa, por ejemplo, para mí las palmeras de chocolate que me como los viernes (y tienen que ser los viernes porque es cuando la experiencia me dice que el hojaldre está mejor) en la cafetería de mi trabajo tienen una gran utilidad porque me aportan un nivel de felicidad difícil de explicar, y como me como una por semana pues tampoco me preocupo demasiado del colesterol.

Cuando se habla de **utilidad marginal**, tiene que ver con la apreciación o importancia que le damos a un bien cuando lo incrementamos. Por ejemplo, si tengo un reloj será genial, pero probablemente cuando tenga cincuenta relojes, a tener un reloj más no le daré mucha importancia, es decir, su utilidad marginal decrecerá. Y lo mismo se aplica a mis palmeras de chocolate, comerme una es genial, dos probablemente también, pero a partir de ahí, es seguro que no me sentiré demasiado feliz y acabaré con una indigestión casi con toda seguridad (y del colesterol mejor no hablar).

Gráficamente esto se ve muy bien con el siguiente dibujo, que muestra como decrece la utilidad marginal a medida que aumentamos la cantidad de un determinado bien (eje X de la gráfica).

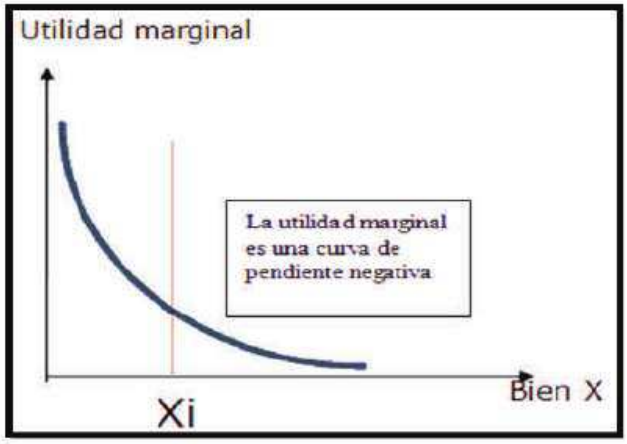


Figura 1.1. Utilidad marginal decreciente

Volviendo al caso del oro (aunque puede aplicarse a todos los metales preciosos), este es considerado el bien cuya utilidad marginal disminuye más lentamente, cada unidad adicional de oro tendrá casi tanta utilidad para quien lo posea y será valorado tanto como la unidad anterior. ¿Te ha quedado claro? Muy bien, pues echa un vistazo al siguiente cuadro, y empieza a reflexionar:

ENTONCES…

La reflexión tenemos que hacerla en el contexto siguiente: si el oro tiene una utilidad marginal decreciente muy baja, y hemos dicho que esto es fundamental para determinar su uso como moneda y dar valor a las cosas, ¿qué pasa con Bitcoin? ¿Es mejor como moneda?

El oro se deteriora muy poco, pero lo hace, no deja de ser algo físico; Bitcoin no se deteriora, son bits de información. Aumentar la cantidad de oro aumenta el espacio y las medidas de seguridad, Bitcoin no necesita espacio adicional a mayor número de Bitcoines, y la seguridad la garantiza la criptografía. Por eso se dice que **la utilidad marginal de Bitcoin es constante**, no cambia nunca, en detrimento de la del oro que es decreciente.

1.2.2 Sigamos reflexionando: ley de los rendimientos decrecientes

Supongamos ahora que somos el alfarero, y como tal nuestro trabajo consiste en producir vasijas que ponemos a disposición de quien las quiera comprar. Ahora bien, para hacer una vasija necesitaremos un poco de barro, un torno de alfarero,

leña, un horno de ladrillo (a poder ser refractario), agua y seguro que alguna que otra cosa más.

Pues todas estas cosas que se utilizan para fabricar otras cosas son lo que se denomina **capital**, es decir, si nuestro buen vendedor tuviera que llevar las vasijas a un mercado y usara un burro para ello, el burro también sería capital, o sea que no solo el capital es dinero, es más, el conocimiento o las habilidades que tiene el vendedor de vasijas para hacerlas también es capital, en este caso **capital humano** (ahora muy de moda).

Sigamos suponiendo y en un ataque de producción frenética, resulta que nuestro alfarero pone todo ese capital en marcha, y se pone a fabricar vasijas o botijos las 24 horas del día, ¿qué sucedería? Pues además de acabar con un buen dolor de espalda, sucedería que acabaría saturando el mercado, y haciendo que el coste de producirlos sea mayor que el beneficio que obtuviera por ello, porque a la larga acabará teniendo que bajar el precio si es que quiere venderlos.

Pero no solo esto, hemos dicho que partimos de una situación en donde existen recursos limitados, ni el alfarero puede trabajar las 24 horas al día, ni tenemos todo el barro, agua y hornos para mantener una producción constante e indefinida en el tiempo; puedo partir de unas reservas que tengo en el almacén, por ejemplo de barro y agua, pero cuando estas se acaben tendré que ir a buscar más, y puede darse el caso de que si agoto (la Tierra es limitada, no lo olvidemos) el pozo de donde saco el agua, tenga que ir a buscar más, más lejos, y por tanto tenga más coste, y lo mismo se aplica al resto de elementos del capital. Esto es ni más ni menos que la ley o principio del rendimiento decreciente, que relaciona el beneficio que obtengo de algo y el coste que me lleva el producirlo, y viene a decir esto que acabo de explicar, que cuanto más produzco de un bien menos beneficio obtengo por ello o más cuesta producirlo.

Y esta cosa tan simple es la que determina qué se produce o qué no se produce en el mundo, intentando diversificar la producción de los bienes y servicios a fin de obtener el máximo beneficio de nuestros recursos limitados. Quién decide qué y cuándo es una mezcla de lo que el mercado demanda y de lo que los gobiernos determinan, y aquí es donde encontramos pensamientos divergentes, unos dicen que el gobierno tiene que intervenir (porque quién mejor que los políticos para decidir qué nos conviene), otros argumentan que es mejor que el mercado se regule solo por la ley de la oferta y la demanda y el ajuste natural de los precios. La realidad es que tenemos actualmente una mezcla de ambas cosas, un **modelo mixto** (keynesiano dirán algunos), pero también un buen follón montado.

Igual que hicimos en el punto anterior, echa un vistazo al cuadro siguiente y piensa un poco en esto que te digo y trata de sacar tus propias conclusiones, después continúa leyendo.

ENTONCES…

Reflexionemos pues: ¿no es lo que hacemos al producir dinero sin control? Hacer que el coste de producirlo supere con creces las ventajas de ponerlo en marcha. Ya veremos que en el futuro (en torno al año 2030) **habrá cómo máximo 21 millones de Bitcoines**, ya que la masa monetaria de Bitcoines crece siguiendo una progresión geométrica cada 4 años. Cuando hablemos de inflación y de la creación del dinero como deuda, quedará claro el significado que quiero darle a esto.

El último Satoshi, nombre que se da a la fracción más pequeña de Bitcoin y que como se divide hasta el octavo decimal equivale a 0,00000001 Bitcoines, se generará en el año **2140**, y el poder de cómputo necesario para hacerlo será increíblemente alto.

No obstante, hasta que se llegue a ese valor, quedan muchos hitos importantes que conseguir.

1.2.3 Dinero de curso legal

Ha pasado un tiempo razonable desde el inicio de nuestra historia del cazador hasta nuestros días, y el dinero se encuentra formando parte de nuestra vida cotidiana, sin embargo, ¿por qué en España tenemos euros en vez de dólares en la cartera?

Esto se debe a lo que se **denomina como moneda o dinero de curso legal o moneda corriente**, y no es ni más ni menos que la forma de pago, definida por la ley de un Estado, que se ha declarado aceptable (recordáis cuando al principio dimos una definición de lo que era el dinero) como medio de cambio y forma legal de cancelar las deudas (¡vaya! La palabra deuda otra vez por aquí (van tres en menos de cinco páginas), anda que si al final va a resultar que todo esto tiene que ver con que estemos endeudados para que funcione la cosa…). O sea, el dinero de curso legal es el que puedo utilizar para comprar o vender cosas en un determinado país.

Hay algunos casos en donde podemos encontrarnos con más de una moneda de curso legal, como en El Salvador donde se usan tanto el dólar como la moneda nacional, o suceder como en el caso de Europa, en donde un grupo de países han acordado utilizar una moneda común como el euro. Si la ley obliga a utilizar una sola moneda de curso legal como única forma de pago aceptable en un país, imponiendo un **monopolio monetario** (y todos sabemos lo buenos que resultan los monopolios

para los usuarios de los servicios que producen), se dice que tenemos una moneda de curso forzoso.

Hay una frase muy buena del **profesor Larry Parks**, y que os podéis encontrar a poco que busquéis por Google sobre las monedas de curso forzoso; la frase dice lo siguiente:

"Si el dinero es bueno y la gente lo acepta voluntariamente, ¿qué necesidad hay de leyes de curso forzoso? Si el dinero no es bueno, ¿cómo se puede en una democracia obligar al pueblo a utilizarlo?".

Esta frase tiene mucho sentido y enlaza con lo que os decía en la introducción del libro, estamos acostumbrados a que mejoren los coches, la ropa, las casas o la comida, pero no nos preocupamos por que la moneda con la que obtenemos todas estas cosas también mejore y sea la mejor posible. Aquí está parte de la gracia de Bitcoin, en que podemos utilizarla de manera voluntaria, ningún Estado, ni ningún político nos tiene que decir si podemos o no hacerlo, es nuestra voluntad la que lo determina. Yo puedo poner a la venta este libro y puedo elegir cobrarlo en Bitcoines (no es el caso, pero de ejemplo me sirve), y tú puedes elegir pagarlo como tal, solo es tuya la elección de hacerlo, y sin necesidad de que nadie medie en el proceso y nos dé su bendición y a cambio se lleve su parte.

Pero es que aún hay más, supongamos que hacemos el siguiente experimento y Bitcoin fuera aceptado como moneda de curso legal y conviviera con el dólar, el euro, y el resto de monedas mundiales, de manera que pudiéramos comprar o vender sin problemas, ¿qué sucedería en esta situación? Bueno pues hay quien dice que entraría en juego algo que se conoce como **las propiedades del buen dinero y el principio de Gresham**.

1.2.4 Las cualidades del buen dinero

Cuando se habla del buen dinero, a lo que nos estamos refiriendo es a las propiedades que tiene que tener una moneda para cumplir en su misión como medio de intercambio de bienes y servicios. La definición más acertada sobre las propiedades que debe tener el buen dinero se atribuye a Aristóteles. Aunque se han venido redefiniendo a lo largo del tiempo, se pueden resumir en las siguientes:

- **Depósito de valor**: atesora valor con el paso del tiempo.
- **Unidad de cuenta**: debe permitir fijar el precio de los bienes y servicios.
- **Medio de cambio**: obtención de bienes y servicios por él.

- **Invariancia física**: las propiedades físicas no cambian a lo largo del tiempo.
- **Homogeneidad**: todas las unidades deben ser idénticas entre sí.
- **Bajo ratio flow/stock**: el *flow* se refiere a la cantidad de dinero producido en un período de tiempo y el *stock* al dinero producido en toda la historia del mismo, si este cociente es muy grande se produce inflación y si es muy bajo deflación.
- **Empleabilidad**: su formato debe ser práctico. Por ejemplo las piedras ray que podían pesar varias toneladas no parecen ideales para llevarlas en el bolsillo.
- **Accesibilidad**: un gran número de personas deben ser capaces de utilizarlo.

La pregunta lógica que tal vez nos podamos hacer ahora que ya conocemos estas simples propiedades es recurrente a lo largo de este libro: ¿el dinero que usamos actualmente en nuestro día a día las cumple?

Hay a quien no le gusta Bitcoin porque dice que es algo virtual y que realmente no existe (¡como si el resto existiera!), pero pensemos en la inflación, ¿no parece lógico pensar que si yo no sé cuánto voy a poder comprar con una cantidad de euros (pongamos 100 o 1.000 euros) al año que viene, no es un depósito de valor demasiado confiable? ¿No se está convirtiendo el dinero de curso legal simplemente en un medio de intercambio y porque nos obligan a ello?

Durante muchos años todas estas propiedades han sido las que han hecho del oro el mejor mecanismo disponible para el intercambio de bienes y servicios, aunque ¿nos dejaría Hacienda ir a pagar los impuestos con unas cuantas onzas de oro? En cualquier caso, el oro tiene más que superado el **teorema de regresión monetaria de Mises**. ¿Qué? ¿Que nunca has oído hablar de este teorema?, no te preocupes, voy a explicártelo porque aquí hay algo muy importante que debes conocer, más que nada porque es otra de las armas que se usa contra Bitcoin.

Respóndeme a la siguiente pregunta: ¿para qué se usa el oro? (venga, piensa que seguro que se te ocurre algo…), algunos ejemplos muy clásicos serían los siguientes:

- Joyería.
- Medicina (implantes bucales y similares).

- Mobiliario (vajillas, cuberterías, muebles, etc.).
- Relojería.
- Electrónica.
- Automoción (airbags de los coches, etc.).
- Aeroespacial (cristales de las cabinas de los aviones, naves espaciales, satélites).
- …

Es decir, el oro tiene una gran cantidad de usos que van mucho más lejos del meramente monetario simplemente porque tiene unas propiedades físico-químicas que lo hacen muy versátil y sería útil aunque monetariamente no lo fuera, por tanto, como bien útil, se puede establecer un valor para el oro por poder desempeñar todas estas funciones. Algo parecido sucede si en vez del oro cogemos otras monedas que se han usado a lo largo de la historia, como la sal (sirve para conservar los alimentos) o el ganado (nos lo podemos comer), etc.

Vamos ahora con el teorema…

El teorema de Mises se debe a **Ludwing von Mises** (1881-1973) y dice algo tan simple como que para que un bien empiece a usarse como medio de intercambio, es necesario que tenga una demanda no monetaria previa que sirva para fijar el precio inicial desde el que arrancar, como le pasa al oro.

Mucha gente pensaba que Bitcoin no podría echar a andar nunca, precisamente porque no había forma de cumplir con el teorema, sin embargo, una vez más, para todos aquellos incrédulos que no lo veían posible, la realidad es que Bitcoin se está usando en todo el mundo. Dado que muchos no se quedan convencidos con la testaruda realidad, siguen argumentando que Bitcoin nunca podrá ser como el oro, se basan en la imposibilidad de encontrarle usos que no sean monetarios, y sostienen que fuera del sistema de intercambios no sirve para nada.

Dicho de otro modo, si tenemos oro y el sistema monetario se fuera al garete, aún tengo algo que sirve para algo (valga la redundancia), tengo ciertas garantías de valor, sin embargo esto no sucede con Bitcoin. Pero nuevamente se equivocan y tienen poca visión de futuro, es cierto que hoy Bitcoin solo tiene valor monetario, pero olvidan que hay muchos grupos de trabajo creando capas adicionales por encima de Bitcoin, y os adelanto algunas palabras que os contaré como Bitcoin 2.0 y 3.0, aplicaciones nativas, contratos y metacoins, es decir, veremos el poder de la cadena de bloques para crear algo más que dinero.

Pero si aun así no se quedan satisfechos, investigando por Internet es fácil que lleguéis a dos tipos: **Nikolay Gertchev** y **Peter Surda**, que explican este

comportamiento tan particular diciendo que Bitcoin, en sus inicios, no tenía una demanda monetaria inicial, y que su valor estaba en servir a sus usuarios como medio de manifestación ante un sistema injusto (el bloque génesis de Bitcoin hace referencia a esto), por tanto su valor no monetario original estaría ahí, cierto que no es un valor que sirva para decorar la vajilla de palacio, o que nos podamos comer, o que sirva para conservar los alimentos, pero nadie puede negar que sea un valor de peso.

Supongo que aun así seguirán sin estar convencidos, qué le vamos a hacer…

Y es que llegados a este punto muchos pensarán que Bitcoin y el oro tienen grandes parecidos, lo que es una gran verdad, aunque **Bitcoin es mejor que el oro**, no solo porque tenga una utilidad marginal constante, como ya comentamos, sino porque las funciones de servir como medio de pago, unidad de cuenta o reserva de valor las desarrolla de un modo más eficiente que este.

Cuando hablamos de **medio de pago** nos referimos a las posibilidades para usarlo para pagar con él, tanto sus posibilidades de homogeneidad, como de transporte o su divisibilidad no se ven afectadas como lo pueden ser las del oro. ¿Hay algo más homogéneo que los bits de información que en última instancia es Bitcoin? ¿Que se transporte de un modo más sencillo que por las actuales redes de ordenadores? ¿Y que se pueda dividir hasta el octavo decimal (incluso se podría modificar el protocolo para que fuera divisible aún más) sin mayores problemas? Si pensamos en el oro, mover grandes cantidades requiere una logística importante, por no hablar de las medidas de seguridad previas que hay que movilizar, y su divisibilidad está limitada por la física.

¿Y de la **unidad de cuenta** qué podemos decir? Es cierto que la actual volatilidad de Bitcoin supone un problema para expresar precios, pero soluciones como las proporcionadas por OKPay son un modo de mitigarlo mientras el proceso de capitalización de Bitcoin acaba por consolidarse. Desde mi punto de vista, esta volatilidad de Bitcoin es solo un problema pasajero y con caducidad en el tiempo. De no serlo, ¿tendría sentido que empresas como Destinia, Expedia, Dell, Showroomprive… por citar empresas que no son precisamente pequeñas, permitan que sus productos puedan pagarse usando Bitcoines? ¿Se han vuelto locas? ¿O no será que las potenciales ventajas de Bitcoin superan con creces sus actuales desventajas y limitaciones?

ENTONCES…

¿Sabías que incluso hay quien ha llegado a utilizar la cadena de bloques de Bitcoin para dejar constancia de su matrimonio? Pues esto mismo es lo que ha hecho la pareja **David Mondrus y Joyce Bayo**, quienes consideran que la tecnología de la cadena de bloques es para siempre, al igual que su amor (y que luego digan que no hay sentimiento en la tecnología).

Cada vez más y más productos expresan su valor en Bitcoines, recientemente hasta Virgin y sus viajes espaciales se pueden adquirir con esta moneda, y es que da igual lo que busques, lo vas a encontrar expresado en Bitcoines y si no preguntárselo a Austin Craig y a Beccy Bingham, esta pareja estadounidense ha recorrido el mundo y solo han utilizado Bitcoines en sus compras. ¿Alguien puede refutar este hecho? Desde CoinDesk se estima que alrededor del mundo hay unos 60.000 comercios que lo aceptan ya y esta cifra no para de subir cada día y prevé un aumento sin precedentes en los próximos años.

De verdad, ¿están todos equivocados y apostando por algo que no tiene para nada futuro?

Si nos fijamos en la **reserva de valor**, las propiedades que se piden a un bien para que actúe de este modo, ¿no las cumple Bitcoin? Dificultad de falsificación, la tiene y garantizada por la criptografía y el trabajo de los mineros, escasez, máximo 21 millones (y esto comparado con el oro es interesante, porque una vez se mine el último Bitcoin, no se generarán más, sin embargo nadie nos dice que no se puedan encontrar nuevos yacimientos de oro en la Tierra, o quién sabe, tal vez en un futuro no muy lejano en la Luna o en Marte), y durabilidad, salvo que apaguemos Internet y todo el mundo le dé la espalda, no parece que Bitcoin no haya venido para quedarse.

El punto más complicado de las anteriores cualidades (para mí incluso mayor que la volatilidad) está en la **accesibilidad**; aunque el número de usuarios crece día a día, aún es necesario mucho esfuerzo y tiempo para que el grueso de la población mundial sea capaz de entenderlo y usarlo con la misma facilidad que el dólar o el euro, y es que aún hoy se requieren ciertos conocimientos técnicos, que aunque se han simplificado enormemente, pueden suponer una barrera de entrada, un motivo más para no dejar de leer el resto del libro.

1.2.5 El principio de Gresham

Y qué mejor que continuar con otro de los muchos ataques que se hacen a Bitcoin. Le toca el turno al **principio de Gresham**.

El principio de Gresham se debe a un comerciante y financiero inglés del siglo XVI, cuyo nombre completo era **(Sir) Thomas Gresham**. Como comerciante y financiero que era, se fijó en una cosa curiosa, que si en un determinado país existían dos monedas de curso legal, y una era percibida por el pueblo como "buena" y la otra era percibida como "mala", la gente prefería pagar con la moneda considerada como mala, para deshacerse de ella, y guardar la buena. Según este principio y en esta situación, ¿qué moneda consideras como buena y cuál como mala?

Hay quien dice que el principio de Gresham es el motivo principal por el que Bitcoin jamás podrá tener éxito (otro más), por la sencilla razón de que quien tiene Bitcoines, los atesorará esperando a que la moneda siga revalorizándose y utilizará el dinero "malo" para pagar en su operativa normal, y es más, lo avalan con el hecho de que la mayor parte de los Bitcoines que se han generado, en la actualidad no han sido utilizados nunca en una transacción económica y que a la larga, la moneda considerada como buena, por el hecho de ser guardada, acabará por desaparecer de circulación.

Es decir, paradójicamente el dinero malo acaba por sustituir al dinero bueno o como dicen los ingleses "bad money drives out good".

Este argumento no deja de ser cierto dentro del contexto en el que se definió la ley de Gresham, sin embargo se olvida de los detalles particulares que afectan a Bitcoin por los que la ley de Gresham no tendría aplicabilidad sobre él:

- El primero, en cuanto al volumen de Bitcoines utilizado, no debemos olvidar que Bitcoin lleva en funcionamiento desde 2010 y que solamente en el último año y medio parece haber generado la suficiente expectación y conocimiento como para que la gente se vaya acercando a interesarse por su funcionamiento y posibilidades, por lo tanto, creo que aún es pronto para usar el volumen de transacciones que usan Bitcoines como argumento. Aunque dicho volumen no para de crecer, para hacer honor a la verdad.

- Quien usa el principio de Gresham contra Bitcoin se olvida de que Gresham hablaba de monedas físicas, y compuestas de un determinado material, que era devaluado por la ley; en esta situación, la percepción de bueno o malo sí tendría sentido porque era el Estado con su intervención quien influía en la percepción. Sin embargo, Bitcoin no es una moneda cuyo

valor lo fije un Estado o un banco central, por lo tanto la percepción de lo buena o mala que es no está controlada por nada ni nadie en particular. Si la gente actualmente atesora Bitcoines es simple y llanamente porque estamos en el **proceso de capitalización de la moneda**, situación que se estabilizará a futuro.

- Y una vez estabilizada, ¿qué sucederá? La gente no atesora el dinero para no usarlo nunca (tal vez el tío Gilito o el señor Cangrejo de Bob Esponja, pero para el común de los mortales no es lo habitual), y que algo sea mejor mañana no significa que espere hasta mañana para comprarlo si tengo la necesidad hoy; dicho de otro modo, el gasto de Bitcoines se producirá en cuanto las cosas que podamos adquirir con ellos representen un valor mayor que el hecho de guardar el dinero de manera indefinida. Esto mismo pasa con prácticamente cualquier cosa que podamos comprar, por ejemplo un coche o un ordenador, somos conscientes de que el ordenador o el coche que me compre hoy quedará obsoleto en dos o tres años (el ordenador incluso antes), sin embargo no espero ese tiempo si tengo la necesidad de comprarlo y esa compra me satisface una necesidad real hoy.

1.2.6 El proceso de capitalización

Vamos a ver si soy capaz de explicar esto de los procesos de capitalización sin meterme en demasiados jardines, porque es precisamente en el momento en el que Bitcoin se encuentra y entenderlo ayuda a clarificar mucho las cosas.

Los procesos de capitalización tienen que entenderse siempre en el contexto de cambio, en la manera de hacer las cosas de un modo para pasar a hacerlas de otro diferente porque con el cambio obtendremos una mejora significativa y un beneficio mayor. Sin embargo, el proceso de cambio no es gratis, implica siempre un costo porque significa que renunciaré a la inversión que hice en algún determinado momento para obtener lo que actualmente quiero cambiar.

Esto se ve muy bien con el clásico ejemplo de sustituir personas por máquinas, adquirir las máquinas tiene un costo, pero con el cambio espero que mi empresa sea más productiva al sustituir la mano de obra humana y podré vender más barato. Pero al hacerlo, puede que tenga que sacrificar la inversión en formación que he venido realizando en los trabajadores que van a ser sustituidos. Gano por un lado, pierdo por otro, lo que importa es que el resultado de la balanza sea positivo.

Por tanto, cuando entramos en un proceso de este tipo, lo voy a hacer porque espero que a la larga la jugada resulte ganadora, por simple sentido común,

nadie juega pensando en perder, aunque el riesgo de perder, inherente a cualquier actividad humana, exista, siempre intentaré escoger la opción que me reporte el **mayor beneficio con el menor coste** (la idea básica que hay detrás de la economía que ya hemos explicado).

Hay quien dice que es mejor no cambiar, pero no cambiar también tiene un coste, mantener las cosas inalterables supone perder oportunidades, si las cosas se mantienen siempre igual, no puede haber progreso y si no hay progreso, antes o después lo que nos espera es pobreza. Es decir, el cambio produce movimiento, el movimiento produce avance (progreso) y el progreso nos acerca a nuestros objetivos de maximizar el beneficio.

Los procesos de capitalización suelen ser lentos, y dependen tanto del ahorro como de las inversiones que se realicen para adquirir el nuevo capital. Y precisamente esto mismo es lo que está sucediendo con Bitcoin, está en proceso de capitalización, de adquirir la fortaleza necesaria para ser el elemento que nos permita pasar de un dinero malo y de curso obligado por los Estados a otro dinero bueno y de uso voluntario por las personas.

¿Podemos permitirnos no cambiar? Si no queremos acabar en la pobreza, indudablemente no podemos seguir como vamos.

1.2.7 Por qué nos debe importar el PIB al hablar de Bitcoin

Ya sabemos que en economía, lo que mide la riqueza de un país es el Producto Interior Bruto, en donde desde un punto de vista muy simplón, lo que se hace no es más que una simple resta entre los ingresos y los gastos del país y se determina si tenemos **déficit** (saco más que meto) o **superávit** (meto más que saco).

¿Por qué nos importa el valor del PIB?, pues muy sencillo, porque en función de cómo esté este valor, las políticas monetarias van a ir en un sentido u otro, por eso hay que vigilarlo siempre, y es más si alguno está conectado a plataformas de *trading*, veréis que este indicador siempre tiene un peso muy importante y hace que el valor de los divisas respecto a sus pares varíen notablemente en función de la información publicada.

Si tengo un PIB alto significa que hay mucho dinero en ese país en movimiento, y un PIB bajo significa que hay poco dinero y que se producen pocas transacciones económicas. El PIB interesa mucho a los gobiernos y a los políticos, porque lo contabilizan siempre sumando los ingresos que se producen, y es por eso que siempre les interesa saber todo lo que una persona gana, de este modo pueden poner los impuestos correspondientes, algo que pueden hacer sin mayores

problemas, puesto que estamos en todo momento identificados, y ¡ay de ti!, si en la próxima declaración de la renta se te ocurre ocultar algo. Tanto tu **salario**, como las **rentas** que percibes por tus propiedades (y de las que también pagas impuestos), los **intereses** que percibes por tus ahorros o por tus inversiones o los **beneficios** que obtienes por arriesgar tu dinero (y que has obtenido por el rendimiento de tu trabajo o porque has invertido con buen tino), todo, todo, todo está gravado por impuestos.

Y aquí tenemos uno de los motivos por los que se tiende a generar dinero y crear inflación, cuando los Estados no tienen suficiente dinero para financiarse a través de los impuestos, se saca dinero de la chistera y se paga con él las obligaciones que como Estados tienen: sanidad, defensa, educación, infraestructuras, etc.

Las alarmas de que algo no va bien se producen cuando tenemos dos lecturas seguidas (lo que se traduce en dos trimestres seguidos) en donde el PIB disminuye, por lo que el Estado pone en marcha **su política fiscal** (que es la que actúa sobre los impuestos) y **su política monetaria**, que afecta sobre todo a los tipos de interés y por tanto al valor de la moneda.

Ahora bien, ¿qué sucedería si estamos en un panorama en donde nuestro anonimato está garantizado en cada transacción económica que realicemos y en el que el Estado no puede interferir? ¿Qué pasaría con el PIB de ese país si fuera la manera generalizada de hacer negocios? ¿A la postre no tratarían los Estados de ir en contra de ese medio de libertad o intentarían criminalizarlo comparándolo con la economía sumergida? ¿Y si resulta que son los ciudadanos los que deciden en qué infraestructuras invertir y deciden que un aeropuerto en Ciudad Real no es necesario, ni líneas de alta velocidad a troche y moche, que el dinero para defensa se puede destinar a investigar o que se puede prescindir de tantos políticos y ejércitos de asesores que los acompañan y el Estado puede quedar reducido a su mínima expresión o desaparecer? Aunque cuando nos centremos en el capítulo dedicado a Bitcoin propiamente dicho veremos qué hay de cierto en el mantenimiento del anonimato (y tal vez sería más adecuado hablar de pseudonimidad), pero suponiendo por ahora que se produjese sin cortapisas, personalmente no soy capaz de imaginarme una sociedad así, ni cómo podría llegar a funcionar, de verdad que me cuesta verlo; aunque intuyo sus beneficios y posibilidades, tampoco estoy haciendo un llamamiento al anarquismo (tal vez al **criptoanarquismo**), pero estoy convencido de que en algún momento tomaremos la pastilla azul (¿es Bitcoin la pastilla azul?), y al igual que hizo Neo en *Matrix*, despertaremos y nos daremos cuenta de hasta qué punto estamos siendo engañados y estafados de manera sistemática.

Sigamos viendo más cosas y volvamos sobre estas reflexiones a medida que avancemos…

1.2.8 Activo y masa monetaria: de M0 a M4

Hasta ahora, hemos estado hablando siempre de bienes y servicios como los elementos que las personas demandan u ofrecen, sin embargo, la palabra que suele utilizarse en el mundo económico para ello es la de activo.

Un activo es por tanto, un bien o servicio, con capacidad funcional y operativa que se mantiene durante el desarrollo de una actividad socioeconómica específica. Los economistas dividen los activos en diferentes tipos según sus características y propiedades, y podéis encontraros con nombres como activo circulante, financiero, intangible, no corriente… pero para el caso es exactamente lo mismo, un bien o un servicio, y dado que para nuestro estudio no es necesario definir mucho más de esto, no entraré en esos berenjenales.

Otra cosa que para nosotros resulta más importante es que relacionado con el concepto de activo, podéis encontraros con el término masa monetaria, que se correspondería con la cantidad de dinero que hay disponible en una economía para poder comprar bienes o servicios, en definitiva, para comprar activos (gastando o invirtiendo). El control de la masa monetaria por parte de los bancos centrales incide tanto en la actividad económica como en la inflación.

Para medir la masa monetaria, se utilizan una serie de medidas que se denominan M0, M1, M2, M3 y M4, siendo M0 la medida menor y M4 la mayor. Cada medida incluye a las anteriores, de modo que M4 incluye desde M3 a M0 y así sucesivamente.

- **M0**: es el dinero que circula en la economía y se define como la cantidad de billetes y monedas en manos de los ciudadanos, además del dinero que los bancos tienen en sus cajas, y depositado en el banco central.
- **M1**: es el dinero que circula en la economía, es decir, las cantidades que los ciudadanos tienen fácilmente accesibles para gastar.
- **M2**: incluiría el dinero disponible a gastar a corto plazo (hasta un año).
- **M3**: incluiría el dinero disponible a gastar a largo plazo.
- **M4**: incluye el resto del dinero que no está en los tipos anteriores.

Actualmente, la masa monetaria mundial se sitúa en torno a 60 trillones de dólares, valor que sigue creciendo tal y como vemos en la siguiente imagen (no olvidéis la forma de la imagen) y que mucho nos tememos no tiene intención de dejar de crecer:

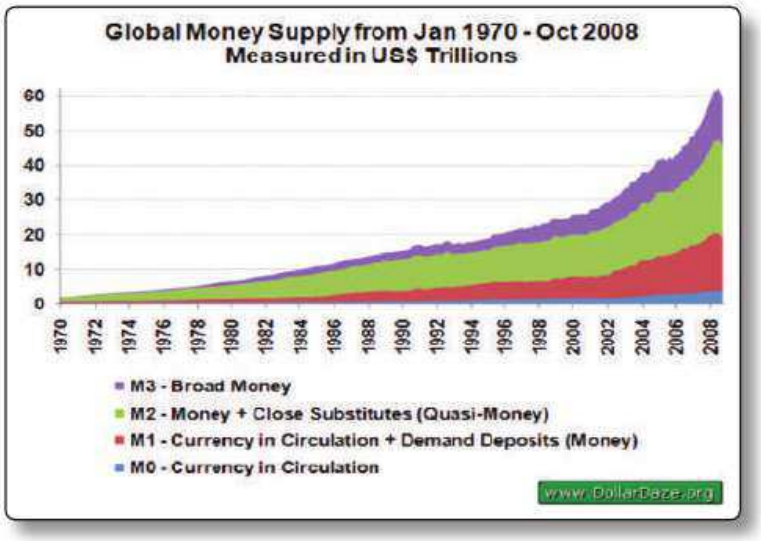


Figura 1.2. Masa monetaria mundial (fuente: dollardaze.org)

¿Qué significa esto para Bitcoin? Pues algo clave, el número total de Bitcoines que habrá en el futuro será de 21 millones, la mayor parte se alcanzará alrededor del año 2030. Esto significa que la cantidad de dinero disponible está prefijada de antemano a este valor, y lo que es más importante, al no poderse crear más, el poder adquisitivo de las personas que los posean no disminuirá por efecto de la inflación. En el siguiente gráfico (fijaos en la diferencia sustancial de la forma del gráfico con respecto al anterior) podemos ver el número de Bitcoines minados a día de hoy:

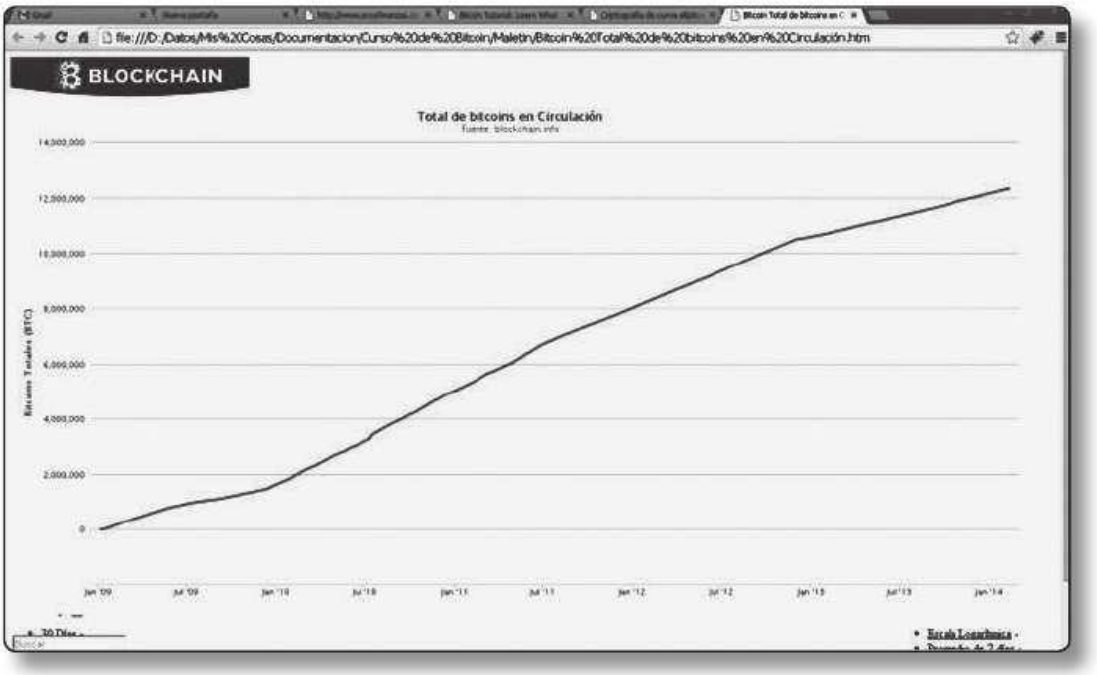


Figura 1.3. Total de Bitcoines circulando (fuente: blockchain.org)

Y ponerlo en contraste con como la **dificultad** para crear nuevas monedas crece de manera exponencial:

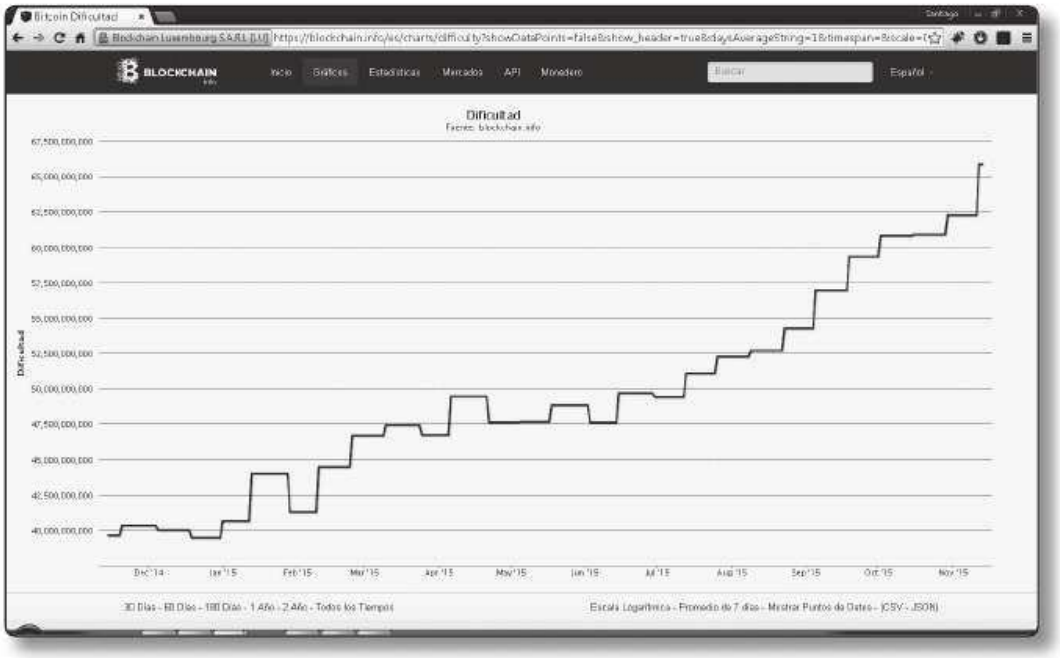


Figura 1.4. Aumento de la complejidad (fuente: blockchain.org)

Al suceder esto, es decir, al entrar Bitcoin en deflación, y dado que tiene la posibilidad de dividirse hasta el octavo decimal o **0,00000001 (1 satoshi)**, se producirá un ajuste de los precios, y unidades como el **microBitcoin** comenzarán a tener sentido (¿cobraremos nuestro salario en microbitcoines?, se haría realidad el dicho de que tenemos salarios microscópicos). Y sin olvidar que para 2030, siguiendo el volumen actual de impresión de papel, no quiero pensar la cantidad de billetes que habrá en circulación que literalmente no valdrán nada o poco más que nada; y si no queremos darnos cuenta de esto, basta con hacer un poco de repaso a la historia de la humanidad, pero si no queréis perder tiempo buscando, en el final del módulo podéis echar un vistazo a lo sucedido en Hungría en 1946 y en Zimbabue a principios de este siglo, para entender qué puede suponer una emisión masiva de papel, y esto no es algo que nos estemos inventando, es simplemente una lección de historia que obviamente nadie quiere que aprendamos.

1.2.9 Volatilidad

Es una medida de **la frecuencia e intensidad** de los cambios del precio de un activo, cuanto mayores son los cambios que se producen en este precio, mayor es la volatilidad. Aquí vamos a descubrir que los conceptos básicos de estadística que

nos enseñaban en el colegio resultan muy útiles, y es que de un modo muy técnico se define como la desviación estándar de dicho cambio en un horizonte temporal específico, aunque usualmente suelen usarse datos mensuales.

Es una medida que se utiliza para cuantificar el riesgo, dado que lo que se calcula es una desviación, podemos saber y por tanto medir cómo la rentabilidad se ha desviado de su media histórica. Si la desviación es alta significa que la rentabilidad ha tenido fuertes variaciones, y por tanto el riesgo y una pérdida potencial son mucho mayores, debido a los altibajos. Todo lo contrario sucede con la baja volatilidad, en este caso la rentabilidad ha sido más estable en el tiempo. La rentabilidad por sí sola no sirve de mucho, y se suele utilizar como valor adicional para realizar comparaciones la media, de manera que con estos dos datos se puede uno hacer una idea más precisa de la situación.

Pero cuidado con esto porque puede llevarnos a un error, la volatilidad es un dato sobre el riesgo pasado, no sobre el riesgo futuro, aunque es cierto que si algo fue volátil en el pasado, es probable que siga siéndolo en el futuro, ya sabemos que la historia tiene la manía de repetirse. No es de extrañar encontrarse con artículos como el aparecido en **CNNMoney** durante el mes de mayo titulado "Strategist Predicts End of Bitcoin" en donde estas circunstancias se utilizan para argumentar el fin de Bitcoin.

Ahora mismo Bitcoin es una moneda sumamente volátil, e invertir en ella debe ser considerado como un elemento de alto riesgo, riesgo que a medida que se va popularizando y conociendo se va mitigando y por tanto, su volatilidad tenderá a estabilizarse. En este sentido, os recomiendo echar un vistazo al documento aparecido en la revista *Forbes* en abril de 2013, que bajo el sugerente título de "An Illustrated History of Bitcoin Crashes" analiza la volatilidad de Bitcoin.

De hecho, acontecimientos tan importantes como fue el cierre de Silk Road supusieron una fluctuación en el valor muy pequeña, y que se recuperó prácticamente al momento, en comparación con la magnitud de la noticia y el bombo que en los medios se le dio, y la asociación de Bitcoin como moneda para la ciberdelincuencia. Es cierto que aún las noticias tanto positivas como negativas afectan mucho su cotización, por ejemplo durante el mes de noviembre de 2013, hemos visto como crece el interés de China por Bitcoin, o incluso funcionarios americanos o el mismísimo **Bernanke** han reconocido el potencial de Bitcoin en un futuro, lo que supuso que la moneda pasara de valer unos 200 dólares a más de 1.000 dólares en menos de un mes (¡burbuja, burbuja!, gritan muchos), con caídas hacia atrás de más de 400 dólares en cuanto los mismos chinos han empezado a poner trabas.

¿Por cuánto tiempo seguiremos en esta pauta? Solamente el tiempo nos lo podrá decir.

A medida que la volatilidad se va estabilizando, tenemos más garantías del éxito de Bitcoin a futuro. Y aunque haya quien diga que con una moneda tan volátil es difícil que las tiendas acaben por aceptarla como medio de pago porque es difícil fijar los precios de los productos, solo hay que echar un vistazo a la relación de tiendas que a día de hoy no tienen problemas en operar con ella. Es decir, que el principio del buen dinero de servir como **unidad de cuenta** (que es lo mismo que decir que el precio de un producto determinado pueda expresarse en Bitcoines), no parece que no esté garantizado o al menos no parece que sea algo que preocupe a estos establecimientos que ponen sus productos a la venta a cambio de Bitcoines, ni tampoco importa a los que compran que al fin y al cabo buscan reducir el coste de la operación en el momento de hacerlo, y el valor futuro no es algo de lo que se preocupen. Se podría argumentar, no obstante, que la volatilidad va en contra del principio de **depósito de valor**, pero esto solo debería preocuparnos si Bitcoin solo fuera un medio de atesorar valor, y no se utilizase para el intercambio.

Por todo esto, augurar el fracaso de Bitcoin basándose únicamente en la volatilidad no me parece muy acertado y deja muchas otras variables fuera.

1.2.10 Devaluación

Pocos de nosotros nos paramos a pensar lo que supone la devaluación de la moneda, y lo que conlleva alterar el valor del dinero en la economía; leí una vez una reflexión que me gustó mucho, creo que fue en el blog de **elbitcoin.org** cuando en un *post* apareció la frase:

"¿alguien se imagina lo que supondría para la arquitectura alterar el significado del valor del metro? Pues esto que es impensable en la arquitectura, es el pan nuestro de cada día en el mundo económico".

La devaluación consiste en la pérdida de valor de una moneda en comparación con algún patrón establecido, ya sea el precio del oro u otras monedas que sean más fuertes, como tradicionalmente ha sido el uso del dólar.

Se entiende muy bien con el ejemplo que usa la Wikipedia para definirlo: partimos de la situación inicial y poseemos 100 unidades de un bien y dichas unidades valen 1 euro, por tanto, tenemos 100 euros en circulación respaldados cada uno de ellos por una unidad del bien. Si aumento en 100 unidades más las monedas que hay en circulación (ahora tenemos 200) tenemos tres escenarios posibles:

1. **Incrementar el valor de los bienes para que valgan 200 euros**: esto es complicado, ¿cómo incrementas el valor de un bien? Mejorando la **productividad** necesaria para producirlo podría ser una opción, pero mira que cuesta hacerlo.

2. **Sacar de circulación 100 euros**: a ver quién es el listo que les quita a las personas que posean los 100 euros creados las monedas, y sin darles nada a cambio. Vamos, ni de broma.

3. **Darle un valor a la moneda de 50 céntimos**: es la opción más sencilla, devalúo el valor de la moneda para adecuarla al valor real del bien que tengo, no toco la productividad ni le quito nada a nadie (eso que te lo crees tú, porque no le quitas la moneda, simplemente le quitas la cantidad de cosas que puede comprar con ella).

Lo más curioso de las devaluaciones es que son los bancos centrales y los países que respaldan a una moneda los que deberían velar por tener una moneda fuerte y saneada, sin embargo sucede que el aumento de la inflación y la puesta en marcha de más papel hacen todo lo contrario, la debilitan. Y lo peor es que parece como si a nadie le importase, porque aunque nos digan que las devaluaciones son buenas para las exportaciones (y malas para las importaciones) y que se crea empleo, porque es más barato comprar nuestros productos, ¿realmente se llega a compensar? ¿Llegamos a ser tan verdaderamente productivos y competitivos y vendemos tanto al exterior que nos sale a cuenta? Igual soy un poco ignorante, pero pienso por ejemplo en los productos que vienen de China, hoy por hoy devaluar la moneda ¿nos permite competir con ellos? ¿No estaremos siendo tan estúpidos que simplemente les salimos más baratos para que sean ellos los que acaben comprando nuestro sistema productivo (nuestras empresas y nuestra deuda) y a la postre se queden con todo? Y dejando China a un lado, ¿qué pasa con el petróleo que se paga en dólares? ¿Devaluamos el euro? ¿Podríamos permitírnoslo?

1.2.11 Tipo de interés

Los tipos de interés forman parte de la política monetaria que los Estados realizan y cuyo objetivo es fijar el precio del dinero, aunque creo que resulta más claro decir que los tipos de interés es el precio que se paga por usar dinero, al fin y al cabo el dinero no es más que otro tipo de bien, un tanto especial porque es el que usamos para hacer nuestros intercambios, pero un bien más. Este precio por el dinero se paga siempre a los bancos, que son los que a la postre nos lo dan, amablemente, a través del **crédito** y del **endeudamiento**.

Se supone que si los intereses son bajos, nos animaremos a pedir dinero, mientras que si son altos, procuraremos no hacerlo porque tendremos que devolver más dinero al prestatario. Por tanto, si se dispone de la capacidad de manipular el valor del tipo de interés, podemos conseguir influir en la marcha de la economía y tendremos un mecanismo para regularla.

Como veremos más adelante, esto de los intereses tiene sus pequeños problemillas.

1.2.12 El banco central y el sistema monetario

Los bancos centrales son una institución que ejerce como autoridad monetaria de un país, y suelen ser los encargados de la emisión de dinero legal y de la ejecución de la política monetaria, y por tanto son los encargados de controlar el buen funcionamiento del sistema monetario.

Un sistema monetario siempre abarca a una región particular del planeta, y es lo que se va a utilizar como medida de la riqueza y estándar de valor. La situación actual ha hecho que con la entrada del euro, muchos países que tenían sus propios sistemas monetarios basados en sus monedas (como era el caso de España con la peseta) y que abarcaban la extensión del país, ahora lo compartan. Los bancos centrales son como el banco de los bancos, ya que a ellos acuden tanto otros bancos como el Estado a buscar financiación.

Independientemente de las fuentes que consultéis, veréis que el objetivo de todos los bancos centrales se resume en dos puntos:

- Preservar el valor de la moneda y mantener la estabilidad de los precios (inflación), para ello modifican los valores de los tipos de interés.

- Mantener la estabilidad del sistema financiero, mediante la concesión de préstamos a otros bancos con problemas financieros o incluso a otros Estados, es lo que se conoce como una **inyección de liquidez**.

Oye, una preguntita tonta, ¿pero los bancos centrales son independientes de los gobiernos, verdad? Bueno, pues la respuesta a esta pregunta es sí, al igual que sucede con los poderes ejecutivo, legislativo y judicial (y al menos en España sabemos que esto se cumple a rajatabla; es en tono sarcástico, claro), en donde actúan unos como garantes de que los otros no realizarán ningún desmán; los bancos centrales son independientes de los gobiernos de los países a los que prestan servicio.

Es más, hay estudios que indican que la independencia del banco central favorece el control de la inflación y ayuda a la estabilidad de los precios, motivo este que hace que esta independencia forme parte de las normas y leyes que lo regulan de manera que no pueda aceptar órdenes ni mandatos de ningún gobierno. Se supone que tanto el Banco Central Europeo (BCE), como la Reserva Federal de los Estados Unidos, como todos los bancos miembros del **Sistema Europeo de Bancos Centrales** actuarían de este modo.

Sin embargo, hay algunas voces que dicen que esto de la independencia no es tan bueno como pudiera parecer en primera instancia o que existe un control velado de los bancos centrales por los políticos de turno, por ejemplo, el premio Nobel de Economía, **Joseph Stiglitz**, en un artículo titulado "Not-So-Independent Central Banks" y publicado en el *Wall Street Journal*, asegura que el comportamiento de las economías de China, India y Brasil, cuyos bancos centrales no presentan una independencia como los de EE. UU. y la eurozona, es mejor que el de los segundos. Y hace una reflexión interesante cuando dice que, si los políticos no toman las medidas necesarias en sus países para reactivar la economía, a los bancos centrales no les queda más remedio que seguir financiando la deuda pública de manera obligatoria de modo que son los políticos, de un modo indirecto, los que estarían controlando el funcionamiento de los bancos centrales al no hacer, por decirlo de algún modo, su trabajo.

1.2.13 Inflación

Hemos estado refiriéndonos al problema de la inflación en los anteriores apartados de manera recurrente, hora es de que le dediquemos el apartado que le corresponde y veamos su significado ya que gran parte del meollo del asunto lo tenemos aquí.

Entonces una de las misiones de los bancos centrales es la de controlar la inflación, ¡umh, qué interesante!, porque entonces pueden actuar como estabilizadores (¿o desestabilizadores?) del sistema influenciados por políticos que no hacen las cosas bien.

Pero, ¿qué es la inflación y por qué es tan importante?

La definición es fácil de comprender:

"incremento generalizado y sostenido de los precios de bienes y servicios con relación a una moneda durante un período de tiempo determinado y asociado a una economía en la que exista la propiedad privada".

La inflación tiene que ver con la capacidad de una moneda para comprar un bien o un servicio. Si aumenta la inflación significa que disminuye el poder adquisitivo de la moneda, es decir, se produce un **empobrecimiento** y esto sucede por el aumento general de los precios. Lo cual si lo pensamos un poquito es lógico, si los precios suben, significa que por cada moneda que tenemos, podremos comprar menos producto y para poder comprar la misma cantidad de producto necesitaremos más monedas. Es por eso que siempre que aparecen los datos de inflación, estos vienen acompañados de algún indicador de cómo van los precios, el más extendido es quizás el **Índice de Precios al Consumo o IPC**.

Que los precios de los bienes y servicios suben es un hecho al que estamos acostumbrados, y hay dos explicaciones básicas para entender el motivo por el que sucede:

- La primera explicación se debe a lo que acabamos de ver, a una **inflación de demanda**, necesitamos más productos en el mercado de los que es capaz de proveer la capacidad productiva disponible. Esto suele suceder en períodos económicos expansivos y tiene un carácter cíclico, como hay dinero disponible queremos comprar cosas, pero el mercado no es capaz de producirlas al ritmo que las queremos.

  Un ejemplo: cuando los españoles con la conquista de América trajeron grandes cantidades de oro y plata a Europa, al haber más demanda y menos producto, el precio subió. Por tanto, siempre que aumenta la cantidad de dinero en circulación, tendremos un problema de este tipo, y es que darle a la "máquina de hacer billetes" es muy peligroso.

- La segunda explicación se debe a un encarecimiento del proceso productivo, o **inflación de coste**, aquí el problema viene por un encarecimiento en la creación del producto, por ejemplo, aumento de los costes salariales o de las materias primas.

La inflación según la magnitud del aumento suele clasificarse en distintas categorías:

- **Inflación moderada**: se sitúa en un valor en torno al 3% o al 4% anual. Tiene que ver con el incremento de los precios de manera lenta. Si los precios crecen lentamente, significa que el valor de mi dinero se va a mantener constante en el tiempo y puedo tener una mayor confianza en dejar el dinero en una cuenta corriente o un depósito de ahorro.

En esta situación, con precios relativamente estables, las personas se fían de este, colocando su dinero en cuentas bancarias (confían en que su dinero no va a perder valor, y no habrá variaciones ni en un mes ni dentro de un año). En sí, las personas están dispuestas a comprometerse con su dinero en contratos a largo plazo, porque piensan que el nivel de precios no se alejará lo suficiente del valor de un bien que puedan vender o comprar. Un valor que se supone válido para este rango es del 3% al 4% anual.

- **Inflación tendencial**: en este caso el crecimiento de los precios es continuo y se convierte en la tónica general. Los valores oscilan entre el 3% y el 20% anual.

- **Inflación galopante**: la inflación galopante sucede cuando los precios se incrementan a partir del 30% en un plazo promedio de un año. Un nivel de inflación por encima de este nivel implicará siempre grandes cambios económicos; estamos ante una situación en donde el dinero pierde su valor de manera rápida.

- **Hiperinflación**: si la situación anterior no se controla, si no hay cambios económicos profundos, pasamos a tener hiperinflación, y en esta situación crítica el dinero pierde su valor muy rápidamente, la población tiende a deshacerse de él y a comprar antes de que no valga nada; aquí se suele también hablar de una **inflación autoinducida** debida al cambio en el comportamiento de los consumidores de un país o una zona geográfica determinada, que no hace más que agravar el problema, porque si todos los consumidores deciden ponerse a comprar a un tiempo, ante el miedo de la pérdida del valor del dinero, aumenta el déficit en productos disponibles y por tanto aumenta la inflación (vamos, una pescadilla que se muerde la cola).

La hiperinflación se produce en países con una crisis económica muy fuerte, que se debe a la emisión de dinero ("darle a la máquina de hacer billetes") sin control y a un pobre control y regulación entre los ingresos y gastos del Estado.

Entonces, ¿es mala la inflación? Bueno, pues aquí también depende de cómo nos cuenten la situación, ya que podemos encontrar que sus efectos en la economía pueden ser tanto positivos como negativos. El mayor problema de la inflación es la devaluación del valor real de la moneda con el paso del tiempo, esto produce incertidumbre y la incertidumbre se convierte en falta de confianza, y la falta de confianza hemos visto que es mala para el funcionamiento de todo el sistema, a nadie

le gusta no conocer el valor futuro del dinero o una eventual escasez de determinado tipo de bienes.

Pero el quid de la cuestión dependerá en función de la perspectiva que se analice y es que la inflación no afecta a todos los bienes por igual, ni a la vez. Si nos suben el precio de la gasolina, tendremos que pagar más por los mismos litros. Desde esta visión, parece lógico que la inflación es negativa para nosotros.

En otras ocasiones podremos afirmar que un aumento de la inflación podría ser bueno, pero depende de a qué se deba (inflación de la demanda, de las expectativas, de los costes, por causas monetarias, etc.). Si por ejemplo la inflación se debe a un aumento del consumo interno, afirmaríamos que sería un síntoma de recuperación económica, y por ende, positivo.

En cualquiera de los casos, una inflación sostenida siempre es causada cuando se emite dinero a mayor velocidad que la tasa de crecimiento económico. Es decir, si no hay crecimiento económico, ¿cómo podemos crear más dinero? ¿No estamos engañándonos a nosotros mismos? Luego lo explico cuando hablemos de cómo se crea el dinero y el papel de la deuda en todo esto.

ENTONCES…

Bitcoin es una moneda **deflacionaria**, premia el ahorro y su gasto de manera racional en bienes y servicios que realmente son necesarios.

La tarea de mantener la tasa de inflación baja y estable se asigna generalmente a las autoridades monetarias de cada país, aplicando lo que se denomina como su mandato. Actualmente, estas autoridades monetarias son los bancos centrales, que actúan en tres frentes:

- Fijando las tasas de interés.
- A través de transacciones en el mercado de divisas.
- Con la creación de la banca de reservas.

¿Cómo funcionaría el Banco Central Europeo ante esta situación? El mandato (el objetivo) del BCE es mantener la inflación interanual en la zona euro entre 0 y 2 puntos porcentuales. Si la zona euro cayera en deflación, el BCE podría recurrir a imprimir dinero (expandir la masa monetaria), mediante la operación electrónica de sumar una cantidad de dinero a las reservas totales del banco y utilizar este dinero recién creado en sus operaciones (comprando **títulos de deuda**, por ejemplo bonos

de los Estados europeos) para provocar un alza en el precio de ese tipo de títulos; este mecanismo inyecta una fuente de inflación en el sistema que puede llegar a contrarrestar la deflación no deseada.

En el escenario más frecuente en que la inflación de la zona euro rebase el objetivo límite del 2%, el BCE puede subir el tipo de interés de los préstamos a corto plazo que ofrece a los bancos comerciales en su calidad de prestamista de última instancia, lo cual encarece los préstamos de dinero y frena la inflación.

El problema de todo este sistema es que nos lo han vendido como un mal necesario, y se considera a la inflación como un mecanismo de regulación que ayuda en la salida de las crisis, porque claro, su contrario, la deflación, nos dicen que es aún peor. Sin embargo, lo que hace esto es que el dinero se deprecie y realmente no ganamos nada, estamos ante una burda mentira, en donde no se produce el estímulo necesario para salir del problema (¿no habríamos visto la luz ya?, digo yo), porque a más dinero, precios más altos, es de cajón; si con 1 euro me puedo comprar una naranja, y ahora tengo 2 euros, pero las naranjas suben 1 euro, ¿realmente me voy a comprar la naranja? Vale, hay más dinero, pero el precio se ha duplicado (en este ejemplo), y ante esta situación, ¿qué hemos ganado? Nada. Bueno sí, hemos conseguido que se deteriore el poder adquisitivo y que no ahorremos, y tendamos a gastar sí o sí, aunque realmente no tengamos necesidad de hacerlo para que la máquina no se pare.

1.2.14 Deflación y el efecto Ricardo

Si el valor de la inflación es negativo, se habla de deflación y en este caso estamos ante una bajada generalizada y prolongada de los precios (se asume en este caso, al menos dos semestres); es un fenómeno contrario a la inflación. Y no hay que confundirla con la desinflación, que es una desaceleración de los precios, pero estos siguen creciendo a menor ritmo.

Si en el caso de la inflación estamos ante un aumento de la demanda, en la deflación se produce todo lo contrario, hay una caída de la demanda que suele tener unas consecuencias mucho peores que la inflación (o al menos eso es lo que nos dicen), por **el efecto Ricardo** (1772-1823).

¿Cómo afecta la deflación a Bitcoin? Hemos dicho en varias ocasiones antes, que como máximo habrá 21 millones de Bitcoines en el futuro, y que más o menos para el año 2030 habremos llegado a generar esa cantidad, y que en torno a 2017 se habrán generado las ¾ partes del total.

Ante una situación como esta, lo más normal es que la moneda entre en deflación; al haber cada vez menos, el valor de Bitcoin tenderá a aumentar en relación a los productos que se pueda comprar con él, esto significa que unidades que hoy no tendrían mucho sentido, por ejemplo pagar en **milibitcoines**, etc., en cuestión de poco tiempo pueden representar una cantidad de dinero verdaderamente importante.

ENTONCES…

Y eso sin tener en cuenta los Bitcoines perdidos, aproximadamente el 4% de los Bitcoines minados no son accesibles por algún motivo, generalmente relacionado con la pérdida de la clave privada asociada; por tanto 21 millones de Bitcoines en circulación es una visión muy optimista de la realidad.

Y esto es algo, desde mi punto de vista, muy bueno porque se incentivará el ahorro y los proyectos a largo plazo, si la moneda no se puede devaluar, no tiene sentido el consumo irracional ni el endeudamiento, y por tanto, se puede abordar proyectos que de otro modo serían impensables porque nos interesa gastar el dinero cuanto antes.

Aquí hay quien dice que se entraría en la llamada "espiral deflacionaria", una especie de agujero negro en donde al entrar los precios tenderían a bajar más y más debido a que la gente guardaría su moneda esperando que valiese cada vez más y más. Esto sin embargo, es un hecho limitado, la **teoría austríaca del ciclo económico** lo explica muy bien, cuando dice que lo que realmente sucede es que ante un colapso financiero, se produce una reubicación de los recursos, todo ello debido a una mala inversión generalizada producida por la intervención estatal e inducida por años de inflación crediticia. ¿Y no estamos ante un colapso del sistema financiero mundial? ¿Podemos seguir negando la evidencia de que "algo" se ha roto y que no se pueden seguir poniendo parches?

Además, si los precios bajan, bajan de todas las cosas, y por ende los costes de producción también son más bajos. Yo siempre que alguien me habla de lo mala que es la deflación intento que me contesten a estas cuestiones, porque personalmente no lo veo; bueno, sí veo que con el sistema actual no interesa a nadie que se produzca, porque la inflación va siempre pareja al crecimiento irracional y al poder pagar las deudas, y como todo el dinero es deuda, el sistema actual se va al garete. Pero es que para mí la cuestión está en que hay que cambiar el sistema actual y no dejarlo como está; mis preguntas son las siguientes:

1. ¿No será que el problema está en **los cálculos de beneficios** de manera anual que buscan algunos y que con deflación no podrían sostener y por tanto les interesa seguir con este sistema? Y es que si este año he tenido un beneficio de 1 euro, el año que viene quiero que sea de 3 euros, pero en un escenario deflacionista se complica un poco conseguirlo aunque siga ganando después de descontar el ajuste por la bajada de precios.

2. Pero, ¿y los bancos? ¿No será que ante la deflación se encuentren con préstamos cuyas garantías que los avalaban valgan menos y por tanto estén menos protegidos contra el riesgo?

3. ¿Y qué pasa con los deudores? Salen perdiendo obviamente ante este nuevo panorama.

4. Nos dicen que con la inflación y con el aumento del gasto se crea empleo, pero ¿hay algo más ineficiente, poco productivo y más cortoplacista que el empleo creado de manera artificial?

5. ¿No es mejor aumentar el nivel de ahorro, reducir el coste del capital y de esta manera impulsar la inversión que producirá empleo de calidad, productivo, sostenible y de largo plazo?

6. ¿No será que hay demasiados intereses en que todo siga igual y que la política del miedo funciona muy bien?

Es muy probable que ahora mismo haya gente que esté comprando Bitcoines y los guarde como un tesoro esperando el momento de la deflación, pero también es cierto que llegará un momento en que la gente comenzará a gastarlos (¿o alguien ahorra para llevarse el dinero a la tumba con él? Yo desde luego no, ahorro para invertir, ganar más dinero y a la postre darme algún capricho y vivir mejor). Os lo decía anteriormente, sé que en unos meses saldrá al mercado un mejor coche, pero por ese motivo no dejo de comprarme un coche hoy si realmente lo necesito, es decir, no pospongo de manera indefinida mi compra, pero si sucede que compro de manera más racional y si pospongo una compra, ¿no será que dicha compra era superflua y por tanto innecesaria?

¿Qué os parece a vosotros?

1.2.15 Entendiendo el IPC

Hemos dicho que la variable que se utiliza para saber cómo vamos de inflación/deflación se denomina **IPC o Índice de Precios al Consumo**, en España se calcula mes a mes por el Instituto Nacional de Estadística y nos ayuda para establecer comparaciones de año en año y entre meses. En este índice se tienen en cuenta productos básicos que cualquier familia compraría a lo largo del mes, de modo que lo que se estudia es la evolución de los precios de esos productos básicos, que constituyen y por simplificar "la cesta de la compra" de los ciudadanos.

El problema es que para hacer la lista de los productos que hay dentro de la cesta, no se tienen en cuenta muchas particularidades del día a día, y resulta que podemos encontrarnos con que puede no ser representativa realmente; por ejemplo, puede ocurrir que la lista de bienes y servicios que hay en la cesta esté desfasada con respecto a lo que los usuarios realmente compran, tampoco se tiene en cuenta que los aumentos de la calidad en muchas ocasiones no llevan pareja una subida de precio (por lo que compramos un valor añadido por el mismo precio) o incluso los cambios de tendencia en los hábitos de compra.

¿No os ha pasado que cuando dan el dato del IPC y de qué productos suben o bajan, se te queda cara de lelo y te preguntas dónde será eso porque en el mercado del barrio todo sigue igual? El mejor ejemplo es el petróleo, qué rápido sube el precio de la gasolina pero cuánto le cuesta bajar, ¿verdad?

Entonces, si para hacer el cálculo de la inflación se está usando un elemento poco representativo de lo que la sociedad demanda, ¿hasta qué punto se puede justificar la inflación y el crecimiento porque sí, si su cálculo puede ponerse en entredicho?

1.3 EL PATRÓN ORO

El patrón oro es un sistema monetario, en donde se acepta como estándar de valor al oro. Consiste en fijar la unidad monetaria en términos de una determinada cantidad de oro. Es decir, quien emite la moneda garantiza que en caso de que el poseedor decidiera cambiarla por la cantidad de oro equivalente, podría hacerlo sin problemas. Pero no solo se garantiza la conversión de dinero en oro, sino que además se permite exportar e importar oro libremente. Durante la vigencia del patrón oro puro, las entradas y salidas de oro regulaban la cantidad de dinero de un país, ya que al ser los billetes convertibles en oro, la cantidad de dinero en circulación debía conservar una proporción de reservas de oro del 100% en el banco central.

El patrón oro no es el único patrón que se ha utilizado a lo largo de los años, también existe **el patrón plata** e incluso **el patrón bimetálico**, en donde el valor de la moneda se respalda en una cantidad por oro y en otra por plata.

1.3.1 Origen

El patrón oro comenzó a utilizarse durante el siglo XVIII pero no fue hasta el siglo XIX cuando se generalizó su uso en el sistema financiero internacional (hay quien llega a considerarlo como el motor que hizo posible la Revolución Industrial, gracias a la estabilidad y prosperidad que trajo consigo), sobre todo desde 1870 hasta la Primera Guerra Mundial. Durante este período, cualquier ciudadano podía transformar su papel moneda en una cantidad de oro equivalente.

El origen del patrón siempre se sitúa en Inglaterra en el siglo XVIII, y en los problemas monetarios por los que atravesaba después de las guerras napoleónicas. Durante el fin del siglo XVIII se establecerían las bases para que el patrón oro pudiera funcionar, considerándose su año de puesta en marcha oficial 1821. No fue hasta 1850 cuando Inglaterra, convertida en potencia mundial, demostraba que el sistema monetario implantado usando el oro, en detrimento de la plata o del bimetalismo, impulsaba la industrialización, modernización y el desarrollo político de la sociedad. De este modo, poco a poco y de manera progresiva y voluntaria, los países fueron adoptando el patrón adecuándolo a sus características particulares.

Se denomina como **núcleo del patrón oro** al grupo de países formado por Inglaterra, Alemania, Francia y Estados Unidos, por ser los que mejor observaron las reglas en su primera etapa. En general el proceso de adopción del patrón oro seguía tres pasos:

1. Adopción del oro como unidad monetaria, fijando su valor respecto a la moneda de plata, la cual es retirada de circulación.

2. Se establece legalmente el patrón oro y se decreta la desmonetización de la plata.

3. Se crea el banco central.

Su funcionamiento es más o menos el siguiente: los valores de las monedas que lo aceptaban se estabilizaban dentro de una franja de valor, dicho de otro modo, cada moneda tenía su equivalente en oro dentro de un rango. Si un país tiene déficit, se produce una salida de oro y se produce una contracción en la oferta monetaria; al producirse esta contracción monetaria, se produce una bajada de precios en el

mercado interno. La bajada de precios en el mercado interno es un aliciente que facilita las exportaciones y reduce las importaciones, lo que origina un flujo de entrada de oro en sentido inverso, es decir, sirve para autoregular y equilibrar los flujos de capital.

1.3.2 El patrón cambio oro

Esta situación finalizó cuando al final de la Primera Guerra Mundial, se comprobó que la impresión de billetes llevada a cabo por los países en conflicto no tenía respaldo, es decir, se habían impreso más billetes para hacer frente a los gastos de la guerra que la cantidad de oro que había almacenada en las reservas y que podía respaldarlo. Ante este panorama, se prohibió a los particulares realizar la conversión y se cambió por el patrón cambio oro o gold exchange standard, en la conferencia de Génova en 1922, período que se conoce comúnmente como los felices años veinte, en donde se inicia un período de crecimiento industrial y prosperidad que finalizaría con el **crack del 29**.

Elaborado originalmente en 1876 por A. M Lindsay del Banco de Bengala como una propuesta de reforma al sistema monetario de la India, el patrón cambio oro consistía en utilizar una moneda intermedia para hacer el intercambio por oro. En vez de que cada moneda, de cada país particular, pudiera convertirse directamente, lo que se hacía era cambiarlas en primer lugar por otra y a partir de esta, se procedía a la conversión en oro.

ENTONCES…

El crack del 29, o la **Gran Depresión**, fue la más devastadora caída del mercado de valores en toda la historia de los Estados Unidos. La caída inicial se produjo el 24 de octubre de 1929 (Jueves Negro) pero no fue hasta el 28 y 29 de octubre de 1929 (**Lunes Negro** y **Martes Negro** respectivamente) cuando el pánico se desató y continuó por un mes. En solo tres días más de 100.000 trabajadores perdieron su empleo. No fue hasta 1954 cuando el Dow Jones retornó a valores previos a 1929.

Las monedas que se utilizarían para la conversión fueron la libra esterlina y principalmente el dólar estadounidense. La conversión a oro se realizaba a razón de 35 dólares por onza para los gobiernos extranjeros. Pero claro, ligar el intercambio al dólar suponía que su fortaleza nunca fuera puesta en entredicho, cosa que sucedió durante 1971 y en la guerra de Vietnam (1959-1975).

La guerra de Vietnam supuso para los Estados Unidos un problema por muchos motivos, y uno de ellos fue el económico, ante la abundancia de dólares en el mercado, se empezó a tener la misma sensación ya sufrida después de la Primera Guerra Mundial y era la aparición de dudas para convertir a oro todos los dólares que había en circulación. Esta situación se agravó cuando los bancos centrales europeos intentaron convertir sus reservas de dólares, poniendo en serios aprietos a los Estados Unidos.

En 1971, y ante una situación que se estaba tornando insostenible, **Richard Nixon** suspendió de manera unilateral la convertibilidad del dólar en oro para el público y devaluó el dólar un 10%, aunque no sirvió de mucho, porque dos años más tarde, en 1973 tuvo que volver a realizar otra devaluación del 10% para finalmente terminar con la convertibilidad del dólar en oro también para gobiernos y bancos centrales extranjeros. Esta situación recibió el nombre de Nixon Shock (quien acabaría dimitiendo el 8 de agosto de 1974, por el escándalo del caso Watergate).

Para finalizar este apartado, comentaros que existe una variante del patrón oro denominada patrón oro en lingotes, o talón invisible, ideado por **David Ricardo**, y que se basa en la idea de que los metales preciosos como moneda aseguran un patrón más estable que cualquier otro, proponiendo que la circulación del dinero se hiciera a través de billetes emitidos por el banco central y que fueran convertibles en lingotes o barras de oro y no directamente convertibles en monedas de oro como en el sistema tradicional. El oro se depositaría en el banco sin acuñarse, asegurando que toda la circulación monetaria estaría respaldada por este.

Suiza fue el último país en abandonar el patrón oro en 1998.

Desde 1973 hasta el día de hoy, se utiliza el llamado **dinero fiduciario** que en vez de utilizar metales preciosos para garantizar su valor, lo hace a través de algo más etéreo, la confianza. Cuánta razón llevaba **Robert Anton Wilkson** cuando decía que el dinero es "una alucinación semántica, el equivalente verbal de una ilusión óptica".

1.4 EL DINERO FIDUCIARIO

El dinero fiduciario es aquel que se basa en la confianza que proporciona al público la entidad que lo emite. Este tipo de dinero puede o no estar respaldado por un metal precioso, las principales monedas del planeta no tienen este respaldo, léase dólar o euro. Aunque pueda sonar un poco fuerte, la verdad del asunto es que, el dinero es dinero, porque alguien dice que lo es y el resto nos lo creemos y lo

utilizamos como tal en el intercambio de bienes y servicios, si no el dinero fiduciario no tendría mayor valor que el del papel en el que se imprime.

El dinero que no tiene respaldo se denomina **dinero fíat o dinero simbólico**, y se emite por parte de Estados o bancos centrales.

Por tanto, un dólar o un euro valen lo que valen en nuestro mundo, porque tenemos confianza en que las entidades que están detrás de ellos (EE. UU., Unión Europea, BCE, FMI, etc.) y la economía en donde se utilizan van a funcionar relativamente bien. Además, tampoco nos queda otra, no es que nos dejen muchas alternativas para poder elegir, por lo menos hasta la llegada de Bitcoin.

ENTONCES…

Bitcoin, ¿es dinero fíat?; hemos dicho que dinero fíat es el que se basa en la confianza que tenemos en alguien que es el encargado de su emisión, pero Bitcoin no tiene un emisor, se genera en una red distribuida mediante un proceso denominado **minería**.

Estamos ahora en posición de entender correctamente dos ideas que han ido apareciendo en los puntos anteriores, me refiero al valor intrínseco y al nominal de una moneda. La parte del dinero que está respaldada por el metal precioso se denomina **valor intrínseco**, mientras que la parte no respaldada se denomina **valor nominal**. A lo largo de la historia, el valor intrínseco ha ido perdiendo importancia en favor del valor nominal: antes las monedas valían su peso (recordar al estatero) en el metal en el que estaban fundidas, luego se mezclaron con otros metales no preciosos y finalmente el papel moneda y el uso del patrón oro abrieron el camino definitivamente para el dinero fiduciario.

Como hemos visto anteriormente, la utilización del dinero fíat comenzó en 1971 con el Nixon Shock acabando con el modelo surgido después de la conferencia de **Bretton Woods** en 1944. Dado que ahora el dinero se basa en la confianza y no en metales preciosos, se ha producido un fenómeno muy importante, y es que tanto los Estados como los bancos centrales han producido una emisión de dinero muy elevada (**financiarización**) creando un mercado financiero más grande que el tamaño de la economía real. Es decir, cuando no hay dinero se le da a la "máquina de hacer billetes" y se pone este en circulación, pero claro, esto trae consigo una serie de problemas.

Cuántas veces no habréis oído frases en donde aparece algo del estilo: "… los mercados tienen o no tienen confianza…" y en función de esto las bolsas suben o bajan como en una atracción de feria. Si no hay confianza en las entidades, si no hay

confianza en la economía, si no hay confianza en el sistema, tenemos un verdadero problema, y ahora ya estáis un poco más cerca de entender el motivo.

Llegados a este punto vamos a preguntarnos algunas cosas molestas:

- ¿Qué es lo que podemos considerar como funcionar relativamente bien la economía?
- ¿Cómo generar confianza cuando el dinero es el instrumento de control al servicio de los Estados y los bancos centrales?
- Tal y como están las cosas, ¿no nos estamos acercando cada vez más a un banco central mundial (tal vez la fusión del FMI y del BCE) que determine cuál es la moneda que nos interesa utilizar?
- ¿Qué papel jugarán los Estados en todo esto, si impone leyes que nos fuercen a usar una determinada moneda?
- ¿No deberían ser las virtudes de una moneda y sus fortalezas frente a sus debilidades los criterios de elección elegidos para determinar su utilización? ¿Qué pasa si no con la democracia del mercado?, y entonces ¿qué llegará a pasar con la confianza en el sistema?
- ¿No estamos llegando a un punto en donde la gente se siente cada vez más estafada y con menos confianza?

¿Para volverse loco, verdad? al menos si has leído hasta aquí podrás empezar a intuir por qué Bitcoin es tan poderoso, porque va de la mano de la libertad, no necesitamos un órgano emisor, no necesitamos tener confianza en que quien lo controla lo hará bien y no se excederá en su manipulación.

Y todo ello sin olvidar que este sistema tiene una debilidad, que consiste en que el dinero fíat tiende a ser por naturaleza inflacionista, simplemente porque la presión y la facilidad para crearlo es muy fácil (que no para destruirlo), si crece la masa monetaria, esta es una de las causas que hacen que aumente la inflación, y por tanto a la larga lleva a un empobrecimiento, y aunque resulte paradójico a la pérdida de valor del propio dinero, por el simple hecho de necesitar cada vez más papel para poder acceder a los mismos bienes y servicios que se encaren en una espiral difícil de parar.

Esto con los patrones oro (o plata) no sucede, los excesos quedan controlados por la cantidad de metal disponible y por su flujo autoregulatorio, como hemos visto.

Por tanto, cuando alguien me dice que Bitcoin no sirve como depósito de valor, y me asegura que el dinero fíat o el papel moneda es un garante y pienso que está controlado por Estados y políticos indecentes, simplemente me entra la risa.

1.5 EL PROCESO DE CREACIÓN DEL DINERO

¡La de cosas que hemos contado hasta ahora! Supongo que tendrás la cabeza como un bombo, si no es así, seguro que consigo que te duela con lo que te voy a contar ahora. He estado hablando en algunos de los párrafos anteriores de que los Estados solo tienen que darle a la "máquina de hacer billetes" para poner más dinero en circulación, vamos a ver un poco más en detalle en qué consiste este proceso, y cuando hablemos de la **minería de Bitcoin**, veremos la diferencia tan grande que existe entre la generación de uno y otro.

Con todo lo que ya llevamos visto, deberíamos tener claro que los responsables de crear tanto monedas como billetes son los Estados, y concretamente su banco central. Puede suceder, como en el caso del euro, que esta responsabilidad quede delegada a otro organismo un poco mayor, el Banco Central Europeo, pero que con matices y para entender lo que nos ocupa, sería equiparable al banco central del país.

Dado que el dinero que usamos hoy en día es dinero fíat, los bancos centrales pueden producir todo el que quieran, independientemente de las reservas que tengan, solo basta dar la orden de imprimir papel y las máquinas se ponen en marcha, con el consiguiente problema de aumento de la inflación.

Hasta aquí todo claro, vamos a dar una vuelta de tuerca a esto y vamos a meter en la escena a otro actor: los bancos nacionales (y aquí metemos también a las cajas de ahorro) centran su actividad en la creación de depósitos bancarios. Estos depósitos bancarios son muy importantes, porque captan los fondos de los ahorradores para prestarlos a los agentes económicos que necesitan financiación.

Sin embargo un banco no puede prestar todo el dinero que capta a través de los depósitos, sino que está obligado a mantener un porcentaje de este para hacer frente a las demandas de efectivo, y que se conoce como **coeficiente legal de caja**, y que desde 1999 está fijado por el BCE en el 2%; todo esto sin tener en cuenta cualquier otra medida adicional que las autoridades monetarias consideren necesarias, a fin de garantizar la provisión en las reservas de efectivo.

Hagamos unas cuentas de la vieja para ver qué significa esto:

- Don Fulano de tal va al banco e ingresa 100.000 euros en su entidad, este dinero queda abonado en su cuenta bancaria. Los 100.000 euros han sido fruto del rendimiento de su capital (ganados con su trabajo o con sus inversiones, es decir, el dinero ha sido generado por una actividad real que don Fulano realiza y para nuestro ejemplo vamos a suponer que dicha actividad es honesta).

- Don Fulano de tal puede sacar su dinero mediante cheques, tarjetas o en efectivo, aunque claro, sacar un efectivo tan grande una vez ha sido depositado siempre implica llamar al banco antes para que nos tengan preparados los billetes.

- El banco retiene en sus reservas el coeficiente legal de caja del 2%, es decir, retiene 2.000 euros y los 98.000 restantes los puede prestar a alguien que los necesite. Y aquí por arte de magia, el banco ya ha creado dinero, tiene 98.000 euros disponibles en metálico y 100.000 en depósito bancario.

- El banco presta los 98.000 euros a don Mengano, que lleva ese dinero a otro banco (rizando el rizo podría ser al mismo banco), en donde el proceso se repite, el banco retiene el 2% y dispone de 96.040 euros para volver a prestar; hemos creado más dinero.

¿El proceso se puede repetir de manera indefinida? Afortunadamente no, llega un momento en que la acumulación de los coeficientes legales de caja de cada operación nos deja sin dinero disponible para seguir prestando, y que se calcula con una simple división:

Depósito inicial/coeficiente legal de caja

100.000/0,2 = 5.000.000 de euros

¡No está mal! A partir de 100.000 euros, podríamos llegar a crear 5.000.000 de euros, ¡ríete tú del milagro de los panes y los peces!, a esto se le llama **multiplicador bancario**, y creo que no es necesario explicar el motivo del nombre. Como el coeficiente legal de caja está en el denominador de la ecuación, cuanto menor sea, mayor será la cantidad de dinero que se podría crear. Dado que el banco solo tiene que tener en efectivo el valor correspondiente al coeficiente legal de caja del dinero del que dispone, si queremos sacar más dinero (más papel) tendremos que llamar uno o dos días antes, para que nos lo tengan preparado, porque literalmente no lo tienen. Luego cuento otro problema que aparece aquí, que es la **reserva fraccionaria**, pero dejarme continuar antes con esto.

Creo que con esta explicación entenderemos por qué los bancos tratan en todo momento de captar el dinero del ahorro, como mecanismo para poder crear dinero y porque siempre se dice, cuando estás ahorrando, que hay que buscar que el banco nos dé un rendimiento superior al de la inflación y lo mismo se aplica a cualquier inversión que vayamos a realizar. Si la inflación sube, y con ella los precios, tener el dinero en casa debajo del colchón no servirá para que nuestro dinero esté a salvo. Una opción sería gastarlo y disfrutarlo ahora (ya lo hemos explicado), total, mañana valdrá menos que hoy o nada, pero esto actuaría empeorando las cosas, porque si fuera el comportamiento generalizado de todo el mundo, la inflación autoinducida aumentaría y el problema se agravaría.

Lógicamente, los bancos nacionales intentan captar el dinero del ahorro, pero los bancos centrales que emiten el dinero que quieran, cuando quieran, no tienen porqué pedirle el dinero a nadie y basta con dar la orden de crear el dinero, que una vez inyectado en el sistema financiero a través de los bancos, puede ser utilizado mediante el sistema anterior para crear a su vez más dinero. Ya, alguien puede decir que los bancos tienen que aceptar entrar en el juego y necesitan aceptar apalancarse con préstamos o inversiones, pero ¿acaso no lo hacen? O como dice el refranero español "entre todos la mataron pero ella sola se murió". Pues eso mismo.

Pero crear más dinero tiene como consecuencia el aumento de la inflación y por tanto el empobrecimiento de la población, que es a la larga quien sufre los excesos de las políticas monetarias ineficientes y abusivas, y todo ello costeado gracias a nuestros impuestos, o ¿alguien se puede creer todavía que toda esta fiesta es gratis?

Pero, si esto que acabamos de decir de que el banco necesita captar nuestros ahorros es importante, mucho más sutil y desapercibida puede pasar la necesidad de que crear dinero como préstamo requiere que haya deudores para que el dinero se ponga en circulación, si no ¿qué necesidad hay de crear el dinero?

Y esto es gran parte del problema de la crisis económica que se inició en 2008, básicamente el problema radica en que se prestó dinero a quien se sabía de antemano que no podría pagarlo (hay un vídeo muy gracioso, pero mejor explicado imposible, que se aplica a España de **Aleix Saló**, llamándola **Españistán**, un juego de palabras entre España y Afganistán, y en donde explica el problema del endeudamiento por los pisos con una frase muy ingeniosa: "Soy un español con un SDM (o salario de mierda) y mi avalista es una tortuga con boina", conclusión, "Hipoteca al canto"; digno de ver); pero si prestamos dinero y no se devuelve la deuda, el sistema se colapsa, la confianza se pierde y se entra en el caos en el que estamos sumidos ahora mismo, por no decir que este escenario se vuelve inmanejable si son los propios Estados, y ya no solo los particulares y empresas, los que son incapaces de pagar la deuda que tienen contraída.

1.5.1 El dinero y la deuda

Entonces, ¿cómo va la cosa? Hemos derogado el patrón oro, y podemos crear tanto dinero como queramos, y por la fórmula anterior, hemos visto como se puede multiplicar el dinero a partir de los préstamos. Pero es que el banco además quiere tener un beneficio (no, no son ONG, ¿alguien tal vez se lo creyó?), por lo que cuando presta dinero, aparte del capital o principal que hay que devolver, hay que pagar unos intereses por haberte dejado el dinero.

Si el dinero que hay en circulación es porque se ha generado a través de los préstamos y por tanto de la deuda, el corolario es que toda la masa monetaria que circula dentro de una economía representa la cantidad de deuda que tiene esa misma economía.

O lo que es lo mismo, si no hay deuda no hay dinero.

Pero como además hay que devolver intereses, resulta que hay que devolver más dinero del que realmente existe (en el ejemplo anterior partíamos de 100.000 euros y la deuda se creó a partir de esta cantidad, no hay más que esos 100.000 euros), por lo tanto hay una escasez monetaria permanente (lo que obliga a crear más dinero para poder pagar los intereses) y obliga a que la economía tenga que crecer sin cesar.

Es decir, el actual sistema monetario no permite el pago de la totalidad de las deudas (es un problema que crece de manera exponencial), y lo que se hace, se mire como se mire, te lo quieran explicar y maquillar como quieran, es poner parche tras parche y dar "patadas hacia delante" evitando el problema real que existe y dejando que el que venga detrás se las componga cuando le toque, y lo resuelva como buenamente pueda, si es que puede.

En este punto llegamos a otra cuestión fundamental, ¿es posible en un mundo finito un crecimiento económico sin fin/infinito? Desde mi punto de vista, decididamente no, y aquí pienso en la aplicación de la idea económica de los rendimientos decrecientes a la creación del dinero (y al crecimiento exponencial de los intereses), y no solo eso, mantener el sistema actual en funcionamiento solo puede hacerse deprimiendo todo lo demás, entendiendo como todo lo demás no solo lo social sino también lo ambiental.

Y es que ante esta situación solo hay tres posibilidades:

1. Inflación.
2. Recesión o depresión.
3. Expansión o crecimiento económico.

ENTONCES…

¿Sabías que según el **Working Paper 12/163 del Fondo Monetario Internacional**, desde 1970 a 2011 a nivel mundial se han identificado 147 crisis bancarias, 218 crisis de moneda y 66 crisis de deuda pública? Si esto no indica que hay algo que va mal, pues que me lo expliquen.

De la inflación no tengo nada más que decir, ya sería ser pesado.

De las recesiones o depresiones, se supone que se sale por el ajuste de los precios, es decir, debido a que la economía deja de crecer, disminuye la producción, lo que implica un aumento del desempleo y falta de dinero, y esto hace que se comience a vender más barato (incluso puede suponer vender por debajo del coste de producción y en muchos casos significa el cierre de la empresa) y todo vuelve a la normalidad, vamos, lo que se llama un **ciclo económico**.

Pero, y es que siempre hay un pero, y uno gordo en este caso, porque aunque el papel lo aguanta todo, la realidad suele ser más tozuda, y es que a los precios les va mal eso de bajar (que no subir, eso lo hacen de maravilla) y el precio que peor baja es uno que nos fastidia mucho que nos toquen, el salario, que no es más que el precio que paga el empresario por la mano de obra y que supone ¿cuánto?, ¿un 60, tal vez un 70% del coste de producir algo? ¿A que pocas veces lo habías pensado de esta manera: "salario que percibes = precio que paga el empresario"? ¿Y a que no te gusta pensar que te lo puedan bajar? ¿Y si no te bajan el salario, cómo podemos hacer para que el empresario pueda bajar los precios y los costes de producir? Por sucede que antes de bajar salarios, los empresarios decidan despedir a parte de la plantilla, a fin de evitar que el descontento influya en la productividad y por tanto, el coste aumente. ¿Y qué hace el Gobierno con su política fiscal y monetaria? ¿Consigue arreglar algo? Pues básicamente no, empeora la situación porque lo que hace son dos cosas:

1. **Subir impuestos** (menos dinero para el ciudadano y empresas), que ya sabemos lo bien que son utilizados y el gran provecho que rinden, ya sean los **directos** (como el que te aplican con el IRPF) como los **indirectos** (el que pagas con el IVA por ejemplo), no hay nada que no esté bendecido por los impuestos estatales.
2. **Se endeuda**, al fin y al cabo, ¿quién no quiere prestar dinero a un Estado sabiendo que son buenos deudores y pagadores? (solo hay que pensar en Grecia para ver lo cierto de esta afirmación), mediante la **emisión de bonos o letras** que paga en un período de tiempo determinado, a un tipo de interés que sube o baja en función de la confianza que se tenga en que sea capaz de devolver el dinero pedido (¡sí, amigo, sí!, la famosa prima de riesgo), dinero que se devuelve gracias a los impuestos que ha recaudado (¡y subido!).

Y sin añadir el "me lo llevo crudo" que en todo buen gobierno siempre existe, independientemente del país en el que nos encontremos. Estoy seguro de que a estas alturas tienes los pelos de punta, yo también.

La conclusión a la que quiero que llegues es que ninguna de las tres es la solución, se puede pensar que la tercera es la opción menos mala, pero acabo de exponer que no creo que sea posible el crecimiento económico sin fin, por lo menos, no con los recursos del planeta Tierra únicamente (intento explicarlo mejor cuando hablo del interés compuesto en el punto siguiente), porque no ataca al problema principal y es que hay que reestructurar el sistema monetario, hay que hacer las cosas de manera diferente, el colapso del actual sistema tiene que llegar, la actual crisis económica (que no ha finalizado todavía por mucho que nos quieran vender la moto) creo que es un síntoma, que vuelvo a insistir, indica no que la maquinaria se esté rompiendo y que algo no funciona sino que está ya rota, puede que tarde cinco, diez o quince años (espero que no tanto) pero es un hecho que llegará, y si hace unos años pensaba que era muy complicado cambiar el sistema, ahora Bitcoin me ha hecho darme cuenta de que no es solo posible, sino que es lo que tiene que pasar si queremos seguir avanzando como sociedad, no hay otra posibilidad.

Y es que hemos pasado del trueque, al uso del oro y del oro, al patrón oro y de allí al empleo del dinero fiduciario, ¿no es hora de que se dé una nueva vuelta de tuerca y avancemos nuevamente?

Hasta ahora los bancos han sido necesarios por su capacidad para hacer llegar el dinero a las personas, financiando Estados y llevándose (como estos últimos) su parte, pero Bitcoin permite que esto no suceda, democratiza el acceso a la moneda a la vez que liberaliza las relaciones económicas entre las partes, y para ello solo necesitas algo tan simple (verás que no es complicado de manejar) como una billetera electrónica y una dirección pública donde recibir y emitir pagos, y por supuesto, un ordenador (o alguno de sus primos hermanos, tableta, móvil, etc.).

ENTONCES…

Tristemente, en España los niveles de corrupción son tan elevados, descarados y mordaces que en los últimos años no paramos de saltar de escándalo en escándalo, y es que solo en 2013, los niveles de corrupción política en España (incluida la casa real) han aumentado solo por detrás de los niveles de corrupción de Siria. Según **el CIS (Centro de Investigaciones Sociológicas)** a los españoles ya nos preocupa más la corrupción política que los problemas económicos. ¿Y son estos los que tienen que decidir sobre el dinero? ¡Dios nos asista!

Es decir, el Estado y la moneda ya no van de la mano, al igual que hace unos cuantos siglos que el Estado y la Iglesia tampoco van de la mano y aunque al principio pudo parecer una aberración, luego se ha demostrado que ha sido una gran decisión.

¡Tío! Esto es imposible que suceda. ¿Seguro? Solamente voy a ponerte un ejemplo, y no voy a insistir más, y es el caso de Argentina, uno de los países más ricos del planeta y completamente arruinado por una sucesión de políticos y dirigentes a cada cual… dejémoslo en menos hábil. Los efectos del corralito argentino han sido portada de noticias en todo el mundo y el debacle económico en los bolsillos de los ciudadanos nadie puede cuestionarlo. Curiosamente es Argentina uno de los países más demandantes de Bitcoines, como un mecanismo para tratar de aliviar la presión a la que están sometidos. Pero esto no lo digo yo, podéis leerlo en *Forbes*, en *Bloomberg* o el *Wall Street Journal*, que con títulos tan sugerentes como "Bitcoin's Promise in Argentina", "Bitcoin Dreams Endure to Savers Crushed by CPI: Argentina Credit" o más recientemente "Bitcoin Downloads Surge in Argentina", analizan esta realidad que tenemos delante de nosotros.

¡Que no, que no son tan ladrones! ¿Seguro? Pues no sé si lo sabrás, pero el FMI se está planteando hacer una quita del 10% a los hogares europeos, una medida que no se tomaba desde el fin de las dos guerras mundiales, dinero que saldría de tu bolsillo para entrar en el del Estado para pagar la deuda; y bueno, si dijéramos que esto resolvería el problema genial, pero es que lo único que se va a hacer es poner un parche más y dejarla a niveles de 2007. Vamos, como lo que se hizo en Chipre, pero para todo el mundo. Y ya veremos por dónde sale la situación griega actual, un enfermo que antes o después acabará por darnos el susto definitivo.

¿Desaparecerán los bancos y los Estados? Presumiblemente creo que no o al menos no del todo y si lo hacen, es de esperar que sea de un modo progresivo, salvo que el poder de la exponencial sea tan dramático que no permita una adaptación paulatina. Desde luego en caso de seguir existiendo, no podrán hacerlo del modo en el que actualmente existen y tendrán que reinventarse y aprender a jugar con las nuevas reglas, y créeme cuando te digo que aún hoy intento imaginar cómo puede ser ese futuro.

Y es que, como decía Albert Einstein el interés compuesto es la fuerza más poderosa que existe en el universo…

1.6 EL INTERÉS COMPUESTO O LA INCAPACIDAD HUMANA DE COMPRENDER LA FUNCIÓN EXPONENCIAL

No sé si os gustará a alguno de vosotros jugar en el casino, a mí personalmente me divierte jugar en estos que han aparecido ahora para móvil, no arriesgas ni un euro (o Bitcoin) si no quieres, y te dan la oportunidad de ver en acción todo tipo de problemas matemáticos y estadísticos que aparecen ligados a la teoría de los juegos de azar (por qué me gustará a mí esto de los juegos tanto).

Una de las maneras que hay de embaucar a la gente para que se enganchen es la famosa **técnica de la martingala** aplicada a la ruleta, seguro que os habrá llegado algún que otro correo del tipo "hazte rico jugando en el casino, técnica imposible de perder", y que consiste en elegir un color (por ejemplo rojo) y apostar un euro, si sale rojo genial, me llevo mi euro más otro que gano, si sale negro pierdo el euro, pero en la siguiente apuesta, lo que hago es apostar dos euros al rojo, doblando la apuesta hasta que por aburrimiento, acabe saliendo el rojo y recuperando el dinero.

Vamos a hacer una tablita muy simple, suponiendo que siempre pierdo:

N.º jugada	Ganancias	N.º jugada	Ganancias	N.º jugada	Ganancias
0	1	3	8	6	64
1	2	4	16	7	128
2	4	5	32	8	256

¿No os recuerda esto a cierto cuento de un tablero de ajedrez y de cierto rey que se quiso pasar de listo, al dar granos de arroz a su inventor?

Al llegar a la jugada n.º 11, para recuperar mi euro inicial tendré que jugar 2.048 euros; a mí personalmente no me sale a cuenta arriesgar 2.048 euros para ganar tan solo 1, pues tiene su cosa, ¿no os parece?; y aunque es cierto que la probabilidad puede ser muy baja, el hecho es que si este sistema fuera infalible los casinos habrían echado el cierre, por no decir que en todos tienen topes máximos de apuesta, por lo que es probable que una cantidad superior a los 600 euros no se pueda apostar a un solo color. Si pintamos la tabla anterior en un gráfico sencillito:

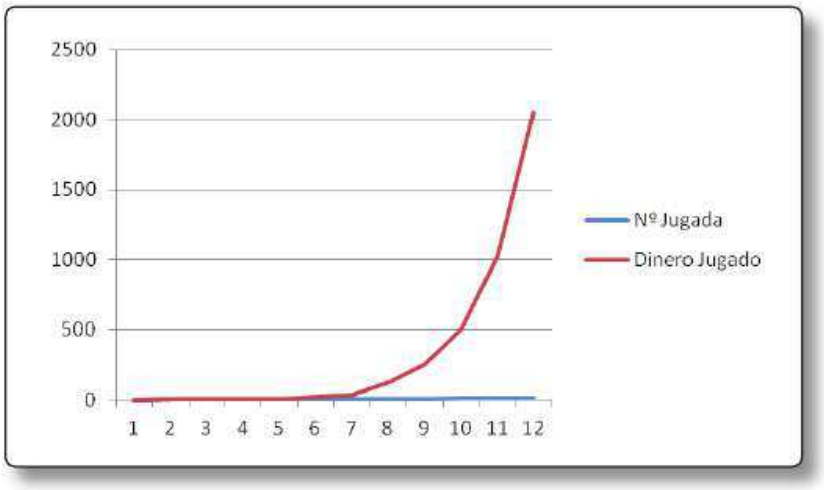


Figura 1.5. Apostando en el casino

Y a poco que os acordéis de las funciones matemáticas básicas que estudiasteis en el colegio, lo que acabamos de pintar tiene un nombre: **función exponencial**, y que curiosamente se parecen a estas otras que tenemos aquí:

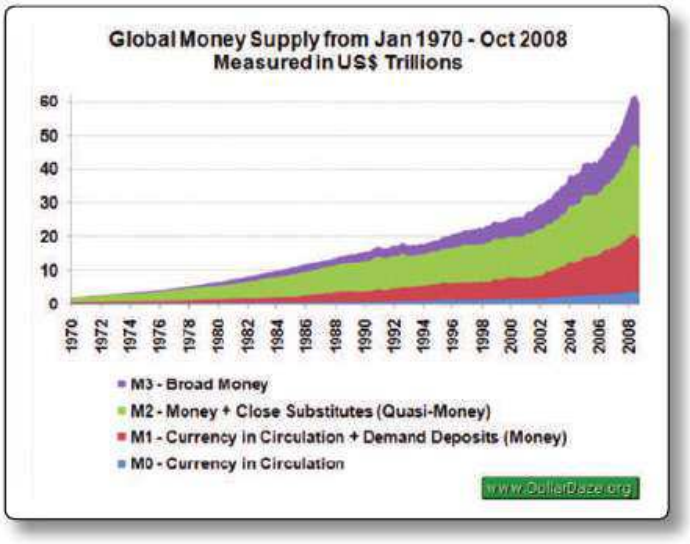


Figura 1.6. Emisión de dinero

El problema es que el jugador, en el corto plazo, ve la exponencial como una función de crecimiento lineal, y es cierto, si nos acercamos a la curva y vemos dos puntos muy próximos efectivamente la sensación es de línea recta y parece que el riesgo es limitado y las variaciones muy pequeñas, pero ¡ay!, cuando se desata el poder de la exponencial, los cambios se producen a tal velocidad, que somos arrollados literalmente por ellos.

Figura 1.7. La exponencial nos engaña

¿Y por qué cuento todo este rollo?, porque esto mismo que acabamos de ver con el juego en la ruleta de los casinos es lo responsable de que no seamos capaces de darnos cuenta de lo que he explicado en el punto anterior, que los intereses crecen a mayor velocidad de lo que la economía puede llegar a producir, y la culpa es del interés compuesto.

Vamos a tirar otra vez de la Wikipedia para definirlo: el interés compuesto representa la acumulación de intereses devengados por un capital inicial (CI) o principal a una tasa de interés (r) durante (n) períodos de imposición de modo que los intereses que se obtienen al final de cada período de inversión no se retiran sino que se reinvierten o añaden al capital inicial, es decir, se capitalizan.

Y se calcula mediante una formulita muy simple:

$$C_{F1} = C_I(1 + r)$$

Vamos a aplicar esto a un euro, cojamos una hoja Excel y hagamos los cálculos para un período de 50 años, en donde el interés va a ser del 10% por ejemplo y seguidamente pintemos la gráfica que nos sale:

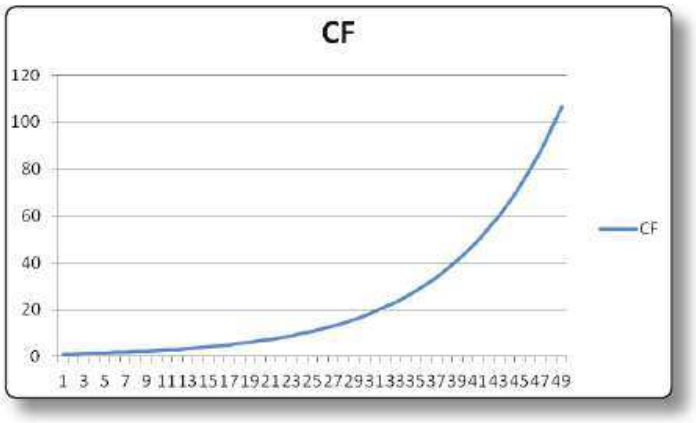


Figura 1.8. Evolución del interés compuesto

Ahora que tenemos esta gráfica vamos a ponerla en contraposición con la gráfica que representa la deuda y que sigue también un crecimiento exponencial.

Vamos a ver, resulta que la deuda sigue una función exponencial, pero es que los intereses siguen también una función de este tipo, la pregunta que hay que hacerse es: ¿se puede crecer a un ritmo exponencial y ser capaces de pagar los intereses generados que también crecen a este ritmo? No es posible y el motivo es muy simple, cada vez hay que destinar más dinero a pagar los intereses generados por la deuda, y como el único mecanismo que nos venden es el del crecimiento económico infinito en un mundo que es finito, pues tenemos un problema de narices. Es cierto que durante un tiempo, la creación de deuda ha servido para crecer y seguir la fiesta, pero es que la fiesta se ha terminado y ahora hay que pagar la cuenta, y ¿sabes quién la va a pagar?, efectivamente, tú y yo que como ciudadanos siempre tenemos que tener la billetera abierta para que los Estados y los políticos incompetentes nos la vacíen.

Y como dijo **Albert A. Barlett** en una frase que personalmente tengo entre mis favoritas:

"El mayor defecto de la especie humana es nuestra incapacidad para comprender la función exponencial".

1.7 EL SISTEMA DE RESERVA FRACCIONARIA

Antes he explicado como los bancos pueden crear dinero mediante el coeficiente de caja y el multiplicador bancario, si esto no te quitó el sueño, probablemente lo siguiente sí que lo haga, porque es el sistema de reserva fraccionaria lo que ha permitido hacer muchos de los desmanes que sufrimos hoy en día, y recordar antes de seguir que cuando hablé de la inflación, dije que una de las misiones de los bancos centrales es la gestión de este tipo de reservas.

El sistema de reserva fraccionaria es el que deja a las entidades financieras dedicar a inversiones y préstamos el dinero que sus clientes depositan en sus cuentas corrientes, estando obligadas únicamente a mantener una fracción del mismo a modo de reservas mínimas para atender las disposiciones de efectivo. Esta fracción es la que hemos llamado anteriormente como **coeficiente de caja**.

El que los bancos puedan hacer esto, dedicar a inversión o a préstamos dinero que no es suyo, es gracias a que los gobiernos lo permiten, y a que se supone que es poco probable que los clientes demanden de forma simultánea una cantidad superior a la fracción que marca el coeficiente de caja. Pero a mí, mi mamá, cuando era pequeño, y mucho más mi abuela Pepa que fue quien me crió, me dijeron que eso de

coger lo que no es mío (por muy loable que sea el fin para el que lo vaya a utilizar) se llama **robar**, o si queremos ser más finos en el habla al menos, apropiación indebida. Y si no recuerdo mal, creo que existen leyes que protegen o al menos deberían proteger de este tipo de cosas.

La **ley de los grandes números** dice que por muy improbable que sea un suceso, si se espera el tiempo suficiente, este acabará por aparecer (en el caso de la ruleta, es raro que salgan doce negros seguidos, pero ¡oye!, puede pasar y, ¿cuánto habría que jugarse para recuperar el euro original en este caso si el casino nos dejase?, cosa que no va a hacer por supuesto). Y fíjate tú por dónde, se ponen a realizar inversiones con poco criterio, la cosa se fastidia y nadie presta a nadie, porque nadie se fía de nadie.

El crear dinero de manera ficticia, y sin un sustento real más que el aire, lleva a donde estamos ahora, a un follón de cuidado en donde aún hay quien nos dice que debemos confiar en los mismos que nos han metido en todo este lío.

Dice un dicho que la primera vez que alguien te engaña es culpa suya, pero la segunda vez que lo hace, la culpa es solo tuya; pues yo digo a este sistema lo siento pero no, gracias.

1.8 ¿TÚ ESTÁS TONTO, O QUÉ?

No, no es que me quiera meter contigo, sin embargo, estoy seguro de que otra de las cosas que habrás oído es que Bitcoin es una burbuja, sí, sí, una burbuja, como lo fueron las empresas .com a finales de los 90 o la vivienda estos últimos años y que nos ha tocado tan de cerca a prácticamente todos los españolitos de a pie. Con estos dos ejemplos puede parecer que las burbujas son un invento reciente, nada más lejos de la realidad, por citar uno de los casos más conocidos solo tenemos que remontarnos al siglo XVII y viajar a los Países Bajos y ver qué sucedió con los tulipanes. La llamada **tulipomanía** hizo que el precio de los bulbos de tulipán se disparara a valores desorbitados. Personalmente creo que con Bitcoin no estamos ante esta situación, pero como siempre vamos a ver de qué va todo esto.

En primer lugar, ¿qué es una burbuja?, una burbuja siempre se produce cuando hay **precios crecientes** en un **mercado abierto** pero que son insostenibles, si queremos podemos decir que están inflados o que son artificialmente falsos, o que se desvían de su precio de equilibrio en el largo plazo.

Y antes de que sigas leyendo quiero comentarte una cosa, hay tantas opiniones serias que dicen que Bitcoin es una burbuja como otras tantas que dicen que no lo es, que es complicado posicionarse de un lado u otro, al menos hasta que

comprendes mejor las connotaciones de Bitcoin. Tal vez lo más razonable sea pensar que con los argumentos y los hechos que conocemos actualmente es difícil saber qué sucederá. El porqué de esta dificultad radica en que determinar si un activo tiene su precio en fase de burbuja no es fácil, sobre todo porque esto implica proyectar hacia el futuro su posible valor. Yo aquí te doy mi punto de vista de por qué considero que Bitcoin **NO** es una burbuja.

Y voy a partir del ejemplo más cercano, como decía en el párrafo anterior, en la vivienda. Los pisos han subido, subido, subido… y la gente ha comprado, comprado y comprado… hasta que ya no se ha podido subir más porque la gente no podía comprar más, o mejor, no se podía endeudar más, porque si se compraba era porque el acceso al crédito era muy fácil. En el caso de los pisos en concreto, era bastante razonable ver que estábamos ante una burbuja (repito, solo en el caso de los pisos); en mi caso particular siempre hacía la siguiente cuenta de la vieja porque es un tema que me ha tocado personalmente: si un piso en una zona de clase media de Madrid vale 300.000 euros, y ese mismo piso se puede alquilar por pongamos 700 euros al mes, o lo que es lo mismo, por 8.400 euros al año, existe una desproporción exagerada que claramente indica que algo no está bien, ¿cómo es posible que algo tan caro se alquile por un precio tan razonable? ¿Habéis tratado de alquilar un coche de lujo? Te crujen vivo y te cobran hasta por mirarlo.

Figura 1.9. Evolución del precio de la vivienda en España

Es decir, estar en fase de burbuja significa que el precio de algo hoy es desproporcionado con el precio que tendrá en el futuro. En el ejemplo de los pisos se ve muy bien, el piso anterior vale 300.000 euros, en 5 años ¿cuánto valdrá?, ¿1.000.000 de euros?, ¿nos hemos vuelto locos? Pero si el salario de un español medio es de 1.000 euros, ¿cómo va a pagarlo por mucho que se endeude? ¿Habrá un tonto que en 5 años vaya a poder comprarlo? La respuesta en este caso era obviamente

no. Pero como siempre digo, analizar datos y situaciones económicas a toro pasado siempre es muy fácil.

ENTONCES…

Por no decir, las voces "serias" que de vez en cuando aparecen por ahí y dicen cosas que resultan difíciles de entender. Por ejemplo, el economista jefe de Citi, **Willem Buiter**, argumenta que el oro es una burbuja de **6.000 años de duración**.

A diferencia de lo que sucede con las estafas piramidales o con el esquema Ponzi, no es necesario que exista una persona, ente o como quieras llamarlo, detrás de la burbuja para que esta se produzca, aunque en ocasiones basta con que haya ciertos entes que actúen como "animadores", como pasaba con los bancos. ¿Necesitas el 80% de la hipoteca? No pasa nada, te doy el 120% del valor del piso y te compras también el coche y te vas de viaje, y además así te crees que eres rico y presumes ante tus amigos. Esto es completamente verídico y si has vivido en España los últimos años sabrás que no miento.

Independientemente de lo anterior, lo que sí se necesita para que una burbuja exista es de tontos, personas que con un comportamiento optimista compran activos sobrevalorados anticipando su venta a especuladores a un precio aún mayor. La burbuja crece mientras los tontos van encontrando otros tontos que compran el activo sobrevaluado y además encarecido por el tonto de turno que lo posee y quiere vender, y termina cuando el más tonto se convierte en el que más ha pagado por el activo y no encuentra a nadie más que pague por lo que compró a un precio mayor. Probablemente, en esta cadena de tontos, los tontos intermedios no deban considerarse como tontos, al fin y a la postre consiguen hacer negocio y sacar su parte, pero la **teoría del gran tonto (**o **greater fool theory)** los considera como tales.

Y ¿qué sucede con Bitcoin? Para explicar la situación vamos a recordar algunos conceptos que ya he explicado anteriormente: el primero el de la utilidad no monetaria del teorema de la regresión de Mises y que decía que para que un bien se utilice como medio de intercambio debe tener una demanda no monetaria que sirva para fijar su precio inicial (como el oro).

Por otro lado, también hablamos de volatilidad, esa medida que nos indica la variación del precio de un activo, y que para el caso particular de Bitcoin ya hemos dicho que es muy alta. Y también conté las características del buen dinero, y en este caso nos vamos a quedar con tres de ellas que son la de depósito de valor, unidad de cuenta y medio de cambio.

¿Qué dirá alguien que ve a Bitcoin como una burbuja?

"Uf, cómo sube esto, qué rápido va la cosa, esto tiene truco".

Y además pensaría:

"No hay valor no monetario, no es posible establecer su precio inicial, por tanto, su valor real es 0 (fuera del sistema de intercambio no sirve para nada) y además está esa alta volatilidad, no me gusta nada".

Y acabaría concluyendo:

"Nada, nada, estamos ante una burbuja, no puede ser que algo que está a 50 dólares hoy, valga 1.000 dólares mañana".

¿Pero tiene sentido esto? O sea, ¿que un activo suba muy rápido significa siempre que hay burbuja? Echemos un vistazo al mercado de valores y encontraremos muchos ejemplos de empresas cuya cotización ha subido como la espuma y nunca ha bajado y no por ello estaban en una fase de burbuja. O volviendo a las .com, muchas empresas se fueron al garete, pero otras muchas se revalorizaron y sobreviven hasta el día de hoy (¿verdad, Amazon?).

Pero es que Bitcoin no es como los pisos o como las acciones de las empresas porque es un tipo de activo diferente, es un activo monetario. A ver si logro explicarlo, cuando un activo está en burbuja significa que en el futuro, la demanda de dicho activo va a caer y por tanto no podré deshacerme de él porque nadie lo querrá, sin embargo, con un activo monetario pasa justamente lo contrario, cuanta más gente lo demanda hoy como activo monetario (y no se puede negar este hecho con Bitcoin), más se estabiliza como tal y por tanto más gente lo demanda mañana (el efecto red, hablaré más adelante de él). Es decir, si Bitcoin hoy es demandado y la gente lo utiliza y la masa de gente que lo acepta crece y a la vez crece el número de sitios que lo aceptan, a futuro lo que sucederá es que este efecto no solo no se reducirá, sino que todo lo contrario se extenderá y generalizará, y aumentará su proceso de monetización, por el simple hecho de que Bitcoin está demostrando que funcionará como un medio de intercambio mejor que otros (y eso sin añadir los usos no monetarios que tendrá a futuro).

En los medios cada vez que Bitcoin sube y cae, enseguida aparece una noticia anunciando el pinchazo de la burbuja, y el fin de la moneda, por ejemplo no hace mucho fue **Robert Shiller**, profesor de economía de la Universidad de Yale y premio Nobel de Economía en 2013 quien hizo esa misma afirmación. Sin embargo, y con el máximo respeto hacia el profesor Shiller, otra vez la tozuda realidad demuestra que Bitcoin supera los **test de estrés** a los que se le somete: superó los ataques a Mt. Gox y su cierre, ha superado los robos de claves, sobrevive a Silk Road, a la prohibición

de Tailandia, a la oposición de China, y superará cualquier otro obstáculo que se le presente.

¿Habrá correcciones en su precio y caídas importantes? No solo es posible sino que es seguro, decir lo contrario sería absurdo y no tener los pies en la tierra, pero cada vez serán menores y más espaciadas en el tiempo.

Tú y yo a medida que usamos y popularizamos Bitcoin contribuimos a que eso ocurra antes.

1.9 ALGUNAS CURIOSIDADES HISTÓRICAS

Anécdotas e historias en donde el dinero es el protagonista hay muchas a lo largo del tiempo, sin embargo no podemos recopilarlas todas, ya me gustaría a mí por lo interesantísimas que son muchas de ellas, así que he decidido hacer un pequeño sacrificio y me he quedado con las que pueden presentar algún punto de particularidad aplicable a todo lo que hemos visto a lo largo de este capítulo.

Y vamos a comenzar con dos ejemplos de hiperinflación que deben servir de toque de atención del peligro que esta supone, y deberían prevenirnos de hasta qué punto estamos ante un acto que debería ser considerado como terrorismo de Estado hacia sus ciudadanos, porque por mucho que digan que por crear papel no pasa nada y que está controlado, podemos vernos como ya se vieron otros. Esperemos que conocer la historia, sobre todo errores sobradamente documentados, nos ayude a no volver a meter la pata.

1.9.1 La hiperinflación de Hungría y de Zimbabue

El caso más bestial de **hiperinflación** que jamás se haya producido es el que sucedió en Hungría durante 1946. La Segunda Guerra Mundial había terminado, y Hungría estaba en una situación muy difícil, fundamentalmente por la deuda de 300 millones de dólares (de 1946, no perder el referente) que debía a la URSS en concepto de **indemnización por la guerra**. La solución que se le ocurrió al gobierno de turno fue imprimir papel moneda con el objeto de estimular el crédito a un interés barato y reconstruir la economía, pero el efecto que tuvo fue todo lo contrario.

No es raro que esto sucediera, la masa monetaria creada carecía de ningún respaldo por detrás, no había metales preciosos ni bienes que el Estado pudiera poner como avales del papel emitido. Y pasó lo que tenía que pasar, un alza incontrolable de los precios hasta límites que rozan lo absurdo.

Por poner un ejemplo de la situación en que derivó la hiperinflación húngara, pensad que en 1941 una barra de pan costaba 1 peng, en abril de 1946 una rebanada de pan (¡UNA REBANADA!) costaba 450.000 pengs, y en julio de 1946 esa misma rebanada costaba 6.000 millones de pengs. Y aunque los salarios se incrementaban a la par que la inflación, no servía para nada, porque el sobrecoste se trasladaba al consumidor (recordar que esto ya os lo decía antes cuando explicamos la inflación).

Se llegó a una situación tan estrafalaria, que los salarios se llegaban a pagar cada cuatro horas, siendo en los casos más extremos de varios trillones de pengs. Algunas empresas llegaron a instaurar el llamado "salario calórico", un modo poético de decir que se pagaba con comida. En agosto de 1946 todo el dinero circulante en Hungría valía la décima parte de un centavo de dólar, con una inflación de 42 mil billones (con b).

Figura 1.10. Billete de mil trillones de pengs (nunca llegó a ser emitido, aunque sí impreso)

No fue hasta que se eliminó el peng y se sustituyó por el **florín** y su respaldo en oro, cuando se eliminó el problema de la inflación húngara.

Que el ser humano es el único animal que tropieza dos veces con la misma piedra es un hecho, porque si de algo debería haber servido lo sucedido en Hungría es que para hacer experimentos mejor hacerlos con gaseosa. Pero en **Zimbabue**, el tirano **Mugabe** no está por las lecciones de historia, y ha sido el primero en hacer que su país ostente el título de primer caso de hiperinflación del siglo XXI.

Y es que lo sucedido es más o menos lo que pasó en Hungría, una emisión desmesurada de papel destinada a pagar a los funcionarios públicos y al Ejército, y políticas agrarias erráticas hicieron que entre 2005 y 2006 los precios se multiplicaran por mil. Para paliar la situación, se creó una nueva moneda, el "nuevo dólar de Zimbabue", cuyo valor equivalía a 1.000 dólares del "antiguo dólar de Zimbabue". Para principios de 2008 el valor de los dólares era ridículo, y estaba tan depreciado que se tuvieron que emitir billetes por valor de 10 millones de dólares (unos 4 dólares americanos), seguidos de billetes por valor de 50 millones (abril) y de 100 y 250 millones (mayo), alcanzándose los 50.000 millones por billete en 2009.

La imagen siguiente:

Figura 1.11. NO ZIM DOLLARS, no tirar al WC dólares de Zimbabue

es el resumen perfecto para ilustrar el dicho de "no vale ni el papel en el que está impreso".

1.9.2 La Operación Bernhard

Siempre he pensado y muchos también coincidiremos en esto, que es en períodos de guerra cuando gran parte del ingenio humano sale a la luz, el instinto de supervivencia aflora y hace que salgan de nosotros todas nuestras capacidades, tanto las buenas como las malas. La Operación Bernhard es uno de estos ejemplos de ingenio, ya que estamos ante la mayor falsificación monetaria de todos los tiempos, y además realizada por un Estado. Es muy probable que el curso de la Segunda Guerra Mundial hubiera dado un giro si el Gobierno británico no hubiera adoptado la decisión que adoptó; pero veamos qué fue lo que sucedió…

Situémonos por tanto en plena Segunda Guerra Mundial, corría el año 1942 y los alemanes buscaban una forma de acabar con Gran Bretaña de un modo total. A parte de los frentes bélicos abiertos, se pensó en cómo asestar un golpe económico al país que resultase irreparable. En aquel entonces, el Servicio de Seguridad alemán tenía lo que se llamaba el **Departamento de Sabotaje**, y fue allí donde se gestó la idea de inundar el mercado británico con una enorme cantidad de papel moneda falsificado.

Para hacerlo, se necesitaba emitir unos 100 millones de libras esterlinas, preferiblemente en billetes de baja denominación (billetes de pequeño valor) y hacerlos circular por los diferentes países, distribuidos por los servicios secretos alemanes. El encargado de llevar a cabo el plan fue el comandante en jefe de la S.S. **Heinrich Luitpold Himmler**, ya que era uno de los que más agentes de campo tenían, y podían hacerse cargo de la puesta en circulación de los billetes.

Himmler le asignó la responsabilidad (y poderes prácticamente ilimitados) a un mayor del Ejército experto en falsificaciones, **Bernhard Krüger** (**Krueger**) y de ahí el nombre que recibió la operación (**Unternehmen Bernhard**). El equipo que conformó Bernhard para el proyecto fue verdaderamente increíble, por un lado estaba **Alfred Naujocks**, encargado de las falsificaciones en los servicios de seguridad y que contaba a su vez con un equipo de profesionales especialistas en grabado, papel, tinta, impresión, etc. Pero lo más sorprendente fue la otra parte del equipo, en ella estaban los mejores falsificadores del momento, incluidos delincuentes procesados que estaban en el campo de concentración de Sachsenhausen, que acabó por establecerse como el centro de operaciones. En total 142 expertos dedicados en exclusiva a esta tarea.

Como primera misión del equipo estaba crear la réplica del papel que se usaba en las libras, tenía que ser tan perfecto que pudiera pasar las pruebas táctiles y análisis técnicos de la época. Como Gran Bretaña obtenía sus materias primas de las colonias, los alemanes hicieron lo mismo, encontrando una tela de algodón que se importaba de Turquía y que se usaba para la confección de trapos de limpieza, que después de ser tratada químicamente, servía para fabricar un papel idéntico en calidad, textura, brillo y color al original. Una vez que se tenía el papel, se hicieron las filigranas, marcas de agua, errores de impresión y se descubrió el código para generar los números de serie válidos.

Una de las ideas era lanzar los billetes desde un avión sobre el país, pensando en que solo unos pocos los entregarían a las autoridades y la mayoría se los quedaría, pero este plan se descartó, porque a la larga los británicos podrían controlar la situación. Así que se comenzaron a introducir mediante transacciones de prueba en el sistema financiero sin que nadie se diera cuenta, llegando días más tarde a través de los mercados internacionales hasta Inglaterra. Ante el evidente éxito, se decide trasladar la fabricación al campo de concentración de Oranienburg, para su producción en serie, confeccionándose un total de 8.965.080 notas de banco perfectas e iguales a las originales y que equivalían a **134.610.810,00 libras**, en billetes de 5, 10, 20 y 50, dejando en reserva los billetes de 100, 1.000 y 5.000 libras.

La colocación de esta cantidad de dinero en el mercado fue llevada a cabo por **Friedrich Schwend** (más conocido como **Dr. Wendig**), un multimillonario que usó sus negocios para poner en circulación el dinero. Al cabo de cierto tiempo, el dinero acabó llegando a Gran Bretaña, siendo un empleado del Banco de Inglaterra el primero en darse cuenta del engaño, al encontrar un billete con el mismo número que otro en el registro de billetes devueltos.

Al detectarse la falsificación, el Gobierno británico se enfrentó a un enorme dilema, y era qué hacer ante esta situación. Había dos posibilidades, una detener la circulación de los billetes falsos, afrontar el pánico de los mercados internacionales,

y quebrar la economía británica (no debemos olvidar la deuda que Gran Bretaña tenía con Estados Unidos, y esta noticia habría resultado letal), y la otra posibilidad era aceptar los billetes como legítimos y seguir usándolos en el mercado internacional como si nada, decisión que fue finalmente adoptada, de manera que billetes falsos y auténticos estuvieron circulando juntos, declarando **Churchill** este asunto como secreto de Estado. Hasta el punto de que cuando en los **Juicios de Núremberg** se intentó juzgar a algunos detenidos por delitos de falsificación, los propios británicos desestimaron los cargos, alegando que los billetes eran legítimos y se negaron a que se les juzgara por este motivo.

En cualquier caso, sea como fuere, el Banco de Inglaterra eliminó los billetes mayores de 5 libras de manera progresiva y no fue hasta pasados los años 60 cuando se volvió a poner en circulación billetes nuevos, los últimos, de 50 libras en 1980.

Si durante la Segunda Guerra Mundial hubiera existido Bitcoin, los alemanes lo habrían tenido realmente difícil para poder falsificarlo, **s**alvo que controlasen el 51% del poder computacional de la re**d**, y no es que sea realmente sencillo de conseguir.

Por cierto, la película *The Counterfeiters* (*Los falsificadores*) centra su argumento en la Operación Bernhard, os recomiendo que la veáis porque no está mal.

1.9.3 Prohibiendo que algo queda

No hace apenas unos meses llegó a mis manos la siguiente noticia: "Tailandia prohíbe la venta de Bitcoin al no considerarla moneda de cambio" ¡Toma ya!, no puede decirse que en este caso no estemos ante una injerencia directa por parte del Estado, ¿verdad? Tampoco es que nos sorprenda.

Como el titular de la noticia dice, el Banco de Tailandia ha prohibido la venta de Bitcoines al no considerarla moneda de cambio y debido a la falta de políticas para regular y controlar esta divisa. Lo más importante de todo esto es que se prohíbe y se considera ilegal utilizar esta divisa para la compra-venta de bienes o servicios en Tailandia, y además también lo es recibir o emitir transferencias al extranjero. Todo ello ha sucedido dos meses después del intento fallido de registrar la moneda en el país para poder operar de manera legal operaciones que están reguladas por el Banco de Tailandia.

Aquí se pone el dedo en la llaga, el quid de la cuestión está en la palabra control, ¿cómo controlamos a Bitcoin? Es como preguntar ¿cómo le ponemos puertas al campo?, la revolución es imparable, no ha hecho más que comenzar y

como Internet, nadie podrá pararla, quizás obstaculizarla como ha sucedido con otras redes como BitTorrent, pero que a la larga no ha servido para nada.

Pero esta situación que se ha dado en Tailandia y que he usado como excusa para iniciar este apartado no es la única, **China** a principios de diciembre de 2013 prohibió el negocio de Bitcoin a las instituciones financieras, indicando que la moneda no era una amenaza para el sistema financiero todavía, pero que había que verla como un riesgo a tener en cuenta a futuro, aunque no prohibió las operaciones entre particulares. Más tarde, entre el 15 y el 18 de abril de 2014 los bancos chinos han decidido cerrar las cuentas que los operadores de Bitcoin tenían abiertas allí, como son los casos de **Huabi.com** con el **Banco Industrial y de Comercio de China o BTC Trade con el Banco Agrícola de China**. Sin embargo, ahora se baraja que **China**, **Noruega**, **Corea del Sur**, **Francia**, **Alemania**… la lista es extensa, pero todos en mayor o menor medida ya se encuentran levantando la bandera roja, y advirtiéndonos de que esto de ir por libres y hacer que el Estado pierda su mayor juguete de control de los ciudadanos, será una batalla que habrá que librar. También la **Autoridad Bancaria Europea (EBA)** se ha posicionado diciendo, en este caso, que el dinero sin regulación (o mejor dicho, **SIN** su regulación, Bitcoin se autorregula solo, gracias) es susceptible de ser atacado por *hackers* expertos, y se quedan tan anchos, como si las entidades financieras no fueran víctimas de ataques de este estilo, o no se falsificaran tarjetas y billetes.

El último país en poner su granito de arena ha sido **Rusia**, quien a principios del mes de febrero de 2014 declaró Bitcoin ilegal y junto con la suspensión de la cotización de Mt. Gox por "problemas técnicos", hizo que el valor de la moneda cayera hasta algo más de los 400 dólares.

ENTONCES…

Sin citar que recientemente el Ministerio de Finanzas ruso ha presentado una propuesta de ley para penar con hasta cuatro años de cárcel la compraventa de Bitcoines y la minería.

En **España** todavía no hay nadie que se haya posicionado de un modo claro, hay una nota informativa del Banco de España en donde más que nada se insiste en los problemas que supone Bitcoin, más que en sus posibles ventajas y oportunidades. Aunque se ha dado algún paso en la buena dirección como no gravar con IVA a Bitcoin ni a las criptomonedas, en este sentido, sitúa las operaciones realizadas con Bitcoines dentro del ámbito de las operaciones financieras, y las empresas que en

nuestro país realicen actividades usándolo tienen que acogerse y cumplir con las medidas de protección de blanqueo de capitales que el Estado provee.

El documento más serio que podéis encontrar sobre la situación de Bitcoin en el mundo es el que pertenece a **la Biblioteca de Derecho del Congreso de los Estados Unidos**, que hizo un estudio titulado *Regulation of Bitcoin in Selected Jurisdictions* en donde analiza la situación de Bitcoin en 40 países diferentes; personalmente creo que se ha quedado obsoleto y os recomiendo para mantenerse actualizado de manera *online* que lo mejor es echar mano de la web *www.bitlegal.net*.

Curiosa ha sido la reacción del congresista de los EE. UU. **Jared Polis** que a modo de sátira ha enviado una carta al Departamento del Tesoro afirmando que:

"El intercambio de billetes de dólar está actualmente desregulado y ha permitido a los usuarios participar en actividades ilícitas", como compra de bienes ilegales, transacciones anónimas o fraude fiscal, y, además, "puede ser objeto de falsificación, robo y pérdida".

Y pide que se actúe con rapidez y además:

"Prohibir esta peligrosa moneda que podría dañar a la clase trabajadora estadounidense".

Como he dicho anteriormente, el acceso a una actividad ilegal es independiente del mecanismo monetario que se utilice.

Es además en EE. UU. donde se está trabajando en una **BitLicense**, que no deja de recibir críticas porque de quedarse como está, no será más que un freno, un obstáculo para la innovación y un sacacuartos, porque aquel que quiera trabajar acorde a la ley, tendrá que obtener la licencia, por el módico precio de 5.000 dólares, algo que para cualquier *startup* pequeñita no sería más que un problema.

Otro ejemplo claro de las intromisiones que se hacen para obstaculizar el avance de Bitcoin lo tenemos en **Australia**, donde algunos bancos han llegado a congelar y cerrar las cuentas de los operadores de Bitcoin implantados en el país de los canguros. Entre algunas declaraciones hechas, me quedo con la de Matthew Canavan ante el Senado donde dijo y cito textualmente: "estas startups son obvias desestabilizadoras del modelo del negocio bancario". De momento la Comisión Australiana de Competencia y Consumo (ACCC) va a investigar lo sucedido para ver si están ante un caso de lo que parece, claramente, competencia desleal.

Pero hay luz al final del túnel. La iniciativa que me parece más llamativa por parte de un gobierno es la que desde el **estado americano de Utah** han hecho, al

aprobar un proyecto de ley que permite a los residentes de este estado el pago de sus impuestos con Bitcoines. De momento solo es un proyecto de ley y puede acabar en nada, pero la iniciativa por sí misma denota una preocupación cada vez mayor por el uso de Bitcoin que trasciende a los frikis y al usuario medio de a pie que ya lo utiliza. También, en este sentido, la decisión del **Tribunal de Justicia de la Unión Europea** que ha dictado sentencia declarando a Bitcoin y a cualquier otra moneda libres de impuestos, y que recibirán el mismo tratamiento que el resto de monedas que están en circulación en el mundo.

ENTONCES…

Y la situación se agrava, los desgraciados atentados de París tendrán dos víctimas colaterales adicionales, porque se planea una ofensiva contra **las monedas virtuales y el oro**, a los que se les acusa de ser el medio de financiación del terrorismo. Sin embargo, echad un vistazo al siguiente cuadro, de la Agencia Tributaria del Reino Unido (un organismo bastante serio *a priori*) donde en su "Evaluación de riesgos nacionales en el Reino Unido del lavado de dinero y el financiamiento del terrorismo", las criptomonedas ocuparían el último lugar.

Table 1.A: National risk assessment on money laundering

National risk assessment on money laundering						
Thematic area	Total vulnerabilities score	Total likelihood score	Structural risk	Structural risk level	Risk with mitigation grading	Overall risk level
Banks	34	6	211	High	158	High
Accountancy service providers	14	9	120	High	90	High
Legal service providers	17	7	112	High	84	High
Money service businesses	18	7	119	High	71	Medium
Trust or company service providers	11	6	64	Medium	64	Medium
Estate agents	11	7	77	Medium	58	Medium
High value dealers	10	6	56	Low	42	Low
Retail betting (unregulated gambling)	10	5	48	Low	36	Low
Casinos (regulated gambling)	10	3	32	Low	24	Low
Cash	21	7	147	High	88	High
New payment methods (e-money)	10	6	60	Medium	45	Medium
Digital currencies	5	3	15	Low	11	Low

1.9.4 Silk Road

Hablar de Bitcoin y no hacerlo de Silk Road dejaría cojo este libro. Silk Road es otro de los casos que más notoriedad han tenido en estos últimos meses, no solo por el hecho de dedicarse a la venta de drogas por Internet sino porque han aprovechado que parte del dinero incautado ha sido en Bitcoines para criminalizar el uso de Bitcoin y propagar (otra vez) que es la moneda del delito, ¡vamos, como si con los dólares americanos no se financiara el narcotráfico!

Silk Road fue creado por **Ross William Ulbricht**, aunque era más conocido por el sobrenombre de **Dread Pirate Roberts**. El *site* inició sus andaduras en Internet en febrero de 2011, después de un período de pruebas de tres meses. Al sitio los compradores podían registrarse de manera gratuita, mientras que los vendedores accedían al sistema previa adquisición de una cuenta vía un proceso de subasta, con el fin de evitar un acceso indiscriminado al servicio y asegurar la calidad de los productos vendidos. Se intentaba con esto filtrar que personas malintencionadas, distribuyeran productos contaminados o adulterados. De todas las ventas, el pirata Roberts se llevaba una comisión.

La mayor parte de lo que Silk Road vendía está considerado como contrabando en prácticamente todo el mundo, y era posible adquirir productos tan saludables como la heroína, el LSD o el cannabis, por citar algunas de las drogas más conocidas. Es curioso que la página no permitiera la venta de productos destinados a dañar a otros, los números de tarjetas de crédito, información personal de terceros, contratar asesinos o las armas de destrucción masiva, no estaban en el catálogo de venta. Entre algunos de los motes graciosos que han puesto a Silk Road está el de **National Public Radio**, que lo bautizó como el "Amazon de las drogas", o el también "simpático eBay de drogas escondido en un rincón oscuro de Internet conocido como Tor", que le atribuyó *The Economist*.

Y he aquí donde aparece Bitcoin en escena, puesto que compradores y vendedores realizaban sus operaciones de compra y venta usándola, con un 99% de satisfacción entre las partes. ¡Toma ya! Y como el anonimato está casi garantizado, pues qué podemos decir, el éxito era rotundo.

Figura 1.12. Imagen que encontramos en Silk Road después de su cese de actividad

Es probable que de no haber tenido tanto éxito, los senadores norteamericanos **Charles Schumer** y **Joe Marchin** no hubieran enviado cartas al procurador general Eric Holder y a la responsable de la Administración Federal del Control de Drogas, **Michelle Leonhart**, solicitando la toma de medidas tanto contra Silk Road, como contra el software Tor y por supuesto Bitcoin.

Hay quien afirma que la motivación de Silk Road está en demostrar la posibilidad de poder comerciar de manera libre con todo tipo de bienes individuales, aprovechando las barreras tecnológicas que proporciona Internet. Es muy curioso el perfil de su creador en LinkedIn, porque va en este sentido. En él, aparte de hablar de sus logros académicos, habla de cómo han cambiado sus objetivos y quiere utilizar la teoría económica como un medio para abolir el uso de la coacción y agresión contra las personas, centrando su atención en los gobiernos como principales causantes de estos problemas, y diciendo que para cambiar la forma de gobernar, hay que cambiar primero las mentes de las personas que son gobernadas. Pero no se queda solo en esto, sino que añade que se encuentra trabajando en una simulación económica para proporcionar a las personas una experiencia en primera mano de lo que sería vivir en un mundo sin el uso sistemático de la fuerza. Aunque todas estas afirmaciones quedarían en nada si se llegara a demostrar que Roberts contrató a un sicario para acabar con la vida de un empleado de Silk Road, que supuestamente habría robado una cantidad de dinero de la empresa antes de desaparecer y ser detenido por la policía. Y aunque el asesinato no se llegó a llevar a cabo, porque el sicario contratado resultó ser un policía, la cuestión está pendiente. Teniendo en cuenta la naturaleza del catálogo de productos que ofrecía Silk Road, no destinados a dañar a terceros, al menos queda la duda.

¿Manipulación? ¿Verdad? ¿Quién mató a Kennedy? ¿Silk Road es una simulación? El debate está abierto y lo dejo aquí para que podáis también reflexionar sobre ello. Si tenéis un rato, no dejéis de leer el siguiente artículo, en donde se ponen en entredicho los métodos usados por el FBI en esta investigación:

http://techcrunch.com/2014/10/02/expert-witness-for-silk-road-suggests-fbi-lied-about-how-they-accessed-back-end-servers/

Para rizar el rizo en toda esta historia, que es digna de un guión para una película en Hollywood, resulta que ahora han aparecido dos científicos israelíes, Dorit Ron y Adi Shimer, que afirman que es posible establecer una relación directa entre Satoshi Nakamoto (el misterioso creador de Bitcoin) y Silk Road. Esta afirmación se basa en que la mayor parte de las transacciones que se realizaban en Silk Road son de un monto relativamente pequeño, sin embargo, hay una transacción de 1.000 Bitcoines que se realizó desde una de las primeras direcciones creadas al inicio del proceso de minería de Bitcoin, que va a parar curiosamente a una de las direcciones supuestamente controladas por Silk Road. Entradas posteriores en Reddit desmentían esta posibilidad y negaban que pudiera ser cierta, pero para los paranoicos la semilla ya estaba plantada.

ENTONCES…

Usando análisis basado en heurísticas, los investigadores Ron y Shamir fueron capaces de establecer esta relación. Poco después el propietario de los Bitcoines a los que se llegó tras realizar este trazado desmintió esta conexión. No obstante, la capacidad de trazado probada es completamente válida como explicaremos en el capítulo 4

Lo paradójico del asunto es que dado que el **Servicio de Impuestos de EE. UU. (IRS)** emitió hace poco un resolución afirmando que Bitcoin debe ser tratado como una propiedad y no como dinero, el abogado de William Ulbricht ha pedido que se retiren todos los cargos, porque si Bitcoin no es dinero, ¿cómo podemos acusar a alguien de blanqueo? Desde luego, una muestra más de que quienes nos dirigen lo hacen con los pies y no con la cabeza.

Y ¿sabes lo mejor de todo y que demuestra que no se le pueden poner puertas al campo? Ya existe **Silk Road 2.0**, una versión mejorada de la difunta Silk Road y en donde se puede volver a comprar todo tipo de sustancias ilegales de manera anónima (incluso su administrador se hace llamar igual). Ross Ulbricht ha sido condenado a cadena perpetua y los Bitcoines encautados subastados, sin embargo, tal y como sucedió con el intento de evitar las descargas ilegales, Napster murió (bueno, realmente evolucionó) pero con él no murieron las descargas, y sucederá siempre mientras Internet exista, el único modo de acabar con este tipo de cosas es apagándola, pero aun así, estoy seguro de que en el caso de que gobiernos intentaran cerrar la Internet oficial, una Internet paralela surgiría, es inevitable. Es lo que tiene la libertad, que como la vida, siempre busca caminos de salir adelante.

ENTONCES…

Mientras se deciden o no a hacer la película, podemos abrir boca con el documental *Deep Web* de **Alex Winter**, donde entre otros temas se habla de Silk Road y de la web oculta.

Como remate final, la historia de Silk Road ha sacado a la luz los trapos sucios de un exagente de la DEA (Administración de Control de Drogas), de nombre **Carl Mark**, que ha sido condenado a 78 meses de prisión por robar Bitcoines de esta web. Pendiente está la sentencia de su colega en diciembre de 2015, el también agente **Shaun W. Bridges**. Entre ambos sustrajeron más de un millón de dólares de Silk Road. A estos dos nombres debemos también añadir el de **Roger Thomas Clark**, un canadiense de 54 años apodado **Vanity Jones**, también acusado de participar en los oscuros negocios de la "siniestra" web y ser asesor principal de Ulbricht.

2

EL DINERO ELECTRÓNICO Y BITCOIN

Hay quien dice (yo mismo no hace demasiado tiempo también lo pensé) que las tecnologías disruptivas del siglo XXI serían fundamentalmente cuatro: el desarrollo móvil (incluyendo los *wereables* y también el Internet de las cosas), el *big data*, el *cloud computing* y todo lo que tiene que ver con el *social media*. Sin embargo, y sin quitar valor a estas, diría que serán las criptomonedas, la descentralización y la inteligencia artificial las verdaderas revoluciones de este siglo, y a partir de ahí, si queremos las anteriores.

Bitcoin y la tecnología de la cadena de bloques son el aceite necesario que debería convertirse en el facilitador de la libertad de los individuos y del incipiente nacimiento de un nuevo orden económico y social. Orden, que dependiendo de cómo se orqueste será el que determinará cómo evolucionará el resto de tecnologías, aunque esto obviamente dependerá del punto de vista del que lea esto y podríamos debatir largo y tendido sobre ello. Lástima del espacio limitado que tenemos.

En cualquier caso, lo dije antes y lo repito otra vez, aunque Bitcoin fuese un experimento monetario fallido, la cadena de bloques estará ahí todavía para nosotros con su poder para desarrollar nuevas aplicaciones y servicios. Y no solo es algo que diga o vea yo, es que en estas últimas semanas, los acontecimientos que han sucedido y que han tenido a Bitcoin y las criptomonedas como protagonistas son sumamente importantes. Por hacer un símil ajedrecístico, poco a poco, pero con paso firme, los grandes jugadores de este mundo van posicionándose respecto a Bitcoin y van colocando sus piezas en una partida que nada tendrá que envidiar a la que Kasparov y Deep Blue jugaron hace dos décadas.

¿No me crees? Bueno, pues qué te parece lo siguiente:

- Empecemos por **PayPal**, la famosa compañía de procesamiento de pagos propiedad de eBay, que permite que los comerciantes puedan aceptar el pago de las ventas de sus artículos usando Bitcoines gracias a su integración con **Braintree** y sus asociaciones con **Coinbase**, **BitPay** y **GoCoin**. Aunque no es una noticia novedosa porque fue anunciado en septiembre del año pasado, tiene su importancia porque es una realidad y está ya en funcionamiento.

- Otras dos de las empresas grandes que andan detrás de la tecnología de la cadena de bloques y del uso descentralizado de la tecnología son, nada más y nada menos, que **Samsung** e **IBM**.

  El director de estrategia en la división de investigación de Samsung, **Steven Rahman**, afirma que la empresa está examinando cómo la *blockchain* puede utilizarse para asegurar la autenticidad de lo que cualquiera dice que es auténtico, y habla de cómo el uso de Bitcoin como moneda es solamente la punta del iceberg, y deja entrever algo de lo que hablaremos más adelante, el establecimiento de contratos sin necesidad de terceros de confianza. Pone como ejemplo una receta médica, pero no da más detalles de lo que Samsung puede traerse entre manos, pero teniendo en cuenta que esta división suele trabajar con tecnologías que pone en la calle en un plazo de entre 2 y 5 años, puede que dentro de poco veamos novedades importantes.

  Tal vez más clara está la alianza entre Samsung e IBM y la plataforma **ADEPT** (*Autonomous Descentralized Peer to Peer Telemetry*, algo así como Telemetría Autónoma Descentralizada entre pares) y que parece podría aplicarse para crear un red distribuida de dispositivos para el Internet de las cosas.

- Los bancos tampoco son ajenos a Bitcoin, y están comenzando a verlo como algo muy serio y una alternativa real al sistema tradicional, y en algunos casos se ha pasado de verlo más que como una amenaza, como una oportunidad de mejora de sus operaciones, aunque con ciertos matices que ahora indicaré.

  Los artículos "One Bank Research Agenda" y "Old Money, New Money" realizados por el **Banco de Inglaterra**, "The Future of Finance: Redefining the Way We Pay in the Next Decade" de Goldman Sachs o "Bitcoin-Money without fisical form" de **Credit Suisse** son algunos ejemplos notorios que no deberías dejar de leer en cuanto tengas ocasión, porque apuntan en este sentido que estoy comentando.

> Precisamente ha sido Goldman Sachs la que ha liderado una ronda de financiación de 50 millones de dólares en la empresa de almacenamiento de Bitcoines **Circle**, situando a esta empresa en la segunda que más financiación recibe por detrás de **Coinbase**.
>
> En España las inversiones más significativas de entidades financieras en empresas relacionadas con Bitcoin han sido las de **Bankinter** en la también española **Coinffeine**, **BBVA** en la americana **Coinbase** y más recientemente el banco **Santander** en Ripple.

No obstante, un aviso a navegantes respecto al interés de las entidades financieras en el mundo Bitcoin: su interés se centra más bien en cómo la tecnología de la cadena de bloques puede ayudarles a reducir sus costos de operación que en Bitcoin como moneda. Esto ha originado lo que se viene a denominar como cadenas de bloques privadas (*privat blockchains*), cadenas de bloques que viven y evolucionan dentro de los servidores de un banco o de una red de bancos en el caso de ponerse de acuerdo entre ellos, y a las que no se tendría acceso desde el mundo exterior. Desde mi modesto punto de vista, lo único que hacen es un intento de evitar perder el control sobre su libro de cuentas. Pero, ¿si una entidad financiera no apuesta por la transparencia que ofrece una cadena de bloques pública como Bitcoin, qué mensaje está queriendo mandar? Este debate daría para más de un libro.

También el Banco de Inglaterra se ha posicionado respecto a las criptomonedas, llegando incluso a decir que Reino Unido debería sustituir el dinero fíat y crear una criptomoneda con respaldo estatal, que sirviese para afrontar los retos y cambios a los que el mundo financiero se va a ver sometido, de manera imparable, en los próximos años. El artículo titulado "Response to fundamental change" es muy recomendable de leer, pero sigue en la línea de apostar por cadenas privadas y supervisadas por algún organismo de confianza.

A pesar de que no vamos a entrar en este debate, me parece interesante al menos que conozcáis (otro más) el reciente artículo de **David Galbraith** titulado "Cadena de bloques y bancos" ("Blockchain and Banks" en su versión inglesa); el artículo explica el modo en que podrían relacionarse las cadenas privadas y la pública de Bitcoin, de manera que las primeras acabarían en algún momento haciendo uso de la segunda, que se convertiría en la columna vertebral de todo un nuevo sistema transaccional, y en donde cualquier contrato quedaría registrado. En las referencias del libro está indicado desde dónde podéis echarle un vistazo.

¡ATENCIÓN! ¡ATENCIÓN!

Dicho lo cual no voy a negar que acercarse al mundo del dinero electrónico, las monedas virtuales y/o las criptomonedas puede ser un tanto intimidatorio al principio (aunque apasionante), y máxime cuando oímos palabras como: criptografía

de clave pública, bloques, *scripting*, algoritmos de *hash*, *gigahashes*, oráculos, tecnología ASIC, poder de minado, CPU, GPU… parece que estemos hablando de los últimos poderes de Superman, y claro más de uno prefiere esperar a ver qué pasa y a ver si el panorama se aclara un poco, que no está la cabeza para complicarse con este tipo de cuestiones.

También es cierto que habrá muchos qué pensarán que ellos usan sus tarjetas de crédito y que no necesitan saber los entresijos de la red VISA o Mastercard, y por qué enfangarse con estos asuntos. Y aunque llevan toda la razón, personalmente considero que no es tan fiero el león como lo pintan, y aunque aún se requiere cierta habilidad técnica para moverse con soltura por los diferentes escenarios, tampoco hay que ser una lumbrera para no perderse, y con un poco de cuidado y yendo pasito a pasito, seremos capaces de entender sin problemas el funcionamiento de todo: no seremos víctimas de a quienes les gusta tergiversar la verdad y hacer de Bitcoin lo que no es, un nido de inadaptados sociales, frikis, terroristas o narcotraficantes que lo usan en la clandestinidad.

Y aquí quiero hacer hincapié en algo muy importante: para **la operativa normal** necesitamos conocer y manejar con soltura solamente cuatro conceptos:

- Qué es una dirección Bitcoin.
- Saber cómo funciona una billetera o monedero digital.
- Cómo asegurar nuestro dinero (probablemente el paso más importante para evitar que nuestro dinero pueda verse comprometido).
- Y saber cómo enviar y recibir pagos.

Con solo esto es más que suficiente para echar a andar con cualquier criptomoneda, lo demás es la guinda del pastel, es saber por qué las cosas son como son y funcionan como funcionan y las posibilidades que nos brindan. No obstante y a pesar de lo que acabo de decirte, es necesario que a lo largo de este libro y en ocasiones, tenga que hacer referencia a conceptos técnicos, que pueden resultar un poco ininteligibles si es la primera vez que nos acercamos a ellos. No os preocupéis, porque nada de lo que estoy contando aquí se quedará sin su debida explicación, de momento, os pido que hagáis un pequeño acto de fe, y cuando os diga que tal o cual cosa funciona de tal o cual modo, creáis en lo que digo para más adelante ir poniendo las piezas que faltan.

Una vez hayamos explicado estos conceptos básicos seguiremos nuestro viaje definiendo qué es el dinero electrónico y las posibles formas que presenta hoy en día, y dedicaremos diferentes secciones a analizar las criptomonedas más interesantes, (*altcoins* o *alternative coins*) que han aparecido a lo largo de los últimos meses siguiendo la estela de Bitcoin y sus diferencias filosóficas.

De momento os recomiendo que paséis por la siguiente página web y echéis un vistazo de lo que tenemos entre manos y al movimiento surgido desde Bitcoin:

http://www.mapofcoins.com

2.1 EL COLORIDO MUNDO DE LAS MONEDAS ELECTRÓNICAS O MAPOFCOINS

No es la primera vez que alguien que se acerca al mundo de las criptomonedas no piensa esto mismo y me lo comenta personalmente. Santiago, esto de Bitcoin y el dinero electrónico está muy bien, pero es un auténtico lío. Me hablas de Bitcoin, de Litecoin, Dicecoin, Zerocoin… ¿cómo es posible que existan tantas monedas electrónicas? Menudo follón, menudo lío, no sé con cuál quedarme, a mí en esto no me metas que bastante tengo yo con gestionar mis escasos euros mensuales.

Razón no les falta.

Antes de explicar las posibles causas, vamos a echar un vistazo a la web que os comentaba al principio:

http://www.mapofcoins.com

En esta web, es posible consultar la evolución de todas las criptomonedas que han surgido en estos últimos años, partiendo de la aparición de Bitcoin.

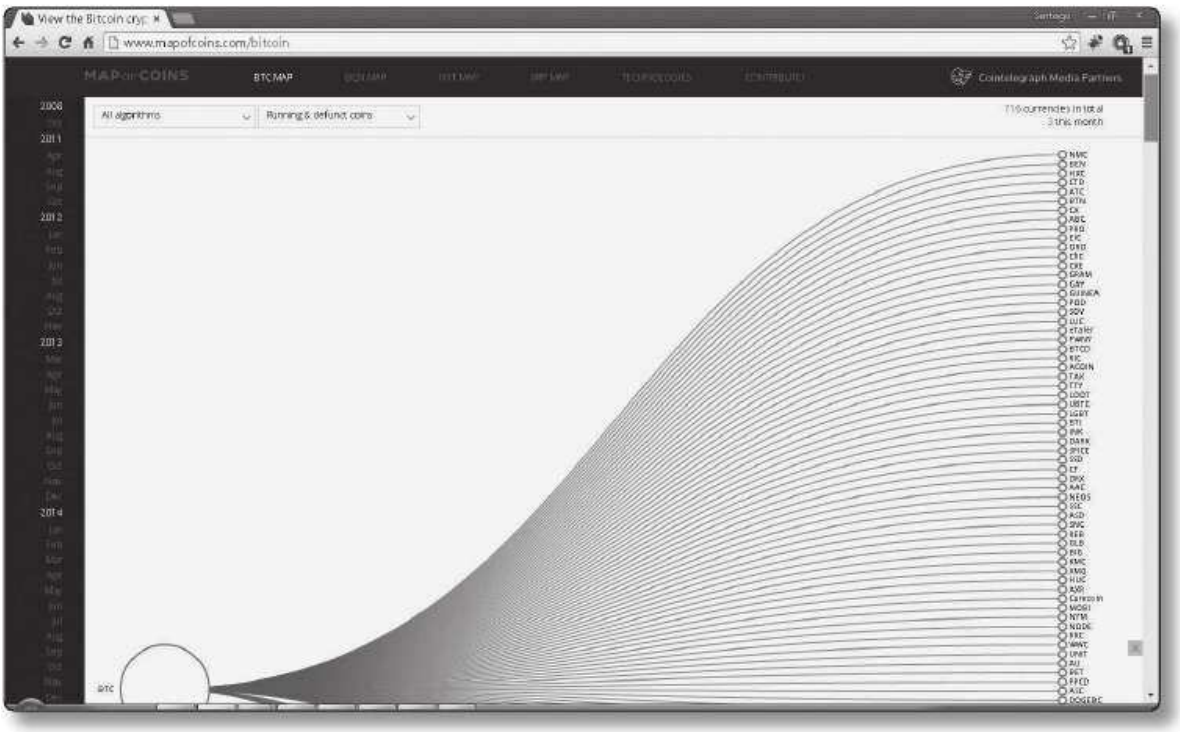


Figura 2.1. Página principal de MapofCoins

¿Qué os parece? ¿Me estás diciendo, Santiago, que actualmente hay aproximadamente 700 criptomonedas diferentes en circulación derivadas de Bitcoin? Pues sí, eso es exactamente lo que te estoy queriendo decir, pero ¡ojo!, dos puntos a tener en cuenta:

- El primero es que este número aumenta casi a diario, por lo que dependiendo de cuándo accedas a esta página puede que haya muchas más.

- El segundo, y más importante, es que **el valor de la gran mayoría de ellas es 0 o próximo a 0**, solamente unas pocas han llegado a causar un impacto lo suficientemente importante como para tenerlas en cuenta, o solo son importantes para un grupo de usuarios muy limitado.

2.1.1 ¿Por qué hay tantas monedas diferentes?

Esta es seguramente la siguiente pregunta que uno se hará después de ver la web, ¿cómo es posible que haya tantas monedas diferentes? Yo creo que hay dos motivos principales pero ambos tienen que ver con una palabra: oportunidad. Pero, ¿oportunidad en qué sentido? Pues muy fácil, en dos sentidos diferentes, una de adopción y otra de mejora.

- **Oportunidad de adopción**:

  Aquellos que comienzan a utilizar una determinada moneda los primeros, los denominados *early adopters*, son los que más posibilidades tienen de ganar dinero si la moneda llega a popularizarse. Pensemos que al principio de la aparición de Bitcoin, era normal obtener muchas monedas en pocas horas de minado. En aquel momento, en donde la minería de la moneda era poco popular (así como los interesados en utilizarla), con un número de mineros muy pequeño y una complejidad computacional necesaria para minar mínima, su valor (el de la moneda) era irrisorio, y prácticamente inexistente. Pero el tiempo ha pasado, y no es raro oír noticias en donde fulano de tal ha hecho una fortuna con los Bitcoines generados o comprados por cantidades ridículas.

  Un ejemplo de esta situación, que salió en todos los periódicos, fue el estudiante noruego **Christopher Koch** que compró, por 24 dólares en 2009, unos 5.000 Bitcoines, y que al cambio actual (235$ en el momento de escribir estas líneas) suponen algo más de un millón de dólares.

Por tanto, teniendo en cuenta esto, no es de extrañar que una nueva moneda aparezca y que aquellos que apuestan por ella confíen en que con el tiempo, paciencia y un poquito de especulación, su uso se generalice y conseguir lo que otros con Bitcoines ya han conseguido. Es muy difícil que esto llegue a producirse pero…

- **Oportunidad de mejora**:

  Todo software tiene sus fallos de programación o de diseño y Bitcoin no es ajeno a ellos (por ejemplo el reciente debate con la salida de **Bitcoin XT** es un claro ejemplo de una deficiencia en el diseño de Bitcoin). Donde unos ven una fortaleza, otros ven una deficiencia, como dice el dicho, nunca llueve a gusto de todos.

  Sea por el algoritmo criptográfico utilizado en el desarrollo, o porque la democracia en la minería no esté garantizada, o porque la escalabilidad a largo plazo esté comprometida o… por lo que sea, lo cierto es que a Bitcoin (como a cualquier software) se le pueden sacar unas cuantas posibilidades de mejora, algo que es muy bueno porque hay más de una cabeza dando vueltas al tema y me sirve a mí para insistir en algo que igual no digo con la suficiente energía, porque reconozco que el potencial de Bitcoin me nubla en ocasiones: Bitcoin sigue siendo y lo será durante algún tiempo, software experimental.

  Las mejoras, ampliaciones o posibles modificaciones que se sugieren para Bitcoin se denominan **Bitcoin Improvement Proposal (BIP)** y basta con escribir a la lista de correo de los desarrolladores de Bitcoin explicando lo que se quiere hacer y si existe un amplio consenso se acepta. En general las mejoras propuestas se publican en una página de Bitcoin dedicada a ello:

  https://es.bitcoin.it/wiki/Propuestas_de_mejora_de_Bitcoin

Dado que algunas de estas sugerencias se toman en cuenta, y otras por el contrario son desechadas, es aquí donde se encuentra la oportunidad de que aparezca una nueva moneda con unas fortalezas/debilidades diferentes.

Por poner algunos ejemplos:

- Una mejora de diseño estaría en el tiempo que una transacción tarda en ser confirmada, 10 minutos en el caso de Bitcoin, 2,5 minutos en Litecoin o 1 minuto en Dogecoin. A mayor tiempo de verificación, más posibilidades de hacer un doble gasto (de falsificar la moneda) aunque ciertamente esto es más fácil de decir que de hacer.

- Otro ejemplo importante está en el algoritmo de *hash* que se utiliza para las comprobaciones de las transacciones y la generación de los bloques. Algunos, como es el caso de Bitcoin o Namecoin, usan encriptación basada en **SHA-256** mientras que otros como Litecoin o Dogecoin utilizan **scrypt**.

La utilización de SHA-256 como algoritmo hace que para Bitcoin sea interesante la existencia de mineros profesionales, que con equipos de tecnología ASIC puedan aportar un gran poder de cómputo a la red. Esto supone que la minería no sea rentable para alguien que no tiene un equipo con estas características, por tanto, si quiero poder jugar de tú a tú con otros mineros, o entro en el juego de adquirir uno de estos equipos o la cantidad de dinero que mi hardware podrá generar será muy pequeña (tan pequeña que sale más a cuenta conseguir la moneda de manera gratuita a través de los múltiples *faucets* o grifos que hay por la red).

Esto no sucede si nos decidimos por Litecoin o Dogecoin, en donde la minería es un proceso más democrático y en donde no son necesarios equipos especiales para poder formar parte del selecto grupo de los mineros.

2.1.2 ¿Tienen sentido las alternativas a Bitcoin?

Hemos dicho que Bitcoin o cualquier otra moneda digital o electrónica no deja de ser más que software que se ejecuta sobre una máquina, aunque en este caso, sean muchas las máquinas que de manera distribuida están trabajando y soportando el software (usando una red de tipo P2P o *Peer to Peer*), el funcionamiento no varía.

Desde que Bitcoin apareció y ganó popularidad, como era lógico esperar, han aparecido muchas imitaciones que funcionan siguiendo un esquema parecido a esta. Algunas monedas han nacido a partir del propio código fuente de Bitcoin, como es el caso de Namecoin o Litecoin, otras por el contrario se han implementado desde cero (se han codificado, programado o como más cómodo nos resulte de entender) siguiendo sus propias directrices de diseño.

Lo más normal es que estas nuevas monedas surjan dentro de una comunidad, es decir, es la comunidad que la usará la que existe primero antes que la moneda, en vez de que exista primero la moneda y luego se cree la comunidad en torno a ella, algo sin duda más difícil. Yo aquí diría que popularizar una moneda desde cero, sin partir de una comunidad previa, puede llegar a ser incluso una tarea imposible, si en toda la historia de la humanidad no lo hemos logrado con las monedas físicas, con las virtuales puede ser una tarea titánica. Además parece lógico pensar, si pensamos en

el origen del dinero que comentamos en el capítulo 1, que las diferentes formas que ha ido adoptando a lo largo de los siglos han estado inevitablemente relacionadas con las comunidades donde nacieron.

Bitcoin ha nacido en un momento en donde los medios de comunicación han contribuido muchísimo a su popularización y conocimiento, y probablemente si se hubiera desarrollado hace 15 años, este conocimiento habría sido mucho menor; al principio, fue un proyecto de unos pocos.

Si hay una mejora o un error en el código Bitcoin, y como estamos ante software puede (de hecho debe), por tanto, mejorarse y corregirse, adaptarse y hacerlo más robusto, seguro o lo que queramos que sea. Obviamente esto tiene implicaciones, las compatibilidades hacia atrás, y más si es algo tan susceptible para el ser humano como es el dinero, deberían estar garantizadas, nadie lo discute, pero el código es probablemente uno de los activos más maleables que existe, si se hace con cuidado (alguno de los ingenieros de software que conozco me darían un coscorrón al decir esto, pero creo que el sentido y el contexto de lo que quiero decir es claro). Las alternativas a Bitcoin son buenas en cuanto aportan estas nuevas panorámicas y visiones, que ayudan a fortalecer a Bitcoin y hacerlo mejor. Es como la selección natural, las mejores ideas sobreviven y se implementan y las peores se desechan. Bitcoin ha sido la primera de las criptomonedas, y la que más ojos tiene puestos encima, es la que más pruebas de estrés ha superado y la que tiene la comunidad de desarrolladores más fuerte, por tanto, veo muy difícil que pueda ser superada por otra criptomoneda.

¿Estoy queriendo decir que las alternativas a Bitcoin no sirven o no tendrán nunca éxito? Todo lo contrario, aunque creo que Bitcoin no será superada, eso no significa que el resto de las *altcoins* no tengan su espacio. Yo incluso iría aún más lejos. Creo que hay espacio para todas las criptomonedas, si pensamos en ellas como elementos que surgen dentro de una comunidad y que sirven para facilitar las relaciones entre sus miembros. A medida que las relaciones entre los grupos se extienden y generalizan, pueden usarse criptomonedas adaptadas más globalmente por estos grupos, de modo que en la cúspide, tendríamos a la más aceptada de todas: Bitcoin, que es además la criptomoneda más líquida.

Fijaos en que para que una moneda tenga valor, tienen que existir comunidades que estén dispuestas a aceptarla, y esto solamente es posible si una moneda es líquida. Pero, ¿qué es esto de la liquidez?

Volviendo a nuestra pequeña historia sobre el origen del dinero del capítulo 1, hemos explicado que algunos tipos de notas de intercambio, como las notas en madera, permanecían en el circuito debido a su liquidez. Desde un punto de vista casi de colegio, la liquidez se refiere a la capacidad de convertir una cosa en otra,

respetando tres propiedades: rapidez, falta de pérdida de valor y temporalidad. Cuanto más fácil sea realizar esta transformación, diremos que la liquidez es mayor o menor.

Un ejemplo, sacado de mi etapa de estudiante en el colegio (yo también soy de EGB), eran los cromos de Arconada (portero de la selección española de futbol para aquellos más jovencitos) que se podían cambiar por otras cosas mucho mejores (por chapas de Coca-Cola u otros cromos, incluso un dónut de chocolate en el mejor de los casos) por la popularidad de este deportista. Por tanto, el cromo de Arconada era más líquido que el de otro portero o jugador de futbol.

Aplicado sobre las notas de madera, la liquidez es la capacidad de transformar la nota en las vasijas, teniendo en cuenta lo siguiente:

- **Rapidez**: lo ideal es que se produzcan en tiempo real o en el menor tiempo posible; en el caso de las notas de madera, resultará un concepto relativo, ya que depende de cuán cerca estemos del alfarero que emitió la nota, pero suponemos que si estamos con él, el cambio de la nota por las vasijas se realizaría al momento.

- **Pérdida de valor**: si la nota originalmente valía cinco vasijas, cuando realice el intercambio por estas, el alfarero me tiene que seguir dando cinco vasijas, ni cuatro ni seis, exactamente las vasijas que me dijo. Veremos que esto en el mundo real no es exactamente así, y que siempre hay pequeñas (y a veces no tan pequeñas) fluctuaciones en el valor, siendo la inflación uno de los elementos determinantes en el precio de las cosas.

- **Temporalidad**: puedo hacerlo cuando quiera, nada me impide ir a la tienda del alfarero y realizar el intercambio.

Hoy en día, ya no usamos tablas de madera como elemento de intercambio, sino que usamos el dinero para tal fin, pero la idea es la misma, lo que nos interesa es saber la liquidez de los activos, o su capacidad para convertirse en dinero efectivo. Por ejemplo, un inmueble como puede ser una oficina o un piso tiene una liquidez muy baja si lo comparamos con un depósito bancario. Cambiar el piso por dinero no es rápido y dependiendo de cuándo lo compramos, puede suponer una pérdida de valor su venta. Convertir el depósito en dinero es tan simple como ir al cajero y sacarlo de allí.

La liquidez nos interesa porque actúa como una medida contra la incertidumbre ante acontecimientos imprevistos, si algo es muy líquido, sabemos que podré cambiarlo por otra cosa rápidamente, y ante eventuales problemas estaré

un poco más protegido. En el ejemplo del piso, si tengo un hijo enfermo y necesito el dinero para llevármelo a EE. UU. para operarlo, tendré que esperar a poder venderlo, mientras que si tengo el dinero en el banco, solo tendré que ir allí y sacarlo, por tanto, ante este evento (y esperemos que improbable suceso) estoy más protegido en el segundo caso que en el primero.

Llevado al mundo empresarial, cuando se dice que tal o cual empresa tiene o no liquidez, lo que se nos está dando a entender es la capacidad que tiene la empresa de convertir sus activos en dinero y hacer frente a sus obligaciones en el corto plazo, y siempre que oigáis obligación a corto plazo se refiere a lo mismo, a la capacidad para pagar sus deudas. El pago de las deudas es algo primordial no solo para las empresas, sino también para los Estados, y es la capacidad de unos y otros para poder pagarlas lo que fortalece la confianza tal y como ya explicamos.

El dinero es de por sí el activo más líquido que existe (¡ya es dinero!).

Bitcoin es la criptomoneda más líquida, la más fácil de cambiar por otras cosas, incluyendo otras criptomonedas, algo que favorece que las relaciones anteriores puedan producirse. ¿Es posible que Bitcoin las fagocite y dado que sea la comúnmente más aceptada llegue a ser la única? Aunque hay opiniones tanto en un sentido como en otro, y parece ser lo más probable, sería muy atrevido por mi parte dar una respuesta rotunda a esta cuestión, y creo que hay que dar tiempo al tiempo.

De todos modos, puede que haya una solución alternativa, quedaos con este nombre: **cadenas laterales** o **sidechains**, porque cuando lleguemos al último capítulo sobre el futuro de Bitcoin, veremos que las *altcoins* pueden acabar teniendo cabida dentro de esta posibilidad. Aunque os anticipo que las cadenas laterales no están exentas tampoco de polémica, faltaría más.

Pero sí que hay una cosa que no es discutible y probablemente, después de haber leído todo esto, hayas llegado a la siguiente conclusión: que las diferencias entre unas monedas u otras en muchas ocasiones son muy sutiles, y afectan más al código (y protocolo) que hay por detrás de la moneda, que al funcionamiento en sí mismo de esta.

Efectivamente, el usuario final, que es al fin y al cabo el que va a tener que usarlas, no encontrará diferencias apreciables al operar, y tendrá que seguir lidiando con los mismos conceptos: direcciones, carteras digitales, saber cómo enviar y recibir dinero y por supuesto cómo protegerlo. Del mismo modo que si estoy en EE. UU. y uso dólares, o en Europa trabajando con euros, cuando dispongo de la moneda, el hecho de ir de compras no presenta variaciones en el proceso, aunque por detrás existan muchísimas connotaciones diferentes que suceden por usar una u otra, y que aunque a la larga no dejarán de afectarnos, pasan desapercibidas en ese momento.

2.1.3 ¿Y yo, puedo tener una?

Volviendo a nuestro mapa de monedas, otra pregunta que nos podemos hacer al verlo es ¿realmente es tan sencillo crear una criptomoneda? Visto lo visto parece ser algo muy sencillo, y la respuesta a esta pregunta es depende de nuestras ambiciones y de lo que queramos hacer.

Crear (aunque yo usaría la palabra **clonar**) una criptomoneda es relativamente simple, y con unos conocimientos del lenguaje de programación C++ no demasiado exigentes, puede llegar a hacerse en unas pocas horas una variación partiendo del código de alguna existente. Pero cuidado con esto, con variar el código me refiero a pequeñas cosas, tal vez la cantidad de monedas que se pueden generar y cosas por el estilo. Las criptomonedas funcionan en base a la definición de unos protocolos con reglas muy estrictas, cambiar una de estas reglas ya no resulta tan trivial y puede suponer tener que modificar gran parte de la codificación del programa, si no tener que hacerlo desde cero, y eso ya no es cuestión de unas pocas horas.

Sí que es cierto, sin embargo, que rizando aún más el rizo, es posible crear una variación de Bitcoin y hacer nuestra propia criptomoneda de un modo relativamente fácil. En la Web hay páginas que permiten a través de un asistente e introducir unos pocos datos, personalizar una criptomoneda en cuestión de minutos o al menos eso garantizan. Esta posibilidad estuvo durante algún tiempo muy de moda, sin embargo, algunas de las páginas más populares, como por ejemplo, **Coincreator** (*http://coincreator.net*), han desaparecido y ya no dan servicio (aunque sigan apareciendo entre los primeros resultados de Google), y las que quedan son de muy diverso tipo, calidad y fiabilidad. Por ejemplo, **BitClone** (*http://bitclone.net*) aún mantiene activa su página web, y permite que te pongas en contacto con ellos para participar en su proceso de pruebas de su aplicación de generación de *altcoins*.

Figura 2.2. Página principal de BitClone

Otras como **CryptoLife** (*http://dev.cryptolife.net*) tienen un asistente donde puedes configurar casi todas las posibilidades que se te ocurran, y que van desde el nombre de la moneda, la imagen o logo que tendrá, su abreviatura, el algoritmo de *hashing* usado (scrypt, SHA-256, X11, X13), el algoritmo para el cálculo de la dificultad (Kimoto Gravity Well, Nite's Gravity Well, Dark Gravity Well, Digishield), el tipo de bloque génesis, etc. Y todo ello lo hacen por el módico precio de 0,15 BTC (el precio puede variar para cuando estéis leyendo estas líneas), cantidad a la que hay que sumar los extras que decidamos que tenga nuestra moneda. Se comprometen además a enviarnos el código fuente y también los ejecutables para realizar la instalación de la billetera sobre Windows.

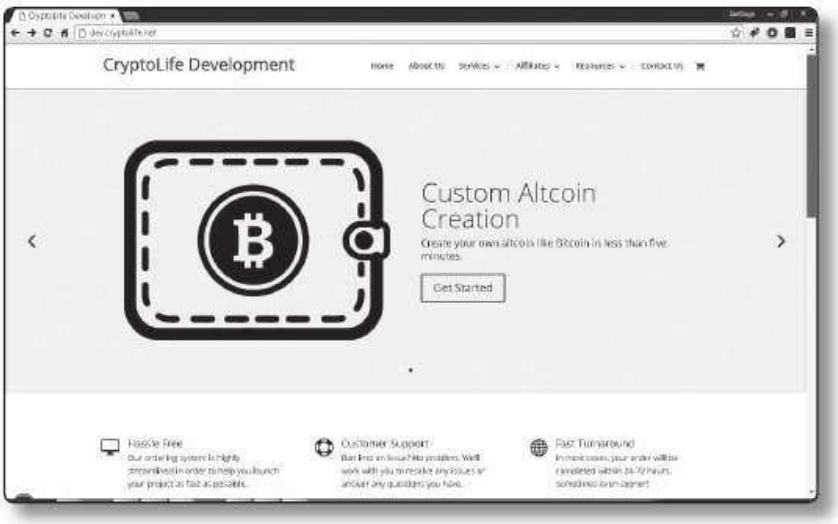


Figura 2.3. Página principal de CryptoLife

Por ejemplo, si vamos a **cryptonotestarter**.**org**, la creación de nuestra pequeña variante de Bitcoin requiere de conocimientos de programación.

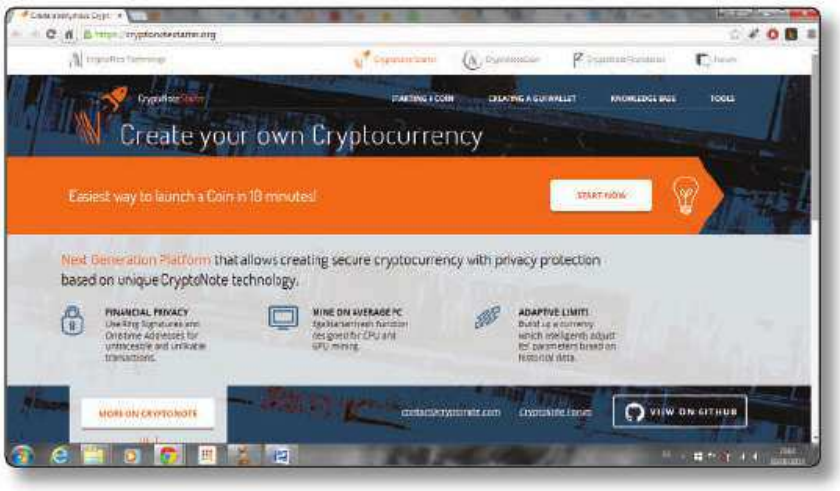


Figura 2.4. Página principal de CryptoNoteStarter

El mecanismo que sugiere para la generación de tu propia criptomoneda no deja de ser curioso, y lo divide en un proceso que resume en 6 pasos (ver imagen):

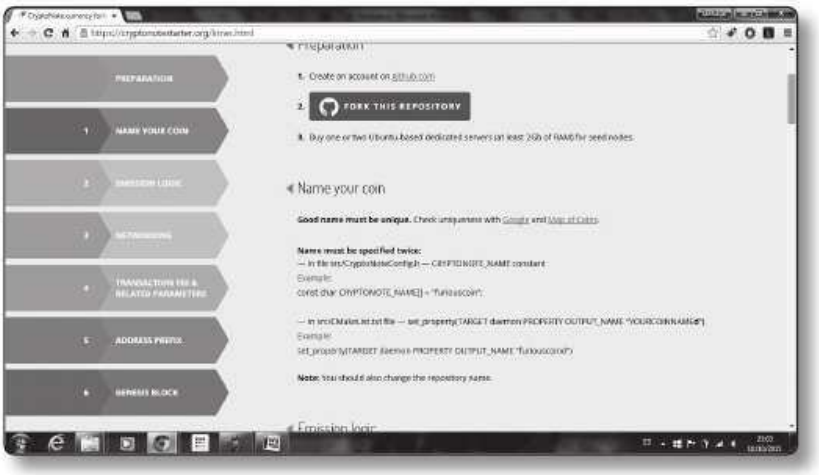


Figura 2.5. Los pasos de CrytoNoteStarter

El primer paso es quizás el más importante, porque consiste en conseguir el código fuente base de su criptomoneda, **CryptoNote**, e ir haciendo sucesivas modificaciones en el mismo. Modificaciones que son explicadas a medida que vas moviéndote por los pasos anteriores. El código del que se parte está publicado en un repositorio de código, muy popular en la comunidad de los desarrolladores de software, que se llama **GitHub**, de casi cualquier cosa que se os ocurra que pueda haberse programado, seguramente existirá un código que estará colgado en esta web.

Solamente tenéis que crearos una cuenta en GitHub para acceder al código e ir cambiando el contenido de los ficheros que se os indica. Una vez finalizado el proceso podéis hacer pública vuestra moneda enviándola a los responsables de CryptoNoteStarter que se encargarán de validarla y hacerla pública en su sitio.

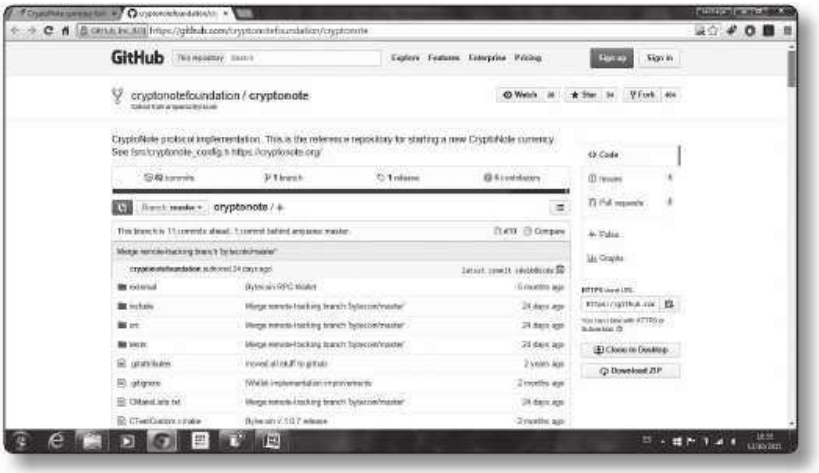


Figura 2.6. CryptoNote en GitHub

Aunque no es objeto de este libro entrar en los detalles técnicos de cómo se realizaría el proceso de compilación, indicaros que las herramientas a usar difieren según el sistema operativo:

- En el caso de sistemas tipo Unix, se recomienda usar GCC 4.7.3 o posterior, CMake 2.8.6 o posterior y Boost 1.55. Una vez hecho el cambio en el código, haríamos un *make* para obtener los binarios.

- En el caso de Windows las herramientas serían Microsoft Visual C++ 2013 o superior, CMake 2.8.6 o superior y Boost 1.55. Igual que antes, hechos los cambios en el código haríamos un *cmake* para obtener los binarios.

Para finalizar, una vez que la moneda esté validada, es posible también crear un **pool de minería** para la misma, pero como de momento no he explicado que es esto de los *pools* de minería, lo vamos a dejar aquí.

2.2 ORIGEN DE BITCOIN. LOS PRECEDENTES HISTÓRICOS

Dado que no nos vamos a enfangar en esto de crear nuestro propio clon de Bitcoin, aunque ahora sabemos que es posible, sigamos nuestro viaje haciendo otra vez un poco de historia y busquemos cuáles son las raíces de Bitcoin.

Bitcoin es la criptomoneda de moda, sin duda, sin embargo no fue algo que se improvisase de la noche a la mañana, y otros antes que **Satoshi Nakamoto** idearon sistemas que solamente Bitcoin parece haber sido capaz de popularizar y hacer llegar al gran público. No obstante, todos perseguían el mismo objetivo: conseguir, sin necesidad de un tercero de confianza, que en el dinero electrónico funcionasen la anonimidad y la descentralización. Tarea nada sencilla como iremos viendo.

La red Bitcoin se puso en marcha el 3 de enero de 2009 con el bloque génesis, justamente unos pocos meses antes de que el proyecto fuera registrado, el 8 de noviembre de 2008 y Satoshi Nakamoto publicara su famoso *paper* "Bitcoin: A Peer-to-Peer Electronic Cash System" describiéndolo, en una lista de criptografía de **metzdown.com** el 1 de noviembre de 2008, y que se relaciona con el movimiento ciberpunk. Podéis acceder desde el siguiente enlace al comentario y al *paper*:

http://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html

Y llegaréis a la página que os muestro a continuación:

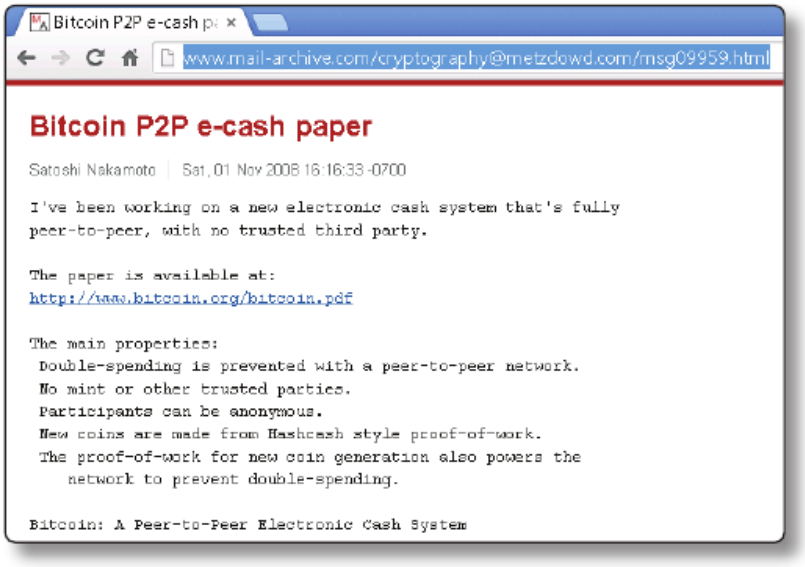


Figura 2.7. Publicación original de Satoshi Nakamoto

En el documento de Satoshi se explican ideas y conceptos que otros autores anteriores a él ya habían desarrollado, aunque se da una nueva vuelta de tuerca al concepto de dinero electrónico y a los problemas de anonimato y descentralización. Por tanto, el que se publicase en una lista de carácter decididamente ciberpunk tiene mucho sentido, y se asume generalmente que los creadores de Bitcoin pertenecen o guardan relación con este movimiento.

Pensad que el movimiento ciberpunk originado en los años 90 está apadrinado y tiene sus orígenes en las corrientes de opinión contrarias a las prohibiciones del Gobierno de EE. UU. de publicar ideas o investigaciones relacionadas con la criptografía (de hecho la criptografía tiene el mismo nivel de seguridad que las armas de destrucción masiva), por el motivo obvio de no ceder ni un ápice en el control al que pueden someternos. Por el contrario, los ciberpunks consideran el uso de la criptografía como algo necesario y vital para poder cambiar la sociedad, un derecho inalienable al que no podemos ni debemos renunciar. Estas ideas están recogidas en dos escritos muy populares: el *Manifiesto Criptoanarquista* y el *Manifiesto Ciberpunk*.

Hacer un análisis ya no exhaustivo sino apenas parcial de estos apenas siete años de historia en la vida de Bitcoin sería toda una aventura, porque por sí solos cada uno de ellos tiene un interés y calado que haría difícil decidir con cuál quedarnos, por lo que os hago otra recomendación más, ir a la siguiente web:

http://historyofbitcoin.org

Desde aquí tenéis una línea temporal que nos muestra los acontecimientos más importantes, para que podáis investigar y saber más sobre los avatares que ha sufrido Bitcoin desde su gestación hasta nuestros días. Dado el espacio limitado que tenemos, a modo de resumen sirva la siguiente tabla como ejemplo de los episodios más destacados a tener en cuenta:

AÑO	ACONTECIMIENTOS DESTACADOS
2008	• Registro del dominio bitcoin.org. • Publicación del *paper* de Satoshi Nakamoto.
2009	• Se pone en marcha la red y se mina el bloque 0 o bloque génesis. • Primera transacción de Satoshi Nakamoto a **Hal Finney**. • Primer cambio de Bitcoines por dólares en el operador New Liberty Standard, 1$ equivale a 1.309,03 BTC.
2010	• Al inicio del año el cambio de 1 BTC es igual a 0,003$ pero finaliza el año en 0,3$. • Mayo de 2010. **Laszlo Hanyecz** compra dos *pizzas* por 10.000 BTC (probablemente las pizzas más caras de la historia). • Julio de 2010. Inicia su operativa **Mt. Gox**. • 15 de agosto de 2010. Detectada la primera vulnerabilidad al protocolo Bitcoin debido a la **no verificación de las transacciones** antes de ser incluidas en la cadena de bloques, lo que permitía crear un número indefinido de Bitcoines. Se emitieron 184 mil millones de Bitcoines en una transacción, que a las pocas horas de ser detectada, fue borrada y corregida. Junto con **la maleabilidad de las transacciones** son las únicas vulnerabilidades que se le han detectado al protocolo Bitcoin hasta la fecha. • Noviembre de 2010: la cantidad de Bitcoines emitidos supera el millón de dólares.
2011	• Se alcanza la paridad con el dólar 1 BTC = 1$, aparecen artículos en Slashdot y *Forbes* explicando qué es Bitcoin. A final de año 1 BTC = 5,27$. • Se crea Silk Road y Wikileaks comienza a aceptar donaciones en Bitcoines. • Se funda Bitstamp y BTCE. • Aparece **Litecoin** por **Charles Lee**, un exempleado de Google. • Primer gran ataque a Mt. Gox. • Internet Archive y Wikimedia comienzan a aceptar donaciones en Bitcoines. • Agosto de 2011: se pone en marcha **blockchain.info**.
2012	• Se considera el año de **consolidación** de la moneda, muchas webs comienzan a aceptarla: Wordpress quizás sea la más importante de ellas. • SatoshiDice inicia operaciones y se acabará convirtiendo en una de las mayores casas de apuestas con Bitcoines. • Se supera la barrera de los 10$ = 1 BTC y el año acaba 1 BTC = 13,30$. • Junio de 2012: se funda **Coinbase** por Brian Armstrong. • Después de un largo desarrollo aparece **Ripple**.

2013	• 1 BTC vale más que una onza de plata. • Bitstamp se traslada a Reino Unido. • Inicio del fin de Mt. Gox, en mayo de 2013 EE. UU. congela las cuentas del operador. BTC China lo acabará superando en transacciones ese mismo año. • El corralito en Chipre hace que el precio de Bitcoin se dispare hasta los 200$, el precio seguirá subiendo hasta sobrepasar los 1.000$ y llegar a equiparar el precio del oro. Posteriormente se especulará que la subida tuvo que ver con Mt. Gox y sus *bots* manipuladores del precio. • Más empresas se suben al carro de Bitcoin: **Virgin Galactic** quizás la más llamativa por lo curioso de su producto y **Lamborghini** por lo exclusivo de sus coches. • Octubre de 2013. El FBI cierra Silk Road y se apodera de 26.000 BTC y se abre el primer cajero de Bitcoines en Canadá (Vancouver). Se funda la empresa **Circle** por Jeremy Allaire. • Noviembre de 2013, James Howell tiró a la basura un disco duro donde había minado 7.500 BTC por error, jamás lo recuperó. Por esas mismas fechas el noruego Kristoffer Kock recuerda que tiene 5.000 BTC comprados en 2009 por 29$. • Diciembre de 2013, el Banco Central chino comienza con sus prohibiciones, y esto junto con la caída de Mt. Gox hacen que el precio de Bitcoin caiga de los más de 1.000$ a algo menos de 600$. Este mismo año se funda el proyecto **Ethereum** por Vitalik Buterin.
2014	• Febrero de 2014. Bitstamp sufre ciberataque DoS, durante varios días no da servicio pero se recupera sin problemas. Mt. Gox se declara en quiebra con pérdidas de 850.000 BTC. Rusia declara ilegal el uso de Bitcoin. • Marzo de 2014, la billetera **Xapo** se abre al público. • Abril de 2014, los bancos chinos cierran las cuentas de los operadores de Bitcoines en el país. • Junio de 2014. Un grupo de mineros (Cex.io) alcanza temporalmente el 51% de la potencia de la red. • El precio de Bitcoin va bajando a lo largo del año hasta situarse en torno a los 200$.
2015	• Agosto de 2015, el estado de Nueva York pone en marcha la BitLicense, la empresa Circle es la primera en obtenerla un mes más tarde. • Noviembre de 2015, en España, el Ministerio de Hacienda declara exentas de IVA las operaciones con criptodivisas. • Octubre de 2015, el Tribunal de Justicia de la Unión Europea declara exento de IVA a Bitcoin equiparándolo a las monedas fiat. En España, Hacienda comienza a investigar a las empresas que aceptan Bitcoines como pago. • El precio **vuelve a romper la barrera de los 500$**, presumiblemente por la devaluación del yuan por el Gobierno chino y el aumento del control de capitales. • Últimas subastas de los Bitcoines incautados a Silk Road.

Aquí tenemos una imagen de la web:

Figura 2.8. La web historyofbitcoin.org

Aunque lo anteriormente contado está muy bien, y hay material para entretenerse más de un rato, podemos preguntarnos, ¿esto tendrá unas bases teóricas, matemáticas o financieras o de algún otro tipo en lo que se sustentará?, y efectivamente así es. Tradicionalmente, si consultáis cualquier libro o fuente en Internet que hable de los precedentes históricos de Bitcoin, siempre se centran en los cuatro mismos autores, y yo en aras de la originalidad, no voy a ser menos. Y, ¿quiénes son nuestros personajes misteriosos? Pues no hay mucho misterio, si habéis investigado antes este tema los nombres seguramente os sonarán, estamos hablando de:

- David Chaum con el sistema eCash.
- Adam Back con el sistema Hashcash.
- Nick Szabo con bit gold.
- Wei Dai con B-Money.

2.2.1 David Chaum y eCash

David Chaum es un criptógrafo muy conocido y afamado, con varios logros importantes a lo largo de su carrera. Es fundador de la **International Association for Cryptologic Resarch** (IACR) y autor de muchos protocolos criptográficos. Gracias al artículo que publicó en 1981 titulado "Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms", se le atribuye el establecimiento de las bases de la investigación de las comunicaciones anónimas.

Su contribución más notable al mundo de los pagos digitales es el protocolo eCash, un sistema de pagos intraceable que se basaba en el uso de **firmas ciegas**. Para comercializar esta tecnología Chaum creó una empresa llamada **DigiCash** en 1990 y estuvo en marcha hasta 1998 cuando se declaró en bancarrota. Fue adquirida por eCash Technologies que posteriormente pasó a formar parte de InfoSpace (actualmente Blucora).

Una firma ciega es un mecanismo que permite cifrar un mensaje sin tener que revelar información del contenido del mensaje, y que aunque puede sonar un poco raro al principio, es muy sencillo de entender con el ejemplo típico que las describe. Básicamente el objetivo es conseguir que a la hora de realizar una transacción, esta se realice de manera anónima para los participantes que entran en juego en ella (ya sea *online* u *offline*). David Chaum trataba de resolver un problema recurrente, ¿dónde van a parar los datos de mi tarjeta cuando realizo por ejemplo una compra telefónica? ¿Qué pasa con mi privacidad? Su aplicabilidad en el dinero electrónico garantiza que ningún tercero pueda determinar los beneficiarios, montos o momentos de pago realizados por un individuo, habilitar que se puedan tener comprobantes de pago, saber el beneficiario bajo ciertas circunstancias y suspender un medio de pago que haya sido robado. El esquema de firma ciega se ejemplifica con el ejemplo de voto con papeleta (fuente: Wikipedia, pero hay otras muchas por Internet que pueden servir de ejemplo y presentan variaciones mínimas sobre este), que sigue el esquema siguiente en donde se parte de un grupo de votantes que no pueden acudir al lugar de votación, y desean asegurarse de que su voto sea secreto y además verificar que este fue contado. Entonces:

- El votante toma su papeleta de votación y la envuelve en papel calco, para luego enviarla en un sobre con su remitente al comisario.

- El comisario abre el sobre, para firmar sobre el papel calco (sin ver qué hay en el interior), y devuelve el paquete en otro sobre. Esta acción permitirá asegurar que el votante se encuentra autorizado para votar.

- Para el día de las elecciones, cada votante manda su papeleta con su voto marcado al comisario en un sobre sin remitente.

- Luego, estos sobres pueden ser abiertos y contados públicamente. Si cada votante recuerda algún elemento característico de su papeleta, como el patrón en las fibras del papel, podrá reconocer su voto en el conteo.

- Por otra parte, como el comisario nunca vio el voto que firmó, y usó la misma firma para todos, no podrá identificar el voto de cada votante.

Aunque todo esto está muy bien, hay un pero, para que el sistema eCash funcione, se requiere de un servidor central de confianza (en este caso un banco), que haciendo uso del sistema de firmas ciegas, es el encargado de mediar entre el comprador y el vendedor (muy diferente del sistema descentralizado de Bitcoin: no hay autoridad central por ningún lado).

2.2.2 Adam Back y Hashcash

Adam Back es un criptógrafo inglés y doctor por la Universidad de Exeter. Al igual que el resto de trabajos que estamos explicando como precedentes de Bitcoin, Hashcash aparece en fechas muy similares, en 1997, como un método para limitar el *spam* en el correo electrónico. Propone el uso de un **token** (un testigo) en la cabecera del correo, su creación requiere cierto coste computacional, no así su verificación, que sería muy rápida.

La gracia de este sistema es que como crear el testigo requiere un coste considerable, un *spammer* tendrá que pensárselo dos veces antes de enviar un correo, puesto que tendrá que invertir mucha capacidad de cómputo a la hora de generar un *token* para que el correo sea considerado como válido. Para un usuario doméstico, que envía correos de manera racional, el tiempo en generarlo no altera significativamente su operativa normal, pero es inasumible en el caso del *spam* en donde se generan muchos mensajes por segundo.

Pero, ¿y qué tiene que ver esto con Bitcoin? Pues tiene que ver con la forma en la que se genera el *token*, puesto que la idea en Bitcoin es muy parecida, de momento quedáos con estos términos: **función de prueba de trabajo** y **SHA-256**.

2.2.3 Nick Szabo y bit gold

Nick Szabo es exprofesor de Derecho de la Universidad George Washington de los EE.UU. y se le considera un experto en derecho, finanzas, criptografía e informática, vamos, la persona ideal que podría definir algo como bit gold, por no decir que es uno de los nombres que más se han barajado para ser la persona que haya detrás del pseudónimo de Satoshi Nakamoto, como veremos.

El sistema propuesto por Szabo en 1998 no necesita de una tercera parte de confianza y los usuarios están representados bajo el pseudónimo de su clave pública. El dinero se crea resolviendo una **prueba de trabajo** (**proof of work**, aunque en el documento original también se refiere a ella como "función de rompecabezas de cliente" o *client puzzle function* y como "función segura de referencia" o *secure benchmark function*, la idea es la misma), es decir, un problema computacionalmente

difícil de resolver, pero cuya solución es fácil de verificar, aunque en este caso, la prueba de trabajo está enlazada con la solución de la prueba de trabajo previa, lo que hace de la creación de dinero un proceso secuencial. Esto es muy interesante, ya que permite a la red ajustar la dificultad que la prueba de trabajo presenta y evita que se pueda producir una creación excesiva de dinero. Cuando un usuario transfiere dinero a otro, lo hace firmando un mensaje con la clave pública de este y propagando el mensaje por toda la red.

En general el proceso que sigue bit gold para funcionar fue resumido por Szabo en siete pasos:

1. Se crea una cadena pública de bits o "cadena-reto" (ver paso 5).

2. Alicia genera en su ordenador la cadena "prueba de trabajo" para esta "cadena-reto" utilizando una función segura de referencia.

3. La prueba de trabajo recibe sellos de tiempo seguros. Esto debería funcionar de manera distribuida, con varios servicios de sellado cronológico diferentes, para que no se dependa demasiado de ningún servicio en particular.

4. Alicia añade la "cadena-reto" y la prueba de trabajo cronológicamente sellada a un registro distribuido de títulos de propiedad bit gold. Aquí, también, no hay un solo servidor de computación del que se dependa excesivamente para operar con el registro.

5. La última cadena generada de oro digital presenta los bits de la "cadena-reto" para la próxima cadena.

6. Para verificar que Alicia es la dueña de una cadena determinada de oro digital, Juan comprueba la serie infalsificable de títulos almacenada en el registro de propiedad bit gold.

7. Para evaluar el valor de una cadena de oro digital, Juan comprueba y verifica las "cadenas-reto", la cadena de prueba de trabajo, y el sello de tiempo.

El artículo completo podéis consultarlo desde la siguiente dirección web y debido a sus similitudes con Bitcoin, hay quien lo considera como su manifiesto fundacional:

http://unenumerated.blogspot.com.es/2005/12/bit-gold.html

2.2.4 Wei Dai y B-Money

El artículo de Wei Dai "B-Money" se publicó también originalmente en una lista ciberpunk, en noviembre de 1998 y parte del trabajo de Szabo. Personalmente siempre me ha parecido muy interesante como comienza, porque hace referencia al *Manifiesto Criptoanarquista* de Tim May, haciendo alusión a cómo se llega a una sociedad sin gobiernos que han sido prohibidos y son totalmente innecesarios y como la amenaza de la violencia no sirve para nada, porque los individuos sobre los que se puede ejercer están completamente anonimados tanto física como virtualmente.

Sin embargo, en una sociedad sin Estado y anónima, ¿cómo es posible establecer relaciones entre los individuos, que impliquen cooperación y participación, cuando se requiere un mecanismo de intercambio como el dinero y existe la necesidad de hacer cumplir los contratos? Ya vimos en el capítulo 1, que son las relaciones entre los hombres las que motivan la invención del dinero como un medio para conseguir un fin. A partir de este problema, Wei Dai propone dos protocolos que pueden ayudar a conseguir estos objetivos.

Para la definición de los protocolos, asume la existencia de una red intraceable, donde los receptores y emisores solamente están identificados por pseudónimos (por ejemplo sus claves públicas de las que luego hablaremos) y donde cada mensaje se firma por el emisor (con su clave privada) y se encripta hacia el receptor (con su clave pública).

En el primer protocolo, cada participante mantiene una base de datos separada de cuánto dinero pertenece a cada pseudónimo. El cómo se actualizan estas bases de datos sería el objetivo de este protocolo, que de antemano Wei Dai afirma que no es práctico por la necesidad de tener un canal anónimo de difusión síncrono e incongestionable.

En este primer protocolo, Wei Dai explica el mecanismo utilizado para la creación de dinero mediante el envío de la solución a una prueba de trabajo (*proof of work*) al igual que hace la propuesta de Szabo. La cantidad de dinero que se crearía sería proporcional a la dificultad del problema y el establecimiento de esta dificultad se determinaría por toda la red mediante un **sistema de votación** (de ahí la importancia de un canal sincronizado y que no pueda congestionarse).

Y aquí aparece un problema, si existiera un ordenador que tuviera una capacidad de cómputo muy superior al resto (en conjunto), puede inundar la red con nuevo dinero antes de que la dificultad pueda ser recalculada por el total de ordenadores que forman la red. Vemos un esbozo, con matices porque no es exactamente igual salvo por lo de la capacidad de cómputo, del **ataque del 51%** del que se habla mucho en el mundo Bitcoin y sobre el que luego volveremos.

Además de explicar la creación de dinero, el primer protocolo también explicaría cómo se produciría el envío de dinero, de un usuario anónimo A, a otro usuario anónimo B, y la gestión de los contratos que entre ambos puedan llegar a producirse. En este caso, introduce la figura de un árbitro que se encargaría de mediar en caso de disputa y la existencia de una compensación por la no satisfacción.

En el segundo protocolo, en vez de que todos los ordenadores tengan una copia del dinero que pertenece a cada pseudónimo, existiría un subconjunto de stos que serían los encargados de realizar el trabajo anterior. Dado que no existen garantías de que estos no se comportasen de manera deshonesta, deberían dejar una cantidad en depósito y publicar periódicamente los saldos a fin de poder ser auditados.

Al igual que sucede con el caso anterior de bit gold, **B-Money** solamente ha sido una propuesta teórica y nunca se ha implementado. Podéis consultar el trabajo de Wei Dai en su web:

http://www.weidai.com/bmoney.txt

Por finalizar estas pequeñas reseñas históricas sobre los trabajos previos a Bitcoin, avanzar algo de lo que hablaremos al llegar al capítulo dedicado a la criptografía, y es que tanto Szabo como Wei Dai, en sus soluciones se encontraron con un problema típico en el mundo de la criptografía, y que tiene que ver con algunos problemas que tienen los generales cuando están en el campo de batalla. Y si queréis saber de qué va todo esto, no os queda más remedio que seguir leyendo y llegar hasta el capítulo 4, pero antes una pregunta fundamental, ¿quién es ese señor que dice llamarse Satoshi Nakamoto? Esta historia es de las más sugerentes de Bitcoin y os gustará seguro.

2.3 ¿QUIÉN ES SATOSHI NAKAMOTO?

Mucho se ha hablado y se hablará durante mucho tiempo sobre quién es en realidad Satoshi Nakamoto. Lo que nadie puede poner en duda es que, sea una persona o un grupo de personas las que están detrás, su nombre quedará para la historia asociado al de Bitcoin, como creador y desarrollador inicial.

Lo que viene a continuación es una recopilación de lo que se puede encontrar en la Wikipedia, foros, blogs, listas *underground*, y demás fuentes, por lo que la especulación y la inexactitud estoy seguro de que estarán presentes (no podría ser de otro modo), así que si has oído o leído algo diferente a lo que cuento yo, puede que estés más cerca de la verdad de lo que lo estoy yo; hecha la advertencia, sigamos.

El origen de Nakamoto podría ser japonés, aunque esto es una suposición que se basa en lo declarado en su perfil de la **P2P Foundation**, en donde aparece que es de origen nipón y que tiene una edad de 37 años. A partir de ahí se saben pocos datos con certeza, salvo que estuvo implicado en el desarrollo del proyecto Bitcoin desde 2007 y que fue reduciendo sus aportaciones hasta finales de 2010. A día de hoy se da como cierto que no participa activamente en su desarrollo.

La clave PGP que utilizó se creó unos pocos meses antes de la fecha del bloque génesis de Bitcoin, y puede consultarse desde la siguiente dirección:

http://forum.bitcoin.org/Satoshi_Nakamoto.asc

¿Por qué se pondría alguien manos a la obra para hacer algo como Bitcoin? Buena pregunta, pues en casi todos los sitios hacen referencia a una posible pista que dejó en el bloque génesis de Bitcoin, y que dice literalmente "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks". Este titular apareció obviamente en *The Times* el 3 de enero de 2009 y se refiere a los excesos y la inestabilidad que el sistema de reserva fraccionaria ha introducido en el mundo financiero.

Este argumento sería bastante sólido si además tenemos en cuenta las siguientes citas que se le atribuyen:

"Sí, [no encontraremos una solución a los problemas políticos en la criptografía,] pero podemos ganar una batalla crucial en la carrera armamentística y ganar un nuevo espacio de libertad por varios años".

"A los Gobiernos se les da bien cortar las cabezas de una red con control centralizado como Napster, pero las redes P2P (redes entre pares) puras como Gnutella y Tor parecen estar resistiendo".

"Resulta muy atractivo el punto de vista libertario si conseguimos explicarlo bien. Soy mejor con el código que con las palabras, sin embargo".

Hay quien a partir de la primera versión del software y de los mensajes publicados ha hecho algunas conjeturas sobre la personalidad de Nakamoto, en los términos siguientes: la versión 0.1 del cliente de Bitcoin solo apareció para Windows, y no disponía de interfaz de línea de comandos. Fue compilada usando Microsoft Visual Studio, y tiene un formato de código irregular, elegante en ciertos aspectos y menos cuidado en otros, por lo que se especula que el autor tiene una gran cantidad de conocimiento teórico pero no tanto a nivel de programación, aunque curiosamente, esta versión 0.1 era muy completa cuando se distribuyó, y si es cierto que solo trabajó él en el proyecto, debió dedicarle muchas horas.

Dado que el código no fue documentado nunca en japonés, se duda de que su origen pueda ser realmente este país y se cree como más probable un origen británico por el uso que hace del inglés, aunque intenta introducir cuando escribe giros americanos para enmascararlo sin mucho éxito.

Todos estos aspectos: código irregular, cantidad de trabajo realizado y el uso del lenguaje, son los que sugieren que Nakamoto no puede ser una sola persona, sino el esfuerzo colaborativo de un grupo de desarrollo con las ideas muy claras. En caso de ser una sola persona, desde luego sería un maestro del juego del despiste.

En el desarrollo del cliente al principio solo trabajaba él (o ellos), y todas las modificaciones posteriores son suyas. Raramente aceptaba contribuciones, hasta que en 2010 fue contactando con otros desarrolladores y cedió el proyecto a **Gavin Andresen** antes de desaparecer definitivamente.

ENTONCES…

Aunque **Gavin Andresen** ha cedido recientemente su puesto a **Wladimir van der Laan** para tener más tiempo como jefe científico de la **Fundación Bitcoin**.

Hay un dato curioso o al menos a mí siempre me ha llamado la atención sobre la figura de Satoshi Nakamoto. Al poner en marcha la red Bitcoin, el número de mineros que había creado moneda era muy pequeño, y la complejidad era muy baja, y por tanto, estos *early adopters* amasaron auténticas fortunas al precio actual, en forma de Bitcoines. En el caso particular de Satoshi, se asume que 1.000.000 de Bitcoines (unos 230 millones de dólares a 230$ al día de escribir esto) estarían en su poder, pero lo más curioso es que ninguno de estos ha sido utilizado nunca. Quizás porque de hacerlo, la pseudoanonimidad de Bitcoin habría servido para saber quién es realmente, curiosos que están pendientes de lo que sucede con esas primeras direcciones creadas en la naciente criptomoneda no faltan y cualquier mínima sospecha de que pasa algo con ellas rápidamente se publicita.

ENTONCES…

Durante el verano de 2015, se produjo un poco de revuelo porque parecía que alguno de los Bitcoines de las direcciones supuestas de Satoshi habrían experimentado un movimiento. Sin embargo, posteriormente se comprobó que todo fue una falsa alarma debido a un control no implementado en la web blockchain.info

Aparte de esta información que acabo de resumir en los párrafos anteriores, poco más se puede saber sobre Satoshi Nakamoto, pero es ahora cuando viene la

parte más divertida de toda la historia. El penúltimo capítulo en la búsqueda de quién es Satoshi Nakamoto lo ha escrito la revista *Newsweek*, desvelando a su juicio quién es el verdadero Satoshi el pasado 6 de marzo de 2014.

Para los reporteros de esta revista, se trataría de **Dorian Prentice Satoshi Nakamoto**, un japonés-americano de 64 años de edad y que viviría a las afueras de Los Ángeles en California. A nivel biográfico los datos que se han recopilado de él han sido por terceras personas, y no porque Dorian haya hecho declaraciones.

Según parece nació en Beppu (Japón) en 1949 y se mudó a California con su madre y hermanos al finalizar la Segunda Guerra Mundial. Estudió en la Universidad Politécnica de California y trabajó para varias empresas importantes como **Hughes Aircraft**, **Radio Corporation of America**, la **Federal Aviation Administration** y otras compañías tecnológicas. Actualmente Dorian está jubilado, vive en Temple City (California), es aficionado a los trenes en miniatura, conduce un Toyota Corolla y sigue un modo de vida muy modesto, que contrastaría con la supuesta riqueza que atesora en forma de Bitcoines.

Según la periodista **Leah McGrath Goodman**, que entrevistó al supuesto autor, este dijo y cito:

"Ya no estoy involucrado en esto y no puedo discutir sobre ello".

Para a continuación rechazar todas las preguntas que se le hicieron posteriormente. Como era de suponer, el aluvión de críticas no tardó en llegar, cuestionando los métodos utilizados para realizar la investigación, y poniendo en tela de juicio si no estaríamos ante un intento por poner en primera línea a *Newsweek*, después de los problemas financieros a los que la revista se ha enfrentado en los últimos años para subsistir.

ENTONCES…

Newsweek fue fundada en 1933 por **Thomas J. C. Martyn** y adquirida en 1961 por *The Washington Post*. Los problemas financieros de *Newsweek* hicieron que *The Washington Post* acabara vendiéndola en 2010 por el precio simbólico de un dólar, al magnate de equipos de sonido Sidney Harman. Antes de su muerte, ocurrida al año siguiente, Harman unió *Newsweek* con el sitio The Daily Beast, de IAC/InterActiveCorp., con Tina Brown como editora, en una acción que buscaba ayudar a ampliar su audiencia en línea. El plan fracasó y *Newsweek* canceló su versión impresa al final de 2012. La revista digital fue vendida en agosto pasado por una cantidad no revelada a IBT, propietaria de publicaciones en línea como *International Business Times*, *Medical Daily* y *Latin Times*.

El artículo estrella para conmemorar sus 80 años de historia y reedición en papel sería precisamente el haber encontrado a Satoshi Nakamoto. La pregunta que muchos nos hacemos es: ¿estamos ante la verdad o es un simple mecanismo barato publicitario para relanzar la versión impresa otra vez?

Y es que Dorian ha negado cualquier implicación y afirma que desconocía la existencia de Bitcoin hasta hace pocas semanas, cuando después de ser contactado por la reportera en el mes de febrero, su hijo le llamara y utilizara el término:

"Después de que me hubiera contactado una reportera mi hijo me llamó y utilizó la palabra, la cual jamás había oído con anterioridad".

Añadiendo que poco tiempo después, la reportera se presentó en su casa y que él llamó a la policía, dado que nunca dio su consentimiento para ser entrevistado. Y ha dicho que sus palabras fueron malinterpretadas, aludiendo a que el inglés es su segundo idioma. Os dejo lo que en declaraciones posteriores Dorian dijo al reportero de *The Associated Press* que le entrevistó posteriormente y quien le preguntó sobre la frase anterior:

"Estoy diciendo que ya no estoy en la ingeniería, eso es todo y aun si lo fuera, cuando nos contrataron yo firmé un documento… un contrato diciendo que no divulgaría ni revelaría ninguna información durante y después del empleo, así que eso es lo que he dado a entender. Sonaba como si estuviera involucrado antes con Bitcoin y miro cómo estoy involucrado ahora, eso no era lo que quería decir, quiero aclarar ese malentendido, no reglamentado e inestable".

Ante estas afirmaciones, **Leah McGrath Goodman** apareció en programas de **Bloomberg TV** y **CBS Morning News** para defender su reportaje ante el desmentido de Dorian Nakamoto de que él es el padre de Bitcoin. La propia *Newsweek* ha emitido un comunicado sosteniendo la veracidad de la investigación y la necesidad de tener que contratar seguridad para Goodman ante las amenazas que la periodista ha recibido, aunque incluso aquí mucha gente opina que la revista se precipitó al publicar el reportaje antes de tiempo y sin conclusiones claras. Para echar más leña al fuego, el propio hermano de Nakamoto afirmó a *Newsweek* que su hermano negaría todo.

El editor de *Newsweek*, **Jim Impoco**, dice que estaba preparado para la tormenta de críticas y defiende el artículo diciendo que la investigación fue realizada siguiendo los mismos estándares de calidad que han guiado a la revista en sus 80 años de historia.

Después de estas nuevas declaraciones de *Newsweek*, Dorian ha contratado al abogado **Ethan Kirschner**, para a través de él hacer un comunicado oficial en el que vuelve a negar su implicación en la creación de Bitcoin y al que de momento *Newsweek* no ha contestado:

"No creé, inventé o trabajé de ninguna manera con Bitcoin. Niego sin reservas el reportaje de Newsweek".

Pero, ¿habría un método fácil de saber si este hombre es en realidad el personaje que buscamos? Difícil de contestar por no decir imposible, lo que no sería tan difícil sería que alguien de manera voluntaria demostrase que es el padre de Bitcoin. ¿Cómo?, muy sencillo, y lo entenderéis mejor cuando lleguemos al capítulo 4 sobre criptografía y veamos el concepto de clave pública y privada.

Por resumirlo mucho y para lo que ahora nos importa, nos basta con saber que una clave pública solo pertenece a una clave privada, dado que la clave pública de Satoshi Nakamoto es pública y conocida (más arriba os he dicho de dónde obtenerla), bastaría con que firmase un mensaje con su clave privada y lo distribuyera para que todos pudiéramos descifrarlo usando la clave pública y decir a coro, "vaaaaleeee, tú creaste Bitcoin", o al menos fuiste lo suficientemente inteligente como para robar la clave privada a su legítimo propietario y ahora hacerte pasar por él.

Recientemente, Dorian ha concedido una entrevista a uno de los medios Bitcoin más reconocidos, *Bitcoin Magazine*, donde explica toda la historia y avatares que le han sucedido desde que su nombre se asoció al de Nakamoto y a Bitcoin. Otra lectura complementaria que también os recomiendo.

Personalmente y después de leer el artículo, opiniones varias, y las declaraciones de Dorian, creo que desde Newsweek se han columpiado de lo lindo y que este pobre hombre se ha llevado un susto de cuidado; aunque quién sabe, igual puede aprovechar el tirón y aparecer en un par de programas de televisión previo paso por caja, o por qué no, denunciar a *Newsweek* por difamación; eso sí, que le paguen en Bitcoines, ¿cómo lo veis?

Por cierto, a los pocos días de aparecer el nombre de Dorian Satoshi vinculado al de Satoshi Nakamoto (¡vaya lío!), se difunde un mensaje desde la cuenta de la Fundación P2P, donde se publicó el primer mensaje del creador de Bitcoin hace cinco años, con el texto: "No soy Dorian Nakamoto", añadiendo un poco más de misterio a la verdadera identidad de nuestro héroe.

2.3.1 Una de espías

Lo más gracioso de todo el asunto es que la historia sobre quién es el padre de Bitcoin no acaba con lo que acabamos de ver, aún hay más, sobre todo si os gustan las teorías de la conspiración, sois fans de 007 y el mundo del espionaje os apasiona. Si os ha parecido divertida la historia de *Newsweek*, no dejéis de leer lo que sigue a continuación.

¿Os acordáis de un tal **Edward Snowden**? Bueno, pues resulta que entre algunos de los documentos secretos revelados, hay uno que relaciona de manera

directa a la NSA **(National Security Agency)**, la famosísima Agencia de Seguridad Nacional estadounidense, y Bitcoin.

Y no las relaciona de cualquier modo, todo lo contrario, en un memorando de nombre "Operación Satoshi", sería la propia NSA el padre de la criatura, quienes la habrían creado bajo la apariencia de ser una moneda irrastreable y anónima, cuando lo cierto es que se comportaría más como una especie de caballo de Troya monetario, y dado que el que la usa lo hace de manera voluntaria, estaría entrando en el juego de la NSA sin saberlo, y creyéndose a salvo de los tejemanejes de los gobiernos y Estados, en este caso del estadounidense.

Todo un guión digno de un Óscar.

Sin embargo, vamos a suponer que estuviera la NSA en la concepción original de Bitcoin, ¿qué pasaría?, ¿estaría comprometido Bitcoin? Yo os doy mi punto de vista y que cada cual saque sus propias conclusiones.

Que la NSA quiera controlar Bitcoin no es algo que pueda sorprendernos, lo raro sería que no quisiera hacerlo (por ejemplo, no hace mucho que se ha conocido que el error denominado como **Heartbleed** en el protocolo **OpenSSL** ha podido ser explotado por las agencias americanas por años). Pero no seamos ilusos, ¡ojalá solo fuera la NSA!, vamos, que no hay quien se pueda llegar a creer que los rusos, los chinos, los británicos, los alemanes, los israelíes… o cualquier otro servicio secreto no esté interesado en lo mismo que la NSA, por mucho que sus países se hayan posicionado en contra de Bitcoin. Otra cosa es el nivel de recursos de los que dispongan para hacerlo y no puedan, porque de interés, de eso os aseguro van sobrados.

ENTONCES…

Edward Joseph Snowden es un consultor tecnológico americano, antiguo empleado de la CIA y de la NSA. Se hizo famoso en junio de 2013, cuando a través de los periódicos *The Guardian* y *The Washington Post*, hizo públicos documentos clasificados como de alto secreto sobre los programas de la NSA, incluyendo a **PRISM** y **XKeyscore**. Huido de EE. UU., ahora mismo se encuentra en un lugar desconocido en Rusia, en donde el Gobierno de este país le ha concedido asilo político durante un año. Los gastos de Edward están siendo sufragados por **Wikileaks**. Considerado como traidor por unos y patriota por otros, su futuro es incierto.

Bitcoin está en manos de toda la comunidad de Internet, por lo que posibles fallos en su implementación original o puertas traseras no dejarían de ser problemas

con una duración limitada en el tiempo, hay muchos ojos mirando como para que alguna oscura intervención no se detectara, y esto es algo muy bueno y que hace de Bitcoin la mejor de las criptomonedas, la enorme base de gente que está interesada en usarla a todos sus niveles, desde usuarios que solo compran o venden, desarrolladores que mejoran su código, emprendedores que inician nuevos servicios, etc.

Pongamos el ejemplo de Mt. Gox (hablo luego sobre este operador), poco se ha tardado en filtrar y publicar el código fuente de la plataforma, junto con mucha más información como hemos visto. Y ahora sabemos al menos que el señor Karpeles no ha jugado limpio con sus clientes.

Sobre el supuesto total anonimato, ya hemos dicho que no es del todo cierto y lo estudiaremos más adelante, por tanto quien opera con Bitcoines y se ha preocupado de interesarse por su funcionamiento, no creo que se sorprenda tampoco mucho de esta particularidad, ni se rasgue las vestiduras al saber que el anonimato no es total.

Otro aspecto es el famoso **ataque del 51%**, también conocido y que se supone podría producirse en el caso de tener un *pool* computacional lo suficientemente potente como para dominar el resto de la red, controlando el 51% de la misma. Cuando hablemos sobre criptografía hablaré un poco sobre el modelo de computación cuántica y los posibles escenarios que tendríamos en esa situación.

Por resumir, yo, personalmente, no acabo de ver claro que la NSA sea la que esté detrás de Bitcoin.

2.3.2 Los lingüistas al rescate

¿No te ha gustado la historia anterior? No hay problema, aún podemos añadir un poco más de color a la búsqueda de Satoshi Nakamoto, y ahora de la mano del **Centro de Lingüística Forense** de la **Universidad de Aston** en Birmingham (Inglaterra).

Si recordáis, cuando comencé a explicar quién era Satoshi Nakamoto, lo primero que dije fue que, por su forma de escribir, podíamos deducir algunos datos. ¿Podemos saber algo más aplicando técnicas forenses al análisis de textos? Bueno, pues eso es lo que 40 estudiantes del último curso de lingüística forense y dirigidos por su profesor Jack Grieve quieren averiguar con su estudio llamado "Proyecto Bitcoin".

Y es que aparte de Dorian Nakamoto, otros nombres que se han barajado como posibles Satoshi a lo largo de estos años han sido los siguientes:

- Vili Lehdonvirta
- Michael Claro
- Shinichi Mochizuki
- Gavin Andresen
- Nick Szabo
- Jed McCaleb
- Dustin D. Trammel
- Hal Finney
- Wei Dai
- Y el trío formado por Neal King, Vladimir Oksman y Charles Bry.

Teniendo en cuenta que todos ellos tienen publicaciones, lo que ha hecho el equipo de Jack Grieve es analizar las similitudes lingüísticas existentes entre estas y el artículo original de Bitcoin, y no les cabe la menor duda de que la mayor probabilidad de ser el auténtico Satoshi Nakamoto cae en **Nick Szabo**, del que hemos hablado anteriormente.

Según los autores del estudio la probabilidad de que Nick Szabo sea el autor original es muy elevada, aunque no pueden descartar que fuera ayudado por otras personas, y afirman que el número de similitudes lingüísticas entre los escritos de Szabo y Bitcoin es asombroso, y que ninguno de los otros posibles candidatos resulta ser tan bueno como para ser nuestro enigmático personaje.

Entre los rasgos lingüísticos distintivos, y que aparecen tanto en los textos de Szabo como en el artículo sobre Bitcoin, están las expresiones "cadena de...", "para nuestros propósitos", "la necesidad de...", "por supuesto", "siempre y cuando", "como por ejemplo" y "solo", utilizadas en numerosas ocasiones; las contracciones; las comas antes de "y" y "pero", los adverbios terminados en "-mente", y los pronombres "nosotros" y "nuestro" en trabajos de un solo autor.

¿Tiene peso y base este trabajo? Personalmente creo que sí y más aún cuando hace unos meses apareció otra investigación realizada por **Skye Grey** en donde llegaba a las mismas conclusiones que el estudio de Jack Grieve. ¿Quiero decir con esto que Szabo es Satoshi Nakamoto? Afirmar eso sería muy pretencioso por mi parte, aunque las evidencias hacen pensar que tal vez y de algún modo sí que estuvo relacionado con la elaboración del texto, igual fue quien lo revisó, editó y publicó, y coordinó el trabajo inicial de un grupo de personas.

En cualquier caso, la pregunta aún sigue abierta. ¿O tal vez no? Sigue leyendo…

ENTONCES…

El pasado 16 de octubre de 2015, Satoshi Nakamoto fue premiado por *The Economist* con el **Premio a la Innovación 2015** en la categoría "Sin Fronteras" (*No Bounderies Award*), compartiendo el premio con empresas de la talla de Tesla y Alibaba entre otras. Aunque quizás más destacable y sorprendente es la nominación para el premio **Nobel de Economía** que ha recibido por parte del doctor en Finanzas **Bhagwan Chowdhry** de la Universidad de California (UCLA), sin embargo la candidatura ha sido desestimada porque nadie anónimo puede recibir el premio. Este año el ganador ha sido el escocés **Angus Deaton** con sus estudios sobre consumo, pobreza y bienestar.

2.3.3 Desde Australia con amor

Fijaos en si es cierto lo que os comentaba de lo rápido que gira el mundo, que estaba haciendo la revisión final del libro para entregarlo a la editorial, cuando me encuentro de bruces con un artículo sobre Satoshi Nakamoto y un nuevo sospechoso de ser nuestro enigmático personaje; un poco más tarde y salimos desactualizados de fábrica, cosa que no digo yo que no acabe por pasar.

En la televisión y la radio se hicieron eco de la noticia unos cuantos días después de que circulara por el submundo informático, y quizás de no haberse producido un registro en plan hombres de Harrelson de su casa, no se habría ni comentado; como se suele decir, es lo que hay, tampoco es que hayan dado mucha información, salvo que se tomaba al asalto la casa del presunto creador de Bitcoin (bueno, la casa y también las oficinas de su empresa, esto tampoco se ha contado, supongo que cuando salga este libro habrán dado más información).

Hágase la luz y veamos quién es el nuevo personaje que tenemos entre manos y demos un salto hasta las antípodas de nuestro país y situémonos en el país de los canguros, os prometo que esta nueva historia es también de lo más emocionante; no sé, quizás debería hacer un juego sobre todo esto, dado que cómic ya hay, ¿qué opináis?

Es probable que el nombre de **Craig Wright** no os diga mucho, para ser sinceros yo no lo había oído nunca. Craig es un australiano, que pensaba mudarse a Reino Unido (entiendo que por su relación con ciertos organismos del país) y su nombre, junto con el de su compañero fallecido **Dave Kleiman** (las cosas se ponen interesantes con esta muerte) se ha asociado al de Satoshi Nakamoto por las investigaciones realizadas por las revistas *Wired* y *Gizmodo*. En su particular búsqueda del padre de Bitcoin, ambas han llegado a las mismas conclusiones, pero ojo, ninguna de las dos lo afirma categóricamente (supongo que no quieren meter la pata como *Newsweek*) y solo dejan apuntando el dedo hacia Craig y su difunto amigo.

Y es que *a priori* tiene un perfil que encajaría perfectamente para serlo, aparte de ser un multimillonario *business man*, tiene estudios de derecho, matemáticas y estadística, un doble doctorado (posible porque los últimos datos pueden apuntar a que esto no es cierto), es académico de la **Universidad Charles Sturt** y desde 2012 es el vicepresidente ejecutivo de **Estrategia de Desarrollo para el Centro de Estrategia Ciberespacial y Ciencias de Seguridad del Reino Unido**… con este currículum podría pensarse de él que es un genio.

También es muy llamativo el perfil del difunto Dave Kleiman, veterano del Ejército americano como técnico de helicópteros y famoso en el mundo de la seguridad y el análisis forense informático, con varios libros publicados y apariciones en canales como la CNN y ABC. La vida de Dave es muy interesante y desconcertante en algunos aspectos. Después de dejar el Ejército trabajó en la Oficina del *sheriff* del Condado de Palm Beach, donde conoció al que luego sería su socio **Patrick Paige** con el que fundó la empresa **Computer Forensics**, con la que adquirió gran reputación como consultor en seguridad. Una de las cosas que por lo visto siempre llamaba la atención de este hombre era su sentido del humor, incluso después de haber quedado parapléjico en 1995 por un accidente, siempre demostró (según todas las fuentes que he consultado) un estado de ánimo y una predisposición hacia la vida excelentes. Algo que parece cambió de manera repentina, meses antes de su muerte. Abandonó el hospital de veteranos donde vivía para recluirse en su casa y evitar el contacto con cualquier persona (incluidos sus más íntimos amigos) y allí estuvo hasta que una infección acabó con su vida, encontrándose días después su cadáver a medio descomponer, rodeado de botellas de alcohol, heces y una pistola que habría sido disparada contra un colchón. Sin embargo en el momento de escribir esto, no se ha encontrado el casquillo de bala, lo que deja abiertas las puertas a más de una teoría "conspiranoica".

Tanto Craig como su difunto amigo David Kleiman siempre han pasado desapercibidos respecto a lo que a Bitcoin se refiere, si revisáis la lista anterior de posibles sospechosos nada hubiera podido apuntar a esta posibilidad.

¿Y cómo *Wired* se interesó o se fijó en Craig? De un modo un tanto absurdo, o al menos a mí me lo parece. En la última conferencia **Bitcoin Investor's Conference** de Las Vegas celebrada en octubre de 2015, había una ponencia donde entre otros ponentes (estaba Szabo también) estaba Craig por videoconferencia. La presentadora le pidió que se presentase y él comenzó a contar un poco quién era, pero sin dar demasiados detalles sobre su relación con Bitcoin. La presentadora le interrumpió y le pidió que fuera un poco más conciso con desde cuándo conocía la criptomoneda, y él dijo que desde sus primeros momentos; la presentadora siguió insistiendo, tal vez tratando de sacar algo más a la luz, aunque personalmente he visto el vídeo y me parece un poco traído por los pelos el que a partir de estas preguntas

y las contestaciones dadas por Craig, *Wired* lo hubiera marcado como sospechoso de no tener algo más antes. A partir de aquí y de una serie de pruebas que aporta posteriormente (donde el propio Craig afirma ser el inventor de Bitcoin), marcan a Craig como Satoshi Nakamoto y elaboran un artículo explicándolo, al que se suma el aparecido en *Gizmodo*, con reportero cámara en mano y todo, que se presenta en la casa de Craig para preguntarle si es Satoshi, obteniendo por respuesta la puerta en las narices. Tanto un medio como el otro habrían sido contactados por un *hacker* que filtró la información que publican, parece ser que esta información llegó antes de la conferencia de Las Vegas, solo así se entendería que la presentadora le interrumpiese e insistiera para que "se descubriera", de otro modo, no le veo mayor sentido.

La entrada en su casa y oficinas por los agentes de seguridad se hizo justamente a los pocos días de publicarse la noticia de ser Satoshi Nakamoto, aunque la Policía Federal Australiana afirma que fueron motivos fiscales los que motivaron el asalto y no otras cuestiones. En caso de ser cierto lo que dicen estos agentes, habría sido una casualidad muy oportuna, claro que a estas alturas no sé quién piensan que puede creerse semejante historia.

Añadamos aún más carne al asador, y para darle más morbo, es que a los pocos días de hacerse pública la noticia, aparece otra vez un mensaje (un correo en este caso), del estilo del que apareció cuando se vinculó a Dorian con Satoshi, pero desde la dirección **satoshi@vistamail.com**, que es la supuestamente usada siempre por Satoshi Nakamoto, que dice: "No otra vez esto. Yo no soy Craig Wright. Todos nosotros somos Satoshi":

[bitcoin-dev] Not this again.

satoshi at vistomail.com satoshi at vistomail.com
Thu Dec 10 06:54:46 UTC 2015

- Previous message: [bitcoin-dev] Segregated Witness features wish list
- Next message: [bitcoin-dev] Forget dormant UTXOs without confiscating bitcoin
- **Messages sorted by:** [date] [thread] [subject] [author]

I am not Craig Wright. We are all Satoshi.

- Previous message: [bitcoin-dev] Segregated Witness features wish list
- Next message: [bitcoin-dev] Forget dormant UTXOs without confiscating bitcoin
- **Messages sorted by:** [date] [thread] [subject] [author]

More information about the bitcoin-dev mailing list

Figura 2.9. Mensaje de Satoshi diciendo que no es Craig

Pero dado que una dirección de correo se puede falsificar y los servidores de correo pueden *hackearse*, hay quien pone en duda la veracidad de la autoría del mensaje, y se cree que fue enviado por alguien que quiere o bien proteger al verdadero Satoshi o con la negativa, apuntar aún más a Craig como autor. Como dije antes, si el verdadero Satoshi quiere despejar cualquier duda de su identidad, puede mandar un mensaje cifrado con su clave privada para que todos podamos verificarlo con su clave pública.

ENTONCES…

Esto del *hackeo* de las cuentas de correo de Satoshi tiene también su historia. En septiembre de 2014, un *hacker* (Degavas1337) consiguió entrar en una de las múltiples cuentas de correo usadas por él (*satoshin@gmx.com)* y supuestamente con la información contenida en ella llegó a establecer su identidad real. Todo parecía indicar que haría pública esta información, sin embargo no lo hizo y se especula que igual intentó extorsionar y chantajear a Satoshi con resultado incierto. La historia sigue abierta, hasta el punto de que **Roger Ver**, uno de los evangelizadores y empresarios más afamados de Bitcoin, llegó a ofrecer una recompensa de **36,7 BTC** a quien diera información sobre el atacante, porque al parecer se trataría de la misma persona que entró en su cuenta de correo.

¿Tienen base las pruebas presentadas por *Wired* y *Gizmodo*? A la luz de lo que se ha ido publicando en Reddit, Motherboard y otros medios similares, todo parece indicar que el cúmulo de pruebas aportado ha sido deliberadamente manipulado para parecer que son reales, y aunque se ha tenido mucho cuidado en hacerlo, las evidencias parecen demostrar que todo es un montaje para señalar a Craig y su amigo como Satoshi Nakamoto. Que las claves PGP presentadas no coincidan con las de este, que claves adicionales se creasen por software que no existía cuando se lanzó Bitcoin, que las cuentas de correo puedan ser *hackeadas*, que haya evidencias de modificaciones en los rastros *online* de Craig en los que aparece Bitcoin donde antes no estaba, o que el mismo Craig haya desaparecido del mapa sin dar explicaciones, a mí me hace cuestionarme que todo esto sea real. ¿Ha sido todo orquestado por Craig? ¿Tiene algún enemigo que lo ha hecho? ¿Tiene problemas con el fisco australiano y este es un movimiento de promoción para ganar notoriedad? ¿Tiene problemas de personalidad como afirma su abogado que dice que Craig realmente cree que inventó Bitcoin? ¿Mienten los familiares y socios de Craig o dicen la verdad? Muchas preguntas y pocas respuestas que resulten claras al ciento por ciento.

No es que a mí personalmente me importe quién sea Satoshi, su contribución es lo que me importa. Tantas pruebas circunstanciales pueden dar que pensar, pero está todo tan perfectamente dirigido y hay tantas evidencias de manipulación, que sigo pensando en Szabo como el más probable Satoshi Nakamoto, pero mientras el verdadero Satoshi quiera seguir estando en la sombra, dudo mucho que lleguemos a dar con él realmente. La historia de Craig promete darnos más de un buen cotilleo que no perderemos de vista, de eso sí que estoy completamente seguro.

2.3.4 BitcoinComic. Tras los pasos de Satoshi Nakamoto

Tal es el interés que ha suscitado la identidad de Satoshi Nakamoto, que hace pocos meses se puso a la venta el cómic *Bitcoin: La caza de Satoshi Nakamoto*. Escrito por **Alex Preukschat** y **Josep Busquet** e ilustrado por **José Ángel García Ares**, e iniciado como un proyecto de *crowdfunding* que logró recaudar más de 20.000 euros para hacer que viera la luz.

La historia está llena de guiños a conceptos criptográficos (por poner un ejemplo, los personajes principales son Alicia y Bob, dos nombres clásicos que se utilizan siempre en criptografía cuando se trata de explicar el funcionamiento de los algoritmos de cifrado) y a las diferentes visiones que se dan de Bitcoin, y todo ello mientras los protagonistas tratan de dar cuenta, en una trepidante aventura, de quién es el misterioso Satoshi Nakamoto.

Mención especial merecen también los anexos del libro, con los nombres de las personalidades más relevantes hasta el momento de la comunidad Bitcoin internacional y de habla hispana. Y guías con información adicional para aquellos interesados en adquirir más conocimientos sobre la criptomoneda.

La edición en castellano puede adquirirse tanto en papel como en edición digital, y se editará también en inglés y en polaco (si no lo han sido ya).

Y dado que Álex tuvo la amabilidad de asistir como ponente a una de las charlas que dimos en uno de los *Meetups* de Madrid (y ahora es uno de los miembros organizadores del evento) para contarnos como se gestó el libro, os dejo una fotillo que nos hicimos al acabar su presentación.

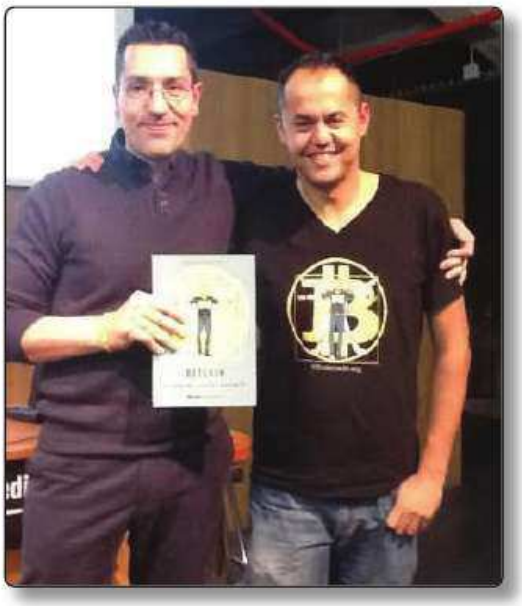


Figura 2.10. Con Álex (derecha) y BitcoinComic

Como nota curiosa, una edición especial de este libro-cómic estuvo circulando por el mundo de la mano de **Juan Llanos de Bitreserve** (ahora Uphold) y recabando las firmas de las personas más ilustres dentro del panorama Bitcoin. El cómic, que fue subastado durante la pasada **laBITconf**, ha conseguido la nada despreciable cifra de 20,4 BTC (unos 8.500 dólares en el momento de la subasta), los adjudicatarios **Rodolfo Andragnes** y **CoinFabrik** tienen ahora en sus manos un poquito de la historia de Bitcoin que hará que más de uno (me incluyo) se muera de envidia (y eso que yo tengo mi propia versión del cómic firmada por Álex).

El dinero recaudado irá a parar a la fundación **BitGive**, que destinará el dinero a su proyecto **Donación Transparente**, que intenta revolucionar la forma en que las ONG manejan las donaciones y rinden cuentas sobre su uso, una iniciativa que desde aquí siempre aplaudiré.

En las referencias tenéis la URL desde donde podéis ver las fotos de los diferentes personajes con el libro. Solo faltaba Satoshi, aunque quién sabe, igual estaba por allí y no lo sabíamos.

2.4 APLICACIONES DE BITCOIN

Hasta aquí, creo que podemos decir que tenemos una idea clara de los orígenes de Bitcoin y de los planteamientos iniciales que hay detrás de todas las criptomonedas, que tal vez, con algún que otro matiz, siguen la misma concepción. Sin embargo, una moneda tiene que ser posible de usar para algo, eso de la liquidez que os contaba antes, el para qué o por qué puedo cambiarla me interesa tanto como el hecho de poder guardarla, y es aquí donde paramos nuestro viaje en este capítulo, para ver los posibles usos que Bitcoin puede tener. Fijaos en que en esta parte voy a explicar los usos, por decirlo de algún modo, estándares y actuales y que ven Bitcoin como una moneda en el sentido estricto de la palabra. Más adelante, en el último capítulo del libro, hablaremos de los usos futuros y de las posibles aplicaciones que se están barajando, tanto para Bitcoin, como para la cadena de bloques; estoy convencido de que vais a sorprenderos, pero no nos adelantemos.

2.4.1 Pagos por Internet

Probablemente esta opción es la más corriente, si Bitcoin es una moneda, habrá sitios en donde podré cambiarla por algo que me interese. Y estás completamente en lo cierto, ¿qué puedo comprar con Bitcoines? Pues prácticamente de todo lo que se te ocurra, cada día hay más sitios donde lo aceptan y es que algo de las propiedades del buen dinero que defendía Aristóteles, alguno que otro parece que sí se las ve.

El inicio de las compras con Bitcoin es como casi todo lo que rodea a la moneda, curioso y poco común. Comenzó el 22 de mayo de 2010, cuando un programador de Florida llamado **Laszlo Hanyecz** y activo miembro del foro BitcoinTalk, anunció en este que pagaría 10.000 Bitcoines a quien le comprara dos *pizzas*. El reto quedó lanzado en la Red y sería otro programador, pero de Reino Unido, quien cogió el guante tirado por Laszlo y ni corto ni perezoso compró telefónicamente dos *pizzas* de *pepperoni* en el establecimiento **Papa John's de Jacksonville** con su tarjeta de crédito, y pidió que se las entregaran a Laszlo, quien pagó los 10.000 Bitcoines prometidos al recibirlas. Obviamente la transacción no puede considerarse una compra típica, pero hay pocas cosas típicas en Bitcoin, de ahí que resulte tan disruptivo. Lo que está claro es que los 25 dólares que costaron las *pizzas*, actualmente equivaldrían a un buen puñado de millones de dólares, por lo que ostentan el récord de las *pizzas* más caras de la historia. Actualmente el 22 de mayo es un día de celebración para la comunidad Bitcoin que lo ha bautizado como el **Bitcoin Pizza Day** y se suele quedar para celebrarlo.

ENTONCES…

Concretamente en Madrid este año se celebró en el restaurante **DoEat** de la calle María de Molina.

Wikileaks, Wordpress, Dell, Overstock, Mega, Destinia, Reddit (que forma parte de Avance Publications, una de las corporaciones más grandes de Estados Unidos), Domino's Pizza, 9flats, Expensify, Virgin Galactic… la lista es tan grande que no podríamos referenciar a todos los establecimientos que día a día se van sumando y que ofrecen sus productos y servicios a cambio de Bitcoines. Y la lista sería aún más grande si tenemos en cuenta la posibilidad de "cargar" **tarjetas regalo con Bitcoines**, y que son aceptadas en algunos de los sitios más importantes de este planeta como son Amazon o eBay.

Uno de estos ejemplos lo tenemos con la empresa norteamericana de tarjetas regalo **eGifter**, quien mediante asociaciones con empresas que actúan como pasarela de pago, como es el caso de **GoCoin**, permiten comprar sus tarjetas usando Bitcoines (aunque también permiten hacerlo usando Litecoin y Dogecoin). Otros ejemplos que hacen esto mismo son **Snapcard** o **Gyft**. Aunque estas empresas aún no operan en España dan una idea de las posibilidades de este sistema adicional para, usando una pasarela entre nuestros Bitcoines y las monedas fíat, permitir acceder a muchos más servicios y productos, aunque en este caso no sería usando Bitcoines de un modo estricto.

Figura 2.11. eGifter, tarjetas regalo compradas con Bitcoines

Hay un par de páginas web que pueden ser útiles para ver cómo va evolucionando la aceptación de Bitcoin y quiénes se suman a su uso. La primera es la página de **Trade de la wiki de Bitcoin** (*en.bitcoin.it/wiki/Trade*), la otra es **coinmap.org**, ambas son de paso obligado (aunque se actualizan más lentamente de lo que sería deseable) para echarles un vistazo de vez en cuando para ver cómo evoluciona la aceptación del Bitcoin como medio de pago.

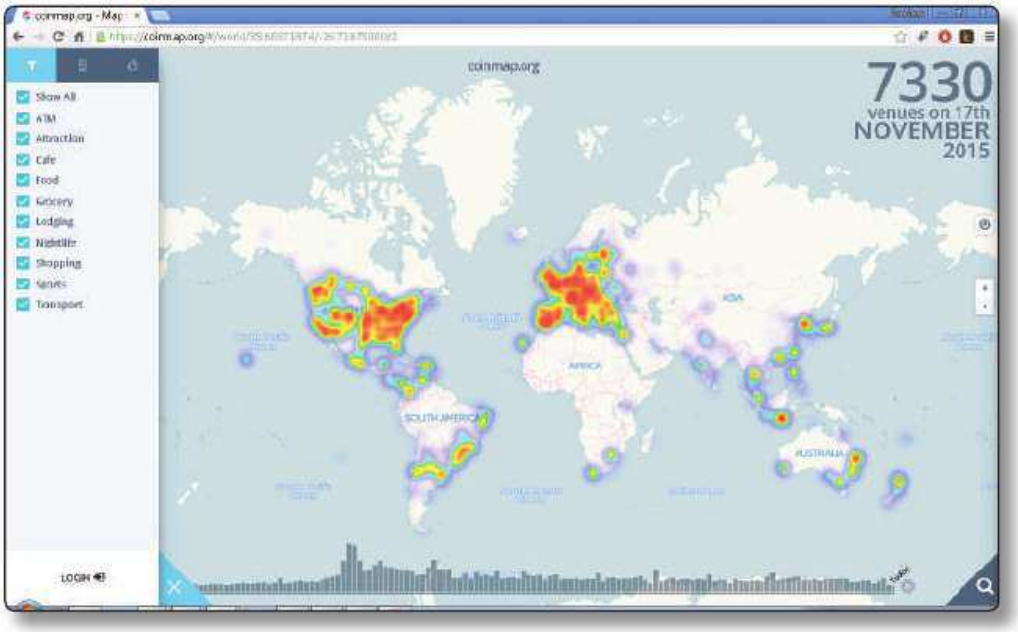


Figura 2.12. Homepage de coinmap.org

Quizás uno de los mayores inconvenientes o críticas que recibe Bitcoin de cara a la compra de productos y servicios sea su irreversibilidad. A diferencia de lo que sucede en un sistema como PayPal, donde tenemos un período de tiempo que permite echar atrás el pago de un bien (las causas para hacerlo son múltiples, por ejemplo, no lo recibimos en el tiempo acordado o nos llega defectuoso), Bitcoin no permite esta posibilidad. Una vez que una transacción se ha efectuado, efectuada queda, no se puede volver atrás.

Antes de que alguno salga huyendo y deje de leer, pensemos un poco sobre la naturaleza de cómo se efectúa la reversibilidad en los sistemas de comercio electrónico actuales; otra pregunta que quiero que me respondas: ¿quién nos garantiza la irreversibilidad en un sistema como PayPal (o VISA, Mastercard, etc., cualquiera nos sirve)? En este caso es PayPal, un tercero de confianza que no tiene nada que ver ni con el comprador ni con el vendedor, es decir, el control del fraude es un servicio que está disponible para los usuarios que utilizan este medio de pago y que es útil desde el punto de vista del comprador, porque seguramente desde el punto de vista del vendedor, estaríamos en el lado opuesto: ¿por qué enviar un producto a un usuario que puede cancelar el pago alegando casi cualquier cosa? Fijaos en el esquema que sigue PayPal para las disputas en este caso:

Figura 2.13. El sistema de disputas de PayPal (fuente: PayPal)

Sin citar que PayPal tiene una guía que recomienda a todos sus usuarios seguir para evitar este tipo de situaciones junto con un equipo de especialistas que proporcionan asesoramiento y consejos. Por tanto, el control del fraude no es algo que por sí mismo forme parte de la moneda usada, euros, yenes, dólares, etc., es decir, no estoy más protegido contra la irreversibilidad por el hecho de usar euros, lo estoy porque hay alguien que por detrás me está protegiendo con un servicio añadido. Sin embargo si le compro unas Ray-Ban a uno de los "vendedores" del top manta del Retiro y estas están defectuosas, que alguien me explique cómo se hace la reversibilidad de

la operación. Tal vez este ejemplo del top manta puede ser un poco extremo, pero lo cierto es que tendemos a comprar siempre en establecimientos que nos garantizan que se puede revertir la operación, pero ¿cuántos comercios una vez que has comprado lo permiten? Salvo las grandes cadenas, como El Corte Inglés, FNAC, Zara… el resto no lo permiten y la operación efectuada, efectuada queda (por no decir que muchas veces ni siquiera nos devuelven el dinero, sino que nos dan un vale para comprar otra cosa dentro del establecimiento; si esto es reversibilidad que me lo expliquen).

Con Bitcoin sucede lo mismo, salvo que ahora la responsabilidad es más nuestra como usuarios, ¿no deberíamos ser cada uno de nosotros responsables de nuestro dinero?, al menos mientras aparezcan empresas que me brinden el servicio que ya brinda PayPal, creo que debería ser de este modo. Ahora bien, Bitcoin ya no está tan en sus inicios, y esta particularidad ha sido tratada por empresas como **btcrow.com** o **escrowcoin.net**, que ofrecen servicios de intermediación en los procesos de compras con Bitcoines.

Este tipo de empresas utilizan generalmente dos tipos de técnicas diferentes para implementar el proceso:

- **Bitcoin Escrow**: consiste en cifrar una dirección Bitcoin con tres claves alfanuméricas muy grandes (106 caracteres) y en donde se deposita el dinero. Una de las claves se da a un tercero de confianza que es el encargado de liberar el dinero cuando las partes involucradas en la operación dan su conformidad.
- **Two-Factor Bitcoin**: en este caso, en vez de tres claves se cifra la dirección Bitcoin con dos claves, no hay un tercero de confianza por lo que se recomienda usar solamente en casos donde existe cierta confianza en la otra parte. Para liberar el dinero, tanto emisor como receptor deben proporcionar su clave de cifrado sobre la dirección que guarda el dinero.

Figura 2.14. Homepage de BTCrow

Ninguno de los dos sistemas es perfecto y se les puede sacar más de una objeción, sin embargo estoy seguro de que en un futuro próximo aparecerán nuevas y mejores formas de implementar servicios de control del fraude ante la irreversibilidad de las transacciones que resultarán más transparentes para los usuarios. Quizás sobre estas mismas soluciones, ya que el código está disponible en la red para ser estudiado, modificado y por supuesto mejorado.

2.4.2 Servicios de bancarización mundial

Nosotros vivimos en el primer mundo, y claro, sucede que muchas veces pensamos que los servicios y las comodidades de las que disfrutamos están disponibles en cualquier lugar del planeta, cuando la realidad es justamente la contraria, y si bien es cierto que los niveles de pobreza se reducen a medida que los años van pasando, aún queda mucho camino por recorrer. Cualquiera que me conoce sabe que soy muy optimista sobre el futuro que nos espera.

Uno de estos servicios comunes que disfrutamos son los servicios bancarios, y es que según el informe **Global Findex del Banco Mundial**, aunque el nivel de acceso a servicios bancarios ha pasado, entre 2011 y 2014, del 51% al 62% de los adultos del mundo, todavía significa que casi un 40% de la población mundial carece de este tipo de servicios.

Fijaos en que igual alguien puede pensar que caigo en contradicción, en el primer capítulo he criticado la gestión ineficaz que los bancos han realizado y las políticas económicas ineficientes a las que nos han sometido y ahora vengo a hablar de las bondades de la bancarización. No confundamos las cosas, el concepto de bancarización en sí mismo, y el acceso a unos servicios financieros que permitan el desarrollo económico y social no son solo buenos sino además deseables. El quid de la cuestión es cómo conseguirlos de una manera que resulte equitativa y con la que todos ganemos; es decir, ¿en manos de quién están los servicios financieros que proporcionan la bancarización y cómo la proporcionan?, porque el modo en el que lo hemos venido realizando hasta ahora no parece que vaya a seguir funcionando, por lo menos a largo plazo, por las razones que expliqué.

Por ejemplo, en Sudamérica, **Chile es el país más bancarizado** y el segundo de toda Latinoamérica, superado solo por **Panamá**. En México, sin embargo, solo 4 de cada 10 personas, y que podrían tener acceso a servicios bancarios, no disponen de ellos, y la cifra es importante, porque hablamos ni más ni menos que de casi 40 millones de personas y eso solo teniendo en cuenta a este país. Según uno de los últimos informes (2012) de la **Federación Latinoamericana de Bancos (FELABAN)**, la situación de los países latinoamericanos es la siguiente:

País	% bancarización medida en función del volumen de los depósitos entre su PIB
Chile	68%
Uruguay	51%
Honduras	47%
Paraguay	40%
El Salvador	40%
Bolivia	38%
Guatemala	37%
Costa Rica	36%
Brasil, Nicaragua y Colombia	35%
Perú	28%
Ecuador y Argentina	26%
México	21%
República Dominicana	20%

Que resulta muy llamativa teniendo en cuenta que estos valores se mueven en torno al 90% si miramos cualquier país desarrollado. Si viajamos al continente africano, la situación es si cabe aún más dramática, y es normal que hayan surgido alternativas que traten de llenar este vacío de las que ahora hablaremos. Para Bitcoin, un continente con una población de más de 1.100 millones de personas puede presentar también una enorme oportunidad. Personalmente creo que África será de donde gran parte de los usuarios de Bitcoin vendrán a futuro, donde los sistemas de pago tradicionales o no están desarrollados o simplemente no existen de ninguna manera.

Los motivos por los cuales existe esta baja bancarización son de muy diversa índole, aunque yo diría que se debe a una combinación de pobreza, sistemas jurídicos inseguros que no garantizan los derechos de los individuos y de la propiedad, falta de competencia entre las empresas, que tienen complicada su subsistencia a causa de esta falta de bancarización, y al no existir formas de medir el riesgo que conlleva dar créditos (aunque visto lo visto durante la crisis de 2008, no creo que nadie pueda dar lecciones sobre valoración de riesgos) la actividad económica se paraliza, y sin actividad económica no se genera empleo y resulta difícil salir de la pobreza. Es decir, un círculo vicioso difícil de romper, ¿o tal vez no; quizás Bitcoin pueda llegar hasta donde otros no llegan?

En África por ejemplo está sucediendo algo muy interesante: por un lado no parece que entre los países puedan llegar a ponerse de acuerdo en tener una moneda

común, como ha sucedido con Europa y el euro. Por otro lado, los diferentes sistemas bancarios nacionales no tienen una fuerza y estabilidad como la que puedan tener los sistemas del primer mundo (recordar el caso de la hiperinflación anterior), ni siquiera si se comparan con los de Latinoamérica, que a pesar del estado anteriormente comentado, están un paso por delante. Sin embargo, África está experimentando un crecimiento espectacular en cuanto al desarrollo de la telefonía móvil, y si hace apenas unos años era casi imposible comunicarse por móvil, actualmente es el continente con mayor crecimiento del mundo según la Asociación Internacional de Operadores de Telefonía Móvil.

Los datos que esta asociación publica son verdaderamente impactantes, porque en el año 2012 el número de tarjetas SIM superó los 738 millones, bastante delante de los 500 millones que se activaron en EE. UU. y se espera que se llegue a un valor próximo a los 1.000 millones para finales de este año. La forma en que el 65% de los africanos usa el móvil para comunicarse es a través de tarjetas prepago, con un interés creciente por los servicios de Internet a través de estos. Uno de los datos que más me han llamado la atención es la situación de Kenia, que tiene un 87% de teléfonos móviles, y solamente el 21% de cuentas bancarias, el caldo de cultivo perfecto para soluciones basadas en pagos por móvil y cómo no con Bitcoin como protagonista.

ENTONCES…

Es Kenia donde la mayoría de empresas de pago por móvil tienen su base de operaciones.

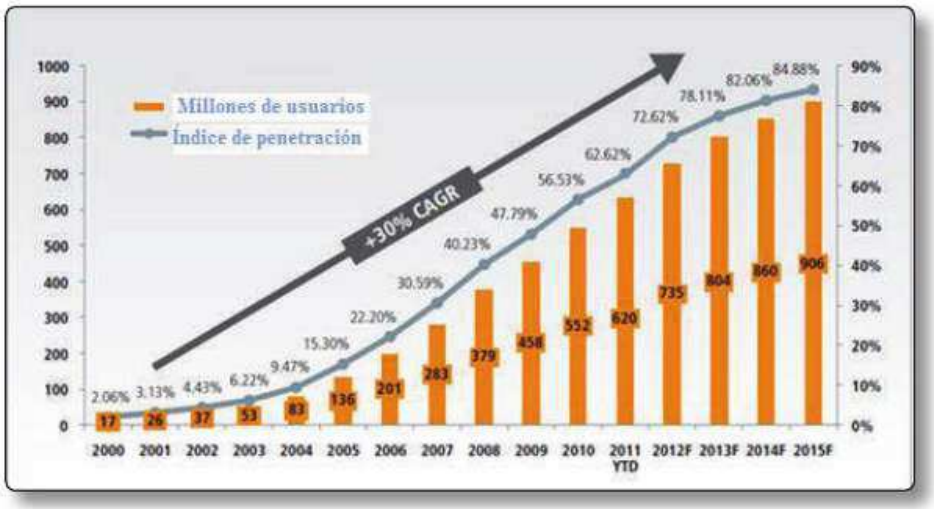


Figura 2.15. Usuarios de móviles en África (fuente: *http://fundacionkhanimambo.org/*)

Las empresas no están siendo ajenas a esta realidad y están viendo oportunidades para cubrir un hueco muy significativo y que producirá, no tengo la menor duda, un nivel de desarrollo en el continente africano que podrá ser el motor para llevarlo a una nueva era de prosperidad.

Quizás la compañía que tiene una estructura más madura en África para esto de los pagos por móvil, más que nada porque detrás está un gigante de las comunicaciones, sea **M-Pesa**, un juego de palabras que viene de M de móvil y Pesa que significa dinero en *swahili*. Es un producto de la compañía **Safaricom** que fue lanzado al mercado en 2007, que a su vez es filial de **Vodafone**, y permite realizar pagos con el teléfono móvil y enviar y recibir dinero entre los usuarios, entre otro amplio abanico de posibilidades. La idea detrás de M-Pesa es muy buena y el hecho de que cada vez más usuarios utilicen sus servicios es un ejemplo de su buena salud, sin embargo, para poder ponerse en marcha, necesitó de la aprobación del Banco Central de Kenia.

Aquí es donde Bitcoin puede entrar en acción. Ejemplo de esto que estoy diciendo lo tenemos con la empresa **Bitsoko**, que ha sido la agraciada por la **Fundación Bill y Melinda Gates** con la beca "Servicios Financieros para los Pobres" de 100.000 dólares, para ayudarla a expandir sus servicios de procesamiento de pagos en Bitcoines para comerciantes en Kenia, Ghana, Zimbabue y Sierra Leona (aproximadamente entre los tres se acercan a los 100 millones de personas); iniciativa que de funcionar bien y cumplir los objetivos podría ampliar la beca hasta 1 millón de dólares.

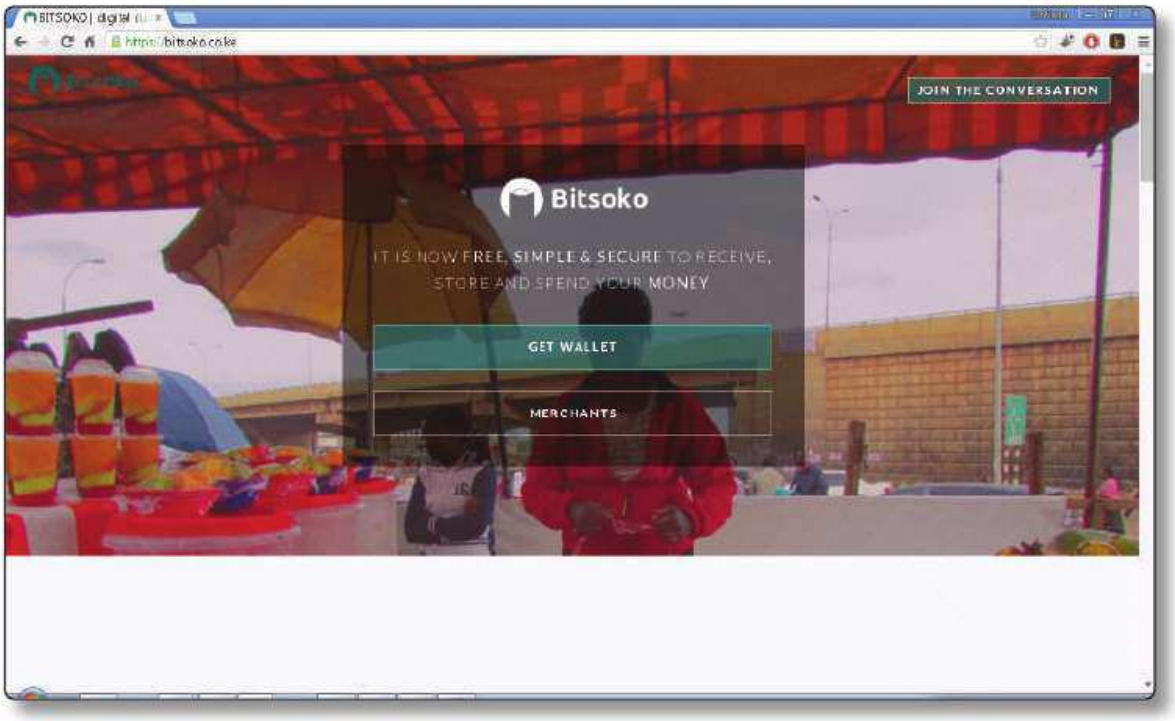


Figura 2.16. Homepage de Bitsoko

A los esfuerzos de Bitsoko se unen también los de otra empresa Bitcoin, **BitPesa**, que en febrero de 2015 consiguió cerrar una ronda de financiación de más de un millón de dólares para expandir sus servicios de remesas a otros países de África. Y es que BitPesa, que tiene sede en Nairobi, se constituyó como un servicio de envío de dinero entre Kenia y Reino Unido y ahora quiere seguir con Ghana, Tanzania y Uganda.

ENTONCES…

BitPesa mantiene ahora una demanda contra Safaricom por intimidación de suspensión de servicios, ya que Safaricom está exigiendo a BitPesa que cuente con licencia del Banco Central de Kenia para seguir funcionando y usando su red de comunicaciones. No se lo están poniendo nada fácil a las empresas Bitcoin en África tampoco. A raíz de toda esta discusión, el Banco Central de Kenia hizo un comunicado recordando a sus ciudadanos que las criptomonedas no son legales en el país, y la fallida Kipochi, la primera *startup* que lanzó sus servicios en Kenia y acabó por desaparecer, ha manifestado: "Deseo suerte a BitPesa: hicieron lo mismo con nosotros en Kipochi"

Estos dos ejemplos, BitPesa y Bitsoko, son solamente la punta del iceberg, algo que ya se demostró en la pasada conferencia **Bitcoin Africa Conference** de 2015 y que promete ser mejor este año.

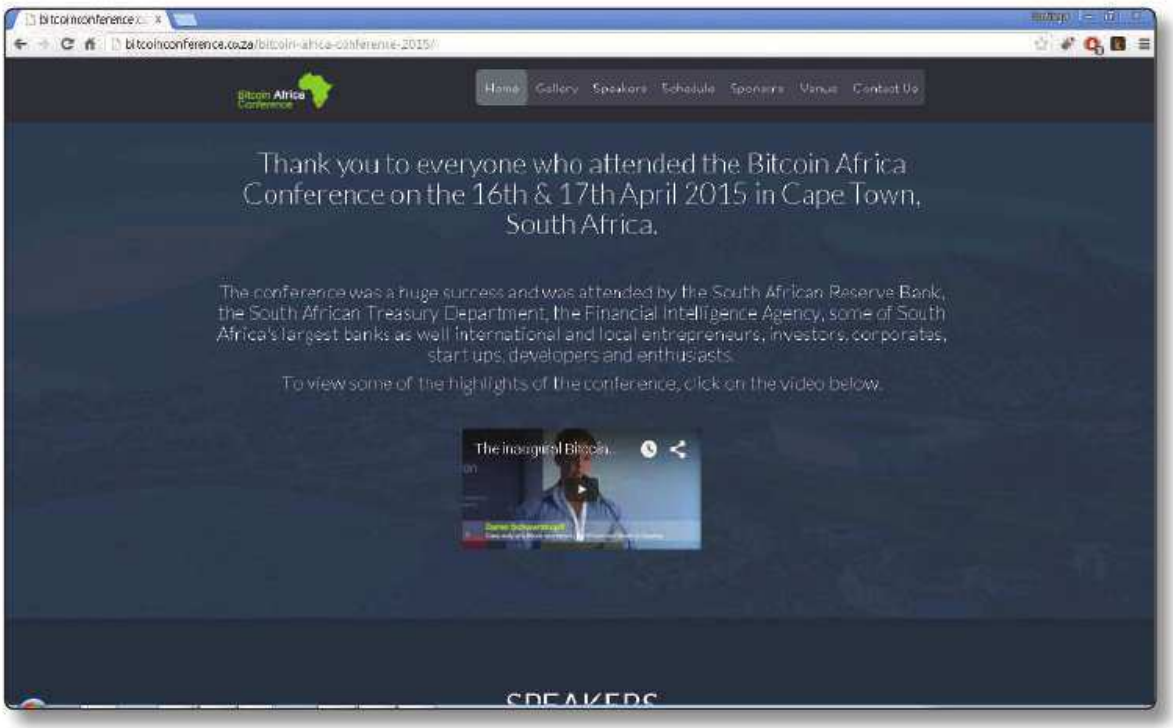


Figura 2.17. Bitcoin Africa Conference

2.4.3 Envíos de remesas

Otro de los posibles usos de Bitcoin lo encontramos en el envío de remesas, como una alternativa muy seria que podría reducir los costes de este tipo de operaciones y que enlaza de manera muy directa con el epígrafe anterior, una parte importante del desarrollo económico de un país subdesarrollado depende de ello.

Una remesa son los fondos que los emigrantes envían a su país de origen, habitualmente a sus familiares y que en muchos casos suponen la fuente de ingresos principal de estos. Ni que decir tiene que ha sido el aumento de las corrientes migratorias las que han propiciado el nacimiento de este tipo de envíos de dinero.

Según la Wikipedia los países más beneficiados por las remesas han sido China, Filipinas, México, Polonia, Bangladés, Pakistán y Marruecos, incrementando la cantidad de dinero que reciben año tras año.

El problema de las remesas radica en el costo que llevan asociadas. Según los datos trimestrales que publica el Banco Mundial es Sudáfrica el país donde es más costoso enviar dinero (un 16,79%) y Rusia y Arabia Saudita los más baratos (en torno al 4%). El medio más barato es usando una oficina de correos, y se dispara si se usan servicios bancarios tradicionales, que superan el 10% de media, quedando en término los operadores de transferencias de dinero del tipo Western Union. En cualquiera de los casos, la disponibilidad del dinero en destino siempre lleva un retraso, de unas horas, en el mejor de los casos, hasta varios días en el peor de ellos.

Viendo estos datos, cualquier alternativa que reduzca estos costes de operación será bienvenida por los usuarios de envíos de remesas. No es de extrañar que las compañías que ofrecen servicios de remesas utilizando Bitcoines hayan comenzado a florecer, con unos costes al usuario que están entre el 1% y el 3%, muy por debajo de los valores que hemos comentado antes y una disponibilidad en destino que es simplemente insuperable, porque es prácticamente instantánea (cierto que está el tema de las confirmaciones de las transacciones que veremos luego, pero es un problema secundario).

Personalmente creo que el reto de Bitcoin como solución para el envío de remesas está en su alta volatilidad, aunque es un problema que como ya expliqué debería irse resolviendo a futuro. Lo cierto es que actualmente mientras que un usuario cambia Bitcoines por su moneda local, puede encontrarse con una desagradable sorpresa si al cambio Bitcoin bajó su cotización respecto de esta (aunque también podría pasar justo lo contrario), en cualquier caso, la posibilidad está ahí abierta.

2.4.4 Micropagos: donaciones y propinas

Un micropago (o *micropayment*) es un pago que un usuario A realiza a otro usuario B de forma electrónica, de una **cantidad de dinero muy pequeña**. No parece que haya un consenso claro sobre cuánto de pequeña debe ser esta cantidad para considerarse como un micropago, cantidades menores de 10 euros se asume que estarían dentro de esta categoría, pero un micropago puede ser algo tan pequeño como una gratificación al autor de un artículo que te ha gustado de 5 céntimos de euro.

El reto de los micropagos es muy interesante, porque cualquier sistema tradicional que lleve asociado enviar dinero de una persona a otra tiene un **coste de transacción**, coste que en el caso de los micropagos se vuelve aún más importante porque puede suponer, respecto a este, un valor considerable que implique que el micropago no resulte a cuenta realizarse, por ser desproporcionado uno (coste) respecto del otro (el micropago). Es decir, los conceptos de micropago y bajo costo van inevitablemente de la mano. Nueva oportunidad para Bitcoin de posicionarse como una alternativa a las soluciones clásicas como veremos a continuación, donde un nutrido grupo de empresas están tratando de aprovechar las ventajas de la criptomoneda para facilitar estas operaciones.

Varios son los motivos por los cuales los micropagos se están convirtiendo en un elemento indispensable para la evolución de Internet, aunque casi todos, o al menos los más importantes, están relacionados con la generación de contenidos y la forma en que estos contenidos se monetizan para los usuarios que los crean. Tradicionalmente, la forma en la que una web obtiene sus ganancias suele deberse a la inclusión de anuncios (*banners*)/publicidad.

ENTONCES…

Existen otras técnicas para monetizar una web, como la venta de espacio publicitario, botones de donaciones, programas de afiliados, etc.

Sin embargo, todos sabemos que la publicidad en muchas de estas webs llega a ser en ocasiones sumamente molesta, no ya porque a veces algunas páginas están tan saturadas de anuncios que resultan incluso difíciles de leer, sino porque también suele servir para rastrear nuestras compras o enviarnos publicidad sin nuestro consentimiento; se hace necesario buscar una solución óptima.

Son los micropagos esta solución que buscamos, a la vez que permiten a un usuario monetizar sus contenidos, resuelven el problema de la publicidad excesiva en los sitios y mejoran sustancialmente el anonimato del usuario. Además, cada vez

se demanda contenido de más calidad en la web, y la única manera de que este contenido siga siendo accesible a un coste cercano a 0 es precisamente si los autores de los mismos son capaces de obtener una rentabilidad por ellos. La fuerza de los muchos pocos, que combinados hacen posible la viabilidad de un sitio web mostrando contenido casi gratis. Y esto que estoy ejemplificando con la web es válido para los videojuegos, el vídeo por demanda, apuestas, deportes… y cualquier cosa que se te pueda pasar por la cabeza.

Alternativas para la implementación de micropagos hay muchas fuera del entorno de Bitcoin. Por ejemplo, Minipay o Micropayments de IBM, Millicent de DEC, Paystone, BitPass, PepperCoin, Patreon, PayPal… hay una buena lista de opciones que se pueden elegir, pero todas comparten la característica de ser soluciones propietarias, basadas en sus propios sistemas internos de gestión y con sus propias comisiones.

Si cambiamos al mundo Bitcoin, el primer nombre asociado a los micropagos que encontraréis es **ChangeTip**, perteneciente a la empresa americana Chaincoin, que ha sido de las primeras en popularizar esto de las propinas (las *tips* en inglés) mediante una solución, que es posible integrar fácilmente en YouTube, Twitter, Google+, Instagram, Reddit… y que es tan fácil de usar como hacer "me gusta" en Facebook, aunque incluye otras alternativas como el envío de propinas por correo electrónico o por SMS.

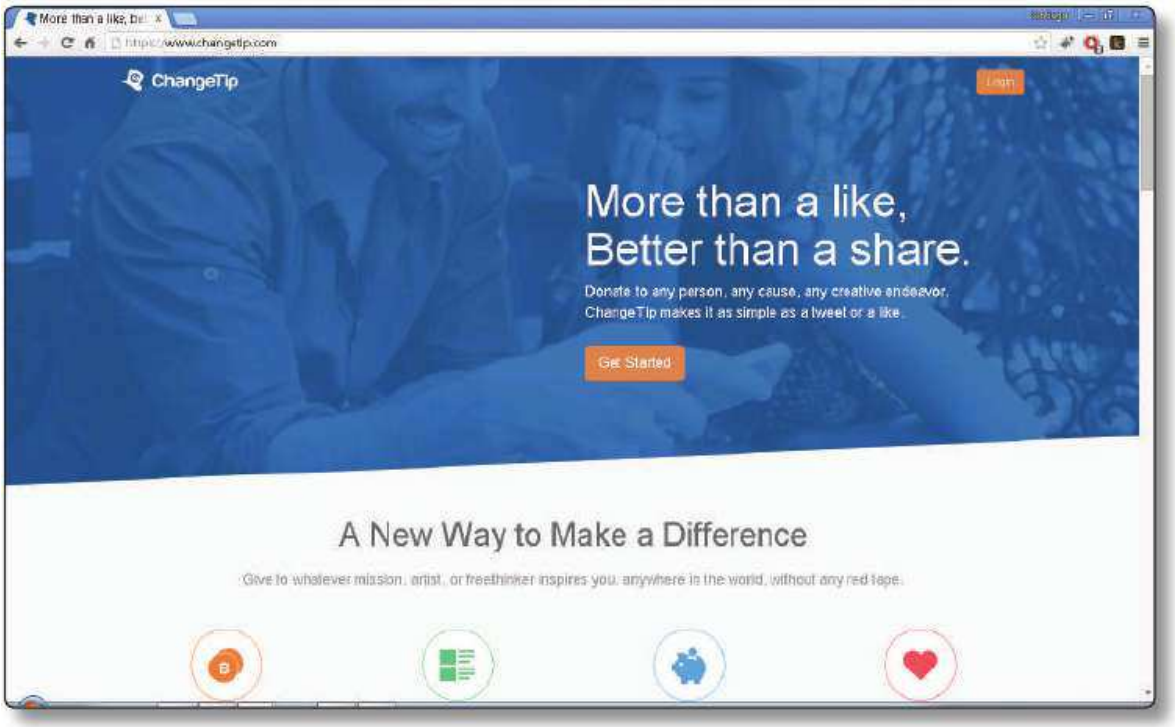


Figura 2.18. ChangeTip

Si hasta aquí te gusta lo que estás leyendo, ¿por qué no me envías una propina?

Figura 2.19. Envíame una propina ;-)

Otras empresas Bitcoin que hacen uso de la posibilidad de hacer micropagos son:

- **BitWall**: utiliza lo que llama un muro de pago, de manera que si quieres acceder a un contenido tienes que hacer un pequeño pago (un céntimo por ejemplo) usando Bitcoin. Tiene planes de cuotas diarias para poder acceder a más contenido de manera global.

- **Xapo**: el modelo usado por la empresa del argentino Wences Casares es un poco diferente, aunque está especializada en el almacenamiento *online* de Bitcoines, permite enviar propinas de hasta 100 bits usando un *hashtag* en Twitter (#xapotip). Como curiosidad, si se usan direcciones de Xapo la transacción es inmediata, tardando casi una hora en otro caso.

- **Tippercoin**: también permite el envío de micropagos por Twitter, ligando la cuenta del usuario con una dirección Bitcoin. Lo más destacable es que si una propina no es "rescatada" por su receptor en un máximo de 21 días, se envía de nuevo al emisor.

- **Tibdit**: incluye un *plugin* para WordPress que se puede insertar en las páginas de un blog. Permite tanto Bitcoines como tarjetas de crédito o débito. Como inconveniente reseñar que para poder usarlo tienes que comprar "Tibs" usando Bitcoines o una tarjeta, a partir de lo cual carga tu cuenta de Tibdit.

- **Cryptiv**: la novedad que presenta es que los envíos de propinas se pueden hacer sobre Twitter y YouTube, sin ningún coste, porque se hacen fuera de la cadena de bloques.

2.5 ALGUNAS DEFINICIONES PREVIAS

¿No está mal, verdad? Ya sabemos para qué puede ser útil Bitcoin y el abanico de posibilidades os aseguro que no hace sino ampliarse a medida que Bitcoin es conocido y aceptado. Ahora demos una nueva vuelta de tuerca y paremos en una serie de conceptos teóricos, algunos de los cuales han aparecido anteriormente pero no nos detuvimos a explicar. Por cierto, muchos (por no decir todos) son comunes a la mayor parte de las criptomonedas, conocerlos nos sirve por partida doble; además como a lo largo del resto del libro iremos ampliando lo que vamos a contar aquí, nos sirve como una base sencilla para entender lo que vendrá después.

2.5.1 Doble gasto

Y comenzamos por el primer problema que el *paper* de **Satoshi Nakamoto** intentaba resolver en una red distribuida, el problema del doble gasto.

Por doble gasto se entiende que un usuario malintencionado pudiera usar (gastar) la misma moneda virtual en dos lugares diferentes al mismo tiempo. En el mundo físico a esto lo llamamos falsificación, y equivaldría a tener dos billetes iguales (por ejemplo de 1 dólar) para gastarlos en dos comercios diferentes. Que dos billetes de 1 dólar sean iguales significa que tienen la misma numeración.

Una de las grandes bazas que presentan todas las criptomonedas es que eliminan la necesidad de tener un tercero de confianza que garantice que no se produce falsificación de la moneda (o doble gasto), es la propia red la que se encarga de ello mediante el uso de la **criptografía de clave pública**.

Por hacer un símil con el dólar y el emblemático "In God we trust", no es raro encontrar por ahí frases del tipo "In Crypto we trust" o "In Math we trust", haciendo alusión a que ahora la confianza se deposita en la fortaleza de los algoritmos de cifrado o en las bases matemáticas que los fundamentan.

Tampoco es raro encontrarse la frase latina *Vires in numeris*, que se puede traducir por la "Fortaleza de los Números", junto con el símbolo de Bitcoin.

2.5.2 La Bitcoin Foundation

Fundada en septiembre de 2012 como una organización sin ánimo de lucro en los Estados Unidos, se creó con la misión de estandarizar y proteger el proyecto Bitcoin y promover su uso a nivel mundial. Los miembros originales de la fundación incluían a **Gavin Andresen**, **Charlie Shrem**, **Mark Karpeles**, **Peter Vessenes**, **Roger Ver** y **Patrick Murck**. De todos ellos Charlie Shrem, Roger Ver y Mark Karpeles están enjuiciados y encarcelados (de momento Shrem por lavado de dinero y Ver por venta de explosivos), con estos antecedentes no es de extrañar que más de uno vea a Bitcoin como el dinero de los capos y mafiosos. Si a esto le añadimos que gran parte de la comunidad Bitcoin la veía como un posible punto de centralización a una tecnología de naturaleza completamente descentralizada tenemos el caldo de cultivo perfecto para entender lo que ha sucedido a lo largo de estos años y el enorme recelo con el que siempre muchos la hemos visto.

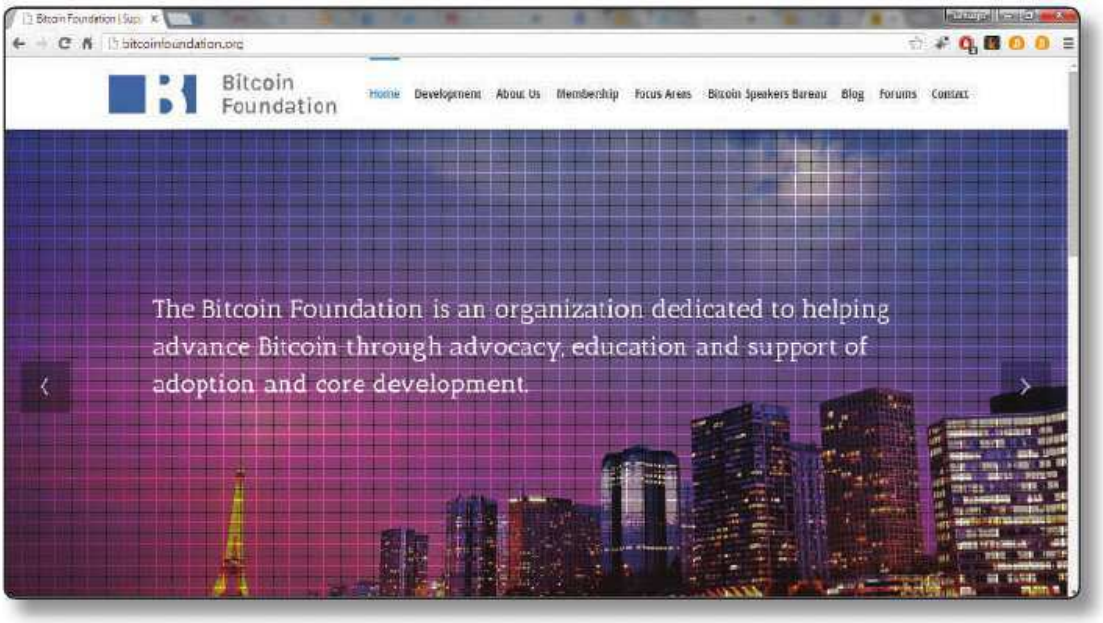


Figura 2.20. La Bitcoin Foundation

Sea como fuera, la Fundación Bitcoin funcionó con relativa normalidad desde su creación hasta abril de este año, superando las alarmantes noticias que iban apareciendo sobre su junta directiva. En abril y al poco de la llegada a la junta directiva de **Olivier Janssens**, afirmó que la fundación se encontraba en bancarrota y que carecía de dinero para soportar los puestos de trabajo teniendo que despedir al 90% de sus empleados, y los que se han quedado lo han hecho como voluntarios.

Los comentarios de Olivier han ido aún más lejos y ha llegado a afirmar que "La Bitcoin Foundation odia la transparencia" y que "si hubieran sido transparentes,

todo el mundo conocería la situación de que no les quedaba dinero", citando además "los gastos ridículos y las decisiones mal pensadas", y ha solicitado la sustitución de toda la junta directiva. Estas afirmaciones tienen su peso porque en 2014 las cuentas de la Bitcoin Foundation contaban con casi 5 millones de dólares, de los cuales solamente 1,8 millones de gasto han sido justificados hasta el momento.

No obstante, además de estas duras críticas, Janssens ha dicho que donará una cantidad de unos 100.000 dólares a un fondo especial destinado a apoyar la moneda digital y crear un nuevo proyecto que a futuro podría reemplazar a la fundación, así como a pagar los sueldos de los desarrolladores principales. Obviamente otros miembros de la junta niegan estas afirmaciones, como es el caso de **Patrick Murck**, director ejecutivo, que dice que aunque no están en bancarrota sí que necesitarían una reestructuración.

¿El futuro de la Bitcoin Foundation? Sin duda incierto, 2016 será un año importante para ellos, veremos si son capaces de renacer de sus cenizas o serán sustituidos por otros proyectos, tal vez liderados por Janssens, o por una nueva alternativa que ha surgido en el horizonte, la **Bitcoin Alliance** liderada por la organización **Coin Center** y un conjunto de empresas del sector; luego hablaremos un poco más de esto.

ENTONCES…

¡Últimas noticias, últimas noticias! Mientras estaba acabando con la revisión final del libro Janssens fue destituido el pasado 15 de diciembre por los desacuerdos mostrados con el resto de la junta directiva de la Fundación Bitcoin. Me reafirmo en lo que escribí, el futuro de esta organización es muy sombrío.

2.5.3 El foro BitcoinTalk

En muchas ocasiones a lo largo de los capítulos de este libro, hago referencia a BitcoinTalk. ¿Cuál es el motivo y por qué es tan importante? La respuesta es muy simple, **bitcointalk.org** está considerado como el gran expositor de mensajes donde todo aquel que tiene que decir algo sobre Bitcoin tiene su lugar para decirlo. Los temas que se tratan son de lo más diverso y abarcarían desde la minería, el *trading*, el desarrollo puro y duro de código, hasta las cuestiones económicas y filosóficas que hay detrás de Bitcoin. En general cualquier cuestión relevante que afecta a Bitcoin suele aparecer publicada aquí en primer lugar. Actualmente hay más de doce millones de entradas.

Los inicios de BitcoinTalk están en manos de Satoshi quien originalmente se basó en un foro de **SourceForge** pero que se perdió. Con el cambio de *hosting* a Sirius, el foro estuvo ubicado durante algún tiempo en **bitcoin.org/smf**, aunque en algún momento se movió a **forum.bitcoin.org**.

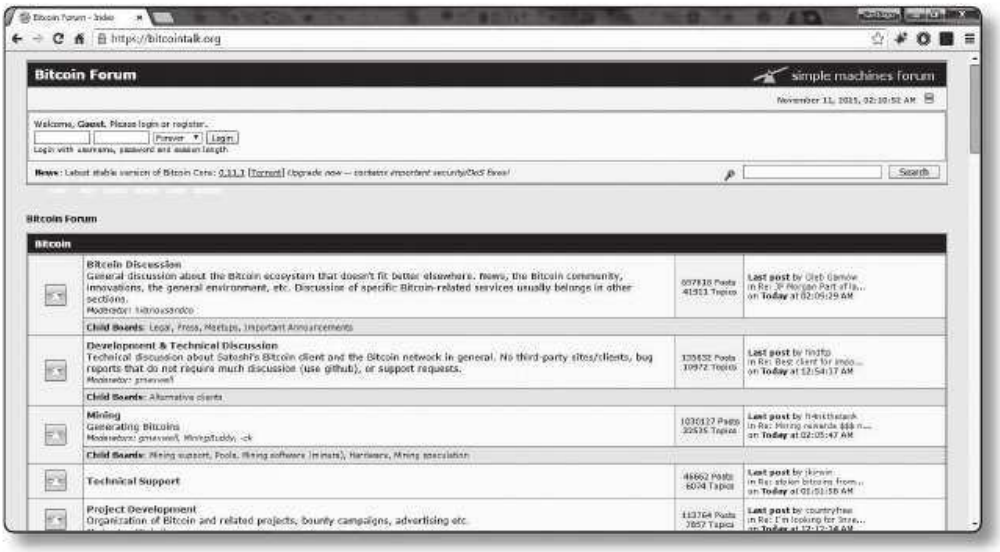


Figura 2.21. Homepage de bitcointalk.org

No fue hasta julio de 2011 cuando BitcoinTalk se mueve a **bitcointalk.org** con el objetivo de no ligarlo al dominio bitcoin.org y hacerlo explícitamente no oficial; en mi opinión hay dos razones para ello:

- La primera es la que tiene que ver con la misma filosofía de Bitcoin, si Bitcoin es un sistema descentralizado, su foro debería serlo también, y cualquiera debería poder crear el suyo con sus políticas de moderación y gestión particulares así como implementarlo con la tecnología que más le convenga.
- La segunda, y que más me convence a mí, sería por evitar controversias en las opiniones que igual pudieran haber aparecido si hubiese estado colgado de bitcoin.org, hasta el punto de que en un primer momento, la entrada al foro desde bitcoin.org redirigía a una búsqueda de Google con el término "bitcoin fórums", entrada que posteriormente, en 2012, se eliminó dejando independiente bitcointalk.org de bitcoin.org.

Esta opción ha demostrado ser una buena estrategia por la variedad de opiniones de toda índole, que a lo largo de los años se han publicado y que de haber estado vinculadas a bitcoin.org podrían haberse considerado como "oficiales", de este modo todo el mundo tiene libertad de decir y expresarse sin necesidad de que esas opiniones se consideren como la postura de bitcoin.org.

2.5.4 Red del tipo P2P

Siempre se dice que Bitcoin (y en general todas las criptomonedas) funcionan en una red del tipo P2P o *Peer To Peer* o red entre pares o red entre iguales y que este esquema es lo que les confiere la enorme potencia y versatilidad de las que disponen.

Las redes P2P son redes descentralizadas, donde no existe ninguna máquina que actúe como servidor central, no hay ni clientes ni servidores fijos, sino nodos que se comportan como iguales (de ahí el nombre) tanto sirviendo información como consumiéndola, con otros nodos de la red. Además, estos nodos, pueden aparecer o desaparecer en cualquier momento, pudiendo conectarse o desconectarse del sistema sin que esto afecte a la red en su conjunto que sigue siendo capaz de funcionar sin ningún problema. Al no existir un nodo central que actúe como maestro, resulta imposible de apagar, porque su cierre llevaría consigo el cierre de todos los nodos que componen la red; en el caso de Bitcoin, equivaldría a tener que apagar Internet, frase que en más de una ocasión verás por ahí publicada. Más adelante os explicaré cómo podéis ver todos los nodos que actualmente están soportando la red Bitcoin.

ENTONCES…

Aunque estoy asumiendo que las redes P2P son descentralizadas, realmente pueden existir arquitecturas P2P con cierto grado de centralización siendo este un criterio que suele usarse para clasificarlas. En el siguiente gráfico podemos ver esta clasificación usando un **grafo de Baran** aplicado a las topologías P2P; a veces se habla de Bitcoin generalmente como descentralizado, sería más correcto hablar de distribuido, daos cuenta de que en la red descentralizada aún puede haber nodos que al dejar de funcionar podrían eventualmente dejar sin cobertura a partes de la red.

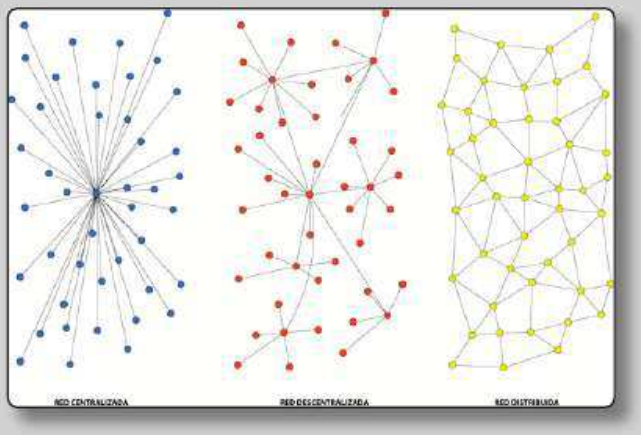


Figura 2.22. Topologías de red P2P (fuente: Wikipedia)

Las redes P2P fueron popularizadas por **Napster**, una aplicación creada por **Sean Parker** y **Shawn Fanning** y que se convirtió en el medio de intercambio de colecciones de música en formato MP3 al inicio del año 2000. Acabó cerrando en septiembre del año siguiente por cuestiones de *copyright* con los autores que demandaron a Napster en masa, teniendo que pagar multas millonarias.

ENTONCES…

Napster acabó fusionándose con **Rhapsody** en 2011, y actualmente dispone de servicios de acceso a su base de archivos musicales (más de 34 millones de canciones) en modalidad gratuita pero limitada y en versión *premium* previo pago.
Otra de las redes P2P más populares, **BitTorrent**, creada por **Bram Cohen**, apareció más o menos por esas fechas, en julio de 2001. Para que os hagáis una idea del volumen de tráfico que maneja, se estima que mensualmente (con datos de 2012), el número de usuarios estaría alrededor de los 250 millones, teniendo en promedio más usuarios activos que YouTube y Facebook juntos.

El germen sembrado por Napster no acabó con las descargas, supuso el comienzo de una nueva era de aplicaciones y la migración de los usuarios de Napster hacia nuevos entornos, hecho que no ha sido frenado ni siquiera por una situación legal complicada y nada homogénea por países.

En España tenemos, por un lado **el artículo 18.3 de la Constitución**, que protege como derecho fundamental el secreto de las comunicaciones, salvo en el caso de una resolución judicial, pero que se da de bruces con la **Ley de Servicios de la Sociedad de la Información y Comercio Electrónico** y la reforma de la **Ley de Propiedad Intelectual** que entró en funcionamiento a principios de 2015 (junto con el canon AEDE, y luego los gobiernos llaman a los usuarios piratas…).

A priori las redes de tipo P2P no presentarían ningún problema, si no hay servidor central difícilmente se les puede aplicar una ley, el problema está en el tipo de contenido que se comparte, que suele estar protegido por derechos de autor (como el caso de la música). De momento, se ha empezado por lo más fácil, cerrar los sitios web que alojan enlaces desde los que descargar contenido, como si eso fuera a servir de algo, las limitaciones por "copia privada" están llenas de ambigüedades y aunque se ha modificado la **Ley de Enjuiciamiento Civil** para que sea más fácil identificar a quien vulnera los derechos de autor, de momento, si hay "buena fe" y no hay "ánimo de lucro" parece que los usuarios "normales" no tendríamos porqué preocuparnos; ¿o sí?

En cualquier caso, al igual que las redes P2P cambiaron la industria musical, esta tecnología y su uso en Bitcoin cambiarán el modo en que funciona el dinero.

2.5.5 Internet oculta

También podéis encontrarla con los nombres de **Internet profunda** (*Deep web*), **Internet invisible** (*Invisible web*), **Internet oscura** (*Dark web* o *Dark net*) e **Internet invisible** (*Hidden web*); con estos nombres no me sorprende que más de uno considere a la Internet oculta como el lado oscuro de la Fuerza.

Realmente la Internet oculta no es más que una parte de Internet que es muy difícil de rastrear, es decir, si no sabemos dónde hay que conectarse y cómo, esta parte de Internet pasará completamente desapercibida para nosotros, por un simple motivo: responderme a la siguiente pregunta, ¿cuando quieres buscar algo en Internet cómo lo haces? El 99% de vosotros me responderá que está claro, preguntado a San Google (o a sus primos hermanos), y aquí está el problema, para Google, las webs que forman parte de la Internet oculta simplemente no existen, no aparecen en sus resultados de búsqueda (o en el caso de aparecer, lo hacen en unas posiciones muy alejadas de las primeras, y ¿cuántos de vosotros pasáis más lejos de la segunda página de resultados?, pues eso), por lo tanto, si para Google no existen, para nosotros tampoco (fijaos en la trascendencia que tiene el que nuestro acceso a los contenidos de Internet se realice mayoritariamente a través de un buscador, otro debate muy interesante pero para el que tampoco tenemos tiempo ni espacio y que podría entrelazarse con la teoría de la exploración de la larga cola).

ENTONCES…

Se estima que el tamaño de la Internet oculta es del orden de 500 veces el tamaño de la Internet superficial. Un estudio en 2010 estimó su tamaño en 550 billones de documentos pertenecientes a unos 200.000 sitios, con una cobertura por parte de los buscadores más importantes que alcanzaba solamente poco más de un 30%.

El término se atribuye a Mike Bergman, que comparó las búsquedas en Internet con la pesca de un modo muy gráfico: “Solo capturas los peces que hay en la superficie, para pescar en las grandes profundidades no basta con navegar solamente, tienes que bajar con traje de buzo y un arpón”.

Las páginas que los buscadores indexan en sus resultados forman parte de la **Web superficial**, esta información resulta relativamente fácil de encontrar y almacenar; no sucede lo mismo con la Internet oculta, que está pensada y diseñada a propósito para pasar inadvertida (pero ojo, no siempre) utilizando mecanismos de generación dinámica que dificultan su acceso, y eso sin contar aquellas páginas cuyo

contenido, a pesar de estar indexado, requiere del uso de sistemas de autenticación para acceder a su contenido real, contenido que puede generarse de manera dinámica porque se obtiene del acceso a bases de datos que cambian con el tiempo. El acceso a parte de las webs de la Internet oculta solamente puede hacerse invirtiendo tiempo y esfuerzo, muchas direcciones se publican en foros o directorios y desaparecen a los pocos días e incluso horas, para dificultar aún más su acceso; otras sin embargo están ahí, esperando que alguien las encuentre.

Técnicamente, la Web superficial se compondría de páginas HTML (código estático) que no varían con el paso del tiempo, y que cuando lo hacen simplemente se actualizan en el servidor donde están alojadas; a esta web también se la conoce como **Web 1.0**, y para los robots de Google, Yahoo, Bing, etc., es relativamente fácil llegar hasta ellas. Con la llegada de los lenguajes de programación dinámicos para la web, léase PHP, ASP.NET, JSP y el resto de tecnologías similares, se dio un paso evolutivo en el desarrollo de las páginas web que propició que estas pudieran ser dinámicas, y que el usuario pudiera interactuar yendo más lejos del simple clic del hipervínculo. Fueron las capacidades para conectarse a bases de datos y poder generar el contenido que el usuario quería en el mismo momento en que estaba navegando lo que originó el *boom* de la enorme cantidad de páginas que estarían dentro de esta Internet oculta, aunque también hay quien la denomina como **Web 2.0**, la web que ha liberado al usuario para poder interactuar con las aplicaciones web como si de aplicaciones de escritorio se trataran y que incrementa la inteligencia de esta creando lo que se conoce como Web semántica, un hito al que poco a poco nos vamos acercando, tal vez la futura Web 3.0.

Esto obviamente ha supuesto lo que decía anteriormente, que el contenido dinámico generado no pueda ser directamente indexado por los buscadores. Os pongo un ejemplo que creo clarificará mucho, ¿puede Google acceder a las publicaciones que hacemos dentro de Facebook?, ¿os imagináis la cantidad de contenido que hay dentro de esta red social o de cualquier otra? ¿Aparece en los resultados del buscador? Pues ese contenido también formaría parte de la Internet oculta. Como consecuencia ahora tenemos una competición en donde aquellos que sí quieren aparecer en las páginas del buscador con sus webs tienen que ingeniárselas para poder estar entre los primeros resultados y existir, eso del SEO y del posicionamiento del que hablan muchos, es decir, salir de la Internet oculta, porque decididamente es donde todo Internet mayoritariamente está.

Con todo esto no sé si os estáis dando cuenta de la conclusión a la que quiero que lleguéis, Internet oculta, *a priori*, no significa necesariamente Internet mala o peligrosa, o al menos no mucho más de lo que puede llegar a serlo una página que sí esté indexada en Google, que haya sido capaz de posicionarse dentro de los primeros resultados y que tenga un troyano que instalemos de manera inocente en

nuestro ordenador. ¿Y qué tiene que ver todo esto con Bitcoin? Pues mucho o nada, según queramos verlo. Me explico, gran parte de los sitios que están en la Internet oculta (en la sección *Dark net* hablaré de ella en el capítulo 4) y que proporcionan servicios ilícitos como puede ser el caso del difunto Silk Road, cobraban utilizando Bitcoin como moneda de cambio, simplemente porque es más difícil de rastrear y se equipararía en estos casos al pago en efectivo. La publicidad que se ha hecho de Bitcoin asociándola exclusivamente a actividades ilícitas y a la Internet oculta, entendiendo lo que acabo de explicar, me parece que ha sido decididamente injusta y se ha tratado de criminalizarlo, como si con dólares o euros no fuera posible realizar este tipo de intercambios. O por poner otro ejemplo, ¿por qué no prohibir el correo electrónico cifrado? Vamos a criminalizarlo también, a fin de cuentas, quién nos garantiza que los criminales no cifren sus mensajes para evitar que la justicia caiga sobre ellos.

Vale Santiago, pero, ¿qué pasa con la red Tor, qué relación hay entre Internet oculta e Internet oscura (*Dark net*) y qué es eso de los niveles que he leído por algún lado? Para esa historia, tendréis que esperar un poco más, la contaremos luego y veréis que no solo de la red Tor vive el hombre y completaremos lo que acabo de contar aquí.

2.5.6 Código abierto. La licencia MIT de Bitcoin

La licencia MIT es una de los muchos tipos de licencia que se pueden aplicar al software y que sirven para delimitar el uso que puede hacerse de este por parte de terceros. Fue creada por el Instituto Tecnológico de Massachusetts para su sistema de interfaz gráfica **X Window System**, bajo el nombre **licencia X11**, por lo que licencia MIT y X11 son sinónimos y pueden usarse igualmente.

El que los desarrolladores de Bitcoin se decantaran por la licencia MIT es muy útil y sin duda una buena elección, porque permite que el código sea accesible para el mayor número de desarrolladores, y posibilita la creación de trabajos derivados y no importa que el código pueda ser usado en software propietario o libre, lo que es, en gran medida, un intento de popularizar el uso del software de Bitcoin lo más posible.

El mensaje básico de esta licencia es “Eres libre para usar este código como quieras”. Es compatible con la GNU GPL, y es corta, sencilla, y fácil de entender.

Otras criptomonedas como **Litecoin** o **Dogecoin** también se distribuyen bajo la licencia MIT.

2.5.7 Monedero o billetera

Imagina el monedero que llevas en el bolsillo y en el que guardas tus monedas y billetes. Pues esa misma idea es la que hay detrás de un monedero digital, es el equivalente a tu monedero físico pero dentro de la red de la criptomoneda que estés usando, por tanto, lo primero que se necesita para poder empezar con Bitcoin (o cualquier otra criptomoneda) es disponer de una aplicación instalada en tu máquina (en tu ordenador de casa o en el móvil), o accesible vía web, que funciona como si de un monedero físico se tratase y en donde vas a guardar tus criptomonedas. También existen monederos físicos sofisticados y con hardware especializado, y monederos tan simples como una hoja de papel con un código QR impreso.

Casi todos los monederos (por no decir todos) están securizados de manera que además de la clave secreta asociada a las direcciones que tenemos creadas dentro de él, tenemos otra contraseña adicional para acceder a nuestro monedero.

¿Y qué pasa si pierdo dónde tengo guardado mi monedero o no me acuerdo de las claves para su acceso? Esto es importante recordarlo, porque por regla general supone la pérdida del dinero. Al igual que si vamos por la calle y alguien nos quita la cartera, el perder la billetera o las claves de acceso a nuestras direcciones implicará perder el dinero que tengamos guardado.

El tema de la seguridad cuando operemos con criptomonedas no es algo que debamos descuidar nunca. Dado que en el capítulo 3 hablaremos de los diferentes tipos de billeteras que existen y de seguridad, nos basta con esto por el momento.

2.5.8 Transacción. Bloque. Cadena de bloques. Confirmación. Pruebas de trabajo

Aún más atentos porque los conceptos que voy a explicar ahora son la base de todas las criptomonedas, y aunque no voy a entrar en los detalles duros y técnicos, eso lo dejaremos para los capítulos siguientes, si entendéis esto el resto será pan comido.

Lo primero que tenemos que conocer es qué es una **transacción**. Muy fácil, una transacción es una **transferencia de valor entre dos monederos**, es decir, muevo la cantidad X de dinero del monedero A (origen) al monedero B (destino). Para poder realizar una transacción, esta debe estar firmada por una clave privada que garantiza dos cosas: la primera que el emisor de la misma es el propietario del dinero que desea transferir, y segundo que una vez que una transacción ha sido emitida nadie puede alterarla *a posteriori*. Las transacciones, una vez realizadas, se difunden por toda la red esperando a que un minero las confirme, algo que suele tardar una media de 10 minutos.

Veamos cómo se hace esto de las confirmaciones. A medida que los usuarios de la red Bitcoin van realizando transacciones, estas quedan en una lista de transacciones pendientes de incluir en un bloque. Y es aquí donde entra en funcionamiento el trabajo de los mineros. Un minero no es más que un ordenador o conjunto de ordenadores (lo que recibe el nombre de **pool**) que tiene una capacidad de cálculo muy, muy, muy grande. Estas capacidades de cálculo tan enormes (que se miden en *gigahashes* o *terahashes* por segundo) son necesarias para poder incluir las transacciones pendientes dentro de los bloques, que son la manera que Bitcoin utiliza para agrupar las transacciones. Cuando una transacción forma parte de un bloque se dice que está confirmada.

ENTONCES…

Hay un tipo especial de bloque, el **bloque génesis**, que recibe este nombre porque es el primer bloque de la cadena de bloques. Se le suele asignar el número 0, todos los demás bloques van a continuación de este

Pero meter una transacción dentro de un bloque **no es algo sencillo de hacer, si** lo fuera, cualquiera podría *a posteriori* realizar cambios en los bloques y alterar las transacciones que incluyen y revertir operaciones ya realizadas. Para evitar esto, el bloque debe llevar una prueba de trabajo matemático. Una prueba de trabajo matemático (o prueba de trabajo a secas, a veces aparece el término en inglés **Proof of Work** o PoW) no es más que una operación muy complicada de resolver, y que requiere realizar miles de millones de cálculos por segundo (quedaos con el nombre de **función hash** porque ahí está el meollo del asunto). Cómo de compleja sea la prueba de trabajo depende de la cantidad de mineros que haya en ese momento compitiendo por resolver el cálculo matemático propuesto, es decir, la complejidad de la prueba de trabajo se ajusta (a más difícil o a menos difícil) de manera automática, en función del poder de cómputo que los equipos mineros aportan a la red Bitcoin y con el objetivo de que el tiempo de resolución ronde los 10 minutos.

El primer minero que es capaz de resolver este problema computacional es el ganador y el que tiene derecho a incluir el bloque, con las transacciones que el minero haya incluido, dentro de la cadena de bloques compartida, que no es más que la concatenación en el tiempo de todos los bloques que los mineros van generando como consecuencia de la resolución del problema computacional. Como recompensa, el minero que ha sido capaz de generar el bloque recibe una compensación de 25 BTC y las tasas (el *fee*) que llevan asociadas todas las transacciones de su bloque. La recompensa recibe el nombre de **coinbase** (no confundirlo con la empresa Coinbase).

ENTONCES…

Inicialmente cuando la red comenzó a operar, la recompensa por bloque era de 50 BTC, sin embargo, el protocolo Bitcoin establece que dicha cantidad se debe reducir a la mitad cada cuatro años. Esta reducción a la mitad cada cuatro años recibe el nombre de **halving**. Realmente el *halving* se produce cada **210.000 bloques**, por lo que en función de la velocidad de la red, podría ocurrir un poco antes (o incluso un poco después).

El primer *halving* tuvo lugar el 28 de noviembre de 2012 y el próximo será el 26 de julio de 2016, cuando la recompensa por minar un bloque se reduzca a 12,5 BTC.

Recordar que como máximo habrá 21 millones de Bitcoines en el año 2140, el *halving* es necesario para mantener la inflación controlada.

Fijaos en un detalle que igual puede pasar inadvertido: a medida que los mineros van añadiendo bloques a la cadena de bloques, una transacción que ha sido confirmada en el bloque N, cuando se incluyan tres bloques más a la cadena de bloques, quedará "enterrada" por estos tres últimos bloques. Cuantos más bloques haya por encima de un bloque dado, más segura se considera esa transacción, o en terminología Bitcoin, más confirmaciones tiene. Comúnmente se acepta que una transacción con 6 confirmaciones, es decir, con 6 bloques detrás de ella, es imposible de revertir, y que el poder computacional que un supuesto atacante necesitaría para hacerlo y la inversión para disponer de tal sistema son tan elevados que no tendría sentido.

Fijaos en que el que haya que esperar 10 minutos para confirmar una transacción no significa que el dinero no esté en el monedero destino casi de inmediato, lo que sí sucede es que el monedero B no podrá gastar ese dinero hasta que no se comiencen a producir las confirmaciones. La confirmación, por tanto, hay que verla como un consenso que se produce en toda la red Bitcoin y que viene a decir que los Bitcoines que han llegado al monedero B están realmente ahí y no han sido enviados a nadie más. Vamos, que son tuyos ahora.

2.5.9 ¿Qué es un fork?

Dado que el código es libre y se puede utilizar libremente, no es rara la aparición de *forks* o proyectos paralelos, o **clones** del código fuente original, y que se basan en la tecnología de Bitcoin para funcionar. Los *forks* existen en cualquier tipo de desarrollo de software y no son patrimonio exclusivo del proyecto Bitcoin.

Estos proyectos, hemos visto que pueden representar a veces oportunidades de aprendizaje por lo que es interesante echarles un vistazo, aunque hay también quien advierte de que su creación puede estar animada por malas intenciones o malas ideas y que hay que tener mucho cuidado cuando uno se acerca a ellos; personalmente no tengo malas experiencias con ninguno para tener una opinión fundada de que esto pueda ser así. Lo que sí suele ser habitual es que un *fork* de Bitcoin acaba con la creación de una nueva criptomoneda.

Como ejemplo de esto último, quizás el *fork* más famoso de Bitcoin hasta la fecha sea **Litecoin**, criptomoneda de la que hablaremos más adelante y cuyos autores la consideran como un complemento a Bitcoin, algo así como la plata lo es al oro, aunque esto tiene sentido cuando existe un problema de divisibilidad, es decir, llega un momento en que el oro no se puede dividir más porque es físicamente imposible, por lo que se utilizan metales de menor valor para cubrir este propósito; pero Bitcoin no presenta este problema porque es infinitamente divisible.

ENTONCES…

Y nuevamente entraríamos en el debate que vimos en el epígrafe donde hablábamos de si tenían o no sentido las alternativas a Bitcoin.

Los *forks* suelen dividirse en tres tipos:

- **Operacionales** o **blockchain forks**: se deben a la operativa normal del funcionamiento de la red y se aplican a la cadena de bloques. En este caso, no se están haciendo cambios en el código de Bitcoin, son la consecuencia natural de la ejecución de una versión de Bitcoin determinada sobre los nodos de la red.

  Es decir, por la naturaleza descentralizada de Bitcoin, puede ocurrir (de hecho ocurre) que los nodos de la red tengan copias desactualizadas de la cadena de bloques y que estas no sean consistentes entre ellas, debido a que los bloques llegan a cada nodo en espacios temporales diferentes, lo que provoca que existan diferentes cadenas de bloques en el tiempo. Sin embargo, esta casuística está contemplada en el funcionamiento de Bitcoin y se resuelve en tiempo de ejecución haciendo converger las cadenas y tomando como válida una sola.

  De momento, de los *blockchain forks* nos vale con esto y en el capítulo 5 entraremos en más detalle de cómo se resuelven estas situaciones.

- **Accidentales**: como su nombre indica se deben a errores que aparecen en el código a consecuencia de una actualización errónea que los propios desarrolladores cometen (sí, son humanos y del planeta Tierra y cometen errores). Cuando pasa esto, pueden suceder varias cosas:
  - **No sucede nada**: el error se detecta antes de que ningún nodo se actualice al nuevo software, se corrige y se pone a disposición de todo el mundo la nueva versión, por lo que aquí paz y después gloria.
  - **Algunos nodos actualizan al nuevo software**: entonces se lía, porque habrá nodos de la red Bitcoin funcionando con una versión del cliente y otros con otra versión. En este caso, sucederá que la cadena de bloques, que los nodos van creando en el proceso de minería, se bifurcará y aparecen dos cadenas de bloques diferentes, una perteneciente al código original y otra perteneciente al código con errores.

¿Y esto es grave? Pues bastante grave, porque puede conllevar la pérdida de dinero. Ya hemos dicho que Bitcoin solamente tiene una cadena de bloques válida, y en el caso de producirse una bifurcación hay que elegir cuál es la correcta. Esto es algo que tarda un tiempo, los desarrolladores tienen que crear una corrección en el código y esta tiene que distribuirse entre los nodos para que surta efecto; si mientras tanto hay transacciones que acaban en una cadena que luego no será válida, esas monedas podrían perderse.

Al menos que yo sepa, la situación de *forks* accidentales se ha vivido dos veces durante la vida de Bitcoin. Una en marzo de 2013 y otra mucho más recientemente, en julio de 2015.

Durante marzo de 2013 sucedió con los cambios de base de datos de las versiones 0.7 y 0.8. Fue **Pieter Wuille**, también desarrollador de Bitcoin, el que dio la voz de alarma, y pidió a los mineros que no migraran a la versión 0.8 y que se mantuvieran con la versión 0.7. Sin entrar en los detalles técnicos, sucedía que en la base de datos (**Berkley DB** de Oracle) usada en la versión 0.7 había un límite interno que rechazaba como válido un bloque que estuviera muy lleno de transacciones, cosa que no pasaba en la versión 0.8 (**LevelDB** de Google). Un minero con esta última versión creó una transacción muy grande y por tanto válida para la versión 0.8 pero no para la 0.7. Como se dio el caso de que había más mineros con la versión 0.8 que con la versión 0.7, el bloque grande fue aceptado y la cadena de bloques se bifurcó, con el consecuente problema de que para los mineros con versión 0.7, este bloque no era válido, así que estos continuaron generando su propia cadena de bloques, diferente a la que generaban los de la versión 0.8.

El problema, que podría haber sido muy serio, se resolvió muy rápidamente. En un primer momento se pidió a los mineros que no migraran a la versión 0.8, y que los que lo habían hecho, volvieran a la versión 0.7. De este modo, el bloque grande fue ignorado por la red, las cadenas de bloques volvieron a converger en una sola y el error quedó resuelto al cabo de unos días, con la versión 0.8.1 de Bitcoin. La red siguió funcionando sin problemas y nadie perdió sus monedas.

En julio de 2015, entre los días 3 y 4, también se produjo como consecuencia de una actualización planificada, con la **implementación de la recomendación BIP66** en los clientes a partir de la versión 0.9.4. Esta recomendación, que obliga a una validación completa del bloque, no fue realizada por algunos *pools* de minería que aceptaron bloques de la versión 2, en vez de rechazarlos y pasar a utilizar bloques en su versión 3. Como consecuencia supuso que otra vez la cadena se bifurcase, y durante al menos 6 bloques existieron dos cadenas de bloques alternativas. No hubo doble gasto en ningún momento pero sí supuso pérdidas económicas para los *pools* de minería que llegaron a estimarlas en más de 50.000 dólares. Durante el tiempo que estuvo la alarma activa, se recomendaba esperar 30 confirmaciones para estar completamente seguros de que el dinero en nuestra cartera estaba realmente ahí y actualizar a la versión 0.10.2 de Bitcoin Core, que corregía completamente el problema.

- **Bifurcaciones duras (hard forks)**: son cambios que se introducen en Bitcoin que presentan incompatibilidades con las versiones de código anteriores y que acaban, invariablemente, con el abandono de la cadena antigua, y la variación a una nueva cadena de bloques, que tiene que ser aceptada por consenso.

El caso de un *fork* duro lo estamos viviendo ahora mismo, con el debate entre Bitcoin Core y Bitcoin XT que contamos un poco más abajo.

2.5.10 Unidades de medida

Uno de los aspectos a mi juicio más importantes para el recién llegado al mundo de las criptomonedas, que hay que dominar, es conocer las **unidades de medida** que se utilizan habitualmente en las operaciones que realizamos. Más que nada porque, si en nuestro día a día estamos acostumbrados a hablar de euros y nos es familiar hablar de monedas de 20, 10, 5… céntimos y vemos el céntimo como la unidad menor que constituye al euro y no tenemos problemas para componer euros a base de céntimos, algo parecido sucede con Bitcoin, pero ahora el rango de posibles subunidades que tenemos se amplía notablemente, y al menos al principio puede resultar un poco confuso.

1 Bitcoin (1 BTC), por diseño, Satoshi Nakamoto decidió que pudiera dividirse hasta el octavo decimal (al ser software nada impediría cambiar la codificación para que pudiera dividirse incluso más, pero en esto y en las implicaciones de llegar a hacerlo no voy a detenerme). ¿Cuál es, por tanto, la fracción de Bitcoin más pequeña que vamos a encontrarnos? Teniendo en cuenta esto que acabo de decir, estaríamos hablando de **un 1 con 8 ceros por delante**, o la cienmillonésima parte de 1 Bitcoin:

0,00000001, a esto se le llama **satoshi**, en honor a Satoshi Nakamoto

Por tanto, 1 BTC equivale a 100.000.000 (cien millones de satoshis). Dado que un satoshi suele ser una cantidad demasiado pequeña, agrupar valores utilizándolos suele ser poco habitual, y lo que se hace es utilizar una unidad un poco más grande, el bit (y no confundir con la idea de bits de toda la vida).

1 bit equivale a 100 satoshis, luego, si tengo por ejemplo 200 bits, lo que realmente tengo es:

200 bits = 200 x 100 satoshis = 20.000 satoshis

Y si tengo 1 BTC:

1 BTC = 1.000.000 bits = 1.000.000 x 100 satoshis = 100.000.000 satoshis

Para rizar un poco más el rizo, además de los satoshis y los bits, es usual hablar de **miliBitcoin** y de **microBitcoin**, pero siguen el mismo razonamiento que acabamos de exponer. Se entiende mucho mejor con la siguiente tabla a modo de resumen:

1 μBTC (microBitcoin) = 100 satoshis = 1 bit

1 mBTC (miliBitcoin) = 100.000 satoshis = 1.000 bits

Entonces:

1 BTC = 1.000 mBTC (miliBitcoin)

1 BTC = 1.000.000 μBTC (microBitcoin)

1 BTC = 100.000.000 satoshis

O lo que es lo mismo:

1 mBTC = 0,001 BTC

1 μBTC = 0,000001 BTC

Actualmente lo más común es que las cifras se muestren en milibitcoines, pero conviene tener soltura en las conversiones anteriores para darnos realmente cuenta de la cantidad de dinero de la que estamos hablando.

2.6 LAS MONEDAS ALTERNATIVAS A BITCOIN (ALTCOINS) MÁS IMPORTANTES

Bueno, pues no está nada mal, y eso que solamente hemos arañado una pequeña parte de este universo. Como confío en que seguirás leyendo el resto del libro, más adelante, si hay alguna cuestión sobre lo anterior que te suscite dudas, seguro que se resolverán. De momento vamos a terminar este capítulo parando en algunas de las criptomonedas más conocidas, mención especial al epígrafe sobre **Bitcoin XT**, porque si bien no estamos hablando de una moneda diferente a Bitcoin, sí que estaríamos ante una de esas decisiones de mejora de las que anteriormente comentaba, de las que todo código alguna vez en su ciclo de vida tiene que asumir.

2.6.1 Litecoin

De símbolo LTC, es considerada por la gran mayoría como la hermana pequeña de Bitcoin. Algo así como la plata es al oro, sin embargo, ya expliqué que esto tiene sentido con los metales preciosos, debido a que estos, llega un momento en que no se pueden dividir más, porque físicamente es imposible, y por mucho que yo quiera hacer más y más pequeña una porción de oro, no podré, así que tiene sentido un metal alternativo de menor valor que actúe como subunidad. Pero en el mundo de los bits de información viajando por las redes de comunicación, la necesidad de una hermana pequeña que complemente el valor de Bitcoin no tiene mucha razón de ser.

Litecoin se presentó en sociedad el 7 de octubre de 2011 por **Charles Lee** (exempleado de Google) y ha ido evolucionando a medida que Bitcoin lo ha ido haciendo, en general adoptando las mejoras que Bitcoin introduce primero, técnicamente Litecoin es igual a Bitcoin. Al igual que Bitcoin, el código de Litecoin es abierto y sigue el mismo tipo de licencia MIT que este. Su icono es el siguiente:

Figura 2.23. Símbolo de Litecoin

Litecoin presenta tres diferencias respecto a Bitcoin:

- El procesamiento de un bloque se realiza más rápidamente, en vez de los 10 minutos de Bitcoin, Litecoin tarda 2,5 minutos, lo que hace que se acelere la confirmación de las transacciones.

- El límite de Litecoines que existirá es cuatro veces superior al de Bitcoines, y se sitúa en los 84 millones de unidades, aunque al igual que este se fracciona hasta el octavo decimal, existiendo 100.000.000 de unidades más pequeñas por unidad de Litecoin.

- El algoritmo para hacer la prueba de trabajo usa **scrypt** de **Colin Percival**, lo que crea un proceso de minería más democrático, no es necesario un equipo con características especiales para minar la moneda (al menos de momento).

Actualmente la capitalización de Litecoin se sitúa cerca de los 200 millones de dólares, con un precio algo superior a los 3 dólares en este momento (finales de 2015), lo que la convierte en la segunda moneda más grande. Lo habitual es obtenerla en alguno de los *exchanges* especializados como Bitfinex, BTC-e, OKCoin, BitBay, Kraken, Yucana, Huobi, BTC China, OKCoin...

2.6.2 Peercoin

También conocida como PPCoin o Peer-To-Peer Coin, o abreviada como PPC, sus autores son **Scott Nadal** y **Sunny King**, que la lanzaron en 2012. Nadal dejó el proyecto en noviembre de 2013 y ahora el líder del proyecto es King. Con una capitalización de mercado de casi 9 millones de dólares, y un precio de **0,38 dólares la unidad** (finales de 2015), Peercoin se situaría en la cuarta posición en importancia en el mundo de las criptomonedas, detrás de Bitcoin, Litecoin y Namecoin. Su icono es el siguiente:

Figura 2.24. Icono de Peercoin

La principal diferencia de Peercoin respecto a sus competidoras está en que se diseñó pensando en ser más segura y con menor gasto energético que sus competidoras, de hecho, el coste energético cara a minar una moneda como Bitcoin (o similares, Litecoin y compañía tampoco se libran de este problema), se compara al gasto de una ciudad de tamaño mediano, gasto que tendrá que subir a medida que la moneda se popularice. Aunar seguridad y eficiencia energética se consigue utilizando una cosa que se llama **Proof Of Stake** (PoS) o **prueba de participación**, que se combina con la prueba de trabajo (PoW).

ENTONCES…

El gasto por kilovatio/hora es uno de los aspectos que se tienen en cuenta cuando se trata de calcular el retorno en la inversión de equipos de minería. Cada vez que un nuevo hardware sale a la venta, este es uno de los parámetros que más preocupan a las personas que lo adquieren para ver si sale a cuenta minar o no.

Aunque explicaré más adelante las diferencias entre los diferentes tipos de prueba, para que tengáis una idea básica de PoS y PoW, es que en la primera se necesitaría tener al menos el 51% de las monedas para poder falsificar una transacción (doble gasto), mientras que en PoW se necesitaría al menos el 51% de la potencia de cálculo. Ambas cosas no son fáciles de conseguir en ningún caso.

No obstante Peercoin hace uso también de prueba de trabajo, al menos durante los estadios iniciales de la generación de la moneda, aunque lo ideal es que el uso de esta tienda a cero. Cada bloque se separa en función del tipo de prueba que utiliza. A diferencia de otras criptomonedas, en Peercoin no hay máximo establecido que haya que generar.

En la prueba de participación juega un papel fundamental el concepto de acuñación, o período de tiempo o edad que una moneda está en posesión de un usuario. El ejemplo clásico con Bob y Alicia, en donde Bob tiene 10 monedas que Alicia le ha enviado, y que guarda durante un período de 90 días, equivaldría a unos 900 días de edad moneda (10 x 90), que se consume cuando Bob las gasta. Este tiempo, que por buscarle un símil financiero equivaldría al tiempo en el que la hemos ahorrado, sirve para generar más moneda, algo así como un interés que recibes por tu dinero a plazo fijo, y que se fija en el 1% anual (al menos debes tenerlas 30 días en tu cartera para que generen algún beneficio).

2.6.3 Namecoin

Namecoin (o por sus siglas MMC) es una criptomoneda interesante por varias razones. La primera es que fue el primer fork del código de Bitcoin y comparte con esta algunas de sus características como estar limitada a 21 millones de unidades y utilizar el mismo tipo de prueba de trabajo. Su icono es el siguiente:

Figura 2.25. Símbolo de Namecoin

El origen de Namecoin se encuentra en una discusión iniciada en el foro BitcoinTalk sobre la posibilidad de extender Bitcoin para usarlo como servicio de nombres de dominio (*name domain service*). El proyecto, que recibió el nombre de **Bitdns**, extendía Bitcoin para el registro, actualización y transferencias de dominios pero enseguida se demostró que Bitcoin no era el mecanismo ideal para soportarlo porque podría presentar problemas de escalabilidad a futuro y se decidió que se creara una cadena de bloques diferente.

La motivación para crear algo como Namecoin es muy interesante y muy en la línea del movimiento ciberpunk, si entendemos lo que realmente significa el servicio de nombres de dominio. Voy a explicarlo sin entrar en complejidades técnicas. Pensad en que cada vez que introducimos en nuestro navegador una dirección web comprensible para los humanos, internamente lo que está sucediendo es que dicho nombre es resuelto y convertido, por una serie de servidores, en una dirección IP (si no hubiera servicio de nombres tendría que conocer la IP para poder conectarme al servidor), y el contenido que hay en esa IP es lo que se nos muestra en el navegador.

Ahora bien, la organización que se encarga de supervisar este sistema se llama **ICANN** (Internet Corporation for Assigned Names and Numbers), que aunque funciona como una organización sin ánimo de lucro, pertenece al **Departamento de Comercio de los Estados Unidos**, o dicho de otro modo, la gestión de los dominios de todo el planeta está en manos de un único jugador, algo que no gusta, ni mucho menos, al resto de países y que ha generado más de un debate sobre quién debería supervisar dicho sistema; ¿la ONU quizás?, ¿un gabinete de expertos mundiales? No son raras las confiscaciones de dominios o la aplicación de políticas arbitrarias que no quedan del todo claras, eso sin contar las leyes americanas **SOPA (Ley para frenar la piratería online)** y **PIPA (Ley para la protección de la propiedad intelectual)** (los nombres son un poco de cachondeo para el hispanohablante) que podrían obligar a cualquier servidor DNS a bloquear las páginas con contenido pirata o sospechoso.

La solución a este problema estaría en Namecoin. En vez de crear un organismo gestor y que puede funcionar siguiendo reglas poco claras o en manos de unos pocos, dejemos que sea la Red el organismo que gestione el servicio de nombres de dominio. Con Namecoin es posible registrar cualquier dominio con extensión **.bit**, para ello solamente necesitas unos cuantos Namecoines, que se cotizan en aproximadamente **0,00112862 BTC** en el momento de escribir estas líneas (finales de 2015), lo que la sitúa en el tercer lugar de las criptomonedas.

Una de las características que hacen a Namecoin diferente de Bitcoin es que en la cadena de bloques de Namecoin pueden almacenarse datos del tipo clave/valor y se añaden transacciones específicas para poder manipularlas (crearlas, actualizarlas y consultarlas). Estos datos están distribuidos por toda la Red y pueden consultarse en cualquier momento. Entre las últimas modificaciones que ha implementado están la de utilizar el minado combinado (*merge-mining*) con Bitcoin, lo que permite aprovechar el resultado de la prueba de trabajo de esta y utilizarla para ver si es también válida para Namecoin.

2.6.4 Dogecoin

Dogecoin es uno de esos ejemplos de lo que se puede conseguir con una campaña de *marketing* bien orquestada, desde mi punto de vista es la única explicación para el relativamente alto éxito de esta criptomoneda, que va más lejos de lo considerado normal como podréis comprobar si seguís leyendo.

Dogecoin o DOGE es un *fork* de Litecoin, creada por un antiguo ingeniero de IBM, **Billy Markus**, al que luego se unió **Jackson Palmer**, que trabajaba en el departamento de *marketing* de Adobe, en Australia. Más o menos la historia fue que Jackson tuiteó (a modo de broma) que quería invertir en "Dogecoin" (la idea del nombre de la moneda es suya) y recibió como respuesta la de Billy, que le contó que él estaba haciendo experimentos con la suya. A partir de ahí se une el nombre de Jackson al código de Billy y nace Dogecoin formalmente. La imagen de la moneda está asociada a la de un simpático perrito de la raza japonesa **Shiba Inu**.

Figura 2.26. El logo de Dogecoin

ENTONCES…

Esto de usar la imagen de un perro como símbolo también tiene su historia detrás y tiene que ver con un perro de nombre **Kabosu** (de la raza Shiba Inu) y su orgullosa propietaria, una maestra japonesa de nombre **Atsuko Sato**.

Resulta que Kabosu iba a ser sacrificado al cerrar la granja de cachorros donde vivía, pero tuvo la suerte de ser adoptado por Atsuko, quien en su afán por denunciar la situación que sufrían muchos animales en estas granjas, inició un blog (kabosu112.exblog.jp/9944144, por si queréis echarle un vistazo y no se os da mal esto del japonés…) que se convirtió en todo un éxito.

En este blog Atsuko **subía las fotos de su peludo amigo Kabosu**, que acabó por convertirse en toda una estrella de Internet. Y a partir de aquí el destino, el azar o la simple suerte hicieron que alguien llegara hasta este blog y utilizara las fotos de Kabosu para hacer un fotomontaje con ellas y un texto denunciando algún hecho o difundiendo algún mensaje, animando además a que todo el mundo hiciera lo mismo. ¡Y vaya si se hizo! Por cierto, si asociados a la imagen del perrito los textos tienen faltas de ortografía, es adrede.

Estos fotomontajes los hay a cientos en Internet con la cara de Kabosu, recibieron el nombre de "doge meme". Al usarse también como logo para la nueva moneda se decidió que el nombre fuera, efectivamente, Dogecoin.

¿Cómo se te ha quedado el cuerpo?

Como os decía, Billy estaba experimentando con criptomonedas, en concreto comenzó sus andanzas haciendo pruebas con una moneda llamada "Bells" basada en el popular juego de Nintendo, *Animal Crossing*, por dos motivos principalmente: partir de una base de usuarios amplia y familiarizados con algo ya existente y para tratar de distanciarse de las turbias relaciones que se habían establecido en la prensa entre Bitcoin, Silk Road y demás gente de mala vida.

Cuando Jackson se une a Billy y comienzan a trabajar, el usar la imagen del simpático perrito le daba a Dogecoin un aire menos serio y formal, simpático si se quiere, que Bitcoin o Litecoin, una especie de broma o parodia de ambas que no aspiraba a competir con ellas y mucho menos a tener el éxito que ha tenido. En palabras de Palmer:

"La comunidad de Dogecoin no se toma en serio a sí misma, no está siendo usada por personas que se preocupan de si van a volverse ricos. Es algo para compartir, para dar las gracias o felicitar a alguien".

ENTONCES…

Lo de ir en broma es muy serio.
Dogecoin es la única moneda que ha creado una **religión parodia propia con seguidores por todo el mundo**. Además es la moneda oficial del **Reino de Enclava** o **Liberland**. ¿Que no sabes dónde está eso? No me extraña, es ni más ni menos que una pequeñísima extensión de terreno, en tierra de nadie y digo de nadie porque nadie ha reclamado jamás esta pequeña extensión de suelo situada **entre Croacia y Serbia**. Autodenominado como el país más pequeño de Europa, fue el lugar ideal para que el político checo **Vít Jedlička** fundara la micronación, con la idea de crear un lugar en la Tierra donde el Estado pudiera estar reducido a su mínima expresión y creando el país más libre e igualitario del planeta. ¡Ah!, que sepas que es posible solicitar la nacionalidad. Citar también que la venta más curiosa de Dogecoin está en la casa de verano de **Matt Thompson**, un empresario americano de 27 años que la puso en venta por 100 millones de Dogecoines

En resumen, en diciembre de 2013 Dogecoin vio la luz. Como características principales están que la cantidad de monedas disponibles es de **100.000.000.000** (cien mil millones de unidades), y al igual que Litecoin, se basa en el algoritmo scrypt de minado, aunque sus transacciones se confirman en apenas un minuto, estando por debajo del tiempo de Litecoin y de Bitcoin.

A principios de 2014, Dogecoin superó en volumen de transacciones realizadas a Bitcoin (pero ojo, no en valor). Actualmente cotiza en **0,000131 dólares** (finales de 2015). Es muy popular en las redes sociales, fundamentalmente en Reddit, como un mecanismo para dar propinas entre los usuarios.

2.6.5 Freicoin o el concepto oxidable

El concepto de dinero oxidable fue creado por **Silvio Gesell** (1862-1930), comerciante alemán (aunque nació en la Bélgica que pertenecía a la Alemania de la época) que emigró a Buenos Aires (el dominio del español lo adquiere durante el tiempo que trabaja en la ciudad española de Málaga) para fundar una empresa de importación, Casa Gesell, que se dedica al material quirúrgico y de farmacia, y más tarde a los productos para el cuidado de los bebés.

En 1916 publica el libro *El Orden Económico Natural*, que se considera su obra más importante, aunque su primer tratado teórico acerca de las finanzas es de 1891 y se titula *La reforma del sistema monetario como puente hacia un estado de bienestar*, en el que analiza el sistema monetario en busca de soluciones a la crisis del Gobierno de Juárez Celman.

Según Gesell, el planeta debía pertenecer a toda la gente que lo habitaba sin importar su raza, género, clase o religión, y considera que la satisfacción del interés particular motiva a ser productivo. Por ese motivo el sistema económico debería estar al servicio de las personas, y no al revés, considerando que el dinero había perdido su utilidad como herramienta de intercambio, y se había convertido en una mercancía en sí misma, usada únicamente para especular, y que solamente servía para generar desigualdades sociales por efecto de la usura y afectando de modo negativo a la economía real. Por estos motivos propone como solución la economía natural, en ella las oportunidades de negocio deben estar disponibles en igualdad para todos, aboliendo cualquier privilegio adquirido anteriormente, y dejando que cada persona confíe en sus habilidades y capacidades individuales a la hora de conseguir sus objetivos, de manera que las personas con más talento son las que deberían obtener los ingresos más altos.

La solución que propuso era crear un sistema en el que las monedas se depreciaran con el tiempo, para evitar que la gente las acumulara, y funcionasen como funciona cualquier otro bien, es decir, cualquier cosa que yo tenga, desde un plátano a una lavadora, pierde valor a medida que el tiempo pasa, porque se deteriora, se desgasta, o en el caso de un bien orgánico como el plátano, sencillamente se pudre.

Aunque Gesell nunca llegó a ponerlo en práctica, más adelante el **experimento de Wörl** demostraría que sus ideas no eran del todo descabelladas.

¿Qué ventajas aportaría el uso del dinero oxidable respecto al dinero tradicional? Aquí tenemos las más típicas:

- **Regularización de la demanda**: el dinero dejaría de ser el medio de ahorro, obligando a cada portador a gastarlo cuanto antes para evitar la oxidación. Como consecuencia habría demandas regulares, no manipuladas arbitrariamente por los poseedores del dinero, lo que estabilizaría la economía.

- **Superación de las crisis económicas**: la circulación sin cesar del dinero posibilitaría la construcción de una sociedad sin crisis económicas.

- **Desaparición del interés del capital**: los prestamistas comenzarían a ofrecer préstamos sin cobrar tasas de interés, porque se verían obligados a evitar oxidación de todas formas.

- **Estabilización de precios**: la Administración Monetaria de cada gobierno frenaría deflaciones por gastar más e inflaciones por gastar menos, controlando así la masa monetaria.

- **Separación entre el medio de intercambio y el de ahorro**: la gente preferiría tener bienes o prestar dinero sin tasas de interés a dinero oxidable para ahorrar su fortuna.

- **Desaparición de capitalistas**: sería imposible ganarse la vida prestando dinero a alguien y cobrar tasas de interés.

Y es a partir de todas estas ideas de donde surge la criptomoneda **Freicoin** en 2012 de la mano de **Jorge Timón** y **Mark Friedenbach**, quienes pusieron en marcha un proyecto de *crowdfunding* en la plataforma **Indiegoo**, que aunque no logró el capital necesario (recaudaron algo más de 1.000$ de los 28.000$ que tenían de meta), sí suscitó suficiente interés en la comunidad de las criptomonedas. El símbolo de Freicoin es el siguiente:

Figura 2.27. Símbolo de Freicoin

El nombre viene de la mezcla de las palabras *Bitcoin* y *Freigeld* (palabra alemana que significa "dinero gratis"). Con una masa monetaria máxima de 100 millones de unidades, el 80% de ellos los repartiría la **Fundación Freicoin** en forma de ayudas y becas a diferentes proyectos (caridad, desarrollo sostenible, conocimiento libre, etc.) por un período no superior a los tres años. Esto significa que a diferencia de Bitcoin, gran parte del dinero que se genera en la red Freicoin no va a parar en manos de los mineros, algo que suscitó más de una crítica.

En Freicoin se implementa una cuota de oxidación (*demurrage*) para reducir el acaparar capital y llevar las ideas que expliqué anteriormente a la práctica, por tanto se aplica un interés negativo sobre el dinero que permanece inmovilizado. Como sucedería con el caso de Peercoin, se considera que el consumo eléctrico es un gasto innecesario y generar dinero no debería llevar parejo un coste de producción.

Al compartir el mismo algoritmo de prueba de trabajo con Bitcoin, puede hacer como las últimas versiones de Namecoin y aprovechar el *merged mining* o minado combinado para mejorar el rendimiento. Actualmente (finales de 2015) el precio de Freicoin se sitúa alrededor de los **0,0006$**.

2.6.6 ¡Los españoles al ataque! Pesetacoin

Esto de crear criptomonedas no es solamente patrimonio de anglosajones o personajes misteriosos, sino que los españoles (bueno, Jorge Timón de Freicoin lo es) también nos hemos subido al carro con la creación de una moneda de decidido carácter español: **la Pesetacoin** (de símbolo PTC), un homenaje a nuestra querida rubia del que dejamos constancia en estas páginas, más por el valor sentimental que presenta que por el impacto que ha tenido que no ha sido mucho, salvo en algunos *pools* de minería chinos. El icono que la representa es el siguiente:

Figura 2.28. Símbolo de la Pesetacoin

Nacida en enero de 2014 de la mano del leonés **Mario Prieto** y **Ramón Martínez**, idearon para Pesetacoin un máximo de **166.386 millones de unidades**, un guiño simpático al valor al que equivalía un euro en pesetas cuando entró en circulación, por aquel entonces 1 euro se cambiaba por 166,386 pesetas, casi 200 "pelas" de las de antaño.

Figura 2.29. Web de pesetacoin.org

El proceso de minería utilizado está basado en el algoritmo **scrypt** y reduce la cantidad de PTC emitidas de año en año. La recompensa por minar un bloque es de 166.386 PTC y al menos durante algún tiempo, desde China se tuvo cierto interés en la moneda. Como única ventaja que aportaba sobre Bitcoin estaría su menor tiempo de confirmación de transacciones (unas diez veces más rápido), sin embargo, más allá de esto o de los motivos meramente sentimentales no hay ninguna razón de peso para argumentar que es una criptomoneda mejor que Bitcoin.

Figura 2.30. El cliente de Pesetacoin en acción con su cotización

Para poder conseguir Pesetacoines podemos utilizar alguno de los grifos (luego explico qué es un grifo) que hay disponibles en Internet, el más popular sin duda es la aplicación Android que hay en Google Play llamada Pesetacoin Faucet, que permite enviarte 5 PTC diarias a la dirección que indiques.

Figura 2.31. La app para acceso al faucet de Pesetacoin

Otra opción era comprarlas directamente desde la web china **coomercia.com**, desde el *exchange* **bittrex.com** o directamente desde **comprarpesetacoin.es**. Sin embargo, la desaparición de esta web (comprarpesetacoin.es), de queespesetacoin.info y de la asociacionpesetacoin.org, junto con el gráfico de cotización en el cliente acercándose asintóticamente a cero, nos hacen pensar que la salud de esta criptomoneda patria no es muy buena y acabará pasando a la historia como un intento fallido más de arrebatarle un poco de gloria a Bitcoin.

Lo decía al principio, no es nada fácil que una criptomoneda llegue a triunfar, ni siquiera aquellas que por su carácter mediático aparecen publicadas en los medios, como fue el caso de esta que nos ocupa.

2.6.7 ¿Y qué pasa con Bitcoin XT?

Si habéis estado siguiendo las noticias aparecidas sobre Bitcoin, es probable que últimamente os haya llamado la atención la aparición del nombre de **Bitcoin XT**; la polémica generada ha sido realmente importante y presenta uno de los retos más serios a los que Bitcoin se ha tenido que enfrentar en su relativamente corta existencia. Es más, desde que se anunció su puesta en marcha, el precio de la criptomoneda ha variado sustancialmente debido a la incertidumbre del qué pasará y ha creado un clima de división en la comunidad Bitcoin, más que nada porque muchos se han llegado a preguntar si es un sustituto y qué ocurrirá con su dinero.

Y es que aunque Bitcoin ha tenido ataques de todo tipo y desde las fuentes más dispares, pasando de los puramente técnicos a los meramente mediáticos, quizás es desde el propio núcleo de la comunidad Bitcoin donde surge el mayor reto a resolver o la prueba de estrés más importante. Y la cuestión no carece de importancia, la supervivencia de Bitcoin a futuro puede depender de cómo se resuelva, porque estamos hablando de cómo hacer que Bitcoin sea escalable y pueda soportar un ritmo de crecimiento que se prevé llegue a ser exponencial.

Tal vez podáis pensar que exagero, pero nada más lejos de la realidad, al ritmo actual al que evolucionan las cosas, la red Bitcoin, tal y como está actualmente, se quedará sin capacidad para poder procesar las transacciones en aproximadamente entre 12-18 meses, sí, estáis leyendo bien, 12-18 meses, y esto significa que los tiempos en procesar las transacciones serán insufriblemente lentos o en el peor de los casos, no llegar a confirmarse nunca.

¿Y todo esto por qué sucede? ¿Cuáles son los motivos? Con lo que ya hemos visto podrás entenderlo a la perfección. Antes hemos definido que la cadena de bloques recibe tal nombre porque está compuesta por el anexado continuo de bloques (por parte de los mineros). Los bloques a su vez están formados por las transacciones que se ejecutan a lo largo y ancho de la red, y por el diseño original de Satoshi Nakamoto, tienen un tamaño determinado de 1 MB, procesando aproximadamente de 3 a 7 (en el mejor de los casos) transacciones por segundo por término medio (no confundir este dato con el número de transacciones que hay dentro de un bloque).

ENTONCES…

Igual no se ve la importancia de esto a simple vista, pero pensad que VISA puede procesar en sus centros de datos más grandes hasta **47.000 transacciones por segundo** o lo que es lo mismo, 150 millones de transacciones diarias. Si a futuro queremos que Bitcoin sea una alternativa real y global, siete transacciones por segundo es un valor que no se puede mantener.

A medida que las transacciones van llegando a los nodos para ser incluidas en los bloques, los mineros van llenando los bloques con ellas. Ahora mismo, los bloques que se minan no están completamente llenos de transacciones, aproximadamente están a un 40% de su capacidad, sin embargo, a medida que crece el volumen de transacciones en la red, este espacio que hay libre en el bloque se llenará, y habrá transacciones que tendrán que esperar a ser incluidas en el bloque siguiente.

ENTONCES…

De hecho durante la última subida de precio de Bitcoin del mes de noviembre de 2015 hasta los 500$, el aumento del llenado del bloque llegó casi al 80% de su capacidad máxima.

Fijaos en la siguiente figura que muestra el número de transacciones por bloque en el rango que va desde que se puso en marcha la red hasta el día de hoy. La figura comienza a parecerse a una exponencial si lo vemos usando la escala lineal:

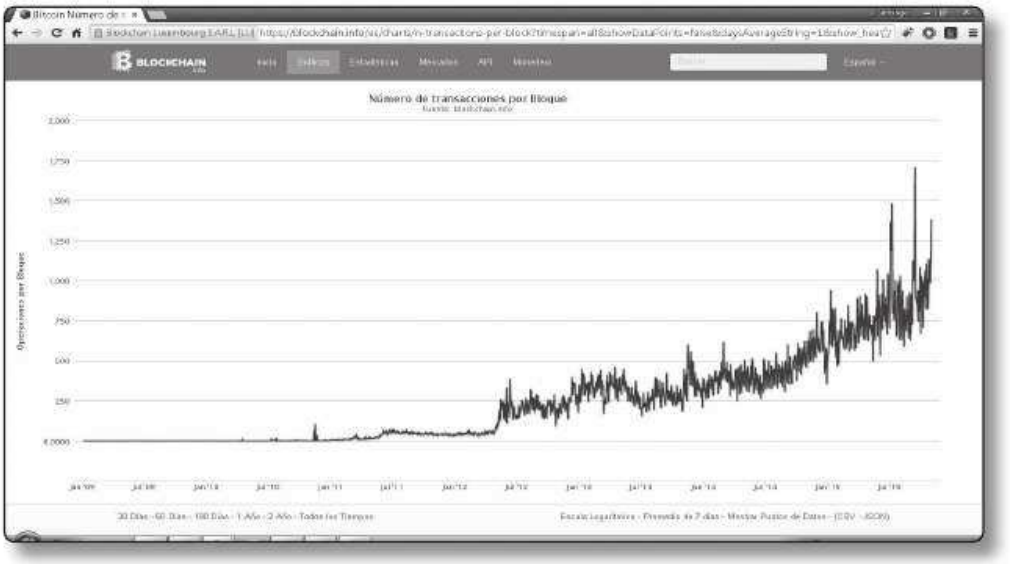


Figura 2.32. Número de transacciones por bloque

Aunque en visión logarítmica (que muestra mucho mejor los cambios bruscos), vemos que la tendencia sería menos pronunciada y las transacciones van aumentando de un modo menos agresivo (fijaos en el salto tan fuerte que se produjo en 2012):

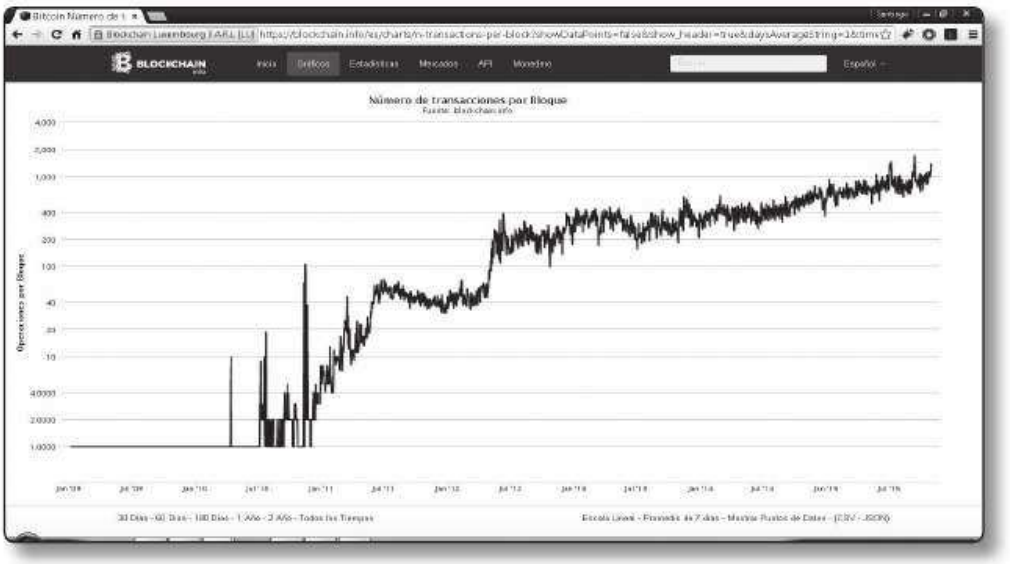


Figura 2.33. Número de transacciones por bloque (logarítmica)

El motivo por el cual Satoshi decidió este tamaño se debió a evitar un posible ataque por denegación de servicio, aunque es cierto que fue un valor arbitrario (podría haber elegido 2 MB o 512 KB) y provisional apuntando a que debería ser

aumentado con toda probabilidad en el futuro. Si no existiera un máximo de tamaño de bloque, alguien con suficiente poder de cálculo podría minar un bloque con un tamaño desmesurado y obligar a que todos los participantes lo aceptaran o por el contrario se tendrían que salir de la red. Digamos que este tamaño de bloque era como una especie de *antispam* para asegurar una red que estaba en sus primeros momentos de desarrollo y para la que cualquier golpe de calado podría haber sido fatal.

Y es aquí y debido a este tamaño donde aparece el problema y la necesidad de hacer evolucionar el protocolo Bitcoin a Bitcoin XT. Bitcoin XT es un protocolo alternativo propuesto por **Gavin Andresen** y **Mike Hearn** y que pretende cambiar el tamaño de 1 MB original a 8 MB, lo que repercutiría en una reducción significativa del tiempo medio que se tarda en confirmar una transacción, y que oscila en torno a los diez minutos. Una mejora en este tiempo haría que Bitcoin pudiera competir contra otros sistemas de pago actuales y facilitaría su adopción masiva o al menos, le sería más fácil plantar cara a los sistemas tradicionales de pago.

ENTONCES…

Mike Hearn es uno de los **cinco desarrolladores** principales de Bitcoin Core y uno de los más férreos defensores de Bitcoin XT.

Que sea Gavin Andresen, líder hasta hace poco del proyecto y actual jefe científico de Bitcoin el que haya sugerido el cambio, como podéis imaginar, ha causado un auténtico revuelo, porque este aparentemente inofensivo cambio implica muchas cosas; ¿os acordáis de cuando hablaba de crear un clon de Bitcoin y que a veces cambiar una regla del protocolo podría suponer meternos en un auténtico jardín? Pues estamos ante un ejemplo claro de esta situación.

La primera versión completamente funcional de Bitcoin XT se lanzó el pasado 15 de agosto de 2015 y la intención es que a partir de enero de 2016 se convierta en la versión oficial de Bitcoin, reemplazando a Bitcoin Core, pero solamente si se consigue el consenso adecuado. ¿De cuánto consenso estamos hablando? Pues ni más ni menos que del 75% de la red de nodos que soportan Bitcoin actualmente, y aunque creáis que es un valor muy alto, muchos de los detractores de Bitcoin XT sostienen que es un consenso muy pequeño y que este debería ser superior al 90%. De no llegarse a un consenso e imponerse Bitcoin XT "por las bravas", no haría mucha gracia y se advierte de las consecuencias nefastas para todo el ecosistema Bitcoin de una decisión tomada de manera unilateral.

En el supuesto de conseguir el consenso, se produciría un efecto dominó sobre todo lo demás:

- En primer lugar, al alcanzarse el 75% de los nodos utilizando la nueva versión de Bitcoin, los nodos "antiguos" o que no se adapten no entenderán estos nuevos bloques, al no formar parte del nuevo conjunto de reglas.

- En segundo lugar tenemos un problema de tamaño, aumentar el tamaño del bloque repercute en el tamaño del ancho de banda necesario para procesarlo, que debería ser de al menos ocho veces el actual y que debería situarse alrededor de los 800 KB por minuto. Esto a su vez repercute en los mineros, que necesitarán enlaces de como poco 10 MB/s para evitar generar bloques huérfanos no reconocidos por la red.

Ahora vienen algunas preguntas interesantes que seguramente te estarás haciendo y te anticipo que puedes encontrar de todo si navegas un rato por la Red para intentar contestarlas:

- ¿Significa esto que los Bitcoines que ya tengo o las transacciones anteriores a Bitcoin XT no serán válidas? Para nada, se mantendría la compatibilidad hacia atrás y el dinero que tengas en tu actual billetera seguirá siendo totalmente válido. En esto al menos hay consenso.

- ¿Arregla el problema definitivamente o es solo un parche temporal? Buena pregunta, porque muchos ven **Bitcoin XT como una solución temporal, motivo** por el que recibe muchas críticas. Y es que llegará un momento en que estos 8 MB también se quedarán pequeños y estaremos ante la misma situación de cuello de botella en el procesado de las transacciones por segundo. Cierto es que la propuesta de Bitcoin XT aumentaría el tamaño del bloque cada dos años hasta llegar a un tamaño máximo de 20 MB, pero ¿a partir de ahí qué? Hay quien argumenta que no se puede establecer un límite y que este debería calcularse automáticamente en función de la oferta y demanda de transacciones; para otros esta consideración es una barbaridad.

- **¿Afecta a todos los implicados en la red por igual?** La respuesta a esta pregunta también es no. A los usuarios no les afectará más que en que sus transacciones se confirmarán más rápidamente, el coste mayor lo tendrán que pagar los mineros, por lo que acabo de contar del aumento del tamaño del ancho de banda. Si se diera el caso de optar por Bitcoin

XT como alternativa, los mineros con poco ancho de banda estarían en desventaja respecto a aquellos mineros que tuvieran mejores líneas y en este caso podría no ser interesante para estos soportar la red. Obviamente, si la mayoría de los mineros se actualizan, Bitcoin podría seguir siendo soportado por la infraestructura de red subyacente y de cálculo, pero hay quien argumenta que esta desigualdad podría suponer el principio del fin de Bitcoin.

Pensad que a medida que nos acercásemos a los 20 MB puede darse el caso de que solamente unos pocos nodos sean capaces de estar procesando esta cantidad de datos de manera continua, lo que podría llevar, paradójicamente, a una centralización de Bitcoin en unos pocos nodos mineros, algo así como la creación de un "monopolio natural", aunque sobre esta posibilidad hay estudios muy interesantes que explican que no es más que una ficción económica, utilizada para justificar determinado tipo de conductas.

ENTONCES…

Os dejo un enlace que traduce un artículo de **Thomas J. DiLorenzo** que clarifica muchísimo esto de los monopolios naturales, y sacad vuestras propias conclusiones de si tiene o no sentido el argumento anteriormente dado:
http://www.liberalismo.org/articulo/270/12/mito/monopolio/natural/

- **Además está también el tema de las comisiones por las transacciones**. Cuando gran parte de Bitcoin esté minado, el único aliciente que un minero tendrá para seguir soportando la red está en las comisiones que estas le reportan, porque cada *halving* reduce la recompensa a la mitad y esta sabemos que tenderá a ser 0. Si existe un tamaño de bloque pequeño y escaso, pero con un gran valor, cuando no haya otra recompensa salvo la de las comisiones, los mineros pueden aumentar su precio, metiendo antes dentro de un bloque aquellas transacciones cuya comisión sea mayor y dejando para más tarde las que les reporten menos beneficios.

Con todo lo dicho, el debate es de lo más acalorado, con posiciones a favor y en contra de aumentar o no el tamaño del bloque. Personalmente creo que no queda otra opción a falta de otras alternativas, y cuanto antes se tome mucho mejor será para Bitcoin; no parece sensato que Bitcoin tenga que tener una limitación en este sentido, si queremos que sirva para una creciente población demandando su

uso. Las incógnitas que se pueden abrir en el futuro habrá que resolverlas cuando se produzcan.

Si queréis estar informados de cómo va evolucionando la adopción de Bitcoin XT por los nodos de la red, lo mejor es que echéis un vistazo a la página web **bitnodes.21.co**. Esta web es una más de las muchas imprescindibles que a lo largo del libro estamos describiendo, y en ella se trata de estimar el tamaño de la red Bitcoin mediante la búsqueda de todos los nodos directamente alcanzables en la red.

ENTONCES…

Estados Unidos y Alemania son los países con más nodos que directamente soportan la red Bitcoin.

Figura 2.34. Los nodos de la red Bitcoin

Los clientes que están en ejecución podemos verlos consultando el *User Agent*, algo así como una marca que determina la versión del código del cliente Bitcoin que el nodo utiliza (las versiones del cliente 0.11 y 0.10 estarían entre las primeras en el momento de escribir estas líneas):

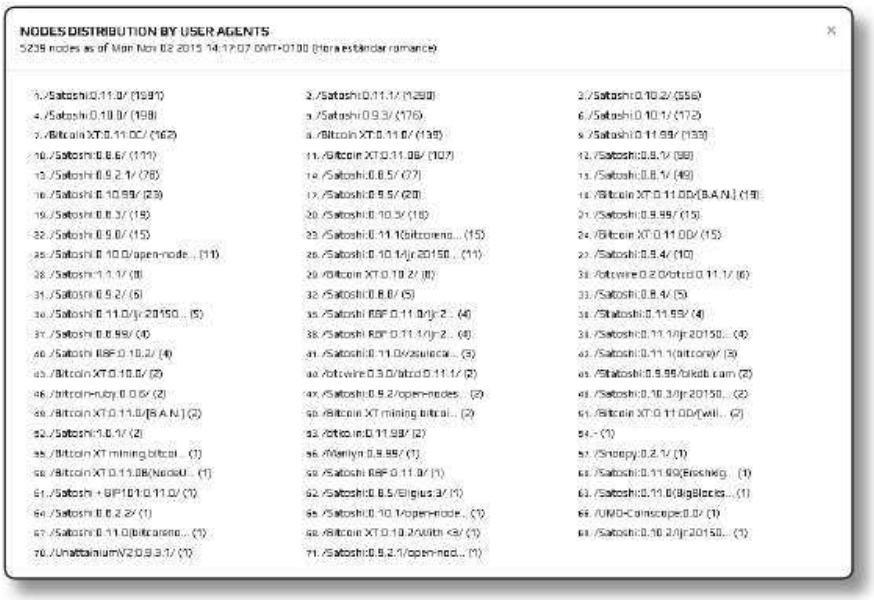


Figura 2.35. Uso de clientes Bitcoin por nodos

La adopción de Bitcoin XT en estos momentos es de 438 nodos de un total de 5.244, lo que equivale a poco más del 8%.

Sacando las últimas noticias del horno…

Y más recién hechas no pueden estar. A finales de Enero de 2016, momento en el que m encuentro escribiendo estas líneas podemos decir, que Bitcoin XT fracasó, al no conseguir (el 11 de Enero) el consenso necesario.

Casi a la par y debido al revuelo generado en torno al consenso al que hay que llegar sobre la escalabilidad de Bitcoin, que se ha montado un grupo de trabajo para debatir sobre las posibles soluciones. La primera parte del evento realizada en Canadá durante el mes de septiembre de 2015 pasó sin pena ni gloria. Hemos tenido que esperar a la segunda parte celebrada a principios de diciembre en Hong Kong para ver algo de luz al final del túnel con la propuesta presentada por **Pieter Wuille**, de la empresa **Blockstream**, que con el nombre de **Testigos Segregados** podría aumentar la capacidad de Bitcoin sin tener que necesitar de un fork duro; en resumen, la propuesta consiste en "sacar fuera" de los bloques cierta información que no es vital para el funcionamiento de los mismos, básicamente la firma del bloque que podría estar en otra estructura de datos diferente.

Con esto se conseguiría que el tamaño del bloque, a pesar de seguir siendo de 1 MB, al estar, digamos, más aprovechado con información "útil" equivaliera a tener un tamaño de 4 MB, lo que también reduciría el actual tamaño de la cadena de bloques de los más de 40 GB a poco más de 20 GB. La idea que parecía muy

buena a simple vista no ha llegado a cuajar tampoco dentro de la comunidad Bitcoin, fundamentalmente por el siguiente motivo: la solución viene, como digo, de la mano de Blockstream, esta empresa, de la que hablo en el último capítulo, es una de las principales valedoras de las cadenas laterales, y en los últimos meses ha ido contratando a varios desarrolladores de Bitcoin Core.

Este movimiento, no ha gustado nada a la comunidad Bitcoin, porque se ha visto como un intento de llegar a monopolizar el desarrollo de la criptomoneda y acabar imponiendo la visión de Blockstream a la misma. Además, Blockstream ha sido una de las empresas más contrarias al aumento del tamaño del bloque, puesto que si Bitcoin escala, sus soluciones de escalabilidad y su producto estrella, Liquid (y de pago) dejaría de tener interés. De hecho, a poco que busquéis por Internet, veréis que desde la propia Bitcoin.org, se ha prohibido a empresas como Coinbase que puedan manifestarse a favor del aumento del tamaño del bloque, en un claro intento de manipulación de la opinión.

Por otro lado, Mike Hearn, desarrollador junto con Gavin Andresen de XT, ha hecho un comunicado publicado en Medium que tampoco ha gustado ni un pelo, y que hizo que la cotización de Bitcoin cayerá de los casi 470$ a unos 360$. En este comunicado, el señor Hearn afirma que Bitcoin es un proyecto fallido y que lo abandona, habiendo vendido todas sus monedas para dejar de formar parte de él. Muchos han visto en esto, primero, una rabieta de niño grande al que le ha cabreado que su solución de Bitcoin XT no haya triunfado, y segundo (y me inclino más por esta opción) la consecuencia natural del movimiento que Mike Hearn ha hecho al irse al consorcio bancario R3 (más en el último capítulo), a los que les interesa la cadena de bloques (cadenas privadas) pero que ven a Bitcoin como una molesta mosca que puede acabar haciéndoles mucho daño (curiosamente a las pocas horas del comunicado inicial, Mike se apresuró a desmentir que su ida a R3 tenga nada que ver con su anuncio).

El enlace a la posición de Mike Hearn podéis encontrarlo en:

https://medium.com/@octskyward/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.gxlui67bu

Sin embargo, no se le puede poner puertas al campo, y aunque Bitcoin XT no ha prosperado, hay luz (y mucha!) al final del túnel, y esa luz viene de la mano de Bitcoin Classic y Bitcoin Unlimited.

Con Bitcoin Classic, liderado también por Andresen, lo que se propone es hacer un hard fork y aumentar el tamaño de los bloques a 2Mb e ir incluyendo mejoras adicionales (como los testigos segregados) en posteriores revisiones. Esta opción es la que más apoyo tiene, de momento, por parte de la comunidad, y los

pools de minería más importantes están de acuerdo en actualizar su software a esta versión (curiosamente en cuanto empezó a correr otra vez la noticia del consenso, el precio volvió a recuperarse y a pasar de los 400$ nuevamente).

Finalmente con Bitcoin Unlimited, en vez de aumentar el tamaño a los 2Mb anteriores, lo que se permite es que sean los mineros quienes aumenten este tamaño de manera manual si así lo desean, y que aunque es una opción más democrática, tiene ciertos retos técnicos interesantes que resolverse para que sea una realidad.

Una nueva era comienza sin duda para Bitcoin.

3

PONIÉNDONOS MANOS A LA OBRA

¿Recordáis lo que decía al principio del capítulo 2 sobre cuáles eran los conceptos básicos que vamos a necesitar para poder operar con Bitcoines? Si hay por casualidad algún despistado que no lo recuerde, vamos a ponerlo de nuevo aquí, son solamente cuatro conceptos, de lo que podemos entender como **operativa normal**:

- **Qué es una dirección Bitcoin**.
- Saber cómo funciona una **billetera o monedero digital**.
- Cómo **asegurar nuestro dinero** (probablemente el paso más importante para evitar que nuestro dinero pueda verse comprometido).
- Y saber **cómo enviar y recibir pagos**.

El objetivo de este capítulo es demostrar, como dice el dicho, el movimiento andando, y lo haremos de un modo que creo que será el más sencillo de seguir: primero describiremos qué es una dirección Bitcoin y qué particularidades presenta, para luego adentrarnos en los tipos de billeteras existentes y analizar varias alternativas que podemos usar para nuestra operativa diaria. Si alguna vez te has preguntado qué es eso de una billetera fría o un monedero de papel o en la cabeza, o qué significa cuando oímos eso del determinismo de una cartera, en este capítulo lo explicaremos también.

Luego haremos un repaso por los diferentes métodos que hay para obtener Bitcoines, sin dejar (o al menos eso creo) ninguno en el tintero. Lo he dividido en dos partes, los métodos clásicos, tales como el uso de los *faucets*, y los nuevos métodos, donde entran los más modernos como son el uso de plataformas de terceros, por ejemplo, HalCash o similares. La idea es que cuando acabemos este capítulo, seamos capaces de operar con Bitcoin de una manera suficientemente autónoma, segura y nos sintamos cómodos haciéndolo.

Para apuntalar esa confianza, hay dos secciones que considero de especial interés y que recomiendo no olvidar de leer, la importancia de la confianza en el operador de compra/venta de Bitcoin y qué es eso de los HYIP; nos ayudarán a ir más seguros en nuestro día a día.

3.1 ¿MI DIRECCIÓN BITCOIN?

Lo primero que necesito para tener una dirección Bitcoin es disponer de un monedero o billetera digital. Al igual que un monedero tiene diferentes compartimentos para mantener separados los billetes de las monedas, organizaremos los monederos en direcciones. El movimiento de dinero se produce moviendo una cantidad X de moneda desde una dirección de origen de un monedero, a una dirección de destino Y de otro monedero, y es la única información que hay que proporcionar para que alguien pague a otro.

Como los monederos pueden pertenecer a cualquiera, no hay un intermediario que sea el encargado de realizar este proceso como sucede cuando pagamos con una tarjeta de crédito. Si yo mando una cantidad de dinero a otra persona, la operación se realiza de manera directa entre él y yo. No media nadie, estamos él y yo y la infraestructura de red que lo soporta todo.

Esto tiene una consecuencia interesante: ¿si yo envío dinero a una dirección y me equivoco, qué sucede? Simple, pierdes el dinero, puesto que el envío de dinero entre direcciones es irreversible como os expliqué en el capítulo anterior. Dado que esto supone un problema, por ejemplo para el comercio electrónico (pago por un producto y no me lo envían, no puedo cancelar la operación) se han orquestado las soluciones de las que ya hablamos: **escrow** y **two-factor**.

De momento, mejor no te equivoques de dirección.

Las direcciones a primera vista asustan un poco, porque no son humanamente inteligibles, es decir, son una secuencia hexadecimal que tiene un aspecto similar al siguiente: 12qia5PK82qoKfqwjBVmjGWtznd3MckYFM.

Lo sé, no es muy fácil de recordar, pero tranquilos, el software de los monederos permite asignarles los nombres que deseemos para que sea más cómodo trabajar con ellos. Por cierto, no hay límite en el número de direcciones que podemos tener dentro de nuestro monedero, y se recomienda crear una diferente para cada transacción en la que vayamos a participar como mecanismo adicional de seguridad (pero de esto ya hablaremos).

Todas las direcciones Bitcoin llevan asociada una clave privada, clave que es la que nos permite gastar el dinero almacenado en esa dirección. Esta clave privada se

almacena en un archivo que se encuentra ubicado donde esté instalado el monedero que estemos utilizando. Siempre existe una relación entre la clave privada y la clave pública, es más, la clave pública (que es a fin de cuentas la dirección Bitcoin que nosotros utilizamos) se difiere o genera a partir de la clave privada mediante la ejecución de una serie de pasos fijos y establecidos de antemano y que luego explicaré. El modo en como la billetera utilice la clave privada para generar la clave pública (nuestra dirección) sirve para clasificar los monederos entre deterministas o no deterministas. Si pierdo la clave privada, podemos decir adiós a los Bitcoines almacenados en las direcciones públicas generadas.

Las direcciones públicas Bitcoin se componen de 27 a 34 caracteres, son sensibles a las mayúsculas y minúsculas y deben escribirse tal cual para poderse utilizar, motivo por el que suelen utilizarse **códigos QR** para simplificar la operación.

ENTONCES…

Lo habitual es que tengan 34 caracteres. A menor longitud, más improbable es que la dirección se genere y se debe a que se partió de valores numéricos con ceros iniciales. La probabilidad de una dirección de 33 caracteres es de 1 de cada 10, de 32 1 de cada 100… y así sucesivamente hasta llegar a 27.

Siempre comenzarán **por 1 o 3**. El 1 sirve para indicar que es una dirección Bitcoin normal, mientras que el 3 se deja para señalar que la dirección es del tipo multifirma, es decir, que para poder acceder al saldo que esa dirección contiene es necesario la firma de al menos dos claves privadas.

Figura 3.1. Ejemplo de código QR desde Bitcoin Core

Solamente hay dos caracteres "prohibidos" en una dirección Bitcoin, la letra "O" mayúscula por su semejanza con el número 0 y la letra mayúscula y minúscula "l", para no confundirlas con el número 1. Las direcciones se pueden crear sin estar conectado a la red, hasta que no entran dentro del circuito de transacciones equivalen a cuando escribimos un cheque y no vamos al banco con él; podemos tener tantos cheques como deseemos, cumplimentados, listos y preparados para usar, esta misma idea es la de una dirección generada sin conexión (*offline*).

Todas las direcciones llevan dígitos de control, de modo que si por algún motivo nos equivocamos al escribir, estos dígitos sirven para indicar que la dirección no es válida. ¿Podría aceptarse una dirección errónea como válida dentro de una transacción? Bueno, esta probabilidad se ha calculado y se estima que es de 1 entre 4.290 millones, que es lo suficientemente pequeña como para no preocuparse de que pueda suceder (es más, el margen de error es mucho menor que el que maneja cualquier empresa de procesamiento de pagos).

Otra pregunta más sutil que podemos hacernos es: si yo tengo mi monedero y genero una dirección Bitcoin, ¿no podría haber otra persona que llegue a generar la misma dirección Bitcoin y se monte un pequeño lío? Matemáticamente es posible que suceda, sin embargo, en la práctica y al igual que el caso anterior, el que realmente se produzca esta posibilidad, que recibe el nombre de colisión, en un tiempo razonable, es prácticamente inexistente y cercana a cero; en el próximo capítulo volveremos sobre esto de las colisiones cuando hablemos de las funciones *hash*.

ENTONCES…

Las colisiones tienen que ver con el uso de un tipo de función que he comentado de pasada anteriormente y de las que hablaremos en el capítulo dedicado a la criptografía, las funciones *hash* que en Bitcoin son básicas para comprender su funcionamiento interno.

A modo de curiosidad, os recomiendo una entrada en reddit.com en donde se inició un interesante debate sobre las colisiones de direcciones Bitcoin y en donde el autor concluye que se necesitarían unos **6.500 millones de años solo para tener una probabilidad cercana al 50%** de que ocurriera y más de **11.700 millones de años para que esta probabilidad fuera de un 99%**. Espero que para entonces, hayamos conquistado gran parte del universo, por la cuenta que nos trae.

https://www.reddit.com/r/Bitcoin/comments/3fgrk5/how_long_would_we_have_to_use_bitcoin_before_we/

3.1.1 Direcciones de vanidad

Si nos fijamos en las direcciones que cualquier billetera nos genera y con lo que acabamos de ver, la forma que una dirección presenta siempre será bastante poco amigable para el usuario. Cierto que los códigos QR ayudan muchísimo lo mismo que las etiquetas que se pueden poner sobre las direcciones, sin embargo, el formato de la dirección propiamente dicha es bastante hostil. Para mitigar en lo posible este problema, han aparecido algunos programas que intentan que la secuencia de caracteres que forman la dirección tenga un formato más amigable y amable, como una forma de personalizarla. Estas direcciones reciben el nombre de direcciones de vanidad (*vanity address*) y pueden parecerse a lo siguiente: 1LibroBitcoi8ALj6mfBsbifRoD4miY36v o 1SantiagoFVj8ALj6mfBsbifRoD4miY36v, donde se ven algunas secuencias de caracteres reconocibles y entendibles. Visto lo cual, el que se llamen de vanidad parece un nombre muy acertado, ¿no os parece?

Para generar este tipo de direcciones en GitHub está disponible la herramienta **Vanitygen**, un programa muy popular que a partir de un patrón de entrada es capaz de generar direcciones como las anteriores y que podéis descargar desde la siguiente dirección: *github.com/samr7/vanitygen*.

ENTONCES…

Ojo con las aplicaciones que utilicéis para generar las direcciones de vanidad (aunque es aplicable a las normales también), conviene saber dónde se están almacenando las claves privadas; si lo hacéis a través de una web y no estáis seguros de que seáis los únicos con acceso a estas claves, no os sorprenda que el dinero *a posteriori* os pueda desaparecer. ¡Estáis avisados!

Este programa funciona mediante un algoritmo de fuerza bruta, lo que hace internamente es realizar todas las posibles combinaciones y cálculos necesarios, uno por uno, hasta que consigue generar una dirección que case con el patrón que hayamos introducido. Los factores que van a influir en el tiempo de cálculo son básicamente dos: el hardware que ejecute la aplicación y la longitud del patrón, a mayor longitud, más tiempo de cómputo. Por tanto, obtener una dirección de vanidad no es gratis.

¿Cómo generaríamos una dirección de vanidad usando este programa? Bueno, aunque la aplicación tiene muchas opciones interesantes, la forma más simple de trabajo es la siguiente (supuesto que hemos descargado el ejecutable para Windows, en caso de Linux tendremos que haber bajado el código y compilarlo con *make*):

- Ejecutamos **vanitygen –v –o claves.txt –i 1Prueba**, los argumentos "–v", "–o" y "–i" sirven, respectivamente, para indicar que queremos salida extendida (–v), es decir, que el programa muestre todo lo que pueda por pantalla y no se corte en darnos información; el fichero donde se guardará la clave privada de la dirección generada (–o), e indicar que para el patrón que queremos generar no importen mayúsculas y minúsculas (–i), lo que hace que tarde aún menos, al reducir un poco más la complejidad del algoritmo. Fijaos en que el patrón debe comenzar con un 1 como todas las direcciones Bitcoin.

- Ejecutamos la orden y al cabo de unos minutos (puede tardar más en función del hardware) tendremos una salida similar a la siguiente:

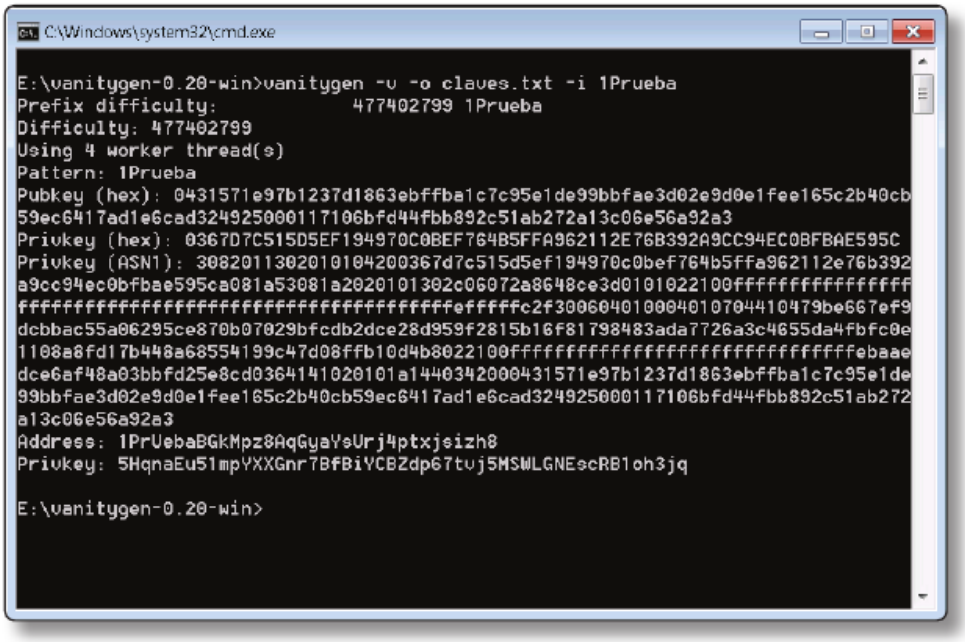


Figura 3.2. Generando una dirección de vanidad

Daos cuenta de que la aplicación nos da una aproximación de la complejidad asociada al cálculo de la dirección con el patrón solicitado, y que puede ser verdaderamente grande en cuanto nos pasamos de cinco caracteres; si tuviéramos mucho poder de cálculo a nuestra disposición, podríamos hacerlo en cuestión de minutos o por qué no, crear un servicio de pago para que todo el mundo pudiera usarlo.

Ahora, solo nos restaría importar la clave privada a nuestra billetera y listo, tenemos nuestra dirección de vanidad disponible para ser utilizada cuando queramos y los fondos que vayan a ella bajo nuestro control. Luego explico cómo hacerlo.

Aunque el uso de direcciones de vanidad puede ser muy bueno por razones de *marketing* o interés comercial (o incluso por marca personal), pensad que cuando estamos haciendo uso de este tipo de direcciones, cedemos parte de la privacidad que Bitcoin garantiza, que aunque sabemos que no es al 100%, con el uso de direcciones de vanidad resulta más fácil hacer un seguimiento del movimiento del dinero dentro de la cadena de bloques. Por otro lado, una dirección de vanidad con un patrón específico no significa que esté asociado ni pertenezca a una determinada entidad, por ejemplo, yo puedo haber generado la dirección con la marca IKEA "1ikEAJRkifuJK4dTsHgp5sARtJGJWEgs1" y sin embargo no pertenezco ni guardo relación con la empresa IKEA, pero podría utilizar dicha dirección haciéndome pasar por alguien de esta compañía y solicitar el pago de una cierta cantidad suplantándolos. Por cierto, he usado IKEA porque son 4 letras y el tiempo en generar la dirección es razonable, no hay más motivo que ese, si os gusta más usad FORD, NISSAN, AEG… o la que más os guste.

ENTONCES…

Este tipo de situaciones donde se convence a un usuario para que envíe dinero a una dirección que no está bajo el control del usuario legítimo al que los fondos están destinados recibe el nombre de ataque de tipo **address tampering** o ataque por manipulación de dirección, y suelen deberse a que es posible hacer otro tipo de ataque del tipo **man-in-the-middle** o JANUS. Es un tipo de ataque en donde un intruso se sitúa justo entre emisor y receptor, de manera que puede leer, insertar o modificar los mensajes entre ambos sin que se den cuenta.

3.2 BILLETERAS O MONEDEROS DIGITALES. TIPOS Y DIFERENCIAS

Acabamos de decir que para disponer de una dirección Bitcoin, necesitamos una billetera o monedero digital, que se encargue de su gestión; vale, ¿cómo consigo una? Una billetera es un programa de ordenador, un programa que nos permite almacenar direcciones Bitcoin junto con las claves privadas que acceden a los fondos que contienen, a fin de que podamos enviar y recibir dinero.

Las billeteras se suelen clasificar de muchas maneras diferentes dependiendo del modo en que generan las direcciones públicas o desde donde son accesibles.

De acuerdo Santiago, pero aún no me has dicho dónde conseguir una. Sigue leyendo, no seas tan impaciente…

3.2.1 El determinismo en las billeteras

Hemos dicho que en función de cómo generemos/manipulemos la clave privada, las billeteras se pueden clasificar en deterministas o no deterministas, veamos qué importancia tiene esto para la operativa normal con Bitcoin.

Una **billetera determinista** es aquella que para generar las direcciones públicas parte de una semilla, una palabra o conjunto de palabras, que se utiliza para generar la clave privada y a partir de ahí las públicas. La ventaja es que puedo usar esta palabra o secuencia para restaurar mi billetera en caso de tener problemas o hacer copias de seguridad.

Originalmente, la billetera implementada en Bitcoin Core generaba un *buffer* de almacenamiento con un conjunto aleatorio de claves privadas para ser utilizadas en la generación de las direcciones públicas (**no determinista**). Sin embargo, el efecto es que una vez que acabamos con este *buffer* (que solía tener un tamaño de 100 direcciones), generar nuevas direcciones públicas implicaba que perderíamos el control de hacer copias de seguridad, es decir, al reutilizar las que tenemos en el *buffer*, el histórico de lo hecho, se esfumaba. Esto no sucede con las deterministas, donde es posible generar un número ilimitado de direcciones al momento y por ende, partiendo de la semilla lograr regenerar la billetera con sus direcciones y saldos completos.

Hay dos tipos de billeteras deterministas:

- **Billetera determinista de tipo 1**

  Es el modelo más simple de generar direcciones a partir de una cadena conocida de partida. Para generar la clave privada se parte de ejecutar la función **SHA-256 (cadena conocida + n)**, donde n es un código ASCII que comienza en 1 y se va incrementando según se van necesitando nuevas claves.

- **Billetera determinista jerárquica de tipo 2**

  Se describe en la **BIP 0032** y su autor es **Gregory Maxwell**, en ell la semilla es un valor aleatorio de 128 bits que se presenta al usuario como una lista de 12 palabras comunes en inglés para ayudarle a recordar. La semilla es usada después de realizar 100.000 pasadas sobre SHA-256 a fin de mejorar la fortaleza y reducir los ataques contra palabras usadas por el usuario que puedan resultar fáciles de atacar.

3.2.2 Billeteras online y offline

Una billetera *online* es cualquier tipo de billetera que está conectada a la Red en todo momento; puede estar instalada en nuestro ordenador, en el móvil o tableta que utilicemos todos los días, o por el contrario estar ubicada dentro de una web como páginas de Internet.

Las billeteras *offline* también reciben el nombre de billeteras "en frío" o "almacenamiento en frío" o "monedero fuera de línea", cualquiera de estas tres definiciones sirve para indicar que es una billetera que no está conectada a Internet de ninguna manera. Por poner un símil con el mundo físico, el almacenamiento en frío es lo más parecido a tener nuestro dinero metido en una **caja fuerte**. Está considerado como el mecanismo más seguro de almacenamiento, puesto que no hay conexión directa entre nuestro dinero y la Red. En estos casos, es muy interesante la posibilidad de poder firmar una transacción de manera offline, proceso del que hablaremos un poco más adelante.

Las billeteras *offline* pueden tener diferentes formatos, que pueden ser tan simples como una hoja de papel (billeteras de papel) o tan complicados y sofisticados como algunos dispositivos hardware específicos que han aparecido comercialmente. Como hablo de las billeteras de papel más adelante, dejadme que me pare un segundo en este último tipo de almacenamiento en frío.

Hardware, como digo, especializado para almacenar Bitcoines cada día hay más (fijaos en que hablo de hardware especializado, pero un ordenador o incluso una llave USB que nunca esté conectado a Internet y que utilice por ejemplo una billetera como Armory, también nos serviría como almacenamiento frío). Hay soluciones de todo tipo y precio, que abarcan las necesidades de cualquier usuario. Personalmente creo que siempre que uno ya empieza a tener cierta cantidad de Bitcoines, la mejor manera de tenerlos a salvo es en uno de estos dispositivos, aunque a medida que ganes confianza y conocimiento seguro que elaboras una estrategia personalizada para mantener a salvo tus finanzas.

Mientras tanto, una buena solución puede ser la proporcionada por **Trezor**, un pequeño dispositivo del tamaño de una tarjeta de crédito que se vende por 99$. Dispone de todas las funcionalidades que se le exigirían a una billetera así como diferentes niveles de seguridad, protección por contraseña, *backup* de la billetera y un modo de trabajo muy simple que se basa en dos botones que permiten aceptar o cancelar las transacciones. Además, si te das de alta en la web puedes ver tu histórico de operaciones y realizar algunas operaciones como puede ser cambiar la dirección de destino antes de que se llegue a procesar por la Red.

Figura 3.3. Trezor, una billetera muy fría

Por cierto, antes de comprarlo echad un vistazo a las FAQ para ver dónde y cómo hacerlo, porque en Amazon sale bastante más caro.

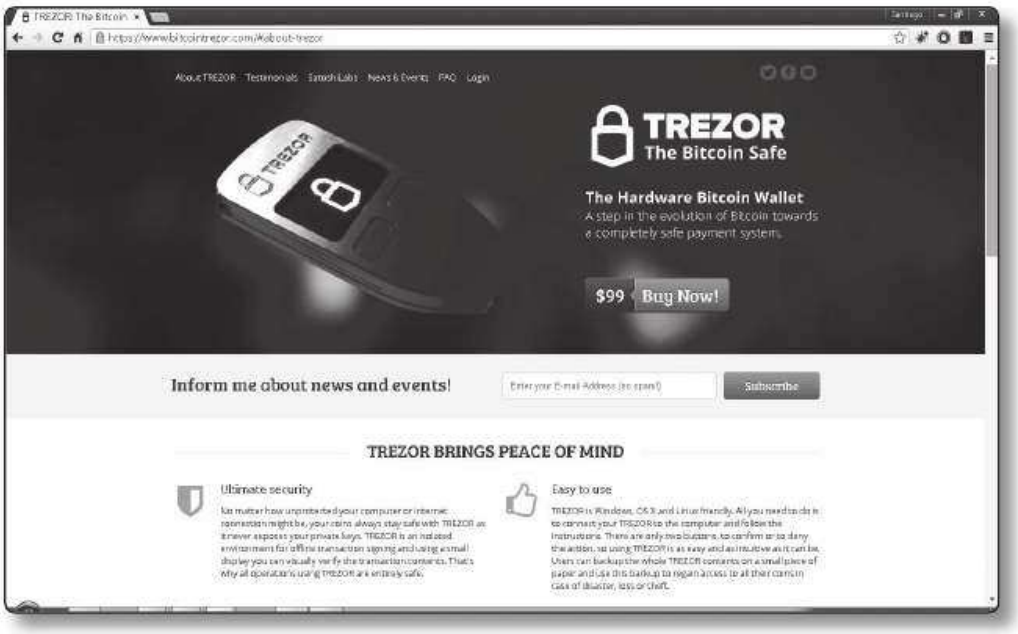


Figura 3.4. Ledger Nano

Otro dispositivo para almacenar en "frío" nuestros Bitcoines es **Ledger Wallet**, que tiene algunas variaciones que podemos considerar. El dispositivo más

interesante es **Ledger Nano**, con apariencia de lápiz USB estándar, sirve muy bien para nuestros propósitos de asegurar el dinero fuera de la Red. Es menos sofisticado que Trezor (aunque más barato) y se integra a la perfección con la aplicación Ledger Wallet (con versiones para Chrome, Android e iOS y de código abierto), que interactúa con el dispositivo y nos permite restaurar nuestro dinero en caso de pérdida o daño y gestionar la billetera de un modo simple.

3.2.3 Billeteras web

Una billetera web es un tipo especial de billetera *online* que como su nombre indica, reside en la web y accederemos como si de una página normal de Internet se tratara, lo que simplifica el proceso de interacción con Bitcoin al no tener que instalar ningún programa en nuestro ordenador. Permiten realizar las tareas típicas de envío y recepción de dinero como si fueran programas de escritorio, y suelen incluir utilidades adicionales como iremos viendo. Habitualmente las empresas que proporcionan billeteras en la web suelen proveer de software adicional para instalar en nuestros terminales móviles, tal es el caso de **blockchain.info**, **Xapo** o **Coinbase**.

Cualquiera de las tres anteriores es un buen ejemplo para ilustrar el uso de las billeteras web, la operativa es siempre la misma: registrarse y comenzar a trabajar. Además aprovecharemos el uso de las billeteras para contar aspectos colaterales que van a comenzar a salir como consecuencia de su uso. Estos aspectos tienen el mismo significado independientemente de la billetera que usemos, por ejemplo, el firmado de transacciones *offline*, la verificación de mensajes, etc., son acciones posibles que podremos realizar desde las billeteras y que aunque van más allá de enviar o recibir dinero, resultan muy útiles de conocer.

3.2.3.1 BLOCKCHAIN.INFO

Blockchain.info es un servicio de billetera así como un explorador de bloques (con algunas utilidades adicionales como una API de programación propia de la que hablaremos en el último capítulo del libro), que entró en funcionamiento en 2011, lo que le convierte en uno de los servicios más veteranos, siendo en el año 2013 la página web Bitcoin más visitada y tiene registradas más de cuatro millones de billeteras, lo que la convierte en una de las soluciones online más utilizadas y populares.

El registro en blockchain.info no requiere más que el uso de una dirección de correo electrónico y una contraseña, aunque si no quieres crear nada y solamente te apetece ver cómo funciona el servicio, tienes la opción **Experimente con la cuenta de prueba** que permite jugar un rato con las opciones del monedero.

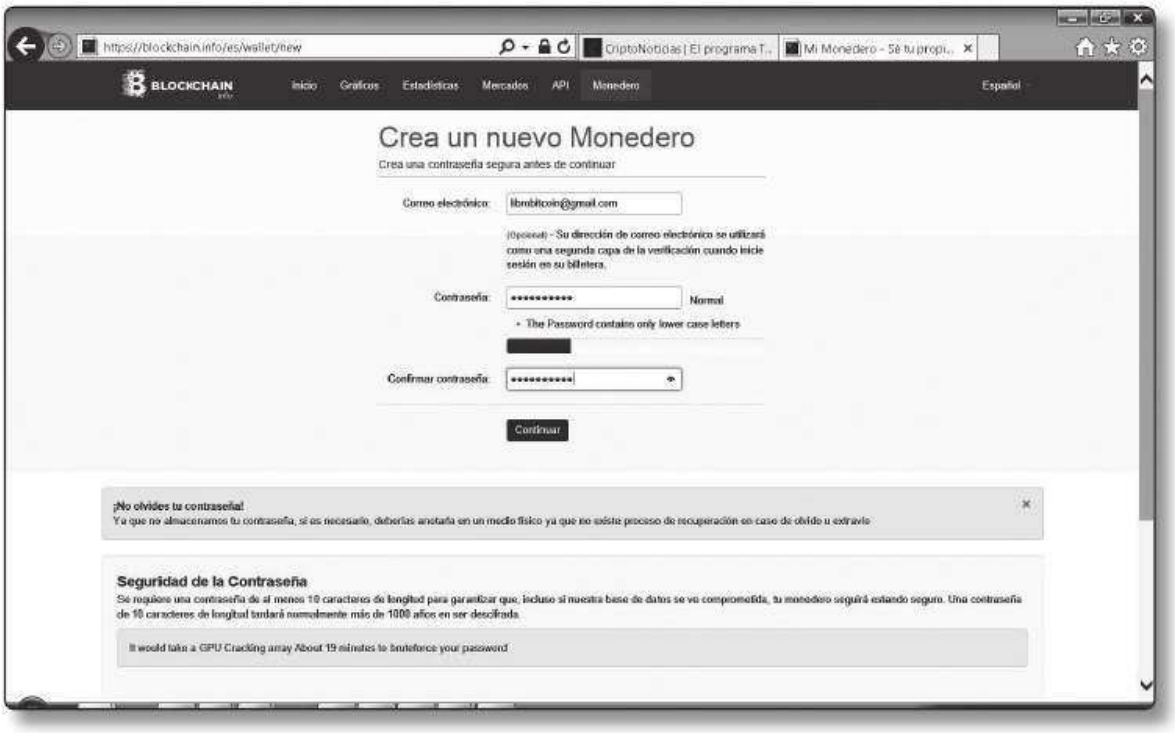


Figura 3.5. Registro en blockchain.info

Para registrarnos pulsamos en **Crear una cuenta de Mi Monedero de manera gratuita** e introducimos los datos anteriores (procurad siempre que la contraseña sea lo más segura posible, con letras mayúsculas y minúsculas, números, que no sean secuencias de palabras fácilmente atacables por fuerza bruta… en definitiva, las reglas que siempre deberíamos de seguir). Por suerte, blockchain.info también ayuda en esto y nos dice cómo de buena es la contraseña que estamos eligiendo.

Como es una billetera del tipo determinista, al registrarnos nos muestra un conjunto de palabras que podríamos usar para restaurar la billetera en caso de pérdida, sería una buena idea guardarla por si ocurre cualquier incidente; obviamente donde guardemos esta información debería garantizar que nadie no autorizado pueda hacerse con el juego de palabras.

Finalizado el proceso de registro, a nuestra dirección de email habrá llegado un correo de confirmación con los datos básicos de acceso y el identificador que usa blockchain.info para nuestro monedero. Podremos acceder a nuestra billetera desde la opción **Monedero** del menú principal. Blockchain.info cifra todo en local usando tu navegador, esto significa que ellos no tienen acceso a ninguna información que pueda considerarse comprometida del usuario. Al estar cifrado en el cliente utilizando JavaScript, cualquier ataque que se realice al servidor queda sin efecto, puesto que la información contenida allí está cifrada en origen y por tanto es ininteligible.

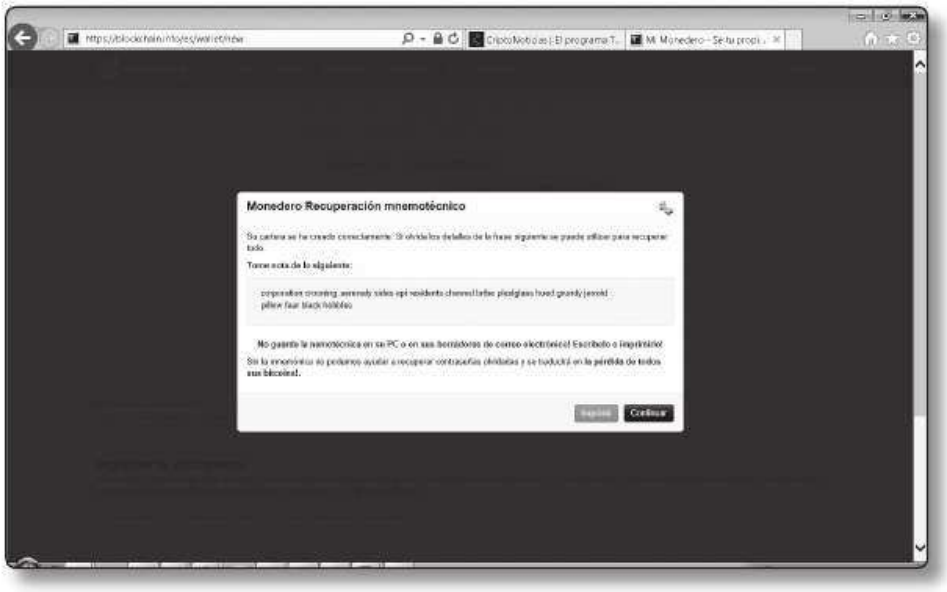


Figura 3.6. Listado nemotécnico de recuperación en blockchain.info

Cada vez que recibamos o realicemos un pago, podremos ser notificados por SMS, *email*, Skype o mediante una llamada HTTP POST. Como aspecto interesante permite el envío de Bitcoines por Facebook, SMS y *email*, lo que la convierte en una de las billeteras más versátiles y al estar traducida al español, la barrera de entrada por el idioma está superada.

Realizada la conexión estaremos en la página **Mi Monedero**, todas las gestiones que podemos hacer se acceden desde aquí. La visión por defecto nos muestra su saldo y el total de transacciones tanto recibidas como enviadas.

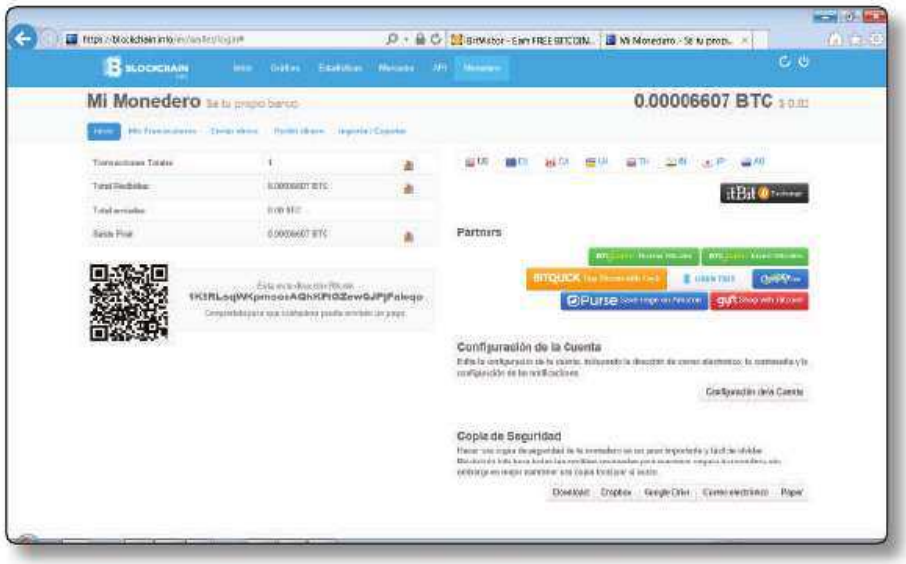


Figura 3.7. Recibir dinero en blockchain.info

Configuración de la cuenta

Al acceder a la configuración del monedero siempre solicita la contraseña de validación como medida de protección. Sin ánimo de entrar en detalle en todas las opciones posibles (situadas en el menú de la izquierda de la pantalla), sí que hay varias cosas de las que debes asegurarte que estén realizadas:

- Que tu **dirección de correo esté verificada** (accesible desde **Personal**), lo que significa que blockchain.info usará la dirección como una capa de seguridad adicional y todos los eventos que sucedan dentro de la billetera se te enviarán.

- Has introducido **un número de móvil válido** (accesible desde **Personal**). Cuidado aquí con los SMS y los operadores, porque a veces pueden producirse retrasos en la recepción de los códigos que se envían y tener problemas para acceder a nuestro dinero.

- El **tiempo de inactividad para cerrar sesión** (accesible desde **General**): por defecto a los 10 minutos de inactividad la cuenta se cerrará, pero puede ponerse un valor menor o incluso dejarlo desactivado (no lo recomiendo, claro).

- **Autenticación de dos factores** (accesible desde **Seguridad**): hay varios tipos posibles: SMS, correo electrónico, Google Authenticator o Yukibei. Activad el que más os guste, de este modo cada acción importante en la web os envía un mensaje (de diferente naturaleza según el método elegido) para reconfirmar la acción.

- **Frase secreta** (accesible desde **Seguridad**): tampoco está de más incluir una frase secreta (hasta 256 caracteres de longitud) que ayuda a blockchain.info a comprobar tu identidad en caso de que pierdas el identificador del monedero.

- **Desactivar IP Tor** (accesible desde **Restricciones de IP**): de este modo no se puede acceder al monedero desde una IP que pertenezca a Tor, comúnmente los ataques pueden venir desde aquí.

Recibir dinero

Para recibir dinero desde **Mi Monedero** disponemos de una dirección pública ya creada junto con el código QR que la representa, basta proporcionar dicha información para que nos envíen dinero a nuestra cuenta.

Sin embargo, en aras de una mayor seguridad, siempre se recomienda utilizar direcciones diferentes para realizar diferentes transacciones, y lo más recomendable es crear tantas como vayamos necesitando en nuestra operativa de trabajo.

Figura 3.8. Mi Monedero blockchain.info

Para hacerlo está la opción **Recibir dinero**. Al pulsarla veis que hay un botón con el nombre **Nueva dirección**, que al accionarlo nos pide que completemos el siguiente formulario con unos datos básicos:

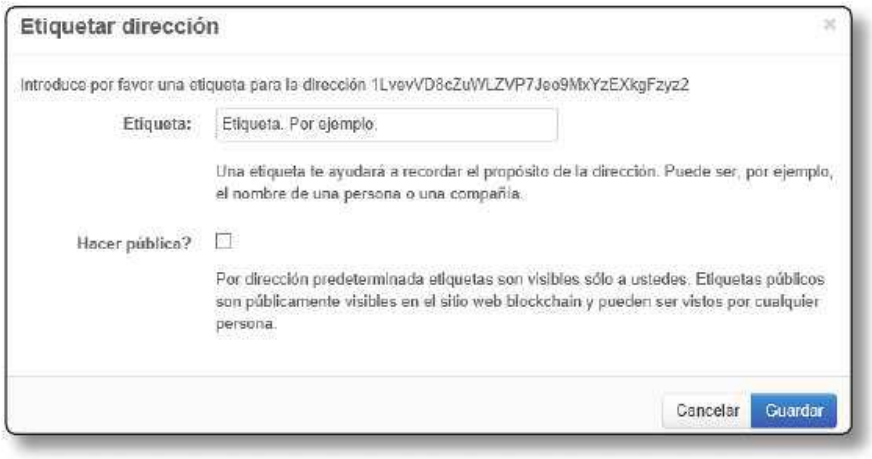


Figura 3.9. Crear nueva dirección con blockchain.info

Es posible añadir una etiqueta a una dirección Bitcoin para que nos resulte más fácil de recordar. Estas etiquetas son privadas y solamente sirven para ti, si queremos podemos hacerlas públicas para que sean visibles desde blockchain.info para todo el mundo.

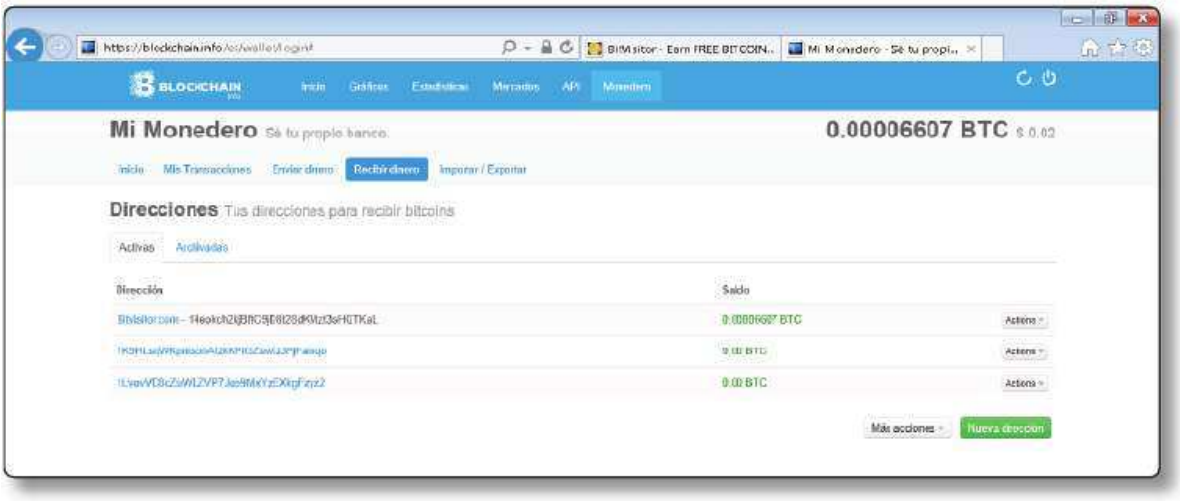


Figura 3.10. Mis direcciones en blockchain.info

Cuando se crea una nueva dirección, tenemos un botón **Actions** con diferentes opciones: por ejemplo archivar la dirección cuando ya no queramos usarla, cambiarle la etiqueta, obtener el código QR asociado, etc. El botón **Más acciones** presenta funcionalidades adicionales, como crear un almacenamiento en frío, ver el diagrama de relaciones, agrupar las direcciones por marca y verificar mensajes.

Las opciones **Verificar mensaje** y **Firmar mensaje** son particularmente útiles, y están disponibles también en otras billeteras. Sirven para ayudar a identificar que una dirección pertenece realmente a una persona, a fin de garantizar que enviaremos el pago a quien debemos. Por ejemplo, si yo firmo el mensaje "Esta dirección es del libro Bitcoin. Guía completa de la moneda del futuro" con la dirección 1LvevVD8cZuWLZVP7Jeo9MxYzEXkgFzyz2, lo que haré será irme a **Firmar mensaje** y completar el siguiente formulario:

Figura 3.11. Firmando un mensaje con una dirección

Pulsamos **Firmar mensaje** y obtendremos la firma siguiente:

H5et1EjgGA+s50LvQii8xgwZJVUFPunQJeJ9tEIubAIXbm7Zm4F9hXN
MGc8XE4AcsNF/M30MfpRFIEzSQX6hNMA=

Ahora toda esta información se la puedo dar a una persona que quiero que me envíe dinero a la dirección anterior: 1LvevVD8cZuWLZVP7Jeo9MxYzEXkgFzyz2, de manera que esta persona puede comprobar desde **Verificar mensaje** en su billetera y antes de enviar el dinero, que la información que le proporcioné es correcta y por tanto que la dirección me pertenece a mí:

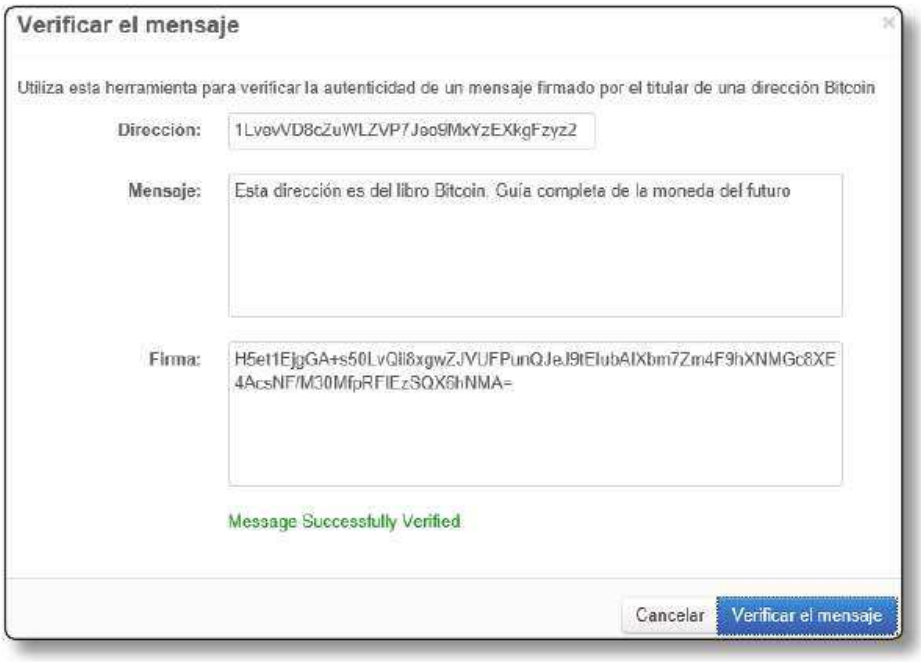


Figura 3.12. Verificando un mensaje

Si alguien interceptara el mensaje anterior y pusiera su dirección Bitcoin, quien realizara la verificación obtendría un error y sabría que algo está mal de antemano. Otro ejemplo, el saldo de las direcciones Bitcoin está accesible desde la cadena de bloques, cualquiera puede ver cuántos Bitcoines hay en una determinada dirección. Fijaos en que saber el dinero que hay en una dirección pública Bitcoin no significa que se tenga el control del dinero que hay en ella, para eso necesitaría tener el control de la clave privada. Dado que yo no sé a quién pertenecen las direcciones públicas, tampoco sé (en teoría, recordad que Bitcoin no es anónimo 100%) quién es el dueño, en el mundo real, del dinero. Podemos usar la herramienta *online* **blockexplorer.com** para saber el saldo de cualquier dirección usando el formato: *http://blockexplorer.com/address/DIRECCION_A_CONSULTAR*.

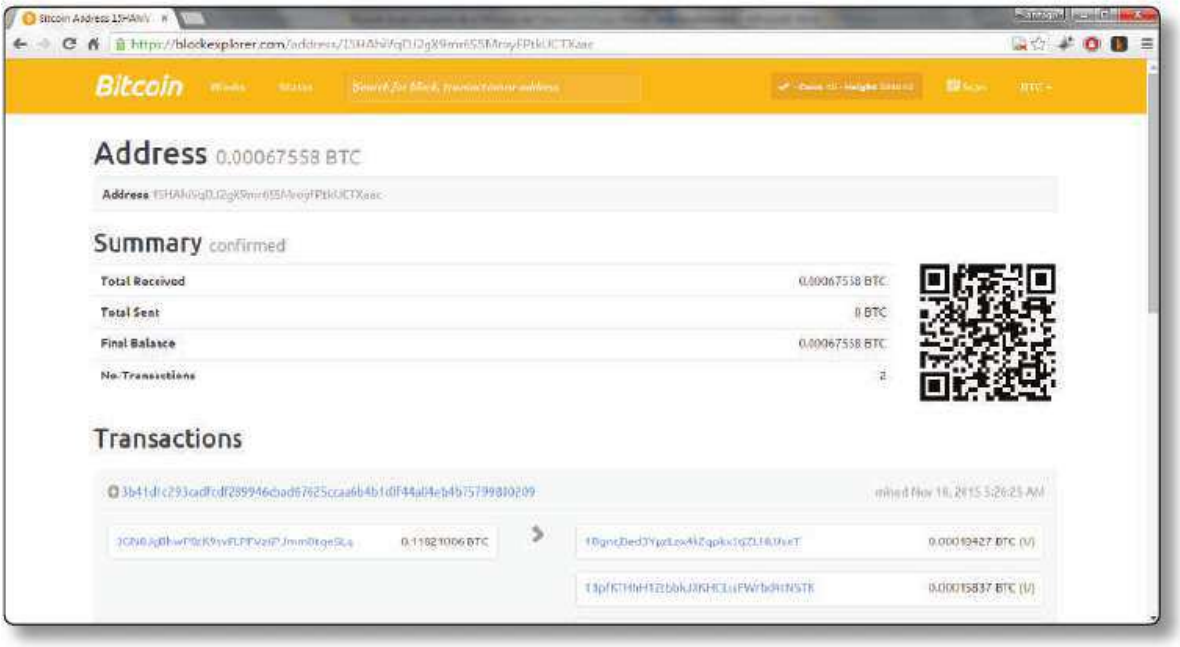


Figura 3.13. Consulta de saldo de la dirección 15HAhiVqDJ2gX9mr6S5MroyFPtkUCTXaac

Vale, sigamos pues. El que yo pueda consultar el saldo de una dirección y el que pueda firmar un mensaje con esa dirección puede ser útil por ejemplo para asegurar a otra persona que dispongo de fondos suficientes y tengo cierta solvencia (habría que analizar otros parámetros pero para el ejemplo que estoy explicando y para que me entendáis vale perfectamente). Supongamos que en 1LvevVD8cZuWLZVP7Jeo9MxYzEXkgFzyz2 he puesto 10 BTC (algo más de 2.000 euros al precio actual), y cambio el mensaje por "Aval de pago de lo que me dé la gana", y firmo el mensaje con la dirección como ya sabemos hacer. Ahora el *hash* devuelto será diferente obviamente.

Esta nueva información se la puedo pasar a otra persona que puede comprobar dos cosas: primero que la dirección me pertenece y segundo que tiene un saldo de 10 BTC. Esta persona puede decidir hacer negocios o no conmigo, en cuanto mantenga el saldo en la dirección, un mecanismo muy simple para implementar un sistema de aval sin muchas más historias y que tiene muchas limitaciones, pero creo que el ejemplo ilustra muy bien las posibilidades de Bitcoin para ir mucho más lejos de la mera compra de bienes y servicios.

Enviar dinero

Lo haríamos desde la opción **Enviar dinero** (lógico) del menú principal. Hay varias opciones posibles, pero la más habitual son las que están definidas como **Envío rápido** o **Envío personalizado**.

En ambas se indica la dirección destino y la cantidad de dinero a enviar, pero la segunda opción permite a su vez indicar varias cosas interesantes:

- La cantidad que se destina como **comisión (fee) de la operación** y que se destinará al minero (luego volveremos sobre el tema de las comisiones) que incluya la transacción dentro de un bloque.

- **La dirección de cambio**: si estamos enviando una cantidad que es menor que la cantidad que tenemos en la dirección, por ejemplo, tengo 3 BTC en una dirección X y envío 1 BTC a una dirección Y. En este caso, hay un "cambio" de 2 BTC que no se debe enviar y que nos tiene que ser devuelto, esa dirección de devolución es lo que indicamos aquí. Pensad que en las operaciones con Bitcoines sucede como con el efectivo en el mundo real, si pago con un billete de 5 euros algo que cuesta 2 euros, me devolverán 3 euros, dónde guarde ese cambio (el monedero o el bolsillo) depende de mí como usuario.

- **Nota pública**: se puede incluir un mensaje que quede registrado de manera permanente en la cadena de bloques. Esto es diferente de lo que expliqué antes, aquí solamente dejamos constancia en la cadena de bloques de lo que deseemos. Por ejemplo, podría poner "Con esta transacción demuestro mi amor por el destinatario"; hay mucha gente que critica que la cadena de bloques se está llenando de *spam* y mensajes absurdos de manera innecesaria, y algo de razón sin duda tienen.

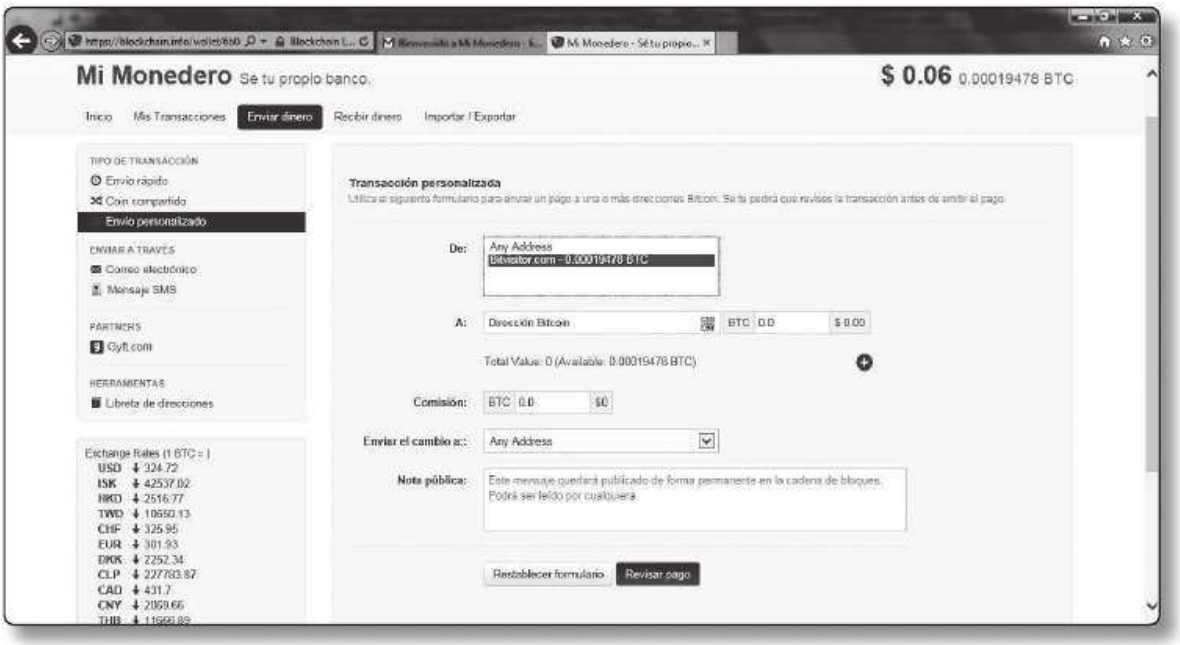


Figura 3.14. Enviando dinero con blockchain.info

Fijaos en que para enviar dinero por correo electrónico o por SMS, tenemos dos opciones en el menú de la izquierda que lo permiten y funcionan de un modo muy simple, se indica el *email* o el SMS, la cantidad y pulsamos el botón **Enviar pago**, y listo, en breve el destinatario recibirá la notificación de que tiene disponible el dinero y que puede proceder a indicar la dirección a donde enviarlo.

3.2.3.2 COINBASE

Coinbase es una de las empresas más fuertes dentro del mundo Bitcoin y una de las que más inversión de capital riesgo ha recibido en estos últimos años. Con sede en San Francisco, fue fundada por **Brian Armstrong** en junio de 2012 y al igual que sucede con blockchain.info, no solamente dispone de servicio de billetera, sino que complementa su rango de productos con una API de programación y una plataforma de compra/venta de Bitcoines *online*.

El registro en Coinbase implica cumplimentar un par de campos más (nombre y apellidos además de la dirección de correo):

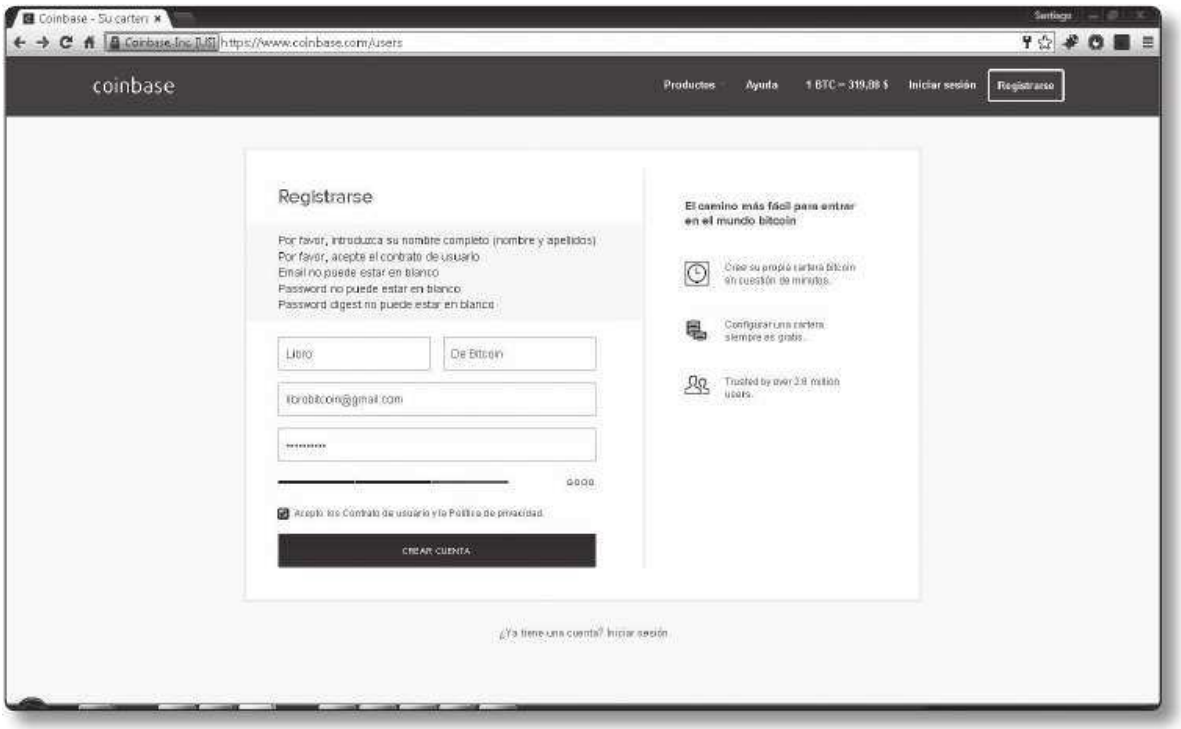


Figura 3.15. Registro en Coinbase

Seguidamente tendremos que verificar nuestra dirección de *email* haciendo uso del correo que deberíamos haber recibido en nuestra cuenta. Una vez que lo hagamos podremos entrar en la cuenta de Coinbase.

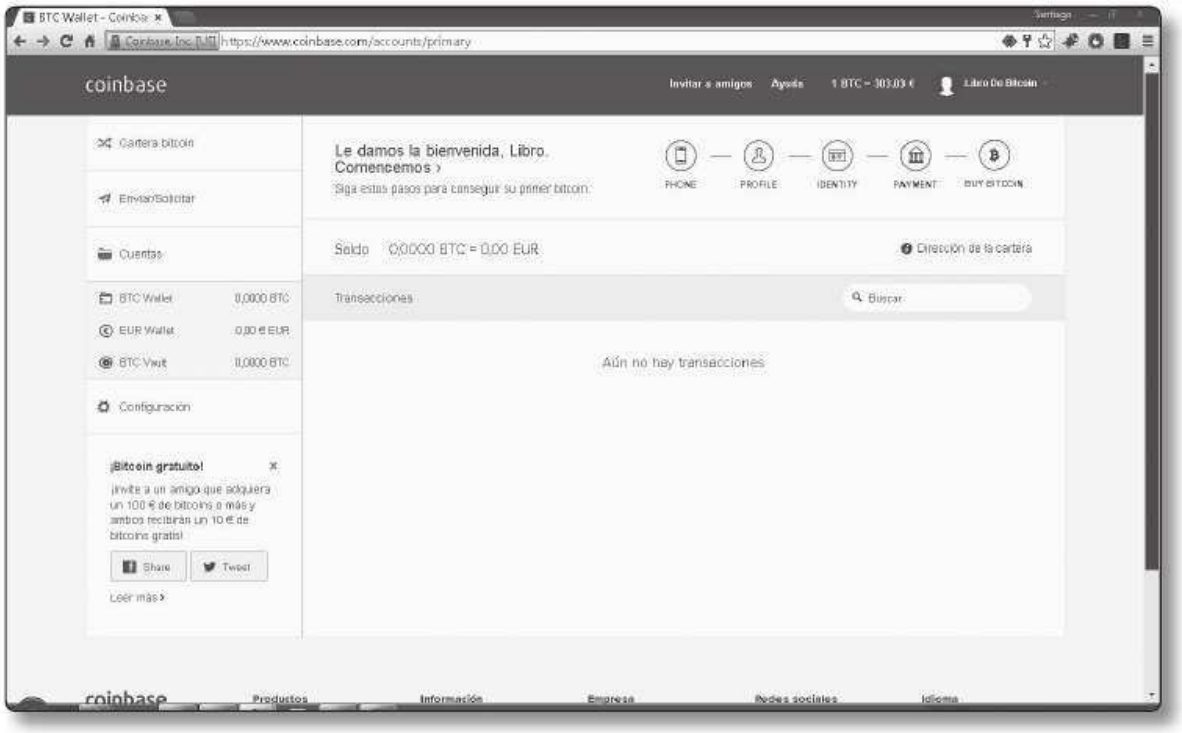


Figura 3.16. Pantalla de inicio de Coinbase

El acceso a la billetera web lo tenemos ubicado en el segundo enlace del menú de la izquierda **Enviar/Solicitar**. Coinbase provee una interfaz muy sencilla para realizar operaciones muy rápidamente.

ENTONCES…

Las operaciones para compra/venta de Bitcoines se hacen desde la opción **Cartera bitcoin**. Si es la primera vez que nos conectamos nos dirá que nuestra cuenta no está completa y que debemos añadir información adicional: nuestro país de residencia, teléfono móvil (si tenemos un código Authy nos lo pedirá también), nuestra dirección postal, código postal, fecha de nacimiento, etc. La inclusión de tanta información personal es algo común en las plataformas de *trading* y se hace siempre como requisito legal que estas empresas tienen por parte de las diferentes administraciones de los países donde operan para evitar el lavado de dinero.

Recibir dinero

Una vez pulsado sobre **Enviar/Solicitar** pulsamos en **Solicitar** y cumplimentamos la dirección de correo electrónico de la persona a la que solicitamos que nos envíe dinero y la cantidad. Podemos escribir un mensaje opcional que se le mostrará también al usuario.

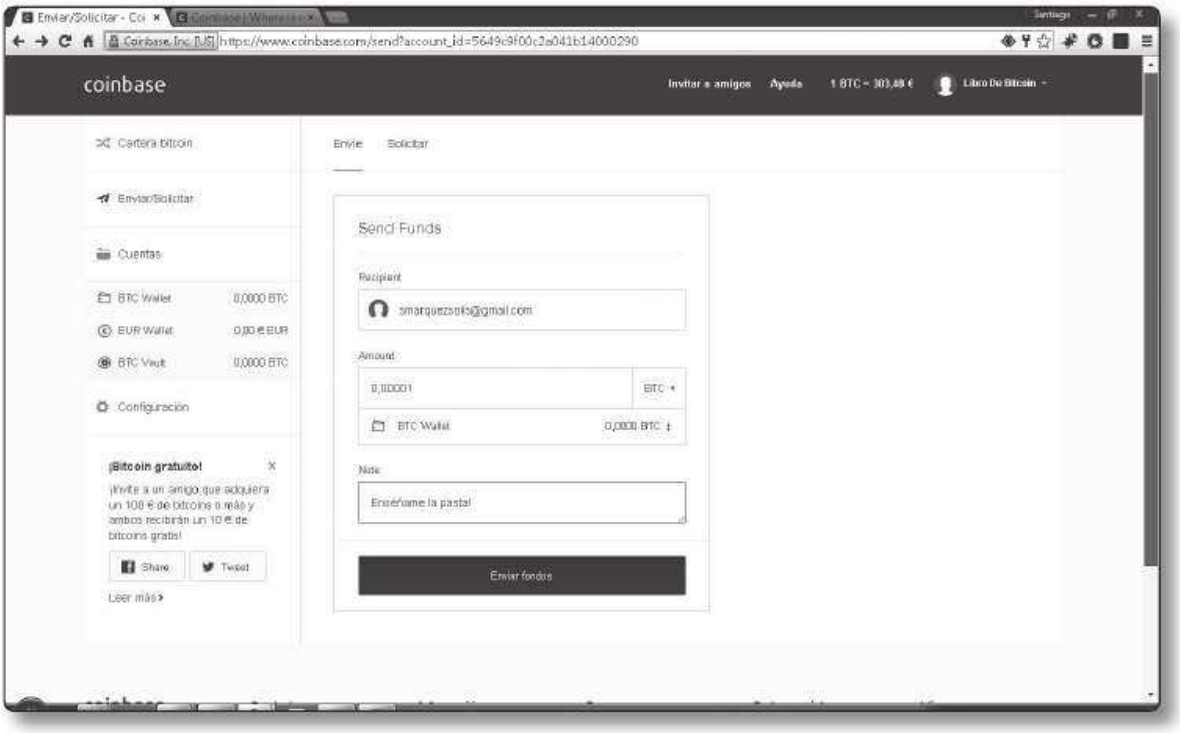


Figura 3.17. Recibir dinero en Coinbase

El destinatario del mensaje recibirá algo del estilo siguiente:

Figura 3.18. Mensaje de pago de Coinbase

Y al pulsar sobre **Haga clic aquí para completar este pago**, se le mostrará la página de pago con el código QR asociado a nuestra dirección pública. Si el usuario la escanea podrá hacernos el ingreso en nuestra cuenta y no tendrá que hacer nada más.

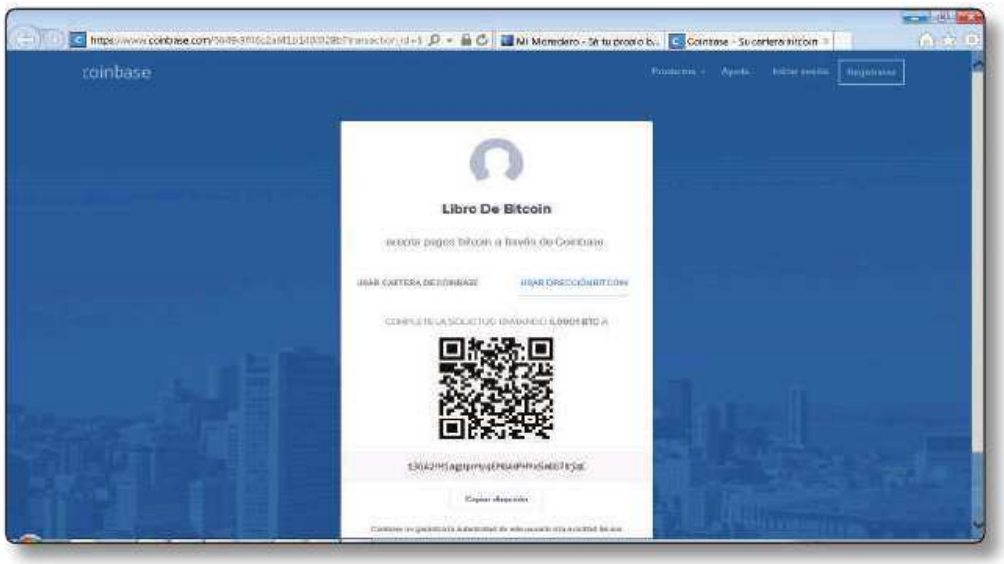


Figura 3.19. Completando la solicitud de dinero

Podremos ver nuestras solicitudes de efectivo nuevamente desde el menú de la izquierda, en **BTC Wallet**.

ENTONCES…

Coinbase permite tener fondos en nuestra cuenta en euros o dólares, es por eso que además de nuestra **BTC Wallet** disponemos de un **EUR Wallet** o **USD Wallet** (en función de nuestro país de residencia). Estas carteras adicionales son útiles para hacer operaciones de compra/venta de Bitcoines.

Fíjate que en Coinbase si queremos crear nuevas direcciones públicas, tendremos que cambiar nuestra perspectiva de navegación desde el menú que hay situado en la esquina superior derecha de la ventana.

Figura 3.20. Cambiando la perspectiva

Seleccionando la opción **Avanzado** tendremos acceso a muchas posibilidades más entre las que se encuentran la creación de direcciones adicionales, crear transacciones periódicas para enviar dinero cada cierto tiempo y acceder a los informes e historial de nuestra cuenta.

Mención especial a la opción Comercios, que nos permitiría abrir una cuenta de uso comercial donde podríamos recibir pagos en Bitcoines y convertirlos en moneda fíat de manera instantánea y recibirlos en nuestra cuenta bancaria tradicional en un par de días. De este modo Coinbase se convierte también en **pasarela de pagos**, al estilo de lo que puede ser PayPal. Aunque no es objeto de este libro, a modo de curiosidad indicaros que a los comercios no les cobra ninguna comisión hasta que hayan procesado su **primer millón de euros**, a partir de ahí, es del 1% para convertir Bitcoines en efectivo.

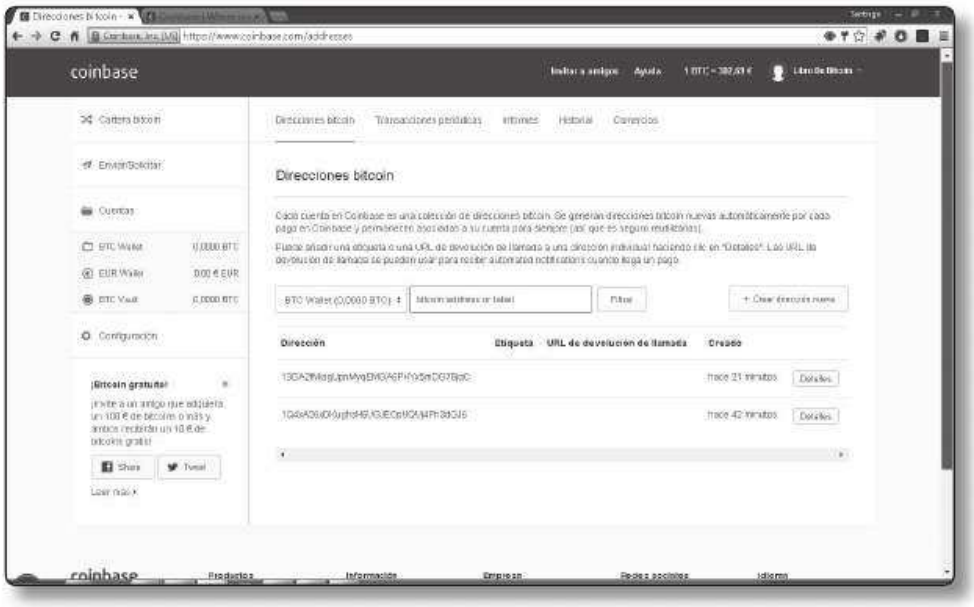


Figura 3.21. Opciones avanzadas en Coinbase

Enviar dinero

En el caso de que seamos nosotros los que deseemos enviar dinero, seleccionaremos la opción **Enviar/Solicitar** del menú de la izquierda y seguidamente marcaremos **Envíe** en la pantalla. Como el caso anterior es muy simple, introduciremos la dirección de correo electrónico o la dirección Bitcoin del destinatario, la cantidad que vamos a enviar y un mensaje adicional de ser necesario. Igual que antes el usuario recibirá una notificación para recuperar el dinero en su cuenta (en el caso de usar el correo electrónico como dirección de envío) o directamente el dinero en la dirección Bitcoin especificada.

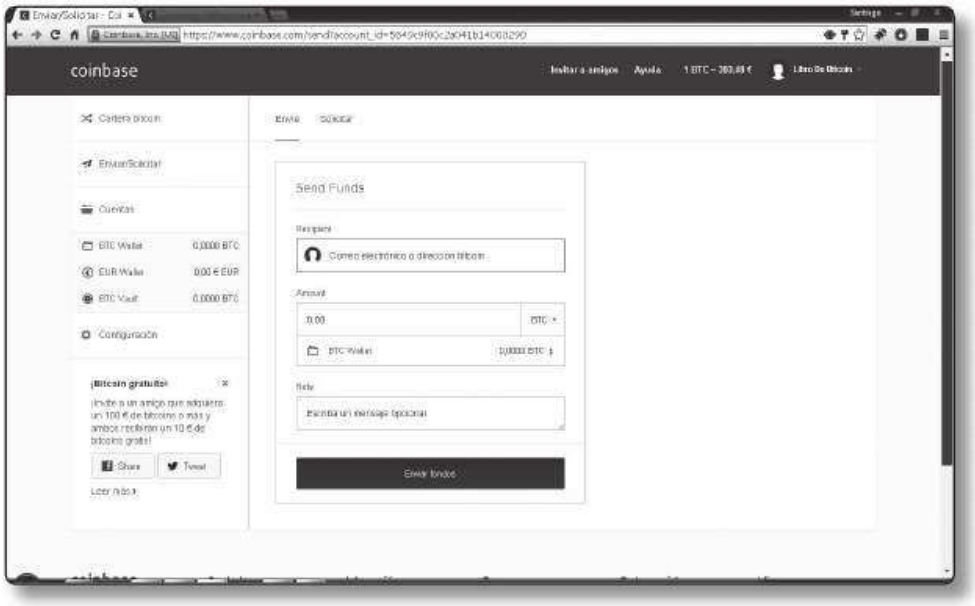


Figura 3.22. Enviando dinero con Coinbase

Configuración de la cuenta

Del mismo que blockchain.info, Coinbase provee un buen número de opciones para configurar la cuenta. Desde **Mi perfil** podremos cambiar nuestros datos básicos de identificación, nombre, dirección, imagen personal, etc.

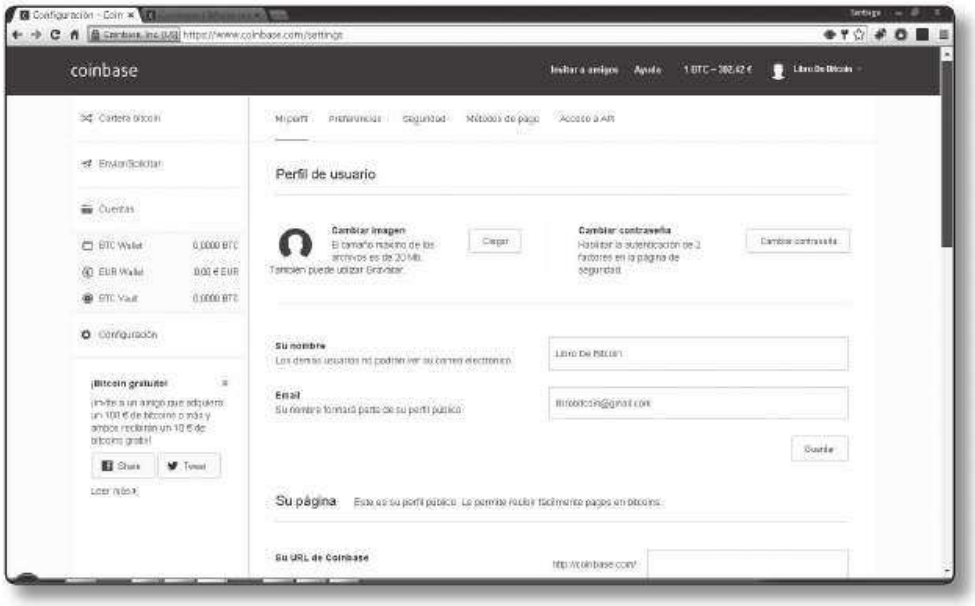


Figura 3.23. Configurando Coinbase

Más interesante es la sección **Preferencias** en donde se especifican nuestra moneda local, zona horaria o unidad Bitcoin preferida (solo admite Bitcoines o bits). También tenemos acceso a las notificaciones, que recomiendo dejar activadas todas ellas, para ser avisados en caso de cualquier circunstancia que suceda.

Desde **Seguridad** podremos realizar la gestión de los aspectos relacionados con la seguridad de la cuenta. Por defecto los códigos de verificación Coinbase solamente los solicita si las cantidades superan algo más de 1,5 BTC diarios, pero personalmente yo dejaría activa la opción más segura de **Cualquier cantidad de Bitcoin**. Una opción también muy recomendable es tener activada la seguridad con **Authy** para tener que introducir el código de validación en cualquier operación importante.

A los **Métodos de pago** solamente podremos sacarles el máximo provecho si hemos completado completamente el proceso de **Verificación de identidad**.

Figura 3.24. Verificación de identidad Coinbase

Verificar nuestra identidad significa que tendremos que dar a Coinbase una prueba de que nosotros somos realmente nosotros; esta prueba viene determinada por país, y puede ser alguna de estas tres: pasaporte, documento de identidad o carnet de conducir. En el caso de España, cualquiera de las tres es válida.

Para poder validar el documento, Coinbase nos pedirá permiso para conectar la cámara de nuestro ordenador, pondremos el documento delante de ella y haremos dos fotografías de la parte delantera y trasera del documento. Seguidamente se procederá a realizar la verificación del documento de manera automática; aseguraos de que la imagen tomada por la cámara es de calidad para que el proceso salga bien.

3.2.4 Billeteras "en la cabeza" y billeteras "de papel"

También reciben el nombre de **brainwallet** o **billetera o cartera mental**, y en este caso como su nombre sugiere, es un tipo de billetera *offline* que se encuentra (como bien sugiere su nombre) en nuestra cabeza. Este tipo de billetera se genera a partir de una contraseña que solamente el usuario conoce y que se utiliza para generar las direcciones públicas. *A priori* puede parecer un mecanismo muy seguro para generar una billetera, sin embargo depende de la capacidad del usuario para generar una contraseña segura (y recordarla) lo que limita su efectividad, porque a la larga puede ser necesario almacenarla en algún sitio si no queremos olvidarla.

Las **billeteras de papel** reciben este nombre porque el medio físico en el que están generalmente hechas es un trozo de papel pero realmente no tendría porqué serlo, cualquier soporte físico que sea capaz de almacenar una clave privada de una dirección podría servir para este propósito, no es extraño que puedan aparecer con la forma de una tarjeta de plástico y en vez de escribir los caracteres de la clave, se usa un código QR por sencillez y comodidad. Sea cual sea el formato físico que adopten, entran dentro de los tipos de almacenamiento en frío o *cold storage*, de los que ya hablamos.

Como este planeta está lleno de gente creativa, los diseños que adoptan las carteras en papel pueden ser de lo más variado, aunque los que se parecen a billetes a mí personalmente me parecen muy simpáticos, más que nada porque el respaldo que tiene este "billete" (*In Crypto we trust*, ¿recuerdas?) me parece mucho más serio del que tiene el dinero fíat y su confianza estatal.

Figura 3.25. Ejemplo de billetera de papel

Podemos generar una billetera en papel desde muchísimas herramientas, por ejemplo desde blockchain.info, si nos vamos a **Importar/Exportar** del menú principal, tenemos la opción **Monedero de papel**, que nos generará un PDF que podemos imprimir de nuestras direcciones. No obstante el diseño no está especialmente currado.

Otra posibilidad es usar la web **bitaddress.org**, un clásico más dentro del mundo Bitcoin y el manejo de carteras de papel que también nos permite crear una cartera mental (entre otras opciones). Tiene como característica adicional que podemos descargarnos el código completo de la página a nuestro disco duro y usarla de manera totalmente *offline* y sin necesidad de conectarnos a Internet, lo que mejora su seguridad.

Figura 3.26. Bitaddress.org

Lo primero que nos pide bitaddress.org es que movamos el ratón por la pantalla para generar un poco de entropía, podéis usar si os gusta más (u os parece más clara) la palabra caos o desorden, lo que se persigue es tener un poco de aleatoriedad en el proceso de generación de las claves, y eso se puede conseguir de un modo muy simple con el movimiento del ratón por la pantalla sin seguir ningún patrón específico (o introducir una secuencia de caracteres al azar por teclado). Iremos viendo que la pantalla se va llenando de puntitos de color verde hasta que se complete el porcentaje al 100%, en ese momento tendremos algo como lo siguiente:

Figura 3.27. Generando un poco de entropía

La cartera en papel podremos conseguirla si pulsamos en **Cartera en papel**, la página por defecto nos mostrará el diseño para tres "billetes" que pueden ser cargados con Bitcoines utilizando el código QR de **Load $ Verify** (dirección pública), o gastados usando el QR bajo **Spend** (dirección privada).

Figura 3.28. La billetera de papel lista para usar

Solamente nos queda imprimir nuestra cartera de papel y guardarla en algún lugar seguro. Una recomendación, tened cuidado si utilizáis una impresora que esté conectada en red (la del trabajo por ejemplo). Las impresoras tienen colas de impresión y memorias internas (*buffer*), y estas a veces pueden no quedar debidamente limpias o reseteadas, no sería el primer caso de una auditoría de seguridad que encuentra este tipo de información en la cola de impresión: la clave privada está ahí mismo, no hay nada que evite que esos Bitcoines puedan ser robados si la billetera ha sido previamente cargada.

La cartera mental solo requiere que introduzcamos una contraseña que nos resulte fácil de recordar y que sea a la vez segura, damos al botón **Ver** y listo, tenemos una dirección pública y privada que podremos utilizar.

Figura 3.29. Ejemplo de cartera mental

3.2.5 Billeteras multifirma

Llegamos al último tipo de billetera que nos queda por analizar en este apasionante viaje por las billeteras digitales Bitcoin. Las billeteras multifirma o **multi sig** (**multiple signature**) son un tipo de billetera en donde para acceder al dinero que hay depositado dentro de una dirección pública, se necesita del acceso de

al menos dos o más claves privadas. Las direcciones Bitcoin estándar comienzan con el **número 1** mientras que aquellas que son multifirma comienzan con el **número 3**.

Sabemos que la seguridad es uno de los principales pilares de Bitcoin, sin embargo, tener una única clave para acceder a los fondos puede suponer un problema en el caso de que el lugar donde esta clave privada esté guardada sufra algún daño; ¿qué sucede si mi ordenador se estropea?, ¿o mi almacenamiento en frío sufre algún daño? De igual modo, pongámonos en el caso de una empresa que desee operar con Bitcoines, ¿quién debería ser la persona que tenga la responsabilidad de guardar la clave privada de una dirección donde estén almacenados los fondos de la empresa?, ¿el director financiero?, ¿el CEO? Pero no nos tenemos que ir a una empresa, qué pasa si tengo una cantidad puesta en una dirección que es el aporte de un grupo de amigos para irse de viaje comprando el billete en Destinia, ¿quién se encarga de guardar la clave? Los ejemplos de situaciones similares son múltiples en el momento que tenemos que garantizar una custodia compartida de unos fondos determinados.

Fue a partir de 2012 que Bitcoin comenzó a soportar la operativa multifirma en su protocolo, las direcciones del **tipo P2SH**. Este tipo de direcciones soportan cualquier número de claves privadas para desbloquear el dinero. Se les suele llamar también del **tipo M de N**, porque pueden soportar N claves privadas pero solamente M son necesarias para el acceso al dinero; por ejemplo tengo 5 claves privadas sobre la dirección X, pero con que se aporten 3 de las 5, el dinero quedaría liberado, en este caso se describiría como 3 de 5. Dicho de otro modo, utilizar la multifirma introduce dentro de Bitcoin un mecanismo para implementar redundancia que garantiza que puntos únicos de fallo, como los descritos anteriormente, puedan ser controlados y reducidos a su mínima expresión.

Gracias a las posibilidades de la multifirma, puedo tener varias claves privadas diferentes, almacenadas en lugares diferentes y por ende, seguir accediendo a mi dinero siempre y cuando conserve al menos el mínimo número de claves definido para acceder.

Algunas carteras que soportan la posibilidad multifirma son Electrum, Armory o Coinbase. Dado que de las otras dos aplicaciones hablaremos un poco más adelante fijémonos en cómo lo hace Coinbase porque aporta un sistema que es muy sencillo de utilizar para el usuario.

Lo primero que hay que hacer para configurar la billetera como multifirma es irnos a la página: *www.coinbase.com/multisig* y seleccionar que queremos **crear una nueva caja fuerte**:

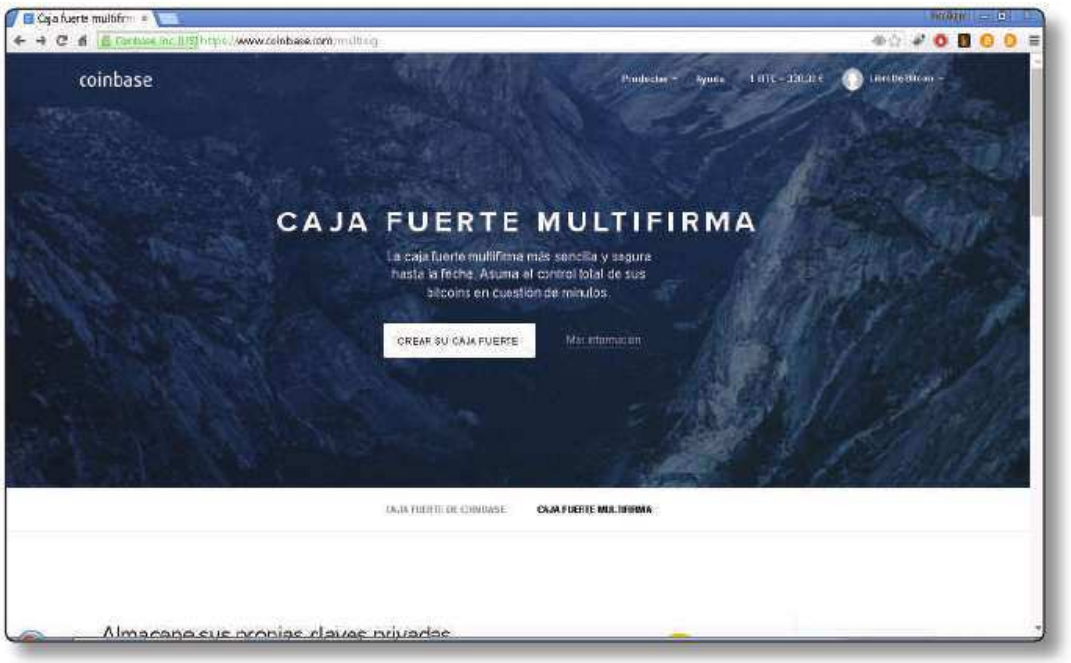


Figura 3.30. Billetera multifirma en Coinbase

Si no estamos "logados" en Coinbase nos pedirá primero que lo hagamos, y seremos redirigidos a la página siguiente, un pequeño asistente de configuración que es muy intuitivo de seguir y entender. El primer paso es ponerle nombre a nuestra nueva caja fuerte multifirma, en el ejemplo usamos "Caja Fuerte Libro Bitcoin":

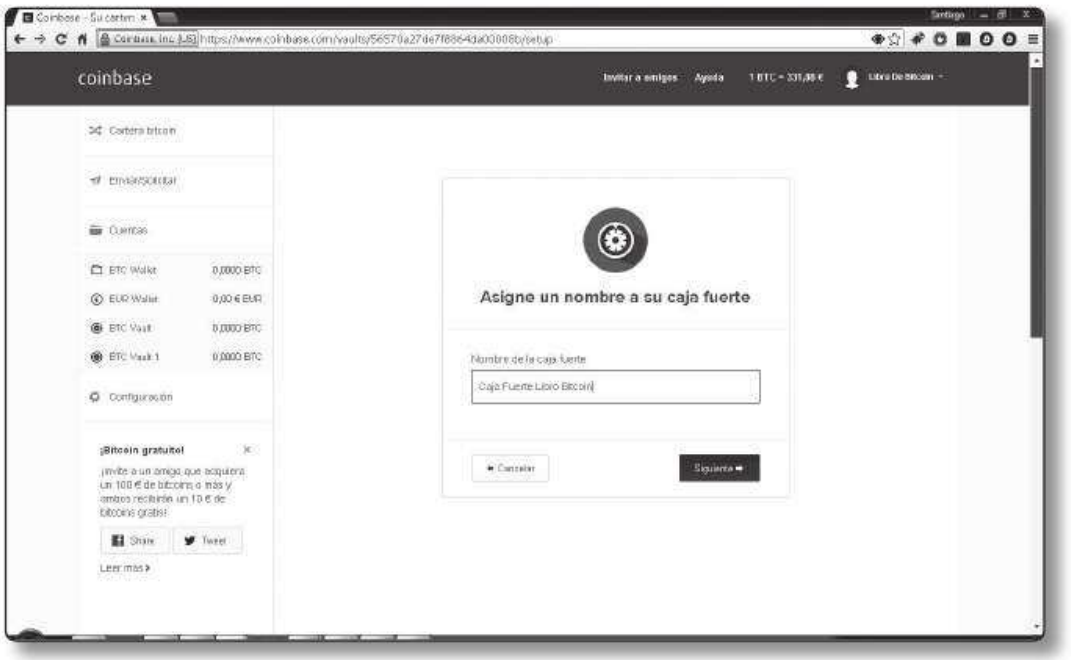


Figura 3.31. Creación de una caja fuerte

Lo siguiente es decir quién es el que podrá aprobar las retiradas de dinero, en el ejemplo he indicado que el responsable de esta aprobación seré yo, pero podría añadir a más personas si quisiera.

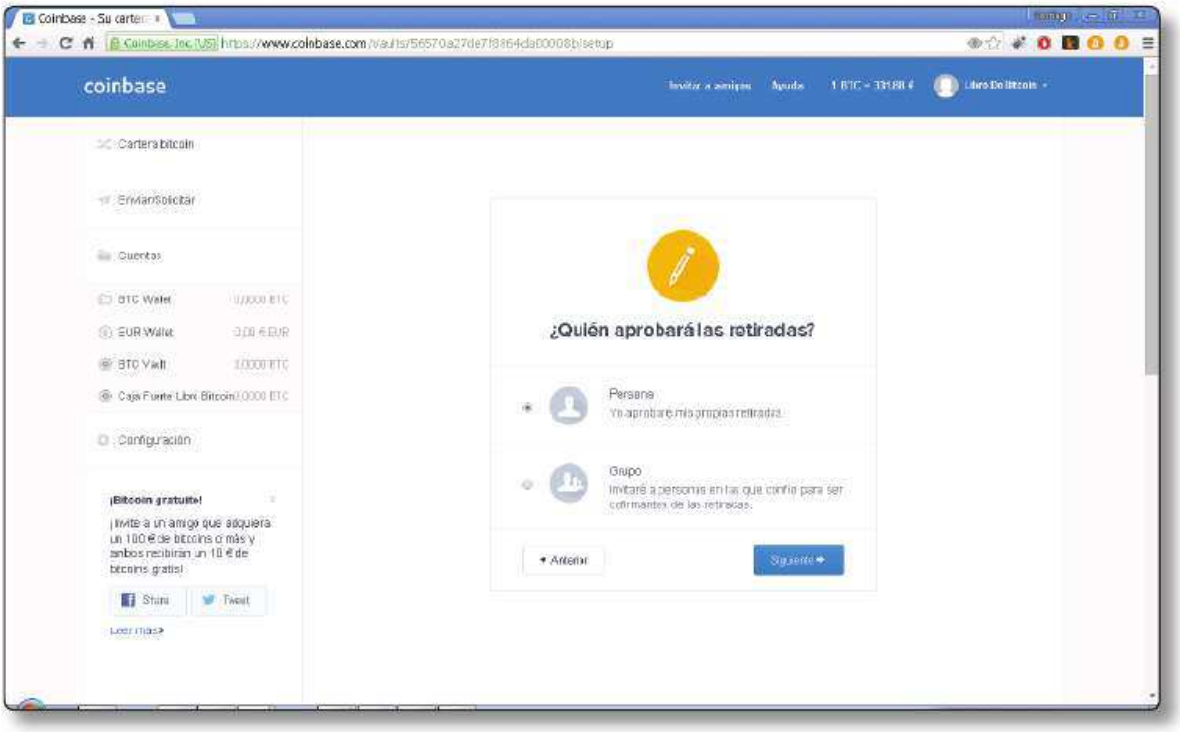


Figura 3.32. Aprobación de las retiradas

Hecho esto, debemos indicar cómo deseamos que se gestione la seguridad de la billetera. Por defecto es Coinbase quien se encarga de gestionar las claves privadas, pero nos da la posibilidad de que seamos nosotros quienes hagamos este proceso. Lo más cómodo es la primera opción, así cada vez que se produzca un movimiento de fondos se nos pedirá una confirmación por correo electrónico; incluye una salvaguarda de 48 horas en donde podremos dar marcha atrás a las operaciones efectuadas.

Queda muy poco para tener lista nuestra caja fuerte. El paso siguiente es determinar las direcciones de correo electrónico de los autorizadores de las operaciones, esta opción depende de que hayáis indicado que sea Coinbase el encargado de la seguridad. En el ejemplo he indicado que solamente *smarquezsolis@gmail.com* y *librobitcoin@gmail.com* puedan hacerlo:

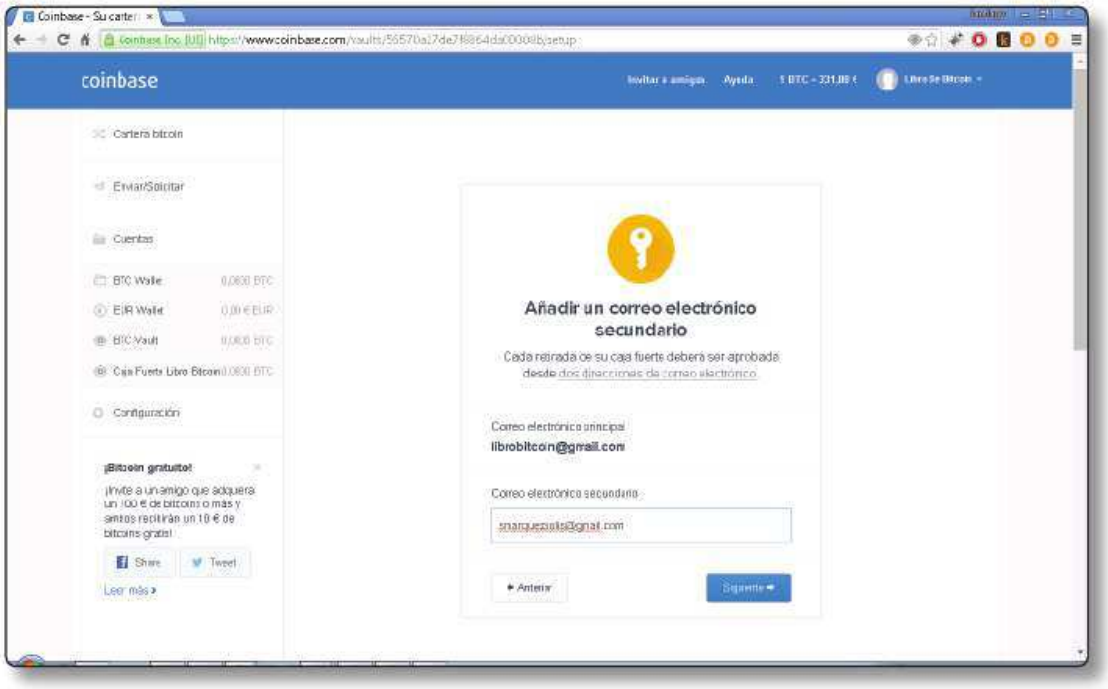


Figura 3.33. Autorizadores de retirada

Ahora al pulsar en **Siguiente** deberíamos recibir un correo para que Coinbase pueda confirmar la dirección como válida y quedará a la espera de que realicemos este último paso:

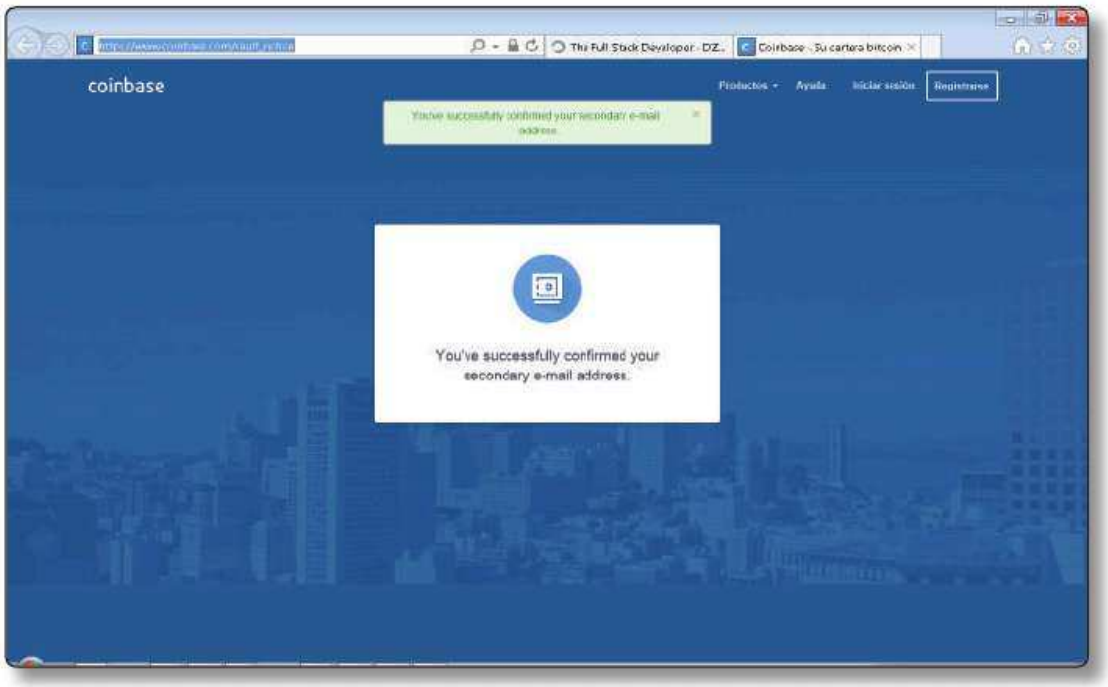


Figura 3.34. Esperando confirmación

Casi hemos acabado, aprobaremos los cambios introducidos, y comprobaremos que todo es correcto, las notificaciones, los autorizadores y el período de retraso que por defecto son 48 horas, más que suficiente para hacer correcciones:

Figura 3.35. Finalizando la configuración

Fin del proceso; confirmados los cambios anteriores desde la consola de Coinbase veremos que se nos ha creado a la izquierda una nueva carpeta con el nombre que dimos a la caja fuerte. Podremos usarla como si fuera una cartera normal salvo que tendremos que autorizar desde nuestros dos correos los movimientos de efectivo.

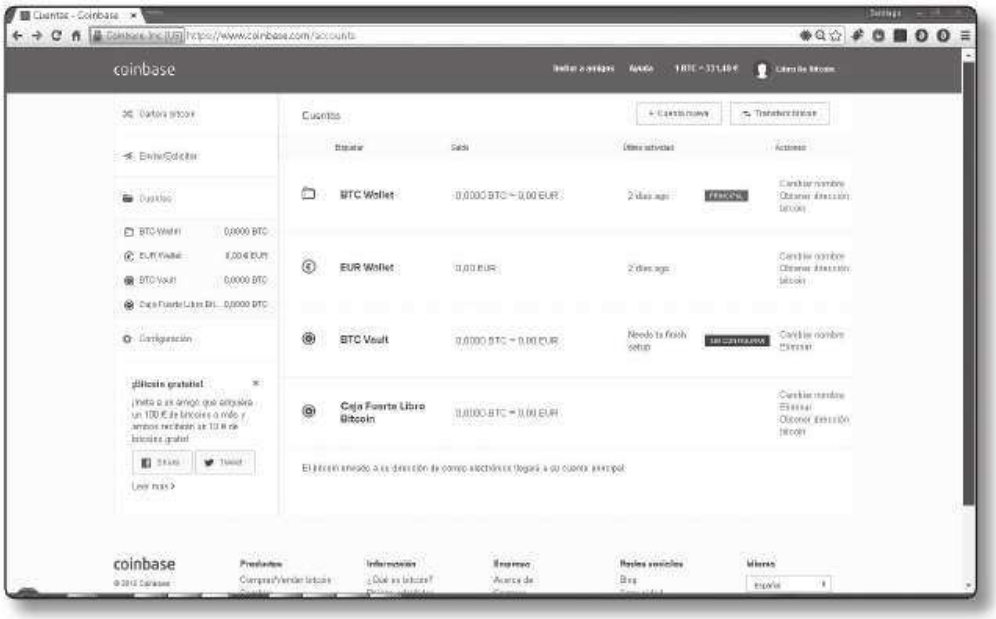


Figura 3.36. Caja fuerte creada completamente

3.3 INSTALACIÓN Y CONFIGURACIÓN CLÁSICAS DE ESCRITORIO

Una vez que tenemos claros los tipos de billeteras con los que nos podemos encontrar, y hemos visto ejemplos de cada una de ellas y explicado su funcionamiento básico, vamos a suponer que no queremos ningún tipo de intermediario entre nuestro dinero y nosotros y que ninguna de las soluciones anteriormente propuestas nos gusta. En este caso, lo mejor sería utilizar alguno de los múltiples clientes de escritorio existentes.

Dado que las posibilidades son cada vez más variadas, y para gustos los colores, he decidido quedarme con las tres más populares y os redirijo a la página del proyecto Bitcoin como lugar de paso obligado a la hora de elegir una billetera. Y es que desde allí vamos a obtener una rápida guía visual que nos aconseja sobre las mejores soluciones disponibles, para móvil (Android, iOS, Windows Phone y BlackBerry), escritorio (Windows, Mac y Linux), hardware y web, lo que cubre el total del espectro que hemos explicado anteriormente.

Figura 3.37. Página principal de Bitcoin Core

Como el espacio que tenemos es muy limitado, y dado que la plataforma más extendida es **Windows**, centraré las explicaciones siguientes en este sistema operativo, aunque los poseedores de un Mac o una distro de Ubuntu observarán que el comportamiento de los programas, una vez instalados, es exactamente el mismo

que lo que describimos para la versión Windows. El único requisito que necesitamos en nuestras máquinas es disponer de suficiente espacio en el disco duro (y solo en el caso de Bitcoin Core este particular es suficientemente importante) para descargar el software; poco más, la gran mayoría de los ordenadores actuales vienen con memoria RAM, procesador y tarjeta gráfica con capacidades suficientes para los objetivos que perseguimos en este libro.

3.3.1 Bitcoin Core

Bitcoin Core es la implementación del cliente completo de Bitcoin y se considera como la columna vertebral de la red Bitcoin (de hecho así se define en la web); el trabajo de los desarrolladores de Bitcoin se ve reflejado en este software, que aunque ofrece unos niveles muy altos de seguridad, privacidad y estabilidad, presenta menos prestaciones que otras opciones (paradójicamente), además de ocupar mucho espacio y memoria. Bitcoin Core es software de código abierto, no podría ser de otra manera, y del tipo **determinista** que explicamos antes.

Hay que tener en cuenta que cuando elegimos esta opción, estamos eligiendo convertirnos en un nodo completo de la red Bitcoin, es decir, tendremos que descargarnos en nuestra máquina toda la cadena de bloques (actualmente algo más de 40 GB, cantidad que crece cada día con el trabajo de todos los que usan Bitcoin). El ser un nodo completo significa que validaremos y retrasmitiremos las transacciones a la red, algo que tiene también una gran importancia cuando de verificar transacciones se refiere; en el momento de verificar los pagos será nuestro propio software el que se encargue de realizarlo al estar sincronizado con el resto de la red Bitcoin, por lo que se realizarán más rápidamente. Fijaos en la diferencia de un cliente que se ejecute en un terminal móvil, es absurdo pensar que en un teléfono o tableta va a descargarse toda la cadena de bloques, por tanto, la verificación de las transacciones en este caso dependerá del resto de nodos de la red y del tiempo que esta tarde en realizarlas y propagarlas.

ENTONCES…

Yo diría incluso más, la cadena de bloques crece aproximadamente a una velocidad de 1 GB al mes, en poco tiempo (ahora son más de 40 GB), llegará un momento en que ocupará cientos de gigas o *terabytes*, e igual el almacenamiento de la misma puede que no interese tampoco en ordenadores domésticos. Este es otro tema que suscita debates muy interesantes. ¿Acabará la cadena de bloques solo en unas determinadas máquinas con suficiente tamaño de disco?

Con Bitcoin Core también tenemos el control total de nuestros Bitcoines, al no residir en una billetera controlada por terceros, estos no podrán congelar o perder tu dinero, salvo que lo pierdas tú mismo claro, algo que no es raro que pueda llegar a sucederte si no tomas las precauciones debidas. Para ayudar a garantizar la **anonimidad de nuestra IP** y evitar que se puedan asociar los pagos realizados con esta, permite su configuración con la aplicación Tor, una posibilidad muy interesante.

Para poder utilizar Bitcoin Core tenemos que seguir los pasos que se enuncian a continuación:

1. **Obtención del software**

   Nada más fácil, desde la web de bitcoin.org podemos obtener tanto un instalable para nuestra máquina como un fichero zip para descomprimir (Windows, Linux o Mac). Actualmente la última versión disponible es la **0.11.0**, algo que no debería dejar de sorprendernos, **¡Bitcoin aún no está en su versión 1!**

2. **Instalación**

   También muy sencilla. En caso de decidirnos por el asistente, la única información que tendremos que proporcionar es la ubicación donde queremos que el software se ejecute.

Figura 3.38. Eligiendo la ruta para Bitcoin Core

   Al finalizar el asistente de instalación, se nos preguntará por la ubicación en donde deseamos que se almacenen los datos de la cadena de bloques. Por defecto la ruta estándar es nuestro directorio de trabajo de usuario: **C:\Users\<<NombreUsuario>>\AppData\Roaming\Bitcoin**, pero podemos seleccionar la ubicación que nos resulte más conveniente:

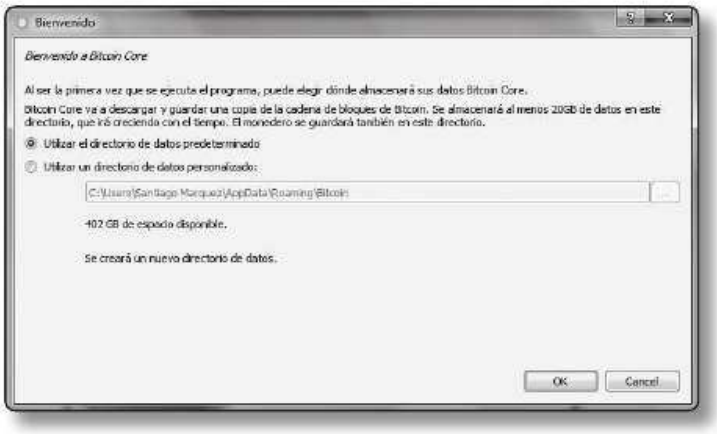


Figura 3.39. Eligiendo la ubicación de la blockchain

Hecho esto, Bitcoin Core comenzará a sincronizarse con la red, a cargar el índice de bloques y a verificar que son correctos. Este proceso puede llegar a tardar varios días, y es que el tamaño de la cadena de bloques en estos momentos es de algo más de 30 GB de datos, tamaño que cada día crece a medida que se hace uso de la red Bitcoin. Siempre que cerremos Bitcoin Core y lo volvamos a abrir, realizará el proceso anteriormente descrito, y podremos ver cómo va en la barra de estado inferior:

Figura 3.40. Sincronizando con la red

Sea como fuere, el aspecto que presenta el programa una vez que se encuentra operativo es el siguiente:

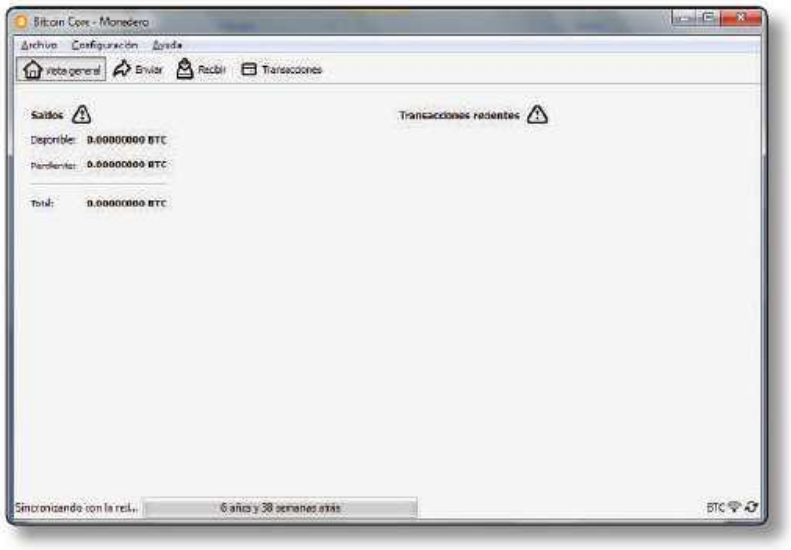


Figura 3.41. Aspecto de Bitcoin Core

Bitcoin Core dispone de dos botones en la parte superior para enviar o recibir dinero. Miremos primeramente la opción **Enviar**. Las opciones que presenta son similares a las que hemos visto en billeteras anteriores (pueden usarse direcciones previamente utilizadas), aunque aquí hay un especial énfasis en el apartado dedicado a las comisiones. Hay varias posibilidades que van desde enviar la transacción si es posible sin comisión, aunque esto puede llevar parejo un mayor tiempo de confirmación porque los mineros pueden tardar más tiempo en meterla dentro de un bloque; hasta la opción **Recomendado** que establece el valor de la comisión según si queremos un tiempo menor de confirmación (que va desde 25 confirmaciones a 0,00002674 BTC/KB a 1 confirmación a 0,00177760 BTC/KB), en ambos casos, las tasas son muy inferiores de lo que supondría un envío tradicional de dinero.

La opción de **Recibir** tampoco tiene demasiado misterio, hay varios campos opcionales para completar, **Etiqueta**, **Mensaje** y **Cantidad** son bastante autoexplicativas, y sirven para incluir una etiqueta que sirva para identificar nuestra operación y un mensaje más descriptivo, junto con la cantidad que solicitamos. Como información adicional, en la parte inferior tenemos el historial de pagos solicitados.

Si recordáis, hablamos antes de la posibilidad de firmar mensajes y verificarlos; desde Bitcoin Core es posible hacerlo también, en el menú **Archivo** están las opciones **Firmar mensaje** y **Verificar mensaje** para hacerlo.

Figura 3.42. Firmando mensajes con Bitcoin Core

Mención especial tiene la opción **Cifrar monedero** dentro de **Configuración**; ni que decir tiene que es más que recomendable que cifremos nuestro monedero, de este modo las claves privadas de nuestras direcciones públicas estarán protegidas de miradas indiscretas. Hecho lo cual y hasta aquí no hay muchas diferencias ni

novedades de lo estudiado en anteriores apartados, salvo que nos vayamos a la opción **Ayuda**, aquí hay algunos aspectos más novedosos que debemos conocer, la **Ventana de depuración** y las **Opciones de la línea de comandos**.

Comencemos con **Opciones de la línea de comandos**; es un cuadro de diálogo en donde se nos recuerdan los diferentes tipos de opciones que pueden utilizarse para configurar Bitcoin Core y que tienen mucho que ver con la **Ventana de depuración**. Las opciones que se configuran van desde la conexión, al monedero, las opciones de depuración/pruebas, los nodos de retransmisión, opciones para la creación de bloques, etc.

La **Ventana de depuración** es una utilidad muy importante, Bitcoin Core viene "de serie" con una consola RPC que permite realizar operaciones sobre la cadena de bloques utilizando una serie de comandos reconocidos por esta.

ENTONCES…

Un RPC o *Remote Procedure Call* o Llamada a Procedimiento Remoto sirve para invocar código de una máquina desde otra sin tener que preocuparnos por las comunicaciones, algo que siempre había de lo que estar preocupándose con la comunicación basada en *sockets* en donde los aspectos de comunicación había que tenerlos también presentes en el código. Los datos devueltos por la llamada son JSON o *JavaScript Object Notation*, que es un mecanismo de intercambio de datos que se ha popularizado muchísimo, es más simple que XML y más entendible por las personas.

Estos comandos son de diversa índole y están relacionados con las opciones que acabo de comentaros que pueden verse desde **Opciones de la línea de comandos**; la salida siempre es en formato JSON. Por ejemplo, veamos cómo funcionan algunos de estos comandos:

- Limpiar la pantalla: a medida que vayamos introduciendo comandos en la consola puede ser necesario limpiar los resultados, para ello usamos la secuencia de teclado **Ctrl + L**.
- Obtención de ayuda: el comando "help [comando]" nos dice cómo funciona la orden introducida. Por ejemplo, "help getinfo" nos devuelve información sobre el comando "getinfo". Si dejamos "help" sin parámetros nos devuelve la lista de comandos disponibles.
- Obtención de información varia de estado: usaremos el comando "getinfo" para ver, por ejemplo, balance, versión, protocolo de la billetera, bloques, dificultad, si estamos usando la red de prueba o no…

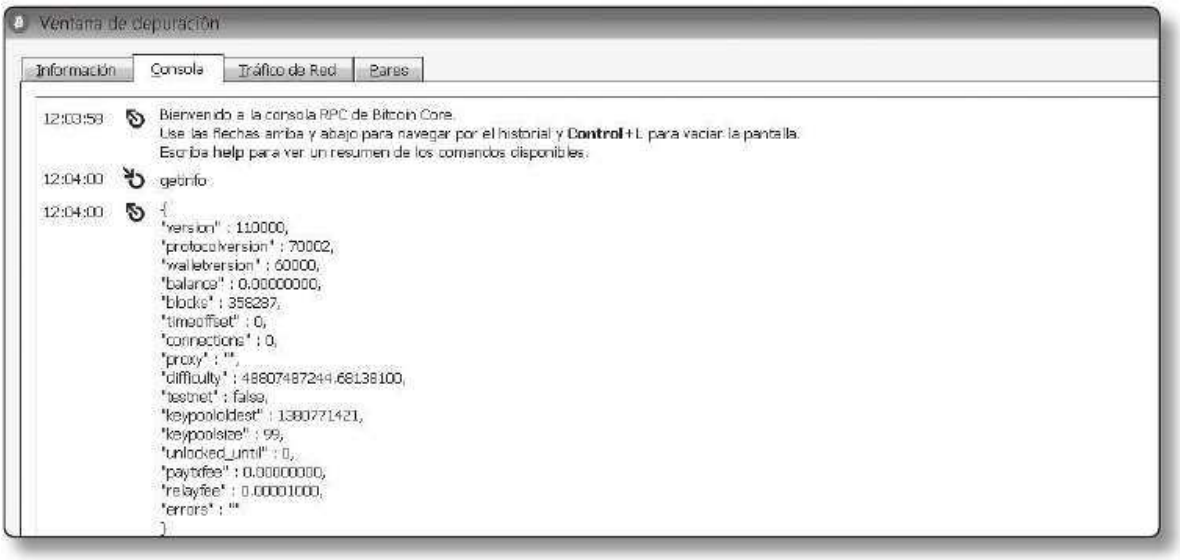


Figura 3.43. Consola Bitcoin Core

- Obtención de información de la billetera: usaremos el comando "getwalletinfo", entre otros, para ver saldo de la billetera, balance sin confirmar, contador de transacciones…

- **Desencriptar la billetera**. Algunas operaciones requieren que previamente introduzcamos la clave de desencriptado de nuestra billetera para poder ejecutar comandos posteriores, para hacer esto podemos usar el comando "walletpassphase [miclave] [tiempo en segundos]"; por ejemplo "walletpassphase "123456" 60" desbloquea mi billetera durante 60 segundos, suponiendo que mi clave sea "123456".

- **Importar una clave privada**. Antes explicaba las direcciones de vanidad y veíamos cómo generar una clave privada; supongamos que deseamos importarla a nuestra billetera, usaríamos el comando "importprivkey [claveprivada]". Suponiendo que mi clave privada sea 5HqnaEu51mpYXXGnr7BfBiYCBZdp67tvj5MSWLGNEscRB1oh3jq, importar en la billetera sería con el comando "importprivkey "5HqnaEu51mpYXXGnr7BfBiYCBZdp67tvj5MSWLGNEscRB1oh3jq". Este proceso tarda un rato en hacerse.

Dado que la lista de comandos disponible es muy extensa, lo mejor es hacer uso de la **Ayuda** de **Opciones de la línea de comandos** o del comando "help" y juguetear un poco hasta familiarizarse con ellos, sin embargo, esto sale fuera del alcance de este libro y me basta con que hayáis entendido los ejemplos anteriores, el resto del camino podéis seguir investigándolo sin mayores problemas por vuestra cuenta.

Los programas bitcoind y bitcoin-cli

Junto con la instalación de Bitcoin Core vienen dos utilidades que acompañan al programa principal; son bitcoind y bitcoin-cli, ambas se encuentran dentro de la carpeta "daemon" que encontraréis desde la ruta raíz de instalación del programa.

Bitcoind es un programa que implementa el protocolo de Bitcoin para utilizarlo desde la línea de comandos. Originalmente se podía utilizar como servidor/cliente RPC, aunque a partir de la versión 0.9 se creó otro programa, **bitcoin-cli**, para asumir las funciones de cliente, eliminando esta funcionalidad de bitcoind. Como bitcoind fue el primer cliente de Bitcoin que se creó, se le da el nombre habitualmente de "cliente de Satoshi" y se considera la implementación de referencia para cualquier otro cliente. La interfaz de usuario de bitcoind es proporcionada por Bitcoin-QT que es la que hemos estado utilizando en los ejemplos anteriores.

La versión con interfaz gráfica es compatible completamente con bitcoind, admiten los mismos argumentos, leen el mismo archivo de configuración y escriben en los mismos ficheros, por lo que solamente puede estar en ejecución uno de los dos programas simultáneamente. Por defecto, bitcoind utiliza como archivo de configuración el fichero "bitcoin.conf" pero puede cambiarse con el parámetro "-conf=fichero"; el resto de parámetros que admite son los siguientes:

Modificador	Significado
conf=<archivo>	Especificar el archivo de configuración (por defecto: bitcoin.conf)
pid=<archivo>	Especificar el archivo pid (por defecto: bitcoind.pid)
gen	Generar Bitcoines
gen=0	No generar Bitcoines
min	Iniciarse minimizado
datadir=<dir>	Especificar directorio de datos
timeout=<n>	Especificar tiempo límite de conexión (en milisegundos)
proxy=<ip:puerto>	Conectar a través de proxy socks4
dns	Permitir la búsqueda de DNS para addnode y connect
port=<puerto>	Estar a la escucha de conexiones en <puerto> (por defecto: 8333 o testnet 18333)
maxconnections=<n>	Mantener como máximo <n> conexiones con pares (por defecto: 125)
addnode=<ip>	Añadir un nodo al que conectarse
connect=<ip>	Conectarse solo al nodo especificado
nolisten	No aceptar conexiones desde el exterior
nodnsseed	No iniciar la lista de pares mediante DNS
banscore=<n>	Umbral para la desconexión de pares con mal comportamiento (por defecto: 100)

bantime=<n>	Número de segundos en el que evitar la reconexión de pares con mal comportamiento (por defecto: 86400)
maxreceivebuffer=<n>	*Buffer* de datos de recepción máximo por conexión, <n>*1000 *bytes* (por defecto: 10000)
maxsendbuffer=<n>	*Buffer* de envío máximo por conexión, <n>*1000 *bytes* (por defecto: 10000)
noupnp	No intentar el uso de UPnP para mapear el puerto de escucha
paytxfee=<amt>	Comisión por KB que se ha de añadir a las transacciones enviadas
daemon	Ejecutar en segundo plano como daemon y aceptar comandos
testnet	Utilizar la red de pruebas testnet (Bitcoines no reales)
debug	Mostrar información de depuración adicional
logtimestamps	Incluir una marca de tiempo (*timestamp*) con la información de depuración
printtoconsole	Enviar la información de trazas/depuración a la consola en lugar de al archivo debug.log
rpcuser=<user>	Nombre de usuario para las conexiones JSON RPC
rpcpassword=<pw>	Contraseña para las conexiones JSONRPC
rpcport=<puerto>	Estar a la escucha de conexiones JSON RPC en <puerto> (por defecto: 8332)
	rpcallowip=<ip> Permitir las conexiones JSON RPC desde la dirección IP especificada
rpcconnect=<ip>	Enviar los comandos al nodo que se ejecuta en la <ip> (por defecto: 127.0.0.1)
keypool=<n>	Establecer el tamaño de la reserva de claves (*key pool*) en <n> (por defecto: 100)
rescan	Volver a explorar la cadena de bloques para detectar las transacciones que afectan a la cartera local

3.3.2 Electrum

Es una billetera del tipo determinista, ligera, por tanto no guarda la cadena de bloques en local como hace Bitcoin Core. Probablemente, de todas las opciones disponibles es la que menos recursos de máquina consume y está entre las favoritas de muchos entusiastas de Bitcoin. Para descargarla nos vamos a la web de Electrum en *www.electrum.org* y en la sección Download elegimos la versión que se ajuste a nuestra plataforma.

Como ejemplo elegimos la versión Windows en su versión instalable (la opción portable es una buena elección también si queremos llevarla a una llave USB y crearnos un almacenamiento en frío por nuestra cuenta, aunque Electrum también permite la

conexión con hardware especializado como Trezor o Ledger que os conté antes). El proceso de instalación es simple, y solamente hay que marcar la ruta de instalación.

Una vez instalado en nuestra máquina, nos dirigimos a la unidad de disco y ejecutamos el programa "electrum.exe" o el acceso directo que se nos crea en Windows, que nos muestra las opciones siguientes:

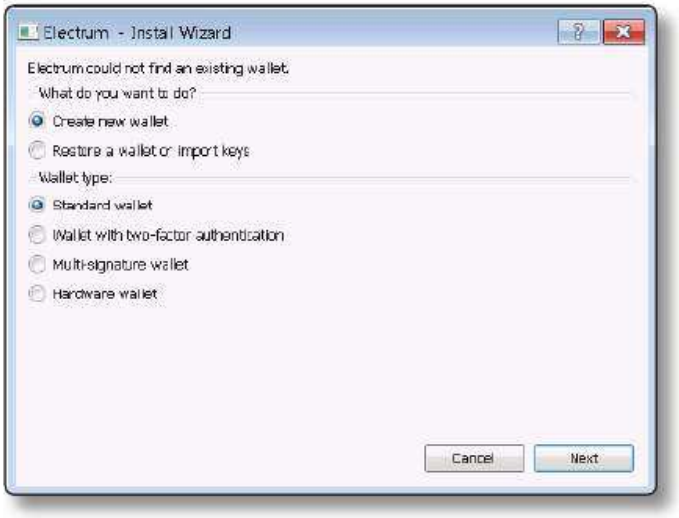


Figura 3.44. Tipos de billeteras en Electrum

Independientemente del tipo de billetera que vayamos a crear con estas opciones, Electrum parte de un conjunto de 13 palabras (no repetidas) que utiliza como semilla y que sirven para restaurar la cartera en caso de ser necesario (imaginemos que por error se formatea o daña el ordenador; vimos que este conjunto de palabras son una salvaguarda importante).

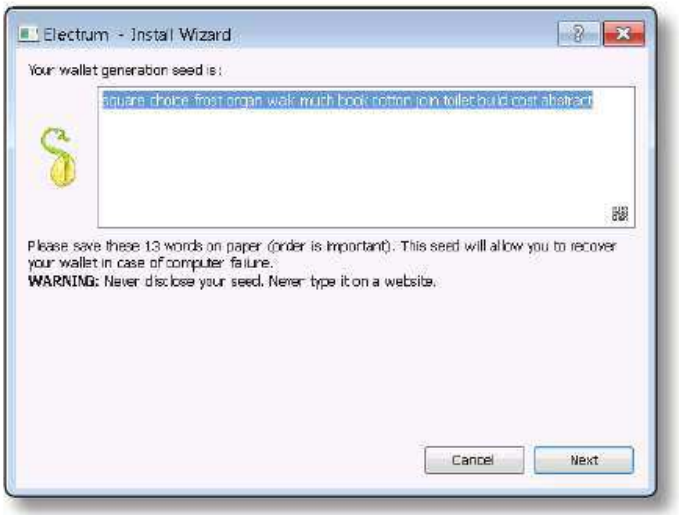


Figura 3.45. Lista de palabras de recuerdo

Esta lista se obtiene de otra lista de 2.048 palabras, y el orden en el que aparecen es muy importante, y no puede ser alterado si queremos, llegado el caso, poder recuperar la cartera. Es por esto que se recomienda apuntarlas y guardarlas (o memorizarlas). Como nivel de seguridad adicional, Electrum solicita una contraseña que utilizará para encriptar las claves de nuestra billetera y aunque da la posibilidad de dejarlas en blanco, lo que deshabilita la encriptación, no lo recomendaría ni siquiera cuando estemos haciendo pruebas. La seguridad es una cuestión de costumbre, y por regla general solemos olvidarla en el mundo informático; si no queremos llevarnos algún susto, conviene usarla siempre.

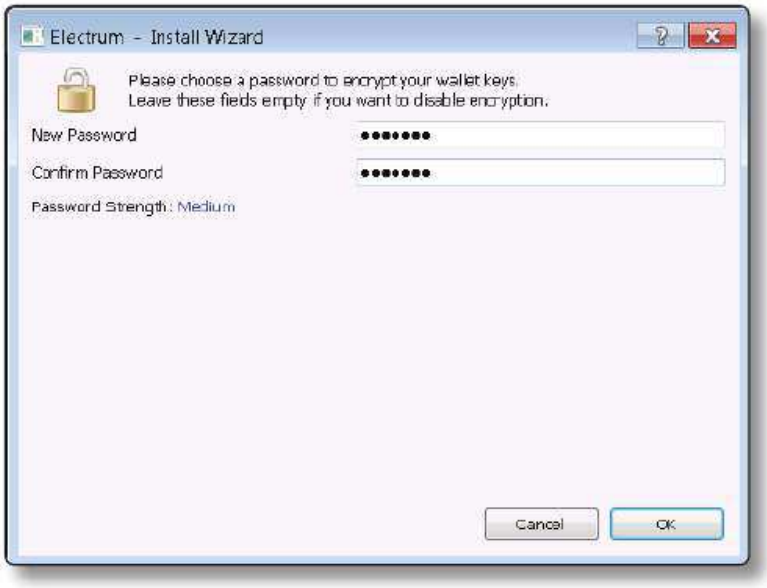


Figura 3.46. Protegiendo nuestra billetera Electrum

Fijaos en que la fortaleza de la contraseña introducida también nos aparece, por lo que haced el esfuerzo y que sea lo más fuerte posible. La contraseña podremos cambiarla *a posteriori* desde las opciones de menú **Wallet** y **Password**. A partir de aquí, ya podremos ponernos a trabajar. Electrum usará la información proporcionada para generar las direcciones de nuestra billetera y verificará si estamos o no *online*.

ENTONCES…

Electrum se comunica con servidores remotos para obtener información sobre el estado de las transacciones y de las direcciones; por defecto se puede dejar que se conecte de manera aleatoria al que elija el programa o indicar el que más nos guste.

Una vez instalado, el funcionamiento no difiere demasiado de lo que acabamos de ver con Bitcoin Core, se basa en diferentes pestañas que sirven para lo siguiente:

- **History**: muestra el histórico de las operaciones que hayamos realizado sobre nuestra billetera, mostrando la fecha, balance, descripción, etc.

- **Send**: como su nombre indica permite el envío de dinero a la dirección que indiquemos.

- **Send**: lo usaremos para enviar dinero a la dirección especificada. Como novedad presenta la opción Request expires que marca la validez del envío de dinero, y varía desde una hora hasta nunca, pasando por un día o una semana.

- **Contact**: sirve como libreta de direcciones, podemos crear tantos contactos como queramos y asociarles la dirección Bitcoin correspondiente. El nombre asociado que demos a la dirección, cuando procedamos a enviar dinero, bastará con escribirlo para que automáticamente nos inserte la dirección en el campo, una posibilidad que resulta muy cómoda.

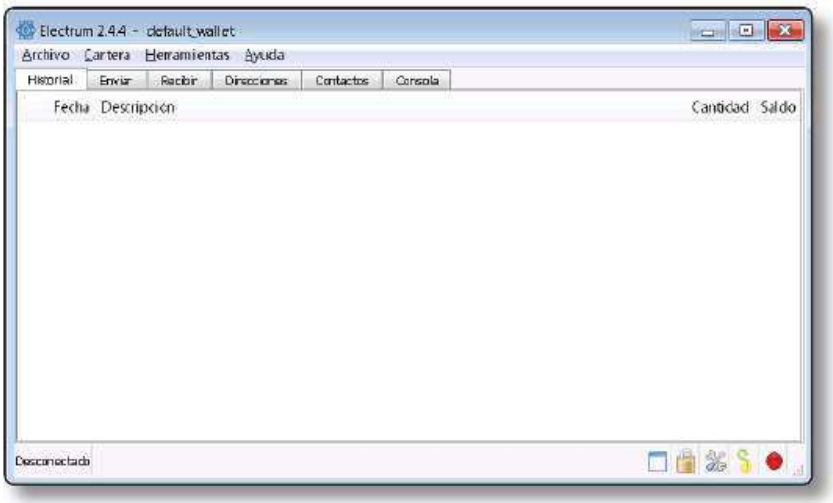


Figura 3.47. Vista principal de Electrum

- **Console**: esta es quizás la opción más potente de Electrum, ya que integra dentro de la propia billetera un intérprete de **Python**, y por ende puede utilizarse para programar nuestros propios *scripts* avanzados que interactúen con la billetera. En la imagen se ve un ejemplo de la llamada a la función "getBalance()" que devuelve el balance de la billetera.

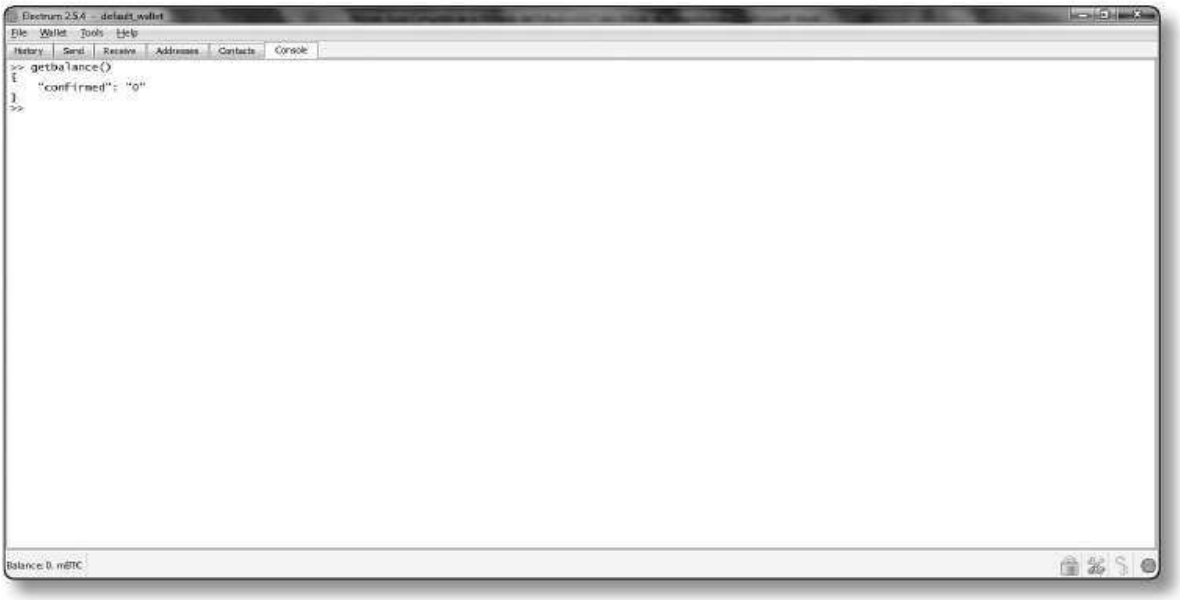


Figura 3.48. La consola de Electrum

¿Algo más?

Electrum dispone de muchísimas opciones adicionales. La firma de mensajes y su verificación al estilo que hemos visto podemos también hacerlas desde **Tools** y las opciones **Sign/Verify Menssage**. Las tarifas de las transacciones se pueden ajustar desde **Preferences** y en la pestaña **Transactions** utilizar el *check* **Dynamic fees** o dejar el valor por defecto y *kilobyte*. También desde **Preferences** puede cambiarse el idioma de la aplicación, indicar la unidad por defecto (milibitcoin en este caso) o incluso el explorador de bloques que deseamos usar, establecido de fábrica el de blockchain.info.

Por ejemplo, de cara a la creación de billeteras multifirma como las que anteriormente describimos, el asistente de entrada nos pedirá cuántas firmas son necesarias para desbloquear los fondos de la billetera.

Figura 3.49. Billetera multifirma Electrum

Se admiten un mínimo de 2 y un máximo de hasta 15 firmas para el acceso a la billetera, pero se puede configurar el acceso a los fondos a partir de 1 firma. En la imagen anterior, la billetera estaría securizada por 2 firmas y ambas serían necesarias para poder acceder.

Si seleccionamos crear una billetera hardware, las opciones que tenemos son:

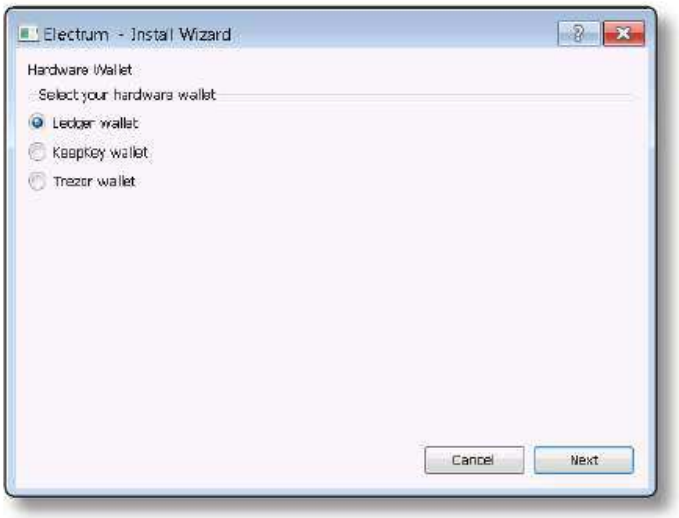


Figura 3.50. Detección hardware desde Electrum

E intentará detectar el hardware conectado en el equipo para crear la cartera sobre él. Están disponibles tanto Ledger como Trezor, y la opción adicional Keepkey, un dispositivo hardware muy avanzado aunque un poco caro a mi juicio (no lo incluí en la sección anterior porque no figura en la web de Bitcoin); aparte de funcionar con Electrum se puede conectar a **Multibit**, otra de las carteras más utilizadas.

3.3.3 Armory

Es uno de los clientes más avanzados de Bitcoin que existen y está muy enfocado al trabajo sin conexión y a la seguridad. La instalación del programa es similar a las anteriores y basta con especificar la ruta en disco para que el software esté listo para funcionar sin muchas más complicaciones; en el acuerdo de licencia nos recuerdan que el equipo de Armory nunca tiene acceso a nuestro dinero y que es responsabilidad nuestra lo que hagamos con el programa, que está todavía en fase beta, por lo que echar un vistazo a la pestaña **Announcements** de vez en cuando para ver si hay nuevas actualizaciones nunca está de más. Como curiosidad, decir que Armory tiene versión que puede instalarse sobre una RaspberryPi.

Figura 3.51. Armory, una billetera avanzada

Si estamos utilizando Bitcoin Core en nuestro ordenador simultáneamente junto con Armory, este se pondrá en modo de funcionamiento *offline*, esto significa que no estamos conectados a la Red y no podremos realizar operaciones en tiempo real, quedando disponibles únicamente:

- La creación, importación o recuperación de billeteras.
- Generar nuevas direcciones para recibir dinero para cualquiera de tus billeteras.
- Crear copias de seguridad e importar claves privadas.
- Cambiar las preferencias de encriptación.
- Firmar mensajes y firmar transacciones creadas desde un sistema que esté *online*.

Para tener acceso a la funcionalidad completa de Armory, hay que indicar dónde se encuentra la ruta de instalación de nuestro Bitcoin Core, en la opción de menú **Settings**, lo que permite que sea Armory el que se encargue de la ejecución en segundo plano de Bitcoin Core y mantenerlo todo bajo control.

Figura 3.52. Configurando Armory con Bitcoin Core

Una vez hecha esta configuración, desde la pantalla principal de Armory veremos como se comienza a realizar la sincronización con la cadena de bloques y el escaneo del histórico de transacciones, finalizado lo cual el programa quedará completamente operativo y en su estado *online*.

Con tres tipos de interfaces: **Standard**, **Advanced** y **Expert**, se amplía el abanico de posibilidades que el programa presenta en función de nuestras necesidades y conocimientos. Cambiar de un entorno a otro implica rearrancar el programa, nos quedaremos con la opción estándar porque nos sirve para los objetivos que perseguimos y comparativa con las anteriores.

Desde el botón **Create Wallet** crearemos nuestra billetera. Los datos son similares a los de antes y se resumen en el nombre de la billetera, su descripción y la contraseña de cifrado, aunque en este caso insisten hasta tres veces en su confirmación para que tengamos constancia de que somos conscientes de la importancia que tiene perderla, y en este caso, no poder volver a acceder a nuestros fondos.

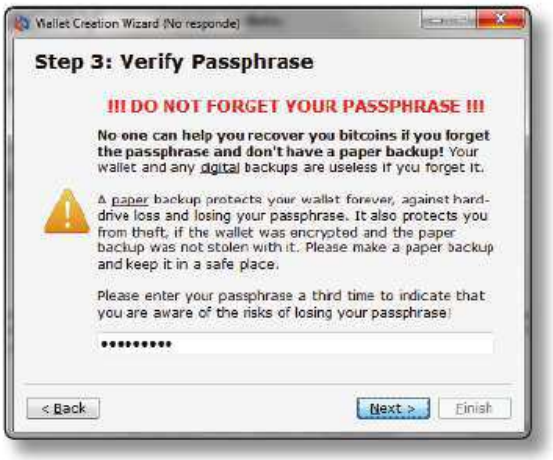


Figura 3.53. Armory, no es por ser pesados ;-)

Ya he dicho que una de las virtudes de Armory es su preocupación por la seguridad, creada la billetera, lo siguiente que nos pide es que hagamos una copia de seguridad de la misma y nos habilita una opción **Create paper backup** con información para restaurar la billetera en caso de algún "accidente". Conviene no dejar de lado el test de verificación que determina que la copia de seguridad se ha realizado de manera correcta, no vayamos a llevarnos sustos luego.

No obstante, en el caso de que optemos por obviar hacer esta copia de seguridad, posteriormente podremos hacerlo si pulsamos sobre la opción **Backup This Wallet** dentro de las opciones de la billetera en específico sobre la que estemos trabajando. Digo esto porque Armory permite crear y gestionar tantas billeteras como queramos, desde su visión principal y la opción **Available Wallets**.

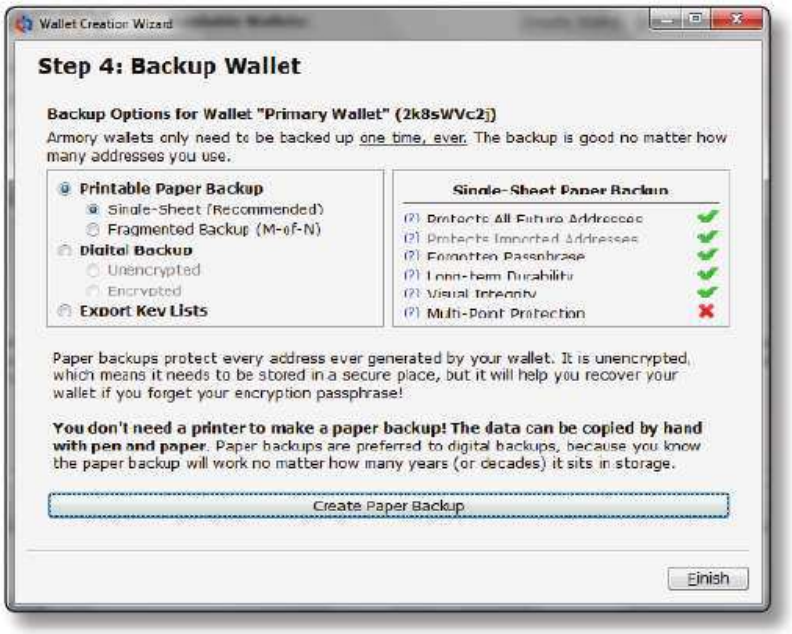


Figura 3.54. Backup en papel de Armory

Suponiendo que hemos finalizado los procesos de configuración anteriores seleccionaríamos la billetera haciendo doble clic sobre ella y vemos lo siguiente:

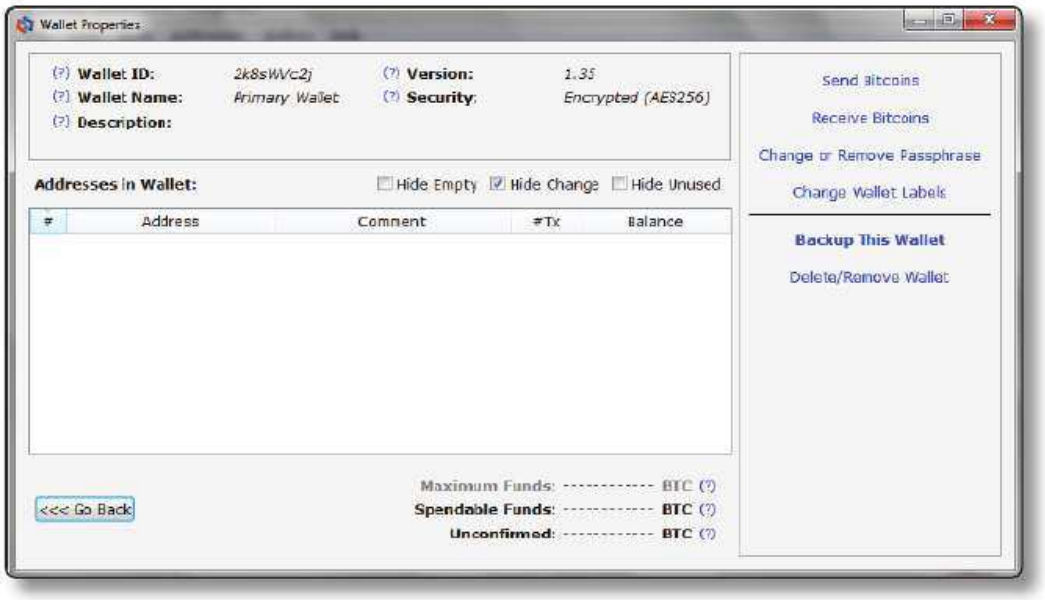


Figura 3.55. Visión de una billetera Armory Standard

Las opciones **Send Bitcoins** y **Receive Bitcoins** se utilizan para el envío y recepción de monedas.

3.3.4 Otros monederos populares

El rango de monederos disponibles no se acaba con los que hemos contado en las secciones anteriores, hay muchos más y como os recomendaba el mejor sitio para encontrarlos es la página web de Bitcoin. Por citar otras opciones tenemos:

- **De escritorio**: además de los tres comentados anteriormente, **Multibit** es uno de los que también nos gusta mucho, además si habitualmente trabajas desde blockchain.info, podrás exportar tu cartera e importarla en Multibit muy fácilmente.

- **Para Android**: los más populares son **Bitcoin Wallet** (personalmente es el que más me gusta) y **Mycellium**, aunque las opciones de **Airbitz** y **Bither** son también muy buenas elecciones.

- **Para iOS**: **Copay**, **Airbitz** y **Bither** están entre mis favoritos, aunque la opción de **Breadwallet** me gusta por su simplicidad (este solo está disponible para esta plataforma). Con Apple, pues eso, que es Apple; no olvidéis que Bitcoin vs. Apple Pay puede ser un desafío, y sabemos cómo se las gasta Apple, no sería la primera vez que retira de su *store* un programa Bitcoin porque no le conviene.

- **Para web**: además de las opciones de **Coinbase** y **Blockchain**, recomiendo que echéis un vistazo a las opciones de **Circle** y **Xapo**.

Desafortunadamente la falta de espacio no nos permite analizar en detalle todas estas posibilidades, sin embargo confío en que con lo explicado en los ejemplos de las billeteras web y de escritorio sea más que suficiente para que podáis moveros con soltura con estas otras, el funcionamiento no difiere demasiado y una vez que tenemos localizadas las opciones el significado de las mismas es idéntico cualquiera que sea el programa que utilicemos. Será la práctica y el probar las diferentes opciones lo que a la larga acabará por hacer que nos decantemos por una solución o por otra.

3.4 OBTENIENDO NUESTROS PRIMEROS BITCOINES

¿Que no tienes Bitcoines aún y te gustaría empezar a tenerlos cuanto antes? Esta suele ser a veces la parte más complicada, por lo que para simplificar las diferentes opciones que tenemos, las dividiremos en dos grupos:

- **Métodos tradicionales**: se refieren a la manera en que se han estado consiguiendo Bitcoines hasta que han aparecido los… efectivamente "otros métodos" de obtención. En este primer grupo estaría la minería, los *faucets* o grifos, el pago por nuestro trabajo, etc.

- **Otros métodos**, cualquier método para obtener Bitcoines que no esté clasificado en el apartado anterior.

3.4.1 Los métodos tradicionales

Los métodos tradicionales pueden resumirse en los siguientes cuatro:

- Minería.
- Los adquiero a través de un operador de Bitcoin o se los compro a alguien que resulte de confianza.
- Hago uso de los grifos o *faucets* que hay en la red.
- Realizo un trabajo por algo y alguien me paga por ello en Bitcoines.

3.4.1.1 MINERÍA

No quiero entretenerme mucho en esta posibilidad porque tenemos un capítulo dedicado a las características de la minería. Simplemente recordar algunas cosas que explicamos en el capítulo 2, en los conceptos básicos.

Minar una moneda, dijimos que consiste en ser capaz de encontrar la solución al problema computacional que el algoritmo de minado de la criptomoneda que estemos usando utilice. Puede ser SHA-256, scrypt o cualquier otro.

Cuando nadie conocía qué era esto de Bitcoin, era una buena manera de conseguirlos, y con un ordenador de casa y usando el poder de la CPU se podía hacer sin problemas. Después la gente comenzó a interesarse por la moneda y a conectar sus equipos a la red y la CPU se quedó corta, fue el momento de pasar a usar el hardware más potente de los ordenadores, las tarjetas gráficas y sus flamantes chips GPU. Quedaron obsoletos también en muy poco tiempo.

Hoy en día, obtener Bitcoines mediante la minería no tiene mucho sentido, salvo que dispongamos de hardware muy especializado (del tipo ASIC que luego explico) y específico, que permita realizar las complejas operaciones matemáticas que se necesitan para poder generar la moneda. Existe la posibilidad de hacer minería

en la nube comprando poder de cómputo a cambio de euros en plataformas como **CEX.io**, pero hay que hacer unos cuantos números para ver qué nos interesa más, si comprar poder de cómputo para minar o invertir ese mismo dinero y cambiarlo directamente por Bitcoines. Una interesante pregunta que no siempre es fácil de responder.

Lo importante de este epígrafe es que minar no es la opción para tener criptomonedas salvo que vayas a invertir una suma importante de dinero en montar una granja de servidores y dedicarte a ello o estés minando una moneda que suscite poco interés y no haya nadie aportando recursos de cómputo y con un ordenador de "andar por casa" puedas hacerlo.

En el caso de Bitcoin no sucede.

3.4.1.2 OPERACIONES A TRAVÉS DE OPERADORES (BRÓKERES) O CASAS DE CAMBIO ONLINE

La **segunda opción** tiene como inconveniente que te tienes que fiar del operador de Bitcoin con el que vas a realizar la operación. Básicamente, trabajar con un operador de Bitcoin se resume en dos pasos:

- Primero hacer una transferencia de la cantidad que deseemos desde nuestra cuenta bancaria a la cuenta bancaria que está en poder del operador (transferencia que suele ser internacional, salvo en el caso de que estés en el mismo país que el banco del operador).

  A veces no es necesario hacer una transferencia bancaria, cada vez más son los operadores los que disponen de la opción de cargar el saldo de tu cuenta de operaciones vía a cargo de tu tarjeta de crédito (¿os acordáis de Coinbase?), lo que se resuelve en el momento. Esto es importante porque si quiero hacer *trading* las ventanas para operar son importantes y disponer del dinero en cuenta fundamental, aunque en estos casos lo habitual es dejar dinero en el operador para poder trabajar sin retrasos. En cualquier caso, utilizar esta posibilidad implica un proceso de validación de varios días, en donde debes proporcionar información y documentación adicional al operador para que te permitan hacerlo. En muchas ocasiones, si el operador tiene dudas sobre la validez de la documentación o información que aportas simplemente rechaza tu solicitud y no puedes usar esta posibilidad.

- Una vez que el operador tiene en su poder nuestro dinero, actualiza nuestro saldo (balance) en su plataforma, y a partir de ahí podemos comenzar a comprar Bitcoines en el mercado, al precio al que se encuentre en ese momento, en la plataforma en cuestión (**hacer trading**).

Que el operador sea de fiar es muy importante para evitar casos como el de **Mt. Gox**, la plataforma de compra y venta de Bitcoin más importante del mundo y que a principios de 2014 quebró dejando un agujero de más de 650.000 Bitcoines (850.000 realmente, pero se recuperaron 200.000), que literalmente desaparecieron como por arte de magia (y esto del arte de magia no deja de tener su gracia por el origen de Mt. Gox), según ellos debido a un robo *hacker*, y según otros a un fraude bien orquestado desde dentro de la propia Mt. Gox (hablaré con más detalle de Mt. Gox más adelante). Sea como fuere, tanto si tenías Bitcoines como euros o dólares en esta plataforma, se esfumaron y Mt. Gox y su presidente **Mark Karpeles** están siendo investigados por la justicia japonesa.

Otra plataforma muy importante que también se ha visto afectada por ataques *hacker* y más recientemente (enero de 2015) ha sido **Bitstamp**, aunque esta última se recuperó de la pérdida de 19.000 Bitcoines y volvió a funcionar con normalidad a los pocos días de su eventual caída, sin que las cuentas de sus clientes se vieran afectadas.

La plataforma china **Bter** ha sido de las últimas en sumarse a la lista de operadores "hackeados" (febrero de 2015), con un robo de 7.170 Bitcoines y ofreciendo una recompensa de 720 Bitcoines a todo aquel que ayude en la recuperación de los fondos robados.

Es posible también encontrar en foros de Internet relacionados con Bitcoin, personas físicas que ofrecen Bitcoines a cambio de euros. El porqué de usar esta opción es muy simple. Si optamos por hacer una transferencia bancaria a otra cuenta, quedamos en todo momento identificados por el banco, quien tiene además por cuestiones de lavado de dinero, que dar cuentas al Estado de nuestras transferencias. Si no queremos transferir dinero a ningún sitio, solo queda la opción de quedar con alguien y darle dinero físico y que él nos transfiera los Bitcoines equivalentes a nuestra billetera. Como el proceso de mover Bitcoines entre billeteras es prácticamente instantáneo e irreversible, es una manera de saltar el eventual control que el Estado quiera hacernos. En este caso la web localbitcoins.com puede ayudarnos a encontrar alguien cercano y con buena reputación para hacer el intercambio.

Figura 3.56. Comprando Bitcoines en persona en Madrid

Esta opción no es para nada recomendable para novatos y aquí sí que tienes que fiarte de con quién estás tratando porque te lo recomiende un amigo o porque su reputación en la red lo avale. En estos casos, se suele quedar con la persona físicamente y se hace el intercambio *in situ*.

Haciendo trading

Veamos un ejemplo de estas plataformas de *trading* para familiarizarnos con los servicios que ofrecen; lo primero volver a recordaros que en última instancia el único responsable de la gestión de tu dinero eres tú, y la elección de la plataforma debería hacerse siempre con cabeza. Para nuestro ejemplo usaré Bitstamp pero lo que explicaré para ella es válido para cualquier otra de vuestra elección, podríamos haber utilizado Coinbase por ejemplo, pero como hablé de esta como ejemplo de billetera en la web, elijo Bitstamp por ampliar nuestro radio de estudio un poco más.

ENTONCES…

Bitstamp es una empresa de *trading* de Bitcoin que tiene su sede en el Reino Unido, aunque sus orígenes están en Eslovenia en 2011 donde inició su actividad de la mano de **Damijan Merlak** y **Nejc Kodric**, miembros muy conocidos de la comunidad Bitcoin. Actualmente es uno de los mercados de compra/venta de Bitcoin más importantes y ha sido capaz de resolver de manera muy eficiente y sin pérdidas para sus usuarios los problemas y ataques en los que se ha visto envuelta.

El primer paso es el típico de cualquier web, deberemos registrarnos para tener acceso a las opciones de compra/venta de Bitcoin. Los datos que nos piden son muy similares a los de Coinbase: nombre y apellidos, dirección de correo electrónico y país de residencia. Al pulsar sobre el botón de confirmación deberíamos recibir un correo de confirmación con nuestro identificador de cliente (usaremos siempre este identificador para conectarnos) y una contraseña segura provisional que deberíamos cambiar la primera vez que entremos en la web.

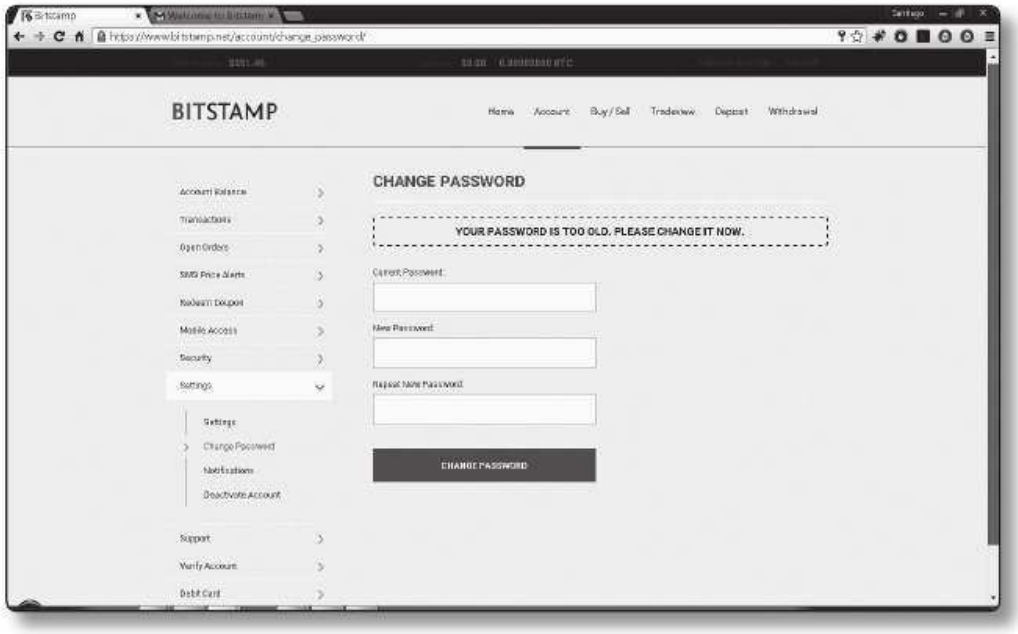


Figura 3.57. Cambiando la contraseña en Bitstamp

Echemos un vistazo a la interfaz que nos proporciona Bitstamp, fijaos en que las opciones que hay en la zona superior (**Home**, **Account**, **Buy/Sell**, **Tradeview**, **Deposit**, **Withdraw**) determinan el contenido del área izquierda de la pantalla. Al igual que sucedía con Coinbase tenemos una sección dedicada a la compra/venta (**Buy/Sell**) pero que no estará habilitada hasta que Bitstamp verifique nuestra identidad.

ENTONCES…

La verificación de identidad es obligada en todas las plataformas por los mismos motivos de siempre; por defecto, todos somos presuntos criminales y hay que prevenir que no vayamos a usar Bitcoin para el lavado de dinero. Por cierto, si por algún motivo no se aprueba tu identidad, no queda otra que ponerse en contacto con el servicio de soporte y tratar de arreglarlo con ellos.

La verificación requiere subir nuestro DNI a la plataforma y rellenar un formulario con unos datos personales, además de una fotografía reciente. Supuesto que el proceso de verificación finaliza con éxito, se habilitarán todas las opciones de la plataforma que estuvieran cerradas por este motivo.

Con la cuenta verificada, lo primero que nos interesa hacer es mandar algo de dinero a la plataforma. El dinero que enviemos puede ser Bitcoines que tengamos en alguna billetera para por ejemplo venderlos cuando suba el precio, o puede ser dinero fíat que tengamos en nuestra cuenta bancaria. Enviar dinero a nuestra cuenta de Bitstamp desde nuestro banco siempre lleva asociado un retraso mínimo de 24 a 72 hora**s** hasta que veamos el saldo actualizado en el balance (zona superior de la pantalla):

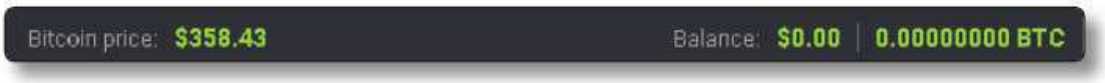


Figura 3.58. Balance en Bitstamp

Siempre el dinero se envía a la cuenta que Bitstamp tiene habilitada en **Eslovenia** en el banco **Gorenjska Banka d.d.** y hay que indicar nuestro usuario en la transferencia, para que los fondos lleguen sanos y salvos al balance; por cierto, no se permite el envío de dinero a cuentas que no sean la tuya. Las transferencias que se hacen en euros (SEPA) se convierten automáticamente a dólares a la paridad marcada por **Raiffeisen Bank** que es de donde Bitstamp toma los datos. Os dejo la URL para que podáis consultarlos por vuestra cuenta por si tenéis curiosidad:

http://www.raiffeisen.si/pripomocki/menjalniski-tecaj/

Experto en trading en 10 minutos o menos

Ahora un poquito de cultura de *trading*, no dispongo del espacio suficiente para poder entrar en profundidad y este libro no pretende ser el lugar para explicarlo (tal vez el próximo) pero es importante que entiendas las siguientes ideas para operar con cierta soltura y entender lo que puedes hacer.

Lo primero, ¿qué es hacer trading? La respuesta más rápida es especular con el valor de un activo, pero como la palabra especular es de las malditas y nos van a mirar mal si la usamos, digamos que es el arte de conseguir una rentabilidad por la negociación de un activo generalmente en un espacio de tiempo corto. En este caso el activo que negociamos es Bitcoin, pero podría ser euros, oro, dólares, acciones de una empresa, petróleo… (basta con echar un vistazo al FOREX para hacerse una idea de todo lo que se puede negociar solamente con divisas/monedas). Cuando

hacemos *trading* de divisas, siempre se hace entre pares, por ejemplo miraríamos el par euro-dólar, o el par libra-yen… o el par Bitcoin-moneda fíat (lo que sea), lo que nos muestra cómo sube o baja el precio entre ambos. Como hay veces en que una moneda está relacionada con otras, caso típico del euro, el dólar, el yuan, el yen, la libra… se habla de correlación como la relación que puede establecerse entre el precio de pares distintos pero que comparten una moneda. Es decir, si tengo el dólar relacionado con el euro, ¿cómo afectan los sucesos que influyen en ese par en el precio del euro respecto del yen? Toda una teoría de estudio.

ENTONCES…

En el caso de Bitstamp, por defecto se nos muestra la relación de precio con el dólar, pero puede cambiarse desde las preferencias (**Settings** del menú de la izquierda y la opción **Preferred Currency**)

La **ventana de tiempo** es muy importante, de hecho hay un tipo de *trading* denominado **intradía** en donde las operaciones se abren y cierran a lo largo de la misma jornada. A veces una operación de compra/venta puede tener sentido durante los próximos 10 minutos, una vez pasada la ventana perdimos la oportunidad, pero seguro que habrá otra; esto es una de las máximas del *trading*, define una estrategia, no te precipites y síguela a rajatabla, evalúala cuando tengas que hacerlo y rectifica lo rectificable y vuelve a empezar. Ten paciencia y como siempre asume los riesgos que puedas asumir sin comprometer tu salud financiera.

ENTONCES…

FOREX son las siglas de *Foreign Exchange* o cambio de divisas. Es un mercado global y descentralizado donde se negocian divisas (o en castellano común, monedas). Surgió para facilitar el **flujo monetario en el comercio internacional**. Tiene un tamaño enorme, de más de 5 billones de dólares, para que os hagáis una idea de lo que esto significa pensad que en un solo día FOREX opera lo que todo Wall Street en un mes.

Una diferencia fundamental con FOREX es que el mercado de compra/venta de Bitcoin no cierra nunca, está abierto 365x24; FOREX sin embargo está sujeto a la apertura de los mercados internacionales y no opera en fin de semana. Otra diferencia es el tamaño del mercado, el de Bitcoin es un vaso de agua comparado con el océano que representa el de FOREX, aunque en ambos los precios se establecen en función de la oferta y la demanda. Una ventaja que tiene Bitcoin (por su propia

naturaleza) respecto a FOREX es que no está sujeto a las decisiones de los bancos centrales, por ejemplo, si el BCE decide aumentar el número de papelitos de euro en circulación, la oferta aumentará y el precio puede variar por esta decisión a la baja.

Abrir una operación significa que voy a comprar o a vender Bitcoines y para ello lo que tengo que hacer es dar una orden al sistema. Las órdenes pueden ser de tres tipos diferentes:

- **Instant Order**: u orden instantánea o a precio de mercado, en este caso abriremos una operación al precio ofrecido por la plataforma, insertándose automáticamente en ella los precios actuales. Es el tipo de orden más simple y puede ser de compra o de venta.

- **Limit order u orden limitada**: estas órdenes también pueden ser de compra o de venta, en este caso se fija un precio máximo para la compra y un precio mínimo para la venta. Por tanto, la compra siempre será a un precio igual o inferior al fijado y la venta a un precio igual o superior.

- **Stop order**: este tipo de órdenes, que también pueden ser de compra o de venta, son una especie de seguro ante posibles variaciones del precio. En el caso de compra, Bitstamp permite comprar una cierta cantidad de Bitcoines si el precio alcanza un determinado valor. La venta es similar pero en sentido contrario, indicaremos la cantidad de Bitcoines a vender si el precio cae por debajo de una cierta cantidad.

Vale, me queda claro lo anterior Santiago, pero, ¿cuándo debo abrir una operación o cerrarla? Bienvenido al mundo del análisis técnico y fundamental, o dicho de otro modo, vamos a intentar poner las matemáticas y lo que sucede en el mundo a nuestro servicio para tratar de averiguar el futuro cual Merlín del siglo XXI. No puedo contestarte a la pregunta anterior, de saber hacerlo perfectamente sería rico y estaría retirado en alguna isla paradisiaca. Lo que se hace es recurrir a algún tipo de análisis sobre el histórico de cotizaciones y tratar de sacar resultados esperando que estos sean lo más acertados posible.

En el análisis técnico se utilizan las gráficas con la evolución de los precios para tratar de buscar tendencias en ellas. Se basan por tanto en la cotización y en el volumen de operaciones; es una aproximación digamos formal, lógica y matemática para prever el futuro y hay definidos un enorme número de funciones e indicadores que se ponen dentro del gráfico y que sirven para ayudarnos en esta predicción, eso sin contar el análisis de las formas que el gráfico hace (hombro-cabeza-hombro, etc.).

El análisis fundamental es más "etéreo" por decirlo de algún modo, porque su fundamento son los indicadores económicos, evolución del paro, valor del PIB, factores sociales, las políticas que se aplican, los acuerdos y pactos entre Estados, el "sentir" de la población ante un hecho, los acontecimientos fortuitos que pueden producirse, las catástrofes naturales, los atentados o terrorismo… entran en juego participantes que a veces no resultan muy fáciles de medir, pero que tienen influencia, y mucha, en el precio. Por ejemplo, un control de capitales por parte de un gobierno, como pasó hace unas semanas con China, puede suponer un incremento del precio de Bitcoin porque hay más demanda que viene de esos países.

En general las mejores decisiones se suelen conseguir mezclando un poco de ambas técnicas.

Aplicando lo anterior en Bitstamp

En Bitstamp, si deseamos realizar *trading* aplicando todo lo que acabo de explicar y suponiendo que disponemos en nuestro balance de una cierta cantidad de dinero fíat o Bitcoin, nos iremos a la opción **Buy/Sell**. En la parte de la izquierda se nos habilita la posibilidad de crear uno de los tres tipos de órdenes que he comentado anteriormente.

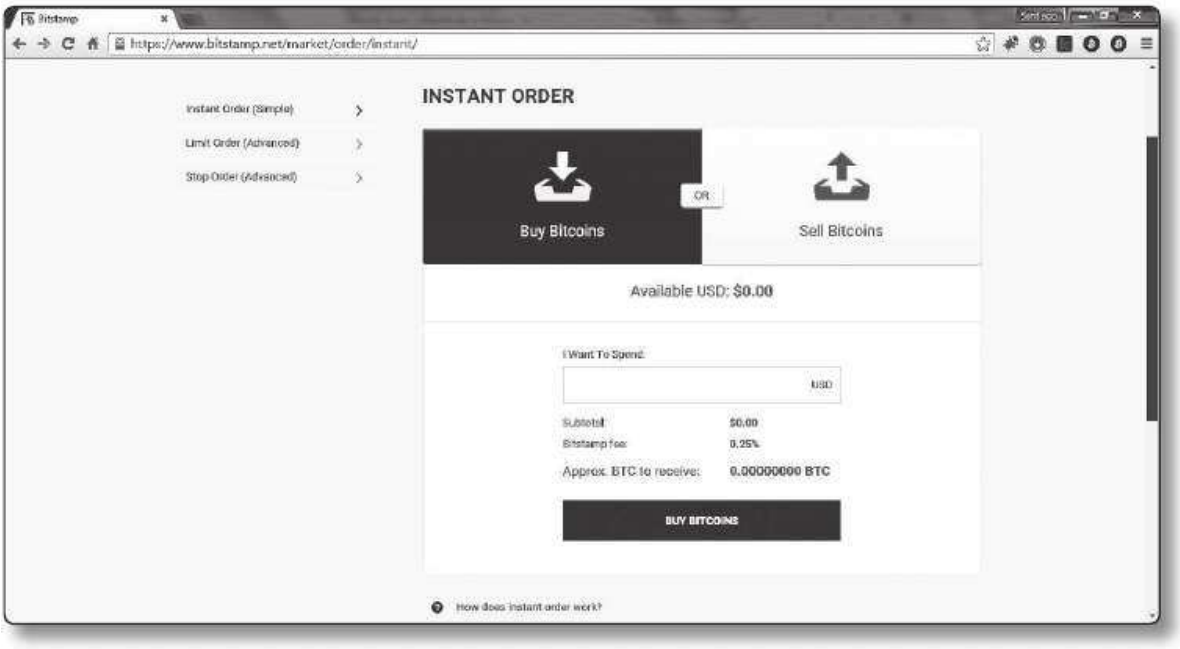


Figura 3.59. Haciendo trading en Bitstamp

Fijaos en que en el caso de las órdenes limitadas hay un enlace que pone **Advanced**, si lo pulsamos tenemos un cuadro adicional **Sell if Executed Price**: o **Buy if Executed Price**:, que actúan como efectos inversores a las órdenes que vamos a definir, es decir, establezco un precio de compra o de venta, pero si reinvierto el proceso si el precio de venta llega a un tope (en la orden de compra) o si el precio de compra sube de un tope (en la orden de venta), sirve para mitigar situaciones en donde los cambios de tendencia puedan hacerme perder dinero.

ENTONCES…

En el mundo del *trading* se utiliza una jerga particular como sucede en otras muchas áreas. Entre estas palabras que podéis encontrar por ahí, está lo que se llama hacer operaciones a corto (se refiere siempre a vender) o hacer operaciones a largo (se refiere siempre a comprar). Junto a estas dos es posible que también veáis el concepto de **bid** que es el precio al que se puede vender. Es decir, se trata de precios a los que las operaciones a corto (venta) se introducen en el mercado, o al que las operaciones largas (compra) salieron. Otro concepto es el **ask** o precio al que se puede comprar. Se trata de precios a los que las operaciones largas (compra) se introducen en el mercado, o al que las operaciones a corto (venta) salieron.

Los conceptos no son excesivamente complejos de entender, pero llegar a aplicarlos con soltura y saber establecer estrategias de compra/venta que resulten a la larga ganadoras es cuestión de mucho tiempo, conocer muy bien los indicadores, tener paciencia y no precipitarse y sobre todo no querer ganar siempre son las mejores recomendaciones que puedo haceros. En general lo importante es tener más operaciones ganadoras que perdedoras, y que el neto resulte rentable.

La mejor manera de poder aplicar técnicas de análisis técnico sobre el precio de Bitcoin es desde la opción **Tradeview**, que nos muestra el diagrama de **velas japonesas** en el intervalo que indiquemos.

ENTONCES…

Las velas japonesas o **candelstick** son una técnica de gráficos y análisis usada en economía iniciada en el siglo XVIII en Japón en el mercado del arroz. Se usan mucho en el análisis bursátil para detectar pautas de comportamiento en los precios y ayudar en la toma de decisiones de compra/venta de activos. Las velas se clasifican en diferentes tipos y se consideran una de las herramientas más útiles para el *trading* y el análisis técnico.

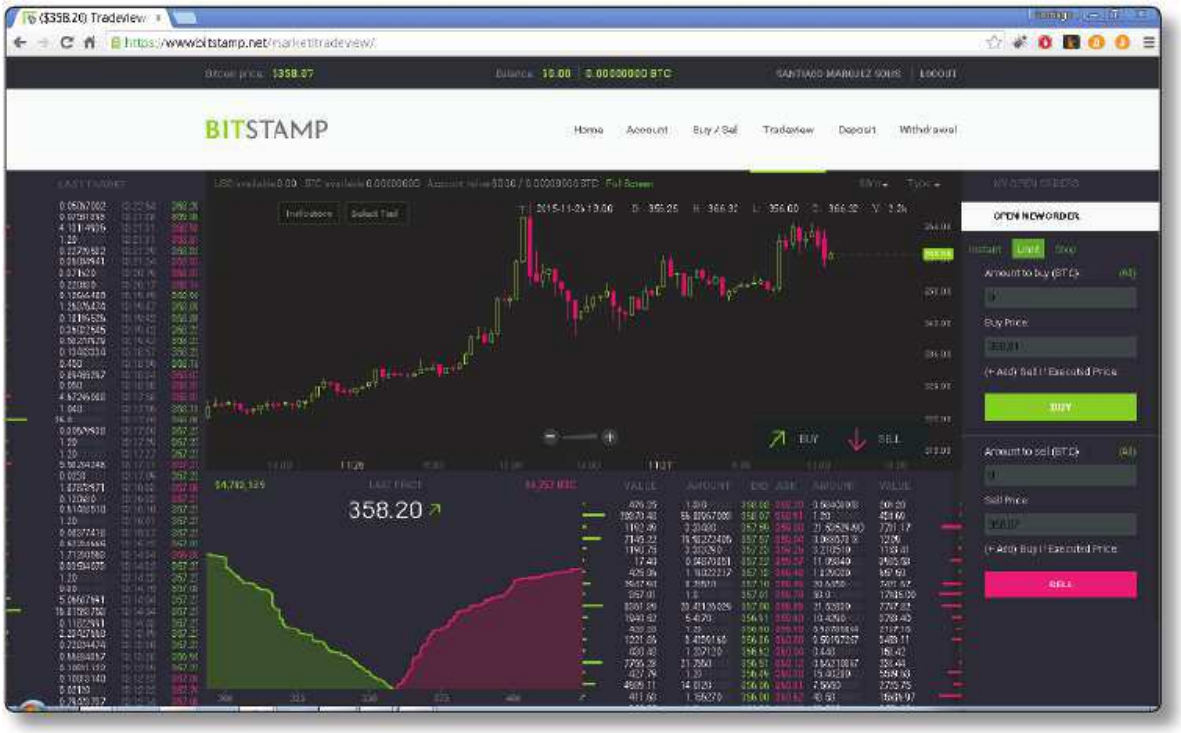


Figura 3.60. Diagrama de velas japonesas en Bitstamp

Embebido dentro del gráfico están los posibles indicadores habilitados para el análisis técnico (botón **Indicators** que contiene algunos muy populares como Accumulative Swing Index, ADX/DMS, Aroon, ATR Bands… entre otros muchos y que junto con el botón **Tools** situado justo al lado nos dan un amplio abanico de opciones); a la derecha de la pantalla en el lateral, desde esta misma vista, podremos abrir órdenes de compra/venta sin necesidad de irnos a la vista **Buy/Sell**, muy útil si queremos operar con el gráfico en pantalla. Los indicadores se muestran sobre el gráfico.

Por finalizar este minitutorial de *trading*, comentaros que hay algunos operadores tradicionales, ligados al *trading* de FOREX y similares, que han comenzado a aceptar la posibilidad de negociar con Bitcoin en sus plataformas (vía CFD por ejemplo), como un servicio adicional para sus clientes. Antes de contratar ninguno de estos servicios informaos y tened claro lo que ofrecen, significan y el riesgo que llevan asociado. Siempre las operaciones que implican especular llevan parejas un riesgo muy alto, que no todo el mundo está dispuesto a asumir.

Los experimentos con gaseosa, por favor.

El caso Mt. Gox y la importancia de la confianza en el operador

Cualquiera que lleve en el mundo de Bitcoin un par de horas (bueno vale, algo más que un par de horas) conocerá el nombre de **Mt. Gox**, por ser la operadora de Bitcoin más importante hasta el momento de su cierre, hecho que sucedió el pasado febrero de 2014, y que dejó a los sufridos poseedores de Bitcoines en este operador (tengo que reconocer que yo soy uno de ellos) con una cara de susto de la que aún nos estamos recuperando; menos mal que diversificamos las compras entre varios operadores.

Y eso que era algo que se veía venir, pero a veces y a pesar de ver que algo va a pasar, nos obcecamos en no hacer caso a las señales y pensar que todo seguirá tal cual; a pesar de que el cierre de Mt. Gox ha sido muy rápido, desde hace más de un año antes se aventuraba que la empresa o cambiaba de rumbo o no terminaría muy bien. Como diría mi abuela Pepa: "Santiago hijo, es que a veces eres muy cabezón".

Mt. Gox fue lanzado en **julio de 2010** y en tan solo tres años llegó a convertirse en el mayor operador de Bitcoin a nivel mundial; para que os hagáis una idea de su importancia, basta decir que en 2013 el **70% de todas las transacciones de Bitcoin** se efectuaban a través de él y según Bitcoin Charts, **en mayo de 2013 el volumen medio era de 150.000 Bitcoines al día**.

Pero hagamos un poquito de historia que eso nos ayudará a poner en contexto lo sucedido. Vayamos al año 2006 y fijémonos en un tal **Jed McCaleb**, probablemente el nombre no te dirá nada, pero si pensamos que detrás de él están los proyectos **eDonkey2000**, **Overnet** y quizás el más importante **Ripple**, podemos decir que el muchacho tiene unas cuantas buenas ideas por la cabeza.

Fruto de estas ideas fue el *site* Mt. Gox, pero ¡ojo al dato!, porque el nombrecillo viene de "**M**agic: **t**he **G**athering **o**nline e**x**change" (he puesto en negrita las letras usadas para formar las de Mt. Gox), y que sería algo así como un sitio de intercambio de compra/venta de las tarjetas del popular juego de magia.

ENTONCES…

Recientemente, McCaleb ha revelado que se encuentra trabajando en un proyecto secreto que estaría relacionado con Bitcoin, aunque en sus propias palabras "será algo bueno para Bitcoin y algo bueno para ti". Teniendo en cuenta su trayectoria estoy seguro de que será algo muy interesante.

Actualmente está buscando *alpha testers*; este proyecto secreto estaba alojado bajo la página *secretbitcoinproject.com* que ahora redirige a *www.stellar.org*, que permite crear productos financieros y ponerlos a disposición de la gente.

Pues no ha dado de sí la cosa dirán algunos, y otra vez más, no les faltará razón.

El dominio **mtgox.com** fue adquirido en enero de 2007 y el *site* descrito puesto en marcha como una beta a finales de ese mismo año. No obstante, McCaleb no tenía mucho tiempo para este proyecto, y a los tres meses de su puesta en funcionamiento, lo abandonó para dedicarse a otras cosas, aunque mantuvo el control del nombre y en 2009 lo llegó a utilizar para anunciar su juego de cartas *The Far Wilds*.

En julio de 2010 y después de leer sobre Bitcoin en **Slashdot**, decidió que la naciente comunidad Bitcoin necesitaría una herramienta que permitiría realizar intercambios de Bitcoines con las monedas de uso corriente, así que el 18 de julio de 2010 creó una nueva web para realizar este tipo de operaciones y reutilizó el nombre de Mt. Gox.

ENTONCES…

El juego *Magic: The Gathering* fue desarrollado en 1993 por **Richard Garfield**, y es considerado como el primer juego de cartas moderno con más de seis millones de jugadores en 52 países. Aparte de la versión estándar, hay una para poder jugar *online*. El precio de las cartas depende de su utilidad y de su rareza, y varía de 0,08 € las más normales, hasta los más de 2.000 € de la carta **Black Lotus**.

Fue en marzo de 2011 cuando McCaleb decidió vendérselo a **Mark Karpeles** (este se hacía llamar **Magicaltux** en los foros *online* por entonces); a pesar de creer que el futuro de Bitcoin era brillante, el tiempo que tenía disponible para desarrollar el potencial de Mt. Gox era a su juicio insuficiente y prefería que otro ocupase su lugar y pudiera llevarlo al lugar que se merecía (aquí no valen chistes facilones de decir que sí, que lo ha llevado a la quiebra, a Mt. Gox quiero decir, que no a Bitcoin). Curiosamente, aunque la propiedad de Mt. Gox pasó a manos de Karpeles, McCaleb ha seguido ligado a la empresa como directivo y controlando el 12% de la compañía, estando el 88% restante en manos de Karpeles. Cómo consiguió Mark el dinero para comprar Mt. Gox o de cuánto fue la compra es otro de los misterios que hasta la fecha sigue sin estar muy claro.

Y ¿quién es Mark Marie Robert Karpeles? Pues en su biografía aparecen algunos datos al menos curiosos, y que pueden tomar más relevancia ahora que Mt. Gox ha cerrado y que demuestran que la personalidad de este hombre es de lo más inestable y probablemente sea la persona menos indicada a la que habría que haber dejado gestionar nuestro dinero.

De origen francés (**Chenôve**) y nacido en 1985, toda su trayectoria profesional y personal podía seguirse y era publicitada por él mismo en su blog, ahora cerrado. Laboralmente destaca los problemas con sus empleadores, que en más de una ocasión le despidieron por su bajo rendimiento y su poco interés por el trabajo, algo que choca con su corta carrera profesional.

De esta carrera cabe destacar:

- El puesto que tuvo durante los años 2003 a 2005 en **Linux Cyberjoueurs** como desarrollador de software y administrador de red. Es despedido de esta empresa por pasar más tiempo chateando que realizando sus labores de programación.
- En 2005 se muda a Israel para trabajar en la empresa **Fotovista**. Es despedido al descubrirse que pasa más tiempo trabajando en sus proyectos personales (la web ookoo.org) que haciendo su trabajo.
- En 2009 se traslada a Japón al comprar la japonesa **NEXWAY Comp., Ltd** la empresa telechargement.fr para la que trabajaba.

Y paralelamente a lo anterior:

- **Colaborador y programador PHP**, haciendo contribuciones al repositorio oficial del lenguaje creando una herramienta llamada proctitle, que permite cambiar el nombre de un proceso sobre sistemas Linux.
- Socio de **Mensa**, la famosa organización que solo acoge entre sus miembros a personas con un alto cociente intelectual.
- En algunas entradas de su blog, publica los momentos en los que se encuentra deprimido y no es raro encontrar alusiones a pensamientos asociados al suicidio.

Figura 3.61. Mark Karpeles (fuente: Yahoo News)

Publicado su blog, este cuenta que cuando era adolescente, fue encontrado culpable de un delito financiero realizado por ordenador y relacionado con un fraude de transferencia de dinero. Por este motivo estuvo durante una temporada sin poder abandonar Francia, teniéndose que presentar de manera regular en los juzgados. Cuenta que el psiquiatra que le examinó concluyó que no era responsable de sus actos y que podría haber estado influenciado por el uso de cannabis, aunque él aseguraba que nunca había consumido sustancias de ese tipo. Aunque fue acusado, la sentencia se suspendió a los tres meses y no quedó rastro en sus antecedentes penales.

A su vuelta de Israel a Francia, volvió a tener problemas con la justicia y pasó 13 horas detenido por el **BEFTI (Brigada de Investigación del Fraude en Tecnologías de la Información)**, aunque fue puesto en libertad posteriormente y solo tuvo que hacer una declaración.

Recientemente y después de lo sucedido, fuentes anónimas dentro de Mt. Gox y entrevistadas por algunos medios han dicho de Karpeles que le gustaba ser alabado continuamente y que se le considerase como el "rey del Bitcoin", y ser CEO de una gran compañía, pero que en el fondo, las tareas de las que es responsable alguien con este cargo y el día a día le aburrían. Algo que no nos sorprende después de saber más sobre su trayectoria profesional.

Esta opinión va un poco en la línea que cuenta su madre (sí, sí, a la madre del señor Karpeles, **Anne Karpeles**, también la han entrevistado), quien ha dicho que su hijo no es deshonesto pero que carece de habilidades sociales y es un pobre comunicador, una persona muy introvertida, de la que cualquiera se puede aprovechar y asegura que esto le pasaba de pequeño cuando sus compañeros de clase le utilizaban para que les hiciera los deberes. También cuenta que no era un buen estudiante y la mayoría de las asignaturas le resultaban aburridas, y que como le sucede a cualquier niño superdotado, pasó de colegio en colegio teniendo muchos problemas con sus profesores. No conseguía que le interesara nada hasta que entró en contacto con los ordenadores, gustándole la programación en PHP que aprendió de manera autodidacta. Karpeles nunca llegó a tener estudios universitarios.

Lo más extraño es que su madre asegura que ella no tenía noticias de que su hijo estuviera involucrado detrás de Mt. Gox hasta que los periodistas se pusieron en contacto con ella, y que fue entonces cuando consultó la Wikipedia para obtener más información.

Y es que hablamos muy poco con nuestros padres, ¿no es cierto, mamá?

Circulan por la Red también los comentarios de otra persona que fue entrevistada para formar parte de la compañía como desarrollador y que quedó escandalizado ante la forma de trabajo que se seguía en Mt. Gox, en donde se carecía de repositorio de código y todas las revisiones que se hacían, antes de ponerse en

marcha, tenían que ser supervisadas por el señor Karpeles, con los consiguientes retrasos asociados a su aparentemente poco profesional conducta.

Como cualquier otro sitio web, Mt. Gox no se ha visto libre de los ataques *hacker*, y al ser el *site* con mayor volumen de operaciones, la cotización de Bitcoin ha fluctuado en función de las informaciones que a este respecto se publicaban.

Según **Jesse Powell y Roger**, dos de las personas que ayudaron a Karpeles a resolver problemas del ataque, comentan que este se mostraba extrañamente despreocupado ante la comprometida situación. Situación que no se veía favorecida cuando aparecían problemas legales con otras empresas, fallos técnicos que obligaban a cortar el servicio o tal vez lo más importante, la regulación estatal.

A partir de abril de 2013 hay algunos acontecimientos que bien pudieron influir en el cierre posterior del *site* y que están muy relacionados con cómo se gestionó Mt. Gox en su relación con el Gobierno americano.

La presión por parte del **FinCEN (U.S. Treasury Departmet's Financial Crimes Enforcement Network)**, un organismo norteamericano destinado a perseguir delitos financieros, hizo que las empresas de intercambio de Bitcoin tuvieran que registrarse para poder operar en los EE. UU., elaborar programas para evitar el lavado de dinero e informar de cualquier actividad sospechos**a**. Probablemente estas declaraciones fueron las culpables de la caída que la moneda tuvo entre el 10 y el 17 de abril de 2013, donde se pasó de 237$ a poco más de 68$; como dice el refrán, el dinero es miedoso.

Poco después, durante el período de tiempo que va desde mayo a julio de 2013, el **Departamento de Seguridad Nacional de EE. UU.** confiscó fondos de Mt. Gox por valor de 5 millones de dólares, amparándose en un estatuto federal americano sobre lavado de dinero. Seguramente esta medida estuvo relacionada con la parada técnica que en junio de 2013 Mt. Gox realizó deteniendo temporalmente la retirada de dólares de su sistema.

ENTONCES…

La presión de FinCEN ha sido siempre tan fuerte, que otro operador, **Bitfloor**, tuvo que cerrar, al ser sus cuentas intervenidas por no haber sido registrada de manera correcta. De igual modo, Mt. Gox no se registró de manera inmediata en FinCEN y esto ha podido también precipitar su caída, pero no solo eso, en un *email* del 13 de abril, Karpeles afirma que el destino de Bitfloor no será el que siga Mt. Gox ya que ellos siguen una política contra el lavado de dinero muy estricta, así como buenas relaciones con todas las partes para asegurar que todo funciona tan bien como sea posible.

Pero ¡ojo al dato!, no fue hasta octubre de 2013, después de pegarse de bruces con la Administración americana cuando Karpeles contrató a un directivo para hacerse cargo de los temas regulatorios.

Todo este despliegue de medios americano es el que se postula como el causante de que **Mizuho Bank**, el banco japonés que gestionaba los fondos de Mt. Gox en Tokio, presionara en los meses posteriores para que la compañía cerrara sus cuentas con ellos.

Los inicios de 2014 iban a ser los que asestaran el golpe definitivo a Mt. Gox, aunque Karpeles parece ser que no se preocupó realmente de la situación hasta mediados de febrero. Durante enero, y según fuentes anónimas de Mt. Gox, Karpeles pasaba más tiempo viendo series de anime y episodios de Breaking Bad que dirigiendo su empresa, y se enfocaba sobre todo en temas logísticos de una cafetería que pensaba lanzar en el mismo edificio en donde estaba Mt. Gox, consultando a chefs franceses y expertos en café. Puede parecer surrealista, pero cuando el río suena…

El 23 de febrero de 2014, Karpeles renunció a su puesto en la dirección de la Bitcoin Foundation, algo que parecía el anuncio de lo que llegaría una semana más tarde y que puede resumirse en el siguiente *email* que todos los clientes recibimos:

26 de febrero de 2014

Estimados clientes de Mt. Gox,

Como hay una gran cantidad de especulaciones sobre Mt. Gox y su futuro, me gustaría aprovechar esta oportunidad para tranquilizar a todo el mundo y decirles que todavía estoy en Japón, y trabajando muy duro con el apoyo de diferentes partes para encontrar una solución a nuestros problemas recientes.

Además, me gustaría amablemente indicarles que se abstengan de hacer preguntas a nuestro personal: han recibido instrucciones de no dar ninguna respuesta ni información. Por favor, visite esta página para obtener más anuncios y novedades.

Atentamente,

Mark Karpeles

El 28 de febrero de 2014, Mt. Gox se declara en bancarrota y suspensión de pagos, al no poder hacer frente a los cerca de 750.000 Bitcoines de clientes y otros 100.000 Bitcoines propios que habrían sido robados, aprovechando un bug en el protocolo Bitcoin conocido desde 2011 y que tiene que ver con la maleabilidad

de las transacciones (veremos en qué consiste esto de la maleabilidad en el capítulo 4, de momento considerarlo como un fallo técnico no resuelto). En su declaración afirmaba que habían perdido el 99,97% de los Bitcoines que tenían en posesión y que ni él ni ninguno de sus empleados se habrían dado cuenta de ello, cosa que no deja de ser un poco rara ya que según sus propias declaraciones, el robo se habría ido produciendo poco a poco y a lo largo de los meses.

Y partir de aquí, ¿ahora qué? Pues han pasado muchas, muchas, muchas cosas desde entonces y todas no dejan de ser sorprendentes, confusas y en muchas ocasiones contradictorias. Por un lado, Mt. Gox publica noticias sobre el estado en que se encuentra su proceso de bancarrota en su página web y recientemente ha dejado a los usuarios que consulten sus saldos en sus cuentas, pero sin ir mucho más lejos. Es más, la propia Mt. Gox advierte que:

"la confirmación de los saldos no constituye una presentación de reclamaciones de restitución ni supone un reconocimiento alguno de deuda".

Pues qué bien.

Figura 3.62. Mt. Gox actualmente

Por otro lado, el 7 de marzo de 2014, Mt. Gox anunció que había encontrado 200.000 Bitcoines en una billetera con un formato antiguo, lo que reduciría el agujero a 650.000 Bitcoines (nada más). Sin embargo, ni siquiera esta buena noticia está libre de polémica, porque aunque el anuncio lo hizo el mismo Karpeles, indicando que el dinero se movería de las billeteras *online* a otras *offline* (con el conocimiento de las autoridades japonesas), las fechas en las que se supone que se realizaron los movimientos, 14 y 15 de marzo de 2014, no coinciden con las fechas que aparecen registradas en la cadena de bloques.

Las últimas investigaciones efectuadas por las autoridades de Japón indican que la manera en la que Mt. Gox gestionaba los fondos de los clientes no era transparente y se utilizaban para cubrir los costes operativos de la empresa y soportar su expansión. Y es que de ser cierto, fueron los propios empleados de Mt. Gox los que pidieron una reunión con Karpeles, para que este explicase qué sucedía con los fondos depositados por los clientes, y que no estaban siendo usados para costear ciertos lujos, entre los que estarían un robot, una impresora 3D, un Honda Civic importado, o el alquiler de las oficinas de Tokio en la misma zona en donde Google está ubicado.

Además, para hacer más interesante toda esta historia, un grupo de hackers ha filtrado después de entrar en los servidores de la compañía (unos días antes del anuncio de la bancarrota), un fichero de más de 700 MB (una pequeña parte de los más de 20 GB que se especula han conseguido) en donde había numerosas hojas de cálculo con registros de transacciones, y que demostraría que hay muchas contradicciones entre el supuesto ataque y robo sufridos por Mt. Gox. Es decir, que de un supuesto ciberataque pasamos a hablar de un fraude de tomo y lomo que podría dar con los huesos del señor Karpeles entre rejas, aunque esto no deja de ser una mera hipótesis, porque no podemos olvidar la naturaleza alegal de Bitcoin y la falta de legislación que hace que todos los escenarios puedan ser posibles.

```
<?php

namespace Money;

class Bitcoin {
        #const BITCOIN_NODE = '173.224.125.222'; // w001.mo.us temporary
        const BITCOIN_NODE = '50.97.137.37';
        static private $pending = array();

        public static function update() {
                // Update all nodes
                $list = \DB::DAO('Money_Bitcoin_Host')->search(null);
                foreach($list as $bean) {
                        $bean->Last_Update = \DB::i()->now();
                        $client = \Controller::Driver('Bitcoin', $bean->Money_Bitco
                        if (!$client->isValid()) continue;
                        $info = $client->getInfo();
                        if (!$info) {
                                $bean->Status = 'down';
                                $bean->commit();
                                continue;
                        }

                        if (($info['generate']) && ($bean->Generate == 'N')) {
                                $client->setGenerate(false);
                        } elseif ((!$info['generate']) && ($bean->Generate != 'N'))
                                $client->setGenerate(true);
                        }

                        $bean->Version = $info['version'];
                        $bean->Coins = (int)round($info['balance'] * 100000000);
                        $bean->Connections = $info['connections'];
                        $bean->Blocks = $info['blocks'];
                        $bean->Hashes_Per_Sec = $info['hashespersec'];
                        $bean->Status = 'up';
                        $bean->commit();
```

Figura 3.63. Fragmento del código de Mt. Gox filtrado

No obstante, la teoría del fraude va cobrando cada vez más peso, y Karpeles ha sido llamado a declarar por un juez de Dallas (Texas), y también por **la Red de Cumplimiento de Crímenes Financieros del Departamento del Tesoro de EE. UU.** (una división contra el lavado de dinero), y dado que sus abogados creen que será detenido nada más poner los pies en el país, y seguirá los pasos de **Charlie Shrem** que está bajo arresto domiciliario (es propietario de **Bitinstant**, operador de Bitcoin que ha sido cerrado por blanqueo de dinero), se está barajando la posibilidad de que otra persona asuma el cargo de la compañía y sea esta la que comparezca en representación de Karpeles, y de este modo evitar su detención.

¡Desde luego no se puede negar que no tiene cara dura!

Y es que poco a poco los afectados por Mt. Gox, se estima que hay 127.000, se están organizando para reclamar a la empresa responsabilidades, en este sentido, los casos de denuncias más sonados hasta el momento han sido:

- La de **Gregory Greene**, un residente de Illinois que asegura haber perdido 25.000 dólares y que ha incluido incluso al mismísimo Jed McCaleb como denunciado.

- El de los comerciantes de Bitcoin canadienses que han presentado una demanda conjunta contra Mt. Gox y contra **Mizuho Bank**, el banco japonés con el que operaba Mt. Gox, y al que acusan de haberse enriquecido a sabiendas.

En español os recomiendo que echéis un vistazo a la plataforma de afectados por el cierre de Mt. Gox, en donde publican puntualmente información sobre el proceso de quiebra, y que está disponible en: *http://afectadosmtgox.blogspot.com.es/*.

Para darle más morbo a todo esto, un grupo de inversores, entre los que estarían **Brock Pierce** (fundador de KnCMiner y GoCoin), **John Betts** (directivo de Morgan Stanley y Goldman Sachs) que podría ser el nuevo CEO y **William Quigley** (de Clearstone Venture Partners), se han ofrecido a comprar Mt. Gox por el precio simbólico de 1 Bitcoin, asumiendo todas las obligaciones que se deriven de esta adquisición, aunque para poder llevarla a cabo se requiere que desde los tribunales japoneses se dé el visto bueno.

En el plan de compra se habla de dos alternativas para hacer frente a los acreedores, la primera sería que los nuevos propietarios reducirían las comisiones por transacción que perciben en un 50%, de este modo, irían pagando a los acreedores poco a poco. La otra opción es que de los 200.000 Bitcoines recuperados, cada

acreedor recibiría una parte prorrateada de los mismos a razón de un 20% del dinero que tuvieran en ese momento en Mt. Gox, u obtener una participación por ese mismo valor en el nuevo Mt. Gox.

La petición de rehabilitación de Mt. Gox cuenta con una campaña de recogida de firmas en Internet, a la que cualquier afectado se puede sumar. Sin embargo, y como decía, estas buenas intenciones necesitan que los tribunales japoneses den su visto bueno, cosa que no están por la labor de hacer, por lo que lo único que le resta a Mt. Gox es liquidarse y desaparecer para siempre.

3.4.1.3 LOS GRIFOS O FAUCETS

Los grifos (o *faucets* en inglés) son un buen mecanismo para experimentar con Bitcoin de un modo muy simple y efectivo, además no se necesita más que un poco de paciencia para acumular unos cuantos satoshis y comenzar a explorar lo que sucede en este universo *a priori* tan extraño. Y como el proceso que hay que seguir para hacerlo es muy facilón veamos cómo comenzar a tener nuestras primeras pequeñas porciones de criptomoneda.

Pero, ¿qué es un grifo o qué hace exactamente un grifo? Si partimos de la imagen mental de un grifo que gotea agua lo entenderemos perfectamente. Cambiar la gota de agua que cae cada x tiempo por una cantidad determinada de moneda que también cae (en este caso a nuestra dirección Bitcoin) y tendréis la imagen mental perfecta de su funcionamiento. Dicho de otro modo, un grifo lo que hace es proporcionarnos pequeñas cantidades de Bitcoin por el visionado de publicidad, que dura unos cuantos segundos. Lo habitual es que a más segundos que dure el anuncio, más cantidad de fracción de Bitcoin ganamos con su visionado.

Fijaos en que digo fracción de Bitcoin, y que nadie se lleve a engaño, las cantidades que pagan están en el orden de los céntimos, así que id olvidando haceros ricos con este sistema; hubo un tiempo, no obstante, en que los grifos eran muy generosos y proporcionaban Bitcoin completos y no fraccionados; quizás uno de los más famosos era el **Bitcoin Faucet de Gavin Andersen**, cerrado desde hace tiempo, aunque la página web aún está accesible en Internet por si queréis echarle un vistazo:

https://freebitcoins.appspot.com/

La idea de los grifos y el obtener fracciones de moneda de esta manera no es ni mucho menos un concepto nuevo. Se lleva usando desde hace muchísimo tiempo pero usando euros o dólares en lo que se conoce como **PTC o Pay To Click**, o "Pago por hacer clic" y hay decenas de webs en Internet especializadas (algunas de las más antiguas y afamadas son NeoBux, ClixSense o NerdBux).

Pero ¡cuidado! Hay que saber que muchos de los grifos que hay en Internet son webs que, con la promesa de pagarte cierta cantidad (o mejor dicho cuando llegues a un mínimo de dinero, y esto suele ser lo común, tanto en los que son de fiar como en los que no lo son), lo único que hacen es que gastes tu tiempo haciendo clic en los enlaces que te proponen y al final no te dan nada o desaparecen de la red sin previo aviso, es por eso que conviene ser cuidadoso y asegurarse bien de con quién nos aliamos. La confianza en el grifo y su reputación son dos de los primeros factores de los que debes asegurarte antes de registrarte en ningún sitio y perder el tiempo haciendo clic.

¿Algún grifo que pueda recomendarte y que tenga la seguridad de que pagan?, generalmente yo suelo comprar usando plataformas de *trading* como puede ser Bitstamp, pero para ilustrar con ejemplos reales esta parte del libro, hice pruebas con algunos de los más populares, y voy a contaros cómo funcionan (y por cierto, no tengo ningún tipo de relación personal ni profesional con ninguno de ellos):

- Btcclicks.com
- Bitvisitor.com
- Bitsforclicks.com

Btcclicks.com

Me registré hace unos meses en la web **btcclicks.com** y hasta la fecha no me ha dado ningún problema y ha pagado religiosamente al llegar a la cantidad mínima establecida (10.000 satoshis), por lo que puede ser un buen punto de inicio, además recientemente ha cambiado su interfaz de usuario, resultando mucho más amigable trabajar en ella. Dispone de opciones tanto para los usuarios que quieren ganar unas cuantas fracciones de Bitcoin, como para aquellos que lo que desean es publicar anuncios.

Veamos cómo lo haríamos en esta secuencia de pasos; como necesitaremos una dirección Bitcoin, podemos usar cualquiera de las que hayáis generado anteriormente cuando vimos los diferentes tipos de billeteras.

Pasos:

1. Obtener una dirección Bitcoin (ir a las secciones anteriores para ver cómo haríamos esto).

2. Abrimos un navegador y nos dirigimos a la URL *www.btcclics.com* y obtenemos la siguiente página:

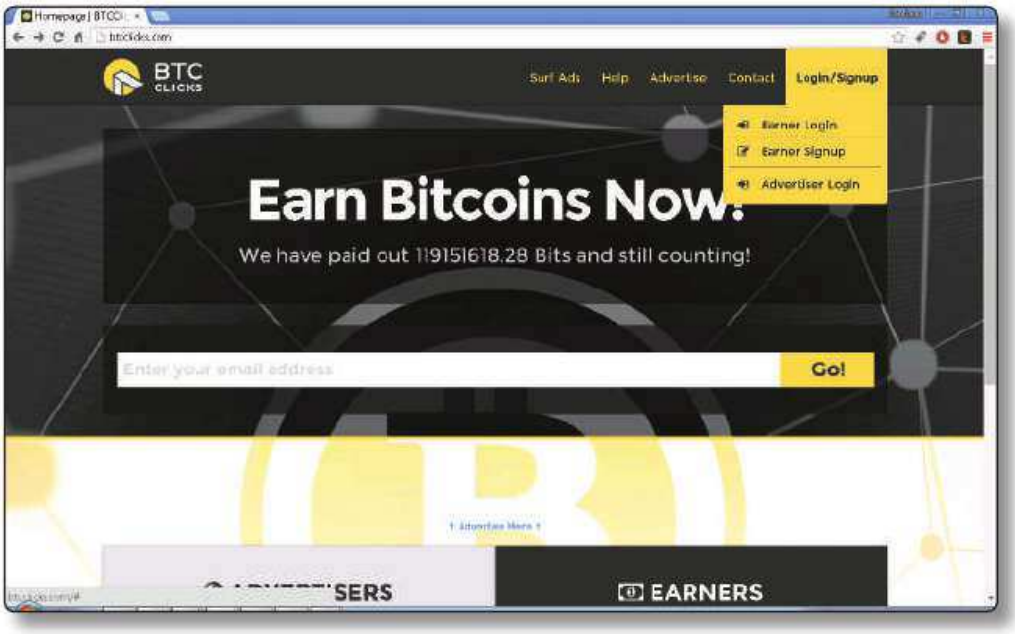


Figura 3.64. Home de btcclicks.com

3. Para registrarnos introducimos nuestro *email* en el campo de texto anterior que está marcado con **Enter your email address** y pulsamos el botón **Go!** También es posible hacer lo mismo desde **Login/Signup** seleccionando la opción **Earner Signup**. En cualquiera de los casos accederemos a la siguiente página:

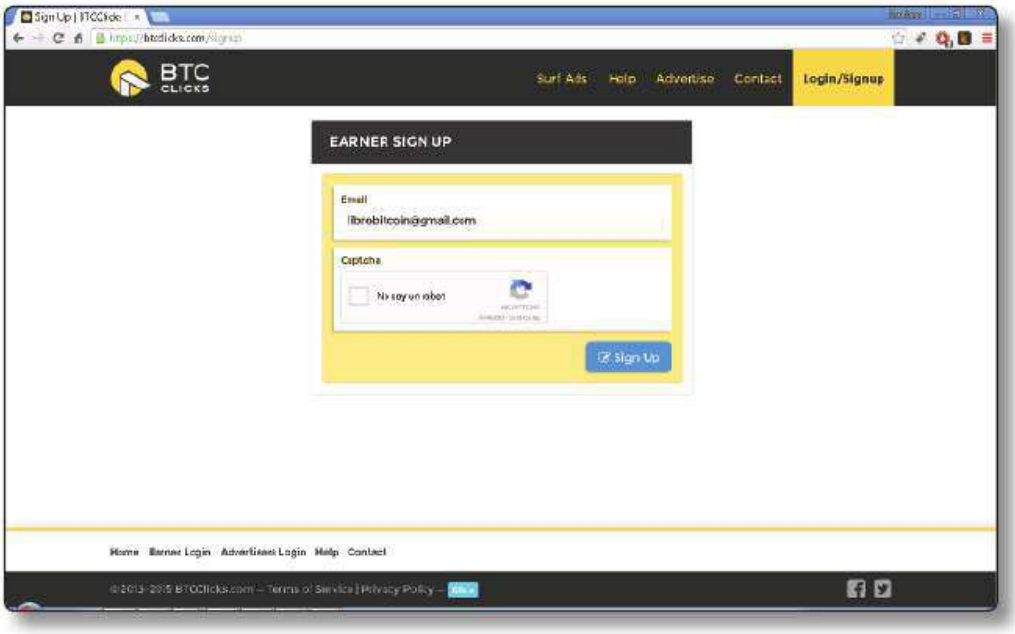


Figura 3.65. Registrándonos en btcclicks.com

4. Ponemos nuestra dirección de *email* y pulsamos en **No soy un robot** y nos aparece un CAPTCHA (una imagen o un texto que sirve para ayudar al programa a determinar que somos humanos y que no se está intentando hacer un registro automático) que tenemos que resolver. Hecho lo cual un mensaje debería llegar a nuestra cuenta de correo para finalizar el registro y que además sirve para verificarla.

Figura 3.66. Confirmación de registro en btcclics.com

5. Al pulsar en **Verify** podremos introducir la contraseña que más nos guste y aceptar los términos del servicio. Al pulsar sobre **Start Earning Bitcoin**, estará nuestra cuenta lista para empezar a ganar fracciones de Bitcoin desde este grifo.

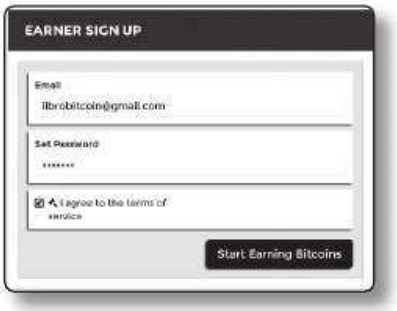


Figura 3.67. Proceso de login en btcclicks.com

Por otro lado, si en vez de hacer el movimiento a una billetera cualquiera, lo hacemos a una **billetera de Xapo**, si la billetera es nueva nos obsequiarán con un bono de 50 bits (5.000 satoshis) en nuestra cuenta. En este caso los movimientos de Bitcoines son instantáneos. Para indicar cuál es la dirección donde queremos recibir los fondos, pulsaremos sobre **Balance** >> **Dashboard** y seguidamente en **Withdraw** (siempre nos pedirá la contraseña cuando hagamos una retirada como medida de seguridad):

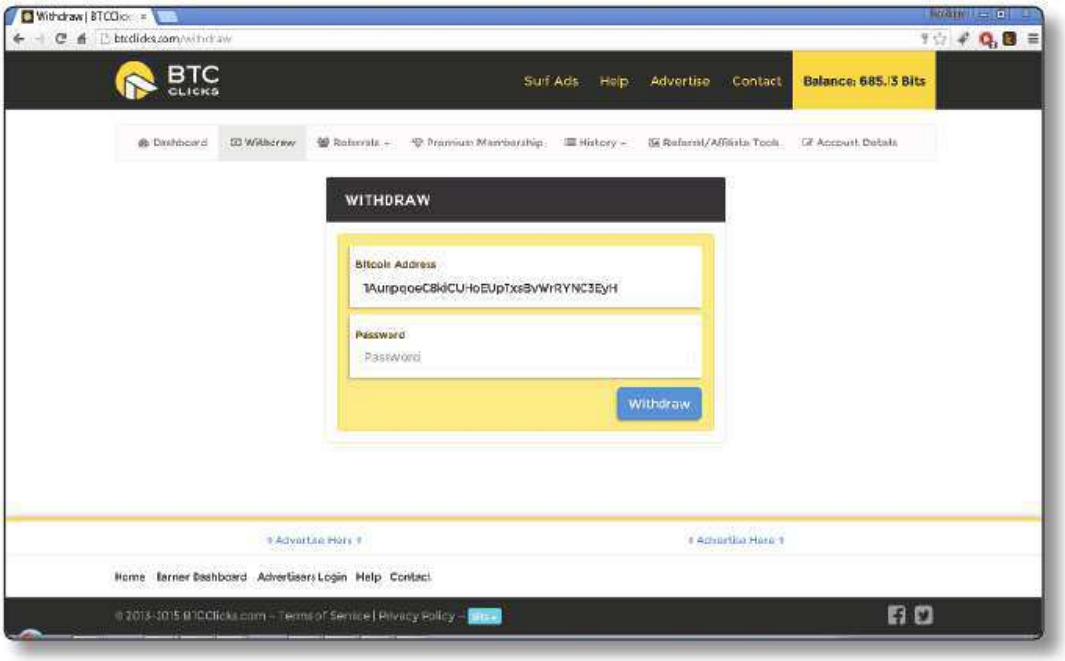


Figura 3.68. Indicando nuestra dirección de retirada

Para comenzar a ganar dinero pulsamos sobre **Surf Ads** y tendremos una lista con los posibles anuncios a visualizar junto con la cantidad que ganaremos por su visualización. Si el anuncio fue visualizado, aparece el texto **Clicked** justo encima de la cantidad de satoshis.

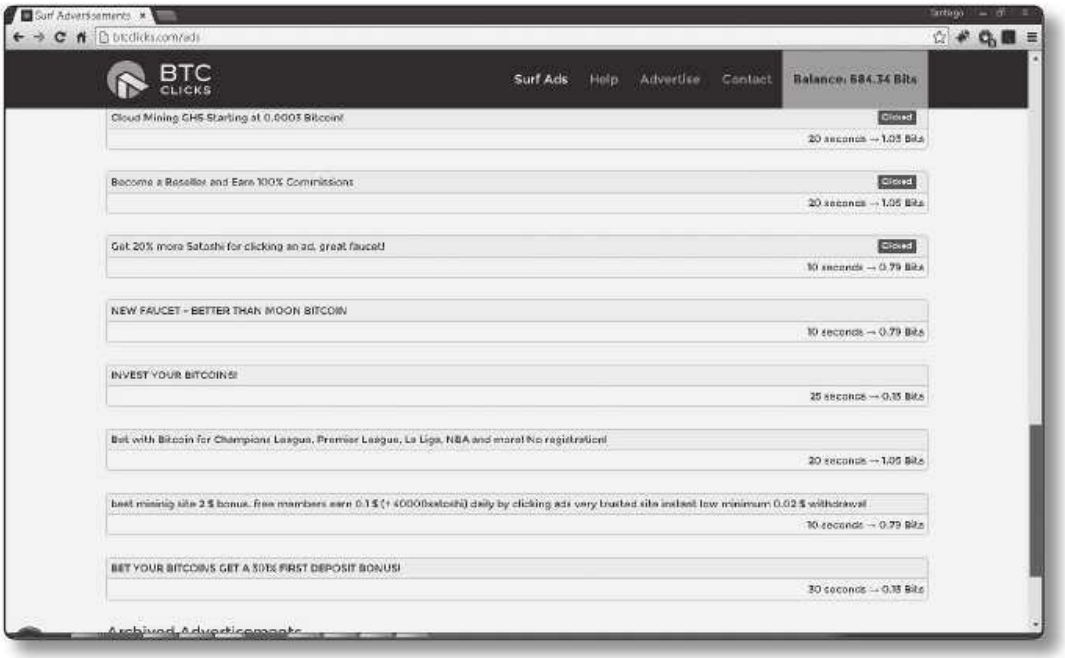


Figura 3.69. Ganando satoshis en btcclicks.com

Y poco más, solo resta hacer clic sobre cada enlace. Se abrirá una nueva página con el contenido de la misma y un contador del tiempo marcha atrás, que nos avisa cuando habremos ganado los satoshis indicados. En todos los casos y para evitar que sea un robot el que se encuentre haciendo este tipo de tareas de navegación, se nos pedirá resolver otro **CAPTCHA** de diverso tipo:

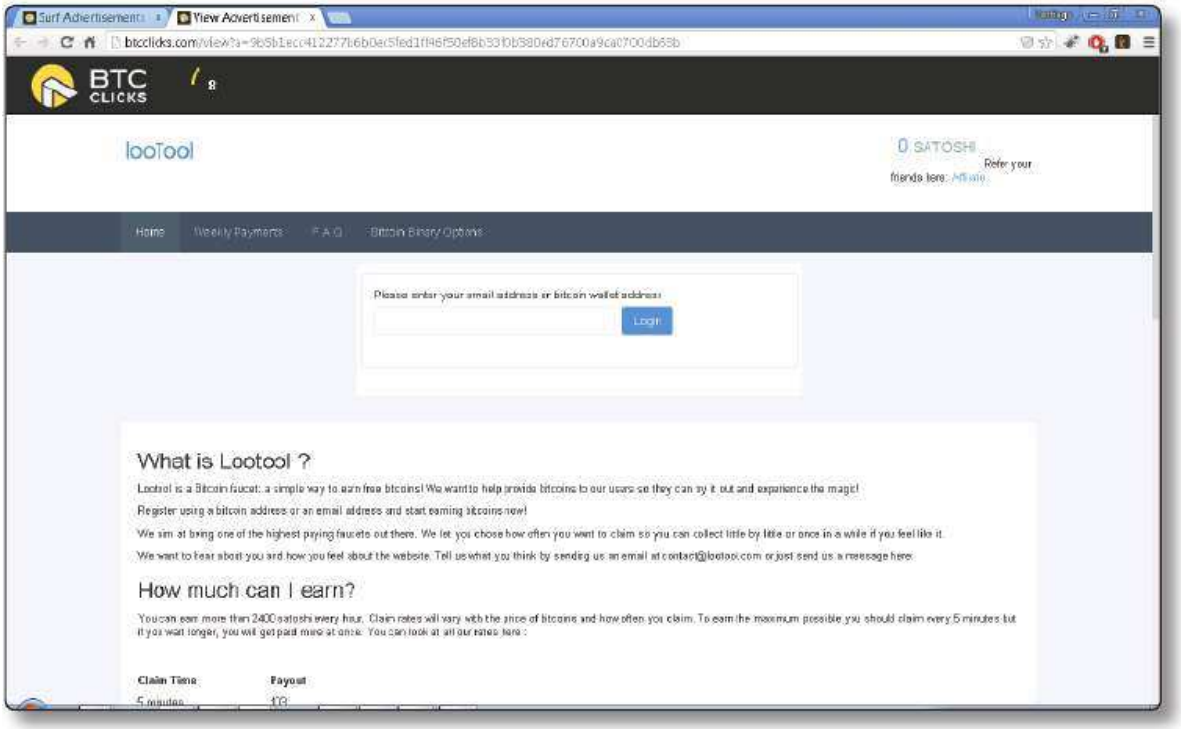


Figura 3.70. Esperando por el contador

Bitsforclicks.com

Bitsforclicks.com, anteriormente **Coinad.com**, siempre ha sido una de las webs famosas por ser de las que más cantidad pagaban con el visionado de publicidad, y lo cierto es que hasta la fecha no ha demostrado que esto no sea verdad y personalmente nunca he tenido problemas con ellos. El funcionamiento de bitsforclicks.com es muy similar al de btcclicks.com, y previo proceso de registro, tendremos una lista de anuncios que se actualiza cada 24 horas. Veamos cómo funcionaría:

Pasos:

1. Nos registramos en la web utilizando el formulario habilitado, no olvidéis introducir una dirección pública de la billetera que más os guste, que será donde recibiréis el dinero:

Figura 3.71. Registro en bitsforclics.com

2. Una vez hecho el registro, en la sección **View Ads** tendremos la lista de anuncios a visualizar:

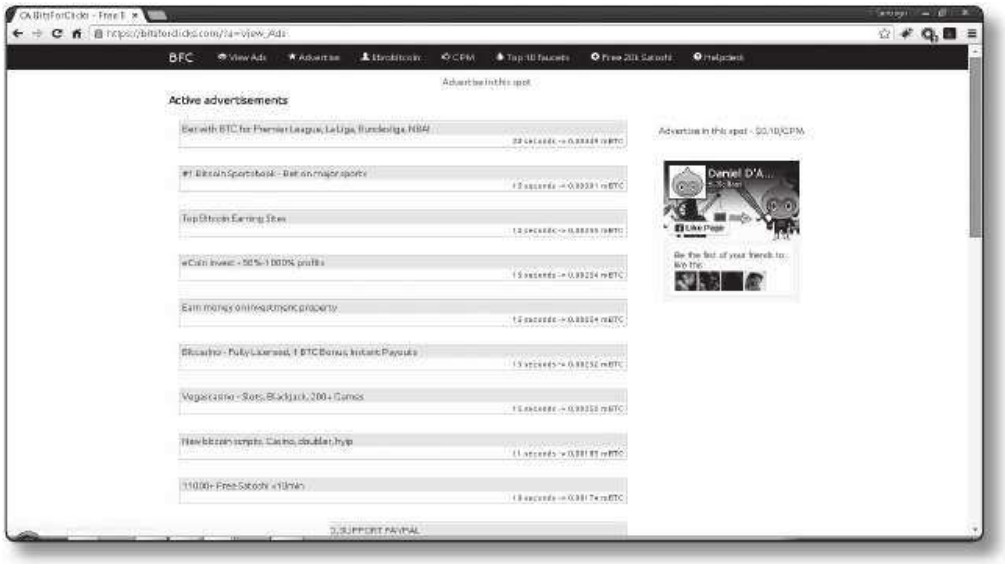


Figura 3.72. Lista de anuncios de bitsforclicks.com

3. Pulsamos sobre el anuncio y seguimos las instrucciones, que como antes puede ser o bien resolver un CAPTCHA o esperar una cierta cantidad de tiempo.

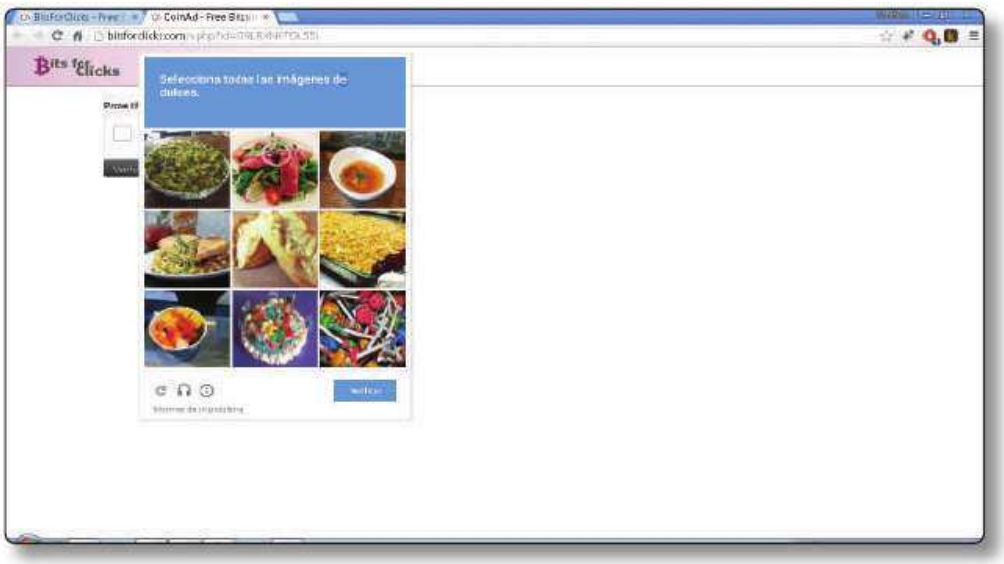


Figura 3.73. Ganando en bitsforclicks.com

Ya solamente nos queda recibir el dinero en nuestra billetera. En la parte superior de la web, al registraros tendréis una pestaña adicional con vuestro nombre de usuario, que al pulsarla nos lleva a una página donde podremos actualizar nuestra dirección pública y ver el estado de las transacciones que hayamos recibido.

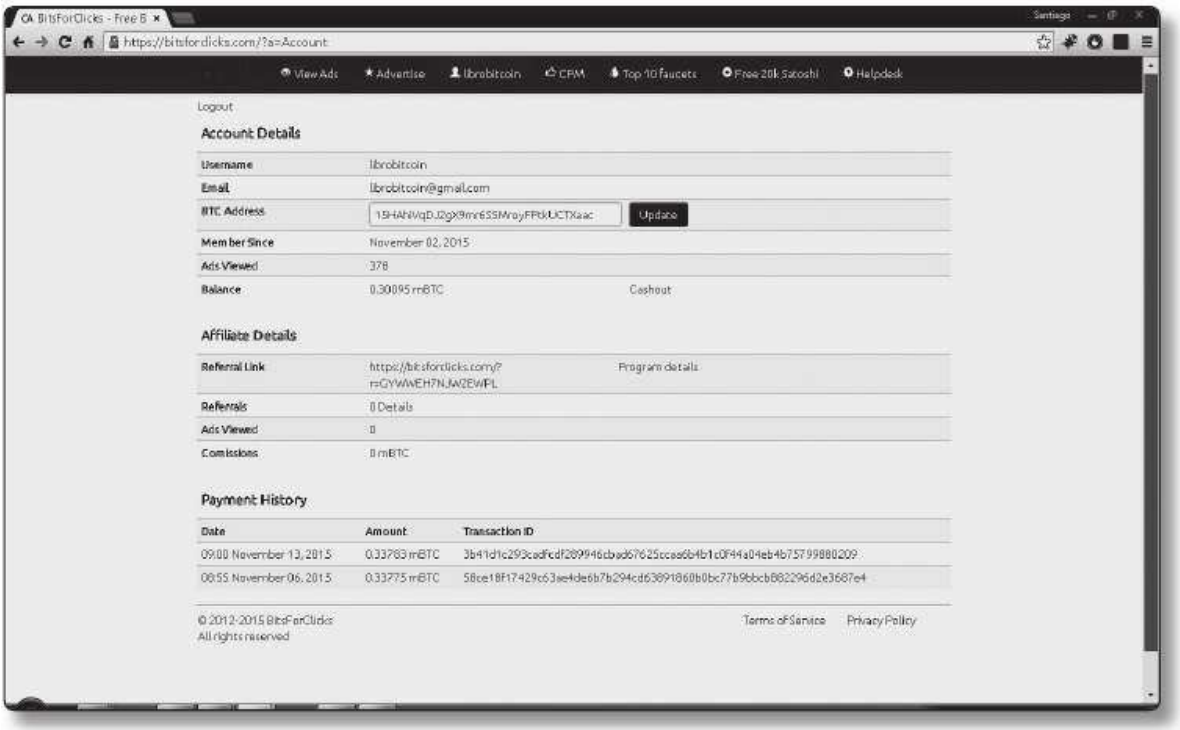


Figura 3.74. Retirando dinero en bitsforclicks.com

Bitvisitor.com

De los tres ejemplos de *faucets* que estamos comentando, bitvisitor.com es el más sencillo si cabe de utilizar, porque a diferencia de btcclicks.com o de bitsforclicks.com, no necesita registro, basta con introducir nuestra dirección Bitcoin para que la web lleve el control automáticamente del dinero que llevamos recolectado, hecho que sucede cada 60 bits (60 x 100 = 6.000 satoshis, no lo olvidéis).

Figura 3.75. Bitvisitor.com

Como podéis apreciar por la imagen, lo único que tenemos que hacer es introducir nuestra dirección Bitcoin en el cuadro de texto que la página nos proporciona y pulsar el botón **Submit**.

Figura 3.76. Recolectando en bitvisitor.com

Generalmente el tiempo que una página de bitvisitor.com necesita estar activa en nuestro navegador suele ser mayor que en los dos anteriores, unos cinco minutos, pero la recompensa es un poco mayor también. Fijaos en que al visualizar la página web, el **Balance** se va actualizando sin que tengáis que hacer nada.

Figura 3.77. Marcha atrás en bitvisitor.com

Utilizando estos tres *faucets*, en unos pocos días si sois constantes tendréis una pequeña cantidad de Bitcoines con los que poder jugar y experimentar todo lo que estamos viendo. En Internet hay muchísimos *faucets* más, con un poco de tiempo y a base de prueba y error, es probable que encontréis otras fuentes alternativas.

Pero antes de seguir, quiero haceros un pequeño aviso…

3.4.1.4 EL PELIGRO DE LOS HYIP

Entiendo que ver la publicidad de los grifos no significa que vayamos a dejarnos llevar por ella, sin embargo, quiero haceros una advertencia antes de seguir y hablaros de lo que se denomina **HYIP**, por si acaso os veis tentados a entrar en alguna de estas webs, luego no digáis que no se os dijo.

¿A qué me estoy refiriendo? Cuando estamos visionando la publicidad de los *sites* que el grifo nos propone, hay que tener cuidado en no caer en la trampa de los propios anuncios. Intento explicarme. Muchas de las webs que se anuncian en los grifos intentan captar la atención de los incautos navegantes con mensajes del estilo siguiente: "invierte X dinero y obtén una rentabilidad Y" o "multiplica tus Bitcoines en 1 día" o cosas similares. Tener en cuenta que el "Y" que siempre prometen es algo desorbitado y absurdo. Los rangos posibles son muy variados (así como el tiempo para conseguirlo) pero suelen prometer rentabilidades del 200% e incluso superiores (he llegado a ver hasta más del 1.200%) en períodos de menos de 90, 60 o incluso 30 días, eso sin contar las ofertas a 1 o 2 días.

Estas webs reciben el nombre de **HYIP o High Yield Investment Program o Programa de Inversión de Alta Rentabilidad** y hay que ser especialmente cuidadoso, porque se basan en estafas piramidales (o esquemas Ponzi, que aunque presentan algunas diferencias con estas, más o menos tienen un funcionamiento similar) en la mayor parte de las ocasiones. Por poner un ejemplo sacado del mundo real (que no del virtual), en España seguramente os sonará el caso de Afinsa y el Fórum Filatélico, acusados de operar siguiendo un esquema piramidal.

Por resumirlo muchísimo: una estafa piramidal consiste en prometer unas rentabilidades superiores a lo que el sentido común dicta, y basan su potencia en su capacidad para captar capital de los incautos que se suman a ella. Lo que se hace es pagar los desorbitados intereses que prometen usando las aportaciones iniciales de las últimas personas que se han sumado a la iniciativa. Es habitual, que cuando nos incorporamos a una de estas estafas, se nos aliente a que propongamos a nuestros contactos que hagan lo mismo. Cuanto antes te das de alta en el sistema, y más crece la base de usuarios por debajo de ti, más posibilidades hay de que obtengas los rendimientos prometidos. Obviamente el sistema acaba colapsando y nadie (o muy pocos, tal vez los primeros que se incorporan) cobra ni un céntimo de lo prometido, salvo el incitador del sistema.

La mayor parte de estas webs de tipo HYIP suelen tener un diseño muy atractivo y profesional, y han dejado atrás el tiempo en donde eran páginas poco trabajadas y que se las veía venir desde lejos. Ahora es muy común que aparezcan con nombres que dicen estar registrados como empresas en algunos sitios (muchos de dudosa credibilidad como las Islas Barbados o las Islas Caimán) y que tienen inversores de alto nivel, que con un gran conocimiento de los mercados (de tipo FOREX y demás) son capaces de generar semejantes rendimientos.

El auge de este tipo de webs ha sido tan elevado, que han surgido los denominados **HYIP Monitors**, webs en donde los usuarios que están registrados en los HYIP pueden valorar su experiencia y la capacidad de los mismos para cumplir con lo que prometen; sin embargo, no es raro tampoco que aparezcan denuncias sobre la validez de los resultados de los HYIP Monitors y su manipulación por parte de los HYIP.

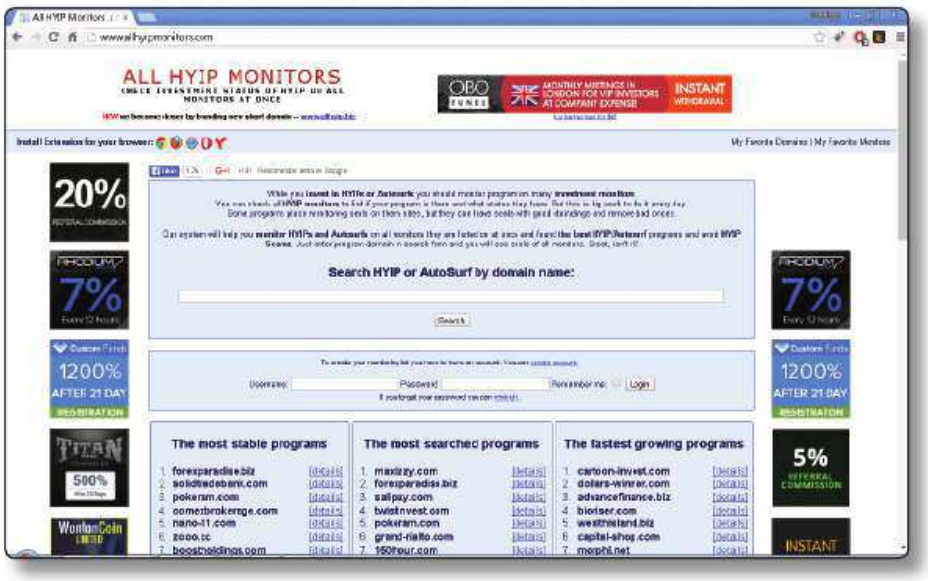


Figura 3.78. All HYIP Monitor, un agregador de monitores popular

Vuelvo a repetir e insisto, hacerse rico rápidamente puede resultar tentador usando estos sistemas, pero no es más que el viejo truco de la martingala de la ruleta de los casinos en su versión siglo XXI.

3.4.1.5 PAGO POR MI TRABAJO

Probablemente la opción que menos nos complicaría la vida sea esta, hacer un trabajo y que alguien nos pague por ello, pero claro, ¿dónde encontramos a alguien que me pague por hacer algo que le interese y además usando Bitcoines? Lo ideal sería, aunque para esto aún quedan unos cuantos hitos por cumplir, que fuera nuestra nómina la que percibiéramos en Bitcoines, de este modo sería por nuestra actividad profesional normal por la que los obtendríamos. Ni que decir tiene, en el caso de que esta opción llegara a popularizarse en algún momento, que probablemente el valor de la moneda se incrementaría exponencialmente debido a la demanda, pero dado que el valor de Bitcoin sigue siendo muy volátil y su aceptación incierta, no creo que en el medio plazo suceda.

A medida que Bitcoin se populariza es más fácil encontrar a gente dispuesta a pagarte en Bitcoines, y eventualmente cuando Bitcoin esté extendido y aceptado globalmente, no me cabe la menor duda de que será el mecanismo estándar de efectuar transacciones, pero mientras ese momento llega, tendremos que buscar alternativas. Una ya la hemos explicado, sería hacer el trabajo de visionado de webs en los *faucets*, esto nos reportará unas pequeñísimas cantidades de dinero pero para empezar por algún lado no está mal.

Tal vez más motivadora es la opción de la web **taringa.net**, que permite desde este mismo año cobrar en Bitcoines por la publicación de contenido en la plataforma. A través de lo que llaman **Taringa Creators**, los usuarios deben tener una billetera abierta en Xapo (lógico, puesto que Xapo también es argentina) para poder recibir los Bitcoines que obtienen en concepto de **Revenue Share**. Básicamente, lo que hace Taringa es en base a la popularidad de un *post* y los ingresos generados por publicidad con estos, al autor le asigna automáticamente una porción de las ganancias obtenidas. Un modelo que no creo que tarden otros muchos en copiar, sobre todo si lo que se quiere es tener contenido de calidad.

ENTONCES…

Taringa.net es una red social argentina creada en 2004. Tiene mucha difusión en el mundo hispanohablante, con más de 105 millones de visitantes y creciendo.

Finalmente, hay varias webs que en los últimos meses han ganado cierta relevancia precisamente porque se encargan de aglutinar ofertas de empleo que tienen como característica común que el pago se realiza en Bitcoines. Las más conocidas son **coinality.com**, **xtbfreelancer.com**, **cryptogrind.com** y **bitcoin-Vacancy.com**; pueden ser una alternativa a tener en cuenta, echadles un vistazo y me contáis que tal os fue.

Figura 3.79. Coinality.com, trabajo por Bitcoines

3.4.2 Otros métodos

Aparte de los métodos anteriormente descritos, durante los dos últimos años, una ristra nueva de posibilidades se ha sumado para poder conseguir Bitcoines; señalemos aquellas que por su interés merecen la pena tenerlas en cuenta:

3.4.2.1 CAJEROS BITCOIN

El pistoletazo de salida a los cajeros automáticos Bitcoin se produjo en Canadá, en la cafetería **The Waves de Vancouver**, donde se montó el primero de ellos. Desde entonces, el número de cajeros en el mundo que permiten cambiar dinero fíat por Bitcoines no ha hecho sino crecer.

ENTONCES…

Un momento curioso de esta expansión ocurrió en el año 2015 en Grecia. Cuando no se sabía qué pasaría con el Gobierno heleno y su situación respecto a Europa, la empresa BTCGreece anunció que instalaría más de 1.000 cajeros en todo el país para atender a las demandas de dinero que pudieran darse ante un más que previsible corralito griego.

Los cajeros Bitcoin son el equivalente en el mundo de las criptomonedas a sus parientes los cajeros tradicionales de toda la vida. El funcionamiento de estos cajeros suele ser sencillo para el usuario, que no requiere de grandes conocimientos técnicos para utilizarlos; de hecho, si se está familiarizado con los conceptos que hemos explicado antes, no hay que saber mucho más.

En general, el usuario antes de usar el cajero tiene que registrarse; aquí en función de la configuración elegida, los requisitos de registro pueden ser más o menos exhaustivos, pudiendo incluso pedirte que escanees una copia de tu documento de identidad (los cajeros proveen en su hardware los medios para poder hacerlo *in situ*), requisitos que se ponen por cumplir la legalidad vigente. Dado que las operaciones en el cajero requieren de una segunda clave de autorización que se envía por SMS al móvil, aseguraos de no introducirla mal y de que vuestro operador deja pasar todo tipo de SMS, a veces esto no ocurre y podéis llevaros una desagradable sorpresa al no poder acceder a vuestros fondos simplemente porque no llegó el mensaje.

Finalizado el proceso de registro, la operativa siempre es la misma, cambiar euros por Bitcoines. Esto se hace introduciendo el/los billete/s en la ranura del cajero que nos muestra los precios de compra actuales con los que trabaja y la comisión correspondiente; después de aceptar la operación, se produce la conversión y tenemos el dinero en nuestra billetera. En general los cajeros suelen disponer de sus propias billeteras accesibles vía web o por clientes para móvil, mover los fondos desde estos a otra billetera de nuestra elección es igual a lo visto hasta este momento.

Ejemplos de este tipo de cajeros son **Lamassu** y **Robocoin**.

ENTONCES…

En Madrid estuvo instalado un **Lamassu** en el restaurante **DoEat** de la calle María de Molina, luego se movió al **ABC Serrano** y ahora mismo no sé exactamente dónde se encuentra. Un cajero **Robocoin** también estuvo disponible en el hotel **One Shot Hotels** de Recoletos durante algún tiempo; mis últimas informaciones indican que a la fecha de salida de este libro probablemente no esté ubicado allí.

Figura 3.80. Cajero Robocoin

Otra de las posibilidades de compra es usar servicios de empresas que tienen acuerdos con las redes de cajeros convencionales o servicios de tarjetas prepago que se cargan con Bitcoines. Tal es el caso de **Bit2Me**, que permite recoger el dinero que se haya vendido dentro de su plataforma en cualquiera de los 10.000 cajeros tradicionales con los que tienen acuerdos en toda España.

3.4.2.2 TARJETAS

En estos casos lo habitual es que las empresas nos provean con una tarjeta electrónica que podemos utilizar para realizar nuestras compras como si de una tarjeta VISA o Mastercard se tratara. Hay muchas empresas que ofrecen este servicio, por citar algunas de las más significativas, **AdvCash**, **BitInvest**, **CoinJar**, **AnxBTC**, **MoneyPolo**, **BitPlastic**, **XMLGold**, **Bitnovo**…

Quedémonos con esta última porque analizarlas todas es imposible, pero sirve para hacernos una idea de este tipo de servicios. **Bitnovo** dispone de tarjeta prepago que podemos recargar desde direcciones Bitcoin o PayPal. Tiene un coste de 10 euros y en función del nivel de dinero que queramos cargar los niveles de seguridad son más exigentes. Para saldos menores de 250 euros no se requiere aportar documentación personal, lo que la hace muy interesante en este sentido. La tarjeta es válida para comprar en todo el mundo.

Figura 3.81. La web de Bitnovo

3.4.2.3 CASAS DE COMPRA/VENTA DESCENTRALIZADAS

El ejemplo que hemos visto anteriormente de Bitstamp es el caso típico de plataforma centralizada, donde todas las operaciones suceden en el interior de los servidores de Bitstamp. Si mañana esta empresa o alguna de sus primas hermanas (Coinbase, etc.) sufriera un ataque o bloqueasen el acceso a sus servidores por cualquier motivo, el dinero que tuviéramos en ellas quedaría comprometido como sucedió con Mt. Gox. Para evitar esta situación, se ha llevado la descentralización también a las casas de cambio con dos ejemplos claros y muy conocidos dentro del mundo Bitcoin:

- **Coinffeine**

  Es una empresa española, en donde entre otros invirtió **Bankinter**. Fundada por **Alberto Gómez Toribio**, **Ximo Guanter**, **Álvaro Polo** y **Sebastián Ortega**, tuvo el honor de ser la primera empresa en constituirse con Bitcoin en el mundo, algo en lo que tuvo mucho que ver la asesoría de **Pablo Burgueño** y el bufete **Abanlex**, probablemente a donde yo me dirigiría en España si tuviera alguna duda legal sobre el uso de Bitcoin en mi negocio. Su modelo de funcionamiento es sencillo (que no su algoritmo de *matching* de operaciones interno que he tenido el gusto de

estudiar), utilizando la pasarela de pago OKPay para las conversiones entre moneda fíat (soportando las más populares) y criptomoneda; una vez que esta está en nuestra cuenta podremos abrir operaciones sobre la red distribuida para compra/venta de Bitcoines, que podrán ser atendidas por el resto de usuarios que formen parte de la red Coinffeine.

- **Bitsquare**

  Fundada por Manfred Karrer, Bitsquare sigue un modelo parecido al de Coinffeine en filosofía (conseguir una casa de compra/venta de Bitcoines), que no en implementación. Bitsquare está orientado a usuarios que ya disponen de Bitcoines, y no presenta (y no parece que vaya a tenerla) la posibilidad de cambiar moneda fíat por criptomoneda. Su software aún se encuentra en fase alfa pero puede bajarse para probarlo y conectarlo a la red de prueba (testnet).

Aunque ambos proyectos se encuentran en estados muy iniciales como para considerarlos fiables y su futuro a largo plazo puede depender de muchos factores, han puesto sobre la mesa una alternativa más que interesante que además va muy en la línea de la filosofía distribuida de Bitcoin. Otras posibilidades que estarían muy relacionadas, aunque no exactamente iguales, serían las ofrecidas por **BitHalo** o **BlackHalo**, aunque su operativa está más enfocada a los contratos digitales, tienen servicios distribuidos que a futuro podrían encajar con la compra/venta de Bitcoines de manera descentralizada. Habrá que ir siguiéndoles la pista más adelante.

3.4.2.4 JUGAR JUEGOS Y LEER LIBROS

Finalmente estas dos son las alternativas más sorprendentes para conseguir Bitcoines, pero que podríamos comparar al uso de los *faucets* que expliqué antes. Los juegos los hay de diferentes tipos, diferentes plataformas (pueden ser web, Android, iOS, etc.) y temáticas, aunque muchos se basan en el funcionamiento de otros juegos que han tenido gran éxito como son *Flappy Bird* o *Candy Crush*, por citar solamente dos de los más famosos. Habitualmente ganar fracciones de Bitcoin se consigue o bien por el avance dentro del juego o bien por la visualización de anuncios embebidos dentro de la dinámica del juego.

Algunos de los juegos más conocidos y populares son: **Coin Flapper**, **Flappy Pig**, **SaruTobi** (solo para iOS), **Bitcoin Crush**… aunque hay muchos más.

Figura 3.82. FlapPig, ganando Bitcoines jugando

En el caso de la lectura de libros, recomiendo que le echéis un vistazo a **paidbooks.com**, que dispone de un sistema en donde puedes acceder a su librería y leer *in situ* cualquiera de los libros disponibles. Cada 10 minutos de lectura obtienes 4 bits (400 satoshis) en tu cuenta; el umbral de pago lo realizan una vez alcanzada la cifra de 200 bits (20.000 satoshis).

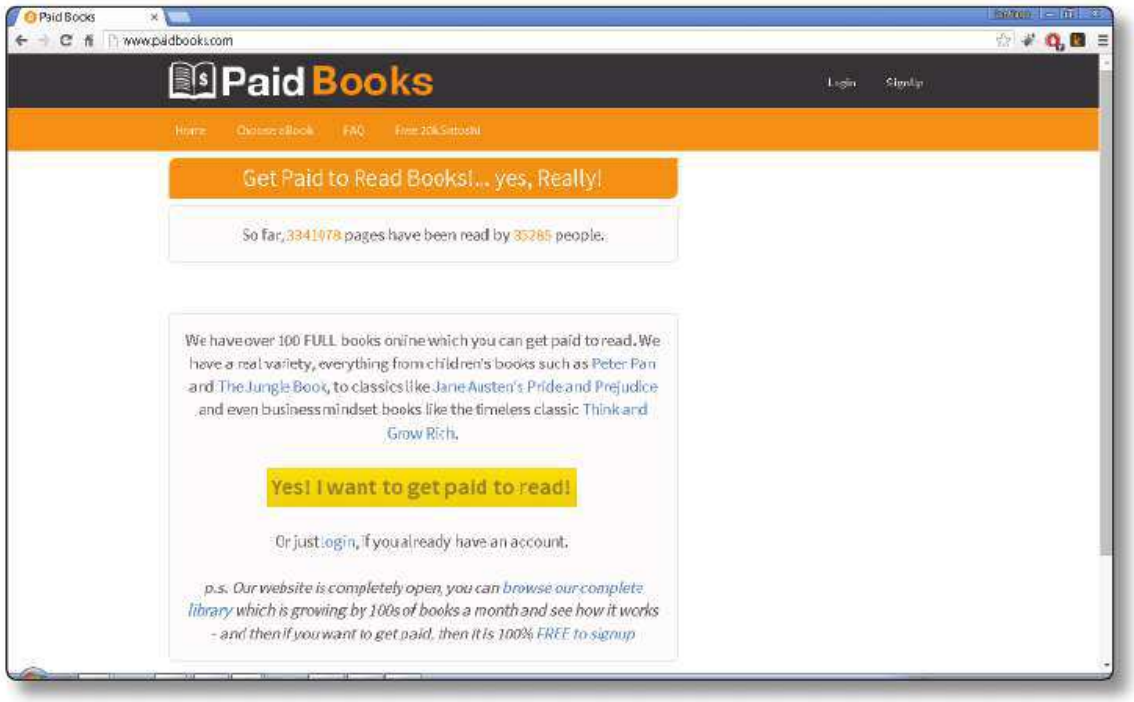


Figura 3.83. Paidbook.com, pago de Bitcoines por leer libros

Con estos dos últimos ejemplos, dejamos listos los medios para obtener Bitcoines y calentamos motores para la criptografía, pero antes, unos consejos para proteger nuestro dinero…

3.5 ASEGURANDO NUESTRO DINERO

He dicho en muchas ocasiones y lo diré otras cuantas más antes de que acabemos el libro, que Bitcoin es software experimental, con un prometedor futuro sin duda, pero aún estamos dando nuestros primeros pasos, y las incógnitas están a la vuelta de cada esquina. Conviene ser cautos y tomar algunas precauciones; sirva este último punto como resumen de lo que debemos siempre hacer.

1. Cuando vayamos a comprar Bitcoines, como cualquier otro tipo de inversión, solamente invertir la cantidad que podamos permitirnos en el peor de los casos perder; si mañana desaparece del mapa que nuestras finanzas no estén comprometidas. Como dicen los inversores, no meter todos los huevos en la misma cesta.

2. Del mismo modo, la alta volatilidad de Bitcoin no lo hace el mecanismo ideal para ahorrar; si tenemos una confianza ciega en su futuro podríamos pensarlo como una alternativa más donde poner una parte de nuestros ahorros, pero no es la mejor opción; para especular sin embargo, con esta alta volatilidad hay muchas oportunidades.

3. En el caso de hacer trading solo operar con los que nos resulten de fiar y nunca dejar cantidades muy grandes en ello durante mucho tiempo.

4. Empieza a trabajar en serio cuando estés seguro. Los *faucets* son un medio estupendo para conseguir fracciones pequeñas de Bitcoin que aunque no te van a permitir hacerte rico ni comprar nada, sí que te van a ayudar a familiarizarte con los conceptos anteriores. Cuando tengas soltura en enviar y recibir dinero y veas que no es complicado y domines la técnica, será hora de comprar Bitcoines en una plataforma de *trading* y dar un paso más lejos.

5. **Utilizar solamente aquellos monederos que sean confiables**. Cualquiera de los que hemos visto son una buena alternativa, sin embargo las billeteras web delegan parte del control de nuestro dinero en ellas, y si no somos precavidos una eventual caída de sus servicios puede dejarnos sin acceso a nuestro dinero. No uséis monederos de páginas web extrañas

o que no podáis verificar su origen, siempre es mejor echar un vistazo al software propuesto desde la página del proyecto Bitcoin, donde están las opciones más seguras.

6. **Hacer copias de seguridad de nuestra billetera**, en diferentes formatos y ubicaciones. Puede sonar paranoico pero yo lo comparo con el código fuente de un programa. No hay nada que me duela más que perder código que he estado desarrollando durante días por un fallo del disco duro; imaginaos si en vez de código es dinero…

7. **Las claves de acceso que utilicemos deben ser seguras**, más adelante en el capítulo 4 hablaré un poco más de esto. Procurar no cometer errores de principiantes, las medidas de seguridad que tomas en la contraseña de tu correo deberían ser las mismas en este caso. Y aunque es obvio nunca las reveles a terceros.

8. **Habilitar siempre que se pueda la confirmación de doble factor**. Este doble factor puede ser un correo electrónico que nos pide confirmar una acción o bien un SMS o usar Auth, o cualquier otro mecanismo que la billetera nos proporcione.

9. **Cuidado con las páginas que prometen altos rendimientos** y retornos de inversión desorbitados, he hablado de ellas antes, pero insisto, los euros a 90 céntimos no existen.

10. Cuando tengamos cierta cantidad de Bitcoines que sea importante, mantenerla en una **billetera fuera de línea que se encuentre en un lugar seguro**. Utilizar una billetera con pequeñas cantidades de dinero que podamos necesitar para nuestro día a día y que iremos recargando desde la *offline* según vayamos necesitando.

11. **Dividir el dinero en varios monederos** es una de las mejores opciones que tienes para mantenerlo a salvo. Igualmente utilizar siempre diferentes direcciones para diferentes transacciones, no cuesta nada crearlas y es más fácil mantener nuestro anonimato en la red Bitcoin.

12. **Mantente actualizado**. Bitcoin es experimental, el software de las billeteras sufre cambios de manera muy habitual. Si no estás actualizado no estarás seguro de que no se aproveche alguna vulnerabilidad encontrada.

Creo que si sigues estas recomendaciones los cacos que codicien tus Bitcoines lo van a tener un poco más difícil. Nos vemos en el siguiente capítulo, ahora sí, la criptografía llama a nuestras puertas, pero lo va a hacer de manera que no nos dolerá la cabeza con ella, en serio; echad un vistazo al capítulo y luego me decís.

4

CRIPTOGRAFÍA DE CLAVE PÚBLICA

Si has llegado hasta aquí, enhorabuena, ahora mismo deberías ser capaz de trabajar con Bitcoin sin demasiados problemas, y se puede decir que conoces lo que un usuario estándar debería conocer para trabajar en su día a día. No obstante, lo que hemos visto hasta el momento no es más que la punta del iceberg, detrás de Bitcoin hay todo un universo de reglas y algoritmos, que se materializan en el protocolo Bitcoin, y que permiten que la magia anterior suceda.

Y parte de esa magia tiene que ver con la **criptografía de clave pública**, sin ella nada de lo que estamos contando podría llevarse a cabo. Sin embargo, la criptografía de clave pública no pertenece ni está restringida solamente al ámbito de Bitcoin o de las criptomonedas en general. Cada vez que utilizamos un navegador y nos conectamos a la web de nuestro banco, compramos un billete de avión, reservamos una habitación o realizamos las cada vez más abundantes gestiones con la Administración Pública, a través de las diferentes sedes electrónicas facilitadas para tal efecto, la criptografía de clave pública está funcionando sin que nos demos cuenta.

Y es que todas estas operaciones generalmente involucran el movimiento de datos de carácter personal y la realización de transacciones económicas, y es fundamental que puedan llevarse a cabo del modo más seguro posible, máxime si cabe cuando estos intercambios se realizan sobre un canal por naturaleza inseguro como es Internet. Y es que nos guste o no nos guste, Internet originariamente nació como un lugar para compartir información y facilitar el acceso, justo lo contrario de lo que luego sucedió, los protocolos y medidas de seguridad es algo que vino *a posteriori*, y hubo que ingeniárselas, a veces con soluciones que tal vez no hayan sido las óptimas para lograrlo. No deja de ser curioso ver como tecnología que no es precisamente nueva ha sido combinada para crear algo tan novedoso como Bitcoin.

ENTONCES…

El protocolo HTTP (*Hypertext Transfer Protocol*) es un protocolo sin estado, esto significa que cada petición que realiza se trata como una transacción independiente que no tiene relación con ninguna anterior. Esta situación se soluciona con el uso de las *cookies* y de las variables de sesión en el servidor. Actualmente la versión activa es la 1.1 aunque existe una revisión de 2012 HTTP/2, y probablemente a partir de 2016, comencemos a verla en funcionamiento.

Por otro lado, la mayoría de los conceptos criptográficos que sustentan Bitcoin fueron formulados desde 1970 hasta finales del siglo XX. Satoshi ha sabido combinarlos para crear un explosivo cóctel, ¿no os parece?

En este capítulo vamos a adentrarnos en este apasionante mundo, pero vamos a hacerlo de un modo que resulte sencillo de entender, que nadie se asuste antes de empezar; para ello remontémonos un poco en el tiempo y hagamos algo de historia.

4.1 INTRODUCCIÓN A LOS MÉTODOS DE CIFRA Y LA CRIPTOGRAFÍA

La necesidad de guardar secretos y alejar de miradas indiscretas cierto tipo de información no es algo del siglo XXI y se puede decir que ha sido un problema recurrente a lo largo de toda la historia de la humanidad. El significado de la palabra **criptografía** es en sí mismo interesante; si nos vamos al diccionario, la palabra proviene del griego, de la unión de otras dos palabras: **krypto** o esconder y **grapho** o escribir, es decir, la criptografía trata o según algunos sería el arte de la escritura secreta, aunque sería más correcto decir que la criptografía se ocupa del diseño de cifras, entendiendo por cifra un método secreto de escritura. Y aunque estos métodos involucran muchas cosas, generalmente se resumen en la definición de protocolos y algoritmos que doten de seguridad a las comunicaciones, a la información y a las entidades que se comunican.

El proceso contrario al diseño de cifras es el **criptoanálisis**, y su objetivo es romper las cifras y tratar de llegar al texto en claro original.

Aunque resulte de cajón, el mecanismo mediante el cual un texto en claro se transforma en un texto cifrado se llama cifrado y al proceso contrario, transformar un texto cifrado en un texto en claro, descifrado. Para poder ir tanto en un sentido como en el otro, necesitaremos hacer uso de claves criptográficas, claves que podrán ser privadas o públicas, como seguidamente veremos y que sirven para clasificar los métodos de cifrado. Este conjunto de acciones que se realizan para cifrar o descifrar, utilizando un tipo de clave (del tipo que sea), se denomina generalmente como criptosistema.

4.1.1 Un poquito de historia

Como casi muchas cosas en la historia de nuestra civilización, los desarrollos de ciertas disciplinas han tenido un origen meramente militar, político o diplomático, siendo la criptografía una de esas ciencias nacidas al calor de este tipo de situaciones.

El primer método de criptografía que está documentado es del siglo V a. C., y se conocía con el nombre de escítala, y era utilizado por los espartanos. Era un sistema ingenioso, que consistía en dos varas del mismo grosor (casi todos los diseños de algoritmos de la antigüedad se basan o en diseños geométricos o en artilugios mecánicos) y una tira de cuero. Cada una de las varas estaba en manos de los participantes de la comunicación, de modo que lo que se hacía para enviar un mensaje era enrollar la tira de cuero en forma de espiral sobre un bastón, y se escribía sobre la tira el mensaje longitudinalmente. Al desenrollar la tira, solamente había un conjunto de letras sin sentido. El mensaje viajaba al receptor, que haciendo uso de la vara gemela, volvía a enrollar la tira en ella, y podía leer el mensaje original.

Una pregunta, ¿cuál es en este caso la clave secreta del sistema de cifrado? Pues muy simple, ni más ni menos que el bastón que enrolla y desenrolla la tira, no vale cualquiera, tiene que ser uno del mismo grosor para que al desenrollar pueda leerse el mensaje.

Figura 4.1. Ejemplo de escítala (fuente: Wikipedia)

Es también muy conocido el sistema de cifrado de nombre **cifrado de César**, y que recibe este nombre porque era usado, supuestamente, por Julio César durante sus campañas. Con un esquema de funcionamiento muy simple, que consiste en reemplazar una letra por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto. Ejemplo con un desplazamiento de 3 (el número usado por César), la frase "LIBRO DE BITCOIN" quedaría transformada en el texto cifrado "OLEUGHELWFRLQ", donde la "L" se sustituye por la tercera letra siguiente a la "L" en el alfabeto, es decir la "O", la "I" por la tercera letra siguiente a la "I" en el alfabeto, es decir, la "L" y así sucesivamente con todo el mensaje que queremos

cifrar; al llegar a la letra "Z" se vuelve a comenzar por el principio del alfabeto (alfabeto cíclico). El sistema de cifrado de César es un sistema muy sencillo de romper, incluso usando fuerza bruta y probando todas las posibles variaciones; sin embargo hay que poner en perspectiva la época en la que se utilizó y probablemente el analfabetismo ayudó a que la fortaleza del cifrado fuera aún mayor. En este caso, la clave es el valor del desplazamiento utilizado sobre el alfabeto (llamémosle k), y por tanto es también una clave simétrica, si conozco el valor de k, puedo hacer el proceso contrario y volver al texto original.

Con estos dos ejemplos tan sencillos, podemos hacer una primera clasificación de los sistemas de cifrado. El primer ejemplo que hemos puesto es lo que se conoce como cifrado por transposición mientras que el de César sería un ejemplo de cifrado por sustitución. Se llama de transposición porque cada carácter que compone el texto en claro se cambia de posición siguiendo un esquema fijo y conocido, mientras que en el de sustitución lo que se hace es cambiar cada carácter del texto en claro por otro (del mismo alfabeto o de otro).

ENTONCES…

También importa mucho el número de alfabetos que se esté utilizando, si solamente se utiliza un único alfabeto se habla de **cifrados monoalfabéticos** y si se usa más de uno, **cifrados polialfabéticos**. Para que lo entendamos fácilmente, si para cifrar un texto en español, solo uso las letras del español estaríamos en el primer caso, si uso además de las del español, las del ruso, estaríamos en el segundo caso. Ejemplos del primer tipo serían el **cifrado afín** y el **fracmason**, y del segundo, el cifrado **Alberti**, el **Vigenere** y el **Vernam**.

No obstante esta clasificación, no sería más que una subclasificación dentro de otra más amplia, actualmente los sistemas criptográficos se dividen en dos grupos:

- **Criptosistemas simétricos o de clave privada**: son aquellos que emplean una misma clave tanto para cifrar como para descifrar un mensaje (los anteriores estarían dentro de este grupo, por eso de hablar de subclasificación). El mayor inconveniente que presentan es que para ser utilizados la clave debe estar en posesión tanto del emisor como del receptor, lo cual nos lleva a preguntarnos cuál es el mejor modo de transmitirles a los participantes en la comunicación esa clave de forma segura.

- **Criptosistemas asimétricos o de clave pública**: estos emplean una doble clave, denominadas como **clave privada** y **clave pública**. Una de ellas sirve para la transformación o función de cifrado y la otra para la transformación de descifrado. Es decir, empleamos una para cifrar y la otra sirve para descifrar. Cumplen que el conocimiento de la clave pública no permita calcular la clave privada, y son ideales para establecer comunicaciones seguras por canales inseguros puesto que únicamente viaja por el canal la clave pública, que solo sirve para cifrar, o para llevar a cabo autenticaciones. Sin la clave privada un observador no autorizado será incapaz de descifrar el mensaje cifrado.

¡ATENCIÓN! Un concepto importante. Tanto la criptografía de clave simétrica como la asimétrica se consideran funciones unidireccionales, porque los procesos de cifrado son fáciles de hacer, pero muy difíciles de revertir. Dicho de otro modo, la complejidad computacional de ir desde el texto en claro al cifrado es rápida, eficiente y barata, pero el proceso contrario, ir desde el texto cifrado al texto en claro, no es ni rápido, ni eficiente ni barato.

Esto de las funciones unidireccionales es muy importante, hay otro tipo de función que nos interesa para Bitcoin, la **función hash** que también reúne esta característica de ser unidireccional y que hace lo mismo, funciona muy bien en un sentido, pero es terriblemente complicado deshacer lo hecho previamente. En seguida lo contamos.

4.1.2 Ataques de fuerza bruta y ataques de diccionario

Seguro que esto de los ataques de fuerza bruta y de diccionario también lo has oído muchas veces, veamos las diferencias entre uno y otro. El ataque de fuerza bruta consiste en encontrar la clave secreta de un algoritmo de cifrado probando todas las posibles combinaciones hasta dar con la correcta, lo que se va haciendo es ir variando secuencialmente los caracteres que forman parte de la clave que vamos a probar hasta que acabamos dando con la correcta.

Los ataques de diccionario son una evolución de los ataques de fuerza bruta, y aprovechan el hecho conocido de que muchos usuarios utilizan para formar la clave privada una palabra conocida de su idioma (o en su defecto de otro) que les ayude a recordarla. En este caso lo que se hace es hacer pruebas usando el diccionario para tratar de encontrar la clave.

Actualmente con la llegada de los ordenadores, los algoritmos de cifrado deben garantizarnos que no es posible realizar ataques de este tipo y que el coste computacional necesario para hacerlos es tan abrumador que si bien teóricamente un algoritmo podría ser roto usando fuerza bruta o el uso de un diccionario, llegar a hacerlo supone tal cantidad de tiempo que cuando se consiga, la validez del descifrado carezca de sentido. Por ejemplo, si descifrar un correo electrónico cifrado tarda computacionalmente en hacerse 100 años, aunque el algoritmo pueda ser atacado por fuerza bruta, eventualmente se puede considerar seguro.

Pensad que la gracia de los sistemas de cifrado está en mantener segura la clave, no el algoritmo utilizado que suele ser público. El que los algoritmos sean públicos implica que mucha más gente puede probarlos y experimentar con ellos y encontrar deficiencias. Como usuarios solamente debemos preocuparnos de dos cosas: mantener segura la clave y que esta sea de una longitud suficientemente grande y pueda considerarse fuerte. Con estas dos simples recomendaciones, los ataques de fuerza bruta o diccionario dejan de ser viables, y si se combinan con mecanismos que controlen el número de intentos de acceso al sistema, los posibles intrusos lo tendrán más que difícil para poder acceder a la información.

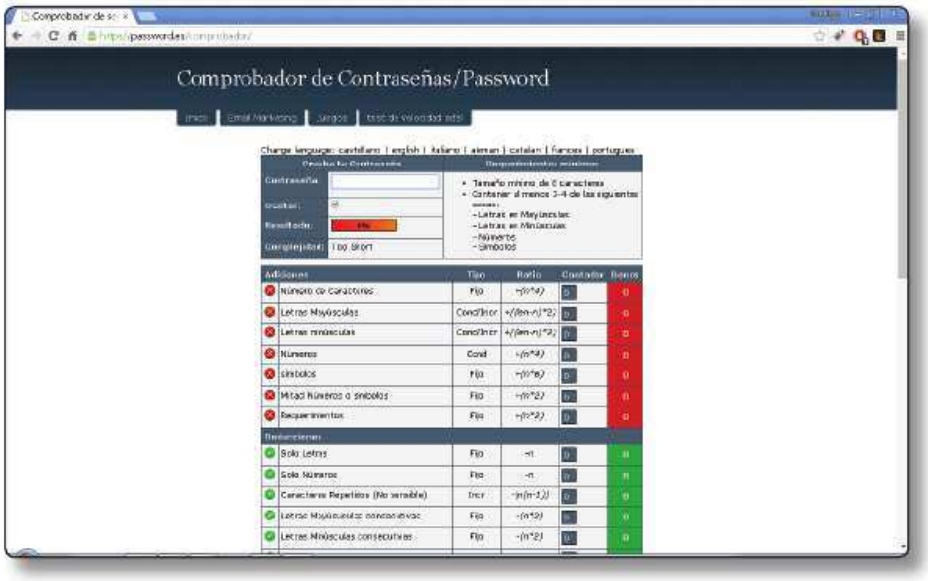


Figura 4.2. Comprobando la seguridad de nuestra clave

En el caso de Bitcoin, siempre debemos asegurarnos de que las claves que protegen nuestra billetera cumplen con estas recomendaciones. Os animo a que juguéis un rato con la web **password.es** para ver la fortaleza de las claves privadas que habitualmente estéis utilizando.

Y llegamos a una de las cuestiones claves de este capítulo, ¿criptografía pero para qué?

4.1.3 ¿Qué nos garantiza la criptografía?

Esa es una buena pregunta, ¿para qué nos sirve la criptografía, qué conseguimos con ella? Independientemente de los diferentes tipos de algoritmos y técnicas criptográficas existentes, la criptografía siempre debe garantizar el cumplimiento de las siguientes propiedades que además sirven para caracterizarla:

- **Confidencialidad**: solamente los usuarios autorizados tienen acceso a la información y nada más que ellos.
- **Integridad de la información**: garantía de que la información original no será alterada, ni intencional ni accidentalmente.
- **Autenticación de usuario**: es un proceso que permite al sistema verificar si el usuario que pretende acceder o hacer uso del sistema es quien dice ser.
- **Autenticación de remitente**: es el proceso que permite a un usuario certificar que el mensaje recibido fue de hecho enviado por el remitente y no por un suplantador.
- **Autenticación del destinatario**: es el proceso que permite garantizar la identidad del usuario destinatario.
- **No repudio en origen**: que cuando se reciba un mensaje, el remitente no pueda negar haber enviado dicho mensaje.
- **No repudio en destino**: que cuando se envía un mensaje, el destinatario no pueda negar haberlo recibido cuando le llegue.
- **Autenticación de actualidad (no replay)**: consiste en probar que el mensaje es actual, y que no se trata de un mensaje antiguo reenviado.

Luego volveremos sobre esto, de momento nos basta con saber que la criptografía de clave pública que usa Bitcoin sirve para garantizar que las anteriores propiedades se cumplan; pero antes de seguir déjame que vuelva sobre una de las cuestiones que dejamos abiertas casi al comienzo de este libro. ¿Te acuerdas de que te dije que los generales tienen problemas? Vamos a ver qué significa eso.

4.1.4 Los generales también tienen problemas

En el capítulo 2, cuando estuvimos contando los desarrollos de Szabo y Wei Dai, explicamos que sus trabajos intentaban buscar a una solución a un problema típico que se produce en criptografía y que recibe el nombre de "Problema de los Dos Generales", aunque también lo podéis encontrar con los nombres de "Problema de las dos armadas", "Problema del Ataque Coordinado" o incluso "Problema de los Generales Bizantinos", todos ellos sirven para situarnos en los retos que hay que resolver cuando se quiere establecer una comunicación a través de un canal de naturaleza inseguro, como es el caso de Internet.

Voy a partir de la exposición del problema tal y como se describe en la Wikipedia porque me parece una de las mejores, es la siguiente:

Dos ejércitos, cada uno liderado por un general, se preparan para atacar una ciudad fortificada. Los ejércitos están acampados cerca de la ciudad, cada uno en una colina. Un valle separa ambas colinas, y el único modo que tienen los generales de comunicarse es mediante el envío de mensajeros por el valle. Desafortunadamente, en el valle se encuentran los defensores de la ciudad y existe cierta posibilidad de que capturen a cualquiera de estos mensajeros (enterándose y/o alterando el mensaje). Téngase en cuenta que aunque los dos generales se han puesto de acuerdo en que atacarán, no han acordado el momento de hacerlo.

Los dos generales deben atacar la ciudad a la vez para no fracasar. Deben, por tanto, comunicarse y decidir el momento oportuno. Como cada general debe saber que el otro ha aceptado el plan de ataque, y por los temores a que el mensaje original sea perdido o modificado por el enemigo (confirmación de recepción del mensaje), la coordinación entre los generales podría ser interminable sin consenso.

Este ejercicio mental implica tener en cuenta cómo se llega efectivamente a dicho consenso. En su forma más simple, un general (al que llamaremos "primer general") será el líder, el cual decide el momento del ataque, y le comunica la información al otro general. El problema consiste en llegar a un algoritmo que les permita a los generales comunicarse de manera efectiva para, así, predecir el momento exacto de la ejecución de las acciones bélicas.

En principio, y según lo expuesto, es bastante sencillo para los generales llegar a un acuerdo en lo que se refiere al momento de atacar. Es suficiente para ello un mensaje satisfactorio con una respuesta igualmente satisfactoria. La sutileza del problema de los dos generales reside en la imposibilidad de diseñar un algoritmo tal que los generales puedan usarlo para que permita llegar a la conclusión anterior.

Es más, está demostrado que no se puede encontrar una solución usando protocolos deterministas con un número limitado de mensajes ni en protocolos deterministas ni en variables de longitud, sin embargo, abordar ambas demostraciones

matemáticamente se sale del alcance de nuestro estudio (y es probable que antes de haber acabado de explicarlas hayas pasado de página). Basta con decir que todos los enfoques prácticos propuestos se basan en la imposibilidad de mitigar la incertidumbre (parece que la teoría del señor Shannon puede estar por aquí, aceptarla al menos en cierto grado y hasta un determinado nivel que se considere satisfactorio, por ejemplo suponiendo que cierto número de mensajes son válidos, aunque esto no garantizaría tampoco en última instancia un ataque coordinado.

Si recordamos las ideas propuestas por Szabo y Wei Dai, en ambas soluciones los servidores deben comunicarse entre ellos para mantener una base de datos común, y es aquí donde el problema anteriormente descrito aparece. Fijaos en que los generales tienen que acordar una estrategia para la batalla y deben comunicarse usando mensajes, pero estos mensajes pueden corromperse o alterarse, justamente algo muy parecido a lo que sucede (salvando las distancias con B-Money y bit gold) aquí. El problema en estos casos es cómo la red puede llegar a un acuerdo del estado en el que se encuentra una base de datos distribuida cuando los mensajes entre los nodos pueden ser alterados o pueden existir atacantes tratando de alterar la base de datos distribuida, y no se puede confiar en ninguna de las partes implicadas.

La solución original de B-Money de Szabo no abordó el problema de los generales hasta un artículo posterior denominado "Byzantine Quorum System" que se basaría en llegar a un consenso entre los ordenadores de la red, consenso que al aceptarse por la mayoría implicaría aceptar los cambios de la base de datos distribuida. Lo mismo que hace Satoshi Nakamoto con Bitcoin y la prueba de trabajo.

4.1.5 De la criptografía clásica a la criptografía moderna

Sigamos avanzando un poco más en el tiempo, para ir situándonos mucho más cerca de lo que realmente importa para Bitcoin. Generalmente se acepta como válido que todos los sistemas de cifrado anteriores a 1949 estarían dentro de lo que se conoce como sistemas de cifrado precientíficos, carecían de un análisis formal de los métodos y técnicas que los sustentaban, y no fue hasta el siglo XX cuando se formalizaron matemáticamente. A estos sistemas precientíficos también se los clasifica a veces como sistemas de criptografía clásicos.

ENTONCES…

Una curiosidad simpática con esto de la criptografía, ¿sabías que hasta el *Kama Sutra* recomienda su uso para que los amantes puedan comunicarse sin ser descubiertos? ¡Cómo se las gastaban los hindúes.

Sea como fuere, sin lugar a dudas, el punto de inflexión en el desarrollo de la criptografía moderna vino después de acabar la Segunda Guerra Mundial, se había visto que el uso de las matemáticas podía ayudar en el desarrollo de la criptografía. Durante la guerra, de sobra conocido es el caso de la máquina de cifrado/descifrado alemana **Enigma**, que se puso en circulación a lo largo de 1920 y que jugó un papel muy importante, al ser adoptada como mecanismo de cifrado por las fuerzas alemanas, debido a su supuesta inviolabilidad algo que se demostró como falso y que según se dice, sirvió para que los aliados pudieran acabar con la guerra, mucho antes de lo que habría sucedido en caso de no haber descubierto su sistema de cifrado.

Figura 4.3. La máquina Enigma (fuente: Wikipedia)

Aunque los inicios de rotura del cifrado de Enigma comenzaron en 1929 por parte de los polacos que interceptaron, casi por error, una de las máquinas que iban de Berlín a Varsovia y por el trabajo del matemático **Marian Rejewski**, que descubrió patrones en el funcionamiento de la máquina, fueron más famosos los intentos británicos. Célebre es la **Escuela Gubernamental de Códigos y Cifrados** en la mansión de **Bletchley Park**, donde un grupo de matemáticos encabezados por **Alan Turing** logró finalmente romper la cifra alemana.

No fue hasta los años 60, con la publicación del libro de **David Khan** *The Codebreakers*, cuando salió a la luz pública todo el entramado de Enigma y lo que

esto supuso (por cierto, la publicación de este libro no estuvo exenta de polémica, porque la NSA presionó para su no publicación y llegó a quitar tres fragmentos específicos).

El salto de la criptografía como arte a la criptografía como ciencia se produce acabada la guerra, con la publicación del artículo "Communication Theory of Secret System" en 1949 de C. E. Shannon. Este artículo, más el libro escrito por Shannon con Warren Weaver titulado *Mathematical Theory of Communication* y la teoría de la información y la comunicación establecen las bases de la criptografía moderna y el criptoanálisis moderno; la criptografía de clave pública difícilmente podría haberse realizado sin los descubrimientos de este hombre.

ENTONCES…

Shannon, además de ser conocido como el padre de la teoría de la información, desarrolló la teoría de la entropía que mide el grado de incertidumbre de una fuente de información. Publicó también trabajos sobre inteligencia artificial y el juego de ajedrez y parte de su vida profesional estuvo relacionada con los Laboratorios Bell y el MIT.

Acabada la Segunda Guerra Mundial y a partir de los años 50, sucede un hecho curioso, con la creación de la NSA en 1952 por el presidente Truman. Todas las publicaciones sobre criptografía que aparecen hasta finales de los años 70 son de escaso interés y se podrían considerar de naturaleza muy básica. Los enormes presupuestos y la casi inagotable financiación que recibía la NSA monopolizaron el trabajo de los científicos, que o trabajaban para el Gobierno o difícilmente podían avanzar en su trabajo. Revelar o publicar nada relacionado con la criptografía se consideraba traición y las patentes eran revisadas por ellos y retiradas en caso de considerarse peligrosas.

Hasta mediados de los 70 (1975), con la publicación del algoritmo **DES (Data Encryption Standard)** propuesto por IBM y revisado por la NSA, no podía ser otra, el interés por la criptografía no vuelve a tener un repunte, aunque siempre bajo la atenta mirada de la agencia. A partir de ese momento y con la llegada de la criptografía de clave pública, los algoritmos se suceden cada pocos años. En 1977 se publica RSA (Rivest, Shamir y Adleman) y un año antes se inicia la criptografía de clave pública. En 1978 IBM reinventa DES con TDES (Triple DES o 3DES), las curvas elípticas en 1985, IDEA en 1991, RC5 aparece en 1994, y en 2001 se publica AES (*Advanced Encryption Standard*) que junto con Twofish y Serpent (no confundir con el lenguaje de Ethereum) son considerados los algoritmos más seguros del mundo.

4.1.6 Limitaciones de la criptografía simétrica

Antes os explicaba que el problema que tenemos con la criptografía simétrica es que para poder cifrar o descifrar un mensaje, tanto emisor como receptor del mensaje deben disponer de la clave secreta utilizada en el proceso. Sin embargo, el problema aquí radica en cómo hacer llegar la clave secreta sin que esta se vea comprometida.

Lo ideal tal vez sería que quedasen en persona y se la dieran en mano, en un **ambiente privado** que se pudiera considerar seguro y protegido de "miradas indiscretas" y en cualquier caso antes de que la comunicación se produzca; sin embargo, en la práctica este mecanismo no es muy funcional, las personas pueden estar ubicadas geográficamente muy distanciadas. Aunque el problema más importante se produce a medida que necesitamos comunicarnos con más personas.

Me explico, si quiero comunicarme con 1 persona, ¿cuántas claves necesito? Obviamente 1, sin embargo si quiero comunicarme con n personas y cada una de estas comunicaciones se considera como independiente, el problema es que tendré que gestionar tantas claves privadas como personas, en este caso n también, y más pronto que tarde la gestión de tantas claves diferentes acabará siendo un problema, y no solo eso, los canales de distribución de estas claves a sus respectivos usuarios destino también tienen que ser gestionados de manera segura.

Además, la clave que utilizan los sistemas de clave compartida debe ser lo suficientemente grande como para que pueda resistir ataques de fuerza bruta o de diccionario que expliqué anteriormente; algunos de estos algoritmos, como puede ser el caso de DES, usan una clave de 56 bits (72 mil billones de claves posibles) y pueden probarse con un ordenador en cuestión de unas pocas horas. Por este motivo, ahora estaréis viendo que las palabras 128 bits (2 elevado a 128 posibles claves posibles), 256 bits (2 elevado a 256 claves posibles) o incluso 512 bits (2 elevado a 512 claves posibles) van al lado de los algoritmos de cifrado para indicar el tamaño de clave que usan y su fortaleza.

Tened en cuenta que aunque se puedan usar muchos bits para la clave, siempre hay que perseguir un equilibrio entre seguridad y eficiencia, una longitud de clave mayor siempre implicará una velocidad de ejecución menor, por tanto, la elección depende siempre de garantizar la seguridad pero sin ir en detrimento de la eficiencia de los algoritmos.

ENTONCES…

Sobre longitudes de clave y recomendaciones sobre estas está la página **keylenght.com** de BlueKrypt; os animo a pasar un rato jugando con esta web y comparando resultados.

4.2 FUNCIONAMIENTO DE LA ENCRIPTACIÓN DE CLAVE PÚBLICA

La mayor parte de los algoritmos anteriores son de clave simétrica (compartida). La siguiente evolución en los sistemas criptográficos se produce con el nacimiento de la criptografía de clave pública en el año 1976 con la publicación del artículo "New Directions in Cryptography" de W. Diffie y M. E. Hellman, que demostraron que era posible una comunicación secreta sin necesidad de transmitir la clave secreta entre el emisor y el receptor del mensaje. También se la conoce como **criptografía asimétrica**.

En este tipo de sistema de cifrado, decíamos que existen dos claves diferentes, la clave privada y la clave pública. Una de ellas sirve para la transformación o función de cifrado y la otra para la transformación de descifrado. Es decir, empleamos una para cifrar y la otra sirve para descifrar. Cumplen que el conocimiento de la clave pública, que se deriva matemáticamente de la privada, no permita calcular esta última, y son ideales para establecer comunicaciones seguras por canales inseguros puesto que únicamente viaja por el canal la clave pública, que solo sirve para cifrar, o para llevar a cabo autenticaciones. Sin la clave privada un observador no autorizado será incapaz de descifrar el mensaje cifrado.

Fijaos en que se llama clave pública, precisamente porque todo el mundo la conoce, está disponible para que cualquiera pueda usarla; es lo mismo que sucede en Bitcoin, la dirección pública es donde nosotros vamos a recibir o enviar fondos, no hay secreto en ella, por no decir que además todo queda registrado en la cadena de bloques. Las claves públicas podemos ponerlas donde nos dé la gana, puedo tenerla en mi sitio web, en mi tarjeta de trabajo, o donde más me guste, y el canal por el que la haga llegar me es indiferente, puede estar plagado de minas o *hackers*, me da igual lo inseguro que sea.

Pero, ¿por qué me da igual? El envío de mensajes usando la criptografía de clave pública sigue el siguiente esquema:

- Bob quiere enviar un mensaje a Alicia que solamente esta pueda leer, para ello Bob lo que hace es coger la clave pública de Alicia que es pública (está en el sitio web de Alicia) y todo el mundo la conoce.

- Bob codifica el mensaje utilizando la clave y la envía por un canal inseguro.

- El mensaje llega a Alicia, que usando su clave privada (que solamente ella conoce) la aplica sobre el mensaje encriptado y obtiene el mensaje original que Bob le envío.

Gráficamente:

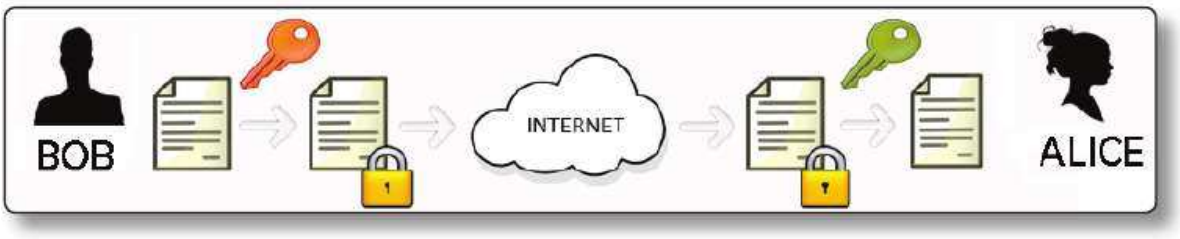


Figura 4.4. Bob envía un mensaje a Alicia (fuente: Wikipedia con algunos retoques propios)

Y ahora vamos a pararnos un poquito en esto, porque a partir de aquí la cosa se pone interesante y tenemos algunos escenarios curiosos…

¿Que Bob le envío? ¿Puede Alicia saber que el mensaje se lo envió Bob y que nadie suplantó su identidad? Sabemos por este esquema que ella es la única que puede leer el mensaje enviado "por alguien" porque está cifrado con su clave pública (la de Alicia), sin embargo, no puede estar segura de que "este alguien" sea su amigo Bob, pudo ser él o pudo ser otra persona desde su ordenador o usando su cuenta de correo electrónico, suponiendo un mensaje de este tipo.

La única manera para que se pueda asegurar que el mensaje enviado lo hizo realmente Bob es que este a su vez firme el mensaje (antes de cifrarlo con la clave pública de Alicia), con su clave privada; luego Alicia aplicará la clave pública de Bob, antes de aplicar la suya propia privada. El esquema ahora es el siguiente:

- Bob cifra el mensaje que desea enviar a Alicia con su clave privada (la de Bob y que solo Bob conoce, valga la redundancia).

- El resultado de este cifrado se vuelve a cifrar usando ahora la clave pública de Alicia (que la conoce todo el mundo) y envía el conjunto doblemente cifrado a esta.

- Cuando el mensaje llega a Alicia, lo que tiene que hacer es aplicar en primer lugar su propia clave privada, de este modo llega al mensaje cifrado con la clave privada de Bob; en este momento, el mensaje de Bob no es todavía legible para Alicia, tiene que quitar ese caparazón.

- Como la clave pública de Bob es también pública, Alicia la utiliza y descifra el mensaje previamente cifrado con la clave privada de Bob y ahora sí, puede leer el mensaje finalmente.

Ahora, Alicia sí está segura de que el mensaje se lo envió Bob porque este utilizó previamente su clave privada para cifrarlo. Hemos conseguido muchas cosas de un solo plumazo:

- Primero, que solamente los usuarios autorizados tienen acceso a la información, es decir, solo Alicia puede leer el mensaje.

- Segundo, podemos saber quién es el remitente y por tanto que no hubo suplantación de identidad. Igualmente podemos asegurar la identidad del usuario destinatario y que la información no fue alterada desde que fue firmada, porque para poder alterarla implicaría disponer de las claves privadas para poderlas aplicar, una vez que el mensaje original fue alterado.

- Tercero, al haber firmado Bob el mensaje con su clave privada, Bob no puede decir que no lo hizo él, porque solamente él y nadie más que él conoce su clave privada.

Esta última propiedad es en la que se basa la **firma digital**. Con la firma digital cualquier mensaje firmado con ella garantiza la autenticación en origen, el no repudio y la integridad. Daos cuenta de que no se garantiza el secreto de la información, el hecho de firmar un mensaje con mi clave privada y hacer visible dicho cifrado al mundo implica que cualquiera con mi clave pública pueda ver lo cifrado.

Sin embargo la criptografía de clave simétrica también presenta algunos problemas conocidos. Los más importantes tienen que ver con la eficiencia, ya que al utilizarse claves muy largas los algoritmos tardan más tiempo con la seguridad, porque al cifrar siempre usando la misma clave, se puede facilitar ataques basados en el análisis de estos textos cifrados; también la clave privada requiere ser almacenada en algún lado, y ese algún lado suele estar protegido también con otra clave habitualmente siguiendo un esquema de cifrado simétrico (os acordáis del fichero wallet.dat, ¿verdad?). Estas desventajas en parte se mitigan con el uso de la criptografía de **clave asimétrica basada en curvas elípticas**.

Actualmente la criptografía de clave pública se divide en tres familias según el problema matemático en el que basan su seguridad; son:

- **El Problema de Factorización Entera** (PFE), aquí tendríamos el algoritmo RSA y de Rabin Williams (RW).

- **El Problema del Logaritmo Discreto** (PLD), aquí estarían Diffie Hellman (DH) y el sistema DSA.

- **El Problema del Logaritmo Discreto Elíptico** (PLDE), ejemplos son Diffie Hellman Elíptico, DSAE, NRE, MQV y por supuesto las curvas elípticas (CEE).

Cada una de ellas supone un reto matemático que hace imposible que una vez aplicado el algoritmo sea posible descifrar el texto cifrado. Comprender estos entresijos matemáticos no es para nada trivial y como no estamos en un curso de criptografía solamente hablaré más adelante del logaritmo discreto elíptico, que es el que nos importa para Bitcoin.

4.3 FUNCIONES CRIPTOGRÁFICAS DE TIPO HASH

Antes de explicar el funcionamiento de las curvas elípticas, hagamos una parada para entender una función criptográfica que hemos referenciado anteriormente y que nos falta por presentar, y eso que su nombre ha aparecido a lo largo del libro varias veces. Me refiero a las funciones *hash*, si Bitcoin funciona es en gran medida gracias a que existen. Estamos ahora mismo quizás en uno de esos puntos fundamentales de entender bien, estad atentos y no despistarse.

Las funciones *hash* a veces reciben el nombre de funciones picadillo o **funciones digest** (nombres que en castellano no me suenan personalmente nada bien); lo que vienen a decir es que dada una cadena de longitud variable y normalmente muy grande, la función *hash* lo que hace es devolver una cadena de longitud fija más pequeña y que sirve como equivalente de la cadena de origen, este equivalente recibe el nombre de **resumen**.

ENTONCES…

Ejemplo clásico de este tipo de funciones son las **sumas de verificación** que seguro has visto más de una vez en la sección de descargas de muchísimas webs bajo el nombre de **checksum**. Una suma de verificación es un tipo de función *hash* que está pensada para detectar cambios cuando se transmite un fichero por una red de comunicaciones. Lo que se hace es que junto al fichero disponemos del valor del *checksum* para el mismo, cuando lo descargamos basta con recalcular el *checksum* para el fichero descargado y verificar que coincide con el publicado en la web, de este modo estamos seguros de que el fichero de origen y el de destino son el mismo. La gracia es que si el fichero es muy grande, en vez de tener que comparar muchos *megabytes* de datos, comparando los pocos datos del *checksum* tengo las mismas garantías de que todo el proceso fue bien. **Alder** o **CRC** son algunos ejemplos de algoritmos de *checksum* muy conocidos y utilizados.

El resumen actuaría como un identificador de la entrada y podrían considerarse como equivalentes. Daos cuenta también de otra cosa, calcular una función *hash* es un proceso que debe ser computacionalmente eficiente y sencillo, pero el proceso contrario no lo es, a partir de mi resumen no puedo reconstruir la entrada original; estamos por tanto, como os decía al principio del capítulo ante otro ejemplo de **función unidireccional**, fácil de hacer pero difícil de deshacer.

Gráficamente la siguiente imagen es muy descriptiva:

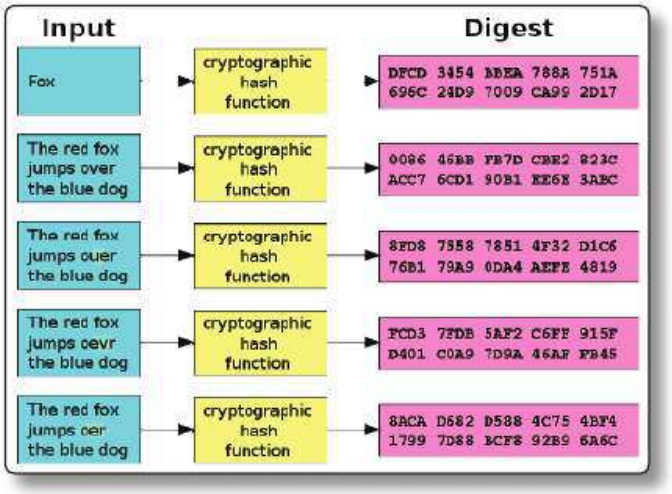


Figura 4.5. Ejemplo de función hash (fuente: Wikimedia Commons)

El texto de la izquierda es el texto en claro al que se le quiere aplicar una función *hash*, la caja amarilla representa la ejecución de la función y el texto de la derecha el resultado; no importa la longitud del texto de entrada, la salida siempre devuelve una secuencia de la misma longitud, aunque diferente. Ir desde el texto de la derecha al de la izquierda es, como ya hemos visto, imposible, sin embargo, no se debe ver a las funciones hash como funciones cuyo objetivo principal es proteger el secreto de la información, lo que hacen es obtener un resumen del texto, que el resultado no permita la vuelta atrás y por ende entender el texto en claro es solo una consecuencia de su funcionamiento.

ENTONCES…

Cuando haciendo criptoanálisis se encuentra una pareja de mensajes que devuelven el mismo resumen/*hash*, se considera que la función ya no es resistente y válida para criptografía y se busca otro algoritmo *hash* para usar. MD5 o SHA-0 son ejemplos de funciones *hash* que han sido rotas (incluso SHA-1 está en entredicho) y que si bien gozaron de mucha popularidad han ido decayendo en uso. Hay muchos tipos de ataques a las funciones *hash*, quizás las técnicas más famosas usadas sean el **ataque de cumpleaños**, el **ataque Wang-Yin-Yun** o **ataque chino** y el ataque **multicolisión**.