

# DOMINIO DE BITCOIN — PARA — PRINCIPIANTES

TECNOLOGÍAS BITCOIN Y CRIPTOMONEDA, MINERÍA,  
INVERSIÓN Y COMERCIO



ALAN T. NORMAN

Alan T. Norman

**Dominio De Bitcoin  
Para Principiantes**

«Tektime S.r.l.s.»

**Norman A.**

Dominio De Bitcoin Para Principiantes / A. Norman — «Tektime S.r.l.s.»,

ISBN 978-8-89-398867-4

Bitcoin no es solo una nueva palabra en la era de Internet o el progreso tecnológico y financiero, ¡es el comienzo de una nueva era en la Tierra! Incluso hace diez años no podíamos imaginarnos soñar con dinero digital - no se puede tocar físicamente, pero se pueden poseer y gastar. ¡Hoy esto es una realidad! La revolución Bitcoin cubrió el mundo entero como una ola enorme, cada vez más gente interesada en este "oro digital". Bitcoin no es solo una nueva palabra en la era de Internet o el progreso tecnológico y financiero, es el comienzo de una nueva era en la Tierra! Incluso hace 10 años no podíamos imaginarnos soñar con dinero digital - no se puede tocar físicamente, pero se puede poseer y gastar. Hoy esto es una realidad! La revolución Bitcoin cubrió el mundo entero como una ola enorme, cada vez más gente interesada en este "oro digital". En los últimos años, Bitcoin ha pasado de ser algo conocido sólo por unos pocos nerds de la tecnología a una moneda revolucionaria que ha cambiado rápidamente la forma en que pensamos sobre el concepto de dinero. Sin duda, ahora se aceptan pagos de Bitcoin en todo tipo de lugares, pero, si puedes crearlo, solía ser un procedimiento bastante complicado para encontrar lugares que te permitieran pagar en Bitcoin. De todos modos, para dirigir el mundo necesitas saberlo todo. No podemos garantizar que usted sabrá TODO de este libro, pero podemos garantizarle que tendrá la noción de una nueva moneda - Bitcoin. ¿Qué es esto? ¿De dónde ha salido? ¿Cómo se usa? ¿Es realmente dinero falso creado por los traficantes de drogas? Eso es precisamente lo que responderemos en este libro. Cubrimos todo lo que necesitas saber para empezar a trabajar con Bitcoin: entender las transacciones de la cadena de bloques y de Bitcoin, dónde guardar tu Bitcoin (cómo elegir una billetera segura), comprar Bitcoin, invertir en Bitcoin, cómo empezar a aceptar y utilizar Bitcoin como parte de tus principios de negocio de Bitcoin, minar. la seguridad de Bitcoin, etc. Además, el autor compartirá contigo datos interesantes sobre Bitcoin y te dará consejos profesionales sobre el inicio de tu camino en la familia Bitcoin. ¿Ya estás

listo para enfrentarte al mundo Bitcoin? Eso espero. Me gustaría ser el primero en darte la bienvenida oficialmente al mundo de Bitcoin!

ISBN 978-8-89-398867-4

© Norman A.  
© Tektime S.r.l.s.

# Содержание

ÍNDICE	7
CAPÍTULO 1. ¿QUÉ ES BITCOIN?	9
El Comienzo	10
Respuestas Centralizadas	11
¿Quién es satoshi?	12
La Creación	13
Cómo Lo Hizo Satoshi	14
Entonces, ¿es una moneda?	15
Acerca de El Costo	16
Entonces, ¿por qué Bitcoin?	17
Aprender sobre Bitcoin	18
Capítulo 2. Comprensión de las transacciones de bloqueo y bitcoin	19
La cadena de bloques y Bitcoin	20
¿Cómo funcionan las transacciones de Bitcoin?	21
Bloques	22
Confirmaciones	23
Tarifas	24
La cadena de bloques y las transacciones	25
Capítulo 3. Cómo empezar con bitcoin	26
Seguridad personal en Bitcoin	27
Nunca Comparta Su Clave Privada	28
No Pierda Su Clave Privada	29
Tener Una Billetera Segura	30
Saber Que El Precio Cambiará	31
No Puede Anular Pagos	32
Las Bitcoins Son Trazables	33
Puede Haber Problemas De Crecimiento	34
Introducción a Bitcoin	35
Capítulo 4. Dónde guardar su bitcoin	36
Конец ознакомительного фрагмента.	37

DOMINIO DE BITCOIN PARA PRINCIPIANTES  
TECNOLOGÍAS BITCOIN Y CRIPTOMONEDA, MINERÍA, INVERSIÓN Y  
COMERCIO

Alan T. Norman

Traductora: Arturo Juan Rodríguez Sevilla

Consigue tus **ballenas Bitcoin gratis: Tipos que engañaron al mundo con** el Libro de Bonos  
(Detalles al final de este libro.)

Copyright © 2017 Alan T. Norman. Todos los derechos reservados.

Ninguna parte de esta publicación puede ser reproducida, distribuida o transmitida de ninguna forma ni por ningún medio, incluyendo fotocopias, grabaciones u otros métodos electrónicos o mecánicos, ni por ningún sistema de almacenamiento y recuperación de información sin el permiso previo por escrito del editor, excepto en el caso de citas muy breves incorporadas en revisiones críticas y ciertos otros usos no comerciales permitidos por la ley de copyright.

# ÍNDICE

## CAPÍTULO 1. ¿QUÉ ES BITCOIN?

El Comienzo

Cómo Lo Hizo Satoshi

Entonces, ¿es una moneda?

Acerca de El Costo

¿Qué es un Criptomoneda?

Entonces, ¿por qué Bitcoin?

Aprender sobre Bitcoin

## Capítulo 2. Comprensión de las transacciones de bloqueo y bitcoin

La cadena de bloques y Bitcoin

¿Cómo funcionan las transacciones de Bitcoin?

La cadena de bloques y las transacciones

## Capítulo 3. Cómo empezar con bitcoin

Seguridad personal en Bitcoin

Introducción a Bitcoin

## Capítulo 4. Dónde guardar su bitcoin

Su dirección Bitcoin

Direcciones de uso único

Creación de una dirección Bitcoin

Billeteras Bitcoin

Cómo elegir una billetera

Almacenamiento en frío

Billeteras Bitcoin

## Capítulo 5. Compra de bitcoin

Principales intercambios en línea

¿Por qué elegir una bolsa grande?

Verificación KYC

¿Algo de lo que preocuparse?

Intercambios solo en criptomoneda

Una nota sobre la seguridad de intercambio

Igual para igual

¿Por qué elegir las transferencias entre pares/iguales?

¿Por qué no?

Nota sobre seguridad y protección

Comprar Bitcoin

## Capítulo 6. Uso de bitcoin

Tarjetas de débito Bitcoin

Uso de Bitcoin

## Capítulo 7. Invertir en bitcoin

Inversión a largo plazo

Precio máximo

Comprender los balances

Invertir en Bitcoin

## Capítulo 8. Bitcoin para empresas

¿Por qué Bitcoin?

Aceptando Bitcoin



[Procesamiento de pagos](#)  
[Bitcoin para empresas](#)  
[Capítulo 9. Minería de bitcoin](#)  
[¿Qué es Bitcoin Mining?](#)  
[Hardware de minería](#)  
[Acerca de la Dificultad Minera](#)  
[Dónde buscar](#)  
[Minería Bitcoin](#)  
[Capítulo 10. Seguridad bitcoin](#)  
[Nodos Bitcoin](#)  
[Entonces, ¿qué se puede piratear?](#)  
[El Ataque Teórico 51](#)  
[Doble Gasto](#)  
[Anonimato](#)  
[Seguridad Bitcoin](#)  
[Capítulo 11. Consejos y datos divertidos](#)  
[Las Historias que Necesita Escuchar](#)  
[Entender las historias en perspectiva](#)  
[Capítulo 12. Conclusión](#)  
[A Usarlo](#)  
[El futuro de Bitcoin](#)  
[En conclusión](#)  
[Sobre El Autor](#)  
[OTROS LIBROS DEL AUTOR](#)  
[Tecnología Blockchain Explicada](#)  
[¡Ayuda a mejorar este libro para todos!](#)



## CAPÍTULO 1. ¿QUÉ ES BITCOIN?

Si ha tomado este libro, lo más probable es que haya oído hablar de Bitcoin.

Tal vez haya oído hablar de ello en los círculos financieros, ya que el valor de Bitcoin ha aumentado rápidamente.

Quizás haya oído hablar de él en un contexto tecnológico, ya que Bitcoin se basa en una nueva tecnología llamada Blockchain.

O, como muchos, puede que haya oído hablar de Bitcoin en la prensa popular por la cantidad de nuevos usuarios, celebridades famosas y empresarios de éxito que empezaron a utilizar Bitcoin el año pasado.

En los últimos años, Bitcoin ha pasado de ser algo conocido solo por unos pocos nerds tecnológicos selectos a una moneda revolucionaria que ha cambiado rápidamente la forma en que pensamos sobre el concepto de dinero.

Aquí está la (muy) básica sinopsis: Bitcoin es una moneda digital. En muchos sentidos, funciona como dólares, euros o yenes, lo que nos permite transferir valor. Sin embargo, la fuerza de Bitcoin es su red. La tecnología de la cadena de bloques permite descentralizar Bitcoin, lo que significa que cualquiera puede acceder y comerciar en el libro mayor de Bitcoin. Con Bitcoin, puede enviar fondos a cualquier persona en el mundo, sin necesidad de grandes instituciones como bancos, conversores de divisas y procesadores de pagos.

Todo sucede en la red pública de Bitcoin.

Además de los pagos de persona a persona, los pagos de Bitcoin se aceptan ahora en todo tipo de negocios. Hace solo unos años, encontrar lugares que te permitieran pagar en Bitcoin era un reto. Para ser honesto, en los primeros días de Bitcoin, podríamos haber llenado esta página con todos y cada uno de los lugares que aceptaban Bitcoin. Ahora, la aceptación de Bitcoin se ha disparado.

En los últimos años ha surgido otro uso de Bitcoin: la inversión. A medida que más gente empezó a usar Bitcoin, su precio ha aumentado drásticamente. Como veremos más adelante en este libro, muchas personas están comprando Bitcoin como un activo que esperan apreciar con el tiempo.

Por supuesto, Bitcoin todavía tiene sus problemas y retos para su futuro. Echaremos un vistazo a algunos de esos desafíos en las páginas siguientes.

En este libro, cubriremos todo lo que necesitas saber para empezar con Bitcoin, así que comencemos con su procedencia.

¿Listo para sumergirte? ¡Vámonos!

## **El Comienzo**

Piensa unos años atrás. En 2008 la crisis financiera estaba en pleno apogeo, y la gente de todo el mundo estaba sintiendo los efectos del desastre económico de Estados Unidos. Este fue uno de esos momentos de la historia en que los problemas de las monedas nacionales mostraron su fuerza. La crisis financiera estadounidense devaluó el dólar, y los desafíos económicos en los Estados Unidos afectaron al mundo entero.

A veces parecía probable que se produjera un colapso económico completo. ¿Dónde estaban todas esas personas que se suponía que debían asegurarse de que nada de esto sucediera? La cagaron a lo grande. Eso es decirlo a la ligera, por no decir más.

## **Respuestas Centralizadas**

Las personas más destacadas "en el saber" decidieron que tenían una respuesta que solo un banco centralizado podía ofrecer. Para combatir el rápido colapso de los mercados financieros, los gobiernos de todo el mundo decidieron lo que se conoce como "flexibilización cuantitativa", en la que imprimían más dinero y lo inyectaban en sus economías para que sus ciudadanos tuvieran los fondos necesarios para evitar otra Gran Depresión.

Este tipo de cambios rápidos conducen a "guerras de divisas" y los gobiernos pronto competían por ser los que tenían los precios más bajos, lo que los mantendría competitivos. Cuando los bancos tuvieron problemas debido al bajo valor de la moneda y a la reducción de los tipos de interés, los gobiernos se vieron obligados a rescatarlos con dinero de los contribuyentes. Como se puede adivinar, esto solo devaluó aún más la oferta monetaria existente.

Aunque esta es una visión muy simplificada de un momento complejo de la historia económica, la lección permanece. Los bancos centrales que manipulaban la oferta monetaria devaluaron las monedas en todo el mundo.

Al final, con los tipos de interés bajos y los rescates de los contribuyentes, los mismos bancos que fueron responsables de los problemas financieros en primer lugar fueron los que se beneficiaron de la casi colapsada economía. Fue durante este tiempo que un hombre conocido como Satoshi Nakamoto se inspiró.

## ¿Quién es satoshi?

Antes de explicar con precisión cómo surgió Bitcoin, vale la pena explorar quién es Satoshi Nakamoto. Su historia es la historia de Bitcoin, y él era misterioso.

La verdadera identidad de Satoshi sigue siendo desconocida hasta el día de hoy. Según sus propias declaraciones de 2012, era un hombre de 37 años que vivía en algún lugar de Japón. Sin embargo, hay muchas dudas al respecto. Escribe con fluidez en inglés, y el software de Bitcoin no está documentado en japonés, lo que hace pensar a muchos que, de hecho, no es japonés, aunque podría haber estado viviendo allí en ese momento.

Con un poco de trabajo detectivesco, un programador suizo determinó que Satoshi podría estar viviendo en Norteamérica, dadas las horas del día que publicaba en los foros de Bitcoin. El codificador hizo esto analizando los tiempos de publicación más comunes y descubriendo que se alineaban con el horario promedio de sueño de alguien que vivía en el continente.

¿Sabremos alguna vez quién es el creador de Bitcoin? ¿Es realmente un equipo de personas? Puede que nunca lo sepamos, pero una cosa es segura: esta persona o personas controlan aproximadamente un millón de Bitcoin. A partir de junio de 2017, ¡esto equivale a casi 3.000 millones de dólares! Con una fortuna como esa, podrían comprar el derecho a la privacidad.

## La Creación

Así que, este codificador anónimo miró el estado del mundo financiero y vio muchos problemas. Las formas tradicionales de resolver esta crisis habían sido probadas y, aunque funcionaban, por ahora, él veía que poco se hacía para prevenir futuros desastres. ¿Qué se podría hacer al respecto? ¿Podría cualquier tipo de solución centralizada arreglar problemas como este para siempre?

Decidió que se necesitaba una fuerza desestabilizadora. Algo que podría cambiar potencialmente la forma en que pensamos sobre la moneda. La respuesta fue una forma de moneda completamente descentralizada y abierta a todos. Ningún banco central la controla, ninguna cadena de transferencias con un solo supervisor. No hay un grupo elitista de personas que tomen decisiones que afecten a todas las personas que utilizan sus monedas.

Descentralización: el traslado de departamentos de una gran organización desde un único centro administrativo a otros lugares.

Esa descentralización fue la principal fuerza impulsora de la labor de Satoshi. Esencialmente, la descentralización significa que todo el mundo es parte de la economía de Bitcoin y todos contribuimos de alguna manera. NOSOTROS somos la fuerza motriz, y no un banco central que controla cuánto vale nuestra moneda y cuánto de ella tenemos disponible en nuestra economía. Mejor aún, al mismo tiempo, ninguno de nosotros tiene el control.

No hay ningún gobierno, banco o intermediario que pueda decirnos cómo usar Bitcoin, ya que literalmente pertenece a todos los que lo usan. Dicho esto, cuantas más personas lo utilicen, mejor funcionará y será más viable. Así es como funciona la tecnología igual para igual. Es directamente por los usuarios.

En el sentido más verdadero de la palabra, es un mercado libre. Hemos oído hablar mucho de los mercados libres a lo largo de los años, pero ningún mercado puede ser verdaderamente libre cuando hay una fuerza motriz que toma decisiones al respecto.

## **Cómo Lo Hizo Satoshi**

Satoshi está lejos de ser la primera persona en trabajar en el problema de la moneda digital descentralizada. Los criptógrafos y codificadores habían estado trabajando en el problema durante años antes de 2008.

El reto de la descentralización es mantener un libro mayor de transacciones. Normalmente, cuando usted paga a alguien, el banco resta el dinero de su cuenta y lo añade a la cuenta del destinatario. La actualización del libro de operaciones es la función principal de un banco.

En un sistema descentralizado, sin embargo, no hay ningún banco. Cualquiera puede enviar una solicitud de transacción a la red descentralizada. Esto hace que el libro mayor descentralizado sea muy vulnerable a los ataques. Los malos actores pueden cambiar el libro de contabilidad o gastar una moneda digital varias veces antes de que la red lo note.

La innovación de Satoshi fue la tecnología que ahora llamamos la cadena de bloques. Encontró una manera de mantener un libro de contabilidad seguro usando marcas de tiempo, mucho poder de procesamiento descentralizado y criptografía. Bitcoin — la primera cadena de bloques — todavía utiliza la arquitectura de Satoshi para asegurar los pagos hoy en día.

## **Entonces, ¿es una moneda?**

Una de las mayores preguntas que la gente tiene sobre Bitcoin es "¿Es una moneda?"

La respuesta está en un área gris. Bitcoin es un pago y una forma de transferir fondos. Puede utilizar Bitcoin para realizar compras o enviar pagos. Es posible convertir Bitcoin a dólares, euros, libras, yenes o cualquier otra moneda. Sin embargo, no está respaldado por ninguna institución. No hay ningún gobierno central al que puedas señalar, y no hay garantías cuando se trata de ser propietario de Bitcoin. Es tan valioso como el número y tipo de lugares y personas que lo aceptan.

Bitcoin es lo que ahora llamamos una moneda digital en su forma más pura, o lo que se conoce como criptomoneda. Bitcoin fue la primera criptomoneda, pero ahora hay muchas de ellas. Las criptomonedas operan de manera diferente a las monedas tradicionales, ya que se basan en el código, no en las decisiones de un banco central. Esta diferencia las hace atractivas pero también más volátiles.



## Acerca de El Costo

Una de las mayores características de una moneda verdadera es su valor estable. Mucha gente argumenta que Bitcoin no es una moneda dado su valor volátil. El precio de Bitcoin ha fluctuado mucho y ocasionalmente se duplica en valor en un corto periodo de tiempo.

Por ejemplo, en julio de 2010, el precio era de 0,08 dólares por Bitcoin. En diciembre de 2017 Bitcoin alcanzó los 20.000 dólares. En promedio, cambia alrededor del 2% por día. Eso es algo que no se ve con las monedas tradicionales, lo que lleva a muchos a decir que es inútil como una sola. Un precio estable es lo que convencerá a la inversión tradicional y conducirá a un crecimiento sostenido.

¿Esto es importante para Bitcoin? Eso depende de cómo lo mires. A corto plazo, la volatilidad del precio puede tener un gran impacto en la confianza de la gente. Cuando se trata de atraer a nuevas personas al mundo de la criptomoneda, los cambios rápidos en los precios pueden ser un problema.

La clave es mirar el panorama general. Si usted es alguien que está interesado en ser parte de un cambio económico verdaderamente revolucionario, el plan a largo plazo es lo más importante.

Teniendo esto en cuenta, muchas investigaciones han demostrado que se espera que Bitcoin se estabilice en algún momento en el futuro y fluctúe mucho menos. Los altibajos típicos se pueden atribuir en gran medida a la publicidad que Bitcoin está recibiendo en un momento dado.

También existe una alta probabilidad de que los gobiernos comiencen a regular las criptomonedas en los próximos años. Mientras que la regulación por sí misma no será capaz de cerrar las monedas descentralizadas, tendrá un fuerte efecto moderador sobre cuánto y con qué rapidez cambian las valoraciones.

¿Qué es un Criptomoneda?

"Criptomoneda: una moneda digital en la que se utilizan técnicas de encriptación para regular la generación de unidades monetarias y verificar la transferencia de fondos, operando independientemente de un banco central".

Definir las criptomonedas requiere mucha información técnica que trataremos más a fondo más adelante en el libro, pero vale la pena presentarla aquí para que pueda entender de qué estamos hablando.

En pocas palabras, una criptomoneda son líneas de código que tienen valor monetario. Mediante la criptografía, la red descentralizada crea nuevas monedas y asegura las transacciones. Algunos miembros de la red descentralizada instalan computadoras que procesan el código. A cambio, estos nodos procesadores, —conocidos como mineros—, reciben una recompensa por asegurar las transacciones en la cadena de bloques.

## **Entonces, ¿por qué Bitcoin?**

Bitcoin está lejos de ser la única criptomoneda. Sin embargo, en los últimos diez años ha mantenido su dominio como la criptomoneda número uno en el mundo.

Hay un fuerte argumento a favor de que Bitcoin no es la mejor criptomoneda del mundo. Los nuevos proyectos han llegado con una escalabilidad, velocidad y privacidad de las transacciones superiores. Sin embargo, estas nuevas monedas no han podido derribar a Bitcoin de su trono.

Parte de la razón por la que Bitcoin ha mantenido su liderazgo es su ventaja. Bitcoin fue el primer Blockchain (cadena de bloques) de la historia. Todo el interés inicial en Blockchain (cadena de bloques), entre 2008 y 2013, se centró en Bitcoin. Esto significa que Bitcoin tenía la mayor base de usuarios y su selección de grandes desarrolladores para construir el sistema.

Este proceso es un círculo virtuoso para Bitcoin. Al tener la red más grande, también tiene la mayor aceptación. Los efectos de red significan que cuantas más personas utilicen una tecnología, más útil será.

Tomemos como ejemplo el correo electrónico. No sería útil en absoluto si fueras la única persona en el mundo con una dirección de correo electrónico. Sería algo útil si usted y algunas otras personas tuvieran correo electrónico. Pero es muy útil cuando casi todo el mundo tiene una dirección de correo electrónico. La adopción de Bitcoin es la misma. Se vuelve más útil cuanto más gente lo acepta.

Bitcoin sigue obteniendo la mayor cantidad de prensa de todas las criptomonedas en la actualidad, sobre todo porque sigue siendo la más grande. Su larga historia también le confiere cierta legitimidad.

A lo largo de una década, Bitcoin ha enfrentado y superado muchos obstáculos y retos técnicos, siempre en ascenso. Su comprobado historial de seguridad también lo convierte en la compra de criptomoneda más segura para principiantes.

Mientras que otras criptomonedas pueden tener un enfoque en funciones específicas, Bitcoin es una moneda digital versátil que está disponible desde casi cualquier cambio en moneda alternativa. En esta etapa, es la moneda la que tiene las inversiones detrás, la base de usuarios, la seguridad y el historial.

## **Aprender sobre Bitcoin**

Todo esto es sólo el principio. A lo largo de este libro, cubriremos todos los aspectos de Bitcoin y le daremos consejos reales sobre cómo empezar.

Hay mucho que aprender. Es fácil atascarse en las minucias de Bitcoin y en cómo funciona la tecnología, pero para empezar con Bitcoin, solo se necesita entender los fundamentos. Eso es precisamente lo que leerán en las próximas páginas.

## **Capítulo 2. Comprensión de las transacciones de bloqueo y bitcoin**

Antes de entrar en los aspectos básicos de la compra y almacenamiento de su primer Bitcoin, repasemos los fundamentos de la tecnología que hace funcionar a Bitcoin: el Blockchain (cadena de bloques). Recientemente, "Blockchain" (cadena de bloques) se ha convertido en una palabra de moda para las nuevas empresas. Mucha gente que usa el término no tiene una idea clara de cómo el Blockchain (cadena de bloques) asegura una red descentralizada. Al final de este capítulo, usted entenderá los fundamentos de Blockchain (cadena de bloques) mejor que muchos entusiastas de la criptomoneda.

## **La cadena de bloques y Bitcoin**

Si recuerda, fue en 2008 cuando Satoshi Nakamoto publicó por primera vez un libro blanco sobre la tecnología Bitcoin y detalló el sistema igual para igual que ejecuta las transacciones de Bitcoin. La propia moneda Bitcoin es una idea revolucionaria. Sin embargo, la tecnología que lo impulsa es la verdadera innovación. El Blockchain (cadena de bloques) de Satoshi hace posible la creación de libros de contabilidad descentralizados seguros para cualquier cosa, no solo para la criptomoneda.

La cadena de bloques de Bitcoin es el libro mayor público que contiene todas las transacciones que se han realizado en la historia de Bitcoin. Dado que no existe un órgano central de gobierno ni una base de datos, el libro mayor se encuentra en una red compuesta por todos los ordenadores que ejecutan el software Bitcoin. Todos trabajan juntos para construir la red.

Todo esto sucede en público, y cualquiera puede ver el tráfico tal y como está sucediendo. Este nivel de transparencia es casi inaudito en cualquier otro sistema financiero. Esta transparencia es lo que hace que las criptomonedas sean únicas.

En términos más generales, el Blockchain (cadena de bloques) puede afectar a cualquier parte de nuestras vidas en la que necesitemos verificar la identidad, realizar una transacción o asegurar un contrato. El libro de contabilidad público en el Blockchain (cadena de bloques) puede ser más rápido, más barato y más seguro que muchas instituciones en las que confiamos hoy en día.

## **¿Cómo funcionan las transacciones de Bitcoin?**

Los Bitcoins no existen físicamente. No hay ninguna bóveda de bitcoins en alguna parte. Cuando lo piensas, eso no es muy diferente de nuestro dinero moderno. El dinero que usted ve cuando ingresa a su cuenta bancaria no significa que haya una caja con sus fondos en ella. De la misma manera, no hay nada que se pueda definir, como "este es un Bitcoin".

En cambio, cuando se inicia una transacción, se envía la solicitud de transacción a toda la red. Los mineros de la red añadirán su transacción al libro mayor público junto con otras solicitudes de transacción que se encuentran actualmente en la red. Este libro se estampa con la hora, se enlaza con el último libro producido y se bloquea con una clave criptográfica. Al sellado, enlazado y bloqueado se llama un bloque.

## Bloques

Los bloques de transacciones contienen todo lo que necesitan tanto para añadir nuevas transacciones como para conectar el bloque a todas las anteriores. En cada bloque se incluyen cuatro cosas: una referencia al bloque anterior en la cadena, todas las transacciones que se añaden, una marca de tiempo y la prueba criptográfica que muestra cómo se creó el bloque.

Esta combinación de estampado, unión y bloqueo de bloques fue la innovación de Satoshi en la creación de Bitcoin. Resuelve los problemas de crear un libro de contabilidad que cualquiera puede añadir:

La marca de tiempo muestra dónde pertenece el bloque en orden, asegurando que los bloques no se mezclen o que la red no respete varios bloques al mismo tiempo.

El enlace es una referencia al bloque anterior incrustado en el contenido del bloque actual. Esto asegura el lugar del bloque en una larga cadena de bloques. ¡El Blockchain!

La cerradura criptográfica del bloque se conoce como hash. Los mineros de la red utilizan su potencia de cálculo para calcular este hash. Para Bitcoin, es un rompecabezas increíblemente difícil que toma a los procesadores más rápidos del mundo una media de 10 minutos para resolverlo.

Al alojar toda esta información en un solo bloque, el sistema Blockchain (cadena de bloques) es capaz de regularse por sí mismo y no requiere un ojo vigilante para su supervisión. No hay necesidad de que alguien verifique manualmente las transacciones. Una vez hecho esto, es casi imposible cambiar el contenido de un bloque.

Cambiar el contenido de un bloque requeriría editar el libro mayor, reconstruir el bloque y luego volver a resolver el rompecabezas criptográfico. Más vale que su computadora sea más rápida que todas las demás computadoras de la red, porque necesitará ganar la carrera para completar el rompecabezas si quiere que su bloque sea implementado. Esto es muy improbable, dada la enorme potencia de cálculo de la red Bitcoin.

Los bloques están organizados en una cadena, y si quiere cambiar una transacción anterior, tendrá que editar ese bloque y resolver el nuevo rompecabezas. Pero la respuesta al viejo rompecabezas original está incrustada en el siguiente bloque de la cadena. Tendría que actualizar el siguiente bloque también, ¡esta vez con la nueva respuesta del rompecabezas! Cada vez que edite un bloque, tendrá que volver a resolver el rompecabezas para cada bloque que venga después. Cuantos más bloques de rompecabezas tenga que resolver, menos posibilidades tendrá de implementar con éxito su ataque. Las transacciones de Bitcoin que tienen más de una hora de antigüedad son estadísticamente casi imposibles de cambiar.

Después de que una transacción se agrega a la cadena de bloques, está ahí para siempre y se registra en todos los equipos de la red. De esta manera, el Blockchain (cadena de bloques) es una de las bases de datos más seguras imaginables.



## Confirmaciones

Las transacciones exitosas deben ser confirmadas para asegurar que sean correctas. Los mineros, que crean un nuevo bloque y lo añaden a la cadena de bloques cada diez minutos, lo hacen. Los mineros verifican las transacciones, las registran en el libro mayor y las añaden al siguiente bloque. Una vez resuelto el bloqueo, la transacción se considera verificada y las alteraciones son improbables.

Como se ha descrito anteriormente, es cada vez más difícil modificar una operación cuanto más atrás se encuentre el bloque en la cadena. Por esta razón, algunas personas prefieren esperar varios bloques antes de llamar a la transacción "confirmada".

Al utilizar Bitcoin en una tienda, es posible que algunos comerciantes no le obliguen a esperar. Sin embargo, esto significa que se están arriesgando a que usted cumpla con el pago. Esto es típicamente más común en las transacciones de bajo valor, ya que existe un menor riesgo de fraude.

## Tarifas

Al igual que con todos los sistemas transaccionales, Bitcoin tiene tarifas con cada transferencia. Sin embargo, hay una distinción importante aquí: Los honorarios no son requeridos y pueden ser determinados por la persona que envía los fondos.

A cambio de confirmaciones más rápidas, los mineros recolectan y procesan los honorarios. Pague lo suficiente y el minero moverá su transacción a la parte superior de la pila para añadirla al siguiente bloque. Una vez que han creado con éxito un nuevo bloque Bitcoin, cobran las comisiones de todas las transacciones incluidas en ese bloque en particular.

Los honorarios son totalmente voluntarios, y la persona que inicia la transacción puede decidir si desea o no incluir un honorario. Sin embargo, al incluir una cuota, puede asegurarse de que los mineros tengan un incentivo para procesar su transacción. Si usted decide no incluir una cuota, los mineros procesarán otras transacciones antes que las suyas. Usted podría esperar horas (o incluso días) antes de que su transacción sin cargo se incluya en un bloque.

Algunos monederos (donde guarda y administra sus Bitcoins) decidirán la tarifa de transacción por ti. Hablaremos más sobre las carteras en breve.

## **La cadena de bloques y las transacciones**

¿Ahora el Blockchain parece un poco menos misterioso? Esto es solo el principio con este increíble invento. He escrito un libro entero sobre la tecnología Blockchain (<http://mybook.to/BlockchainExplained>). Si le interesa, ese recurso le sumerge en el fondo del asunto.

Más adelante, hablaremos más sobre los mineros sobre los que seguir leyendo, pero por ahora pasemos a alguna información útil sobre cómo conseguir y gastar Bitcoins.

## **Capítulo 3. Cómo empezar con bitcoin**

Con una criptomoneda como Bitcoin, lo más importante es obtener buena información y entender el sistema antes de sumergirse. Bitcoin no tiene una autoridad central, por lo que las transacciones no pueden ser revertidas. Si comete un error con su Bitcoin será permanente. Dicho esto, tenga cuidado, invierta poco a poco y haga su investigación.

Este libro es una buena introducción, pero no puedo cubrir todo lo que encontrará en el mundo de Bitcoin. El mejor consejo que puedo darle es que lea tanto como pueda.

Bitcoin puede parecer aterrador o complicado. El objetivo de este capítulo es que se sienta cómodo con los conceptos básicos y las reglas básicas para empezar con Bitcoin. Tenga en cuenta que habrá explicaciones más profundas de estas cosas en el libro, así que no se preocupe demasiado por ninguno de estos aspectos.

## **Seguridad personal en Bitcoin**

Antes de dar cualquier consejo sobre cómo comprar, mantener, vender y realizar transacciones en Bitcoin, tenemos que hablar de seguridad. La red Bitcoin es altamente segura. Bitcoin nunca ha sido pirateado directamente, y es extremadamente improbable que alguien pueda cambiar una transacción en el libro mayor de Bitcoin.

El riesgo para la seguridad de ser propietario de Bitcoin proviene de un descuido personal o de un trato con terceros proveedores de servicios. Aquí hay algunos consejos:

## **Nunca Comparta Su Clave Privada**

Esta es la primera regla de seguridad de Bitcoin, y no hace falta decirlo. Ninguna empresa o persona legítima le pedirá nunca su clave privada de Bitcoin (a menos que esté autorizando un gasto). Las direcciones de Bitcoin no están vinculadas a su identidad. Usted no tiene que proporcionar identificación al crear la mayoría de las billeteras, y lo único que distingue al propietario de una billetera es conocer la clave privada.

Como tal, cualquiera que tenga su clave privada puede gastar su Bitcoin. Punto. Y no hay forma de anular transacciones o denunciar fraudes en Bitcoin. Nunca comparta su clave privada.

## **No Pierda Su Clave Privada**

Un efecto secundario de las direcciones anónimas es que no hay manera de recuperar su clave privada si la pierde. La única manera de acceder a su dirección es con esa llave. Si pierde su llave, sus fondos se irán para siempre.

La mayoría de las billeteras se encargan de esto por usted y almacenan su información clave para usted con una contraseña recuperable. Sin embargo, asegúrese de hacer una copia de seguridad de toda la información de su clave privada en varios lugares.



## **Tener Una Billetera Segura**

Como usted supondrá, una billetera es lo que contiene el Bitcoin que usted recibe. Hay muchas opciones diferentes que discutiremos, incluyendo las basadas en la web, basadas en hardware, móviles y más. Muchas personas guardan su Bitcoin de todos los días en una cartera web normal, mientras que el resto lo guardan en una cartera más segura que pueden respaldar y mantener a salvo. De esta manera, ni siquiera alguien que esté hackeando su computadora podrá tocar sus ahorros. Hablaremos más adelante sobre las diferentes carteras.

## **Saber Que El Precio Cambiará**

El precio de Bitcoin cambia cada minuto. Es importante entenderlo porque a veces puede ser un viaje accidentado. Ha ido subiendo de forma constante, pero también ha sufrido una buena parte de las caídas de valor. Hace unos años, era casi increíble que un Bitcoin valiera 100 dólares. Al momento de escribir esto, son más de once mil dólares. Aunque se espera que suba con el paso del tiempo, habrá días en los que el precio será bajo y que sepa que todo es parte del viaje.

## **No Puede Anular Pagos**

Los pagos Bitcoin no son como las tarjetas de crédito o PayPal. Una vez que usted envía dinero a alguien, es la única persona que puede devolvérselo. Con esto en mente, es vital que confíe en la persona a la que le está enviando los fondos y que siempre verifique la dirección de la billetera.

En el caso de que envíe Bitcoin a una dirección incorrecta, no es probable que lo recupere. Verifique doble y triplemente todos los detalles de la transacción antes de enviar fondos.

Si algo sucede, no hay una compañía central que pueda ayudar. Esto tiene efectos buenos y malos en el uso de Bitcoin en comparación con otros métodos de pago, pero hablaremos de todo esto un poco más adelante.

## **Las Bitcoins Son Trazables**

Dado que Bitcoin funciona en un libro de contabilidad público, cualquiera puede ver el historial de transacciones en la red. Las transacciones son solo una lista de direcciones públicas e importes de transacción. Aún así, los investigadores inteligentes pueden crear una red de transacciones e identificar tendencias. Con el tiempo, un investigador dedicado podría averiguar cuál es su dirección y ver todas las direcciones a las que ha realizado pagos con Bitcoin.

Hay formas de evitar ser rastreado en Bitcoin. Puede utilizar muchas direcciones, o incluso una nueva dirección para cada nueva transacción. También puede utilizar servicios de mezclado de monedas que enmascaran la fuente de los fondos mezclándolos con otros fondos. Aún así, vale la pena reconocer, de entrada, que el libro de cuentas público es sólo eso: público.

## **Puede Haber Problemas De Crecimiento**

Bitcoin está creciendo rápidamente, y podría haber muchos cambios que vendrán en el futuro. Las nuevas actualizaciones pueden hacer que algunos proveedores reconsideren sus servicios y precios, que las confirmaciones se ralenticen, que las tarifas suban o que ocurran muchas otras cosas. No hay forma de saber cómo cambiarán las cosas, pero mientras entiendas lo que hay detrás de todo esto, estarás bien.

## **Introducción a Bitcoin**

Esto es sólo el principio con Bitcoin. Hay mucho que aprender, pero yo te guiaré a través de él para asegurarte de que te sientas lo suficientemente seguro y bien informado para entrar en esta moneda digital de rápido crecimiento ¡que solo va a crecer!

## **Capítulo 4. Dónde guardar su bitcoin**

### **Su dirección Bitcoin**

Ha enviado un correo electrónico a alguien antes, ¿verdad? Esa dirección específica permite a esa persona enviar y recibir mensajes a cualquier otra persona en la web con una dirección de correo electrónico. Las direcciones de Bitcoin funcionan de forma similar aunque hay una diferencia clave.

## **Конец ознакомительного фрагмента.**

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.