

BITCOIN

LA MONEDA DEL FUTURO



TODO LO QUE DEBES SABER SOBRE
BITCOIN Y LOS MONEDEROS VIRTUALES
EN 60 MINUTOS

FERNANDO AMADOR

BITCOIN: LA MONEDA DEL FUTURO

**Todo Lo Que
Debes Saber
Sobre Bitcoin Y
Los Monederos**

Virtuales, En 60 Minutos

**Fernando
Amador**

Título: Bitcoin: La Moneda Del Futuro

© 2018, Fernando Amador

© De los textos: Fernando Amador

Ilustración de portada:
www.kin25.com

Revisión de estilo:
www.escritoyhecho.com

1ª edición

Todos los Derechos Reservados.

Para Isabel, por toda la felicidad
que has traído a mi vida.

Para David, con admiración.

Para Mamá y Papá, por ser pilares
inquebrantables.

¡¡IMPORTANTE!!

No tienes los derechos de Reproducción o Reventa de este Producto.

Este libro tiene Todos los Derechos Reservados.

Antes de venderlo, publicarlo en parte o en su totalidad, modificarlo o distribuirlo de cualquier forma, te recomiendo que consultes al autor.

El autor no puede garantizarte que los resultados obtenidos por él mismo al aplicar las técnicas aquí

descritas, vayan a ser los tuyos.

Básicamente por dos motivos:

Sólo tú sabes qué porcentaje de implicación aplicarás para implementar lo aprendido (a más implementación, más resultados).

Aunque apliques en la misma medida que él, tampoco es garantía de obtención de las mismas ganancias, ya que incluso podrías obtener más, dependiendo de tus habilidades para desarrollar nuevas técnicas a partir de las aquí descritas.

Aunque todas las precauciones se han tomado para verificar la

exactitud de la información contenida en el presente documento, el autor y el editor no asumen ninguna responsabilidad por cualquier error u omisión.

No se asume responsabilidad por daños que puedan resultar del uso de la información que contiene.

Así pues, buen trabajo y mejores Éxitos.

Tabla de Contenidos

[Antes De Comenzar...](#)

[Introducción](#)

[Capítulo I. Sentando Las Bases](#)

[Capítulo II. ¿Por Qué Confiar En El Bitcoin?](#)

[Capítulo III. Cómo cambiará El Bitcoin al mundo](#)

[Capítulo IV. Riesgos Del Bitcoin](#)

[Capítulo V. Seguridad Del Bitcoin](#)

[Capítulo VI. Monederos Virtuales](#)

[Capítulo VII. Cómo Mantener Tus Monedas A Salvo](#)

[Conclusión](#)

[Recursos Y Links De Interés](#)

ANTES DE COMENZAR...

Así como el correo electrónico y la telefonía móvil han cambiado las comunicaciones; hoy día, el Bitcoin cambiará la forma en la que vemos el dinero y nos permitirá acceder a una economía más libre, accesible y versátil.

Al momento de crear este libro, que forma parte de una serie de 6 libros, tomé en cuenta las diferentes oportunidades que el uso del Bitcoin podría proporcionarte, con la esperanza de que sea para ti

una guía fácil y completa para entrar en el universo del Bitcoin.

¿Y por qué 6 libros cortos y no uno más extenso?

Porque considero que así, te será mucho más fácil asimilar los conceptos específicos que toco en cada uno de ellos, y de los que te voy a hablar en un momento, de tal manera que al consultar sobre algo en específico, te será mucho más sencillo encontrar la información.

Esta serie de 6 libros tiene la finalidad de que tú, como nuevo usuario de Bitcoin, te puedas poner marcha y comiences a entender las

virtudes del Bitcoin.

Esto, no solo te ayudará a emprender nuevos proyectos, sino que te permitirá tomar la iniciativa de fortalecer esta comunidad que va en aumento.

A través de este libro, y los 5 que vendrán posteriormente, te quiero entregar todo el conocimiento de base e infinidad de tips claros y simples, que te permitan avanzar por ti mismo.

En otras palabras, en lugar de cubrir minuciosos detalles técnicos, te voy a explicar todo lo que debes saber, de una manera simple y

clara para que logres entenderlo al instante y avances de manera rápida y eficiente.

Para entender y utilizar el Bitcoin requeriras entender los conceptos básicos que lo rodean, este libro te permitirá hacerlo de manera fácil y agradable.

Al igual que con el surgimiento de cualquier nueva tecnología, es necesario disponer de información amigable, que seamos capaces de comprender y poder aplicar en nuestro día a día.

Por eso, he creado esta serie de 6 libros que espero que te ayuden de

tal forma que sean tu ticket de entrada al tren de esta nueva manera de ver la economía y compruebes por ti mismo todo lo que puede llegar a ser el Bitcoin y el beneficio que obtendrás de él si lo dominas.

¿Qué obtendrás de cada libro?

Esta es una perspectiva global de los temas que te voy a mostrar en cada libro:

En este, el primer libro de la

serie, te voy a mostrar los fundamentos básicos de la red Bitcoin, para que tengas claro cómo se generan los Bitcoins, cuáles son las medidas de seguridad e incluso, te voy a contar los riesgos que implica esta tecnología emergente.

Es decir, una vez termines la lectura de este libro, tendrás una visión general y clara del funcionamiento del Bitcoin y cómo obtener tu primer monedero virtual.

En el segundo libro te contaré cómo intercambiar tus Bitcoins, algunos temas legales que debes

considerar, cómo debes usar las llaves privadas y públicas y las diferencias entre las principales criptomonedas.

Ya en el tercer libro, te enseñaré a usar de manera práctica tus monedas. Desde cómo invertir en ellas, pasando por cómo usarlas para pagar y cobrar productos y/o servicios, hasta cómo usarlas en tu vida diaria.

En el cuarto libro profundizaré un poco más en el uso de las carteras o monederos virtuales y en el tema

de la minería de Bitcoins.

En el quinto libro te voy a dar ejemplos prácticos, herramientas y algunas recomendaciones sobre cómo integrar esta tecnología en tu negocio.

Este es el siguiente paso en la economía.

Y en el sexto libro te hablaré sobre el enorme impacto y las repercusiones que tendrá globalmente el Bitcoin y de qué manera cambiará al mundo.

Además, te ayudaré a reflexionar acerca del nuevo paradigma económico y de cómo te beneficia o perjudica.

¿Qué hay detrás de este libro?

Detrás de todo proyecto existen incontables horas de investigación apasionada y horas de trabajo sin descanso para alcanzar una meta, pero en este caso, tenemos que sumar los años de avances tecnológicos que han contribuido a la implementación y crecimiento de

la tecnología del Bitcoin.

Tanto este libro que tienes ahora ante ti como toda la serie, no solo se apoya en estos grandes esfuerzos, sino en toda la comunidad de desarrolladores, inversores y usuarios que han ayudado a consolidar el Bitcoin como la moneda del futuro.

Quiero que tomes este primer libro como una guía para el manejo de Bitcoin y la instalación de tu primer monedero virtual, algo muy importante para ti, ya que te va a ayudar a entender conceptos que en adelante serán esenciales y que te prepararán para usar los Bitcoins

de manera fácil y segura.

Es por eso que este libro cubre específicamente toda la parte inicial que debes conocer, es decir, una vez termines de leer y aplicar todo cuanto estoy a punto de entregarte, vas a tener una base firme para avanzar rápidamente en el mundo de las criptomonedas.



¿Qué vas a aprender concretamente?:

Qué es el Bitcoin, su diseño, filosofía y lo que puede hacer por ti.

Definiciones relevantes de esta nueva tecnología y **por qué debes confiar** en el Bitcoin.

Algunas opciones para invertir en Bitcoins y la forma en la que éste cambiará al mundo.

Verás un breve tutorial de **introducción a los monederos virtuales** para usuarios sin experiencia previa, que te proporcionará el suficiente

conocimiento para que puedas moverte por ti mismo en el mundo del Bitcoin y dar tus primeros pasos en la compraventa de criptomonedas.

Una introducción a los riesgos y el manejo de la seguridad del Bitcoin.

En definitiva, este libro tiene como objetivo guiarte en tus primeros pasos para que comiences a inmiscuirte en el mundo del Bitcoin.

No sé si tienes experiencia previa en economía, ni en informática, ni en ingeniería, realmente da igual.

Lo que sí espero es que, durante tu aprendizaje, te remitas a otras fuentes de información que te ayuden a comprender aquellos temas que te generen curiosidad sobre otros tópicos relacionados al Bitcoin.

Para ello, al final del libro te proporcionaré una lista de referencias útiles para que estés familiarizado con algunos términos informáticos.

En definitiva, mi principal objetivo es que lleves a la práctica todos los conocimientos adquiridos, a medida que vayas leyendo cada capítulo del libro.

No te entretengo más, vamos a ponernos manos a la obra...

INTRODUCCIÓN

Si analizas los últimos 50 años, verás que hemos pasado de ser una sociedad tecnológicamente mecánica a una sociedad tecnológicamente digital, parte de la cuarta revolución industrial.

El auge de una vida cibernética ha afectado profundamente todo tipo de relación que tenemos y esto se manifiesta cuando analizas las siguientes preguntas:

¿A cuántos de tus amigos en

Facebook conoces realmente?

¿A cuántos de ellos has visto en persona los últimos 5 años?

¿Con cuántas personas pasas más tiempo conversando que chateando?

¿Cuándo fue la última vez que felicistaste a alguien en una fecha especial sin que te lo recordara una red social?

Ciertamente, la tecnología crece a grandes pasos día tras día y es imposible mantenerse ajeno a cambio.

A pesar de esto, la vida se ha vuelto simple.

Hemos pasado de reunirnos con personas a conversar, a hacerles llamadas telefónicas o enviarles mensajes de Whatsapp.

De portar grandes cantidades de dinero en efectivo, a pagar con transferencias electrónicas o tarjetas de débito y crédito; incluso puedes realizar inversiones en la bolsa desde tu teléfono móvil.

Hasta la comunicación ha evolucionado de manera que en vez de cartas nos llegan correos electrónicos o leemos el periódico en tabletas electrónicas o en nuestro móvil.

Sin duda, la tecnología se ha apoderado del mundo y no lo soltará.

Entonces, si la manera en la que vivimos nuestro día a día ha cambiado a causa de la tecnología, me pregunto:

¿Qué hace falta para que el cambio tecnológico llegue al mundo como la economía?

¿Qué hace falta para poder enviar y recibir dinero internacionalmente, de la misma forma que enviamos un correo electrónico?

La moneda y la economía han sufrido diversos cambios durante

años para llegar a ser como hoy la conocemos.

En los albores de la humanidad llegamos a negociar con trueques hoy en día lo hacemos con monedas de diferentes valores, en poco tiempo lo haremos de manera totalmente virtual, sin la necesidad de dinero físico.

Todo evoluciona y hoy en día estamos en la transición de una nueva forma de enviar y recibir dinero, de pagar y comprar productos y servicios y de cómo almacenar todo ese valor.

Si bien muchos países manejan el

formato electrónico y físico para operaciones comerciales, la moneda de la que te voy a hablar, es completamente diferente.

Al igual que cualquier tipo de moneda, esta posee reconocimiento, es difícil de falsificar, sencilla de manejar, divisible y portable, cuenta con diferentes tipos de monederos, más otras características que la hacen muy confiable y segura en cualquier aspecto.

Y puede que estés pensando, "pero Fernando ¿realmente es confiable una moneda de manejo exclusivo en el campo electrónico para

realizar operaciones comerciales de todo tipo?”

La respuesta es **Sí**.

La tecnología ya ha tocado puntos fundamentales de nuestras vidas que quizá consideraste imposibles hasta hace bien poco; como el comercio, la política y ahora la economía.

Esto es posible debido a que la forma anteriormente considerada abstracta, ha resultado ser segura, moderna y confiable.

La moneda digital no es nueva, lleva operando al menos 2 décadas, aun cuando es considerada cara,

difícil de utilizar y dependiente de instituciones bancarias.

Gracias a tantos y tantos avances en el ramo tecnológico para las operaciones monetarias, es normal pensar que la creación de un "nuevo dinero" que se envía al igual que un correo electrónico es totalmente posible.

Para el año 2009, un "nuevo dinero" fue creado con muy buenos resultados, tomando forma en una economía que cada año se globaliza más. Esta nueva moneda permite operaciones transparentes, seguras y de costos muy bajos en comparación a otras monedas.

Te hablo del **Bitcoin**, un sistema económico independiente a cualquier ente gubernamental o institucional, que se rige por las inalterables y constantes leyes matemáticas.

Dicho sistema tiene como soporte la tecnología **blockchain**, la cual se asemeja a un libro contable abierto al público, con el cual se puede ver el historial de operaciones.

¿Acaso esto no será contraproducente?

No, pues gracias a este sistema se reduce al mínimo la posibilidad de

estafas, fraudes y robos, el blockchain enlaza la última transacción con todas las anteriores, de esta manera es prácticamente imposible alterar una sola operación sin alterar todo el historial del Bitcoin desde sus comienzos.

Parece increíble, pero el Bitcoin es completamente digital, descentralizado y está disponible para todo el público, lo que lo vuelve universal; de uso voluntario, sin intermediarios ni inflación, con transacciones prácticamente inmediatas y seguras.

Gracias a estas características,

miles de empresas alrededor del mundo han comenzado a adoptar el Bitcoin como método de pago. (www.aceptamosbitcoin.com)

Una nueva etapa en el comercio y en la economía está por empezar y más vale que estés preparado para estar en ella.

El Bitcoin dejó de ser un juego de nerds para convertirse en un sistema sólido, confiable y de gran alcance, con un gran avance respecto a su antecesor plástico: la descentralización.

Uno de los grandes pilares para esta tecnología es la comunidad de

desarrolladores que suma el esfuerzo de millones de personas que le dan credibilidad al sistema, esto se logra sin tener vínculos gubernamentales o algún banco en el mundo.

Por su parte, el Bitcoin tiene costos de mantenimiento mínimos gracias a que toda su infraestructura se basa en el poder computacional que los mineros aportan a la red.

Cuando comencé a escuchar acerca del **Bitcoin** vi una oportunidad potencial para poder generar ingresos extra, explorar nuevas formas de pago confiables e instantáneas y el siguiente paso en

la evolución de la economía.

Aun cuando hoy el Bitcoin continúa con grandes variaciones en su precio, vale la pena estar preparados para sacarle provecho a esta tecnología que cobra importancia día tras día.

Mi padre solía decir: "La información es poder" y esto me permitió entender que vale la pena invertir mi tiempo y dinero en conocer y aprender todas las tecnologías posibles, pues estas pueden aportar un beneficio significativo a nuestras vidas y a nuestra economía.

Considero que el Bitcoin es parte de ese grupo de tecnologías que merece recibir, tanto mi atención como mi tiempo para comprenderla mejor, pues dentro de los próximos años su valor seguirá aumentando.

Por mi parte, no fue hasta hace 2 años que invertí en el Bitcoin y desde ese momento sigo en la constante búsqueda de nuevas tecnologías, divirtiéndome en el proceso.

El Bitcoin ha cambiado por completo los conceptos, esquemas y paradigmas que conocíamos de la economía, pues ahora tenemos frente a nosotros una clase de

dinero descentralizada y de uso global.

Pero realmente, ¿qué es lo que motiva a aprender acerca de los Bitcoins?

Pues, obviamente, Invertir en el futuro.

Pero eso lo aprenderás en los siguientes libros de la serie.

Por ahora, quiero que comprendas los conceptos básicos para poder iniciar sobre una base sólida de conocimientos. Por lo tanto, en este libro me centraré en ayudarte a entender qué es el Bitcoin, cómo se desarrolla, sus ventajas, riesgos y

los primeros pasos para obtener tu primer monedero virtual.

Entremos en materia...

CAPÍTULO I.

SENTANDO LAS BASES

Comenzaré hablándote de algunos conceptos que son indispensables para poder familiarizarte con este nuevo abanico de oportunidades que se abrirán ante ti y que necesitas tener presentes para entender el Bitcoin.

En primer lugar, imagina que el mundo trabaja con un número de cartas limitadas; te hablo de cartas

comunes y corrientes, de esas que recibes en tu buzón.

Al enviar una carta, esta pasa a ser propiedad del destinatario que eliges, y al haber un número limitado de cartas en el mundo, estas tienen un valor determinado que puede aumentar cada día.

De esta forma trabajan las Bitcoins, pero a diferencia de las cartas, que pueden ser duplicadas, estas no pueden ser creadas por nadie más y es ahí donde reside su valor.

Pero no basta con que algo sea único y especial para ser valioso, ese algo también debe ser útil.

Veamos un ejemplo:

El aire es un elemento de gran utilidad, pues es indispensable para la vida. Pero, este es abundante y algo totalmente imposible de controlar o acaparar, razones por las que no es posible asignarle un valor.

Un segundo ejemplo puede ser la escasa cantidad de cabellos que tenga un hombre, pueden ser muy pocos, pero no por ello se les puede asignar un valor económico.

El Bitcoin contiene ambas características y muchas más, que lo hacen poseedor de valor

intrínseco, que le ha llevado a ser un cambio en el sistema monetario actual.

El Bitcoin convierte al sistema monetario en algo más práctico, estable y seguro, ya que te permite evitar los elevados costos de aranceles internacionales, al mismo tiempo que te da la libertad de revisar las transacciones en cuestión de segundos, teniendo la seguridad de que tus datos están protegidos.

Esta revolución económica creada por Satoshi Nakamoto (creador de los Bitcoins) ha tenido un impacto en la economía global, del mismo

modo que los correos electrónicos llegaron a cambiar las comunicaciones.

De hecho, me atrevo a decir que el dinero ha sido reinventado.

Sea cual sea el caso, el Bitcoin es una unidad de valor que tomará auge de forma gradual, de acuerdo a la aceptación de sus usuarios y empresas, gracias a que no fue creada ni depende de un ente gubernamental o bancario.

En la economía que conocemos, el acto de depositar nuestro dinero en un banco genera a este una responsabilidad que se puede

llamar "Deuda".

Esta deuda se crea al dejar nuestros bienes en manos de un tercero con el fin de garantizar su seguridad, pero siempre y cuando este tenga la capacidad de devolver en cualquier momento la totalidad de lo depositado.

El Bitcoin no sigue este modelo.

La moneda digital está completamente libre de este compromiso o deuda; ya que no dejas al cuidado de un tercero tu dinero, sino que eres tú quien tienes el control total de tu posesión.

Además, el acto de pago también cambia con el uso del Bitcoin o cualquier criptomoneda.

Lo normal en la economía de hoy es que cualquier individuo realice gastos que no registra o no se preocupa por controlar, por lo que a veces el presupuesto desaparece más rápido de lo que se planea.

En cambio toda operación con Bitcoin queda registrada en ese gran libro contable abierto que ya te mencioné anteriormente, dejando prueba fidedigna del envío y recepción de la moneda con el registro de ambos usuarios.

Esto permite un control total del pago y al mismo tiempo, fusiona estos procesos en uno solo, facilitando el comerciar con Bitcoin.

¿Qué es una criptomoneda o criptodivisa?

Oxford lo define como...

“Una moneda digital que emplea técnicas de cifrado para reglamentar la generación de unidades de moneda y verificar la transferencia de fondos, y que opera de forma independiente de

un banco central”

Y Cambridge como...

“Una moneda digital producida por una red pública, en lugar de cualquier gobierno, que utiliza la criptografía para asegurar que los pagos se envían y reciben de forma segura.”

En palabras simples:

Una criptomoneda es una **moneda virtual** que sirve **para intercambiar bienes y servicios** a través de un sistema de transacciones electrónicas, **sin la necesidad de un intermediario y de forma segura y confiable.**

¿Qué es un Bitcoin?

Es una criptomoneda creada en 2009 por un grupo de personas bajo el pseudónimo Satoshi Nakamoto.

Es una "moneda digital" descentralizada, es decir, no hay ninguna entidad financiera o gobierno que controle la oferta de dinero, por lo tanto, el Bitcoin es una idea de dinero intangible que no pierde valor.

En pocas palabras, es un medio digital de intercambio.

Así como hoy en día se paga con

billetes y monedas, en el futuro pagaremos con "criptomonedas".

En 2017, el Bitcoin ya era utilizado en miles de comercios alrededor del mundo, debido al incremento en la aceptación de los usuarios y de las empresas como método de pago.

¿Cómo se generan los Bitcoins?

A pesar de tener un concepto sencillo, el proceso para generar Bitcoins es complejo al momento de aplicarlo.

La adquisición de Bitcoin requiere

realizar un proceso de "minería".

Dicho proceso requiere resolver algoritmos informáticos complejos por los que la "red premia" con un fragmento de Bitcoin a todos aquellos que aportaron "valor informático" para resolver dicho problema.

Es decir, todos aquellos que se dedican a ayudar a que la transacción sea realizada, reciben una comisión por ello.

Este algoritmo está diseñado para generar un Bitcoin cada 10 minutos, sin embargo, la existencia se limita a únicamente a la cantidad de

21.000.000 Bitcoins.

¿Por qué?

Para lograr que esta cantidad limitada, evite la caída del valor del Bitcoin en el mercado y al mismo tiempo se reduzca el riesgo de inflación al punto de evitarlo por completo.

En (www.blockchain.info) podrás encontrar detalles sobre el valor en tiempo real del Bitcoin, la cantidad de transacciones que se llevan a cabo en el día, recibirás más información sobre el Bitcoin, podrás adquirirlo y además, podrás tener acceso gratuito a un monedero

virtual.

El número total de Bitcoin que ya te mencioné, tenderá a permanecer dentro de ese rango con la expectativa de que para 2018, se generarán $\frac{3}{4}$ partes de la producción total de Bitcoin en la historia.

Al acercarse a este límite, la economía Bitcoin comenzará una etapa en donde el poder adquisitivo de cada unidad aumentará hasta alcanzar estabilidad.

¿Solo existe el Bitcoin?

No.

Existen muchos tipos de criptomonedas o criptodivisas.

Por ejemplo: Litecoin, Ripple, Dogecoin, Ethereum, Bytecoin, Zcash, entre otras y cada una de ellas cuenta con protocolos y características diferentes.

Entre estas, el Bitcoin ha sido la criptomoneda que ha demostrado más estabilidad desde su creación; sin embargo, esta cualidad se comienza a notar ya entre las demás criptomonedas.

¿Quién determina su precio?

Así como con todo producto que depende de oferta y demanda, el precio del Bitcoin lo determina todo aquel que quiera participar en su proceso de compra y venta, es decir, sus usuarios.

Sin embargo, a pesar de que esto suele ser el determinante más importante sobre el precio del Bitcoin, otros factores pueden influir en su valor.

Dado que el comercio de Bitcoins a través de plataformas de

intercambio (conocidas como exchanges) permite la distribución de Bitcoins y otras criptomonedas, las leyes de la economía influyen sobre el Bitcoin.

Es decir, cuando hay una gran cantidad de compras, su precio aumenta; mientras que una gran cantidad de ventas el precio disminuye.

Por esta razón, los productores (en el caso de Bitcoin, los mineros) pueden proponer un precio al vender sus Bitcoins a los interesados, llegando a acuerdos como en cualquier acto de comercio.

De esta forma se establecen tratados o contratos en los cuales se propone un precio, se negocia y una vez aceptado, se procede a completar la transacción.

Así se determina el precio del Bitcoin: bajo el viejo método de la oferta y la demanda.

La gran batalla: Moneda real vs Criptomoneda

El Bitcoin representa una nueva clase de economía pues, a diferencia del dinero común, este no sigue las reglas tradicionales

que se le aplican a la moneda física (conocida como Fiat).

Te mostraré algunas características que te permitirán ver el Bitcoin como una moneda real y al mismo tiempo, percibirás sus fortalezas en contraste con la moneda común:

El Bitcoin se basa en las ventajas que nos da la tecnología de hoy en día: por lo que cada propietario puede acceder en todo momento a sus fondos sin la necesidad de un tercero.

Escasez: su cantidad es finita y

predecible. Imposible de variar, pero de un valor creciente.

Fácil de transportar: Es posible transportarlos en cualquier dispositivo electrónico (Smartphone, Laptop, tablet, memoria USB) y cada cartera o monedero de Bitcoin es capaz de almacenar todos los Bitcoin deseados en un espacio mínimo.

Fungibilidad: como toda moneda, tiene usos prácticos y su aceptación está en aumento, por lo cual, puede ser utilizado para la adquisición de bienes, como método de ahorro o como método de inversión.

Fácil reconocimiento y seguridad accesible: El Bitcoin es fácil de identificar, de ocultar y difícil de falsificar, debido a que los monederos de Bitcoin son únicos e imposibles de clonar. Cada uno está compuesto por una llave privada (que sirve para firmar las transacciones) y una llave pública (que te identifica ante otros usuarios sin revelar la identidad de quien posee dicha llave).

Divisibilidad: se puede dividir en unidades pequeñas y estas pueden combinarse para formar grandes unidades. EL Bitcoin es

divisible hasta en 8 decimales.

Privacidad: Cada monedero Bitcoin es tan anónimo como el usuario decida.

Aceptación universal: Un aspecto en el que mejora día a día.

Como puedes ver, todas estas características vuelven al Bitcoin una moneda transparente, de bajo costo, descentralizada y totalmente segura.

CAPÍTULO II.

¿POR QUÉ CONFIAR EN EL BITCOIN?

Aunque ya te he mencionado con anterioridad qué características te permiten confiar en el Bitcoin, te las resumo en dos:

Código abierto y descentralización: cualquier persona en el mundo puede

verificar como funciona.

Seguridad: todos los pagos se realizan sin terceros y la legitimidad de las monedas está basada en la red, no en un gobierno o banco central.

Desde su creación, el Bitcoin ha tenido variaciones de costo y demanda por diversas razones, pero como resultado, se ha dado lugar a etapas estables de incremento de valor y ajuste de precios de forma equilibrada, lo cual no sucede con las monedas comunes (o Fiat), que tienden a

pasar por procesos de inflación constantes.

Ya que el valor del Bitcoin varía según su demanda, el mismo depende de la aceptación en su uso para su incremento de valor.

¿Vale la pena tener Bitcoin?

Sinceramente te digo que **Sí y No.**

Sí, porque cada fracción aumentará su valor en un mediano a largo plazo.

No, si lo que quieres es tener un

capital solvente.

Una de las más grandes necesidades del Bitcoin es la aceptación por parte del comercio actual, en medida que las empresas la comiencen a ocupar para la adquisición de bienes y servicios el Bitcoin se fortalecerá como medio de intercambio global.

Cada día son más las empresas que permiten el Bitcoin como forma de pago, conscientes de que su valor incrementa y se consolida a medida de que sigue adquiriendo importancia, lo cual convertirá cada unidad en parte de la economía del futuro.



¿Por qué debes invertir en Bitcoin?

Porque gracias a las grandes ventajas que tiene, su importancia se incrementa de forma gradual elevando su valor a la vez.

La web es un aspecto que está presente en muchas facetas del día a día y en vista de que el Bitcoin trabaja en este entorno y cobra importancia en el mismo, vale la pena promover su uso y aprovechar los beneficios de su crecimiento.

Por ser la criptomoneda pionera,

posee mayores ventajas que otras monedas de este tipo y debido a que sus usuarios obtienen grandes beneficios al trabajar con Bitcoin, existe una retro-alimentación entre los mismos para solucionar problemas que surjan al trabajar con la moneda.

Recuerda: No inviertas más dinero del que puedas darte el lujo de perder. El Bitcoin es sin duda pieza clave de la economía del futuro, pero su precio aun es volátil e inestable. Por lo cual deberás tener cuidado de no invertir más de lo debido.

Formas de invertir en Bitcoin

Para comenzar, debes conocer las 5 formas básicas de invertir en Bitcoin:

Minería de Bitcoins

Esta primera opción es un proceso que se realiza por medio de una o más computadoras que resuelven algoritmos complejos y determinan los momentos apropiados para realizar transacciones con Bitcoin.

Gracias a esto, los mineros

obtienen comisiones de pequeñas fracciones de Bitcoin.



Intercambio de Divisas por Bitcoin

Es el proceso de compra de la moneda en forma de unidades o fracciones de unidad a cambio de las divisas del país del comprador u otra criptomoneda.

En esta forma de inversión vale la pena mencionar las ICO's (Initial Coin Offering) que son aquellas plataformas que ofrecen nuevas criptomonedas en pre-venta.

Esta práctica ha tomado mucho auge últimamente y se ha prestado a grandes fraudes, por lo cual muchos gobiernos han decidido

imponer reglamentaciones estrictas para este tipo de ofertas.

Si tienes pensado invertir en alguna ICO verifica cuáles son sus usos a futuro, quién la sustenta y quién la desarrolla antes de invertir tu dinero.

Broker

Este proceso permite hacer inversiones por medio de un broker (agente de bolsa).

Es decir, de la misma forma que se compran y se intercambian acciones en la bolsa de valores, el Bitcoin se

puede trabajar con algún agente online, de manera que abres una cuenta hasta con \$10 y comienzas a invertir en la criptomoneda que tu desees.

Cajeros de Bitcoins

A pesar de no ser una opción disponible en todo el mundo, en algunas ciudades de Europa, Estados Unidos y México existen cajeros a través de los cuales es posible comprar Bitcoin.
(www.coinatmradar.com)

Se espera que en un futuro, estos permitan venderlos para obtener

dinero Fiat.

Aceptación como Método de Pago

Esta es la verdadera razón de ser del Bitcoin.

Al aceptar pagos en Bitcoin, las personas pueden demostrar que es viable el uso de las criptomonedas y colaborarán con su aceptación.

En el tercer libro de esta serie te mostraré con más detalle estos ejemplos y la aplicación de los mismos, pero vale la pena que te los mencione ahora, para que tengas en cuenta esta información.

CAPÍTULO III.

CÓMO CAMBIARÁ EL BITCOIN AL MUNDO

El Bitcoin influirá de tal forma en la vida de las personas, que se espera que pueda realizar los siguientes cambios en el mundo:

Permitirá la realización de transferencias bancarias de forma rápida, segura y económica

La forma en la que los bancos manejan el dinero hoy día llega a resultar lenta e incómoda sobre todo por los grandes aranceles internacionales y la compatibilidad entre bancos de todo el mundo.

Las transferencias a nivel internacional pueden tardar entre 1 semana y 15 días en hacerse efectivas y los impuestos que se aplican a estas, restan parte de esos fondos al propietario del dinero y en algunos casos, el intercambio de datos de pago entre un país y otro llega a presentar dificultades en su proceso.

Sin embargo, esto no aplica a las

criptomonedas.

Sin importar la ubicación entre quienes realicen transacciones con ellas, las transferencias se llevan a cabo al instante con un mínimo de comisión y con la garantía de que se ejecutarán.

La aplicación de este sistema a la economía común, brindará a cualquier operación bancaria estas mismas ventajas.

Impulso a las remesas mundiales

Anualmente, quienes emigran a otros países en búsqueda de

mejores oportunidades, envían a sus hogares un promedio de 500 mil millones de dólares en remesas.

A estas remesas se les aplican tasas de porcentajes entre el 6% y el 10% a cada \$200 USD, una carga realmente alta para estas personas.

Pero como ya te he dicho, la tecnología de las criptomonedas puede eliminar estas cargas e incluso, permitir que el envío se haga directo a sus familiares sin la necesidad de la intervención de un tercero.

Además, se evita la espera de reposición de dinero a la cual

suelen verse expuestos quienes utilizan compañías tradicionales de transferencia de dinero; de esta forma también se reducen los requerimientos de capital para las empresas que trabajen con monedas digitales.

Con la reducción de estos gastos, será posible que nuevos corredores de remesas o personas con el deseo de invertir en este mercado puedan hacerlo; lo cual permitirá que zonas menos pobladas o aisladas puedan obtener acceso a este beneficio.

Oportunidad de asegurar ahorros confiables para comunidades vulnerables

La tecnología tuvo una explosión de aceptación en África tan grande, que permitió demostrar que los países en desarrollo pueden liderar cuando se trata del uso de tecnología sofisticada.

Solo en Kenia, se estima que más del 60% del comercio se lleva a cabo por medio de créditos de telefonía móvil como medio de intercambio.

De esta forma, cualquier persona con un dispositivo móvil puede, no

solo almacenar en él cantidades destinadas al comercio para realizar pagos, sino también recibirlos.

Pero al igual que las operaciones de transferencias de fondos a nivel internacional, estas presentan un problema, las comisiones que se aplican sobre las transacciones, que representan un 20% del total de los créditos otorgados y utilizados.

El uso del Bitcoin plantearía una nueva forma de manejar el mercado sin este problema y además, sin el riesgo de pérdida en países de alto nivel de inflación, ya que el almacenamiento de Bitcoin ofrece más seguridad que la forma

convencional de guardar dinero y posee valores estables a nivel internacional.

De esta forma, se ampliaría el acceso a los mercados financieros mundiales y al mismo tiempo, podría llegar a eliminarse la amenaza de la inflación.

Otra ventaja en este aspecto, es que le brindaría a las personas sin acceso a servicios bancarios una forma de establecer un capital con garantía internacional.

Explotar el potencial del E-commerce

Los fraudes con las tarjetas de crédito (TDC) se incrementan cada día, lo que mueve a los negocios a dejar atrás el uso de TDC como formas de pago.

Los fraudes se presentan principalmente en las transacciones internacionales, por lo que muchas empresas cierran las puertas a este tipo de pagos o imponen altas tasas de comisión.

En el caso de que una empresa decida implementar el Bitcoin como opción de pago en su plataforma, ya está garantizando la ejecución de la transacción, ya que una vez enviado un pago en Bitcoin no hay

forma de deshacerla, lo que influye directamente en la disminución de las estafas a comerciantes que desean ofrecer servicios internacionales.

Por otro lado, el comerciante tiene la facilidad de enviar fondos de la misma forma en la que utiliza el correo electrónico, lo que incrementa las compras online y las hace más sencillas de completar.

En el caso de que una PYME o empresa pequeña que provenga de un país en desarrollo desee invertir en el comercio mundial, podrá completar transacciones sin ningún problema y generar un capital

estable y en constante crecimiento.

De hecho, esto se refleja en la forma en la que algunos comerciantes latinoamericanos con productos artesanales completan ventas a nivel mundial.

Otro ejemplo de cómo se puede explotar el E-commerce es dando clases por Internet y recibir pagos en criptomoneda, algunos jóvenes chinos ofrecen clases de Mandarín vía Skype, por lo que las empresas utilizarían plataformas de publicidad online para promover sus productos y servicios incrementando su público y concretando ventas pagando con Bitcoin u otra

criptomoneda.

Además, al realizar movimientos por pequeñas cantidades de Bitcoin, estas generan tasas de transacción muy bajas lo que simplifica compras de valores más bajos.

La implementación de contratos inteligentes y dinero programable

Esto será posible gracias a la automatización de los movimientos una vez que el dinero sea netamente digital; lo que permitirá crear cuentas de garantías bloqueadas como las que se emplean en operaciones

inmobiliarias de gran envergadura.

Estas cuentas permiten que el comprador de una propiedad realice un depósito de forma condicional y el dinero no se libera hasta que el vendedor no entregue el título de dicha propiedad, lo que garantiza a ambas partes que el negocio se concrete de forma correcta.

Otro caso de la implementación de esta tecnología es la MultiSign o Multifirma, que es un tipo de cuenta en la que el dinero solo será liberado si varios individuos autorizan la transacción; lo que reducirá en gran manera el robo de fondos digitales y también les

permitirá a las grandes empresas garantizar que su dinero no se pierda cuando se realicen movimientos con contratistas u organizaciones no gubernamentales radicadas en países en desarrollo.

La confianza lo es todo a la hora de hacer negocios, por lo que muchos se resisten a comercializar con personas que no conocen o que no se encuentran en su país así que, si se implementa este tipo de sistema en todas las plataformas digitales, sea cual sea su origen, el comercio fluirá mucho mejor gracias a todas estas garantías de pago.

Por otro lado, el dinero

programable tiene una gran participación en los contratos de gran trascendencia debido a la participación de varias personas en un acuerdo complejo.

Por ejemplo, imagina que se deposita una cantidad de dinero en un contrato financiero que solo dará beneficios de acuerdo a lo que suceda con el valor de ciertas acciones.

En este sistema se implementará un programa informático donde se pueden vincular la cotización bursátil de Bloomberg, por poner un ejemplo, y una vez que el sistema analice dichas acciones o la

combinación de ellas, se realizará un depósito automático en las cuentas de los beneficiarios del contrato.

CAPÍTULO IV.

RIESGOS DEL BITCOIN

A continuación entraré en detalles sobre cuáles pueden ser los problemas que se te presenten al trabajar con Bitcoin.

Lejos de ser información ficticia o una falsa alarma, debes tomar en cuenta estos puntos como verdaderos riesgos a tener en consideración:

Falta de Respaldo con Reservas

A diferencia de la moneda común, las criptomonedas o monedas virtuales como el Bitcoin no tienen un respaldo en activos físicos que un banco o alguna autoridad pueda soportar con reservas.

El valor de intercambio de estas depende del uso y aceptación de la misma, si llegara el punto en el que todos los usuarios de la red dejaran de usar el Bitcoin repentinamente el valor podría reducirse drásticamente e incluso llegara a cero ya que el único soporte de Bitcoin es su uso y aceptación.

La cantidad de Bitcoin está limitada a un número máximo establecido y su divisibilidad de 8 dígitos permite que muy pequeñas fracciones puedan ser utilizadas para comercio evitando así la inflación y devaluación del Bitcoin.

Esto podría provocar que si el precio se vuelve demasiado elevado, se genere el abandono de los usuarios con menos capital.

Sin embargo, esto no significaría el fin del Bitcoin ya que el simple hecho de que una sola persona ejecute el protocolo en su computadora, permitiría al Bitcoin mantenerse con vida.

Aunque por otra parte, esto implicaría reiniciar el proceso de adquirir credibilidad de forma completa.

Falta de Regulación

Al no ser dependiente de ninguna institución que le brinde respaldo, tampoco depende de estas para ser regulado (esto es para el Bitcoin y también para otras criptomonedas).

Esta ausencia de regulación aplica incluso para las comercializadoras de criptomonedas o plataformas de intercambio, ya que en la mayoría de los estados del mundo en que

estas son reconocidas, se permite que su uso avance y sean aceptadas dentro de los planes económicos nacionales.

Un claro ejemplo de esto es la instalación de cajeros de intercambio de divisas por criptomonedas.

He aquí la importancia de avanzar en su uso y aceptación por parte de gobiernos.

Desprotección ante un Mal Uso

MT.Gox, una de las plataformas más conocidas de gestión de

moneda virtual, es un ejemplo de otro factor de riesgo que presenta el uso de Bitcoin.

Esta plataforma cerró algunos años atrás, generando grandes pérdidas a los usuarios, debido a que algunos de ellos se valían de este medio para financiar actividades ilegales.

Si bien, ni la plataforma ni el resto de los usuarios inocentes eran responsables de este mal uso, fueron afectados de igual forma.

Esto sirvió como precedente para tomar medidas y evitar problemas similares, pero puede llegar a

ocurrir de nuevo.

Culpar al Bitcoin por financiar actividades ilegales es lo mismo que culpar al dólar por hacer lo mismo.

Falta de Ubicación Fija

Ya que los domicilios de las plataformas de intercambio están esparcidos por todo el mundo, no solo su regulación sino también su vigilancia escapan a todo ámbito de la ley, por lo cual, el factor confiabilidad sigue siendo su fortaleza pero a la vez su talón de Aquiles.

Procedencia Desconocida de los Usuarios

La probabilidad de que se utilice la criptomoneda para llevar a cabo actividades fraudulentas o ilícitas sigue latente.

Al no requerirse una explicación de la procedencia de los fondos con que se adquieren las fracciones o unidades de Bitcoin, pueden provenir de sectores dedicados a actividades criminales sin que dichas operaciones pueda delatar estos actos, como lo haría la gestión de estas a través de

cualquier divisa común.

Falta de Garantía Privada o Estatal

Ningún tipo de inversión con criptomonedas puede ser amparado con algún tipo de seguro.

El hecho de que ninguna garantía privada o estatal le sea conferida al Bitcoin o a cualquier otra moneda electrónica, impide estas coberturas, por lo tanto, queda bajo el criterio del usuario el asegurar las transacciones.

Falta de Obligación de

Cumplimiento

En algunos casos, existe la probabilidad de estafa, puesto que no hay mecanismos que obliguen el cumplimiento de las transacciones con monedas virtuales.

Esto implica un cierto riesgo de incumplimiento por parte de algunas de las partes involucradas en el proceso, sin que se tomen medidas a favor o en contra de ambas partes.

CAPÍTULO V.

SEGURIDAD DEL BITCOIN

La seguridad en las transacciones en Bitcoin es alta debido a los pasos que se deben cumplir para llevarlas a cabo.

Definamos estos pasos como las transferencias y la creación de bloques.

Tal como indica su nombre, una

transferencia es una operación de entrada o salida que requiere el ID de cada uno de los participantes de la operación, la cual se efectúa por cualquier razón.

Lo importante en este paso es el ID.

¿Por qué?

Porque una vez que se realiza una operación, con cada ID se procede a la creación de bloques de información. Estos bloques de información no solo registran el destinatario y la procedencia de la moneda, sino también el historial de movimientos de las mismas.

Dichos bloques contienen sellos de tiempo, números de verificación y los datos proporcionados por el bloque anterior, con lo cual, se genera una base de datos temporal que valida cada operación solo después de confirmar que el dinero a enviar no ha sido gastado antes de la transferencia.

Si una transferencia se realiza tratando de evitar el proceso de cadena de bloques, no se dará por válida y por lo tanto, no se llevará a cabo y si por el contrario la transferencia procede, queda registrada inmediatamente en la cadena actualizando la información

de la misma.

Te muestro un ejemplo de cómo sería el proceso con dos individuos que denominaré A y B:

Por una razón determinada, el usuario "A" decide renunciar a la pertenencia de cierta cantidad de Bitcoin cediéndola al usuario "B".

Para poder realizar esta transacción, ambos usuarios utilizan sus llaves privadas o identificación, que sirve como firma o aprobación del proceso.

Al efectuarse esta operación, la información se transmite a la red de P2P (Red que brinda Soporte al

Protocolo) a través de la cual se procede a autenticar las firmas y verificar la disponibilidad de unidades de Bitcoin.

Una vez que comprobados los datos, se procede a validar la transacción.

Dicha operación es registrada de forma que no se utilicen los fondos transferidos nuevamente para una operación completamente distinta.

Así que, al igual que cuando gastas el dinero en efectivo ya no puedes disponer de él, aquí también te sería imposible.

¿Qué pasaría en caso de un holocausto mundial, caída mundial del Internet o algo similar?

Ya que el Bitcoin depende de Internet, podría presentar una pausa indefinida en caso de que ocurra una de estas circunstancias.

Esto se debe a que su dependencia es absoluta. El Bitcoin vive, crece y se mueve en Internet.

Una de estas circunstancias podría generar la suspensión de las telecomunicaciones de forma temporal o indefinida.

Sin embargo, ya que bastaría una

sola computadora corriendo el protocolo, no podemos descartar la posibilidad de que vuelva a la vida esta criptomoneda.

Simplemente se debe continuar el proceso de validación de información, recuperación de datos y las transacciones comunes requeridas para que el protocolo, otorgue, transfiera y/o valide Bitcoin.

¿Qué sucedería si alguien comprara todos los Bitcoin y generara un monopolio de esta nueva moneda?

Puedo asegurarte que esta persona no lograría nada en caso de poder realizar dicha compra.

Además, es improbable que un solo individuo adquiriera los 21 millones de unidades, pues su precio no lo permite.

La sola compra de unos pocos miles requeriría millones de dólares, por lo tanto, el acaparamiento de todas las unidades no es algo viable.

En caso de que un individuo se propusiera hacerlo, se encontraría con algunos problemas.

Primero, en vista de que poseería la mayoría de las unidades y él

decidiría su precio, las personas podrían optar por no adquirirlas y recurrir a otro tipo de criptomoneda, lo cual desplomaría su precio generando pérdidas en lugar de ganancias y la probable muerte del Bitcoin.

Y por otro lado, esta persona tendría que luchar contra la decisión de no vender por parte de algunos de los dueños del Bitcoin. Estos podrían simplemente guardarlos e impedir de esta forma el acaparamiento.

¿Las direcciones de cobro y de

pago están vinculadas de alguna manera con la persona que los utiliza?

Sí y no.

Las cuentas o billeteras de Bitcoin están a nombre de alguien, sin embargo, no se pueden utilizar para descubrir la información de su dueño, por lo tanto, no son vinculantes.

Únicamente podrían llegar a hacerlo si el nivel de anonimato de su usuario es suficientemente bajo como para que él desee brindar su información y no precisamente por medio de la cartera.

Esto se debe a que estas carteras por sí solas no servirían para este propósito, pues se identifican con una serie aleatoria de 33 letras y números sin información de su dueño.

CAPÍTULO VI.

MONEDEROS VIRTUALES



Así como cada producto tiene una

característica que lo identifica y lo hace resaltar entre sus similares, los monederos Bitcoin cuentan con funcionalidades que los vuelven singulares.

Debes tener muy en cuenta, que no existe un monedero Bitcoin que tenga todas las características que el mundo desea.

Sin embargo, hay muchos que se ajustan a las necesidades de cada usuario.

Quiero enseñarte qué son los monederos virtuales y cuál sería el más adecuado para cada usuario según su necesidad y objetivos:

¿Qué es un monedero Bitcoin?

Es la herramienta más indispensable para trabajar con criptomonedas.

Puedo definirlo como la interfaz personal en la red Bitcoin, que funciona como la cuenta bancaria en línea de cada usuario, así como su punto de partida para adentrarse en el mundo de las criptomonedas.

Es gracias a esta interfaz que podemos recibir, almacenar y/o gastar Bitcoin.

Esto se debe a que en los monederos se almacenan las claves privadas o códigos secretos, que permiten gastar o recibir Bitcoin y sin los cuales, estos procesos serían imposibles.

Pero ¿se almacenan en estos las criptomonedas?

No, los Bitcoins no necesitan ser almacenados o asegurados, pero sí que requieren pasar los protocolos de seguridad que te mencioné para que sea posible llevar a cabo transacciones con ellos y estos protocolos necesitan las claves privadas que almacenan las carteras o monederos de Bitcoin.

En palabras simples, son simples aplicaciones, dispositivos o sitios web, que administran tus claves privadas de Bitcoin.

Tipos de monedero de Bitcoins.

Es momento de enseñarte cuáles son los tipos de monederos disponibles en el mercado y sus características, así que, vamos allá:

Monederos hardware

Como indica su nombre, son

dispositivos electrónicos físicos creados con el único y simple propósito de asegurar Bitcoins.

Este monedero Hardware debe estar conectado a otro dispositivo electrónico (computadoras, tablets o teléfonos inteligentes) justo antes de hacer cualquier transacción.

Entre los monederos Hardware más populares están:

Ledger Nano S.

KeepKey.

Trezor.

Estos son una buena elección, si la

seguridad y un almacenamiento confiable y conveniente son tu prioridad.

A pesar de que estos monederos parecen simples pendrives, no debes confundirlos, pues en lugar de descargar todas las claves privadas en los dispositivos, estos las utilizan para las operaciones al mismo tiempo que las mantienen separadas de los equipos, de forma que nunca sean vulnerables al conectarse a Internet.

Esto es posible debido a que mantienen dichos códigos privados en un entorno seguro fuera de línea, en el monedero hardware,

reteniéndolas y protegiéndolas en caso de ser conectados a un dispositivo infectado con un malware.

Este tipo de monederos brindan una enorme ventaja para protegerte en caso de diferentes tipos de robo.

¿Cómo es posible?

Gracias a que generan y almacenan las claves privadas fuera de línea, aseguran que cualquier intento de los hackers sea ineficiente, pues estos deben tratar de conseguir las claves privadas a las cuales nunca tendrán acceso gracias a este sistema.

“Pero ¿y si el robo es en la forma común? Si llego a extraviar mi monedero hardware o se daña, ¿lo perdería todo?”

No, en estos casos puedes contar con una opción que debes configurar de manera previa. Se trata de un código secreto de backup con el cual puedes recuperar tus Bitcoin.

“¿Y si el ladrón trata de hackear el dispositivo?”

No pasaría nada, ya que necesitaría también el código PIN que hayas asignado para la protección del dispositivo al cual difícilmente

tendrá acceso.

En resumen, los monederos hardware son una buena opción ya que:

Es sencillo utilizarlos para almacenar Bitcoins de forma segura.

Son una herramienta con la que **es muy fácil recuperar y asegurar tus Bitcoin.**

Tienen un margen mínimo de error y además, su instalación es sencilla incluso para usuarios con muy poco conocimiento técnico.

Y por nombrarte alguna desventaja, todos estos beneficios... ¡No son gratis!

Monederos dinámicos

Este tipo de monederos no necesitan ser conectados a ningún dispositivo, ya que a diferencia de los anteriores, existen en la red. Por esta razón, funcionan en cualquier equipo que tenga acceso a Internet.

Estos monederos no portan las claves privadas que son generadas, al contrario, las generan por sí

mismos en el dispositivo que estés utilizando.

Pero existe un pequeño problema, estas claves no pueden ser consideradas seguras al 100%.

Siendo este el caso, ¿por qué deberías utilizarlos?

Los monederos dinámicos presentan las siguientes ventajas:

Son la forma más fácil de almacenar pequeñas cantidades de Bitcoin.

Son muy convenientes para realizar y recibir pagos de

forma rápida y sencilla.

Algunos monederos dinámicos **permiten acceso a los fondos a través de múltiples dispositivos**, lo cual es un beneficio extra para quienes utilicen diferentes equipos en sus gestiones de criptomonedas.

Y como desventajas te diré que:

Debido a su sistema de trabajo y al hecho de que sus claves de seguridad no son plenamente confiables, **no es recomendable utilizarlos cuando se manejan grandes cantidades de**

Bitcoin.

¿Qué monedero es el mejor para ti?

La elección de un monedero dependerá de lo que quieras hacer con las criptomonedas, ya sea ahorrar o invertir.

Por un lado, los monederos hardware son muy útiles si lo que quieres es ahorrar, ya que mantendrán tus monedas a salvo donde quiera que te encuentres.

En el caso contrario, si necesitas realizar envíos y recibir de forma

continua lo mejor son los monederos software.

Sin embargo, sea cual sea tu decisión, tienes que sopesar los pros y los contras de cada tipo de monederos, pues el objetivo es que soluciones problemas y no generarlos por tomar una decisión apresurada.

Puedes evaluar la orientación de cada monedero para evitar estos inconvenientes, así como el enfoque que le dan a cada característica.

Por ejemplo, algunos monederos están orientados a la seguridad,

mientras que otros están más enfocados en la privacidad de los datos que otros.

Es necesario que lleves a cabo este proceso de análisis pues no existe "el Mejor Monedero Bitcoin", así que la elección de una persona puede ser completamente diferente a la de otra.

Más adelante te mostraré un listado de monederos disponibles para compra o descarga, pero aunque te sugiero que utilices estos, te recomiendo que investigues y analices cada uno de ellos antes de adquirir o descargar el que elijas.

Ah, una cosa más...

Puede que encuentres recomendaciones de monederos en tiendas virtuales como Google Play Store y Apple App Store, solo te voy a decir una cosa con respecto a estos...

¡¡EVÍTALOS!!

Muchos de estos monederos están diseñados para robar los Bitcoins de la gente.

Si te decides por alguno de estos, al menos trata de obtener información de su código abierto y buenas referencias de sus usuarios para considerar la posibilidad de

utilizarlos.

Los monederos que te recomendaré en el siguiente capítulo, te permiten revisar su código y comprobarlo por ti mismo.

CAPÍTULO VII.

CÓMO MANTENER TUS MONEDAS A SALVO

Lo más esencial para lograr esto es dejar claro un punto, hay monederos que no son gratuitos y otros que sí.

Veamos qué tipos de monederos tienes a tu disposición para que sepas elegir el que más te convenga según tus necesidades:

Monederos hardware

Tal y como te he comentado anteriormente, los monederos hardware son de pago y si bien el precio de algunos puede parecerse elevado, la seguridad que brindan cuando se tiene una cantidad significativa de Bitcoin justifica su costo.

Esto se debe a que un solo monedero hardware puede proteger desde unos cuantos cientos de Bitcoin hasta algunos millones de ellos.

Sin embargo, debes tener en cuenta que no son una billetera o chequera portátil. Es decir, de estos no sacarás milagrosamente X cantidad de Bitcoins para realizar operaciones.

Simplemente manejan las claves privadas en modo offline de cada usuario con el fin de evitar robo por hackeo de información.

¿Por qué es tan importante un monedero hardware con pantalla?

Parece raro imaginar que un dispositivo portátil como estos

tenga una pantalla, sin embargo, resulta muy útil pues te permite verificar los detalles importantes del monedero.

En vista de que estos monederos son casi imposibles de hackear, puedes confiar en la información que se refleja en estas pantallas y en las computadoras a las cuales los conectas.

Te menciono a continuación algunos detalles de los monederos hardware más utilizados:

Ledger Nano S: Es el más barato de los tres monederos

hardware con pantalla. Ledger, una de las compañías de seguridad Bitcoin más conocidas, lanzó el dispositivo en agosto de 2016.

Trezor: Fue lanzado en agosto de 2014 como el primer monedero hardware Bitcoin, ofreciendo almacenamiento seguro de Bitcoins, además de la habilidad de poder gastar con la conveniencia de un monedero dinámico. Trezor es un dispositivo pequeño, del tamaño de un pulgar.

KeepKey: Lanzado en septiembre de 2015, fue el

segundo monedero hardware Bitcoin en ofrecer una pantalla. La gran pantalla del KeepKey te otorga características de seguridad adicionales en comparación al Nano S y el Trezor los cuales carecen de estas.

Ledger HW.1: Puede ser considerado un monedero hardware económico. No tiene pantalla, así que no es tan seguro como las tres opciones mencionadas anteriormente. Sin embargo, te dará más seguridad que un monedero dinámico.

Monederos dinámicos

Este tipo de monederos dependen de una conexión a Internet para su funcionamiento y generan claves privadas que permiten realizar las transacciones virtuales con Bitcoin.

Puedes acceder a dichos datos desde una computadora, teléfono móvil, o tablet pero deben ser usados con cuidado pues no se consideran completamente seguros.

**Monederos Bitcoin
online (Monederos web)**

Por medio de un sistema de encriptación de datos asociado a la contraseña del usuario, este tipo de monederos almacena las claves privadas de cada propietario de unidades Bitcoin.

Si bien es cierto que el nivel de seguridad que ofrecen es inferior en comparación a otro tipo de monederos, estos tienen una ventaja, son accesibles desde cualquier equipo o dispositivo que pueda conectarse a Internet.

Entre estos monederos hay uno que me ha llamado mucho la atención, GreenAddress.

GreenAddress es un monedero Bitcoin multi-signature disponible en la web, para escritorio, iOS y Android.

También es compatible con monederos hardware como Trezor, Ledger Nano y HW.1.

Trabaja en un contexto "Multi-signature", lo que significa que el sitio requiere una confirmación manual de tu parte para mover tus monedas; lo cual aumenta la seguridad en gran medida.

Monederos Bitcoin para Android

Anteriormente ya te advertí sobre los monederos virtuales disponibles para teléfonos inteligentes que pueden ser considerados como una opción viable para la gestión en este tipo de dispositivos.

Puedes confiar en algunos de ellos, pero asegúrate bien de sus intenciones.

La razón de su surgimiento fue un problema de mercadeo para el cual Android brindó la solución.

Durante un tiempo, los monederos Bitcoin fueron prohibidos por Apple y frente a este problema, los programadores mantuvieron su

objetivo pero dedicaron sus esfuerzos, tiempo y atención a la plataforma Android.

Entre los monederos dignos de mención en Android, te muestro los siguientes:

Mycelium

Este monedero Bitcoin para Android es uno de los preferidos entre los usuarios debido a que es veloz, permite añadir un mayor nivel de seguridad a tus Bitcoin al mantener la característica de almacenamiento offline y cuenta con funciones que lo vuelven atractivo.

Entre ellas destaca un control absoluto de tus códigos privados, compatibilidad con otras plataformas, uso de un código PIN para asegurar tu monedero y gestión de los datos a través del Tor (un sistema de enrutamiento de alta-seguridad utilizado inclusive por la Agencia Nacional de Seguridad de EEUU).

Breadwallet

Esta fue la primera aplicación de Wallet Bitcoin creada dentro de la plataforma de Apple, más adelante te daré detalles específicos de esta

versión, pero ya que cuenta con una edición para Android vale la pena mencionarla porque es un verdadero monedero independiente con características de seguridad que lo vuelven interesante.

Entre ellas destaca que no cuenta con un servidor que pueda ser hackeado o desestabilizado. Además, ambas aplicaciones solo requieren un dispositivo móvil para conectarse a la red Bitcoin.

GreenBits

GreenBits es la versión nativa de Android de GreenAddress.

Es un monedero multi-signature que también soporta monederos hardware como Trezor y Ledger.

Además, permite a sus usuarios recuperar Bitcoins en caso de desaparición a través de nLockTime.

Bitcoin Wallet

También conocida como "Schildbach Wallet", fue el primer monedero Bitcoin móvil.

Bitcoin Wallet es más seguro que la mayoría de los monederos Bitcoin móviles, porque se conecta

directamente a la red Bitcoin.

Tiene una interfaz sencilla y la cantidad justa de funcionalidades, haciendo de él un gran monedero y una gran herramienta educativa para los principiantes de Bitcoin.

Como no requiere registro o un servidor en la nube, permite una interacción directa persona a persona.

Además, puedes realizar la conversión a algunas divisas nacionales, utilizar códigos QR, o direcciones Bitcoin para el envío y recepción de criptomonedas e incluso, en caso de no poder

acceder a Internet, puedes realizar los pagos vía Bluetooth.

Monederos Bitcoin para iOS y iPhone

A pesar de que en Febrero de 2014, Apple prohibió los monederos Bitcoin en la App Store, se decidió revertir esta decisión unos meses después.

Gracias a eso, los usuarios de estos dispositivos cuentan con muchas opciones para gestionar sus Bitcoin a través de ellos.

Entre los monederos virtuales para

iOS tienes:

Breadwallet

Considerado uno de los mejores monederos para iPhone, te permite controlar todas tus claves privadas y tiene una interfaz sencilla, con lo cual, el envío y la recepción de Bitcoin no se vuelve un proceso engorroso sino algo simple.

Trabaja con el modo SPV (siglas de Verificación de Pago simplificado en inglés).

Este monedero se enfoca en la seguridad del usuario, ya que está

diseñado para proteger contra agujeros en la seguridad del navegador, robo físico y malware.

Además, cuenta con un cifrado en hardware AES, un llavero firmas de códigos y zona de prueba de aplicaciones.

Lo hermoso de todo esto es la simplicidad del diseño de la aplicación gracias al cual, no solo te es posible revisar o restaurar la información de tu cartera, sino también analizar el historial de tus transacciones incluso en una fase de recuperación.

Airbitz

Al igual que Breadwallet, Airbitz es un monedero Bitcoin disponible tanto para iPhone como Android.

Cuenta con un sistema de inicio de sesión muy sencillo y fácil de configurar, funciones robustas de seguridad que se ejecutan en segundo plano, un directorio de negocios adaptable y un sistema configurable muy amigable, incluso a la hora de realizar la ejecución de pago.

A diferencia de otros monederos, Airbitz crea backups automáticos por lo que no es necesario

preocuparte por realizarlos de forma manual.

Por otro lado, la privacidad del sistema te permite mantener el anonimato, incluso para los programadores de la plataforma, lo cual significa que ningún tercero podrá acceder a tu información personal ni a la de tus Bitcoin.

Monederos de escritorio

Los monederos de escritorio (en inglés desktop wallets) son softwares que se instalan directamente en tu computadora

para que puedas acceder a tus criptomonedas, controlar tus balances o realizar y recibir transferencias.

Estos gestionan el sistema de claves secretas desde el disco duro de tu computadora en lugar de mantenerlas en la nube, permitiendo así que el acceso a ellas sea solo a través del programa.

Si utilizas este tipo de monedero debes realizar respaldos frecuentes para evitar pérdidas en caso de daños o pérdidas de datos en el disco duro y a su vez, debes crear contraseñas de un nivel de

dificultad fuerte, pero que puedas recordar, de forma que solo tú puedas acceder a las direcciones y sin perder los datos consecuencia de olvidar la clave.

Entre estos tipos de monederos se encuentran aquellos denominados full nodes o los light clients.

¿Qué diferencia a unos de otros?

Que mientras que los full nodes almacenan una copia completa de la información del Blockchain, los "light clients" en cambio, dependen de fuentes externas para acceder a ellos y retienen solo la información de los Bitcoins que se poseen.

Entre los monederos de escritorio existe una larga lista de recomendaciones; sin embargo, me centraré en señalarte las características que debes buscar a la hora de elegir uno:

Facilidad de Uso: Si bien una interfaz atractiva suele ser lo que más llama la atención, es mucho más importante que tenga un buen soporte, una seguridad por lo menos de nivel moderado y preferentemente, la oportunidad de retener o almacenar Bitcoins aun sin conexión.

Posibilidad de Adaptación: No te centres solo en un tipo de monedero, en ocasiones es conveniente contar con más de uno, por lo que vale la pena utilizar un monedero de escritorio con soporte para monedero hardware.

Actualización de Datos: Es importante que el monedero que elijas cuente con una revisión y actualización periódica, por lo tanto, infórmate sobre los periodos de mantenimiento de las plataformas de estos, pues si bien no quieres utilizar uno obsoleto, tampoco deseas utilizar otro que

reciba actualizaciones muy frecuentes o innecesarias.

Los monederos que te recomiendo son los siguientes:

Electrum

Es un sistema muy completo que te permite incluso, gestionar el número de Bitcoin que ofreces a los mineros.

Tiene una interfaz sencilla y aprovecha sus recursos para mantener una buena velocidad de trabajo y simplificarlos, al mismo

tiempo que te ofrece la opción de trabajar offline.

En caso de avería o error del sistema de tu computadora, puedes recuperar todos los datos de acceso a tu monedero por medio de la configuración de una frase secreta.

Además, te es posible gestionar los pasos más complejos del sistema de trabajo de las criptomonedas a través de sus servidores remotos.

Bitcoin Core

Es el pionero entre estos monederos y tiene una amplia

aceptación gracias a su confiable historial y la transparencia con que se realizan las operaciones.

Además, sus constantes actualizaciones te ofrecen mejoras en lo referente a privacidad y seguridad.

El único problema que presenta es que no es sencillo de utilizar y ocupa mucho espacio en la memoria, aunque este defecto es compensado por tener acceso completo al blockchain.

Copay

Este monedero admite más de un usuario por lo que es perfecto para aquellos que manejen cuentas corporativas y necesiten más de una firma de aprobación para proceder con transacciones.

Al igual que el Bitcoin Core, no es muy amigable para los usuarios nuevos y puede serte complicado de entender.

Bitcoin Armony

Considerado uno de los monederos más seguros, este cuenta con tres diferentes modalidades de servicio: Standard, Advanced y Developer;

cada uno con sus respectivas ventajas para cada tipo de usuario.

Es compatible con Mac, Linux y Windows y tiene buenas funciones de cifrado y respaldo.

GreenAddress

Este monedero te permite la gestión de Múltiples firmas, además de que cuenta con un sistema de seguridad que requiere confirmación de algunos pasos antes de llevar a cabo las transacciones.

A diferencia de otros monederos de

este tipo, es muy sencillo de utilizar por lo cual recibe cierta preferencia por parte de los usuarios.

CONCLUSIÓN

Bueno, pues ya hemos llegado al final de este libro, en el cual he querido darte luz en el camino de iniciación en el mundo de las criptomonedas y en concreto del Bitcoin.

Si hay algo que creo que te ha quedado casi tan claro o más que a mí, tras este análisis que he efectuado junto a ti a lo largo del libro es que el punto de vista que tienen muchas personas sobre las criptomonedas (casi el mismo que

con las criaturas míticas) queda descartado para ti desde este momento.

Ya sabes que no estamos tratando con fantasmas ni criaturas irreales, sino que estás ante un modelo económico que se ha establecido poco a poco y que se está convirtiendo en la forma de trabajo del futuro.

¿Qué debes hacer ahora?

Mi recomendación es que actúes.

Infórmate, experimenta con los softwares, navega y aprende lo máximo que puedas sobre el Bitcoin.

Seguramente habrás notado que la economía mundial lo está absorbiendo, no para suprimirlo sino para adaptarlo a ella y que no son pocos los programadores que están dedicando tiempo y energía a este sistema. Así que tu decisión debería ser aprovechar todas esas ayudas para beneficiarte y afianzar tu lugar dentro de este mundo que está cambiando y se expande delante de ti.

Quítate los temores y empieza a experimentar por ti mismo para empezar a ser parte de esta red de trabajo.

Probablemente dentro de unos

años, al igual que yo estoy haciendo ahora contigo, tú puedas ayudar a otros a desenvolverse en esta área, en la que pasarás de ser un simple explorador a un guía experimentado.

Ya sabes, a tomar acción y nos vemos en el siguiente libro.

Ah, una cosa más...

Si necesitas de mi ayuda para resolver las dudas que te surjan mientras implementas lo aprendido, me puedes encontrar en:

Correo electrónico:
hola@fernandoamador.com.mx

Facebook:

www.facebook.com/BitcoinLaMoneda

Página

web:

www.fernandoamador.com.mx

Estaré encantado de ayudarte.

Fernando Amador

RECURSOS Y LINKS DE INTERÉS

Glosario

Bitcoin

Es una moneda, pero completamente digital. Es decir, se considera una divisa como el dólar y el euro, pero se centra en ser usada enteramente por Internet. Nada de transacciones físicas.

Altcoin

Es una construcción simplificada de las palabras "alternative" y "coins". Por lo tanto, podría traducirse literalmente como "monedas alternativas".

El término Altcoin se refiere a criptomonedas que derivan del código fuente de Bitcoin también conocidas como "Forks", es decir, ramificación, bifurcación.

Exchanges de Bitcoin

Son empresas que permiten operar

con divisas digitales a cambio de otros activos tales como dinero Fiat (Euro, Dólar, Libra...) o entre diferentes monedas digitales.

Prueba de Participación (PoS)

Protocolo de consenso distribuido blockchain en el que las transacciones son procesadas probando la posesión de las propias criptomonedas.

La posibilidad de que un participante encuentre un bloque y lo descifre es proporcional a la cantidad de criptomonedas almacenadas por él mismo en la

red.

Prueba de Quemado (PoB)

Protocolo de consenso distribuido blockchain en la que una cantidad de fichas son quemadas, es decir, enviadas hacia una dirección que a su vez no puede gastarlas.

Esta prueba no consume tanta energía como la prueba de trabajo, sino únicamente las fichas en cuestión.

Prueba de Trabajo (PoW)

Protocolo de consenso distribuido blockchain consistente en la resolución de problemas matemáticos, una secuencia hash, que tiene una variable que lo dificulta.

Resolver la prueba con éxito suele requerir tiempo y energía, por esto, en última instancia, este sistema condiciona la capacidad de minado al poder computacional del usuario.

Blockchain

Nombre que reciben actualmente la tecnología Bitcoin y sus bifurcaciones, pero que se refiere

específicamente a la secuencia de bloques que almacenan información y que han sido verificados por los usuarios de la red desde sus inicios.

Satoshi Nakamoto

Es el pseudónimo utilizado por la persona o grupo de personas que desarrollaron el protocolo de Bitcoin.

Está retirado desde 2010.

Minería

Es el acto de resolver un bloque,

validando todas las transacciones que contiene.

Dinero FIAT

Es un tipo de dinero establecido como moneda por regulación gubernamental o por ley.

Históricamente el dinero era una mercancía con valor intrínseco y las monedas valían su peso en el metal que estaban fundidas.

ICO

Initial Coin Offering

Links de Interés

www.pequenocerdocapitalista.com

www.bitcoin.org

www.bitso.com

www.blockchain.info

www.oroymfinanzas.com

www.coinmap.org

www.coindesk.com

www.criptonoticias.com

www.elblogsalmon.com

www.criptoeducacion.com

www.aceptamosbitcoin.com

www.coinatmradar.com