



# CRIPTOMONEDAS

**CRIPTOMONEDAS PARA PRINCIPIANTES**



**BLOCKCHAIN Y BITCOIN**

**JORDAN SMITH**

Blockchain Y Bitcoin

Jordan Smith  
**Criptomonedas**

«Tektime S.r.l.s.»

**Smith J.**

Criptomonedas / J. Smith — «Tektime S.r.l.s.», — (Blockchain Y Bitcoin)

ISBN 978-8-87-304974-6

Muchas oportunidades de inversión han aparecido y desaparecido. Ahora es el momento de las criptomonedas, así que no pierda el tren. Las criptomonedas son la mayor redistribución de la riqueza de la historia, que apenas comienza a llamar la atención. La gente todavía está confundida sobre lo que es la cadena de bloqueo, y muy pocos entienden el potencial que tiene. ¿No es este el momento perfecto para aprender más sobre el tema? Si usted tropezó con este libro, entonces usted debe tener un interés en criptomoneda. Tal vez, sin embargo, el tema no está muy claro para usted. Este libro le informará sobre esta nueva forma de oro digital. Si está considerando invertir o si sólo desea obtener información sobre criptomoneda, este libro es para usted. En este libro, primero le familiarizaremos con los conceptos de criptomoneda, le explicaremos los diversos beneficios y riesgos que conlleva y le daremos los consejos que debe seguir al invertir en criptomonedas. Muchas oportunidades de inversión han aparecido y desaparecido. Ahora es el momento de las criptomonedas, así que no pierda el tren. Las criptomonedas son la mayor redistribución de la riqueza de la historia, que apenas comienza a llamar la atención. La gente todavía está confundida sobre lo que es la cadena de bloqueo, y muy pocos entienden el potencial que tiene. ¿No es este el momento perfecto para aprender más sobre el tema? Si usted tropezó con este libro, entonces usted debe tener un interés en la criptomoneda. Tal vez, sin embargo, el tema no está muy claro para usted. Este libro le informará sobre esta nueva forma de oro digital. Si está considerando invertir o si sólo desea obtener información sobre criptomoneda, este libro es para usted. En este libro, primero le familiarizaremos con los conceptos de criptomoneda, le explicaremos los diversos beneficios y riesgos que conlleva, y le diremos los consejos que debe seguir mientras invierte en criptomonedas. Incluso si usted piensa que la criptomoneda es completamente abrumadora y confusa - este libro lo analiza todo en un lenguaje simple y fácil de

entender - a menos que usted quiera otra historia de "si solo..." - el momento es ahora. Tome el libro hoy mismo.

ISBN 978-8-87-304974-6

© Smith J.  
© Tektime S.r.l.s.

## Содержание

Capítulo 1: Introducción	8
Capítulo 2: Conceptos básicos de Criptomoneda	10
Capítulo 3: Criptomonedas Contra moneda Fiat	12
Capítulo 4: Subida de Criptomoneda	13
Capítulo 5: Comprensión de la Tecnología de las Cadenas de Bloques	15
Capítulo 6: ¿Por qué debería alguien invertir en criptomoneda?	18
Capítulo 7: Ventajas y Desventajas	19
Capítulo 8: Mitos y Conceptos Erróneos	22
Конец ознакомительного фрагмента.	23

## Criptomonedas

### Criptomonedas para principiantes

(Blockchain y Bitcoin)

Jordan Smith

Arturo Juan Rodríguez Sevilla (Traductor)

Este documento está orientado a proporcionar información exacta y fiable en relación con el tema y la cuestión tratados. La publicación se vende con la idea de que el editor no está obligado a prestar servicios de contabilidad, oficialmente permitidos o de otro tipo. Si el asesoramiento es necesario, legal o profesional, se debe ordenar a una persona que ejerza la profesión.

- De una Declaración de Principios que fue aceptada y aprobada igualmente por un Comité de la Asociación Americana de Abogados y un Comité de Editores y Asociaciones.

De ninguna manera es legal reproducir, duplicar o transmitir cualquier parte de este documento, ya sea por medios electrónicos o en formato impreso. La grabación de esta publicación está estrictamente prohibida y no se permite el almacenamiento de este documento a menos que se cuente con el permiso por escrito del editor. Todos los derechos reservados.

La información aquí proporcionada es veraz y consistente, en el sentido de que cualquier responsabilidad, en términos de falta de atención o de otro tipo, por cualquier uso o abuso de las políticas, procesos o instrucciones contenidas en ella es responsabilidad exclusiva y total del lector receptor. Bajo ninguna circunstancia se tendrá responsabilidad legal o culpa contra el editor por cualquier reparación, daño o pérdida monetaria debida a la información aquí contenida, ya sea directa o indirectamente.

Los respectivos autores poseen todos los derechos de autor que no están en posesión del editor.

La información aquí contenida se ofrece únicamente con fines informativos y es universal en cuanto tal. La presentación de la información se realiza sin contrato ni ningún tipo de garantía.

Las marcas registradas que se utilizan no cuentan con ningún consentimiento, y la publicación de la marca registrada no cuenta con el permiso ni el respaldo del propietario de la marca registrada. Todas las marcas registradas y marcas dentro de este libro son sólo para propósitos de aclaración y son propiedad de los mismos propietarios, no afiliados con este documento.

#### Tabla de Contenidos

[Capítulo 1: Introducción](#)

[Capítulo 2: Conceptos básicos de Criptomoneda](#)

[Capítulo 3: Criptomonedas Contra moneda Fiat](#)

[Capítulo 4: Subida de Criptomoneda](#)

[Capítulo 5: Comprensión de la Tecnología de las Cadenas de Bloques](#)

[Capítulo 6: ¿Por qué deberías alguien invertir en criptomoneda?](#)

[Capítulo 7: Ventajas y Desventajas](#)

[Capítulo 8: Mitos y Conceptos Erróneos](#)

[Capítulo 9: Minería](#)

[Capítulo 10: Minería de nubes](#)

[Capítulo 11: Problemas Comunes que un Minero Puede Enfrentar](#)

[Capítulo 12: Factores a Considerar antes de Invertir](#)

[Capítulo 14: Empleo en Criptomoneda](#)

[Capítulo 15: Ganando Dinero con Criptomoneda](#)

[Capítulo 16: Altcoins - Otras Criptomonedas y Fichas](#)

[Capítulo 17: Invertir](#)

[Capítulo 18: ¿Cuáles Son Algunos de los Términos Importantes?](#)

[Capítulo 19: Cómo encontrar las mejores carteras para sus inversiones](#)

[Capítulo 20: Estrategias de Inversión](#)

Capítulo 21: Las Mejores Plataformas de Negociación

Capítulo 23: Bitcoin

Capítulo 24: El Futuro de Criptomoneda

Conclusión

## Capítulo 1: Introducción

Antes que sigan Adelante, echen un vistazo a este regalo gratuito.



**10 LIBROS GRATIS**

★★★★★

**Descargar libre**

[Haga click aquí para obtener acceso instantáneo gratuito](#)

Criptomoneda. La última palabra de moda. Parece que las noticias aparecen en las noticias casi a diario. Sólo que la palabra parece tener una llamada mágica. Sin embargo, lejos de la magia, la criptomoneda emplea principios muy científicos de la computación moderna y los principios matemáticos que permiten que tales sistemas funcionen de manera perfecta.

Las criptomonedas no podrán existir sin las computadoras.

La criptomoneda no podrá existir sin Internet.

Y el mundo no puede mantener las economías nacionales sin Internet.



Por lo tanto, el mundo de los humanos, los gobiernos que se oponen en gran medida a la criptomoneda, deben aceptar el medio económico. Más que esto, el público necesita entender cómo usar la criptomoneda y los inversores necesitan saber cómo fomentar el uso, porque el uso (la demanda) es necesaria para que el comercio se produzca dentro de la oferta. De hecho, sin demanda, no hay necesidad de oferta.

## Capítulo 2: Conceptos básicos de Criptomoneda

Criptomoneda es el nombre dado a cualquier moneda digital que se considere segura debido a la criptografía - o a un tipo particular de método de encriptación que es perfecto para todo el proceso de la cadena de bloques. Lo que es asombroso acerca de las criptomonedas es que ninguna autoridad central las gobierna. Son orgánicas y son un sistema perfecto por sí mismas. El gobierno o cualquier persona que no está involucrada en Blockchain (cadena de bloques) no puede manipularlos de ninguna manera, manteniendo sus fondos siempre bajo control. De hecho, es virtualmente imposible para cualquier cuerpo gobernante rastrear cualquier transacción y asociarla a un individuo. Esto es lo que hace que las criptomonedas sean tan fascinantes y por qué algunos gobiernos están muy en contra de las criptomonedas.

Una cosa acerca de las transacciones en criptomonedas es que pueden ser utilizadas para actividades ilícitas - como la evasión fiscal o incluso el lavado de dinero. Antes de una mayor adopción en 2017, particularmente en los primeros años, ha habido mucha controversia sobre los usos de las criptomonedas, que sólo se utiliza para actividades realizadas en la red oscura, incluyendo el tráfico de drogas.

Esto es diferente en 2017, donde ha habido una mayor aceptación de las criptomonedas, con algunos bancos que incorporan la tecnología Blockchain (cadena de bloques) y varias compañías que aceptan criptomonedas como forma de pago. El principal argumento a favor de las criptomonedas es la capacidad de las partes para enviar y aceptar fácilmente fondos entre sí, incluso en forma de criptomoneda, y sólo con comisiones de transacción mínimas. También hay muchos otros usos para la criptomoneda, incluyendo la financiación colectiva y la votación en línea. Después de todo, a las personas les resulta más fácil gastar las monedas en línea en lugar de las reales, ya que tampoco le causan demasiadas molestias.

Criptomoneda es dinero creado por el uso de técnicas de encriptación de programación avanzada de computadoras. Estas mismas técnicas se utilizan para llevar a cabo y verificar la transferencia de fondos. Las criptomonedas son independientes de los bancos centrales y están descentralizadas. Esto significa que las partes pueden enviar y recibir fondos directamente entre sí sin necesidad de intermediarios. Para la mayoría de la gente, enviar dinero es una molestia, especialmente cuando se quiere enviar dinero al extranjero. Si está transfiriendo dinero entre bancos locales, los bancos podrán tardar días en compensar y verificar las transacciones que se van a realizar. Cuando se envía al extranjero, este es un caso diferente; en ciertas situaciones esto podrá tomar más de una semana, por no hablar de las tarifas de procesamiento de las transacciones. Algunas compañías importantes como Western Union permiten transacciones más rápidas, pero esto tiene un costo, los cargos. Bienvenido Bitcoin.

En 2009, Bitcoin se convirtió en la primera criptomoneda practicable, demostrando que podía existir una moneda descentralizada. Esto es irónico, dado que el inventor de Bitcoin, Satoshi Nakamoto, nunca se propuso crear una nueva forma de dinero. Quería resolver el problema del efectivo digital centralizado y crear un sistema de efectivo digital de igual a igual. Terminó desarrollando Bitcoin, una forma de moneda totalmente no regulada, que se basaba en extensos cálculos matemáticos para validar la autenticidad. Fue con el nacimiento de Bitcoin que la criptomoneda se convirtió en una realidad, cambiando para siempre la forma en que realizamos las transacciones.

Las implicaciones de la criptomoneda son tan grandes que algunos bancos centrales han intentado involucrarse en la tecnología, y algunos han intentado emitir sus propias criptomonedas. Sin embargo, la moneda que producen no se considera oficialmente criptomoneda ya que sólo pueden desarrollar dinero centralizado. La idea detrás de la descentralización es permitir que el mercado abierto influya en el poder. Con la centralización, todo el poder y control está en el

cuerpo centralizado, los bancos centrales, lo que significa que usted y yo no tenemos voz ni voto en cuanto a la cantidad de dinero que se crea ni en cuanto a su valor. En este sentido, la Reserva Federal puede manipular el valor de las monedas tradicionales (es decir, el dólar estadounidense) imprimiendo más dinero y no hay nada que podamos hacer. Los partidarios de la criptomoneda están muy interesados en mantener la "verdadera" moneda digital descentralizada y, debido a ello, las criptomonedas han demostrado ser muy favorables. Debido a la naturaleza única de las criptomonedas, es realmente deflacionaria; a medida que pasa el tiempo, el valor de la mayoría de las criptomonedas subirá.

## Capítulo 3: Criptomonedas Contra moneda Fiat

Bitcoin y otras criptomonedas son actualmente muy volátiles. ¿Quiénes quieren comprar cualquier moneda con una fluctuación tan alta? Desafortunadamente, ahora es mucha especulación y FOMO (Miedo a perderse algo, por sus siglas en inglés). La gente no tiene idea real de para qué pueden usarlo o cómo podría cambiar el mundo, pero sólo quieren subir a bordo porque ven esas locas ganancias y quieren ser parte de él. Pero déjame preguntarte algo:

- ¿Cree usted que su moneda real, como el dólar estadounidense o el euro en su bolsillo, valdrá lo mismo mañana?

Si su respuesta es afirmativa, significa que está intangiblemente optimista acerca de la economía de su país. Cualquier moneda tiene valor porque la gente cree que seguirá teniendo valor. Cuando andábamos por ahí con monedas de oro en los bolsillos, puede que no supiéramos adónde iba el precio del oro, pero sabíamos que el oro seguirá siendo oro, y esto era todo lo que contaba en el pasado: la confianza en el sistema.

Ninguna divisa puede estar totalmente libre de volatilidad - la tendencia a subir y bajar de valor. Por el momento, nuestra moneda fiduciaria familiar está menos sujeta a fluctuaciones salvajes que la criptomoneda, pero aún no sabemos cómo va a cambiar en el futuro.

Los gobiernos económicamente atados pueden anunciar una mañana que han decidido dar a los ahorros de todos un pequeño recorte en la parte superior! Si usted se fija en cualquier crisis actual como la de Venezuela, verá que el gobierno tiene el control total de su dinero y sus ahorros. De repente, ya no funciona ningún cajero automático, y si no tiene un montón de dinero en efectivo o comida en alguna parte, puedes estar en serios problemas. Ahora para muchos, este es un ejemplo extremo, y nadie puede imaginar que esto nos suceda porque hemos estado viviendo en tiempos de paz durante mucho tiempo. Piensa que su moneda es estable hasta cierto punto y que seguirá siéndolo en el futuro.

Otro ejemplo de control y regulación total de la moneda fiduciaria puede ser la impresión bajo demanda. Aunque la mayoría de la gente piensa que esta afirmación está sobrevalorada, todos los órganos rectores de todo el mundo pueden crear fácilmente moneda fiduciaria adicional de la nada. Al aumentar la oferta total de FIAT (dinero regulado por el gobierno, por sus siglas en inglés) respaldada por el valor anterior, todo el dinero en circulación se vuelve menos valioso. Hablando de moneda fiduciaria "respaldada" por activos para simplemente crear la ilusión de valor, el dólar estadounidense no ha estado atado a un activo tangible desde hace bastante tiempo. De hecho, cada dólar estadounidense en circulación está respaldado únicamente por "la fe y el crédito plenos de los Estados Unidos" y ya no tiene ningún valor inherente o intrínseco.

Además, una vez que se ha generado nuevo dinero impreso de la nada sin valor para él, el Tesoro de los Estados Unidos distribuye todos los fondos adicionales a uno de los doce bancos de la Reserva Federal. Los Bancos de la Reserva Federal crearon un ecosistema no transparente en el que un puñado de personas determinan la riqueza de toda una nación. Todas estas instituciones financieras pueden simplemente hacer lo que les plazca, ya que no hay un supervisor directo de ninguna rama del gobierno. Esta es una gran preocupación para el mundo libre.

## Capítulo 4: Subida de Criptomoneda

Las criptomonedas, como Bitcoin, Ethereum, Litecoin y otras, han tenido mucha publicidad, especialmente en 2017. Esto se debe principalmente a la gran exposición dada por las noticias, los medios sociales y las instituciones financieras. A medida que los niveles de alfabetización financiera/digital de la población en general han aumentado, la aceptación de la criptomoneda también ha dado un salto en el poder adquisitivo. En 2010, un inversor de Bitcoin, conocido como Laslo, afirmó haber comprado dos pizzas por aproximadamente 10.000 Bitcoins. Se considera el primer caso en el que se utilizó una criptomoneda para realizar una compra. En ese momento, Bitcoins prácticamente no valían nada. A partir de noviembre de 2017, Bitcoin tiene un valor superior al del oro, con una moneda de casi 10.000 dólares.

Al principio, la mayoría eran muy escépticos respecto a Bitcoin y su tecnología, ya que la veían como una forma de falsificación o como un dispositivo de delincuentes. Esto fue particularmente así cuando se publicitó como el medio de comercio en la "Ruta de la Seda", una parte de la oscura Internet donde todo tipo de comportamiento desagradable era desenfrenado.

Sin embargo, ahora hay una creciente participación de empresas y gobiernos legítimos con criptomoneda. Se incorporan nuevas aplicaciones e incluso cajeros automáticos para permitir que se realicen transacciones en criptomoneda. Como consecuencia, la capitalización de mercado de todas las criptomonedas es de más de \$250,000,000,000,000!

A mediados de 2017, hemos visto un aumento en las criptomonedas, revelando más de 1000 criptomonedas. La mayoría de la gente ha oído hablar de Bitcoin, especialmente desde que los recientes ataques de rescate han exigido el pago en Bitcoins. El beneficio para los criminales de esto es que cualquier pago por parte de la víctima será imposible de rastrear.

Si se revisa el sitio web de coinmarketcap, se verá que hay un pequeño gráfico al lado del tipo de criptomoneda, cada uno mostrando el movimiento de la moneda en la última semana, así como el cambio porcentual en las últimas 24 horas. Se verá que hay una disparidad significativa en los valores de las diversas criptomonedas con un Bitcoin que vale casi \$10,000 y una capitalización de mercado total de más de \$150,000,000,000. Otra moneda criptográfica llamada Bytecoin valía menos de un centavo, aunque la capitalización total de Bytecoins era de más de 200 millones de dólares. Algunas criptomonedas tienen pequeñas capitalizaciones. Un ejemplo es mikethemug criptomoneda con una capitalización de aproximadamente \$1000! Sólo leyendo esto, se está preguntando cómo una moneda como 'mikethemug' puede ser tomada en serio, y con todo respeto por mikethemug, es realmente más fácil de lo que la mayoría de la gente piensa crear y emitir una moneda, lo que hace que algunos individuos sean bastante escépticos acerca de las criptomonedas.

Aunque hay muchos proyectos potenciales válidos y emocionantes dentro de las criptomonedas, hay que tener en cuenta que también hay muchas monedas de 'broma' sin valor fundamental real. Un buen ejemplo es Dogecoin que yo mismo encuentro bastante histórico, sin embargo, la moneda en sí no sirve para nada más que para representar el patriotismo que la sociedad ha creado a través de memes históricos e Internet. Para ponerlo en perspectiva, Dogecoin tiene una capitalización de mercado de más de 200.000.000 de dólares, basada en el meme de un perro.

Tendremos más que decir sobre la calidad y el valor de las criptomonedas más adelante.

Criptomoneda como dinero

A pesar de la palabra "moneda" en la palabra "criptomoneda", existen mayores similitudes entre criptomonedas y stocks que entre criptomonedas y criptomonedas fiat. Una compra de un poco de criptomoneda es semejantemente una compra de una acción de la tecnología, de una entrada en un libro mayor digital llamado un blockchain, y de una parte de la red digital para esa criptomoneda.

La compra de criptomoneda es similar a la compra de acciones porque cada 'criptomoneda' representa un proyecto diferente. Cuando usted compra estas criptomonedas, está comprando una acción dentro del proyecto. Un ejemplo de lo cual es Ethereum o Ether. Tener Ether permite al inversor participar en la votación dentro de la red Ethereum.

La criptomoneda es un medio de intercambio que utiliza la criptografía para que las transacciones sean seguras. Se utilizan para ejercer control sobre la fabricación de otras unidades de la moneda. Las criptomonedas son un tipo de lo que se llama monedas alternativas; diferentes de las monedas tradicionales, como las que todo el mundo conoce, el dólar estadounidense, el euro, la libra esterlina, etc.

Debido a sus frecuentes y grandes fluctuaciones de valor, uno de los dos fundamentos del dinero, a saber: "una reserva de valor", está ausente. Dentro de cualquier mercado nuevo, hay grandes fluctuaciones en los precios de los activos. Pero a medida que el mercado comienza a crecer con el tiempo, verá la estabilidad de precios, así como más usos institucionales y comerciales. Un buen ejemplo es el mercado de valores en períodos de recesión, donde la incertidumbre generalmente conduce a grandes fluctuaciones en los precios. Sin embargo, la mayoría de las veces, los precios de las grandes empresas de capitalización en el mercado de valores son bastante estables. Dentro del mercado de la criptomoneda, Bitcoin está empezando a desarrollarse como la criptomoneda más estable.

Inicialmente, Bitcoin se lanzó inicialmente para permitir la realización de transacciones descentralizadas entre pares, pero debido a la explosiva popularidad de Bitcoin en los últimos años, Bitcoin se ha convertido en una tienda de valor debido a los ridículos costes de transferencia de Bitcoin entre carteras. Muchos individuos ven a Bitcoin como el estándar de oro dentro del mundo de las criptomonedas, y al igual que el oro, muchos inversores eligen mantener a Bitcoin dentro del mercado de las criptomonedas. Algunas monedas digitales exhiben el comportamiento de países con inflación significativa en los que no se retiene ese valor.

## Capítulo 5: Comprensión de la Tecnología de las Cadenas de Bloques

Si has oído un par de cosas sobre las criptomonedas, puede que haya oído hablar de la cadena de bloques, que es la tecnología que impulsa a Bitcoin y a cientos de otras criptomonedas. Más allá de esta definición común, ¿sabe qué es realmente la cadena de bloques? ¿Sabe cómo funciona?

La cadena de bloques tal y como la conocemos hoy en día es la ingeniosa idea del inventor pseudónimo de Bitcoin, Satoshi Nakamoto. Descrito de manera sencilla, la cadena de bloques es un registro público descentralizado y permanente de transacciones. En otras palabras, la cadena de bloques es un libro mayor público donde las entradas no pueden ser alteradas una vez que han sido agregadas. Sin embargo, también es descentralizada. ¿Qué significa esto?

La descentralización significa que no hay una autoridad central a cargo del poder de tomar decisiones. En cambio, esta responsabilidad se delega a todos los miembros de la organización. Con la cadena de bloques, esta responsabilidad recae en todos los ordenadores de la red. Por lo tanto, ninguna entidad puede regular la cadena de bloques. En cambio, los miembros se relacionan entre sí basándose en reglas matemáticas que todos tienen que obedecer. Si hay que tomar una decisión o realizar una transacción, todos los ordenadores de la red tienen que estar de acuerdo en que se ha producido para poder verificarla. Para facilitar la comprensión del concepto de descentralización, utilizaré una ilustración:

Tradicionalmente, cuando dos personas querían colaborar en un documento, una persona trabajaba en él y se lo enviaba a la otra para que le añadiera sus revisiones. En este escenario, la primera persona no puede ver las modificaciones realizadas por la otra persona hasta que se devuelva una copia del documento revisado. La primera persona también tendrá que esperar a que el documento revisado sea devuelto antes de hacer cualquier otro cambio. Al final, será una sola persona la que decidirá qué versión deberá utilizarse como la versión correcta. Sin embargo, si las dos personas utilizaran el software Google Docs, ambos tendrían acceso al documento simultáneamente. Ambos podrían hacer cambios al mismo tiempo y la última versión del documento estaría disponible para ambos al mismo tiempo.

Tener que enviar el documento para que se realicen los cambios se puede comparar con el funcionamiento actual de las bases de datos. Este es el sistema utilizado por los bancos para procesar los saldos y transferencias de dinero. El acceso se bloquea brevemente en un lado, se realiza la transferencia y luego se vuelve a abrir el acceso. La cadena de bloques, por otro lado, puede compararse con la aplicación de Google Doc, en la que todo el mundo tiene el mismo registro del libro mayor público en todo momento. Sin embargo, en lugar de ser compartida entre dos personas, la cadena de bloques se distribuye entre varias personas. Sin embargo, la cadena de bloques lo lleva un paso más allá. En lugar de que una persona tome una decisión sobre qué documento debe utilizarse como la versión correcta, todas las personas con acceso al documento tienen que llegar a un acuerdo sobre la versión correcta. Esto le da a la cadena de bloques una robustez similar a la de Internet. No puede ser controlado por una sola persona y no tiene un solo punto de fallo.

Al igual que la aplicación Google Doc, la cadena de bloques siempre está en un estado de consenso. Se comprueba cada pocos minutos y se actualiza automáticamente a la última versión de todos los nodos. Los grupos de transacciones entre cada actualización automática se conocen como un bloque. El constante estado de consenso tiene dos efectos. En primer lugar, mejora la transparencia, ya que la última versión de la base de datos es visible para todos los miembros de la red. Más importante aún, significa que la cadena de bloques no puede ser corrompida. Corromper la cadena de bloques significaría obtener el control de la mayoría de los ordenadores de la red. Aunque esto parece posible en teoría, es muy poco probable que ocurra, ya que necesitaría

grandes cantidades de potencia computacional. Tomar el control de la cadena de bloques también destruiría el valor de las criptomonedas.

#### Una Red de Nodos

La cadena de bloques está formada por una red de ordenadores conocidos como nodos. Estas computadoras ejecutan el protocolo de cadena de bloques, lo que les permite enviar y recibir mensajes entre sí. Los nodos pueden unirse a la red voluntariamente. Una vez que un nuevo nodo se une a la red, descarga automáticamente la última versión del bloque. Estos nodos son uno de los elementos más importantes de cualquier red de cadenas de bloques. Una vez que un nodo se une a la red, se convierte en un co-administrador de la red. Se le ha dado la responsabilidad de ayudar a verificar cada una de las transacciones que se realizan en la cadena de bloques. Después de la verificación, el nodo registra la operación en un bloque. Esto continúa hasta que se completa un bloque, después de lo cual el nodo lo añade a la cadena de bloques. La posibilidad de ganar monedas de nueva creación actúa como un incentivo para que los nodos realicen estas tareas administrativas en la red de la cadena de bloques.

Cuando un usuario envía monedas a otro usuario, los nodos verifican los datos de la transacción para asegurar la validez de la misma. Compara los datos de la transacción con su versión de la cadena de bloques y comprueba que las monedas no se han gastado dos veces. En caso de que el nodo determine que los datos variables no son válidos, rechaza automáticamente la operación. También rechaza cualquier otra comunicación con el nodo que envía la transacción. Los nodos tienen una relación no basada en la confianza con otros nodos de la red. Por lo tanto, si un nodo envía datos no válidos a los otros nodos, inmediatamente cortan la comunicación con este nodo y lo banean de la red.

Sin embargo, si el nodo determina que los datos de la transacción son válidos, la transacción se envía a los mineros. Los mineros agrupan las transacciones en orden cronológico para formar bloques. Una vez que se completa un bloque, se devuelve a los nodos para su verificación. Toda la validación se realiza por nodos ya que es imposible para ellos propagar información incorrecta. Una vez que los nodos confirman la validez de un bloque, pueden añadirlo a la cadena de bloques.

La eficacia de la tecnología de cadenas de bloques se basa en las siguientes tres tecnologías principales:

#### Criptografía de clave privada

La cadena de bloques hace posible que las personas puedan realizar transacciones a través de Internet sin necesidad de un tercero de confianza. Sin embargo, para que la transacción sea segura, tiene que haber una forma de confianza. En Internet, la confianza se reduce a dos cosas: autenticación (prueba de identidad) y autorización (prueba de permisos). En pocas palabras, tiene que haber una manera de verificar que alguien es realmente quien dice ser y que tiene el permiso para hacer lo que sea que está tratando de hacer.

En el caso de la tecnología de cadenas de bloques, la confianza se establece mediante el uso de criptografía de clave privada. La criptografía se basa en las matemáticas para cifrar la información en un código secreto al que no pueden acceder entidades no autorizadas. Para acceder a la información, necesitan una clave para descifrarla.

Una transacción en criptomoneda básicamente involucra a alguien que envía datos encriptados a otra persona. Cada vez que alguien realiza una transacción en la cadena de bloques, la transacción se cifra utilizando claves criptográficas. Para cada transacción se generan dos claves enlazadas matemáticamente: una pública y otra privada. Para realizar una transacción cifrada, se necesita la clave pública. Para descifrar la transacción, hay que tener la clave privada. La clave privada es la dirección de la billetera de criptomoneda, que permite a cualquiera enviar datos cifrados (las monedas cripto) al propietario de la billetera. Sin embargo, para que el propietario reciba las monedas, tiene que descifrar los datos utilizando su clave privada. La clave privada muestra que usted es el propietario de la dirección de la billetera. La clave privada también confirma



que tiene permiso para realizar transacciones, es decir, que tiene suficientes monedas para realizar transacciones. A través de la clave privada, la cadena de bloques confirma la autenticidad y la autorización, resolviendo así el problema de la confianza.

#### Una red distribuida

Para que la cadena de bloques sea efectiva, la autenticación y la autorización no son suficientes. También se necesita una red distribuida de par a par. Esta red ayuda a resolver el problema de seguridad y mantenimiento de registros. Para que las transacciones sean aceptadas como válidas, deben ser confirmadas por toda la red. Esto puede ser explicado usando un famoso experimento de pensamiento conocido como "si un árbol cae en el bosque". Sin embargo, nuestro experimento de pensamiento será modificado ligeramente.

Si un árbol cayó en un bosque y hay dos cámaras grabando el evento, entonces podemos estar seguros de que el árbol realmente cayó ya que hay evidencia visual del evento. Sin embargo, si una cámara grabó la caída del árbol mientras que la otra no lo hizo, entonces no podemos estar seguros de que el árbol realmente cayó. Este es el concepto detrás del valor de la red de cadenas de bloques. Los nodos dentro de la red son las cámaras en nuestra analogía. Si los nodos están de acuerdo en que el evento ocurrió en un momento determinado, entonces hay certeza de que el evento ocurrió. Para que una transacción sea confirmada como válida, la mayoría de los nodos tienen que llegar a un consenso de que la transacción realmente ocurrió. Sin embargo, en lugar de utilizar cámaras, los nodos utilizan rompecabezas matemáticos para la validación.

Cuando la criptografía de clave privada se combina con esta red distribuida, la cadena de bloqueo se vuelve más eficaz. Una persona, usando su clave privada para probar autenticidad y autorización, anuncia a la red que está haciendo una transacción, toda la red observa la transacción y confirma que efectivamente ha ocurrido.

#### Un incentivo para la seguridad y el mantenimiento de registros

Mientras que la combinación de la criptografía de clave privada y una red distribuida parece infalible, tiene un defecto. ¿Por qué los nodos deberían estar esperando para observar y confirmar que una transacción ha tenido lugar? Dicho de otra manera, ¿cómo atrae la red a los nodos para confirmar las transacciones y hacer que la red sea segura? Aquí es donde entra en juego la minería. Al realizar tareas administrativas y garantizar la seguridad de la red, los nodos son recompensados con monedas de nueva creación. El interés propio de los nodos se utiliza para el bien público.

## **Capítulo 6: ¿Por qué deberías a alguien invertir en criptomoneda?**

Blockchain (cadena de bloques) es la base de varias criptomonedas y blockchain es lo más grande que le ha pasado a la contabilidad desde la invención de los cheques de papel. Más grande, de hecho. No va a ninguna parte y seguramente se implementará de muchas maneras creativas en las próximas décadas. Con esa base intacta, la gente continuará desarrollando y usando criptomonedas.

Las criptomonedas democratizan las economías, poniendo el poder en manos del pueblo y fuera de los bancos centrales tan vilipendiados en la era de la información. Además, debido a que estas monedas se encuentran en las etapas iniciales de desarrollo, aún queda mucho dinero por ganar y cualquiera puede empezar a invertir en cualquier momento.

Finalmente, dada la enorme popularidad de las criptomonedas, esta tecnología no va a desaparecer. Entrar en el comercio de criptomoneda hoy en día es como lanzar un sitio web en Internet cuando todavía había dominios de una sola palabra.

Por lo tanto, cualquier persona interesada en invertir o comerciar en criptomonedas necesita entender por qué existen, cómo llegaron a ser, y qué le depara el futuro a la nueva economía. El Capítulo Uno ayuda a los lectores a hacer precisamente eso.

El Capítulo Dos examina cómo las criptomonedas son diferentes y como son las monedas nacionales tradicionales. También desarrolla los principios sobre los que se crean las criptomonedas. Esto ayuda a los inversores a entender cómo utilizar las estrategias existentes en la nueva economía.

Para aquellos que no están familiarizados con el comercio de moneda nacional, el Capítulo Tres lo examina en los términos más sencillos. Para aquellos que están aprendiendo, será interesante y revelador. Para los experimentados, deberá ser un viaje humorístico por el sendero de los recuerdos.

Por supuesto, como muchos ya saben, Blockchain es el genio mágico detrás de Bitcoin. Sin embargo, existen sistemas alternativos que se basan en el modelo de libro mayor distribuido de la contabilidad moderna. Los Capítulos Cuatro y Cinco consideran la tecnología que hace posible el sistema económico más democrático jamás concebido, junto con las razones para utilizar la nueva moneda.

El Capítulo Seis es para aquellos que simplemente quieren comerciar e invertir en criptomonedas como el comercio en los mercados monetarios tradicionales o en acciones. Se discuten los principios que ayudan a los inversores a saber cómo ayudar a sus monedas a tener un mejor rendimiento, cómo identificar las mejores criptomonedas y cómo localizar las bolsas preferidas.

Finalmente, en el Capítulo Siete se proporcionan a los lectores varias herramientas útiles para guiarlos en la compra, venta, comercio e inversión en criptomonedas en todo el mundo. Por ejemplo, aquellos que tienen problemas para encontrar un intercambio adecuado y que tienen un sitio de wordpress pueden decidir usar un plugin para crear el suyo propio. De hecho, wordpress tiene una gran cantidad de plugins relacionados con varias características del comercio en criptomoneda.

Entonces, ¿por qué deberías a alguien invertir en criptomonedas?

Con eso, podemos ofrecerle una feliz inversión en cripto.

## Capítulo 7: Ventajas y Desventajas

Si usted invierte en criptomonedas sabiamente, puede conducir a un camino de fortuna.

Erik Finman es un ejemplo de una historia de éxito. Invertió en bitcoins a 12 dólares cada uno en 2011. Actualmente (diciembre de 2017), 403 fichas bitcoin están en su poder, y actualmente, esas fichas bitcoin valen millones!

Por otro lado, incluso si usted invierte en criptomonedas sabiamente, hay una posibilidad de que usted todavía puede perder. Después de todo, el precio de tales inversiones no está garantizado que suba continuamente. Pero esto no es raro, no solo para las inversiones en criptomoneda, sino para todo tipo de inversiones.

El lado positivo



Una de las principales ventajas de las inversiones en criptomoneda es la descentralización. La descentralización puede lograrse mediante la creación de tokens proxy. Un sistema de depósito en garantía también puede funcionar bien.

La descentralización es favorable para la mayoría, si no para todos, los ciudadanos. Esto significa que ninguna autoridad central está a cargo de las criptomonedas. Nadie puede tomar las decisiones sobre ellas, ni siquiera el gobierno. Por lo tanto, si usted es el dueño de criptomonedas, la manera de su distribución depende de usted.

Esto también significa que una criptomoneda es procesada a través de una red de base (de igual a igual). Con un sistema descentralizado, las transacciones se realizan directamente en vez de pendientes de acuerdo a las acciones de un intermediario.

Aparte de la descentralización, aquí están las otras ventajas de las criptomonedas:

- **Transacciones Instantáneas.** Las transacciones realizadas utilizando criptomonedas en la red de la cadena de bloques niegan la necesidad de servicios de terceros. Si bien pueden ayudar en dichas transacciones, estos proveedores de servicios de terceros (por ejemplo, notarios, abogados y corredores) pueden causar retrasos.

- Debido a su ausencia en las transacciones, los individuos pueden hacer transacciones directas - casi instantáneamente. Tan pronto como deciden enviar dinero, estas personas pueden esperar que sus transacciones estén listas para su procesamiento inmediato, y en cuestión de horas, anticipan su finalización.

- **Accesibilidad Pública.** Hay más de 2.000 millones de personas en todo el mundo que tienen acceso a Internet. Pero no todas estas personas tienen acceso a los sistemas de intercambio tradicionales. Esta es una solución práctica para su problema, ya que no sería necesario que estuvieran buscando un banco cuando no lo hay.

- Por ejemplo, Kenia tiene un sistema M-PESA, un sistema de financiación y microfinanciación. Si usted es residente del país, poseer una billetera en criptomoneda puede abrirle las puertas.

- Particularmente, si usted posee una billetera móvil basada en criptomoneda, usted es elegible para hacer transacciones desde la comodidad de su hogar.

- **Más Asequible.** Como ya se ha mencionado, las transacciones realizadas con criptomoneda no requieren la participación de un tercero. Debido a esto, es innecesario cubrir un porcentaje que se supone que es para el tercero.

- Además, los cambios de criptomoneda no cobran comisiones de transacción... Por supuesto, la ausencia de comisiones de transacción equivale a comisiones globales más bajas. Esto es posible gracias a la compensación automática para los mineros de la red de una criptomoneda en particular.

- **Reconocimiento Universal.** Las criptomonedas son operacionales a nivel universal, lo que significa que son aceptables en cualquier país. Esta ventaja no se ve con las monedas tradicionales, que le obligan a convertirlas primero antes de usarlas.

- Por ejemplo, si usted está en México, necesita que su moneda fiduciaria sea convertida a MXN (peso mexicano). De lo contrario, los establecimientos en México podrán considerarlos inaceptables y, por lo tanto, no utilizables.

- Por otro lado, si está en México con tokens de Ether, no necesita convertir tus tokens de Ether a MXN. Si un establecimiento en México acepta tokens de Ether, usted puede usar estas criptomonedas para comprar tantos bienes y/o servicios como desee.

- Cero casos de robo de identidad y transacciones fraudulentas. Las criptomonedas están diseñadas para funcionar según un sistema de "empuje". Esto permite que las transacciones se realicen sin problemas sólo con información sobre la cantidad exacta entregada al comerciante.

- Los titulares de tarjetas de crédito se ven privados de esta ventaja. Cuando envían un pago, necesitan enviar su tarjeta de crédito (junto con otra información personal) al comerciante. Esto significa que un comerciante puede acceder fácilmente a la información personal.



### Los inconvenientes



Cuando usted profundiza en las inversiones en criptomoneda, hay una regla para memorizar su nombre de usuario y contraseña - o al menos, asegurarlos. Tales detalles son vitales y la recuperación es casi imposible una vez que se pierden.

Si olvida el nombre de usuario y la contraseña de su cuenta de correo electrónico, una solución rápida es pulsar el botón "¿Olvidé la contraseña? Link. Pero una billetera en criptomoneda no funciona de la misma manera. Con una billetera de criptomoneda, no existe tal cosa como una solución rápida.

Aquí están los otros inconvenientes de estas inversiones:

- **Una tasa relativamente baja de adopción.** Mientras que su popularidad está aumentando, las criptomonedas son extrañas para algunas personas. Peor aún, una parte de esa gente no muestra el más mínimo interés en aprender su sistema.

- Incluso bitcoin, que es el más popular en su categoría, no es conocido por todos. Bitcoin existe desde hace más de cinco años. Pero aún así, no todo el mundo puede utilizarlo porque una de las partes (o ambas) en una transacción es nueva en su concepto.

- **Transacciones Irreversibles.** Las transacciones en Criptomoneda son altamente seguras. Aunque esto debería ser ventajoso, podría ser contraproducente para usted. No puede intervenir una vez que has iniciado el proceso.

- Es necesario tener mucho cuidado cuando se envía una gran cantidad de criptomonedas a alguien. Usted necesita estar absolutamente seguro de que está enviando dinero a la persona correcta.

- De lo contrario, la única manera de recuperar el dinero perdido es pedirle a la persona del otro lado que lo devuelva. El triste hecho es que puede que no lo conozca en absoluto. Recuerde, el anonimato es parte del trato.

- Es un gesto amable de su parte devolverlo. Pero si decide no hacerlo, puede ser casi imposible recuperarlo.

- **La Necesidad de Internet.** Usted no puede iniciar transacciones en criptomoneda sin una conexión a Internet decente. Esta es una gran preocupación para las personas que viven en países del tercer mundo (por ejemplo, India y Cuba) y, si Internet se hunde durante un día (aunque es poco probable), los mercados financieros sufrirán una caída devastadora.

- Una cualidad redimible de esto es el rápido desarrollo de propuestas para una conexión a Internet decente en todo el mundo. Con esto en mente, este inconveniente puede superarse con el tiempo.



### El límite de suministro actual



Otro factor molesto es el límite de suministro de una criptomoneda - con la excepción del suministro de monero -. De acuerdo con aquellos que están preocupados por su estado de suministro, llegarán el día en que el suministro se vacíe. De hecho, una persona puede presentar una ecuación de cuando se agotará el suministro de una criptomoneda.

La ONU (Organización de las Naciones Unidas) dice que la población mundial alcanzará la friolera de 9.700 millones para el año 2050. Digamos que aunque sólo una tercera parte de esa población, que es de aproximadamente 3.230 millones, posee una sola muestra de criptomoneda, el suministro parece estar lejos de ser adecuado.

Bitcoin, por su parte, tiene una oferta de 21 millones (a partir de 2018). En total, usted puede extraer sólo 21 millones de bitcoins. Para 3.230 millones de personas, 21 millones de bitcoins son muy pocos.

El lado positivo es que la oferta puede crecer. Aunque todavía no se ha hablado de ello, sigue siendo una posibilidad.

¿Quién sabe? Los desarrolladores pueden cambiar el protocolo de criptomoneda para permitir más espacio. Tal vez, pueda alcanzar más de un trillón para entonces.

Otro lado positivo es que el número de criptomonedas en particular está aumentando. En los primeros días, había menos de cinco de ellos. Ahora, hay una alineación de Altcoins. Tiene ADA, IOTA, dogecoin, EOS y monero. Si puede recordar, el suministro de Monero es ilimitado.

## Capítulo 8: Mitos y Conceptos Erróneos

Muchas personas todavía dudan en invertir en criptomoneda o incluso en intentar utilizarla. Los diferentes mitos y conceptos erróneos que rodean a la criptomoneda podrían ser los principales culpables de este comportamiento, y la negativa de la gente a dar a la moneda digital la oportunidad de demostrar su valor. Lo alarmante es que los mitos y conceptos erróneos parecen ser auténticos a los ojos de las personas que no tienen suficiente conocimiento sobre la criptomoneda. Lo desafortunado es que estas personas no se molestan en investigar más sobre criptomoneda y ver si la información que obtienen es verdadera o no.

## **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.