La Guía Definitiva

del Inversor Bitcoin

Todo para entender el mundo

de las criptomonedas y lucrar

con ellas.

“*I think that the internet is going to be one of the major*

forces for reducing the role of government. One thing that's

missing, but that will soon be developed, is a reliable e-cash,

a method whereby on the internet you

can transfer funds...in

a way which I can take a 20 dollar bill and hand it over to you

and there is no record of where it came from and you may

get that without knowing who I am".

"Creo que la internet será una de las mayores fuerzas de

reducción del papel del gobierno. Algo que está faltando,

pero que será desarrollado en breve, es una moneda

electrónica confiable, un método en que se pueda transferir

fondos por internet... de una forma que yo pueda darte una

nota de veinte dólares sin que haya registro de dónde vino y

usted puede recibir sin saber quién soy.
"

Milton Friedman, ganador del premio Nobel de economía,

en una entrevista con National Taxpayers Union, en 1999.

Disponible en

http://youtube/mlwxdyLnMXM

Sobre los Autores

André Zabini, CFA

Financista, programador, graduado en Administración de

Empresas por la Facultad de Economía y Administración de

la Universidad de São Paulo, FEA-USP. Desarrollador de

sistemas automatizados de negociación de activos en bolsa.

Tiene experiencia con programación en lenguajes C, C ++,

Java, Assembly, JavaScript y PHP. Amplia experiencia con

inversiones y *trading* de diversos tipos de activos en

mercados local e internacional, en su mayor parte operando la

propia cuenta, siendo registrado en la Comision de Valores

Mobiliários de Brasil como gestor de fondos desde 2014.

Bruno Buscariolli

Graduado y maestro en Administración de Empresas por la

Facultad de Economía y Administración de la Universidad de

São Paulo, FEA-USP. Doctorado e investigador de la

Fundación Getulio Vargas de São Paulo, FGV-EAESP.

Autor de los libros "Econometría con EViews: Guía Esencial

de Conceptos y Aplicaciones", "Todo lo

que necesitas para

entender economía y finanzas" y "Derivados de Cambio en

Brasil - Análisis en series temporales". Tiene publicaciones

en periódicos académicos y es profesor de finanzas y

estrategia

empresarial.

Es

especialista

en

métodos

cuantitativos y econometría.

También es consultor de planificación estratégica y

evaluación financiera. Trabajó en proyectos con empresas de

los sectores público y privado para evaluación de inversiones,

mejora de eficiencia operacional y estrategia para creación de

valor.

Sumário

Introducción

" *Bitcoin has the balance and incentives right, and that is why*

it is starting to take off"

“Bitcoin tiene el equilibrio e inventivos adecuados y es por

eso que está empezando a despegar."

Julian Assange, fundador de Wikileaks

El 10 de diciembre de 2017, la Chicago Board of Trade, una

de las mayores y más antiguas bolsas de valores de Estados

Unidos, abrió negociación para contratos futuros de bitcoins

y el mundo vio su precio subir de 15.500 a 18.700 dólares en

menos de 24hs. Al día siguiente, esa valoración fue noticia en

los principales medios de comunicación internacionales. A

pesar de la enorme repercusión, todavía es difícil encontrar a

alguien que pueda responder a la

pregunta fundamental:

después de todo, ¿qué es bitcoin?

Entre octubre de 2013 y diciembre de 2017, el valor de

1 bitcoin pasó de aproximadamente 200 a 18 mil dólares.

Pocas veces en la historia algo valoró tanto en tan poco

tiempo. Los cambios tecnológicos llegaron a un nuevo nivel,

más complejo y profundo. La capacidad de almacenar y

compartir información ha aumentado drásticamente y está

afectando a antiguas y sólidas estructuras burocráticas, como

los operadores y reguladores del sistema financiero.

Instituciones que desde hace siglos prestan los mismos

servicios caminan hacia la obsolescencia. Así como el tren

reemplazó las carrozas y el ordenador la máquina de escribir,

lo que vemos ahora son bancos e

intermediarios financieros

perdiendo parte de sus funciones para tecnologías que

eliminan la necesidad de atravesadores. Hoy, como en el

pasado, muchos tienen miedo de nuevas tecnologías por no

entender cómo funciona e intentan mantener las estructuras

sociales lo máximo posible. Sin embargo, el tiempo muestra

que la tecnología fue la clave para el avance de la humanidad

y los que intentaron luchar contra el curso natural de esa

evolución acabaron perecer.

Es en ese contexto de innovación tecnológica

constante y rápidos cambios en nuestras vidas que surgen las

criptomonedas. La más conocida de ellas es la bitcoin.

Una Breve Historia De La Moneda

En un pasado lejano, cuando surgieron las primeras formas de

organización social, los intercambios de mercancías eran

hechos por trueque, o sea, una mercancía era cambiada

directamente por otra. Con el tiempo, los pueblos crearon

referencias para los intercambios para estandarizar las

relaciones comerciales. El origen exacto de la moneda como

se conoce hoy es desconocido, pero civilizaciones antiguas

usaban objetos como conchas, sal, y

posteriormente metales

preciosos como oro y plata, para comercializar productos y

servicios.

La invención de la moneda posibilitó la expansión del

comercio y la integración entre los pueblos, el mercantilismo

y la globalización, caracterizándose como uno de los grandes

avances de la humanidad.

Durante la edad media, los metales

preciosos eran la

principal forma de moneda y los bancos medievales eran

empresas que guardaban las monedas en un lugar seguro.

Ellos daban un certificado al dueño depositante de las

monedas para que él pudiera rescatar sus valores

presencialmente cuando quisiera. Con el tiempo, los

comerciantes pasaron a usar los certificados de depósito de

monedas en lugar de las propias monedas. Así, los metales

quedaban físicamente seguros mientras las personas podían

comprar y vender usando sólo los comprobantes en papel.

Esto facilitaba el comercio, pues era posible hacer

transacciones de valores grandes sin necesidad de cargar un

montón de barras de metales preciosos y garantizar cierto

nivel de seguridad, pues los banqueros

conocían a los

comerciantes que depositaban las monedas.

Esta dinámica dio origen al papel moneda, que

representaba, en realidad, un depósito de metal precioso bajo

custodia de algún banco. Durante el mercantilismo, los

gobiernos se apropiaron de ese sistema y acabaron creando

un monopolio estatal sobre el control y emisión de papel

moneda. Esta lógica dio origen al sistema de Bancos

Centrales que existe en el mundo hoy.

El sistema en que una cédula de dinero equivale a una

determinada cantidad de metal precioso depositado en banco

se llama patrón oro. Durante más de dos siglos esa fue la

principal regla del sistema financiero del mundo. Este sistema

acabó sólo en 1971, por decisión unilateral del Presidente

norteamericano Richard Nixon.

La moneda es una invención humana. Sólo tiene

sentido cuando se inserta en un contexto social y no es un

fenómeno natural, como la gravedad. En este aspecto,

necesitamos entender el comportamiento y la historia de la

humanidad para entender la función de la moneda. Las

transacciones sólo son posibles cuando hay personas que

quieren realizarlas.

En un análisis muy objetivo, el dinero físico es sólo un

pedazo de papel. Él no sirve como alimento, ni para suplir

necesidades básicas. El papel moneda sólo es válido porque

todos lo aceptan como medio de cambio y reserva de valor.

Este es el concepto de moneda fiduciaria, es decir, un título

que no posee lastre en bien o producto, como metales o

commodities, y no tiene valor en sí mismo. El valor del

dinero resulta de la confianza que la gente tiene en quien lo

emitió, actualmente quien emite dinero son los gobiernos a

través de la casa de la moneda.

En este aspecto, la bitcoin puede representar un gran

cambio de paradigma, en el que las personas empiezan a

reconocer que un producto digital que no existe en el mundo

físico tiene las mismas propiedades de transacción y reserva

de valor que la moneda física.

Por supuesto, un cambio tan significativo no sucedería

repentinamente. El concepto de criptomoneda surgió en 2009

y sólo empezó a llamar la atención de las personas que no

trabajaban con tecnología informática alrededor de 2013. A

pesar de la gran valorización y especulación sobre las

criptomonedas, aún existe mucha desconfianza sobre ellas,

principalmente porque la mayoría de la gente no entiende lo

que son y ni cómo se producen.

Instituciones financieras privadas y organismos

reguladores, como bancos centrales, critican mucho las

criptomonedas, afirmando que no es seguro comprarlas o que

son una burbuja especulativa. Estas afirmaciones son

comprensibles, porque las criptomonedas no están reguladas

por ninguna empresa u órgano central, y eso puede quitar el

poder de control de gobiernos y banqueros sobre las finanzas

mundiales, si pasan a ser ampliamente aceptadas.

En los próximos capítulos usted entenderá lo que son

criptomonedas, cómo se forman y cuál fue la intención de sus

creadores. Vas a entender también cómo

se hace para

comprar y venderlas, cuáles son los riesgos y cómo la gente

está ganando dinero con ellas. Este libro va más allá de las

criptomonedas y aborda su lógica computacional, llamada

blockchain, que tiene diversas aplicaciones en otras áreas.

Seguramente, esta nueva tecnología está en fase inicial y

mucho de lo que conocemos hoy sobre el registro de datos

cambiará en los próximos años. Tal vez en el futuro, los

bancos, operadores de tarjetas de crédito y las oficinas de

registro civil se vuelvan obsoletos.

El Mago de OZ

El patrón oro está muy presente en la cultura

popular, aunque casi nadie lo sepa. La famosa historia del

Mago de Oz, publicada originalmente como libro en el

año 1900, ganó varias secuencias, se convirtió en un

musical de Broadway en 1901 y película en 1939 de gran

éxito comercial.

Su escritor, Lyman Frank Baum, nació en una

familia rica de Nueva York y empezó a trabajar aún en la

adolescencia, convirtiéndose en emprendedor, poeta,

dramaturgo y escritor. Crítico del contexto económico de

su tiempo, Baum creó a Dorothy y sus amigos como

metáfora del contexto político de la época, siendo el

propio nombre una referencia al patrón

oro. Oz es la

abreviatura de la palabra inglesa ounce, unidad de

medida de volumen utilizada en los países anglosajones

para líquidos y metales preciosos. A pesar de las diversas

adaptaciones para teatro y cine, las referencias indirectas

son la esencia de la alegoría.

En la historia, una familia que vive en una granja

en Kansas es golpeada por un tornado que lleva a

Dorothy y su perro Totó a una realidad fantástica.

Dorothy se despierta después del desastre en un lugar

desconocido y se da cuenta de que su casa cayó sobre

una bruja, matándola. Dorothy le pregunta a las

personas locales cómo podría volver a su granja y es

orientada a seguir por el camino de los

ladrillos

amarillos, una referencia al oro, a la ciudad de las

esmeraldas, piedra verde que simboliza el dólar. En el

camino ella encuentra un espantajo que sueña en tener

un cerebro. Este personaje es una metáfora para la

situación del sector agropecuario de Estados Unidos a

finales del siglo XIX.

A continuación, Dorothy encuentra a un hombre

de lata que está oxidado y quiere un corazón. Este

personaje es una metáfora para la situación de las

industrias y sus trabajadores en la misma época. Por

último, encuentra a un león miedoso, que representaría

al candidato demócrata a la presidencia de Estados

Unidos derrotado en 1896, William

Jennings Bryan. Él

discursaba con frecuencia contra el mantenimiento del

patrón oro, pero perdió espacio dentro del propio

partido con el tiempo debido a disputas políticas.

Hay varios estudios e interpretaciones sobre las

metáforas del Mago de Oz, pero pocos espectadores de

la película saben lo que el autor realmente quiso

expresar. La discusión sobre la confianza en la moneda

y los criterios que hacen referencia a las relaciones

comerciales y económicas forma parte de la vida de

todos, aunque no lo sepan.

Capítulo I

¿Qué es Bitcoin?

" *Bitcoin is a remarkable cryptographic achievement and the*

ability to create something that is not

duplicable in the

digital world has enormous value"

"Bitcoin es una notable realización de la criptografía y la

habilidad de crear algo que no es duplicable en el mundo

digital tiene enorme valor"

Eric Schmidt, CEO de Google

Protocolo, Protocolo, Protocolo

En primer lugar, Bitcoin es un protocolo. La Internet está

hecha de protocolos. Es comun escuchar de TCP / IP, HTTP,

etc. Lo que estas siglas tienen en común es el P al final. El P

es de Protocolo. Y eso es exactamente lo que significa.

Cuando hablamos de protocolos diplomáticos, estamos

hablando de reglas bajo las cuales las conversaciones entre

países deben someterse y seguir.

El IP, por ejemplo, significa "Internet Protocol". Es

básicamente un conjunto de reglas que los programas de

computadora siguen para conseguir establecer una conexión,

identificarse y así intercambiar datos. El IP sirve para

organizar una red de ordenadores conectados.

Si no tuviéramos protocolos, todo sería caótico, pues si

un programa de informática establece una regla de conexión

entre dos ordenadores pero no sigue

protocolos externos, esos

dos ordenadores pueden comunicarse entre sí, pero no con las

demás computadoras. En este sentido, es mejor usar el IP,

pues así conecto mis dos ordenadores y todos los demás que

también usan IP.

Por lo tanto, el IP es un conjunto de reglas que los

ordenadores siguen para comunicarse e identificarse en red.

En nuestra sociedad, tenemos protocolos y también tenemos

leyes. Las leyes son creadas por el gobierno, que a su vez

representa los intereses de la sociedad. Si esta teoría ocurre

en la práctica, dejo a otro libro. Las leyes son un conjunto de

reglas que todos los miembros de la sociedad deben seguir.

Haciendo una analogía al protocolo Bitcoin, éste fue

creado por una persona, o grupo de

personas, que nadie sabe

quién es, pero todos los que usan el sistema saben las reglas y

están de acuerdo en usarlo. De esta forma, no interesa saber

quién creó el Bitcoin, a no ser por mera curiosidad. Si los

usuarios del sistema que aceptaron usar las reglas quieren

cambiar el protocolo, lo pueden. Por lo tanto, el protocolo no

está sujeto a su creador o origen. La idea original de la

creación era justamente dar la libertad para decisiones de

consenso entre participantes. Una alternativa a la autoridad

central.

Así como un gobierno que crea y cambia leyes, los usuarios

de Bitcoin también pueden proponer cambios. La diferencia

es que en uno, existe una autoridad central concentrando la

función, y en otro, la tecnología hace posible la eliminación

de la autoridad. En este sentido, el gobierno se vuelve

automatizado.

En otro sentido, la sociedad humana crea las leyes que

las computadoras siguen para comunicarse, intercambiar

valores, etc. Los protocolos de internet, y ahora los de

criptomonedas, sirven como reglas que generan la "sociedad"

de las computadoras, de cierta forma. Las computadoras

siguen los protocolos creados por los seres humanos. Así, la

sociedad humana es la autoridad que rige la sociedad de

ordenadores.

Las

dos

sociedades

están

interconectadas

e

interdependientes. En el momento, las computadoras son

meros intermediarios de las acciones humanas, debido al

hecho de que no existe una inteligencia artificial. Si esta

inteligencia un día vendrá a existir depende mucho de lo que

llamamos de libre albedrío y conciencia. Pero dejemos esta

discusión para otra hora, porque no sabemos si eso será

posible, y caso sea todavía es algo muy

lejos, por lo menos

algunas décadas.

Activo, Moneda, Commodity

Bitcoin es la primera criptomoneda creada en el mundo.

También se denomina moneda digital, pero este nombre no es

muy esclarecedor, pues en la actual economía digitalizada, el

dólar, el euro, el yen y todas las demás también pueden ser

transaccionadas de forma digital. En una

compra por internet,

estas monedas sólo existen como señales eléctricas en

ordenadores. La diferencia entre las criptomonedas y las

monedas reales usadas en transacciones digitales está en

cómo se procesan las transacciones y cómo son emitidas.

A pesar del nombre criptomoneda, la moneda bitcoin

hoy se comporta más como un commodity digital altamente

especulativo. Esto pasa porque es una clase de activo

reciente, con sólo 8 años de existencia. En el nuevo sistema

de

criptomonedas,

hay

espacio

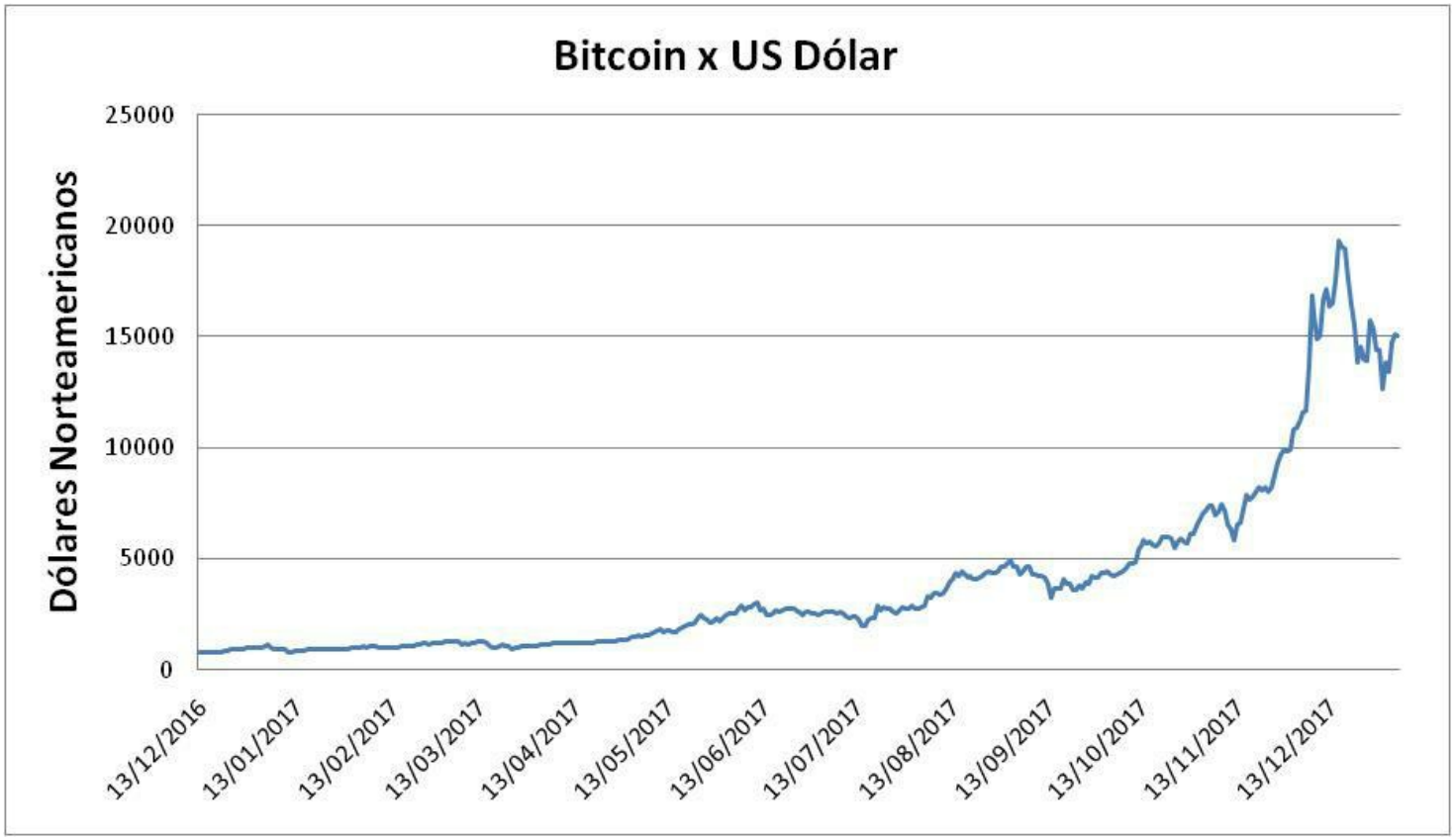
para

diversos

posicionamientos de nichos y vamos a

hablar de ellos en

seguida.



Cotización Bitcoin x US Dólar entre 2013 y 2017

Sistema de Mensajes

En primer lugar, tenemos que separar el sistema Bitcoin

(escrito con B mayúsculo) y la moneda bitcoin (b minúsculo,

su código es BTC). Bitcoin es, esencialmente, un sistema, o

protocolo, de transmisión de mensajes en que los usuarios

pueden decir que están transmitiendo valores directamente

unos a otros. Estos valores son los

bitcoins, la moneda

original del sistema de mensajería.

logo oficial del bitcoin

Cuando un usuario del sistema realiza

una transacción

con otro, comunica la transferencia de bitcoins de forma

digital a los demás usuarios que están conectados más cerca

de él. Estos, a su vez, repasan la información a otros, y así

sucesivamente de forma que toda la red que utiliza la

plataforma toma conocimiento de la transacción en pocos

segundos.

El modelo p2p (*peer to peer*), es decir, de persona a

persona, es aquel que no necesita de intermediario para

conectar a dos usuarios. Ellos conversan directamente entre

sí. Un buen ejemplo de las tecnologías p2p ya existentes son

Napster, BitTorrent, Pirate Bay y todos los demás programas

que conectan a los usuarios directamente para el intercambio

de archivos. Bitcoin, en cierto modo, es

para el dinero lo que

Napster fue para la música. La creación de Napster fue el

comienzo del proceso que popularizó la distribución de

archivos musicales diezmando a las grabadoras musicales.

Quienes están en esta posición ahora son los bancos y los

procesadores de tarjetas de crédito, e incluso servicios como

PayPal.

Los sistemas p2p de comunicación son conocidos por

la extrema dificultad para ser controlados. El drama

involucrando a Napster fue intenso, con procesos judiciales y

discusiones calientes sobre moralidad y legalidad. Después de

Napster, vino una ola de programas p2p, que permitían a los

usuarios compartir no sólo canciones, sino vídeos, libros y

todo lo demás que podría ser

transmitido de forma digital,

generando una guerra entre las autoridades y usuarios, que no

estaban respetando leyes de propiedad intelectual impuestas

por los gobiernos. Por más que hubiera amenazas de prisión y

propagandas diciendo que la descarga de música era ilegal, la

gente siempre podía encontrar una manera de compartir

archivos. Siempre que un programa p2p estaba prohibido,

otros nuevos surgian para ocupar el lugar.

Nadie puede predecir el futuro, pero algo es cierto, las

empresas que no se adecuan al nuevo modelo desaparecerán.

Estamos viendo incluso el advenimiento de bancos digitales,

lo que es un paso intermedio en la adaptación al nuevo

sistema financiero digital. Aun no está claro en cuánto tiempo

la extinción de bancos físicos, o bancos

en general, ocurrirá.

Al final, las instituciones financieras tienen un gigantesco

poder en el sistema político mundial y el interés del gobierno

es mantener a toda costa la estabilidad financiera y

económica del país. Las grabadoras que rompían no

amenazaban el sistema económico actual. Los bancos

quebrando globalmente son otro nivel de amenaza al orden

económico mundial.

Escaso

Bitcoin es revolucionario porque fue el primer sistema

exitoso al crear escasez en el mundo digital. Esto significa

que cada bitcoin es único, y por lo tanto no se puede copiar

con un simple "copiar" y "pegar", como sucede con un

archivo de música, por ejemplo. El problema de la piratería

con música, que Internet ha ayudado a

aumentar, es

justamente la facilidad de crear infinitas copias de los

archivos a un costo prácticamente nulo.

Si la bitcoin fuese copiada, existirían potencialmente

infinitas copias de la moneda, y eso llevaría su valor a cero,

no pudiendo ser usada como moneda. Todos los que ya

vivieron en un ambiente hiperinflacionario lo entienden. La

población de vários países sudamericanos de la década de

1980 y 1990 sabe bien que el dinero puede valer nada, y la

solución para medir el precio de algo es cambiar la referencia

y utilizar por ejemplo el dólar de Estados Unidos, que es una

moneda "fuerte". Muchos países latinoamericanos acceptan

dolares como moneda informal hasta hoy. Por lo tanto, el

hecho de que la bitcoin sea un bien

escaso permite a los

participantes asignar algún valor diferente a ella, y también

utilizarla como medida contable.

Oro Digital

La teoría económica dice que un bien tiende a tener un valor

mayor conforme su escasez aumenta. Un buen ejemplo de

escasez es el oro. El oro es un metal raro en el universo, pues

es un elemento con muchos protones en su composición, lo

que requiere altos niveles de energía y presión en el momento

de formación de las estrellas y planetas.

A pesar de tener

utilidad industrial y como en joyas, su uso es limitado, y la

mayor parte de su valor se deriva simplemente de que la

gente quiere comprar oro y su oferta es limitada. ¿Por qué las

personas atribuyen tanto valor al oro, siendo que su utilidad

es limitada? Bueno, justamente por el hecho de ser escaso.

El oro funcionó como moneda en el pasado porque

tiene otras propiedades, como ser portátil, fácilmente

distinguible, y compacto. El oro es un metal perfecto para ser

usado como moneda. No existen tantos metales en la tabla

periódica que no causan daños a la salud, tienen baja

reactividad y son escasos. Pero la característica principal que

hace que el oro funcione como moneda es su escasez, y eso

es lo que se creó digitalmente con

Bitcoin. Por este motivo

hay personas que se refieren a la bitcoin como "oro digital".

Teorías de valor y el mercado de arte: ¿cuánto vale un

Basquiat?

¿Cuánto crees que vale este cuadro?

El cuadro en cuestión es del artista Jean-Michel

Basquiat, llamado "Untitled" (Sin título). ¿El cuadro

tiene valor?

Para responder a esta pregunta, tenemos dos

teorías. La teoría del valor intrínseco y

la teoría de la

percepción de valor. Un ejemplo de valor intrínseco es

una acción que paga dividendos. Asumiendo que esta

acción continúa generando ganancias para soportar sus

dividendos, la idea es que el valor intrínseco de la acción

sea la suma de la estimación de todos sus dividendos

futuros traídos a valor presente (descontado por la tasa

del costo de oportunidad).

De esta forma, incluso si nadie quiere comprar la acción

del propietario, no hay problema, pues el recibe el valor

intrínseco en forma de dividendos.

La teoría del valor intrínseco es la base de todo el

análisis fundamental de acciones. Inversores como

Warren Buffet utilizan este tipo de análisis para

encontrar buenas empresas en el mercado y comprar

acciones, participando así en los beneficios de la

empresa. No hay nada malo en esta manera de pensar,

pero es incompleta. Según esta teoría, los activos que

no producen flujo de caja no tienen valor. Por eso que

Warren Buffet no invierte en oro y habla a su público de

pasar lejos de Bitcoin.

La teoría de la percepción de valor dice que algo

vale lo que la gente cree que vale. Como el valor sólo

existe en un contexto social, tiene sentido que las

personas definan lo que tiene valor y lo que no tiene. El

cuadro en cuestión fue vendido por 110.5 millones de

dólares en mayo de 2017 para el señor Yusaku

Maezawa, multimillonario japonés. Sólo

la teoría de

percepción del valor puede explicar ese fenómeno, pues

ella cuenta justamente con la subjetividad de los

agentes y el arte es pura subjetividad.

Ahora, usted puede decir: "pero yo nunca pagaría

110.5 millones en un cuadro, por mejor que sea". En

realidad eso está mal, pues en teoría, usted podría

recoger los millones prestados (ver bien: teoría) y

comprar el cuadro por 110,4 millones, y así venderlo al

señor Maezawa, ganando 100 mil en el proceso, por

ejemplo . El punto es que en un mercado transparente y

eficiente el cuadro vale exactamente cuánto la gente

está dispuesta a pagar por él. El precio justo es el precio

de mercado, y nada más.

En la misma línea, Bitcoin representa diferentes

cosas para diferentes personas, por lo tanto su valor

también tiene un elemento de subjetividad involucrado.

En un mundo donde películas, juegos de videojuegos y

fotografías se consideran nuevas formas de arte, no

sería absurdo decir que las líneas de código también

pueden alcanzar el estado del arte,

principalmente

cuando causan impacto social.

Blockchain

El sistema Bitcoin procesa mensajes de transmisión de

valores entre los usuarios. Cuando se realiza una transacción,

se registra en un periódico contable. Este periódico se

distribuye públicamente entre todos los usuarios del sistema,

y contiene todas las transacciones ya realizadas, desde su

concepción hasta la más reciente. Lo que

esto quiere decir es

que todos los participantes tienen acceso a todos los saldos de

todas las direcciones que hayan hecho transacciónes.

Además de ser distribuido públicamente entre los

participantes del sistema, el periódico se construye de una

forma que lo hace incorruptible. Lo que esto quiere decir es

que ningún participante del sistema puede adulterar el

periódico una vez que se actualiza. Este periódico, cuando

fue construido y distribuido de esta forma, se hace en forma

de blockchain. Vamos a separar aquí el sistema blockchain,

sustantivo masculino, de la línea de bloques criptografados

blockchain, sustantivo femenino.

Probablemente ya has escuchado esta palabra, sin tener

idea de lo que es. Se sabe que el blockchain no es más que un

periódico público y distribuido digitalmente, construido de

forma que un bloque de información se procesa y se enlaza

con el bloque anterior. Este vínculo es lo que hace que el

periódico sea incorruptible, pues si alguien intenta engañar y

alterar alguna información del bloque, el periódico entero va

a cambiar, no sólo el bloque adulterado. Como el periódico es

público, los demás participantes, viendo

que los bloques

pasados cambiaron, van a rechazar la información

proveniente del participante deshonesto.

El blockchain, por lo tanto, hace todo más eficiente y

transparente, con la ventaja de ser un sistema distribuido sin

la posibilidad de ser adulterado o censurado. La tecnología de

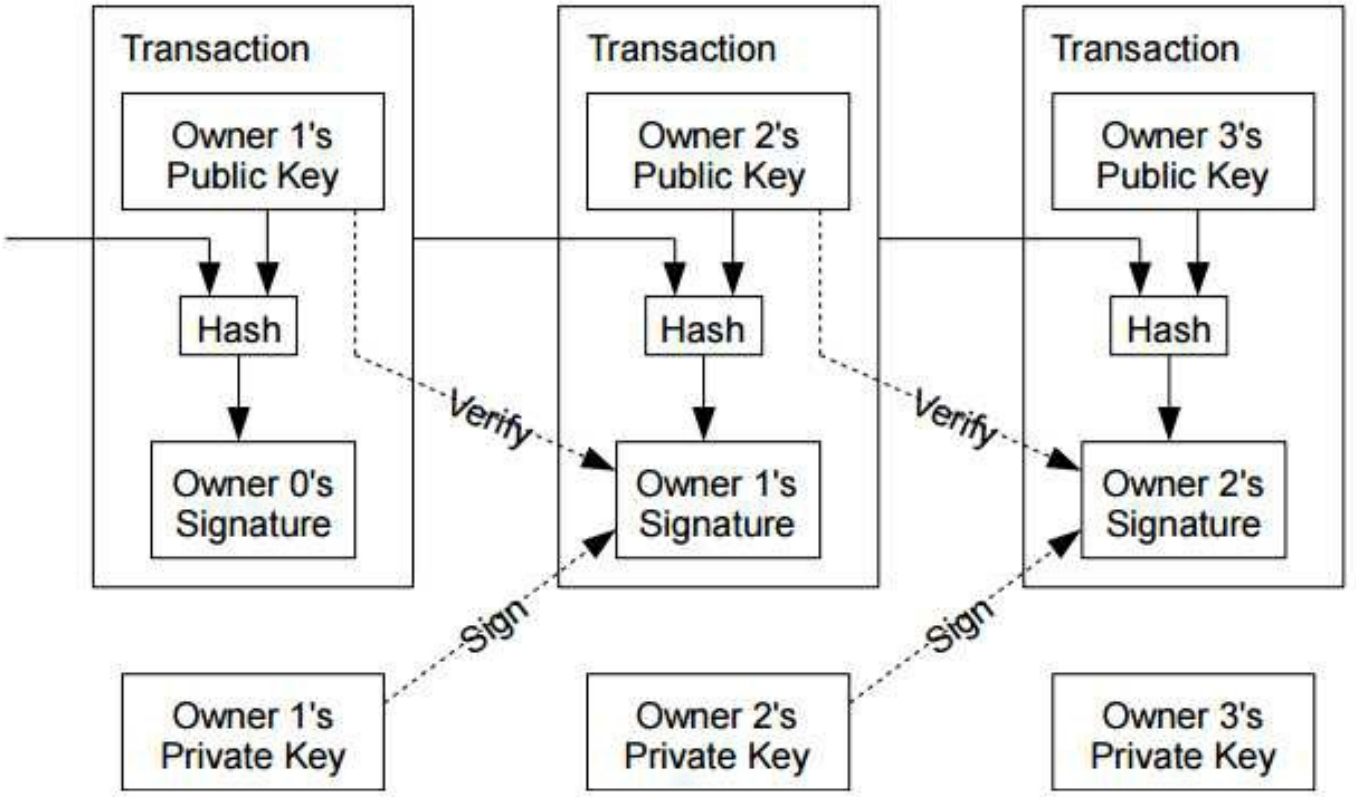
blockchain se utilizará en el futuro para otras aplicaciones

además de la transferencia de valores. Hoy, la mayoría de la

información escaneada en el mundo se almacena en grandes

servidores, de forma no unificada o centralizada, lo que causa

ineficiencias e incoherencias de datos.



Más A Fondo En Blockchain

En el WhitePaper original de Satoshi Nakamoto,

tenemos la siguiente explicación gráfica:

La figura ilustra el proceso de verificación de la

clave pública con la clave privada. Cada propietario

(owner) transfiere la propiedad al siguiente. La

transferencia se realiza cuando el propietario firma el

hash de la transacción anterior y de la clave pública del

siguiente propietario. De esta forma, el receptor puede

verificar todo el historial de propiedad de esa moneda

siendo transferida.

Las transacciones se van colocando una tras otra,

dentro del bloque. Cuando un bloque llega al final de su

capacidad, se cierra el bloque con algunas

informaciones extra que no se refieren a las

transacciones en sí, y se empieza un nuevo bloque,

matemáticamente ligado al anterior y que acomodará

nuevas transacciones.

¿Qué Es Un Bloque? ¿Donde Viven? ¿Cómo Se

Reproducen?

Si estás cansado de escuchar personas hablando de los

bloques, ¿por qué no ver uno de cerca? El primer bloque en

un blockchain surgió el 3 de enero de 2009, el llamado

genesis block. En la versión hexadecimal, parece más o

menos así:

01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E

67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA

4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C

01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00

00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D

01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F

4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C

6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20

73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66

6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05

2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27

19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6

79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4

F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57

8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00

Comprendiste? Tal vez se transformen los bytes en letras sea

mejor:

.....

....;
£íýz{.²zÇ,>gv.a.È.ÃˆŠQ2:Ÿ¸ªK.^J)«_Iÿÿ

....ÿÿÿÿM.ÿÿ....EThe Times 03/Jan/2009 Chancellor

on

brink

of

second

bailout

for

banksÿÿÿÿ..ò.*....CA.gŠý°þUH'.gñ¦q0·.\Ë

Lï8ÄóU.å.Á.Þ\8M÷º..WŠLp+kñ._¬....

No ha mejorado mucho, pero observe la frase que aparece en

el centro del código " *Chancellor on brink of second bailout*

for banks". Este es el titular del diario The Times, de

Inglaterra, del 3 de enero de 2009, demostrando que el bloque

no podría haberse creado antes de esta fecha. Tal vez también

sea una protesta contra las políticas monetarias en la época.

Véase la primera página del periódico con la noticia:

THE TIMES

Max 5C, min -5C | Saturday January 3 2009 timesonline.co.uk No 69623 | £1.50

Eat Out from £5

More than 900 great restaurants, including four **Gordon Ramsay** favourites from £15

Start collecting tokens today Pullout inside

Israel prepares to send tanks and troops into Gaza

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes News, page 3

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", The Times has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the hoil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed guarantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.89 to 1989 levels Business, page 47

Michael Sheen
Frost, Nixon and me
Magazine

Working mums
So that's how she does it
Body&Soul

Detox in style
The best spas on the planet
Travel

Salman Rushdie
I won't marry again
Pages 22, 23

Giant killing?
Guide to the FA Cup third round
Sport

En cualquier caso, estos bytes no representan nada si no

sabemos la estructura del bloque. Dividiendo el bloque por

partes y separando los datos, tenemos la siguiente

información y formato:

PARTE 1

01000000 - Versión

PARTE 2

00000000000000000000000000000000

00000000000 - Bloque anterior

PARTE 3

3BA3EDFD7A7B12B27AC72C3E6776

A51323A9FB8AA4B1E5E4A - Raíz Merkle

PARTE 4

29AB5F49 - El tiempo

PARTE 5

FFFF001D - bits

PARTE 6

1DAC2B7C - nonce

PARTE 7

01 - Número de transacciones

PARTE 8

01000000 - Versión

PARTE 9

01 - input

PARTE 10

0000000000000000000000000000000(

00000000000FFFFFFFFF - salida

anterior

PARTE 11

4D - tamaño de la secuencia de comandos

PARTE 12

04FFFF001D0104455468652030332F4

04368616E63656C6C6F72206F6E2062

7365636F6E64206261696C6F7574206

- firma de la secuencia de comandos

PARTE 13

FFFFFFFF - secuencia

PARTE 14

01 - outputs

PARTE 15

00F2052A01000000 - 50 BTC

PARTE 16

43 - tamaño de pk_script

PARTE 17

4104678AFDB0FE5548271967F1A671

03909A67962E0EA1F61DEB649F6BC3

E51EC112DE5C384DF7BA0B8D578A4

C - pk_script

PARTE 18

00000000 - traba

No es nuestra intención explicar en detalle la función de cada

parte estructural del blockchain, pero observe en la parte 15,

que es la más interesante (para la mayoría de las personas).

Esta parte del bloque representa la cantidad de BTC

transacción.

Cuando se creó el segundo bloque (bloque 1) de la

historia, se añadió sobre el bloque de genesis (bloque 0). El

bloque 1 tiene una relación matemática con el bloque de

genesis. El bloque 1 contiene el hash del bloque génesis. El

bloque 2 está sobre el bloque 1, conectado con el bloque 1, y

así sucesivamente. Cambie algo en el bloque de genesis, y

usted cambia todos los datos hasta el bloque actual!

Los saldos de BTC se calculan mediante el escaneado

de todo el blockchain para saber qué direcciones han hecho

cuántas transacciones. A partir de estos datos, es posible

sumar los saldos y saber qué direcciones poseen BTC y

cuánto. Es básicamente un registro histórico de todas las

transacciones. Hay sitios que hacen esta

lectura en blockchain

y ofrecen información de forma gratuita, como el

https://blockchain.info

Los Mayores Propietarios de Bitcoin del Mundo

La gran dispersión y anonimato del mercado de

criptomonedas nos lleva a cuestionar si hay personas

que tienen grandes carteras, si están concentradas en

algún país o grupo de inversores.

Se sabe que la mayoría de los mineros de bitcoin

están en China, ya que se trata de un país que produce

ordenadores a precios bajos, lo que representa una

ventaja competitiva en el mercado de la minería. Sin

embargo, hay algunas carteras curiosas que llaman la

atención de la comunidad de criptomonedas.

El FBI, la Policía Federal de Estados Unidos, es

dueña de algunas de las mayores carteras de bitcoin del

mundo. Esto sucede porque ellos incautan

criptomonedas provenientes de actividades criminales

en una cartera propia. En 2013, el FBI cerró una pagina

llamada Silk Road y aprehendió, sólo en ese caso, 144

mil bitcoins.

Se estima que Satoshi Nakamoto (el supuesto

inventor del bitcoin) tiene aproximadamente 1 millón

de bitcoins en su posesión, que habrían sido minados

cuando nadie sabía o se interesaba por ellas.

Otro fenómeno intrigante es el de los "Zombi

Coins",

que

son

criptomonedas

perdidas

o

abandonadas, que no pueden ser transacionadas, y que

representan aproximadamente el 30% del total de

bitcoins emitidos. Esto puede suceder por varios

motivos, como la pérdida de la clave de acceso, la

ruptura de un disco duro que contenga la clave o incluso

el fallecimiento de un propietario de bitcoins que no

pensó en dejar la clave accesible para sus herederos.

Un caso trágico es el del experto en tecnología

de información James Howell, del País de Gales. Él

descartó, por accidente, un Hard Drive que contenía la

contraseña de su cartera con 7.500

bitcoins. La prensa

local afirma que pasó semanas moviendo toneladas de

desechos en un relleno de reciclaje en Newport,

tratando de encontrar el HD, sin éxito. A los valores de

diciembre

de

2017,

esta

cartera

valdría

aproximadamente 112 millones de dólares.

Mitos

Hay algunos mitos que no tienen ningún sentido y vamos a

tratarlos ahora, antes de hablar de riesgos verdaderos en los

próximos capítulos. En primer lugar, la criptomoneda no es

un fraude. No fue una invención al azar de la cabeza de algún

hacker para engañar a inversores codiciosos. El sistema de

blockchain y el Bitcoin son realidades,

independientemente

de la opinión de las personas. El número de negociadores de

esas monedas en todo el mundo ya es lo suficientemente

grande para que la opinión de los medios o del ciudadano

común sea poco relevante en el precio de las mismas. La

lógica detrás de las criptomonedas es muy sólida, segura y

millones de inversores, incluso en las bolsas de valores,

reconocen su valor.

Criptomoneda no es esquema de pirámide, como

aquellos en los que alguien vende algo con comisión para

más y más personas y sólo los inventores ganan dinero. En la

mayoría de los países, ese esquema es un crimen.

El argumento de pirámide viene de personas poco

esclarecidas que llegan a la lógica equivocada de que como

Bitcoin no genera flujo de caja, la única forma de ganar

dinero con ella sería vender a un "tonto mayor". Si vamos a

llevar esta lógica adelante, oro y otras materias primas, y

también cualquier acción que no paga dividendos, sería

esencialmente un esquema de pirámide, pues la única forma

de realizar el lucro es vendiéndola en el mercado. Estas

personas llegan a la conclusión de que

se trata de una

pirámide porque no creen que Bitcoin tiene ninguna utilidad

aparte de la especulación. Dejamos al lector juzgar si la

creación de una moneda sin control gubernamental, que

guarda dinero sin depender de bancos en un periódico

contable público e incorruptible, y que permite transacciones

de grandes valores a cualquier parte del globo en cuestión de

segundos a un costo cercano de cero, es inútil.

Algunas personas argumentan que Bitcoin es la

solución a un problema que no existe. Pero la Internet en sí

siguió la misma lógica. La Internet era inútil y no resolvía

casi nada cuando sólo dos personas la usaban, pero crece de

valor según la base de usuarios aumenta.

Hay quien teme que las criptomonedas puedan

simplemente

desaparecer,

ya

que

son

activos

de

computadora. Eso no sucede. Es posible que la clave de

acceso a una cartera sea perdida o robada, y también hubo

ataques de hackers que robaron bitcoins de algunas bolsas de

transacciones, pero en esos casos las monedas fueron

trasladadas a algún lugar, no hubo desaparición. Una vez

registrada la transacción de una criptomoneda, se quedará

para siempre en una cartera. Puede que el valor de la

criptomoneda caiga, pero nunca desaparecer.

¿Por Qué Los Bancos Y Las Entidades

Reguladoras

Critican Tanto Las Criptomonedas?

Todo lo que quita a alguien de la zona de confort tiende a ser

criticado. Las instituciones financieras hacen los mismos

servicios y actividades desde hace décadas y son

extremadamente conservadoras. Cuando surge una tecnología

que es capaz de reducir sus ganancias, más fácil que competir

es criticarla, esperando que no crezca y se convierta en una

amenaza.

Por supuesto, existen riesgos que involucra el mercado

de criptomonedas, pero muchos inversores ya han ganado

fortunas comprando y vendiéndolas, especialmente los

tempranos, los primeros en creer en la tecnología cuando

nadie ni siquiera sabía que existía. Estamos pasando por un

momento de crecimiento de ese mercado y los bancos están,

al menos por el momento, optando por quedarse fuera y

criticar en lugar de invertir en la tecnología y llegar a ser

mejores y más competitivos.

En cuanto a los órganos reguladores, ya sabemos cómo

funcionan las instituciones públicas en Brasil. Son

administrados por funcionarios concursados que nunca serán

despedidos y que no tienen casi ningún incentivo para ser

más productivos. Hasta que los técnicos del Tesoro Nacional

y del Banco Central consigan pensar en una regulación

adecuada para las necesidades del mercado de criptomonedas,

habrán corrido muchos años. Hasta entonces, es más fácil

recomendar que las personas no compren estos activos y no

tener que montar toda una infraestructura

de supervisión y

control.

Capitulo II

Filosofía y Aspectos Técnicos de las

Criptomonedas

"I understand the political ramifications of [bitcoin] and I

think that government should stay out of them and they

should be perfectly legal".

"Yo entiendo las ramificaciones políticas de la bitcoin, creo

que el gobierno debería quedarse fuera de eso y ella debe

ser perfectamente legal."

Ron Paul, ex diputado norteamericano del partido

republicano por Texas

Código abierto

Bitcoin es la última gran creación de un movimiento que

viene tomando cada vez más fuerza en el mundo digital, el

movimiento *open source* (código abierto). El código abierto

significa que el código de programación utilizado para

construir el software (programa de ordenador) es público y

cualquier persona puede leerlo en su totalidad, posibilitando

saber lo que cada línea de comando del programa hace.

Los programas de código abierto generalmente son

construidos por comunidades de desarrolladores no

remunerados directamente por una empresa o organización.

Estos desarrolladores tienen

motivaciones además de ganar

dinero. Al contribuir con una aplicación abierta, por ejemplo,

el desarrollador puede ganar fama en la comunidad, y

también confianza entre los usuarios y programadores, y

tener ingresos de otras formas que no la venta directa de la

aplicación.

A diferencia de programas propietarios, que también

se llaman cajas negras, por no ser posible saber lo que el

código contiene, el código abierto acaba teniendo mejor

calidad, por pasar por "auditorías" de toda la comunidad

involucrada en la construcción del código. Esto significa que

los posibles errores en la programación se corregir

rápidamente. Esta comprobación pública del código también

genera confianza entre los usuarios, ya

que están seguros de

que el programa no está haciendo nada malicioso, como por

ejemplo, recogiendo información sin el conocimiento del

usuario.

Es importante destacar que en la comunidad de

desarrolladores existen muchos idealistas, algunas veces

radicales. Estas personas contribuyen al desarrollo de la

cultura de código abierto como una filosofía de vida

colaborativa y anti-corporativa.

Wikipedia

Un ejemplo del movimiento del código abierto es la

Wikipedia. Cualquier usuario puede ir en la enciclopedia y

actualizarla de forma colaborativa.

Los escépticos decían que Wikipedia no serviría como

fuente de datos por no ser sujeta a una autoridad central y por

ser pasible de vandalización por cualquier persona usando

internet. Sin embargo, la enciclopedia consigue mantenerse

actualizada diariamente sin corromper su integridad, gracias a

voluntarios que contribuyen con contenido y también hacen

su control de calidad.

La Wikipedia hasta hoy se mantiene con donaciones,

pues no tiene anuncios y no remunera a la mayor parte de sus

colaboradores. Este es un modelo de negocio difícil, pero esta

enciclopedia está empezando a ser cada vez más aceptada,

incluso en el medio académico.

Linux

El otro gran ejemplo de código abierto y gratuito es Linux, el

sistema operativo que sirve como alternativa a Windows, que

a su vez es un programa propietario de Microsoft, una

empresa que busca el beneficio a través de la venta de

códigos de computadora. Gran parte de la comunidad de

desarrolladores prefiere Linux,

precisamente por ser un

código abierto y transparente. Como Linux es una

construcción

colaborativa

que

agrega

mucho

más

desarrolladores que una sola empresa, acaba teniendo una

ventaja competitiva en términos de calidad y facilidad de uso.

La única razón por la que Microsoft sigue existiendo es que

fue el *first mover*. Ella llegó antes en el mercado y logró

establecer un monopolio de sistemas operativos. Las

empresas todavía pagan a Microsoft sólo por inercia. El costo

de cambiar a un sistema operativo gratuito es grande, ya que

todas las empresas utilizan el mismo

sistema (Windows) y

esto

puede

generar

problemas

de

compatibilidad,

esencialmente aportando más costos al comienzo del cambio.

En el largo plazo, sin embargo, la tendencia es que los

problemas de compatibilidad disminuyan y las empresas

empiecen a cambiar al código abierto cuando se dan cuenta

de que ya no tienen que pagar por software.

Gran parte de la comunidad de desarrolladores no

aprecia los productos de Microsoft, justamente por tener un

beneficio con un modelo que recuerda al señorío, ofrece un

producto discutiblemente inferior, con

pocas innovaciones.

Microsoft, a su vez, tiene gran poder financiero y consigue

atraer y remunerar desarrolladores de calidad. Es una guerra

entre el viejo modelo empresarial y el nuevo modelo

comunitario.

Encriptación

Esta es quizás la parte más difícil de entender. La blockchain

sólo es incorruptible gracias a la

encriptación. La bitcoin sólo

es escasa debido a la criptografía. Es más allá del alcance de

este libro explicar en detalle las propiedades matemáticas de

las técnicas criptográficas, pero vamos a proveer una base

para entender como funciona todo.

La criptografía está presente en toda la internet y es

básicamente lo que trae seguridad a la red. Cuando entramos

en una página en que antes de la "www" aparece escrito

"https", significa que la conexión se cifra (el "s" en https es

de "seguro"). Cuando sólo aparece escrito http, significa que

la conexión no está cifrada. Esto quiere decir que un agente

malintencionado puede monitorear su tráfico de Internet, sin

que usted lo sepa. Si la conexión es encriptada, el agente

puede supervisar, pero no podrá

descifrar nada de lo que está

monitoreando.

Las bases de datos de grandes empresas son hackeadas

a menudo. Si estas bases no estan encriptadas, hay acceso a

toda la información. Por otro lado, si la base está encriptada,

aunque disponible, el hacker no sabrá leer lo que está escrito.

Las firmas digitales se basan en el cifrado. Hoy sólo es

posible firmar digitalmente algo porque existen técnicas

criptográficas para esto.

¿Cómo Funciona el Cifrado de Bitcoin?

La criptografía de Bitcoin utiliza claves asimétricas. Primero,

vamos a dar un ejemplo de clave simétrica.

Suponga que desea enviar un mensaje cifrado. Puedo crear la

siguiente clave:

A = 1

B = 2

D = 4

E = 5

I = 9

N = 13

U = 15

Usando esta clave, si quiero encriptar la frase "buen día", el

resultado sería: 2 15 5 13 4 9 1.

Para descifrar esta frase, yo usaría la misma clave, es decir, 2

15 5 13 4 9 1 vira B U E N D I A.

La clave se llama simétrica porque la misma clave se utiliza

para cifrar y descifrar.

Un par de claves asimétricas es aquel en que las llaves

presentan una relación matemática entre sí. Hay la clave

privada y la pública. La pública es de conocimiento de todos,

mientras la privada debe ser de conocimiento sólo de un

usuario. La clave pública descifra lo que la clave privada

cifró, y viceversa. El ejemplo más simple de clave asimétrica

es el siguiente:

Vamos a considerar el par de claves:

Clave privada = (33,3)

Clave Pública = (33,7)

Vamos a considerar también que la letra "B" sea representada

por el número 2.

Para encriptar la letra "B", tenemos que hacer el siguiente

cálculo:

B = 2 ^ 3 mod 33 = 8

Si aplicamos la fórmula para las demás letras de la frase

"buen día", tenemos: 8, 9, 19, 31, 3, 1.

Para revertir el texto cifrado, sólo es posible hacerlo con la

clave pública, a través del siguiente cálculo:

B = 8 ^ 7 mod 33 = 2

Es así que las firmas digitales funcionan. Si hago un texto

encriptado con mi clave privada (que sólo yo tengo posesión),

cualquiera con la clave pública (que cualquiera puede tener

posesión) sabe que este texto vino de mí, ya que si no viniera

de mí, la clave pública no funcionaría, y el texto sería

ilegible.

Por el contrario, todos los que poseen la clave pública

me pueden enviar mensajes en Internet con seguridad, porque

sólo yo conseguire descifrar el texto cifrado con la clave

pública, ya que sólo yo tengo la clave privada, que es lo que

transformará el texto en algo inteligible .

Es así que las bitcoins se transforman en propiedad.

Sólo puedo transferir mis bitcoins a través de la clave

privada.

Hashes

Hash es una forma de criptografía que deriva una clave

pública con un formato específico de una clave privada de

formato diferente. Bitcoin utiliza algoritmo sha256 para hacer

una parte de la criptografía. Para entender mejor, podemos

dar como ejemplo lo siguiente:

Imagínese que desea encriptar las siguientes frases con el

algoritmo sha256:

Frase 1:

¡Hola buenos dias! Soy un ejemplo de encriptación del

algoritmo sha-256.

hash:

7228ed117b2532948f09b79bfd1c1b2ee8

330c2f4c6d4d

Frase 2:

Hola.

hash:

ee6494f54a3e6a4605ff8fd710ff6980f65

bc71335e659f

Frase 3:

Hola

hash:

5aeabdff63d243ede0cf64001a9ae5396e1

54ceb9d7a6b

Se percibe en los ejemplos que las frases encriptadas tienen

extensiones diferentes, pero la cifra resultante es siempre en

el mismo formato. También percibe que la diferencia de la

frase 2 a la 3 es sólo un "." (punto), pero la pequeña adición

del punto cambió completamente el resultado de la cifra.

Estas son algunas de las importantes propiedades

criptográficas que hacen que las claves sean prácticamente

imposibles de romper.

La seguridad criptográfica de los algoritmos utilizados

por Bitcoin nunca se ha roto. No es posible probar que sea un

sistema 100% seguro e imposible de romper, pero hasta hoy

nadie ha logrado, incluso con la participación de muchas

personas inteligentes y altamente especializadas en

investigaciones de seguridad digital.

La

única

forma

de

romper

la

criptografía

implementada es a través del *brute forcing*, o sea, usar la

fuerza bruta del poder de procesamiento de las computadoras

para intentar millones de combinaciones

por segundo para

encontrar la clave privada correspondiente a la clave pública.

Pero con esta técnica, incluso usando todo el poder de

procesamiento de todas las computadoras del mundo al

mismo tiempo, trabajando las 24 horas del día, tardarían

millones de años para encontrar la clave correcta. Para tener

una idea concreta de eso, es mucho más fácil alguien ganar

várias veces en las loterias más dificiles del mundo que

romper la criptografía implementada.

Un riesgo contra el algoritmo criptográfico actual es el

advenimiento de los llamados ordenadores cuánticos, que

pueden presentar una mejora de desempeño exponencial en el

poder de procesamiento de las máquinas. Obviamente la

comunidad de desarrolladores lo sabe, y cuando el ordenador

cuántico se convierte en una realidad, un nuevo algoritmo

más fuerte será propuesto y aceptado democráticamente por

la comunidad de usuarios, desarrolladores y mineros.

Minería

Es muy posible que ya hayas oído hablar de minería de

bitcoins. La minería es el proceso en que varias computadoras

compiten para intentar encontrar un hash que satisfaga las

condiciones impuestas por el protocolo de Bitcoin. Cuando

un equipo encuentra el hash, gana el derecho de validar el

bloque. Esto significa que gana el derecho de añadir un

bloque en el blockhain. Cuando un bloque es validado, todos

los ordenadores de la red reciben esta información, y

entonces todos ellos parten para intentar encontrar el hash del

próximo bloque.

Cuando el bloque es validado, el ordenador que lo

encontró recibe bitcoins como recompensa, además de tasas

de intermediación, como un incentivo por el trabajo. Es ese

sistema de incentivos que hace la red segura, pues si no

hubiera remuneración, no existirían muchos mineros, apenas

unos pocos voluntarios. Cuanto más mineros, más poder de

procesamiento tiene la red y más se

vuelve segura. La

seguridad viene en la forma de más usuarios atestiguando que

el blockchain es válido en ese formato, y también impide el

llamado ataque del 51%, que podría suceder si el poder de

procesamiento se concentra en sólo una entidad minera.

Para un usuario, los dos sistemas implican confianza.

Con los bancos centrales, los usuarios deben confiar en la

autoridad monetaria y en el gobierno. Deben confiar en que la

autoridad tomará la mejor decisión posible en favor de la

sociedad y la economía. En el otro, existe la confianza en las

matemáticas, en el protocolo. El protocolo es el decisor, y el

protocolo ya está establecido, no existe imprevisibilidad en la

oferta de moneda. Alguien puede preguntar: pero ¿quién

decide el protocolo? ¿Cómo estoy

seguro de que no van a

cambiarlo?

El protocolo fue creado por un programador (o grupo

de programadores) conocido como Satoshi Nakamoto, pero ni

él no tiene el poder de cambiarlo. Bitcoin tiene el código

abierto como filosofía, entonces los códigos son todos

definidos por la comunidad y los votos de los participantes.

Es público y se distribuye a todos los usuarios, mineros y

desarrolladores. Si alguien quiere participar en el sistema,

debe seguir las reglas del consenso.

Esto no quiere decir que el protocolo es inmutable. Si

hay consenso en la comunidad de que alguna parte del

protocolo deba ser cambiada, será planteada una propuesta y

ésta será votada. Si, por ejemplo, la comunidad votara que la

oferta de bitcoin deba ser aumentada, entonces eso será

discutido democráticamente y decidido. Aquí es importante

resaltar el auto-interés de los individuos, sea este interés

económico, vanidad, o ideología.

Los mineros, desarrolladores y usuarios tienen interés

en mejorar el sistema para que sea más útil y valioso. Un

aumento en la oferta de bitcoins llevaría, en las condiciones

actuales, a una quiebra en la confianza del protocolo, lo que

no es del interés de nadie. Esto no significa que nunca puede

haber un aumento en la oferta de bitcoins. Pero en el

momento, no existe la necesidad de hacerlo, y muy

probablemente no va a existir, dado que 1 bitcoin es

fraccionable en 100 millones, o sea, incluso si el precio sube

drásticamente, y un bitcoin se vuelve

muy caro para ser

negociado en la unidad, las personas podrán negociar

fracciones de la moneda, los llamados "satoshis", menor

fracción posible de la bitcoin (1 bitcoin = 100 millones de

satoshis).

Vamos a explicar la minería por medio de un ejemplo:

Usemos como referencia el bloque genesis. Ya sabemos lo

que es un hash. El hash del bloque
génesis es el siguiente:

000000000019d6689c085ae165831e934

3f1b60a8ce26f

Se percibe el número de ceros al
comienzo del hash. Es así

que el protocolo controla la dificultad
de encontrar el hash,

por el número mínimo de ceros
necesarios. Hay un campo en

cada bloque de blockchain, que se llama
"nonce". Si usted

mira en el ejemplo del bloque génesis, sería la parte 6 de su

estructura. Este nonce es un número que se debe cambiar

constantemente para minar, y cada vez que se cambia esta

parte del bloque, se genera un hash diferente. El bloque sólo

se valida cuando se encuentra un hash con un determinado

número mínimo de ceros. Esta es la condición que el

algoritmo impone para evaluar si un

bloque se ha validado

apropiadamente o no.

Es así que ocurre el *brute forcing*. Los mineros se

quedan cambiando el nonce y calculando nuevos hash en

todo momento, hasta que alguien encuentre un hash que

satisfaga la condición, es decir, un hash que tenga el número

de ceros correcto. Cuanto más ceros al principio, más difícil

de encontrar un hash de este tipo. Cuando se encuentra el

nonce, el bloque se agrega con aquel nonce y nada más en el

bloque cambia.

Cuando un minero encuentra el nonce que genera el

hash correcto, este minero transmite su hallazgo a toda la red.

El resto de los mineros prueban si el nonce realmente genera

el hash transmitido. Si los demás mineros comprueban la

validez del hash, todos agregan el bloque validado y parten al

siguiente.

Es posible que dos mineros minen bloques diferentes

al mismo tiempo. Cuando esto ocurre, momentáneamente,

habrá dos versiones de blockchain en la red, pero esta

condición no dura mucho tiempo, pues el protocolo instruye a

dar prioridad a la blockchain con mayor número de bloques.

De esta forma, un blockchain concurrente rápidamente es

descartado cuando pasa a ser menor que la blockchain oficial.

En otras palabras, la blockchain oficial es siempre la que

presenta mayor número de bloques.

Proof of Work, Proof of Stake

Todo este procesamiento consume mucha energía, e

implica mucho trabajo de las computadoras. El proceso de

minería de Bitcoin por lo tanto adopta un concepto llamado

proof of work (PoW), o prueba de trabajo. PoW es

simplemente la forma de recompensar al equipo que presentó

el hash correcto, que sería la prueba de que el ordenador

contribuyó a mantener la red funcionando.

Una alternativa al PoW que viene ganando fuerza es el

Proof of Stake (PoS). En el PoS, no se

mina la moneda, sino

que se forja. El PoS da el derecho al usuario de forjar cierta

cantidad de monedas proporcionalmente a la cantidad de

monedas que tiene en posesión. Cuanto más monedas tenga

un validador, mayor será la posibilidad de que sea elegido

como validador del próximo bloque.

El PoS consume menos energía que el PoW, pues no

implica cálculos intensos para encontrar el nonce correcto,

por lo tanto es más eficiente y ambientalmente amigable. El

PoS también alinea los intereses de los agentes, pues los

validadores están obligados a poseer la moneda que están

forjando, además de ser un sistema más justo con los

usuarios, que ganan una oportunidad mejor de entrar en la

validación y contribuir a la seguridad de

la red.

El problema de ASIC y GPUs

ASIC (Application Specific Integrated Circuit) es un equipo

desarrollado con un único propósito: minería. Este equipo

sirve muy bien para esta tarea, y no puede hacer nada más. A

pesar de que no es muy versátil, este tipo de ordenador es

muy eficiente en el proceso de minería.

En el comienzo de Bitcoin, la gente

podía minar con

sus CPU o computadoras domésticas, de acuerdo con la

visión inicial del proyecto de "un ordenador, un voto". De

esta forma, los usuarios tenían poder de voto y tenían más

poder de decisión en el protocolo. No tardó en que algunas

personas comenzasen a minar con GPU (Graphical

Processing Units). Se trata de computadoras con tarjetas

gráficas de alta capacidad de procesamiento, que se pueden

utilizar en paralelo. Los usuarios que antes usaban las tarjetas

para procesamiento de datos o juegos digitales, pasaron a

montar máquinas con decenas de GPUs para ganar rapidez en

la minería de bitcoins.

Con la entrada de empresas en el desarrollo de ASICs,

hubo gran aumento de eficiencia y la competencia por

minería fue a un nivel profesional. Hoy, el poder de

procesamiento de la red es tan grande, que los pequeños

usuarios se quedaron fuera del juego. No compensa minar

con CPUs domésticos, pues se gasta más en energía eléctrica

que las ganancias con la emisión de nuevas monedas. Este es

un problema en el sistema, pues existe una concentración de

poder en la mano de los mineros, que se

han convertido en

grandes empresas de procesamiento de transacciones.

En base a esto, otras criptomonedas más nuevas

corrigieron este problema e hicieron algoritmos de minería

resistentes al ASIC. Esto significa que no hay aumento de

eficiencia al usar un ASIC para minar la criptomoneda.

Esto trajo la minería de vuelta al campo de las GPU.

Cualquier individuo con conocimiento para cómo montar un

ordenador puede participar en la minería. Así estas nuevas

monedas se mantienen fieles a la visión original del proyecto.

Irónicamente, la moneda original, bitcoin, no logró

mantenerse en un nivel de minería doméstico, por sus

desarrolladores

no

habían

previsto

este

tipo

de

desdoblamiento. Hoy en día, con el poder excesivo de los

mineros y su resistencia a enfrentar más competición, es muy

difícil que el algoritmo de minería sea cambiado para

favorecer al pequeño usuario. La buena noticia es que hay

muchas otras monedas buenas en el mercado que tiene menos

concentración de poder.

Grietas en la Comunidad, hardforks y softforks

Siendo Bitcoin un protocolo definido por consenso, existen

divergencias de opinión. Una discusión técnica polémica en

la comunidad es en relación al tamaño del bloque en el

blockchain. Bitcoin hoy enfrenta problemas de escalabilidad,

ya que aún no puede procesar muchas transacciones por

segundo. Uno de los motivos de esta limitación es el tamaño

del bloque. Aumentar o no el bloque no es una decisión tan

simple como parece, pues involucra problemas de seguridad,

capacidad de almacenamiento y concentración de poder de

los mineros. Por esa y otras polémicas,

ocurren grietas en la

comunidad. Cuando un grupo influyente no puede votar su

propuesta en la comunidad, ellos pueden aceptar la derrota, o

salir de la comunidad. Cuando estas personas salen de la

comunidad, a veces toman la decisión de hacer el llamado

hardfork. Un hardfork en blockchain es exactamente como

suena. Si el blockchain se ve como una línea de bloques, uno

encima del otro, la bifurcación ocurre cuando la línea se

separa en dos.

La bifurcación se debe a que estas personas deciden

cambiar el protocolo independientemente del resto de la

comunidad aceptar y pasar a la versión modificada del

protocolo. Esta nueva versión no es compatible con el

software antiguo utilizado por el resto de la comunidad. En el

momento en que se cambia el protocolo, un nuevo blockchain

pasa a existir en paralelo con el original. Como las

blockchains ahora son distintas, las monedas pasan a ser

distintas también. Los mayores ejemplos de hardfork hasta el

momento fueron las creaciones de Bitcoin Cash (BCH),

Bitcoin Gold (BTG), y también la separación de Ethereum

(ETH) y Ethereum Classic (ETC).

Hay todavía algo llamado softfork, que es cuando se

producen cambios en el código, pero la nueva versión es

retrocompatible. Esto significa que incluso si no todos los

usuarios actualizan la versión de su software, los bloques

generados seguirán siendo válidos para el nuevo código. Esto

impide la racha y la creación de nuevas monedas, ya que

todos los participantes todavía pueden

conversar. El hardfork

a su vez, es incompatible con otras versiones de código, y la

actualización de software es obligatoria, generando dos

versiones incompatibles de blockchain.

Airdrops

Los Airdrops se producen con hardforks. Cuando existe la

división de blockchain en dos, los usuarios que tenían saldo

en la moneda original también pasan a tener las nuevas

monedas. Esto ocurre pues la moneda nueva tiene el

blockchain en común con la moneda original en fechas

anteriores al hardfork. También existe la

posibilidad de

airdrops como forma de promoción de nuevas monedas. En

este caso, los usuarios que se involucran en el proyecto

pueden recibir dinero de forma gratuita, pero los airdrops

derivados de hardforks son nuestro principal foco aquí.

Una analogía en el mercado de acciones sería el

desdoblamiento de acciones. Cuando esto ocurre en una

proporción de 1: 2 por ejemplo, una acción se vuelve dos y su

precio cae a la mitad. Para el inversionista, el total financiero

no cambia, pues ahora tiene dos acciones con la mitad del

precio, totalizando el mismo importe original.

Pero la analogía queda ahí. A diferencia del

desdoblamiento de acciones, en que se sabe de antemano el

precio de las nuevas acciones

inmediatamente después del

evento, en el fork de monedas el precio es incierto, y puede

ser que si la nueva blockchain no está bien hecha, su valor

caiga a cero. El mercado lo decidirá. En este sentido, las

nuevas monedas pueden captar una parte del mercado de la

moneda original, o también pueden atraer nuevos inversores,

creando su propia cuota de mercado.

Un ejemplo es el siguiente. Cuando hubo el fork del

BTC (bitcoin) en BTC + BCH (bitcoin cash) en agosto de

2017, se puede argumentar que el precio del BTC *post fork*

no es directamente comparable al BTC pre-fork. El precio del

BTC pre-fork debe ser comparado con el precio del BTC *post*

fork sumado con el precio del BCH.

Este enfoque es el más correcto, ya que fue un

hardfork con airdrops. Todos los que tenían BTC antes de

agosto de 2017 ganaron gratuitamente el BCH, pero el BCH

probablemente sacó una parte del precio del BTC pre fork. Es

difícil creer que el precio del BCH subió sin perjuicio alguno

al BTC, y que hubo creación de dinero de esta forma. Por lo

tanto, para un inversionista que desea comprar el BTC

original, se podría argumentar que debe

comprar BTC y

BCH, en una proporción parecida a la relación de precio

original justo después del fork. Ejemplo: El BCH valía

aproximadamente el 10% del precio del BTC después del

fork. Entonces un inversor podría comprar R $ 1 de BCH

para cada R $ 10 de BTC comprado.

Es de buen sentido pensar que si no hubiera ocurrido el

fork, el precio del BTC sería más alto hoy. Pero a pesar de

que esto es lógicamente coherente, la verdad es que nunca

sabremos, y puede argumentarse que el propio fork ayudó a

elevar el precio de las dos monedas, justamente por haber

sido un gran fork exitoso, y por eso haber aumentado la

confianza en sistema de criptomonedas como un todo.

Infraestructura

¿Cuáles son los factores principales que determinan el precio

de las monedas recién creadas? Básicamente, el factor más

importante es la confianza de las personas en el nuevo

proyecto. Si la gente ve un propósito para que la nueva

moneda se cree, entonces apoyarán el proyecto. Los mineros

validarán las transacciones de la

moneda, las bolsas de

criptomonedas proporcionarán soporte para la negociación de

la moneda, y los desarrolladores seguirá mejorando el

proyecto.

Sin el apoyo de infraestructura, es decir, usuarios,

bolsas y mineros, una moneda no puede tener éxito. Y esta

infraestructura sólo será lograda a través de un proyecto con

propósito bien determinado. Los propósitos pueden ser de los

más variados: cambiar el algoritmo de minería, aumentar la

capacidad de blockchain, aumentar la privacidad, satisfacer

algún nicho de mercado que demandando una función

específica, etc.

Es común oír el argumento de que la escasez de la

bitcoin es falsa porque cualquiera puede crear una moneda

parecida,

aumentando

infinitamente

la

oferta.

Este

argumento, aunque no es teóricamente incorrecto, en la

práctica no es válido. Bitcoin tardó años en ganar tracción y

tener una masa crítica de infraestructura

que generó confianza

de las personas en el sistema. La oferta de criptomonedas es

potencialmente infinita, pero la oferta de bitcoin es limitada.

Con cientos de monedas en el mercado hoy, la mayoría

probablemente no sobrevivirá, pues no habrá demanda para

todas. Sin duda, el mercado de criptomonedas es

suficientemente grande para soportar algunas decenas de

monedas bien desarrolladas.

Hay

varias

criptomonedas

exitosas,

que

son

competidoras del Bitcoin, pero al mismo tiempo también son

complementarias, pues ayudan al mercado de criptomonedas

como un todo a desarrollarse. Esto acaba por beneficiar a

BTC, y BTC beneficia a las otras monedas. En esta etapa de

alta incertidumbre y riesgo en cuanto al futuro de las

criptomonedas, tener más activos complementando el sistema

es positivo. El problema de escalabilidad de Bitcoin será

resuelto parcialmente por una mejora en el algoritmo, y en

parte por la existencia de otras monedas

que ayudarán a

quitar la presión sobre un solo sistema. De esta forma,

podremos de hecho caminar hacia una economía global

basada en las nuevas tecnologías de código abierto.

Otra respuesta al argumento de que cualquiera puede

crear un sistema de criptomonedas, es que esto ocurre en

cualquier mercado. Cualquier persona puede crear un sitio

para competir con Google. Cualquiera puede crear un nuevo

sistema operativo para competir con Windows, pero esto no

passa porque la base de usuarios ya está instalada. Si millones

de personas pasan a usar Bitcoin, esto en sí ya genera una

ventaja competitiva. Hay barreras de entrada, pues hoy una

moneda debe comenzar con una cierta infraestructura, lo que

puede requerir altos niveles de capital

intelectual y financiero

involucrados. Pocas personas son capaces de crear esto.

Capítulo III

¿Por qué invertir en Criptomonedas?

"You can't stop things like Bitcoin. It will be everywhere and

the world will have to readjust. World governments will have

to readjust"

"No se puede parar cosas como el bitcoin. El va a estar en

todo lugar y el mundo tendrá que reajustarse. Los gobiernos

del mundo tendrán que reajustarse ".

John McAfee, fundador de McAfee

La Internet está repleta de noticias y discusiones sobre

criptomonedas, incluyendo reportajes hechos por periodistas

no especializados ni en tecnología ni en finanzas. Vamos a

pasar aquí por los principales argumentos pro y contra, para

que usted sea capaz de sacar sus propias conclusiones y tener

un posicionamiento personal sobre el tema.

Argumentos Pro Criptomonedas

Los principales argumentos en favor de las criptomonedas se

vinculan a la defensa de la libertad, la privacidad, el libre

mercado, el aumento de la eficiencia, la no intervención de

los gobiernos y la reducción de la tributación. Los defensores

más comunes son profesionales relacionados con la

tecnología de la información, seguridad digital y mercados

financieros que entienden la lógica que guía el mercado de

criptomonedas. Ellos tienden a considerar que los

intermediarios financieros (como bancos y operadores de

tarjetas de crédito) imponen un enorme costo de transacción a

los consumidores y que ese costo puede ser evitado. Algunos

de estos defensores consideran que las

agencias reguladoras

(como los bancos centrales o órganos de gestión del tesoro

nacional) que controlan y fiscalizan los mercados financieros

también son barreras a la libertad de los individuos, pues los

gobiernos tienden a defender monopolios y beneficios de

empresas públicas y privadas poco eficientes (normalmente

los mayores contribuidores de campañas políticas) haciendo

todo el sistema lento y costoso.

En general, los defensores de las criptomonedas son

personas jóvenes, familiarizadas con la tecnología y que

buscan romper con estructuras burocráticas preestablecidas,

pues las consideran obsoletas, caras y no democráticas.

Si continúan popularizándose, las criptomonedas

tienden a ocupar el espacio de mercado de instituciones

financieras. ¿Usted se imagina cómo sería un mundo en que

no hayan tasas bancarias ni interés de tarjeta de crédito? O en

que usted pueda comprar y vender bienes de personas que

están en el extranjero sin pagar los absurdos impuestos de

importación? Piense en un mundo sin papeles, sin necesidad

de autenticación de documentos, reconocimiento de firma,

burocracias que piden copias en dos

vías del DNI, seguridad

social y licencia de conducir. Imagínese registrar un

inmueble, o la venta de él, sin pagar valores extorsivos a los

cartones que sellan y archivan papeles. Este es el mundo

defendido por el blockchain y por las criptomonedas.

Un ejemplo simple y real de beneficio: imagine que

usted quiere viajar al exterior y no quiere pagar la carísima

tasa de cambio de dólar turístico. Ya es una realidad comprar

criptomoneda en su país, ir al exterior y cambiarla por dólar o

cualquier moneda no digital en el país de destino sin pagar

tasas ni para gobiernos, ni bancos ni corredoras de cambio.

Quien viaja siempre al exterior y ve al gobierno cobrar

pesados impuestos sobre movimientos financieros y compras

en el exterior entiende rápidamente la

ventaja de esa forma de

transacción.

Todavía estamos lejos de un mundo libre de

atravesadores y muchos problemas todavía pueden surgir

antes de que el blockchain sea algo ampliamente aceptado,

pero la gran popularización de las criptomonedas en países

desarrolladores de tecnología como Japón, Corea del Sur y

Estados Unidos muestra que ese futuro es posible y mucha

gente trabaja para que se concretice.

Argumentos Contra Criptomonedas

Los críticos de las criptomonedas son, en general, personas

que no entienden (o no quieren tener el trabajo de aprender)

cómo ellas funcionan o individuos que representan a grupos

amenazados por los avances tecnológicos. No es exagerado

decir que muchos de los críticos son inversores que perdieron

el buen momento de comprar y critican en un intento de

justificar para el propio ego la pérdida de la oportunidad de

inversión. Algunas críticas, sin embargo, son válidas y deben

ser consideradas.

Por ser un mercado sin un órgano central de control, el

robo por medio de ataques de hackers es una amenaza real y

ya ha ocurrido algunas veces en bolsas de diferentes países.

La compra y transacción de criptomonedas no son intuitivas y

fáciles de hacer como en los mercados de acciones o

commodities. No existe estandarización, márgenes de

seguridad ni casas de liquidación y custodia. Es casi como

comprar y vender pepitas de oro en un mercado sin nadie

supervisando, hecho sólo por internet.

Para negociar criptomonedas es necesario aprender un

poco de informática, instalar y operar softwares que aún no

son muy amigables y estar dispuesto a investigar sobre ellas

constantemente, prestando atención a posibles fraudes o

regulaciones adversas que pueden surgir. Una dificultad que

obstaculiza a los inversores acostumbrados a los productos

clásicos de mercado financiero es la falta de referencia para

establecer un precio justo por las

criptomonedas. La lógica

del *Valuation*, usada para atribuir precio a acciones y títulos

de deuda, no se aplica a las criptomonedas, cuyo precio se

comporta más como el del oro, pero con mucho más

oscilación. Una forma más adecuada de valuación sería algún

modelo macroeconómico de cantidad de moneda y su

velocidad de giro, o aún mejor, alguna valuación basada en

teoría de redes, que afirman que una red crece de valor más

que proporcional según su base de usuarios aumenta.

Una crítica común, pero poco fundamentada, es la de

que repentinamente las criptomonedas pueden perder valor,

pues las personas dejarían de aceptarlas cuando entendieran

que no tienen vínculo como ningún bien físico. Esta

hipótesis, sin embargo, es improbable,

pues lo que se observa

en la práctica es una tendencia mundial contraria. Más que

eso, las monedas emitidas por los gobiernos tampoco tienen

vínculo como ningún producto físico. La población las acepta

como medio de cambio y reserva de valor debido a una

programación mental colectiva, un hecho que nadie cuestiona

y acepta casi como un dogma, una regla absoluta. Pero así

como la sociedad cree y vive en función del valor de un

pedazo de papel emitido por gobiernos y sus burócratas, la

población también puede creer en una tecnología mucho más

avanzada que reemplaza las funciones de diversos

atravesadores y adoptarla como medio de cambio.

Algunos profesionales razonablemente respetados de

mercado financiero critican a las

criptomonedas afirmando

que se trata de una burbuja especulativa que debe estallar en

algún momento pronto. El consejero delegado de JP Morgan,

Jamie Dimon, afirmó en una entrevista con Bloomberg en

septiembre de 2017 que despediría a funcionarios que

negociaran bitcoins por tratarse de un fraude. Robert Shiller,

ganador del premio Nobel de economía que predijo la

burbuja de las empresas punto-com a finales de los años 1990

y de los inmuebles en 2008 también cree que las

criptomonedas están en situación de burbuja.

Por otro lado, John McAfee, creador de la firma de

seguridad digital McAfee, afirmó, también en 2017, que cree

en la continua valorización y aconseja a inversores a

continuar comprando criptomonedas.

Definitivamente no

existe consenso y eso es bueno para quien quiere ganar

dinero, pues demuestra que existe potencial de mayor

adopción.

El Mercado de Criptomonedas y Sus Transacciones

El mercado de criptomonedas sigue siendo relativamente

pequeño en comparación con los mercados financieros ya

establecidos, como el de acciones o commodities. Esto puede

ser bueno y malo. Bueno porque en mercados principiantes

las oportunidades de ganancia son mayores, cuanto más gente

decide comprar un activo, más tiende a valorizarse. Hoy en el

mundo existe un fuerte movimiento de entrada de nuevos

inversores. Esto es evidente cuando se analizan los

volúmenes transaccionados de

criptomonedas, su valor de

mercado y el brutal aumento de variedad disponible.

En diciembre de 2017, el valor total del mercado de

bitcoin, o sea todos los bitcoins existentes multiplicados por

su valor de mercado, varió aproximadamente entre 240 y 250

mil millones de dólares. En comparación con una gran

empresa,

Microsoft,

en

el

mismo

período,

valía

aproximadamente 600 mil millones de dólares. Es decir, hay

mucha gente apostando en las criptomonedas y existe

bastante espacio para crecimiento.

Un lado malo de entrar en un mercado incipiente es la

falta de liquidez, es decir, la velocidad con que es posible

vender los bienes. En el caso de los bitcoins, el mercado es

bastante "líquido", es fácil encontrar compradores y

vendedores de bitcoins queriendo negociar. Para otras

criptomonedas, sin embargo, puede no ser fácil encontrar

compradores y esto implica riesgo. Otra

dificultad puede ser

la oscilación rápida del precio de las criptomonedas, pues aún

no existen referencias mensurables para sus valores, como

existen para acciones y commodities. Un mercado nuevo

puede oscilar más que un mercado maduro y establecido, a

pesar de que esto no es una regla.

Cabe al inversor entender sobre esos riesgos y decidir

si vale la pena entrar en ese mercado o no. En esencia, no es

muy diferente de comprar acciones o oro, los cuidados

necesarios son los mismos y los riesgos son parecidos.

¿De Qué Forma Es Posible Ganar Con El Comercio De

Criptomonedas?

Para explicar sobre las estrategias de compra y venta de

criptomonedas, vamos a establecer un paralelo con las

acciones. Una acción es un título de propiedad parcial de una

empresa. En resumen, cuando alguien compra una acción,

compra una fracción, digamos un milésimo, de la empresa y

tiene derecho a un milésimo de los beneficios de ella. Esta

propiedad es reconocida por el sistema jurídico legal de los

países de forma razonablemente bien estandarizada. Él

inversor declara esa propiedad en su

impuesto sobre la renta

y, si vende la acción, paga un porcentaje de impuesto sobre la

valorización que obtiene.

Las criptomonedas no representan propiedad de un

producto físico, como el oro, no pagan dividendos, como las

acciones, ni los intereses, como los títulos de deuda. Su

valoración depende de la oferta y demanda y el valor de uso

deriva del potencial de facilitar transacciones entre individuos

sin depender de reguladores o atravesadores.

La forma más simple de ganar dinero es comprar la

criptomoneda y venderla a un precio mayor. La minería

también es una forma posible de ganar en ese mercado, a

pesar de las dificultades de esa inversión. Es posible, sin

embargo, ganar especulando de otras

formas, por medio de

instrumentos derivados que serán explicados en los próximos

capítulos.

El Misterio Sobre Satoshi Nakamoto

Se atribuye la invención del Bitcoin y el concepto

de criptomonedas a un individuo de identidad

controvertida llamado Satoshi Nakamoto. Durante años

nadie supo quién era Nakamoto, a pesar de que se

correspondía por correo electrónico ocasionalmente

con algunos miembros de la comunidad que ayudó a

popularizar las criptomonedas.

Propuso el concepto de comunicación directa

entre partes y la solución del problema de la duplicación

de datos a través de la criptografía y el acceso universal

a datos en la publicación "Bitcoin: Peer-to-Peer

Electronic Cash System" el 31 de octubre de 2008. Este

artículo

original

está

disponible

en

https://bitcoin.org/bitcoin.pdf. En sólo 9 páginas de un

texto conciso y objetivo, Nakamoto propone esta

solución para diversos problemas relativos a las

transacciones digitales y crea el concepto de

criptomoneda. El artículo es muy elogiado por expertos

en tecnología de la información por presentar una

solución simple pero muy eficiente para el problema de

las transacciones digitales.

Algumas pessoas ainda duvidam que Wright seja

realmente o inventor do Bitcoin, pois acreditam que os

inventores seriam um grupo de pessoas que preferem

se manter anônimas para evitar perseguições de

governos ou ataques de hacker e ladrões. O próprio

Wright disse que não desenvolveu o conceito sozinho,

mas não identificou quem seriam os contribuidores.

La

identidad

de

Nakamoto

todavía

es

cuestionada, pero muchos aceptan a Craig Steven

Wright, un científico de computación y emprendedor

australiano como la verdadera identidad de Satoshi

Nakamoto. En mayo de 2016 dio una entrevista a la

emisora BBC afirmando ser el creador de Bitcoin y que

evitó revelar su identidad por tantos años por miedo a

sufrir persecuciones y amenazas, sin especificar cuáles.

El mismo día, su casa fue objeto de operación de

búsqueda por la policía australiana, demostrando que

sus preocupaciones estaban justificadas.

En esta entrevista, Wright afirma que ofreció

transparencia sobre el concepto de Bitcoin para las

autoridades reguladoras del mercado financiero en

Australia y que explicó el concepto de las

criptomonedas para auditores de empresas privadas. Él

niega que quiera mantener el sistema anónimo o

convertirlo en algún tipo de territorio libre para

transacciones criminales.

Wright es doctor en ciencia de computación e

investigador de la Universidad Charles Sturt, en

Australia. Publicó libros y artículos sobre seguridad

digital y encriptación. Trabajó en diversas empresas del

sector de tecnología de la información y hoy es socio de

empresas que desarrollan y transacción criptomonedas.

Algunas personas todavía dudan que

Wright sea

realmente el inventor de Bitcoin, pues creen que los

inventores serían un grupo de personas que prefieren

mantenerse anónimas para evitar persecuciones de

gobiernos o ataques de hackers y ladrones. El propio

Wright dijo que no desarrolló el concepto solo, pero no

identificó quiénes serían los contribuidores.

Capítulo IV

¿Cómo Está el Mercado

de

Criptomonedas?

“Right now Bitcoin feels like the Internet before the

browser.”

"Hoy, el bitcoin se parece a la internet antes del navegador".

Wences Casares, fundador del Banco Lemon, ganador del

juego de Xbox del año, por el juego Assault Heroes.

Bitcoin surgió en 2009, pero ese año no ocurrió ninguna

transacción en mercado organizado. Los gráficos de precios

de bitcoin inician el registro de precios en julio de 2010,

cuando las negociaciones comenzaron a ocurrir. Las primeras

apreciaciones significativas ocurrieron en 2013, año en que el

valor de un bitcoin pasó de aproximadamente 14 a 980

dólares. Después de eso, la cotización

cayó gradualmente,

alcanzando una mínima de 224 dólares en agosto de 2015. En

los meses siguientes, la cotización fue subiendo gradualmente

hasta febrero de 2017, cuando alcanzó la marca de 1000

dólares y siguió subiendo hasta un máximo de 19.579 dólares

en 17 de diciembre de 2017, volviendo a caer al nivel de 15

mil dólares poco antes del final de aquel año. Son variaciones

bastante acentuadas en el precio, mucho mayores que las

variaciones medias de otros activos financieros.

El mercado de criptomonedas está lejos de una

situación de madurez. En el sector financiero, sólo pequeña

parte pequeña de los profesionales entiende el concepto de

criptomonedas, por tratarse mucho más de una invención de

tecnología de información que de

finanzas. Después del gran

aumento de precio del bitcoin en 2013, cientos de

criptomonedas

surgieron.

En

2017,

el

sitio

coinmarketcap.com, uno de los mayores sobre cotización de

criptomonedas del mundo, listó más de 1.300 de ellas, la gran

mayoría formada después de 2013.

Entre 2013 y 2017 hubo drástico aumento en el

número de criptomonedas y valores negociados a través de

ellas. Es difícil decir, sin embargo, cuáles se mantendrá en los

próximos años y caules desaparecerán. Ciertamente muchas

dejarán de existir, principalmente debido a la falta de

liquidez. El bitcoin debe seguir siendo referencia durante los

próximos años, por haber sido la primera y por varias otras la

utilizan como referencia. Otras criptomonedas importantes,

como Ethereum, Ripple y Litecoin también deben ser

duraderas.

Ethereum

Si has llegado hasta aquí, ¡felicitaciones! Prepárese ahora

para dar un paso adelante en el entendimiento de los impactos

de estas nuevas tecnologías. Para entender el Ethereum es

importante tener un buen fundamento en cómo funciona el

blockchain. Creada en 2014 por Vitalik Buterin y otros

miembros de la comunidad de

desarrolladores de Bitcoin,

esta tecnología podría ser considerada como Bitcoin 2.0, o

incluso una criptomoneda de segunda generación.

Imagine un blockchain que no registra sólo los saldos

BTC, pero que da la opción de crear otras monedas también.

Ahora piense no sólo en las monedas. Piense que usted podría

registrar cualquier cosa que quisiera. La única cosa que usted

necesita hacer sería inventar un código para registrar tal cosa.

Es lo que el Ethereum intenta conseguir.

Lo que el Ethereum en esencia permite es que

cualquiera pueda escribir un pedazo de código y distribuirlo

en el blockchain. La gente pasa a interactuar con el código, y

éste responde automáticamente de acuerdo con lo que debe

hacerse. Estos pedazos de códigos se llaman *smart contracts*,

o contratos auto-ejecutables. Conceptualmente, lo que esta

blockchain permite es distribuir código en la red para crear

una supercomputadora mundial integrada por blockchain.

Esto es posible debido a la facilidad de transmisión y

ejecución de códigos creados por los usuarios.

El blockchain del Ethereum, que tiene como moneda

nativa el Ether (ETH), es mucho más

flexible que el

blockchain del BTC. Fué hecho para los

desarrolladores,

siendo mucho más programable. El sistema posee un lenguaje

de programación propio llamado Solidity y cualquiera que

entienda cómo programar algo puede escribir un código

creando un tipo de moneda o contrato y registrarlos en el

blockchain. Estas monedas o contratos creados se llaman más

apropiadamente de tokens, pues no necesariamente todos los

tokens creados son monedas. Tokens generalmente

representan algún derecho que puede ser transferido o

consumido. A partir de ahí, las personas pueden transferir

esos tokens apoyándose en la infraestructura de blockchain

del Ethereum.

Un ejemplo trivial para entender mejor lo que el

Ethereum propone es imaginar una rifa. Un desarrollador

puede crear un código que recibirá pagos y a cambio dará una

cuota de la rifa a la persona que pagó. Por último, en una

determinada fecha, el programa calcula automáticamente el

sorteado. Todo esto ocurre automáticamente de forma

distribuida a través de blockchain. El procesamiento de la rifa

está distribuido y no se encuentra en un único servidor

central. Una vez agotadas todas las rifas,

el contrato puede

generar un número aleatorio, decidir el ganador y pagarlo

inmediatamente, todo de forma automática. Una vez

terminada la rifa, el contrato puede ser reaprovechado para

otras rifas o destruido.

El Ethereum también utiliza un concepto de

combustible para procesamiento, el GAS. Cuanto mayor sea

el costo del procesamiento, más GAS se gasta, y el precio del

GAS varía con la demanda de procesamiento de los usuarios.

El precio del GAS se mide y se paga en ETH. De esta forma,

se debe tener ETH para poder distribuir su código de forma

efectiva. Por lo tanto, cuanto más aplicaciones existan para el

Ethereum, más demanda por moneda es generada, y más esta

tiende a valorarse.

Esta facilidad de programación de blockchain ha

permitido crear una nueva modalidad de captación de fondos,

los ICO. Pero el hecho es que se pueden desarrollar

aplicaciones mucho más complejas en blockchain. El

potencial del sistema sólo está empezando a ser explorado.

¿Qué es el ETH Classic?

En mayo de 2016, un fondo de venture capital

llamado The DAO levantó en un ICO 168 millones de

dólares para lanzar un fondo de inversión con

decisiones de inversión automatizadas basadas en los

votos de los tenedores de los tokens en blockchain. En

el código de DAO existían vulnerabilidades que fueron

explotadas por hackers, que acabaron por robar 3,6

millones de ETH, que en la época

equivalían a 50

millones de dólares. Asi, la comunidad decidió hacer un

hardfork para revertir los fondos a los poseedores

originales. Una minoría de la comunidad no quiso seguir

esta decisión, y decidieron continuar con el blockchain

original, o sea, con el blockchain en que sucedió el robo.

A pesar de ser el blockchain original, como era una

minoría, ésta acabó siendo obligada a cambiar el

nombre de la moneda a otra cosa que no ETH. De esta

forma, el ETH continuó en el blockchain sin el robo, y el

ETH Classic sigue en el blockchain con el robo. El precio

del ETH classic es sólo una fracción del ETH, pero

todavía recibe soporte de sus miembros.

Initial Coin Offering - ICO

El Ethereum permitió una nueva forma de captación de

recursos, el *Initial Coin Offering*, o ICO. De esta forma,

existen varias monedas siendo emitidas en la plataforma del

Ethereum.

ICO fue un nombre hecho de forma análoga a los

tradicionales IPO (initial public offering). IPOs son ofertas

primarias en el mercado de valores. Cuando una empresa

quiere captar recursos de inversores en la bolsa, pasa por un

proceso de apertura de capital, que es cuando el gran público

inversor puede comprar por primera vez acciones de esa

empresa. Este dinero está destinado a la expansión del

negocio o a la compra de participación en la empresa de

algún gran accionista.

El ICO, a pesar del nombre, se acerca más al

crowdfunding, que generalmente es cuando proyectos que

inicialmente no son suficientemente grandes para atraer la

atención de instituciones buscan financiamiento en los

pequeños inversores. El *crowdfunding* sería un similar de

tomar dinero prestado con amigos y parientes para comenzar

un negocio. La diferencia es que la Internet permite a estos

emprendedores captar dinero de

desconocidos, debido a la

facilidad de comunicación y transacción. El blockchain lleva

esta facilidad a un nivel arriba.

Los ICOs, entonces, permiten al pequeño inversor

participar en proyectos que a menudo son restringidos y

dominados por empresas de Private Equity que invierten el

llamado Venture Capital. Estas empresas normalmente tienen

mucho dinero y conexiones en la industria. Una empresa de

Private Equity normalmente es quien gana mucho dinero en

el IPO, pues es cuando la empresa es vendida para el público

en general. El Private Equity, habiendo invertido al comienzo

del proyecto, paga muy barato por su participación y vende

por un precio decenas de veces mayor después. Venture

Capital es un negocio de alto riesgo, ya

que la mayoría de las

empresas pueden fallar antes de ser vendidas. Pero el

beneficio

de

los

proyectos

lucrativos

generalmente

compensan a los que fallan. Estas empresas ya tienen mucha

experiencia en saber qué negocios tienen mayor potencial, y

algunas veces interfieren en la administración de la empresa

comprada.

Para explicar este concepto, vamos a contextualizar

con la historia de la moneda Ethereum (Código ETH).

Cuando esa moneda fue creada, rápidamente la gente percibió

que podían crear sus propias monedas en el blockchain del

Ethereum. Desde entonces muchas personas pasaron a emitir

criptomonedas, los llamados tokens y pueden, teóricamente,

representar cualquier cosa del mundo real. Contratos,

inmuebles, acciones, cuotas, derechos, activos, pasivos,

propiedad, etc. La aplicación más obvia sería crear e intentar

vender los tokens creados. ¿Por qué alguien pagar por un

token creado en el blockchain del

Ethereum, si ya tenemos el

ETH? Porque en realidad estos tokens representan algo de

interés para el inversionista.

Lo que sucede de hecho en la mayoría de los casos es

que estas personas no están haciendo nada más que crear

cuotas de participación en emprendimientos, algo que ya

existe desde la edad media, como en la Compañía de las

Indias Occidentales. La diferencia es que los buenos

emprendimientos lanzados en el blockchain generalmente

están ligados con la propia tecnología de blockchain. Los

buenos ICOs son negocios relacionados con la expansión del

blockchain para integrarlo con el mundo real. Empresas que

han identificado la solución de problemas a través de

blockchain y lanzan un ICO pueden tener

éxito.

Por otro lado, si el negocio no tiene nada que ver con

blockchain, debería recaudar fondos de otra manera, como

IPOs, Venture Capital, o plataformas tradicionales de

crowdfunding. Cabe al participante del ICO juzgar donde el

negocio encaja y lo que ofrecen los tokens.

Los tokens normalmente se venden por ETH. El ETH

a su vez se adquiere a través de BTC, que se adquiere por

moneda fiduciaria. Ese fue el camino al principio. Hoy la

infraestructura ya está tan desarrollada que es posible

comprar los tokens directamente por tarjeta de crédito,

aunque no sea la forma ideal. Con el ETH siendo una de las

principales monedas, ya es posible cambiar moneda fiduciaria

directa por ETH.

Una vez que las personas que crearon los tokens

recaudan ETH, normalmente venden estos ETH en el

mercado para adquirir moneda fiduciaria, y así poder realizar

algún emprendimiento. En el futuro, si el ETH está bien

integrado en la sociedad, no será necesaria la venta de ETH

para comprar papel moneda y así pagar por insumos para

realizar el emprendimiento. El propio

vendedor del insumo

aceptará ETH.

ICOs ya mueven más dinero que el mercado

tradicional de Venture Capital. Lo que el ICO está haciendo

actualmente es democratizando este mercado, que ya no está

sólo en manos de algunos privilegiados con dinero. A pesar

de esta democratización, ningún inversor al por menor que

debe comenzar a invertir en ICO. Normalmente el

inversionista medio no tiene tiempo ni el conocimiento para

saber qué proyectos son fraudes, qué riesgos y recompensas,

etc. Lo que el ICO hace es devolver el poder al individuo, de

participar en un mercado de donde antes era excluido. Sin

embargo, este poder no necesariamente será bien utilizado

por todos.

Otra diferencia muy importante entre ICOs e IPOs es

que en el IPO un inversionista está comprando una

participación en la empresa, siendo dueño efectivamente de

una fracción de la compañía. En los ICO, los dueños de la

empresa no venden propiedad sobre la empresa, sino otros

tipos de participación. Algunas empresas emiten los tokens

como si fueran cupones, que se

convierten en la única forma

de comprar el producto que se está ofreciendo. Muchas veces

la empresa crea tokens sin un propósito, simplemente para

recaudar fondos. De esta forma, el modelo de negocio y la

utilidad de los tokens no quedan claros, y los inversores

deben pasar lejos de este tipo de ICO.

Otros ICO emiten tokens que representan participación

en las operaciones de la empresa, pagando incluso

dividendos. Desde el punto de vista económico, este tipo de

token es equivalente a una acción, pero desde el punto de

vista jurídico, el inversionista no es dueño de la empresa, lo

que significa que no puede participar en su proceso decisorio,

recordando mucho la llamada acción preferencial , que es una

acción que tiene preferencia en la

recepción de los

dividendos, pero no tiene participación en el control de la

compañía.

Otra diferencia obvia, pero importante, es que las

acciones preferenciales se registran en una autoridad central

custodiante. El token se registra en blockchain, lo que es una

ventaja, ya que es un registro público fácilmente accesible,

hecho a un costo mucho menor, velocidad mucho mayor, y

sin necesidad de confiar en una autoridad central.

El problema de los ICO es que este es un mercado

totalmente desregulado y, por lo tanto, no ofrece protección a

los inversores. Si una empresa captar su dinero por ICO y

desaparice del mapa, no hay casi nada que pueda hacer

legalmente. La tendencia de las

autoridades será una de dos:

o la prohibición de este tipo de captación, como hizo China, o

la regulación del mercado. La SEC (Securities Exchange

Comission), órgano regulador de valores y valores

mobiliarios en Estados Unidos, ya se ha manifestado diciendo

que los tokens que pagan dividendos y se comportan como

títulos de valores están bajo la misma reglamentación de

títulos tradicionales. La CVM (Comisión de Valores

Mobiliarios), órgano regulador en Brasil, siguió la misma

línea. A pesar de estas manifestaciones, aún no está claro

cómo estos organismos reguladores pueden ofrecer la

protección necesaria para los inversores.

Bitcoin Cash

Bitcoin Cash (BCH, o BCC en algunos lugares) vino

directamente de la esencia de Bitcoin. En otras palabras, una

parte de la comunidad que antes era activa en el proyecto

Bitcoin se separó por divergencias en cómo llevar el proyecto

adelante. No fue un proyecto original, sino simplemente una

grieta en la comunidad. De esta forma,

hubo un debate para

ver quién se quedaría con la marca Bitcoin y, naturalmente, el

blockchain con la mayoría de la infraestructura permaneció

con la marca original.

El debate que llevó a la racha giraba alrededor del

tamaño del bloque. El grupo que defendia el aumento para

procesar más transacciones, reducir tiempos de confirmación

y tasas de transacción decidio salir del Bitcoin. La otra parte

de la comunidad preferió continuar con el tamaño del bloque

en 1 MB, alegando cuestiones de seguridad y concentración

de poder. Fue esta parte de la comunidad que permaneció con

el nombre Bitcoin y el código BTC.

La comunidad disidente entonces aumentó el bloque a

8 MB, haciendo el hardfork en agosto de 2017 creando

Bitcoin Cash. El nombre tiene la intención de dar la idea de

que la nueva moneda podría ser usada como si fuera dinero

digital de forma eficiente, a diferencia de Bitcoin, que estaba,

y todavía está, sufriendo con altas tasas de transacción en la

red, y es utilizada más como reserva de valor que para

transacciones. El BCH también cambió el algoritmo de ajuste

de dificultad de minería para responder

a variaciones de

procesamiento en la red con más suavidad.

Naturalmente, existe una gran rivalidad entre las dos

comunidades, por ser originalmente la misma y por

desarrollar proyectos muy semejantes. Es fácil confundir las

dos monedas, pues el logo es muy parecido:


Bitcoin Cash

En el comienzo del fork, muchas personas veían con

escepticismo el nuevo proyecto, pero éste se probó exitoso, y

el precio del BCH representa una fracción cada vez mayor del

precio del BTC. Es difícil decir si esta tendencia va a

continuar. Una cuestión interesante es: si el BCH gana más

valor de mercado que el BTC (el llamado *flippening*), el BTC

sigue siendo BTC? ¿O el BCH sería el nuevo BTC en el

caso? ¿Cómo se define lo que es el

BTC? ¿Sería el protocolo

con mayor valor de mercado?

Cuestiones complejas, pues nadie tiene la patente

sobre la marca. La cuestión de qué comunidad seguiría con la

marca BTC fue resuelta de forma pacífica en este caso, pero

nada impide que ex miembros de la comunidad resentidos

lanzen otra moneda con exactamente el mismo nombre,

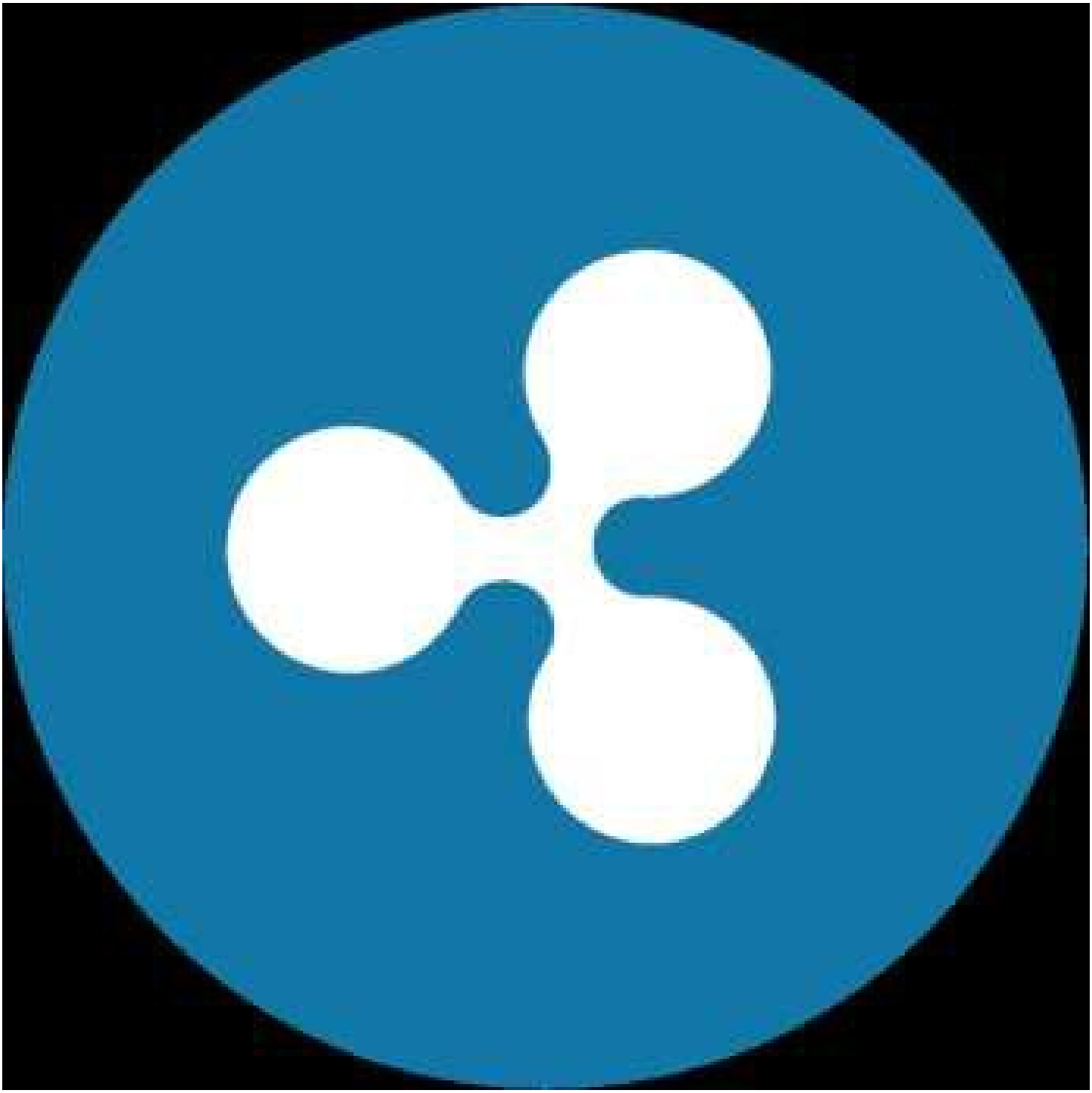
confundiendo a los participantes del mercado, o aún, si con el

flippening, la comunidad BCH se sienta en el derecho de

apropiarse de la marca BTC. Naturalmente, si esto ocurre, la

comunidad BTC no lo aceptará de buen grado.

Ripple



Ripple es un sistema de transacción y liquidación, que

utiliza como moneda nativa una moneda con el mismo

nombre (código: XRP). Ripple es un sistema controvertido,

por tener una empresa detrás (Ripple Labs), y por ser pro-

bancos. Muchas de las filosofías anti-corporativas en el

mundo de las criptomonedas no se siguen en el Ripple. Por el

contrario, él busca alianzas

institucionales.

La propuesta de Ripple Labs es proporcionar a las

instituciones financieras y usuarios de la persona física una

nueva plataforma de transacción, ofreciendo así a los bancos

e individuos una puerta de entrada en la tecnología de

blockchain. Los bancos actualmente utilizan un sistema de

mensajería llamado SWIFT para realizar transacciones

internacionales. Una de las funciones del Ripple sería

reemplazar este sistema.

Otra distinción importante del sistema Ripple en

relación a los demás es que es inspirado en el Hawala, un

sistema informal de transacción utilizado antiguamente en el

oriente medio. El sistema Hawala depende de una gran red de

corredores que tienen conexiones entre sí.

De esta forma, si el usuario A quiere enviar, por

ejemplo, oro para usuario B, A utiliza el corredor X. El

corredor X a su vez tiene una relación con el corredor Y. El

corredor Y tiene B como cliente. De esta forma, A deposita

su oro en X, y B saca el oro en Y. Entonces, X crea una

deuda en oro para Y, pero como estos tienen una relación de

confianza, Y acepta la deuda de X. En

una transacción

inversa de B para A, X podría quitar su deuda con Y, o

también podría simplemente transferir el oro a Y

posteriormente si no había una transacción inversa.

Obviamente, este tipo de sistema sólo funciona para bienes

que sean idénticos, como commodities y monedas, de lo

contrario el producto que un usuario saca sería diferente del

producto depositado.

Utilizando la lógica de este sistema, y sustituyendo a

los corredores por llamados, el Ripple posibilita transacción

de prácticamente cualquier cosa en su blockchain, incluso el

oro del ejemplo. En el caso de oro, existen alianzas con

fundidoras que aceptan cambiar oro por certificados de

depósito, que dan derecho de saque, negociados en la

blockchain. Si un usuario deposita oro en la casa de

fundición, la casa emite un certificado en blockchain en

nombre del usuario y éste puede negociar el certificado por

ordenador. Quien comprar el certificado puede retirar el oro

en alguna casa ligada en el blockchain. Estas casas de

fundición serían puertas de oro en el vocabulario Ripple.

Es posible negociar Bitcoins en el

blockchain del

Ripple también. Un usuario puede simplemente depositar

BTC en su cuenta Ripple a través de una puerta de enlace y

negociar un certificado de depósito de BTC en el blockchain

del Ripple. Sólo cuando alguien quiere "sacar" el BTC,

sucedería una transacción en el blockchain nativo del BTC.

En otras palabras, Ripple es compatible con cualquier

cosa para la que se quiera emitir un certificado de depósito.

En el caso del BTC, la compatibilidad existe porque las

propias puertas de acceso del sistema Ripple tienen

direcciones de BTC. En el Blockchain nativo del BTC sólo

ocurren dos transacciones: el depósito de BTC en una

dirección de puerta de enlace Ripple y el saque de alguna otra

dirección BTC cuyo dueño es otra

puerta de acceso Ripple. A

partir del depósito, las puertas de enlace realizan las

transacciones de certificados BTC entre sí en el blockchain

del Ripple, sin mover el BTC en su blockchain nativo.

Note una cosa importante tanto en el caso del oro

como BTC. Lo que se transmite en el blockchain de Ripple

son certificados de depósitos, y no el activo en sí. Es decir,

existe el riesgo de contraparte en el sistema Ripple. Riesgo de

contraparte es aquel en que existe la posibilidad de la persona

con la que se ha transado no cumplir el acuerdo. Los

certificados de depósitos son equivalentes a los títulos de

deuda, los famosos I.O.U. (Una sigla para I owe You, o "Yo

debo a ti", en traducción libre). Por lo tanto, lo que se negocia

en el blockchain del Ripple es deuda, y

no el Activo en sí. La

deuda se crea con la recepción de un depósito por la puerta de

enlace, y sólo se presenta cuando se saca.

Entonces, en este caso, se debe tener confianza en el

emisor del certificado, la puerta de enlace. Por este motivo, el

sistema Ripple también es criticado por miembros más

radicales de la comunidad, pues esencialmente se deja de

tener la propiedad del activo de hecho hasta un eventual

saque. Por eso también se dice que la moneda Ripple es la

moneda nativa del sistema, pues es la única que se puede

tener propiedad de hecho dentro del ambiente, sin depender

de una puerta de enlace. De esta forma, la XRP sirve también

como "puente" para la conversión de dos activos no nativos

del sistema. Obviamente no se puede

sacar o depositar XRP,

pues ella sólo existe dentro de su ambiente virtual, así como

otras criptomonedas. Su utilidad, y por lo tanto su valor,

depende de cuán crezca su ambiente.

Técnicamente, el ambiente que fue desarrollado por el

protocolo permite recrear todo el sistema de crédito bancario

dentro de su blockchain. Recuerde que los bancos

comenzaron como casas físicas de depósito de oro, en las

cuales los dueños percibieron que podían emitir más

certificados que la cantidad de oro en custodia, debido al

hecho de que era muy difícil que todos los depositantes

sacasen el oro al mismo tiempo.

Esto se denomina *fractional reserve banking*, y

significa que los bancos necesitan mantener reservas reales de

sólo una fracción de sus préstamos. Esto permite el famoso

apalancamiento de los bancos. Muchas instituciones

financieras operan hoy con 10X de apalancamiento, lo que

significa que para cada 10 que el banco presta, éste sólo

mantiene 1 en caja. Pero cuando ocurre un pánico, todos

quitan el dinero de los bancos al mismo tiempo. El alto

apalancamiento aumenta el riesgo de

quebrar el sistema

financiero, así como ocurrió en 2008 y tantas otras veces.

Esta retirada en masa es prácticamente el único evento

que puede romper un banco. Por ese peligro, nos

preguntamos si un sistema de creación de moneda a través de

crédito será desarrollado en el blockchain del Ripple. A pesar

del peligro, si la historia es una guía, la respuesta es sí, es

sólo una cuestión de tiempo. Y si esto ocurre, entonces

efectivamente será posible la creación de BTC, o mejor

certificados de BTC, que en la práctica no existen.

La pregunta es si los usuarios de criptomonedas

aceptarán utilizar este tipo de crédito, ya que parte de la

filosofía de la nueva tecnología es justamente evitar ciclos

violentos de contracción de crédito, y

usar BTC como reserva

de valor. Todas estas posibilidades de un nuevo sistema de

crédito en blockchain, sin embargo, muestran el potencial del

sistema Ripple.

El Ripple también tiene el potencial de disminuir

mucho costos con remesas de moneda extranjera, debido a la

posibilidad de negociar certificados de otros activos, como

USD (Dólar americano), EUR (Euro), JPY (Yen japonés), etc

en un sistema más amigable para monedas fiduciarias, a

diferencia de otros sistemas de criptomonedas.

Los bancos ya usan un sistema parecido al Hawala en

el mundo digital, no transfiriendo el dinero de hecho durante

el día de un banco a otro. Como las transacciones son muchas

y en ambas direcciones, gran parte de la

deuda se compensa

naturalmente. Las diferencias en el saldo se cierran al final

del día en el mercado de *Money Market*. El Ripple elevaría la

eficiencia de este sistema a niveles dignos del siglo XXI.

Las transacciones en el Ripple son extremadamente

rápidas, haciendo la transferencia de valor en 3 a 5 segundos.

A diferencia de otras monedas, la XRP no es minera. Esto

quiere decir que todo el suministro de monedas ya existe y no

habrá nuevas emisiones. Los bloques son validados por

consenso, es decir, cuando una mayoría absoluta llega en la

misma versión de blockchain. Como XRP no es minero, el

sistema cuenta con validadores clave que tienen interés en

mantener el sistema estable y funcionando. Si el sistema se

utiliza para transferencias

interbancarias, los propios bancos

mantendrán voluntariamente nódulos de validación activos

sin mucho costo, pues en este caso no es necesario gastar

grandes cantidades de energía eléctrica con cálculos

matemáticos.

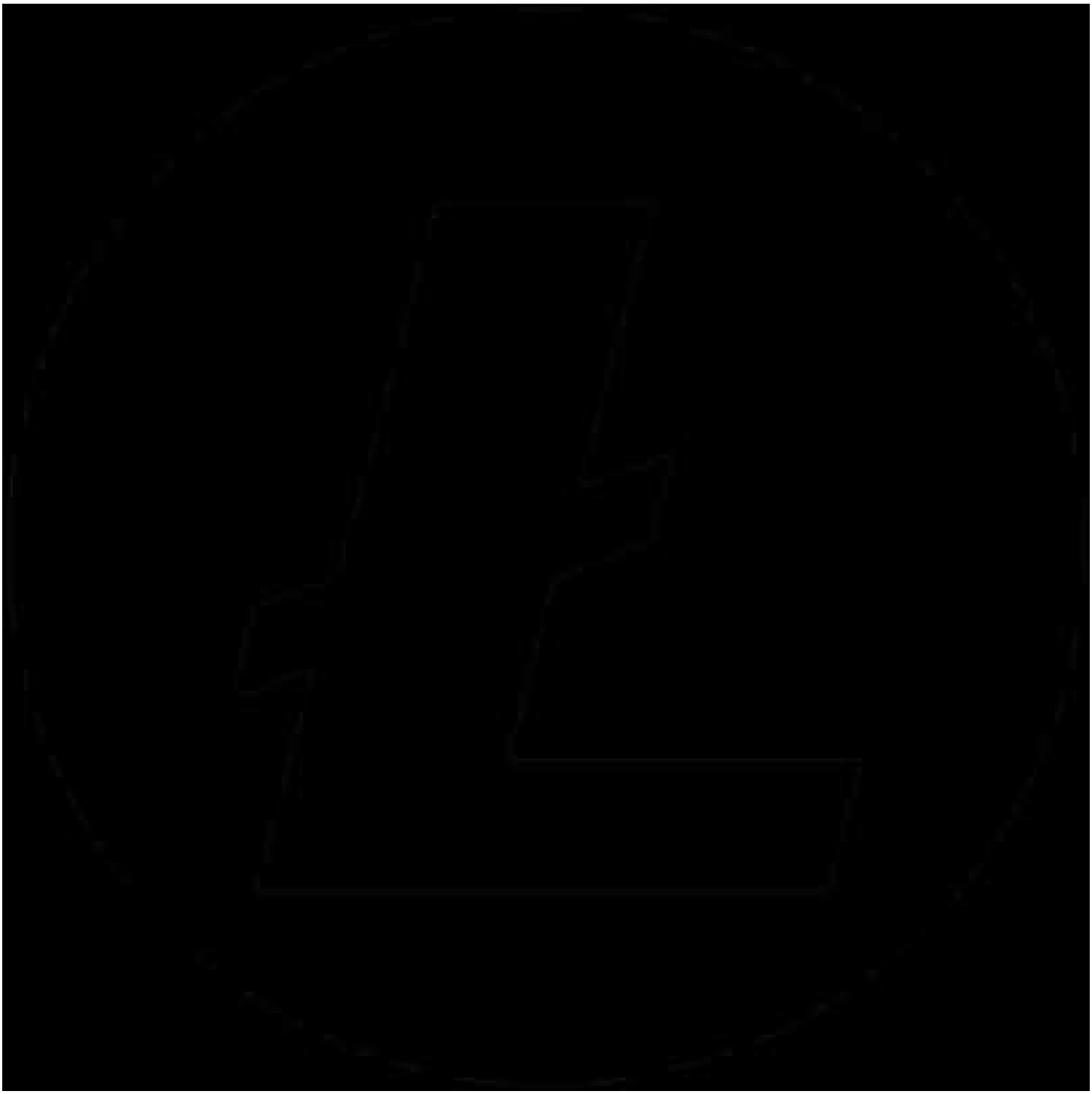
El volumen total de XRP es de 100 mil millones, y

gran parte de esta moneda está en manos de la empresa

Ripple Labs, empresa detrás de la moneda. El modelo de

negocio de la empresa es dar soporte a la plataforma de modo

que la moneda suba de valor, y la empresa gana dinero con el



tiempo vendiendo la moneda en mercado. Eso también

desconcentra la posesión de la moneda.

Los bancos ya manifestaron interés en el sistema, pero

no quieren la nueva moneda XRP, pues en principio no ganan

con eso. La Ripple Labs, por su parte, dice que la XRP es

parte integral del sistema y éste no existe sin la moneda. De

esta forma, si los bancos soportan los nódulos validadores,

automáticamente estarán soportando el precio de la moneda

también, a pesar de no tener interés directo en el activo, al

menos en el momento.

Los inversores en XRP, en último caso, deben contar

con la adopción del sistema por los bancos y confiar en las

buenas intenciones de Ripple Labs, incluso en la intención de

no emitir más monedas en el mercado. A pesar de eso, el

protocolo Ripple puede sobrevivir incluso sin la empresa por

tratarse de código abierto y la Ripple Labs se está esforzando

para ser transparente.

Litecoin

El Litecoin (LTC) es una moneda de primera

generación, creada en octubre de 2011 por un ex funcionario

del google, Charlie Lee. El Litecoin es un clon de Bitcoin,

con algunos cambios técnicos, de los cuales las principales

son el aumento en la velocidad (2.500 en vez de 10 minutos),

aumento en la cantidad de emisión de

moneda (84 millones

LTC X 21 millones BTC), y cambio en el algoritmo de

minería, impidiendo el desarrollo de ASICs para la minería,

siendo de esta forma minerada por GPU.

Dash

Dash (código de moneda: DASH) significa Digital

Cash, y es una moneda que busca mejorar ciertos aspectos del

sistema de criptomonedas. Dash aprovechó la base de código

de LiteCoin (que a su vez aprovechó la base de Bitcoin), y

agregó en su código la integración de la comunidad con el

sistema. Lo que esto significa en la

práctica es que usuarios,

desarrolladores y mineros logran tomar decisiones sobre el el

sistema votando dentro del propio sistema. Eso trae más

cohesión, organización y eficiencia en la toma de decisiones

sobre cambios en el protocolo, lo que evita posibles hardforks

y mantiene la comunidad fuerte y unida. También ofrece

opciones de privacidad más avanzadas que Bitcoin, y da al

usuario la opción de elegir si desea que su transacción sea

rastreable o no.

Dash también consigue un modelo más claro de cómo

remunera a sus desarrolladores a través de votos por

consenso, evitando así la influencia de empresas terceras en

el desarrollo del sistema. En el caso de Bitcoin, por ejemplo,

existen empresas como BlockStream que acaban por influir

en las decisiones de la comunidad por remunerar a los

desarrolladores de Bitcoin. Dash intenta traer de vuelta el

poder a las manos de la comunidad a

través de la

organización por blockchain.

Una moneda que tiene un claro plan de desarrollo y

consigue tener una base para innovar mejor tiene una gran

ventaja competitiva. Se puede decir que lo que el sistema

Dash pretende alcanzar es convertirse en una organización

digital

autónoma,

o

DAO

(Digital

Autonomous

Organization). Una sociedad que una vez computados los

votos

de

los

participantes

ejecuta

las

decisiones

automáticamente.

Monero

El Monero (XMR) es una moneda cuya principal

característica es la preocupación con la privacidad. Su

blockchain, a pesar de pública, no ofrece informaciones

concretas de qué direcciones hicieron qué transacciones.

Usando el concepto de *ring signatures*, es decir, firmas en

conjunto, la moneda puede ser completamente anónima en

sus transacciones. El concepto de firmas en conjunto hace

que la firma del usuario sea mezclada con la de otros usuarios

en el sistema, imposibilitando destacar uno del otro.

Debido al hecho de ser completamente

anónima, esta

moneda es actualmente aceptada, así como bitcoin, en el

mercado negro de Internet. Cuestiones morales y éticas

aparte, el hecho de que la moneda sea aceptada en este medio

muestra que tiene éxito en su propuesta de proteger la

identidad del usuario. Pero eso no significa que el uso de la

moneda sea restringido al mercado negro.

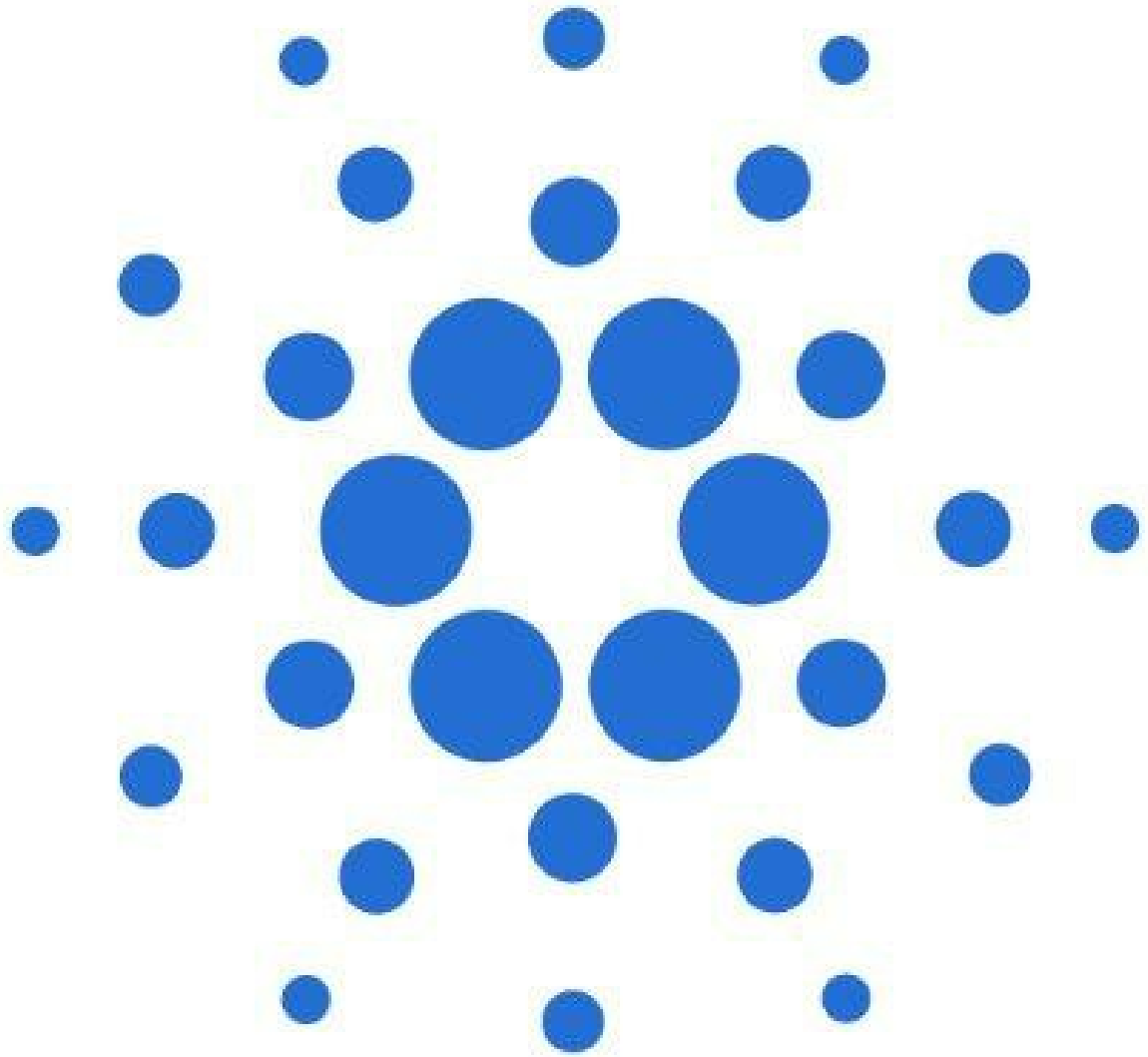
Cardano

Cardano es un sistema más nuevo. Su moneda nativa

se llama ADA. Esta podría ser llamada de moneda de tercera

generación. El foco del Cardano es, al igual que el Ethereum,

tener un blockchain programable. La novedad en Cardano es



que el sistema hace la separación de capas, o funciones. El

blockchain en el Ethereum almacena datos y metadatos (datos

sobre datos) de forma conjunta, y por lo tanto la blockchain

acaba quedando cargada de informaciones que podrían estar

mejor organizadas y no necesitan ser consultadas cada vez

que se quiere ver un dato específico en el blockchain . Sin la

optimización de la asignación de los datos, la eficiencia

máxima no se alcanza entonces, y se

vuelve difícil de

aumentar la escala de la blockchain.

Cardano hace esta optimización, y permite mayor

agilidad y flexibilidad en el blockchain, lo que hace el

sistema más fácil de ser personalizado específicamente para

ciertos nichos de mercado, como el de apuestas, por ejemplo.

En este nicho se podría con el Cardano automatizar más

partes del sistema y hacerlo más eficiente, de modo que

disminuiría los costos para la casa de apuestas, agilizar la

interacción del sitio con los usuarios, y permitiría a los

gobiernos aplicar sus regulaciones, incluyendo la recogida de

impuestos, de forma automatizada, sin necesidad de

interferencia humana.

Cardano también lo usa el PoS (Proof of Stake) como

forma de validación, que es un sistema que el Ethereum tiene

la intención de adoptar en el futuro.

Es tentador hablar que el Cardano, por ser más joven

que el Ethereum, será fatalmente la mejor plataforma. Pero la

realidad es que Ethereum ya tiene una base de usuarios,

desarrolladores,

mineros

y

intercambios,

o

sea

infraestructura, mucho mayor, a pesar de tener un código más

antiguo. La comunidad de Ethereum sabe que el código debe

ser actualizado y trabaja para eso. La ventaja de Cardano es

que la base de código ya viene más optimizada, pero tienen el

desafío de conquistar el público.

Además del Cardano,

existen otras blockchains programables que compiten con el

Ethereum, como el NEO, EOS y WAVES.

Una Nueva Clase De Activo

Cuando se habla en el estado del mercado de criptomonedas,

es necesario reflejar que estamos hablando de una nueva

clase de activo. Este es un acontecimiento poco frecuente en

la historia de los mercados financieros, por decir lo menos.

Como contraste, podemos pensar en los bancos, que se

quedan creando productos deslumbrante y caros para sus

clientes. Hay miles de empleados trabajando en bancos que

actúan en un área llamada genericamente de "ingeniería

financiera", responsable por los llamados productos

estructurados. Estos productos generalmente no son más que

la combinación de dos o más instrumentos financieros

diferentes en un solo producto. Estos

productos forman parte

de la categoría derivados, es decir, productos cuyo precio

deriva de algun otro activo, no representan un producto en si.

Las criptomonedas, a su vez, son productos

completamente nuevos y sin relación con otro instrumento

financiero ya existente. Esto quiere decir que su correlación

con otras clases de activos es muy baja. Sólo por eso ya

tienen valor, pues ofrecen diversificación en la cartera de los

inversores. Cuando el precio de acciones o inmuebles están

cayendo, puede ser que las criptomonedas estén estables o

subiendo.

Como estamos hablando de una nueva clase de activos

con sólo 8 años de existência, y que probablemente no dejará

de existir, es de buen sentido hablar que el mercado de

criptomonedas aún no ha llegado a su madurez. Puede ser que

eso lleve algunas décadas. Esto sólo tiene en cuenta el prisma

de la inversión. Si tomamos en consideración los cambios en

el comercio global, queda claro que todo sigue siendo muy

incipiente.

Masa Crítica de Adopción

¿Cómo está la adopción de los Bitcoins por comerciantes?

Antes de enumerar algunas grandes empresas que aceptan la

moneda, hablemos un poco de inflación. ¿Qué tiene que ver

la inflación con la adopción de Bitcoin? Todo economista

sabe lo que es inercia inflacionaria. En un proceso

inflacionario fuerte, los precios suben, y las personas

entonces esperan que los precios continúen subiendo. Debido

a esta expectativa, los comerciantes

elevan el precio de sus

productos para no perder para la inflación. Cuando la

elevación de precios ocurre, la inflación que todos estaban

esperando se confirma. Esto también se llama profecía auto-

realizable.

De la misma forma, es necesario que el precio de la

bitcoin suba para ganar la atención de los medios de

comunicación y comerciantes. La especulación en bitcoin, tan

criticada por algunos, es esencial para hacer la profecía auto-

realizable. Si nadie estuviera mirando a Bitcoin, el sistema no

estaría siendo pensado para su uso. El mercado está

imponiendo el cambio a los comerciantes renuentes. Las

personas adoptan el sistema porque esperan que más personas

lo adopten, y eso hace que el precio

suba. Conforme el precio

sube, más gente adopta, y así el precio sube nuevamente. Es

un sistema inercial retroalimentable que está ganando masa

crítica suficiente para entrar en un camino sin vuelta. En

cierta forma, la sociedad está imponiendo sobre sí misma la

adopción del sistema.

¿Pero Quién Acepta Bitcoin Hoy?

Aquí tenemos una lista de algunas

grandes empresas que ya

aceptan bitcoin:

WordPress.com - Empresa en línea de herramientas para los

usuarios crearen sus propios sitios web.

Subway - Franquicia global de sándwiches. No son todas las

tiendas, pero en Buenos Aires (Argentina) ya lo aceptan.

Reddit - Foro de Internet. Se pueden comprar algunas

características premium con la moneda.

Wikipedia - Enciclopedia libre. Acepta donaciones en

bitcoin.

Wikileaks - Enciclopedia de documentos confidenciales.

Acepta donaciones en bitcoin.

Intuit - Empresa estadounidense de software financiero y

contable. Famosa por el sistema Quickbooks.

ExpressVPN.com - Empresa que ofrece servicios de VPN

(Virtual Private Network).

JmBullion.com - empresa americana que vende oro, plata y

otros metales preciosos.

Expedia.com - Página web de viajes.

Virgin Galactic - Empresa de turismo espacial.

Newegg.com - Empresa online al por menor de electrónica.

Microsoft - ¿Necesita explicar?

En el momento de publicación de este libro, hay rumores

sobre Amazon y Ebay aceptar la moneda. No se sabe si esto

sucederá de hecho, pero caso suceda, podemos esperar un día

de fuerte alza en los precios de las monedas.

¿Cómo Está La Regulación De Criptomonedas En El

Mundo?

En la mayoría de los países, las criptomonedas no

tienen ningún tipo de regulación específica y acaban siendo

tratadas como un commodity. Las autoridades monetarias de

varios países han emitido notas oficiales alertando sobre los

riesgos de las criptomonedas, pero pocos crearon

restricciones sobre ellas.

Son pocos y pequeños los países que restringen o

prohíben las criptomonedas. Entre ellos están Bolivia,

Ecuador, Marruecos, Kirguistán, Bangladesh y Nepal.

La Unión Europea no tiene regulación específica ni

restringe criptomonedas, pero el parlamento europeo

determinó la formación de una comisión para monitoreo de

monedas virtuales como forma de prevención a actividades

ilegales y terrorismo.

En los Estados Unidos y en América en general, las

criptomonedas se consideran un tipo de activo, que debe

pagar impuesto sobre la valorización. La mayoría de los

países latinoamericanos, incluyendo Brasil, Chile, Colombia

y Argentina, no tienen regulación específica para

criptomonedas.

Los países típicamente desarrolladores de tecnología

como Japón, Corea del Sur y Taiwán reconocen y facilitan el

uso de criptomonedas. En muchos de ellos es posible comprar

bitcoins en tiendas físicas y muchos establecimientos aceptan

monedas digitales como pago de transacciones normales.

China no prohíbe a las personas físicas comercializar

criptomonedas, pero prohíbe empresas y bancos. China es

uno de los países que más minan criptomonedas en el mundo.

Como regla general, se observa que los países

pequeños y desarrollados tienden a

reconocer y facilitar el

uso de criptomonedas. Los países grandes prefieren actuar

con cautela, no prohibiendo, pero no incentivando, y algunos

países pequeños y pobres consideran las criptomonedas una

amenaza e intentan restringirla.

Hasta el momento, lo que parece ser la gran

preocupación de los gobiernos es el uso de las criptomonedas

como forma de pago de crímenes, financiamiento al

terrorismo y tráfico de drogas. Algunos están preocupados

por la posibilidad de perder recaudación, pero esta

preocupación todavía no parece suficiente para que se creen

regulaciones específicas.

Capítulo V

¿Es posible Ganar Dinero Con Bitcoins?

"I really like Bitcoin. I own Bitcoins. It's a store of value, a

distributed ledger. It's a great place to put assets, especially

in places like Argentina with 40 percent inflation, where $1

today is worth 60 cents in a year, and a government's

currency does not hold value. It's also a good investment

vehicle if you have an appetite for risk. But it won't be a

currency until volatility slows down."

"Me gusta Bitcoin. Tengo bitcoins. Es una reserva de valor,

una tecnología compartida. Es una gran alternativa para

asignar activos, especialmente en lugares como Argentina

con un 40% de inflación, en que $ 1 hoy vale 60 centavos

después de un año y la moneda del gobierno no mantiene

valor. Es también una buena inversión para quienes tienen

apetito para el riesgo. Pero no será una

moneda mientras la

volatilidad no disminuya ".

David Marcus, CEO de Paypal

Cómo Empezar a Invertir

Ahora que ya entendemos cómo funcionan las monedas

digitales y la lógica detrás de ellas, podemos hablar de

aspectos prácticos. La pregunta más frecuente de las personas

que se interesan por el tema es: cómo comprar o vender

Bitcoins? Es importante recordar las palabras de Milton

Friedman. Bitcoin es el equivalente digital de una transacción

donde una persona da una nota de dinero a otra en la calle.

Usted no necesita saber quién es la persona, no hay otras

partes implicadas en el proceso, y todo esto se hace en un

lugar público.

En el mundo digital, si usted desea comprar bitcoin y

encontra a alguien que quiere vender la moneda, simplemente

pide a la persona para transferir a bitcoin. Lo que la persona

va a exigir a cambio puede depender. Ella puede querer 1

centavo, 1 millón de reales, una empanada de queso o un

masaje. Usted hace el masaje y ella le transfiere el activo

digital directamente en su dirección. Simples así.

¿Por qué entonces la gente utiliza bolsas

para comprar

o vender la criptomoneda? Hay varias razones. Lo principal

es que es difícil encontrar gente queriendo comprar o vender

aleatoriamente en Internet o en la calle. Las bolsas son

creadas para reunir compradores y vendedores, de esta forma

creando liquidez y estandarización en los precios. Existen

bolsas de acciones, futuros, productos agrícolas, metales

preciosos, monedas, opciones, y otros. Ahora también

tenemos criptomonedas.

Dicho esto, así como monedas tradicionales, nada te

impide transacción fuera de una bolsa. La ironía es que una

acción, que antes podía ser un pedazo de papel que pertenecía

a su portador (así como un billete de dinero) y podía ser

negociada libremente, hoy sólo puede ser negociada en bolsa.

Como las acciones de empresas, usted no detiene la custodia

de ellas. Las acciones se quedan en casas de custodia

especializadas. La única forma de negociación es electrónica.

Las grandes empresas utilizaron la tecnología como una

forma de restringir las opciones de los ciudadanos. Hoy

tenemos una tecnología que permite transacciones fuera de

plataformas centralizadas. Este es uno

de los innumerables

motivos que criptomonedas agradan a los libertarios.

La primera cosa que se debe hacer para empezar con

criptomonedas es tener una cartera. La cartera no es más que

un programa que sirve básicamente a dos funciones: la

primera es generar direcciones para poder recibir las

monedas. La segunda es firmar las transferencias para poder

enviar las monedas.

Las funciones de recibir y enviar están conectadas por

la dirección. La cartera sólo le deja recibir en direcciones

cuyas claves privadas están en su posesión. Por lo tanto, la

cartera genera un par de claves públicas / privadas. En el caso

de Bitcoin, por ejemplo, la dirección en la que recibe sus

monedas es un hash de la clave pública. Cuando se quiere

gastar las monedas, se usa la clave privada correspondiente a

esa dirección.

Existen las llamadas " *desktop wallets*", o " *hardware*

wallets", que son carteras en las que se baja un programa en

el propio ordenador, y también existen las " *online wallets*",

que son carteras que quedan en servidores. En la práctica,

estas carteras online no son más que sitios de Internet que

proporcionan la funcionalidad de las carteras. Hay también

las " *paper wallets*", que son claves criptográficas impresas en

un papel.

En el caso de las carteras online, existen algunos tipo

que no permiten al usuario tener posesión de sus claves

privadas. Los proveedores de carteras que no dejan al usuario

tener la clave privada esencialmente funcionan como bancos

en el sentido de que el usuario debe confiar su dinero a un

tercero. Si alguien tiene acceso a su clave privada, ese alguien

tiene la capacidad de gastar las criptomonedas en cualquier

momento. Por lo tanto, no es recomendable utilizar carteras

en las que el usuario no controla sus propias claves privadas.

Las carteras también sirven para acompañar el saldo de

moneda en las direcciones controladas

por esa cartera. Si un

usuario sólo desea seguir el saldo de su cartera, no es

necesario utilizar las claves privadas. Como el blockchain es

público y distribuido, es posible ver cuánto una dirección

tiene de saldo sólo consultandola. Como la función de

escanear el blockchain no necesita claves privadas, es posible

sólo usar una página que lee el código para saber el saldo de

aquella dirección.

Una analogía que se puede hacer es que la cartera es

como si fuera una cuenta bancaria. Es fácil confundir el

concepto de dirección con cartera, con muchas personas

pensando que una dirección corresponde a un número de

cuenta. Una cartera tiene varias direcciones, y por lo tanto

varias claves privadas. Estas claves y direcciones tienen una

relación matemática basada en una *seed*.

Una "seed" puede ser, por ejemplo, un conjunto de

palabras, agregadas seún un conjunto de claves relacionadas

matemáticamente.

Estas

direcciones

vinculadas

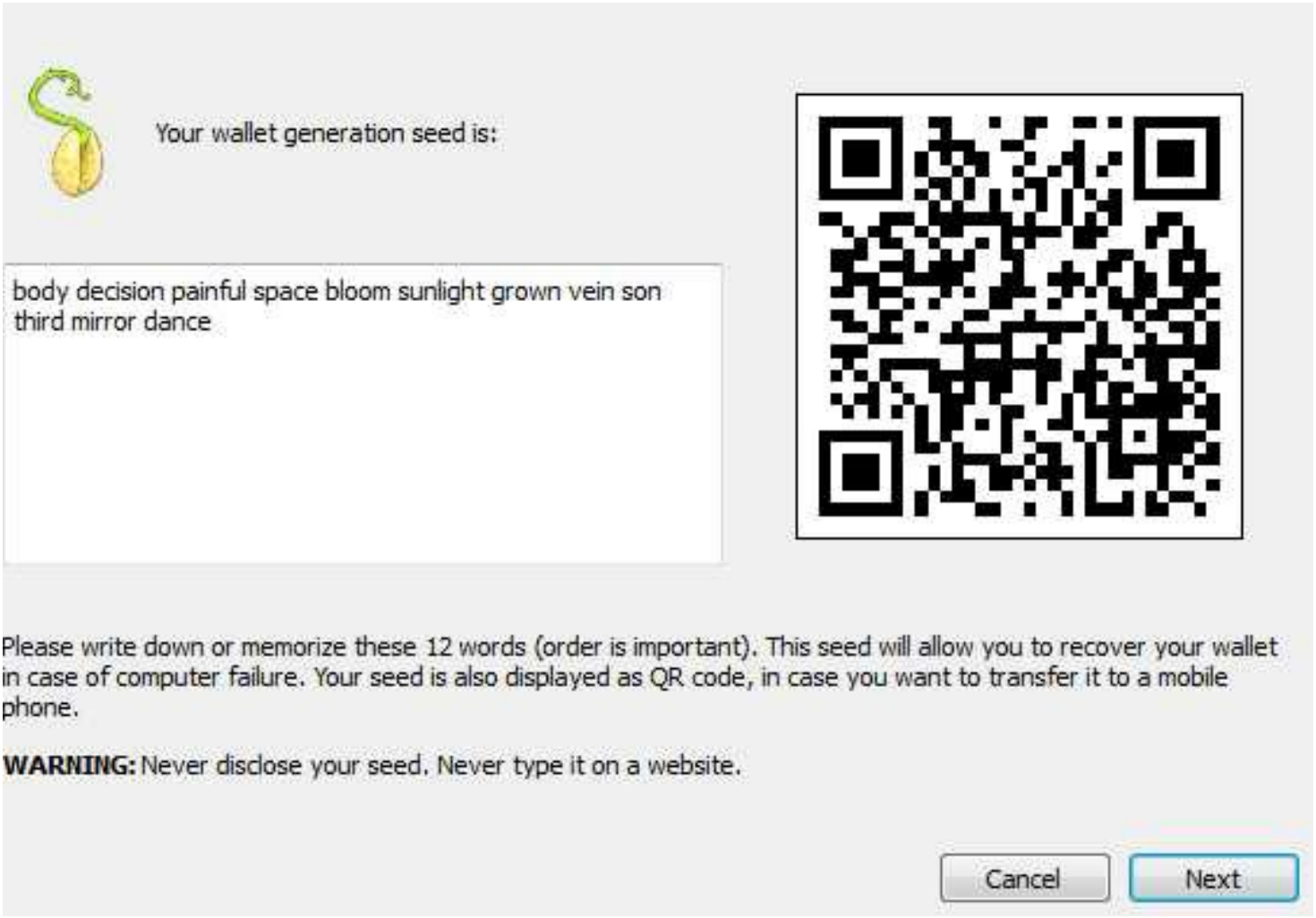
conjuntamente forman la cartera.

Formas de Backup

Para guardar sus claves privadas, es decir, hacer el backup de

seguridad de su cartera, hay algunas posibilidades. Para hacer

una copia de seguridad, debe tener la posesión de la *seed* o de



las claves privadas derivadas de la *seed*. Las llaves y las *seeds*

se pueden salvar en un archivo txt, ou notepad, y guardar en

un HD, o también pueden ser impresas en papel. En la

práctica, la *seed* es una combinación de 12 palabras en inglés

que permiten acceder a su cartera en caso de pérdida de la

clave o defecto en el ordenador que almacena la cartera.

Otras criptomonedas tienen diferentes *seeds*, con más o

menos palabras, o palabras inventadas que no son del idioma

inglés.

Sólo 12 palabras aleatorias dan seguridad suficiente

para que nadie pueda invadir y robar una cartera? La

respuesta es sí. Considerando todas las palabras de lengua

inglesa posibles para esa combinación, se necesitarían

millones de años para una computadora encontrar una

combinación correcta aleatoriamente.

Ejemplo de *seed* de bitcoin:

Es recomendable no guardar grandes cantidades de

dinero en carteras online, pues son más susceptibles a ataques

de hackers por estar siempre conectadas a internet. Las

carteras offline (HD o papel) son más seguras, pero el usuario

debe preocuparse por la pérdida, el robo y el hurto físicos. En

esta nueva era, algunos pendrives pueden valer más que

barras de oro. Es posible que tengas que guardar su pendrive

o un pedazo de papel en una caja fuerte.

Pero llega de teoría. Vamos a ver a continuación cómo

hacer para empezar a entrar en el mundo de las

criptomonedas con ejemplos prácticos.

Paso 1: Descargar una cartera

Resaltamos que es altamente recomendable tener una cartera

en su propio ordenador, en lugar de dejar sus activos en

posesión de una exchange o bolsa. Cuando usted deja sus

activos con terceros, usted está confiando a ellos la custodia

de las mercancías que te pertenecen. Cuando el activo está

bajo custodia, lo que usted tiene en la práctica no es el activo

en sí, sino una deuda de la correduría para usted.

No es necesario tener una cartera, pero altamente

recomendable. Si no tiene interés en tener una cartera propia,

puede ir directamente al paso 2

(comprar bitcoins).

Hay variás paginas web diferentes en que se puede

crear una cartera de criptomonedas. Vamos a usar el ejemplo

del sitio bitcoin.org, que es una organización sin fines de

lucro que ayuda en este proceso, pero se pueden usar varios

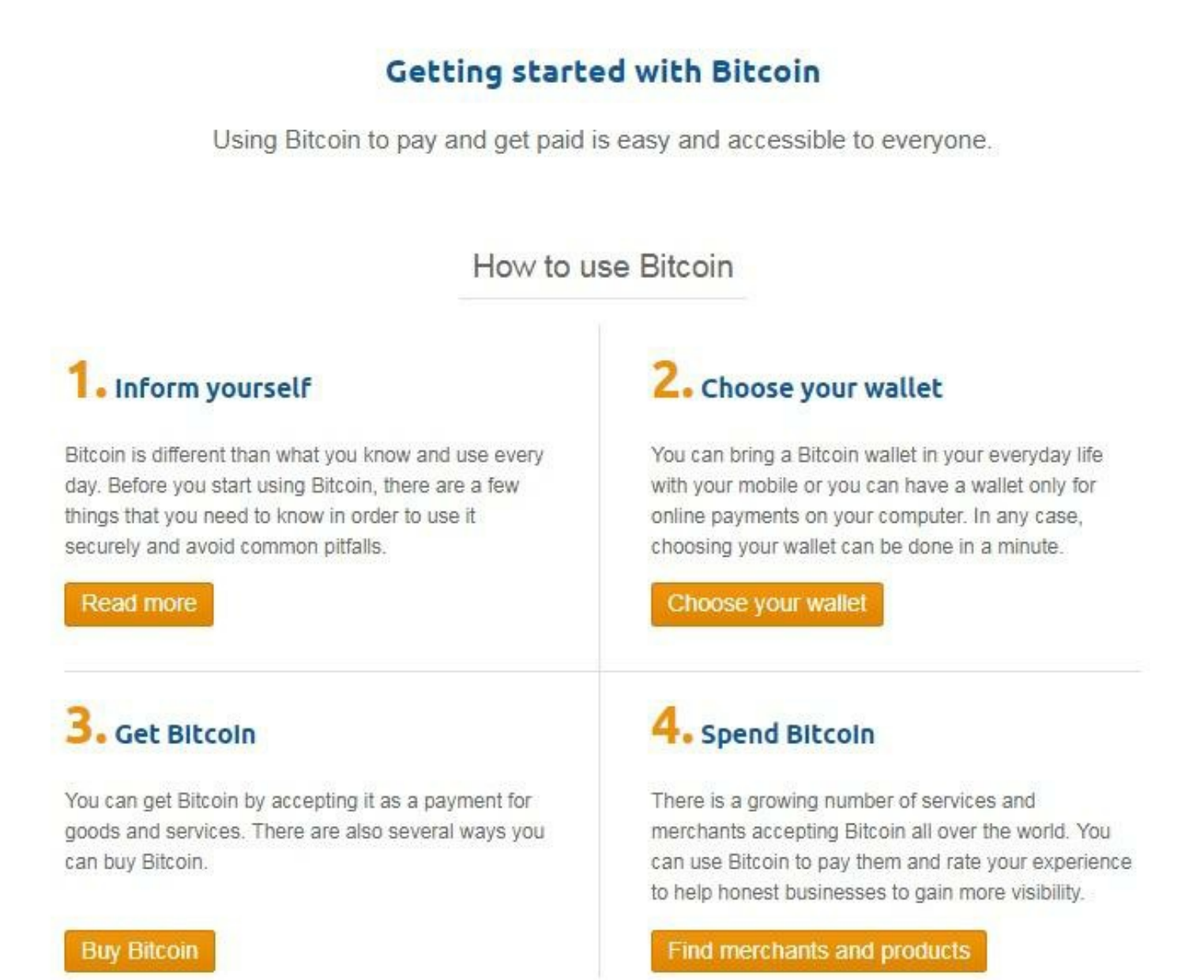
otros sitios.

En primer lugar, es necesario entrar en la dirección

bitcoin.org y descargar una de las carteras sugeridas por el

sitio. En nuestro caso, vamos a bajar a Electrum.

Acceder a bitcoin.org y hacer clic en el botón azul.



Clic en elegir cartera (numero 2)

Choose your Bitcoin wallet

Find your wallet and start making payments with merchants and users.

Desktop Hardware Mobile Web


Bitcoin Knots


Bitcoin Core


Green Address

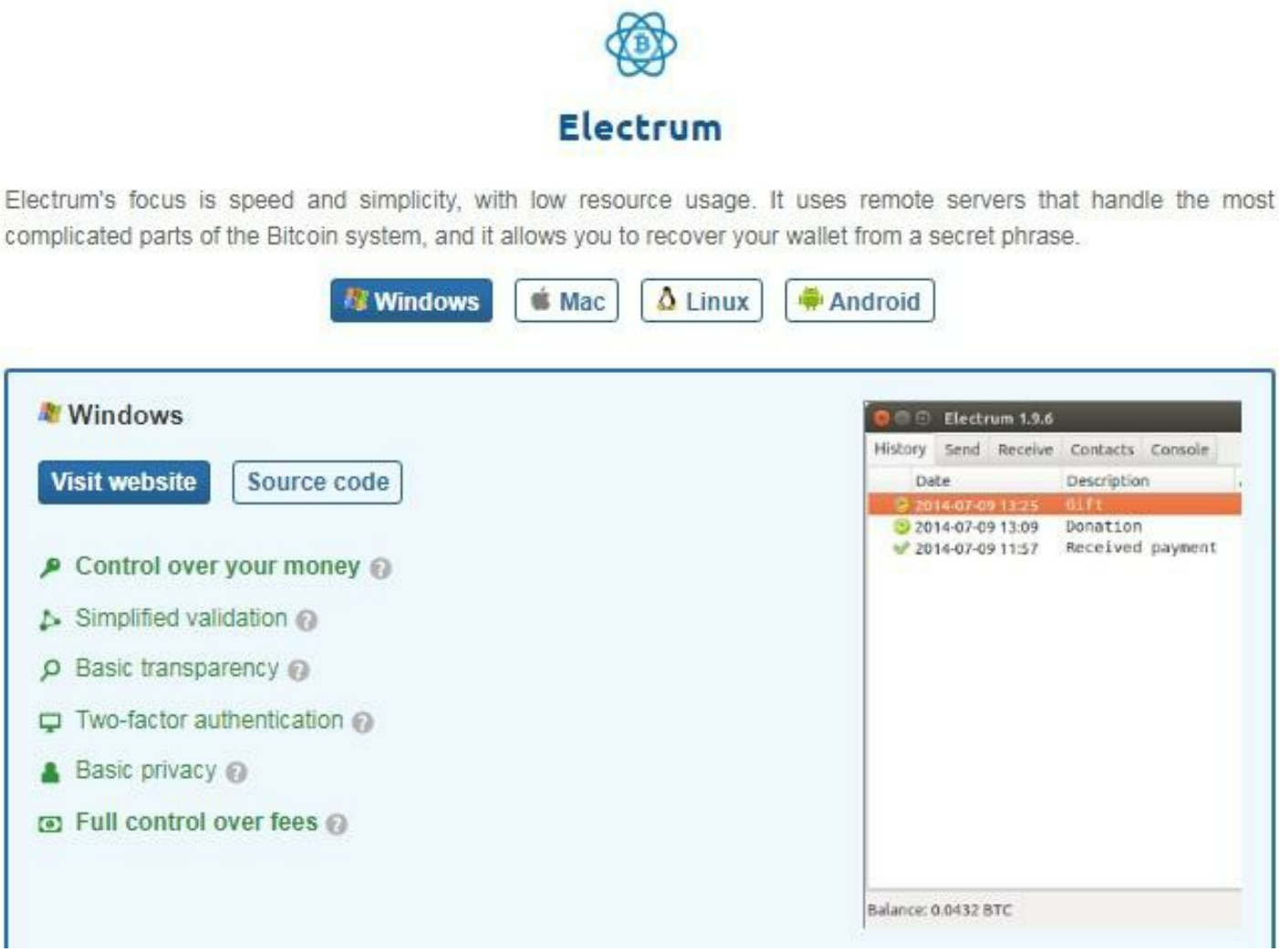

ArcBit


mSIGNA


Armory


Bither


Electrum



Elegir la cartera Electrum:

Visitar la página web de la cartera:

Safe

Your private keys are encrypted and never leave your computer.

Forgiving

Your funds can be recovered from a secret phrase.

Instant On

Electrum is fast, because it uses servers that index the Bitcoin blockchain.

No Lock-In

You can export your private keys and use them in other Bitcoin clients.

No Downtimes

Electrum servers are decentralized and redundant. Your wallet is never down.

Proof Checking

Electrum Wallet verifies all the transactions in your history using SPV.

Cold Storage

Keep your private keys offline, and go online with a watching-only wallet.

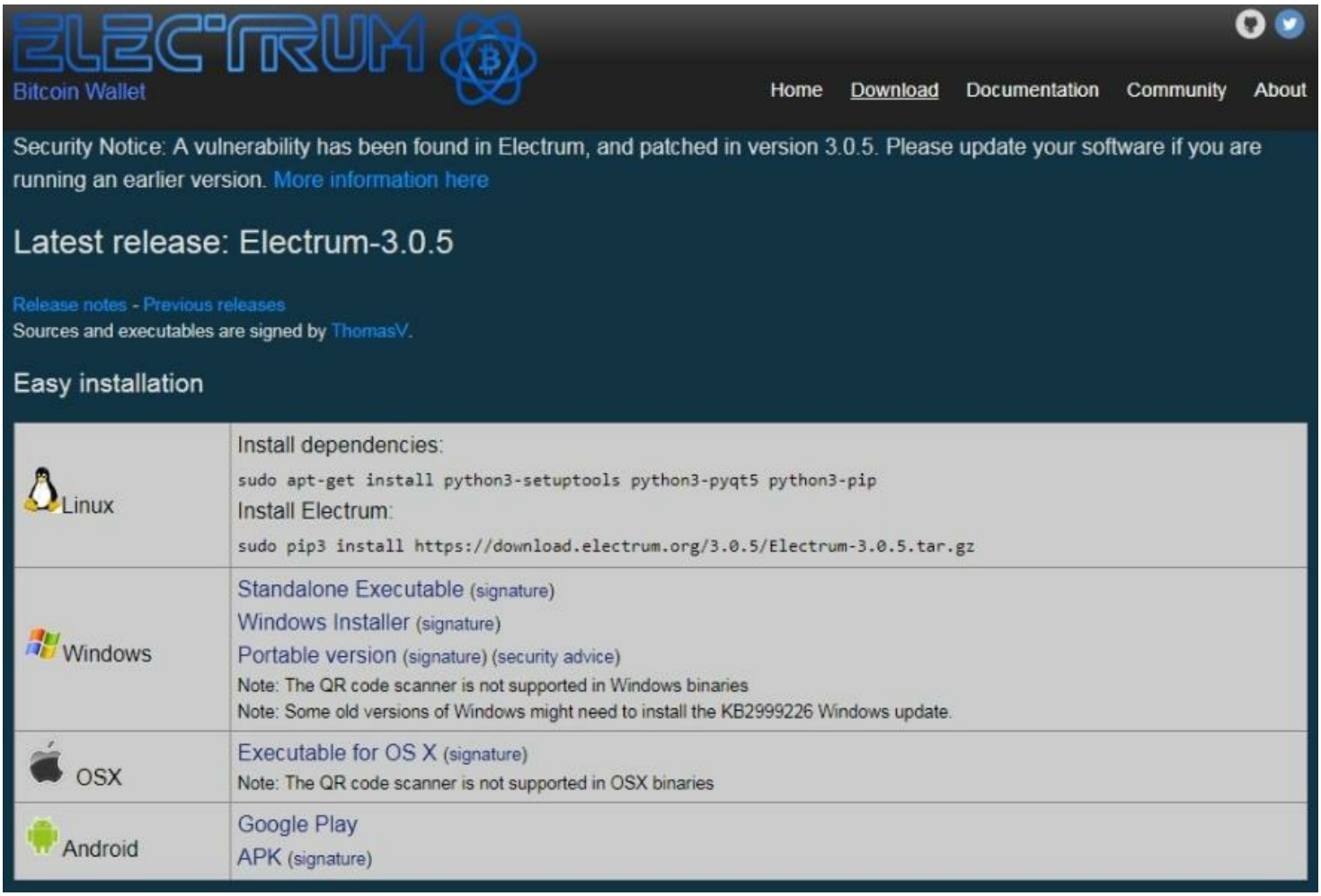
Multisig

Split the permission to spend your coins between several wallets.

Add-ons

Electrum supports third-party plugins: Multisig services, Hardware wallets, etc.

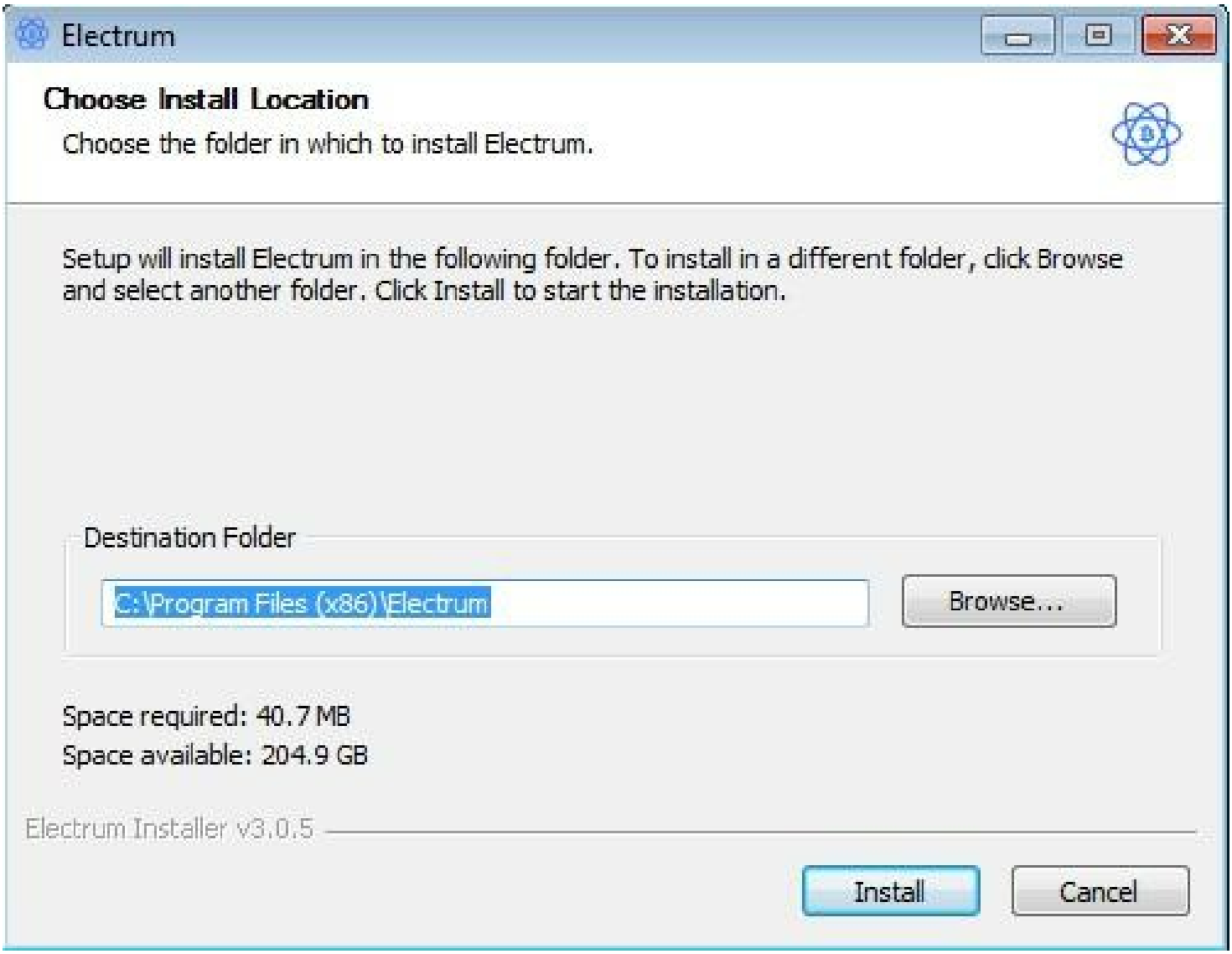
Download Electrum

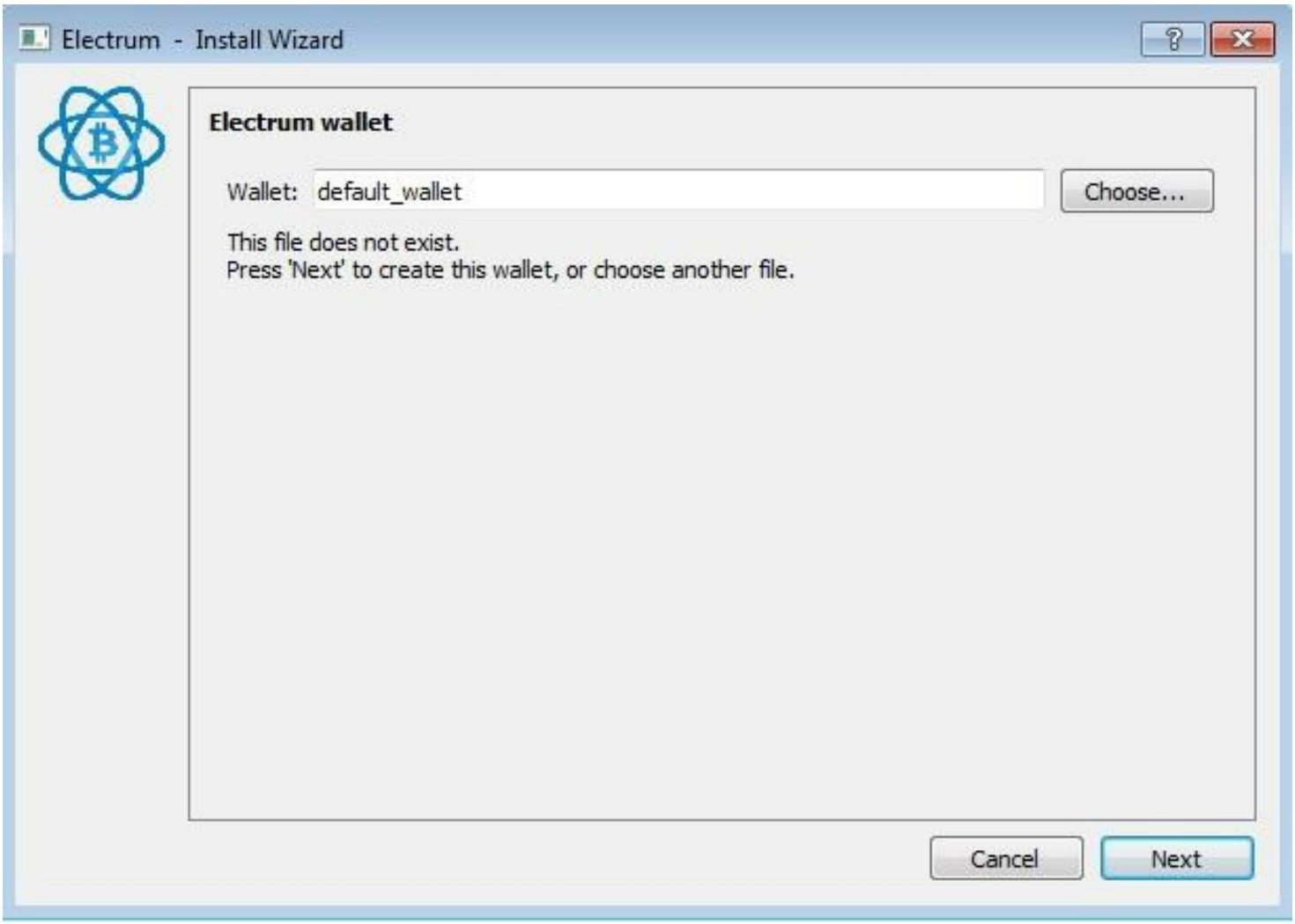


Haga clic en el botón "Dowload Electrum":

Elegir el tipo de instalación. En este caso, vamos a elegir la

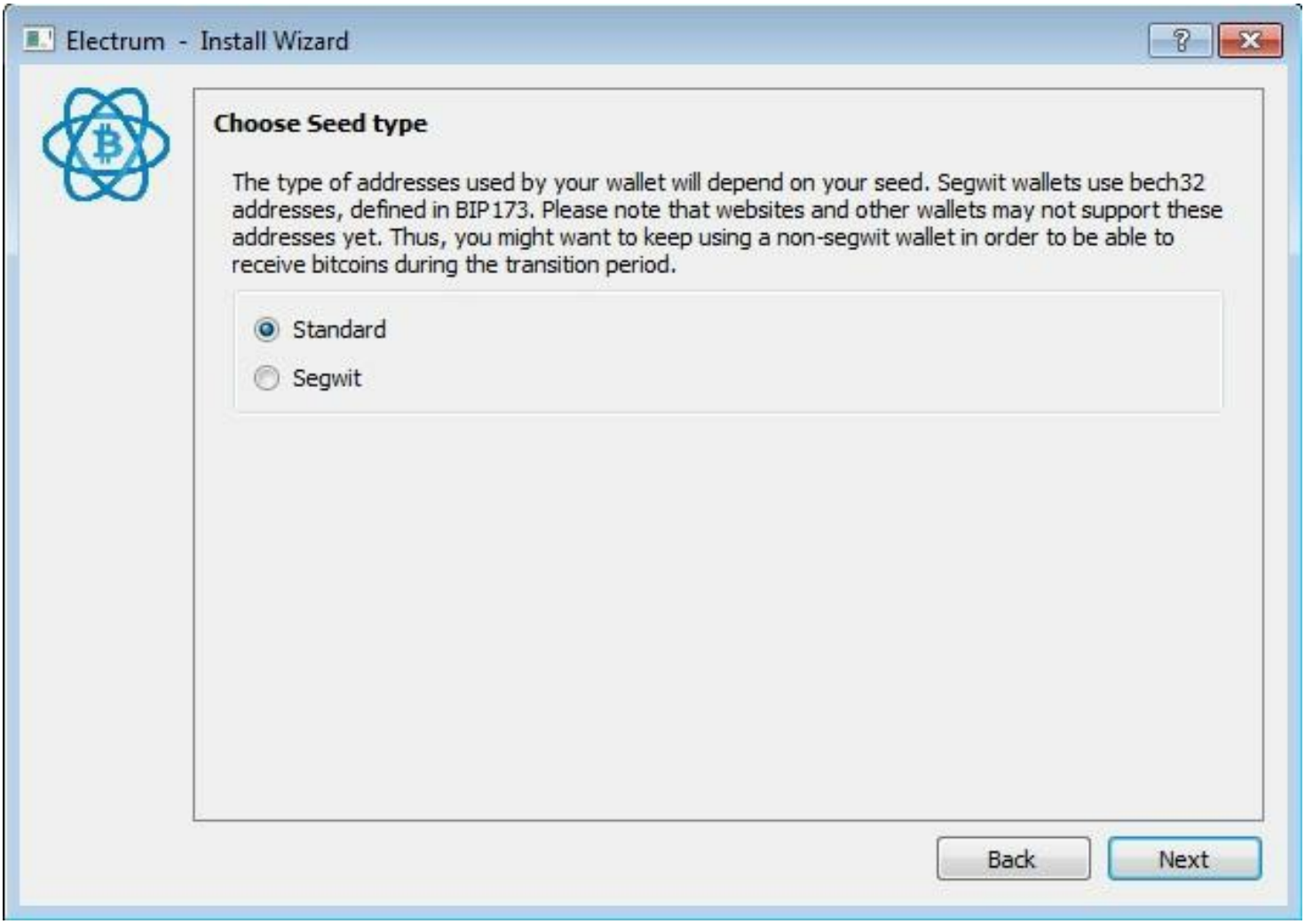
versión "windows installer":


Electrum
Choose Install Location
Choose the folder in which to install Electrum.
Setup will install Electrum in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\Program Files (x86)\Electrum
Browse...
Space required: 40.7 MB
Space available: 204.9 GB
Electrum Installer v3.0.5
Install
Cancel



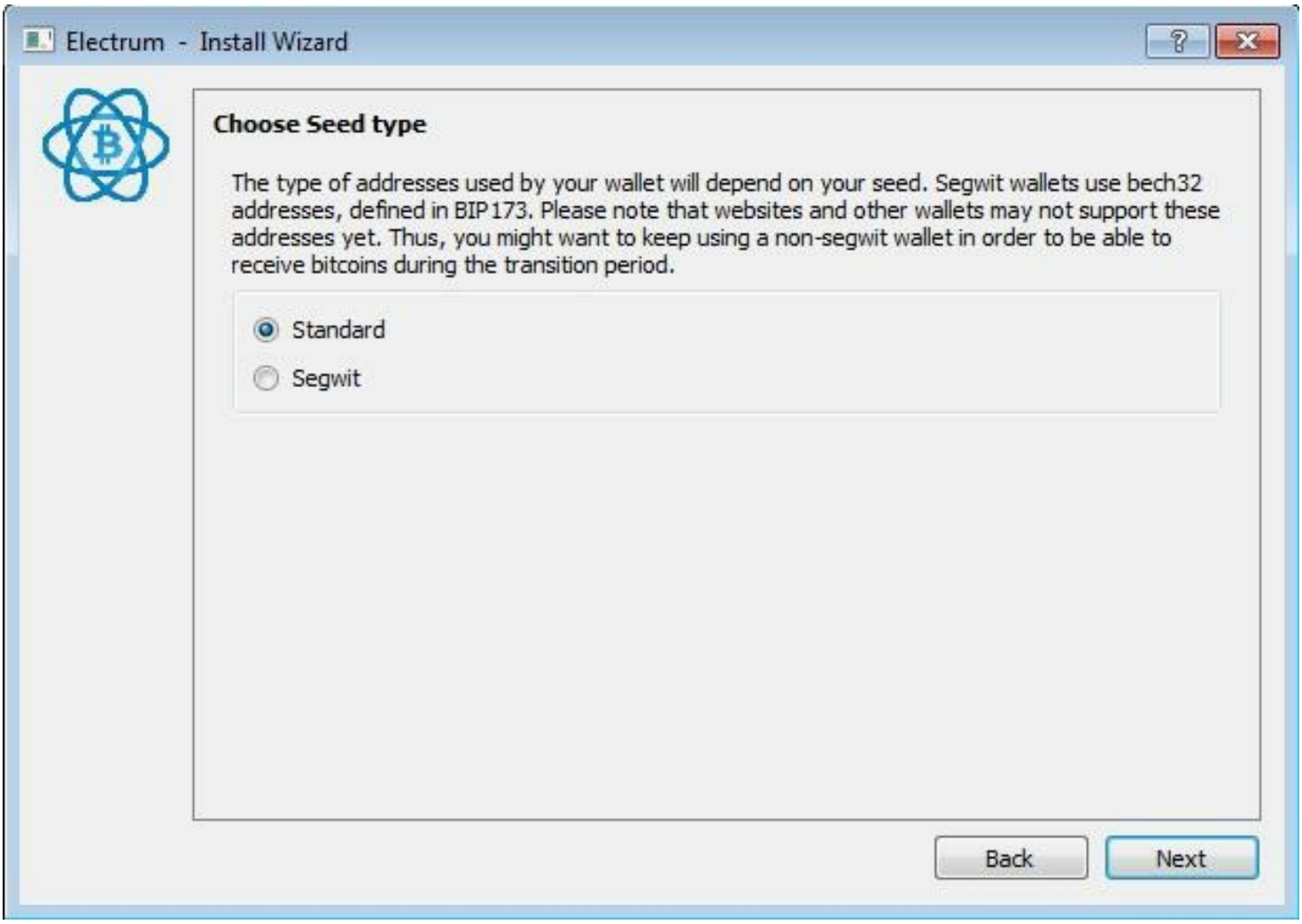
Cuando haya terminado de descargar, ejecutar el instalador:

después, debes ejecutar en Electrum y clicar "next":


Electrum - Install Wizard
Choose Seed type
The type of addresses used by your wallet will depend on your seed. Segwit wallets use bech32 addresses, defined in BIP173. Please note that websites and other wallets may not support these addresses yet. Thus, you might want to keep using a non-segwit wallet in order to be able to receive bitcoins during the transition period.
Standard
Segwit
Back
Next

a continuación, elija "standard wallet":

a continuación, elija "Create a New Seed":



elegir "standard":

Esta parte es la más importante. El programa proporcionará

12 palabras que servirán como "seed". Estas palabras son el

equivalente a una contraseña que no se debe perder nunca.

Anote las palabras y guárdelas en un lugar seguro, sea

digitalmente o por escrito. Tenga cuidado de no anotar mal o

fuera de orden. Después de anotar, haga clic en "next". En

seguida, el programa le pedirá que escriba las palabras que

acaba de anotar. Escriba las palabras y haga clic en next:

Electrum - Install Wizard

Your wallet generation seed is:

enforce galaxy volcano wear repeat select forest carry cancel bike display cup

Options

Please save these 12 words on paper (order is important). This seed will allow you to recover your wallet in case of computer failure.

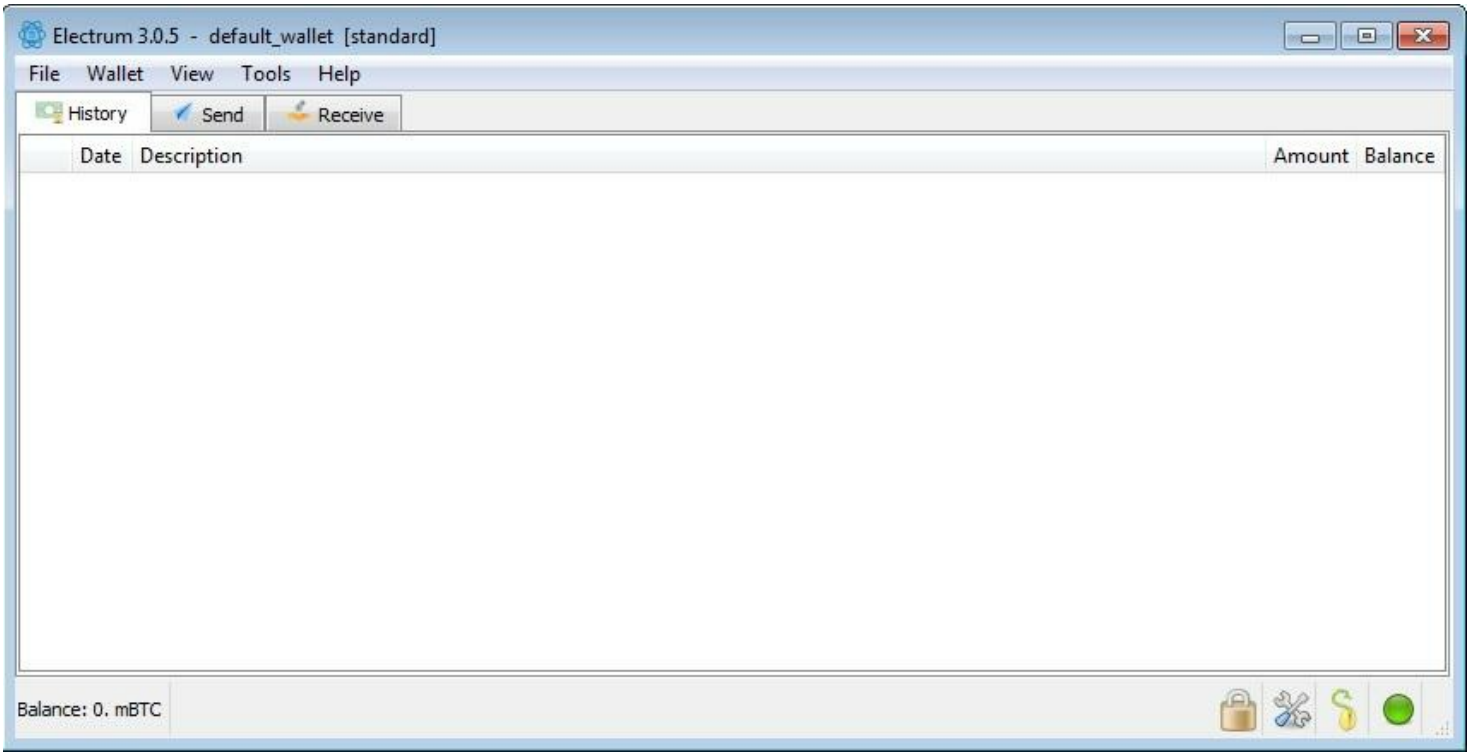
WARNING:

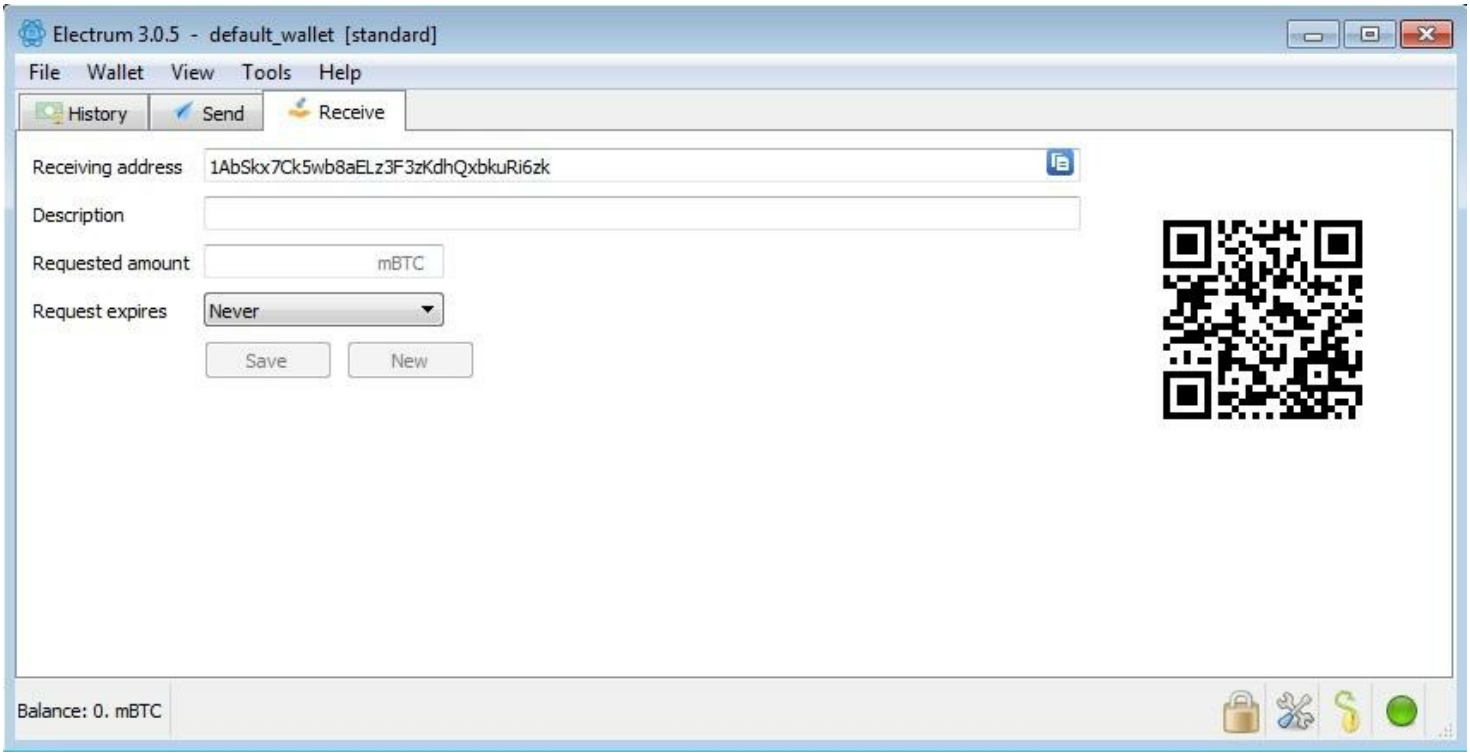
- Never disclose your seed.
- Never type it on a website.
- Do not store it electronically.

Back Next

A continuación, debe elegir una contraseña para acceder a la

cartera. Defina su contraseña y haga clic en "next":


Electrum 3.0.5 - default_wallet [standard]
File
Wallet
View
Tools
Help
History
Send
Receive
Date
Description
Amount
Balance
Balance: 0. mBTC



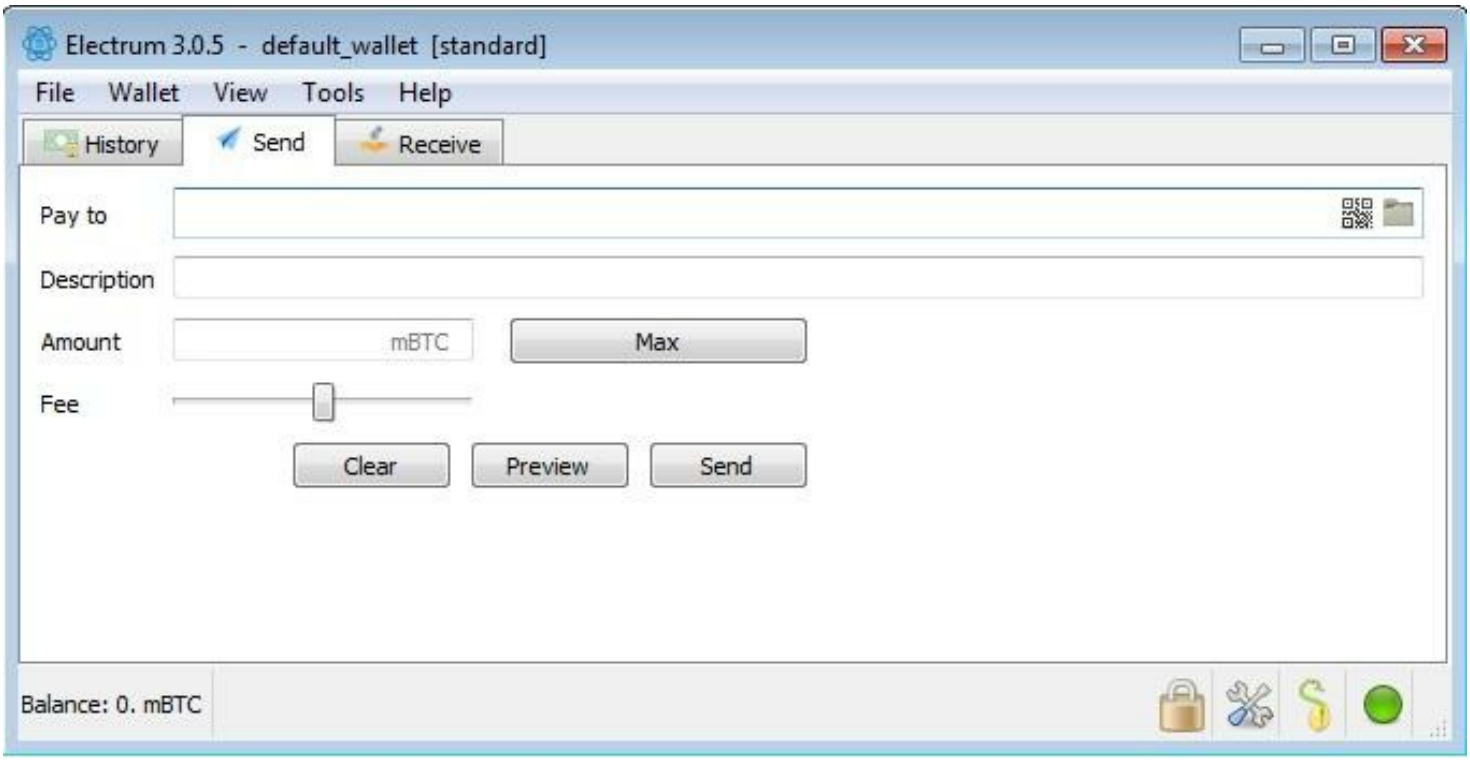
Listo! Debe ver la siguiente pantalla:

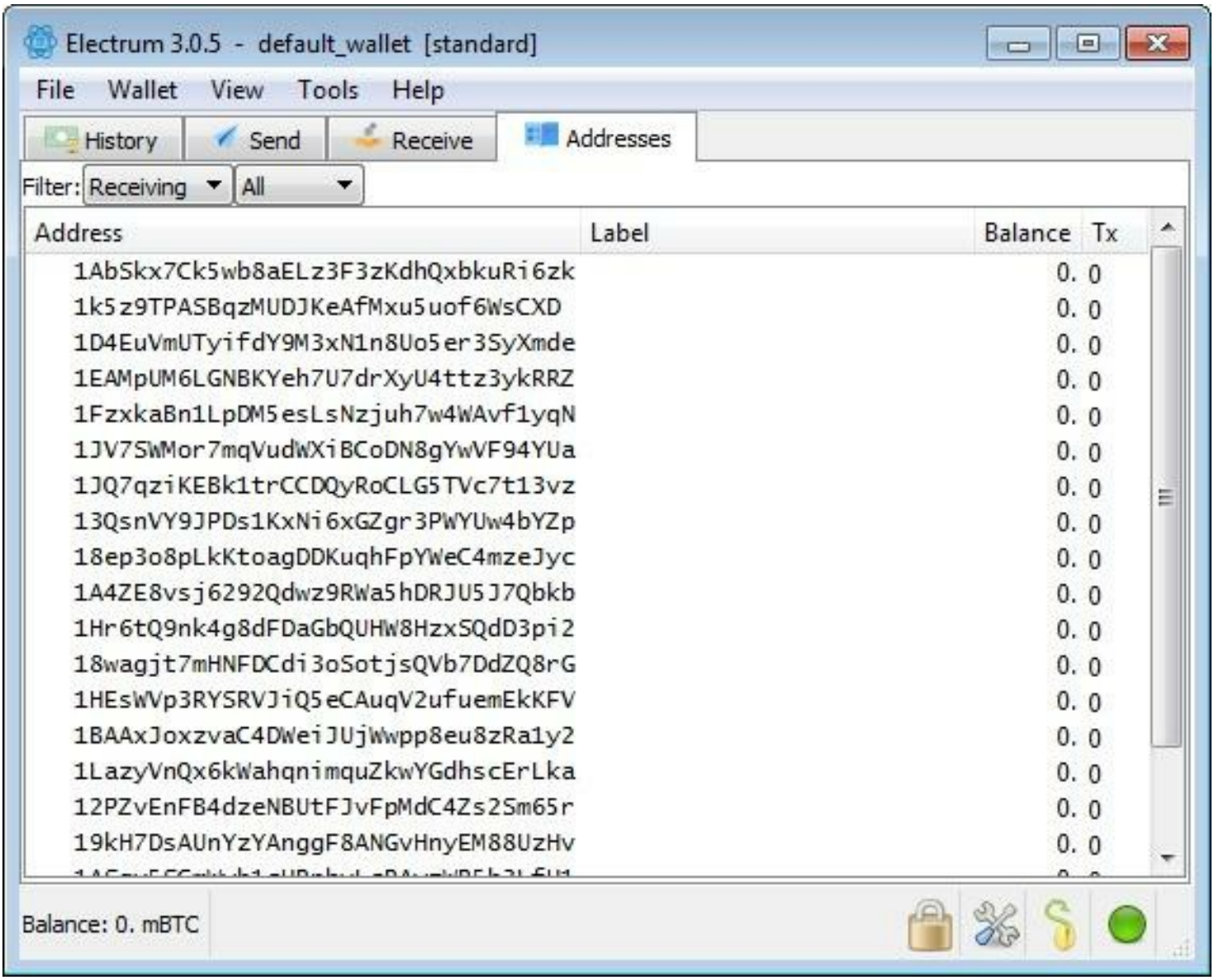
Si hace clic en la pestaña "Receive", verá su dirección en la

que puede recibir bitcoins, en forma de letras y también en

forma de "QR code". Esta es la dirección que la gente debe

saber para mandar bitcoins para usted:



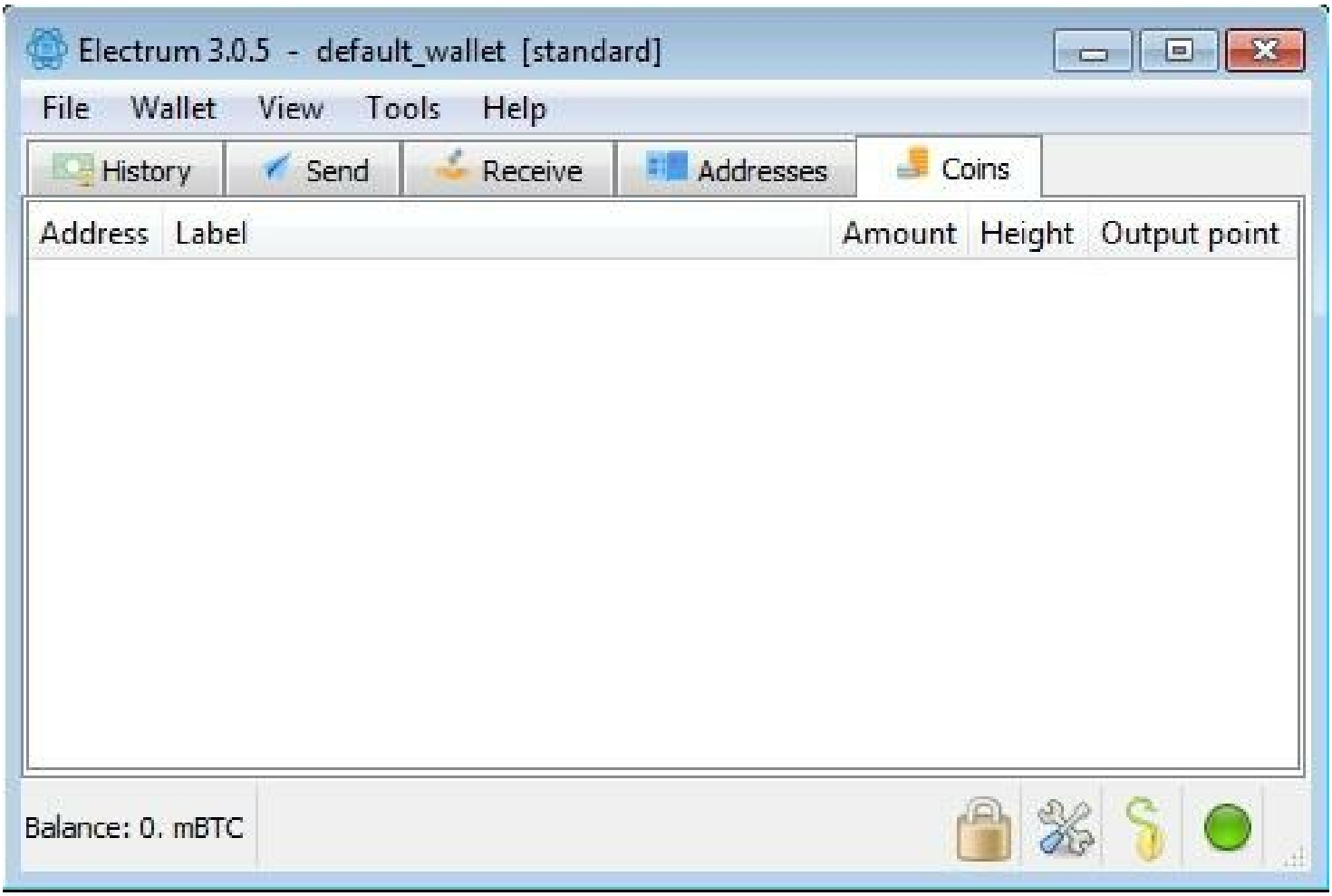


Para mandar bitcoins, haga clic en la pestaña "send", y

coloque la dirección a la que desea mandar.

Para ver todas las direcciones en las que puede recibir, puede

hacer clic en View> Mostrar direcciones:



Para ver el saldo, puedes hacer clic en View> Show Coins

Estas son las características básicas más importantes de la

cartera.

Paso 2: Comprar Bitcoins

Ahora tenemos una cartera en nuestro ordenador, pero está

vacía. Tenemos que encontrar a alguien dispuesto a transferir

bitcoins. Usted puede publicar su dirección en Internet

pidiendo donaciones, pero una forma más rápida de conseguir

bitcoins es la compra de alguien. Para esto existen bolsas de

criptomonedas.

En este paso, el inversor debe buscar posibles

corredores / bolsas de bitcoins por cuenta propia, y abrir una

cuenta en una de ellas, o en varias, si lo desea. Se recomienda

seguir algunas bolsas que operan en latinoamerica hoy, pero

que cobran tarifas diferentes, tienen techos diarios de

COMPRA			VENDA		
Comprador	Quantidade	Preço	Preço	Quantidade	Vendedor
Pie_900492	฿ 0,20000000	R$ 46.055,00	R$ 46.099,99	฿ 0,01321434	Pulpo_901439
Pie_899869	฿ 0,02172968	R$ 46.020,00	R$ 46.100,00	฿ 0,00779766	Zebra_900257
Gaiota_901570	฿ 0,10867675	R$ 46.008,00	R$ 46.201,09	฿ 0,02164451	Cerf_901660
Puma_901863	฿ 0,04565776	R$ 46.000,06	R$ 46.298,98	฿ 0,00262565	Coelho_900914
Otter_901855	฿ 0,00100000	R$ 46.000,00	R$ 46.299,00	฿ 0,01000000	Corvo_901572
Whale_900787	฿ 0,00217391	R$ 45.999,99	R$ 46.299,99	฿ 0,79170694	Ram_900116
Hund_900807	฿ 1,24119338	R$ 45.801,09	R$ 46.300,00	฿ 0,00431965	Orca_900594
Crock_901595	฿ 0,06550183	R$ 45.800,09	R$ 46.300,00	฿ 0,19000000	Zebra_901088
Zebra_901561	฿ 0,42466446	R$ 45.800,04	R$ 46.300,00	฿ 0,10000000	Pie_902857
Lynx_901552	฿ 0,02729255	R$ 45.800,03	R$ 46.400,00	฿ 0,15975149	Sloth_900853
Gallo_902196	฿ 0,13932240	R$ 45.750,00	R$ 46.487,65	฿ 0,21600000	Zebra_901545
Pony_901709	฿ 0,17445962	R$ 45.703,01	R$ 46.498,98	฿ 0,05829793	Hund_899913
Wal_901540	฿ 0,03656412	R$ 45.703,00	R$ 46.498,99	฿ 0,02150584	Pombo_900352
Wal_901540	฿ 0,03656412	R$ 45.703,00	R$ 46.526,00	฿ 0,10000000	Urso_900356
Wal_901540	฿ 0,03656412	R$ 45.703,00	R$ 46.527,00	฿ 0,01074644	Ruc_902229
Wal_901540	฿ 0,03656412	R$ 45.703,00	R$ 46.528,00	฿ 0,02149243	Pombo_900352
Wal_901540	฿ 0,03656412	R$ 45.703,00	R$ 46.529,97	฿ 0,06525294	Pop_899493
Wal_901540	฿ 0,03656412	R$ 45.703,00	R$ 46.530,00	฿ 0,01000000	Poney_899780
Wal_901540	฿ 0,03656412	R$ 45.703,00	R$ 46.565,99	฿ 3,00000000	Ruc_899250
Loro_900018	฿ 0,09990000	R$ 45.702,00	R$ 46.566,00	฿ 0,02147489	Pombo_900352

volumen de transacción, por lo que es necesario que el

inversor se informe cuando se registre en alguna de ellas.

Para o caso de España, las bolsas

operan en la zona del euro,

entonces son bolsas europeas.

El proceso de registro en bolsas es rápido y simple,

pero puede variar de un país a otro. En Brasil, ellas solicitan

que el negociador mande informaciones personales, fotos de

documentos y comprobante de residencia para comenzar a

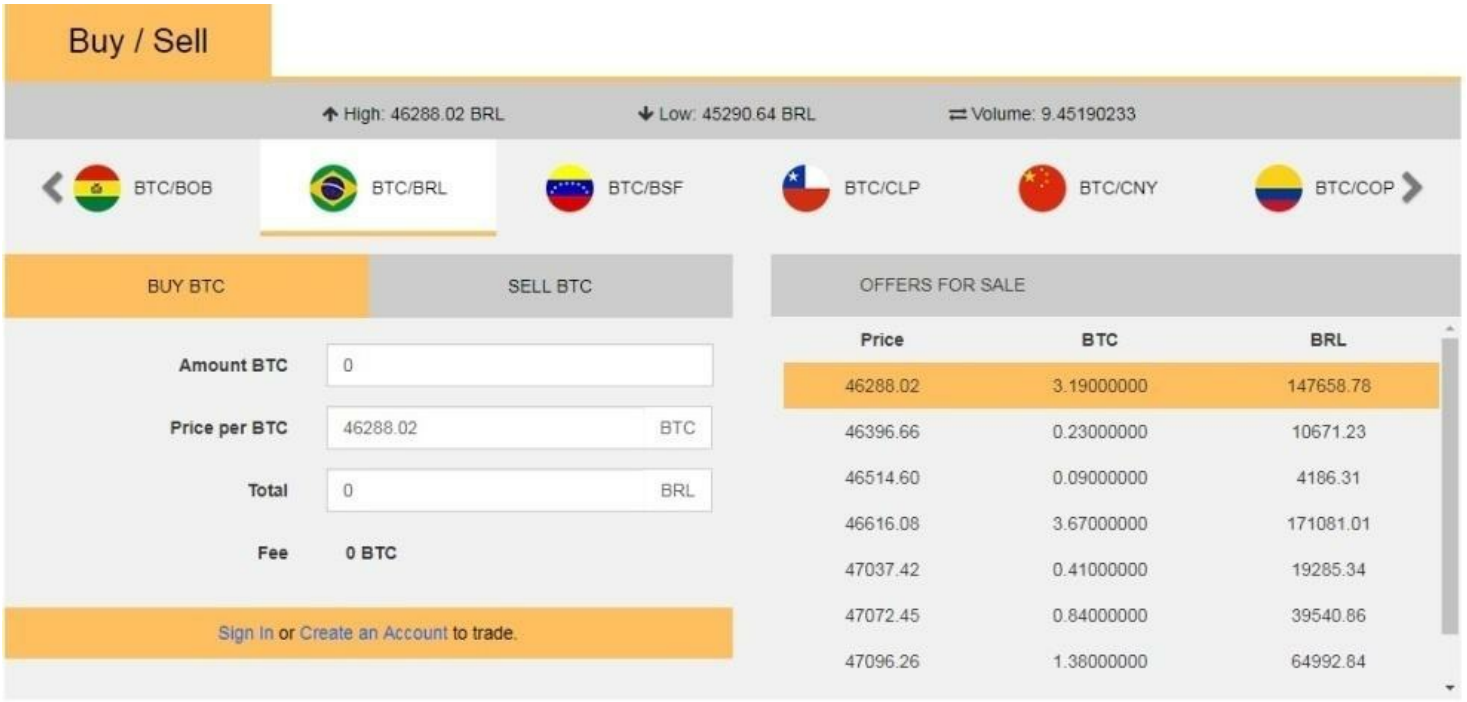
operar.

Cuando haya decidido qué bolsa usar y

hacer registro e

login, el comprador se encontrará con una pantalla más o

menos así, pero que puede variar entre los diferentes sitios:



Después de entrar en el sitio, haga clic en la compra / venta.

Entonces poner la cantidad de compra deseada y comprar. En

algunas bolsas la interfaz puede ser diferente

O puede aparecer como si fuera una lista de anuncios

Cuando compre los bitcoins, el saldo BTC debe aumentar de

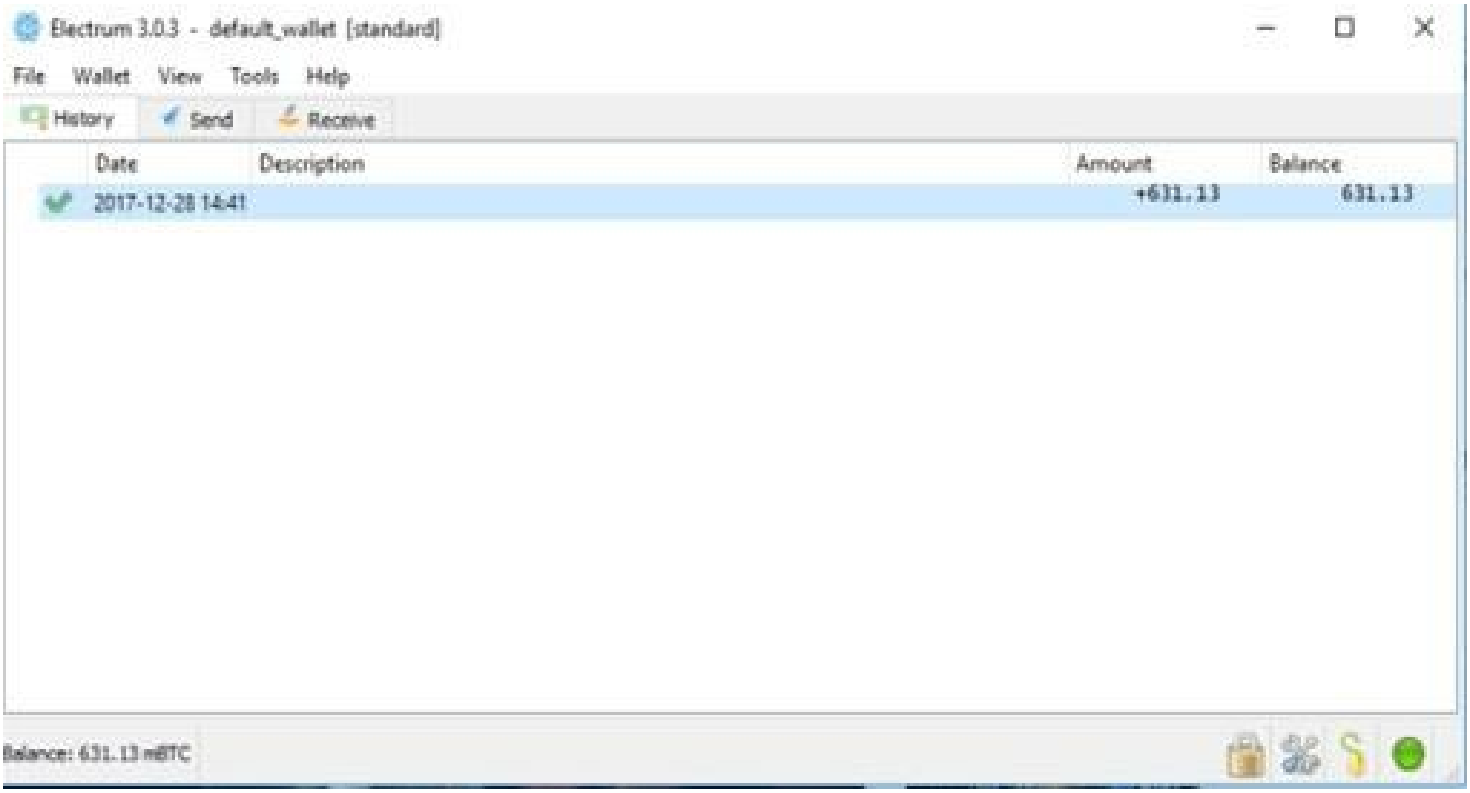
acuerdo con su compra. Ahora ya es posible retirar el BTC de

la bolsa y mandar a su cartera. Vaya en retirada, elegir

Bitcoin, y luego coloque la dirección de su cartera y la

cantidad a ser retirada. Después de unos minutos su cartera

recibirá los créditos.



Usted puede elegir dejar el BTC en la cartera de la

correduría, pero recuerde que mientras usted tiene BTC en la

correduría, usted está confiando que ésta le entregará el BTC

cuando pida. Es como si estuviera dejando su dinero en un

banco o en una correduría tradicional. Usted no tiene el

activo, usted tiene una promesa de entrega del activo. Usted

sólo tiene el activo cuando de hecho transfiere a su propia

cartera.

Cuando la transferencia esté completa, el valor debe aparecer

en su cartera de escritorio.

Paso 3: Comprar Cosas Con Bitcoin, O Vender.

Tanto para comprar cosas con bitcoins como para vender

bitcoins, usted debe usar la pestaña "send" para enviar sus

bitcoins a la dirección de alguien. Si quieres vender sus

bitcoins, enviará sus monedas a la dirección de una bolsa. Si

está comprando algo, enviará la moneda a la dirección del

comerciante.

Para comprar bitcoins con rapidez en su país, es necesario

tener una cuenta en alguna bolsa local. A continuación se

muestran algunas de las principales bolsas latinoamericanas

actuales. La intención no es listar todas las bolsas de cada

país porque es cada mes surgen nuevas bolsas. Sólo queremos

dar algunas referencias para quien quiera abrir una cuenta y

empezar a operar.

Argentina

www.southxchange.com

Brasil

foxbit.com.br

braziliex.com

Colombia

www.bitcoinsuramerica.com

Chile

www.surbtc.com

chilebit.net

Mexico

https://bitso.com

Paraguay

www.guaranibitcoin.com

Peru

www.bitinka.pe

Uruguay

www.spectrocoin.com

Venezuela

www.monkeycoin.exchange

www.surbitcoin.com

Las bolsas todavía tienen altos costos de transacción,

cobrando un porcentaje sobre las órdenes, en lugar de cobrar

un costo fijo por orden. Conforme la competencia aumenta en

las bolsas, estas tasas tienden a caer. Algunas bolsas, como el

MercadoBitcoin en Brasil, llegan al extremo de cobrar por el

depósito de dinero! Recomendamos pasar lejos de este tipo

de bolsa.

En el mundo, algunas de las principales son:

https://www.bitstamp.net/

https://www.coinbase.com/

https://www.gdax.com/

https://www.bitfinex.com/

Abrir cuenta en estas bolsas es rápido y fácil, y

normalmente se puede operar luego después de la validación

de tus informaciones personales, pero sólo para usar una

criptomoneda para comprar otra, por ejemplo comprar ETH

usando BTC. Si el inversionista desea utilizar moneda

fiduciaria (monedas como el Peso, Dólar y Euro) para

comprar criptomoneda, o vender la criptomoneda por dinero

fiduciario, tiene que enviar documentos

como DNI y

comprobante de residencia para verificación en la bolsa.

Todo esto puede ser hecho por internet. Después de unas

horas o días, debido al hecho de ser una persona verificando

los documentos, si es aprobado, el inversionista queda

liberado para usar dinero fiduciario también.

Esta identificación ocurre porque los gobiernos están

presionando fuertemente a las bolsas para identificar sus

clientes. En Estados Unidos, el gobierno llegó al extremo de

prohibir que los bolsas fuera de Estados Unidos reciban

clientes estadounidenses.

Los gobiernos argumentan que esta presión en

identificar a los inversores es para prevenir el lavado de

dinero, pero un otro motivo muy importante es que los

gobiernos no quieren dejar de recaudar impuestos sobre la

renta.

Este es el único punto en que los gobiernos logran

tener algún control en las transacciones. En el punto en que el

dinero fiduciario es intercambiado por criptomoneda en

bolsas online. Si el inversionista desea privacidad, debe

buscar otros medios de comprar criptomonedas, como en

transacciones privadas o en paginas como mercadolibre o

craigslist.

La Bolsa Que Bitcoin Merece: Conozca A Bisq

Bisq es el nombre de una bolsa que está totalmente alineada

con la filosofía de Bitcoin. Es un programa p2p, de código

abierto, transparente, que se baja en el ordenador. El

programa entonces conecta a usuarios alrededor del mundo

directamente. En otras palabras, es una bolsa descentralizada

con una cartera embutida, o una cartera con una bolsa

embutida.

El programa es gratuito para descargar y el usuario

sólo paga las tasas de transacciones necesarias para hacer las

transferencias. El programa utiliza la red TOR para conectar

los usuarios, por eso es totalmente segura y anónima.

El único pero de Bisq es que no presenta mucha

liquidez, pero para transacciones puntuales es más que

suficiente. Si más usuarios adoptan Bisq, será sin duda la

mejor opción para transacciones.

Para comprar BTC, por ejemplo, el usuario hace una

oferta y espera que alguien la tome, o entra en el libro de

ofertas y toma alguna oferta de venta disponible. El usuario

entonces espera al vendedor hacer la transferencia. La BTC

entonces se bloquea en una dirección en el software, y sólo se

libera al comprador cuando éste transfiere el dinero al

vendedor, normalmente por transferencia electrónica directa.

Cuando el vendedor confirme la recepción del depósito, el

BTC se libera, y la transacción es finalizada. Para realizar la

transacción, tanto el vendedor como el

comprador deben

ealizar un depósito de garantía del 10% del valor de la

transacción. Concluida la transacción, las partes reciben el

depósito de vuelta. Esto se hace para que los usuarios

malintencionados no abusen del sistema.

Recomendamos Bisq para usuarios más avanzados,

que se sienten más cómodos en el mundo de las

criptomonedas. En Bisq toda la intermediación es por

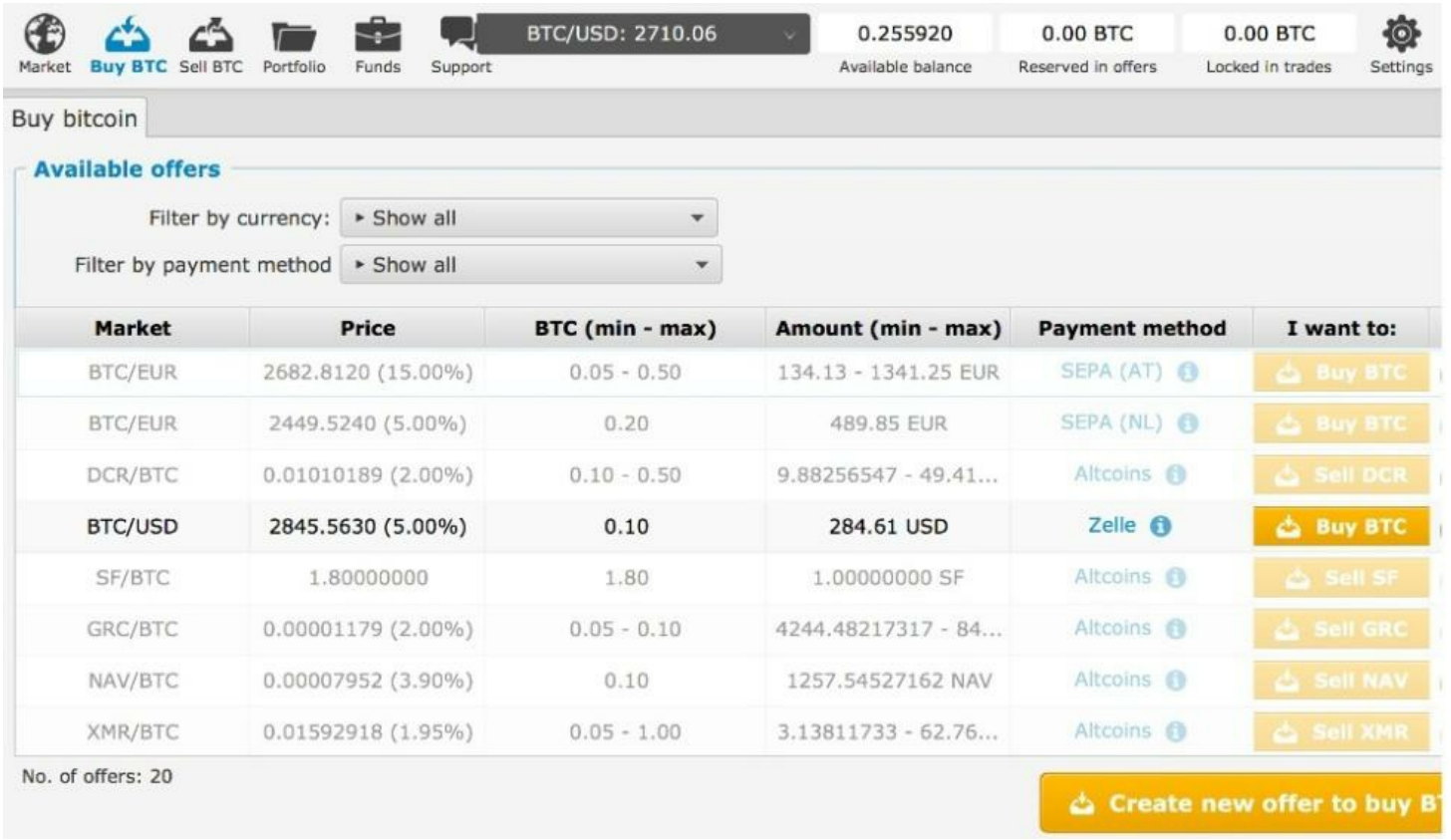
software, entonces no existe la posibilidad de la bolsa

congelar sus fondos. Las ventajas de Bisq son los costos, la

seguridad (Bisq nunca va a romper, ya que no guarda su

dinero por usted), y la protección de su privacidad. Como no

existe una empresa detrás de la bolsa, los gobiernos no



pueden obligar a nadie a mostrar los datos de los

participantes. El único que tendrá acceso a su identidad será

su contraparte. Por este motivo, no se recomienda usar la

bolsa en países donde Bitcoin está

prohibido, pues la

contraparte puede ser alguna autoridad pública disfrazada de

participante.

Mira cómo es la cara de Bisq:

Minería de Bitcoins

La otra forma de adquirir bitcoins además de comprar

es minar. Comentamos que la minería de bitcoins exige la

compra de equipos específicos, llamados genéricamente de

ASIC. No hay muchos fabricantes de ASIC de minería. La

mayor empresa en este sector se llama Bitmain y opera en

China. La empresa fabrica equipos de minería para varias

monedas. Que vende parte de su producción al mercado, pero

la mayor parte del equipo se utiliza en operaciones de minería

de la propia empresa. Por este motivo, es muy difícil comprar

un equipo directo de Bitmain, que

tampoco tiene mucho

interés en ofrecer el equipo al mercado. Es posible encontrar

ese tipo de ordenador en mercado de usados, en sitios como

E-bay y Amazon, pero aún así es difícil, el equipo usado

puede acabar costando más caro que uno nuevo y peor, sin

garantía.

Hablando en garantía, la propia Bitmain es famosa por

tener pésima atención al consumidor y entregar equipos

defectuosos. Es claro que la empresa no está muy interesada

en vender su equipo producido, pues logra ganar mucho con

la minería propia. En el futuro, esperamos que la competencia

en la fabricación de este tipo de hardware se intensifique,

reduciendo la concentración de mercado de Bitmain, después

de todo existe mercado para que esto

suceda. Hoy en día, la

demanda de equipo de minería es tan grande que hasta

empresas como NVIDIA, que produce tarjetas gráficas

(GPU) para el procesamiento de datos y videojuegos, no

están consiguiendo atenderla.

Hoy, cuando se valida un bloque, se gana 12.5 BTC.

Entonces 12.5 BTC se distribuyen a cada 10 minutos. Esta

recompensa se mantiene durante 4 años, período después del

cual esa minería cae a la mitad. Debemos recordar que los

mineros ganan las comisiones de validación de los bloques

también. Estas comisiones están determinadas por el

mercado. Es posible que un usuario elija no pagar nada de

tasa, pero tiene grandes posibilidades de que su transacción

no se valide de esta manera, porque la

competencia de los

usuarios para tener sus transacciones validadas hoy es grande,

y la capacidad del bloque es limitada.

Volviendo al ASIC, la unidad más avanzada y

eficiente de Bitmain llama a Antminer S9, y tiene poder de

procesar 14 TeraHashes (TH) por segundo. Esto significa que

el equipo puede probar 14 billones de hash en un segundo. El

equipo demanda 1375 Watts para funcionar. Por lo tanto, si

permanece conectado 24 horas al día, gasta 33 kWh al día.

Esta relación de TH X Watt es la mejor del mercado. Esto

significa que es el equipo que consume menos energía para

calcular un hash, y al mismo tiempo es más rápido también.

Por otro lado, es el equipo más caro, costando cerca de 3.000

dólares estadounidenses. Además, el

equipo es grande,

pesado, y emite mucho ruido y calor, no siendo cómodo

dejarlo funcionando en su sala de estar, por ejemplo.

Debido a esta eficiencia y rapidez del ASIC, la

dificultad de la red ha aumentado mucho, lo que significa que

ya no es posible minar con CPU o incluso GPUs, en el caso

de Bitcoin, pues se gastaría más energía de lo que se ganaría

en criptomonedas. Afortunadamente, hay monedas que tienen

el algoritmo de minería ajustado para ser resistente a las

ASIC, por lo que pueden ser minadas con GPU. La minería

con CPU hoy sucede más por hobby de los participantes de la

comunidad, por no ser eficiente ni lucrativo. Hay también

monedas no minerables, que se emiten de otras formas

distintas de la minería, o que no se

emiten en absoluto.

Minerar solo es un poco como jugar en la lotería.

Suponiendo que usted compra una unidad de Antminer S9,

Cuando usted encuentra un hash, ganará mucho dinero. Pero

tardará algunos años hasta encontrar unohash, si encuentra.

Por eso, las personas hoy minan en los llamados *pools*. Usted

puede comprar el equipo y conectarse a una red de

procesamiento con otros mineros. De esta forma, cuando un

minero del grupo encuentra un hash, divide la recompensa

entre todos del grupo, disminuyendo la recompensa por

validación del usuario individual, pero haciendo el tiempo de

validación esperado mucho más previsible, y también

haciendo las validaciones más frecuentes.

En el caso de minería en *pool*, todavía

existe otra

opción, que es alquilar el equipo de minería de una empresa

que ya tiene una estructura montada, y así participar del *pool*

organizado por la empresa. De esta forma, el usuario no tiene

el trabajo de montar el equipo, ni de mantenimiento, y

tampoco tiene el costo de energía. Por lo tanto, el usuario

compra por un determinado período de tiempo el poder de

procesamiento en posesión de la empresa.

Recomendamos investigar bien antes de entrar en un

pool de minería en el que se alquila poder de procesamiento,

ya que hay muchas empresas de fachada que son fraudes.

Una empresa legítima de minería en grupo que alquila poder

de procesamiento llama Genesis Mining

(https://www.genesis-mining.com/).

Cálculo Del Beneficio De La Minería

Aqui tenemos un ejemplo de cálculo de rentabilidad de

minería, asumiendo algunas premisas.

Dificultad de la Red: 13.823.824.128 GH / s

Tasa de aumento de dificultad en la red al día: 0%

Costo del equipo: 3.000 USD

Capacidad de procesamiento del equipo: 14.000 GH / s

Potencia del equipo: 1375 watts

Precio BTC: 15.000 USD

Recompensa del bloque: 12,5 BTC

Frecuencia del bloque: 10 minutos

Costo de la energía: 0,20 USD / kWh

Primero encontramos cuánto de procesamiento estamos

contribuyendo a la red porcentualmente. Por lo tanto,

hacemos 14.000 / 13.823.824.128 = 0,0001%

Después, encontramos cuántos BTC son minados en el día:

12,5 BTC / 10 min = 75 BTC / hora = 1.800 BTC / día

Si un BTC vale 15.000 USD, la recompensa de la red es de

1.800 X 15.000 = 27.000.000 USD / día

0,0001% de 27.000.000 USD = 27 USD por día de

recompensa.

Ahora, en relación con los costes:

Consumo de energía: 1375 vatios X 24 horas = 33.000

WattHora = 33 kWh

33 kWh / día X 0,20 USD / kWh = 6,6 USD / día

Por lo tanto, tenemos un beneficio neto por día de 27 - 6,6 =

20,4 USD / día.

Considerando que pagamos 3.000 USD en el equipo, tardar

3.000 / 20,4 = 147 días aproximadamente para recuperar la

inversión.

147 días para el 100% de retorno en la inversión es un

número muy atractivo. Recuerde que estamos asumiendo que

participamos en un *pool* que paga diariamente. En el caso de

que se haga solo, el pago diario no se produce de esta forma.

Podemos ver por qué hay tantas personas minando los bits.

Pero no todo es perfecto. Nuestras premisas asumieron un 0%

de aumento en la dificultad de la red y que el precio de la

bitcoin se estable en estos próximos 147

días. Lo que sucede

en realidad es que el retorno no es tan bueno, porque

seguramente será más difícil minar en el futuro. ¿Cómo

sabemos? Justamente porque el beneficio es grande, lo que

acaba por atraer a más mineros. Con más mineros en la red, el

beneficio por minero acaba por caer, hasta un momento que

no valga más la pena minar. Es una carrera para ver quién

consigue minar primero.

La otra variable es el precio. Si el precio de la bitcoin

cae, puede ser que mañana la minería no sea más lucrativa.

Esto a largo plazo causará una salida de mineros de la red, y

así será más fácil de minar, elevando de nuevo la

rentabilidad. Por otro lado el precio sube, los 147 días pueden

disminuir.

Ganando en Alta y Baja

Ya debes haber entendido hasta aquí cómo ganar dinero con

criptomonedas cuando suben, simplemente comprar en un

valor y vender cuando ese valor sube. Pero, ¿y si usted no

cree mucho en el concepto de las criptomonedas, piensa que

realmente es una burbuja y que es cuestión de tiempo hasta

que el precio caiga bruscamente, es posible ganar dinero

cuando el precio de algo cae? La respuesta es sí.

La forma más habitual de ganar dinero en el mercado

financiero cuando el precio de algo cae es vendiendo

contratos futuros de aquel producto. Vamos a hablar aquí un

poco sobre este tipo de contrato.

Contrato futuro es un instrumento financiero que sirve

como seguro para garantizar el precio de un bien en una fecha

en el futuro. Vamos a pensar, por ejemplo, una empresa de

Brasil que importa máquinas de Estados Unidos y paga el

proveedor en tres cuotas mensuales en 30, 60 y 90 días.

Vamos a suponer que la empresa importó una máquina que

cuesta 300 mil dólares y va a pagar tres parcelas de 100 mil

dólares. Vamos a suponer también que

el tipo de cambio

actual sea 1 dólar = 3 reales. Si el tipo de cambio sigue igual,

serían tres pagos de 300 mil reales. Pero, si el tipo de cambio

es de 3,20 o 3,50? Los pagos continuarían en 100 mil dólares,

pero en real serían de 320, 350 mil reales. Estos aumentos

pueden acabar con el beneficio de la empresa o peor, causar

grandes pérdidas.

Para evitar los riesgos de esta oscilación, la empresa

importadora puede comprar un contrato futuro y garantizar la

compra de dólares a una tasa fija. Es decir, paga un pequeño

valor sobre los 300 mil dólares para garantizar el tipo de

cambio. En la práctica, ella va a una bolsa de futuros (en

Brasil es la BM&F) y compra 100 mil dólares a ser

entregados en 1 mes a una tasa pre

establecida. Si el cambio

es 1 dólar = 3 reales, puede comprometerse a pagar 3,05

reales en la fecha final. Esta diferencia entre el valor actual y

el futuro es el beneficio de la parte que vende el contrato. Si

realiza esta operación para los tres meses que tiene pagos

pendientes, fija exactamente cuánto va a gastar en reales. Si

el precio del dólar sube, no pagará más por ello.

Y si la cotización del dólar cae en lugar de subir,

yendo de 1 USD = 3 reales a 1USD = 2,50 reales? Si el

importador compró el contrato para pagar 3,05 reales por

dólar en 30 días, está obligado a comprar estos dólares a esa

tasa, incluso si el valor presente es menor.

Si el contrato es a "termino" (nomenclatura adoptada

en el mercado financiero), esta

transacción se produce sólo en

la fecha final, independientemente de las oscilaciones entre

las fechas inicial y final. Si el contrato es un futuro normal, ni

una parte ni la otra necesitan mover una enorme cantidad de

dólares. Lo que sucede es un ajuste diario según ocurren

variaciones de precio.

Continuando el ejemplo de la empresa importadora. Vamos a

suponer que ella compró 100 mil dólares en contrato futuro.

Tenemos la siguiente situación:

Valor principal 100 mil dólares, cambio 1 USD = 3 BRL

Supongamos que el día 1 el tipo de cambio passa a 1 USD =

3,10 reales, luego a 3,20 al día siguiente y así sucesivamente.

Dia

0

1

2

3

4

Tipo de cambio

3,00

3,10

3,20

3,50

3,40

Valor em reales 300.000

310.000

320.000

350.000

340.000

Diferencia

-

R$ 10.000 R$ 10.000 R$ 30.000 -R$ 10.000

Es posible notar que existen diferencias diarias entre el

valor total en reales. En los contratos

futuros, cuando ocurren

esas oscilaciones, una parte paga la diferencia a la otra al

final de cada día. De esta forma, no es necesario comprar

todos los dólares y pasarlos de mano en mano, sino que las

partes paguen entre sí el valor referente a la oscilación diaria.

En el ejemplo, el comprador de los contratos recibiría

del vendedor 10 mil reales el primer día, después 10 mil más

en el segundo, después 30 mil en el tercero y tendría que

pagar 10 mil al vendedor el cuarto día. Los ajustes van en esa

lógica hasta la fecha de vencimiento del contrato. En la

práctica las oscilaciones no son tan exageradas como en el

ejemplo, entonces para garantizar que esos ajustes se hacen

todos los días, basta que cada parte de la negociación haga el

depósito de una parte del valor total

como garantía y todo ese

sistema queda bajo custodia de la bolsa (que hace los pagos

entre las partes todos los días).

El valor depositado es el margen de seguridad y puede

variar de acuerdo con el tiempo, según criterios definidos por

la bolsa. De esta forma, si usted quiere comprar 100 mil

dólares en contratos futuros, necesita depositar, en

condiciones normales, aproximadamente el 15% del valor

total. Este valor es para contratos de bienes cuyos precios

oscilan más, como el dólar, y aproximadamente el 5% para

bienes agrícolas como la soja y el maíz. Con eso, para

protegerse contra la oscilación de 100 mil dólares, sólo tienes

que tener el 15% de ese valor depositado en una cuenta en la

bolsa.

Este principio se llama apalancamiento y facilita la

participación de operadores menores en el mercado futuro.

Esta operación es un juego de suma cero, lo que un lado gana

el otro necesariamente pierde y cualquier persona que posea

el valor del margen de seguridad puede operar comprando y

vendiendo esos contratos.

El precio de los contratos futuros se otorga, en

condiciones normales, por el tipo de interés relativo al

período entre el inicio y el final del contrato. Es decir, si entre

hoy y el vencimiento del contrato futuro la tasa de interés de

referencia es del 1%, entonces el precio del contrato futuro

será de aproximadamente el 1% del valor total. En la práctica

no es tan simple, porque los tipos de interés como referencia

cambian de acuerdo con el país de la

negociación, cuando el

contrato futuro implica dos monedas diferentes, los tipos de

interés de las dos entra en el cálculo y a veces los precios se

escapan momentáneamente a esa lógica por eventos como

guerras, anuncios de cambio en políticas públicas o embargos

económicos a países exportadores de petróleo como Irán.

Cuando el precio de un contrato futuro está por encima

o por debajo del valor que reflejaba el tipo de interés durante

el período de vigencia de este contrato, surgen oportunidades

para el arbitraje. Sin entrar mucho en detalles sobre ese tipo

de contrato (al final ese libro es sobre criptomonedas y no

derivados), arbitraje es cuando surge la oportunidad de

realizar operaciones que posibilitan ganancias sin riesgo. En

general, las operaciones de arbitraje

implican la compra y

venta de varios activos y contratos diferentes al mismo

tiempo para compensar una variación de precio entre activos

que tienen una relación directa entre sí. Por ejemplo, el barril

de petróleo en la bolsa de Londres y en la bolsa de Chicago.

Si el precio entre los dos no es muy cercano, un inversor

puede comprar barriles en la bolsa en que sea más barata y

vender en la bolsa más cara. Como hay miles de personas

mirando los valores de estos contratos 24 horas por día, los

precios entre ellos acaban quedando siempre muy cerca, pues

cuando surge una diferencia rápidamente algún inversor

profesional entra arbitrando y eso trae los precios nuevamente

al equilibrio.

Con ello, los precios entre contratos futuros y valores a

la vista de los bienes tienden a estar siempre próximos y

estables. Si mucha gente compra algún contrato futuro, el

precio a la vista es influenciado y lo contrario también.

En el mundo, es posible comprar contratos futuros de

gran variedad de monedas, metales (oro, hierro, aluminio,

uranio, etc.), productos agrícolas (soja, maíz, azúcar, café)

títulos de deuda pública, índices de

bolsas de valores (Dow

Jones, S&P 500), combustibles (gasolina, etanol, petróleo

diesel), petróleo (barril Brent y WTI) y prácticamente

cualquier commodity que se negocia en gran cantidad. En el

mundo, las principales bolsas que negocian este tipo de

mercancía en contrato futuro son el Chicago Mercantile

Group (que unificó las principales bolsas de Estados Unidos),

la National Commodity and Derivatives Exchange de la

India, Moscú Exchange, Shangai Futures Exchange, Eurex y

la BM&F en Brasil.

En diciembre de 2017, dos de las mayores bolsas de

Estados Unidos, la CBOT y la CME, abrieron negociación de

contratos futuros de bitcoins. Esto trae gran legitimidad al

bitcoin y a las criptomonedas en general, pues aumenta el

alcance de inversores tradicionales a ellas y representa el

reconocimiento de los mayores organizadores de mercados

financieros del mundo en ese mercado. Inversores

conservadores consideran que esas bolsas no abrirían

contratos futuros de activos que fueran sospechosos o

fraudulentos. El resultado inmediato de la apertura de estos

contratos fue un fuerte aumento de

precios en las dos

semanas después de la apertura.

Ahora que usted ha entendido como futuros funcionan,

vamos a explicar en líneas generales cómo hacer para

conseguir de hecho operar en este mercado. En primer lugar,

los contratos futuros requieren un valor mínimo para operar.

Los futuros no son tan fraccionables como los bitcoins reales.

Hasta 2017, sólo la CBOT y CME ofrecían ese tipo de

contrato, ambas en Chicago, Estados Unidos. En el futuro, las

bolsas más pequeñas pueden decidir poner a disposición

contratos futuros de BTC, pero mientras tanto, los inversores

del mundo entero sólo tienen a Estados Unidos como opción

para operar este contrato.

La primera cosa que hay que tener en mente es que

para operar futuros, se necesita un volumen mayor de

disponibilidades. El tamaño del contrato de bitcoin en la

CBOE es 1 BTC, y en la CME 5 BTC. En la CME, la

fluctuación mínima es de $ 5 por bitcoin, o $ 25 por contrato.

A pesar de que el inversor no necesita todo ese dinero,

debido a la posibilidad de operar con margen, el riesgo es

grande para quien no tiene mucho

dinero. Debido a la

volatilidad del BTC, la exigencia de margen es del 43% del

valor del contrato, muy por encima del promedio de otros

futuros. También existen límites en la variación de precio del

7%, 13% y 20%. Cuando se alcanzan estos límites, el circuito

de interrupción se activa y las negociaciones se paralizan

durante un período de tiempo. Estos interruptores no existen

en las bolsas de BTC spot.

Los contratos futuros de bitcoin negociados en la CME

y CBOT no tienen liquidación física, es decir, no es necesario

poseer una cartera digital para operar el contrato. Toda la

liquidación se produce por diferencia financiera. Los

contratos futuros toman como referencia los precios de

bitcoin negociados en GEMINI, creada por los hermanos

Winklevoss, que tienen la ambición de convertirse en una

bolsa que atiende a los más altos niveles regulatorios, a

inversores persona física y que también institucionales.

Para operar en las bolsas de Chicago es necesario que

el inversor tenga una cuenta en una correduría americana

tradicional, es decir, una correduría de valores como acciones

y futuros. Recomendamos al inversor

hacer su propia

investigación sobre dónde abrir una cuenta, pero una

recomendable es la Interactive Brokers

(https://www.interactivebrokers.com/en/

Esta corredera presenta bajos costos de corretaje y

ofrece una amplia gama de bolsas que se pueden acceder

alrededor del mundo. Esta correduría permite acceder a

mercados de títulos de gobierno,

acciones, futuros, ETFs,

opciones, y productos estructurados de regiones como

EE.UU., Canadá, Japón, Hong Kong, Singapur, Australia, y

varios países de Europa.

A pesar de estas ventajas, es una correduría indicada

para el inversionista más experimentado que sabe lo que está

haciendo, y preferentemente que sabe Inglés, pues no ofrece

servicios de asesoramiento para donde invertir, o cómo

funcionan ciertos productos financieros. Si el inversor opta

por utilizarla, se recomienda que tenga un cierto espíritu

autodidacta y que dispuesto a desafíos.

Para abrir una cuenta en esta correduría no es

necesario ir a los Estados Unidos personalmente o tener una

cuenta bancaria en el país extranjero. Tener una cuenta

corriente en banco en los EE.UU. ciertamente facilita el

proceso, pero no es obligatorio. El dinero puede ser enviado

directamente de una correduría de cambio brasileña o banco

brasileño para la correduría estadounidense, a través de una

transferencia internacional. El dinero en la transferencia

internacional tarda de 2 a 5 días laborables para llegar,

dependiendo de los bancos

involucrados. Para traer el dinero

de vuelta es el mismo proceso. Se debe pedir un saque en

forma de transferencia internacional de la correduría a su

banco local.

Capítulo VI

¿Cuáles Son Los Riesgos De Las

Criptomonedas?

“We have elected to put our money and faith in a

mathematical framework that is free of politics and human

error.”

"Elegimos poner nuestro dinero y fe en una estructura

matemática libre de política y errores humanos"

Tyler Winklevoss, co-criador do Facebook

Tipos de Riesgos

Cuando hablamos de bienes y productos de mercado

financiero existen dos tipos de riesgos, el sistemático o no

diversificable y el riesgo no sistemático, o diversificable.

Riesgo no diversificable es aquel que afecta todo el ambiente

de negocios al mismo tiempo, como una crisis económica

mundial de grandes proporciones. En

estos casos, incluso si

usted divida su dinero entre diferentes bienes y productos, no

evitará pérdidas.

El riesgo diversificable es el específico de una

inversión. Por ejemplo, piense en una inversión en empresas

del sector petrolero. Una caída en el precio internacional del

barril hace caer el beneficio de las empresas de ese sector,

pero no influye significativamente en otros sectores como

empresas de tecnología de información o de comercio online.

Si un inversionista compra acciones de empresas de varios

sectores diferentes, está diversificando el riesgo, pues si un

sector sufre alguna pérdida específica, los demás no están

sujetos a las mismas oscilaciones.

En las criptomonedas, el riesgo no diversificable es

que todo el sistema sufra algún tipo de colapso o que todos

los países del mundo decidan simultáneamente prohibir su

uso. Se trata de un riesgo muy bajo en virtud de que la

tecnología de las criptomonedas se piensa exactamente para

evitar este tipo de problema y la naturaleza autónoma y

pública de la criptografía. A pesar de la ocurrencia de

episodios puntuales de ataques de

hackers a empresas que

comercializan monedas digitales, no se trata de riesgo capaz

de afectar todo el sistema. Es mayor el riesgo de que los

gobiernos se sienten amenazados por las criptomonedas y que

quieran prohibir su uso para evitar la evasión fiscal. Sin

embargo, hasta 2017, pocos países democráticos prohibieron

el uso de las criptomonedas. En 2013 China prohibió que las

instituciones financieras hagan transacciones en moneda

digital, pero las personas físicas pueden utilizarlas

libremente. Estados Unidos y la Unión Europea no tienen

restricciones. En Brasil, el Banco Central emitió un

comunicado en 2017 alertando sobre riesgos de las

criptomonedas, pero sin ejercer ningún tipo de actividad

regulatoria sobre ellas.

En cuanto al riesgo diversificable, podemos establecer

un paralelo entre las criptomonedas y las acciones. La acción

representa una pequeña fracción de la propiedad de una

empresa. Si el inversor compra, por ejemplo, acciones de

empresas del sector bancario, de bebidas y de empresas de

tecnología al mismo tiempo, diversificará el riesgo de pérdida

en caso de choque en un sector

específico. La lógica es la

misma con las criptomonedas. Así como los inversores

pueden comprar varias acciones diferentes, también pueden

comprar varias criptomonedas diferentes, ya que sus precios

no están directamente relacionados. Así, si una criptomoneda

pierde valor, las demás no seguirán el mismo patrón (excepto

cuando la causa de la caída sea sistémica y haya prohibición

de uso de todas las criptomonedas). Es posible diversificar el

riesgo de las criptomonedas a través de la compra de algunas

de ellas al mismo tiempo.

Riesgos De Comunes A Todos Los Activos

Cualquier bien cuyo precio se negocia libremente en un

mercado ofrece riesgo a su propietario. Hasta la compra de un

coche usado o de un inmueble ofrece riesgo al inversor, ya

que el precio puede caer. Por lo tanto, el riesgo es un factor

inherente a cualquier bien cuyo valor puede variar.

En mercados financieros, hay una infinidad de

contratos que no necesariamente implican la compra de un

producto, pero representan una forma de seguro vinculado a

la oscilación de precios. Es el caso de las opciones y de los

contratos futuros. Estos contratos sirven,

en general, para

ayudar a los productores y compradores a protegerse de la

oscilación de los precios de mercado. Por ejemplo, un

granjero que planta soja puede comprar un contrato que fije,

en una fecha en el futuro, el precio que va a vender su

cosecha de soja, garantizando así sus ingresos de venta.

Existen también agentes, como los propios bancos, que

compran o venden esos contratos sin tener ninguna relación

con los productos negociados. Usted no necesita ser un

granjero para ganar dinero con la oscilación del precio de la

soja o del maíz. Usted puede apenas ser el vendedor del

seguro y ganar dinero en caso de que el comprador nunca

utilice el servicio. Hoy, existe gran facilidad para que

personas físicas y jurídicas negocien

contratos de ese tipo.

Esto facilita que los especuladores dispuestos a correr muy

riesgo o con poco conocimiento entren en el mercado y

pierdan dinero. A pesar de las facilidades tecnológicas, estas

pérdidas existen desde hace siglos, como la burbuja

financiera de los tulipanes en Holanda en el siglo XVII, la

crisis de 1929 y la crisis del subprime en 2008.

El Concepto De Liquidez

Sin embargo, al mismo tiempo que operar en mercados

financieros crea un riesgo de pérdida, la existencia de un

número enorme de personas vendiendo y comprando

instrumentos financieros posibilita algo muy positivo, que es

la liquidez. De forma simplificada, la liquidez es cuando un

bien se convierte en dinero vivo. Por ejemplo, una plantación

de maíz tiene baja liquidez, pues sólo puede convertirse en

dinero vivo cuando se vende en la época de la cosecha. Una

acción puede tener alta o baja liquidez, dependiendo de la

facilidad con que las personas puedan negociarlas. Las

acciones de Cemex, por ejemplo, son muy líquidas, en pocos

segundos es posible venderlas y

transformarlas en dinero

vivo. Las acciones de algunas empresas pequeñas pueden ser

poco líquidas, o sea, puede ser que demore mucho hasta que

aparezca algún inversionista queriendo comprarlas.

Las principales criptomonedas, como la bitcoin,

litecoin y ethereum poseen alta liquidez, o sea, no es difícil

encontrar a alguien queriendo negociarlas. Hay otras, sin

embargo, que pueden tardar más para ser vendidas. Si un

inversor tiene criptomonedas de baja liquidez y necesita

venderlas rápidamente, tal vez se vea obligado a bajar mucho

el precio para poder negociarlas o aún puede que muchas de

estas criptomonedas no sean aceptadas por otras personas a lo

largo del tiempo, perdiendo valor de transacción.

Algunos "expertos" critican instrumentos

financieros

(acciones, contratos futuros, opciones y criptomonedas)

acusándolos de ser la causa de especulaciones negativas a la

población. Esta crítica parte de personas que no entienden

cómo funcionan los mercados libres y los enormes beneficios

que ellos roporcionan a las empresas, al gobierno y la

población.

También sobre los riesgos de las criptomonedas

comunes al mercado financiero, existe la oscilación abrupta

de precios, conocida como volatilidad. Esto puede ocurrir

cuando algún hecho relevante afecta el precio de un bien

cualquiera. En el caso de las empresas, eventos como

desastres ambientales, guerras, fusiones o adquisiciones, un

anuncio de ganancias inferiores a lo

previsto, entre varios

otros motivos pueden dejar los inversores desconfiados y

llevarlos a vender sus acciones. Estos acontecimientos

pueden causar una gran variación rápida de precios. A veces

los precios oscilan sin razón aparente, lo que también es

normal.

Otro riesgo bastante común es la manipulación de

precios. La historia está repleta de episodios en los que los

precios se vieron afectados de forma deliberada por personas

que querían beneficiarse de eso. La forma más común es

cuando alguien compra gran cantidad de un producto

elevando su precio artificialmente y luego vende a un precio

más alto. Esto puede ocurrir con acciones de empresas y

commodities como soja y hierro, pero

también con monedas

extranjeras (algo que los gobiernos de países grandes hacen

constantemente). La manipulación también ocurre fuera del

mercado financiero, por ejemplo, con especuladores de obras

de arte que compran pinturas de artistas fallecidos en subastas

para forzar un aumento de precios e incluso con inmuebles,

como cuando una constructora compra terrenos y casas en un

barrio cuando descubre que una estación de metro será

construida en la región.

La manipulación de precios no es exclusiva de los

mercados financieros ni de las criptomonedas, es algo que

puede suceder con cualquier objeto que pueda ser negociado.

Esto nos lleva a otro riesgo, el de burbuja especulativa.

Podemos definir burbuja como un período en que ocurre un

gran aumento de precio de un producto seguido de una rápida

devaluación. Las burbujas pueden ocurrir por varias causas,

siendo la especulación más común.

Las burbujas también pueden ocurrir por exceso de

optimismo, facilidad de crédito (como ocurrió en la crisis del

subprime en los Estados Unidos en 2008), efecto manado

(*herd behaviour*), en que grupos de personas empiezan a

actuar de la misma forma sin una causa racional, por

información asimétrica y, por último, debido a la búsqueda de

un activo como reserva de valor. Tal vez sea la razón que

mejor explica el aumento de precio de las criptomonedas, a

pesar de que es imposible decir con certeza.

Riesgos Específicos de las Criptomonedas

En mercados libres y competitivos, es

decir, aquellos en los

que ningún participante es capaz de influir en los precios

actuando solo, es imposible predecir con exactitud lo que va a

suceder con el precio de un bien. La gente hace apuestas

cuando compra algo esperando que el precio suba. Esta es la

esencia de cualquier mercado, comprar algo esperando que el

precio suba para vender después. Es en esta etapa que se

encuentra el mercado de monedas digitales. Hay millones de

participantes que transaccionan constantemente, el precio de

las monedas flota libremente y sin una autoridad central para

controlar o garantizar las reglas. No hay evidencias hasta el

presente de que los bitcoins, o las otras criptomonedas

importantes, estén cambiando de precio debido a alguna

forma de manipulación. Incluso porque

la información sobre

la minería y las transacciones son públicas, entonces algún

intento de manipulación o fraude sería identificado en poco

tiempo por todos los negociadores.

Es posible que haya una burbuja especulativa con la

bitcoin y demás criptomonedas? Sí. Esto ha ocurrido varias

veces en la historia con inmuebles, acciones (empresas de

tecnología en la llamada burbuja del mercado punto-com),

monedas extranjeras, metales preciosos, objetos de arte y los

tulipanes holandeses. ¿Es posible estar seguro de que se trata

de una burbuja? No, a partir del momento en que la mayoría

de los participantes en el mercado cree que el precio de un

activo está excesivamente valorado, o pasa a creer que el

precio va a caer, esto se convierte en

una profecía auto

realizable y el precio de hecho cae.

Estamos hablando aquí de aspectos mucho más

psicológicos que objetivos. Daniel Kahneman ganó el premio

Nobel de economía en 2002 por su investigación sobre

aspectos psicológicos y conductuales en las finanzas. Al

contrario de lo que asumen las premisas clásicas de la teoría

económica, Kahneman afirma que el comportamiento de los

inversores no es exactamente racional, sino influenciado por

una gran diversidad de sentimientos y juicios que varían

mucho de acuerdo con la situación e interpretación que el

individuo tiene del contexto en que está insertado.

Algunos

analistas

de

mercado

financiero,

especialmente aquellos vinculados a bancos, afirman que el

mercado de criptomonedas está en una situación de burbuja,

pero esa opinión no es consensual, pues si fuera el precio ya

habría caído drásticamente. Hasta el momento en que ese

libro fue escrito, el precio de las

criptomonedas continúa en

un nivel alto a pesar de la gran oscilación de cotización. Las

demás monedas importantes también presentan oscilaciones

variadas, sin una tendencia evidente de caída para todas al

mismo tiempo.

Riesgos de Tributación y Regulación Adversa

Un riesgo bastante real es que, con el tiempo, los gobiernos

empiecen a imponer restricciones sobre las criptomonedas,

especialmente si se convierten en una forma popular de

ocultar el patrimonio o realizar transacciones sin pagar

impuestos. En algunos países ya existen restricciones, a veces

sólo para empresas y bancos, en otros casos también para

personas físicas.

La tributación sobre criptomonedas aún no es una gran

preocupación de los gobiernos, principalmente porque

políticos y burócratas difícilmente entienden lo que

significan, pero es un tema con potencial para traer dolor de

cabeza al poder público. Una transacción en criptomoneda se

realiza directamente entre dos partes, no dejando ningún tipo

de registro nominal o supervisión para árbitro o supervisor.

De

esta

forma,

los

gobiernos,

que

se

financian

mayoritariamente con impuestos sobre la renta y el consumo,

no tienen medios de monitorear las transacciones y, en

consecuencia, tributarlas.

En el momento, las criptomonedas todavía son una

pequeña fracción del dinero disponible en el mundo y pocas

son las empresas no conectadas a internet que la aceptan

como moneda para transacciones corrientes. Imaginemos, sin

embargo, que en el futuro todas las tiendas, empresas y

prestadores de servicios del mundo acepten criptomonedas. Si

el gobierno tiene problemas, pues no podrá monitorear, por

medio del servicio de administración tributária o cualquier

otro órgano de control, cuánto una empresa vendió y no

tendrá base para tributarla. La eventual popularización de las

criptomonedas dificultaría mucho la vida de los fiscales de

impuestos, pues no existe obligatoriedad, en la lógica de

blockchain, que alguien se identifique

ante las autoridades

para rendir cuentas de transacciones.

El anonimato de las criptomonedas nos lleva a un

segundo gran problema para el poder público: el pago de

actividades ilícitas y criminales. Como las monedas virtuales

pueden ser transacionadas sin dejar rastros, ellas sirven para

el pago de actividades criminales. El tráfico de drogas, armas,

robos y cualquier otro delito puede ser pagado con

criptomonedas sin que los gobiernos tengan ningún control

del origen y destino de los recursos, y peor, no saben ni el

objeto de la transacción. Algunas monedas se crean con la

intención de permitir el anonimato total a sus poseedores y

esto puede aumentar mucho la integración y el poder del

crimen organizado. Al mismo tiempo,

dificulta que la policía

y la justicia consigan establecer el nexo causal de

infracciones, o sea, identificar la conducta que caracteriza

crímenes. Cuando grandes bandas y traficantes comienzan a

realizar transacciones en criptomonedas, el poder público

tendrá el gran desafío de identificar y caracterizar crímenes.

Un camino posible para evitar que esto suceda es

intentar prohibir totalmente el uso de las criptomonedas. Sin

embargo, una prohibición total es poco probable para las

personas físicas, aunque establecida en ley, debido al carácter

descentralizado y anónimo de la tecnología. Los gobiernos

también reconocen la importancia de esta innovación

tecnológica, y por eso no quieren prohibirlas.

Si el gobierno de algún país grande,

como Estados

Unidos o China, decida prohibir transacciones con

criptomonedas, es probable que su precio caiga. En

economía, el surgimiento de alguna legislación contraria a los

intereses de un sector se llama regulación adversa. A pesar de

ser un riesgo posible, existen criptomonedas que garantizan el

secreto absoluto a su poseedor. Si los gobiernos comienzan a

imponer restricciones burocráticas o impuestos sobre el uso

de criptomonedas, los desarrolladores de tecnología acabarán

encontrando medios para continuar promocionándolos,

especialmente por la ventaja de no depender de una autoridad

reguladora central.

Todavía hay muchas críticas de que las monedas

virtuales serían un tipo de esquema fraudulento, pero ya

aclaramos que no es el caso. Sin embargo, existen riesgos de

que algunos de los cientos de criptomonedas disponibles no

sean totalmente confiables. No se trata de un fraude en el

concepto de criptomoneda, sino en los criterios de desarrollo

de alguna de ellas. Las bitcoins se componen o se minan de

forma transparente y constante con un número finito que se

va a emitir. Es posible, sin embargo, que

alguna otra moneda

inicie la negociación pública con buena parte del total posible

ya minado, lo que sería una forma de adquirir ventaja sobre

los demás entrantes.

Sin embargo, si las demás monedas siguen el patrón de

blockchain establecido inicialmente por Bitcoin, será posible

que todos en el mercado sepan cuánto de la moneda ha sido

emitido y cuánto está por ser emitido y si, aún así, las

personas deciden entrar en el mercado, elección o falta de

información de las mismas. En el mundo de las

criptomonedas, no sirve procesar a nadie en caso de pérdida o

robo, no hay autoridad regulatoria, los participantes son

totalmente responsables de sus ganancias y pérdidas.

Riesgos Vinculados Al Robo Físico

Ya sabemos que el acceso a la cartera de criptomonedas se

realiza de forma personal en un ordenador a través de una

clave. El sistema de criptografías impide que la moneda sea

robada por medio de transferencias, pero es posible robar la

clave personal que da acceso a la cartera. En caso de pérdida

o extravío de la llave, las monedas asociadas a esa cartera se

pierden para siempre.

Lo que ya sucedió de hecho es el robo de la clave

física. Es decir, un ladrón que invade una casa y roba el un

memory stick con el código impreso de acceso puede obtener

las criptomonedas sin que nadie pueda identificarlo. El robo

pasa a ser una preocupación del mundo físico y mucho menos

en el mundo digital. Es algo similar a un robo de barras de

oro. El ladrón puede llevar el metal,

derretirlo y venderlo

como joyas por ejemplo. No hay como probar que aquel

metal pertenecía anteriormente a una persona.

De esta forma, el mayor riesgo de robo de

criptomonedas se da en el mundo físico. Incluso los casos

informados de ataques de hackers ocurren a través del robo

de la clave de acceso a carteras, y no por medio de

transferencias entre cuentas, como puede ocurrir en el sistema

bancario convencional.

Robo Por Ataque de Hackers

El riesgo de ataques de hackers es real y ha ocurrido algunas

veces contra empresas que transforman criptomonedas,

llamadas genéricamente de corredoras. El robo no ocurre, sin

embargo, por medio de quiebra de la criptografía y sí por el

robo de la clave que da acceso a la cartera. Algunos casos

conocidos sobre robos de criptomonedas no fueron

totalmente aclarados, pues las empresas que realizan las

transacciones no están reguladas y, en general, no tienen

compromiso de rendición de cuentas o transparencia ante el

poder público. Muchas de ellas cerraron, exponiendo falta de

confiabilidad y de mecanismos de seguridad digital, además

de imponer pérdidas significativas para

los propietarios.

Para prevenirse contra un ataque de este tipo, es

recomendable que el propietario de las criptomonedas evite

usar servicios de custodia de corredores, que compran y

guardan criptomonedas a terceros sin ningún tipo de

fiscalización o control, y aprendan los mecanismos para

negociación y compra por cuenta propia . El propietario de

criptomoneda que mantiene su clave en lugar seguro contra

robos físicos corre poco riesgo de ser robado de forma digital.

Criptomonedas Como Pago Para Los Secuestradores

Existen casos noticiados en diversos medios de comunicación

sobre programas de computadora maliciosos usados como

forma de secuestro contra organizaciones. En general, el

modo de operación de los

secuestradores es infectar el

sistema deseado con algún tipo de virus o software de control

remoto y exigir que se efectúen transferencias de valores en

criptomonedas para que el ataque sea revertido.

Peor que eso, secuestros de la vida real exigen cada

vez más a menudo el pago de rescate en bitcoins, debido a la

dificultad de rastrear al receptor. Casos fueron reportados en

varios países, como Hong Kong, Costa Rica y Brasil. En la

mayoría de los casos, una cuadrilla realiza el secuestro

personal de empresarios, ejecutivos o miembros de sus

familias. El crimen de secuestro continúa practicado de la

forma ya conocida, lo que cambia es la solicitud de pago.

Robo De Bitcoins

Hay varios casos de robos de criptomonedas que

se han vuelto públicos, en general contra empresas que

negocian para terceros, como las bolsas o corredoras de

criptomonedas. Algunos de esos robos llevaron lasa

autoridades nacionales a pensar en algún tipo de

regulación para impedir el uso de las

monedas virtuales

en operaciones criminales o ilegales, pero todavía

existen medios para ocultar esos robos.

En diciembre de 2017 la empresa surcoreana de

transacciones de criptomonedas Youbit sufrió un ataque

por internet y perdió aproximadamente el 17% de los

valores que administraba. La empresa fue obligada a

declarar la quiebra, devolviendo sólo el 75% del valor de

las criptomonedas para los clientes. Varios medios de

comunicación declararon la sospecha de que hackers a

servicio de Corea del Norte habrían sido los

responsables del robo. No hubo aclaración oficial sobre

cómo ocurrió el ataque.

En Corea del Sur, las criptomonedas han crecido

en popularidad, siendo aceptadas en cada vez más

establecimientos comerciales y negociadas por

personas sin conexión profesional con el mundo

tecnológico. Esto llamó la atención de las autoridades

locales contra posibles fraudes semejantes, pues un

eventual ataque al mercado de criptomonedas puede

resultar en grandes pérdidas para una

parte significativa

de la población del país.

Otro caso muy significativo de fraude y robo de bitcoins

ocurrió en la correduría Mt.Gox, ubicada en Tokio,

Japón. Fundada en el año 2010, entre 2013 y 2014 fue la

mayor bolsa de negociación de bitcoins del mundo,

llegando a transaccionar el 70% de todas los bitcoins

disponibles hasta entonces. En 2014, sin embargo, la

empresa suspendió las negociaciones e inició el proceso

de liquidación judicial. La empresa anunció la "pérdida"

de aproximadamente 850 mil bitcoins que

desaparecieron por robo y mala gestión. Desde

Desde entonces, aproximadamente 200 mil bitcoins

fueron recuperados, pero después de la

investigación se

descubrió que funcionarios robaron los bitcoins de la

cartera de la propia empresa gradualmente, sin que ella

fuera capaz de impedir esas prácticas.

Dos casos menores, pero significantes de robo

ocurrieron en las bolsas BitFinex, en las que fueron

robados 120 mil bitcoins, y Bitstamp, que perdió 19 mil

bitcoins en enero de 2015. Ambos ataques fueron hechos

por hackers y los responsables no fueron identificados.

¿Por Qué Nadie Encuentra A Los Criminales Que

Reciben Criptomonedas?

Una pregunta común para quien comienza a entender sobre

criptomonedas es: ¿por qué nadie puede impedir o al menos

identificar criminales que reciben criptomonedas? Y la

respuesta a esta pregunta no es simple.

Ya sabemos que una cartera de criptomonedas es

anónima, o sea, todos los participantes saben el código que la

identifica, pero nadie sabe a quién la cartera pertenece como

persona física. Cuando se produce un robo de criptomonedas,

o cuando el rescate de un secuestro se paga con transferencia

de bitcoins, todos saben el número de identificación de la

cartera que recibió, incluso sin saber quién es el propietario

en el mundo físico. Entonces el número de la cartera que

recibió criptomonedas sucias queda público y basta que todos

los participantes dejen de negociar con esa cartera que el

dueño

no

tendrá

qué

hacer

con

ella,

¿verdad?

Desafortunadamente, no.

Vamos a hablar primero de las características

tecnológicas. Hay un servicio controvertido en el mundo de

las criptomonedas llamado *cryptocurrency tumbler* o

mezclador

de

criptomoneda.

Este

servicio

consiste

básicamente en transformar una criptomoneda rastreable

(posible de identificar la cartera que recibió la primera

cantidad

procedente

de

actividades

criminales)

en

criptomoneda anónima o limpia. Hay varias empresas que

hacen este servicio y son muy criticadas por autoridades y

reguladores de mercado financiero.

En líneas generales, el "lavado" se

realiza por medio

de operaciones de compra y venta de monedas en cuentas

separadas, división de las criptomonedas en gran número de

carteras diferentes, en valores pequeños que luego se agregan

a carteras con criptomonedas limpias y vendidas en conjunto

y operaciones casadas usando diferentes criptomonedas en

bolsas independientes entre sí en países distintos. Todo ese

proceso puede incluso no hacer totalmente anónima la

criptomoneda sucia, pero queda tan laborioso y costoso

rastrearla que nadie lo hace. Existen listas de carteras de

criptomonedas sucias que se les impide negociar en varias

bolsas, pero los criminales crean nuevas carteras a una

velocidad más rápida que la comunidad es capaz de

identificarlas.

Se trata de un proceso similar al lavado de dinero

clásico, en el que un contraventor abre cuentas y mueve

dinero entre diversos países, principalmente aquellos que no

divulgan informaciones sobre sus correntistas a autoridades

internacionales, o que aceptan crear cuentas bancarias en

nombre de personas jurídicas cuyos propietarios se mantienen

anónimos. Aunque los investigadores

intenten encontrar el

dinero sucio, tienen gran dificultad en probar que esos

recursos pertenecen a un delincuente específico o que el

dinero procede de actividades criminales. Hay hoy un

movimiento global para presionar a los gobiernos de paraísos

fiscales a divulgar información sobre sus correntistas a través

de tratados internacionales y acuerdos para evitar el lavado de

dinero. Estos acuerdos, sin embargo, no alcanzan las

criptomonedas, que todavía sirven para ese tipo de crimen.

Hay, sin embargo, varias criptomonedas que son

intencionalmente anónimas. Más aún, existe competencia

entre criptomonedas para ser la más anónima de todas. Los

idealizadores de esas monedas y sus algoritmos estructuran la

criptografía de modo que el número de

identificación de las

carteras no sea público, ni la conexión de internet que accede

a esas carteras pueda ser conocida y aún agrupan las

transacciones en bloques que dificultan la trazabilidad y

mezclan las informaciones entre usuarios. Entre las más

conocidas están Monero, Dash, Zcash y Verge (antiguamente

llamada Dodgecoindark).

Con eso, es posible deducir que los compradores de

algunas de esas monedas no están preocupados en garantizar

que sólo reciben criptomonedas limpias y están dispuestos a

correr los riesgos inherentes a ellas. Saben que si son robados

no tendrán medio de recuperar los valores perdidos y

compran así mismo porque el beneficio del lavado del dinero

supera el riesgo de pérdida.

Naturalmente, no todos los

compradores de ese tipo de moneda están involucrados en

actividades delictivas, pero probablemente no están

preocupados por saber el origen de esos valores.

Capítulo VII

¿Cómo Las Criptomonedas Y La

Blockchain Pueden Cambiar Las

Relaciones Económicas En El Mundo?

“It’s not that everyone trusts bitcoin so much. It’s just that

they have stopped trusting you (banks).”

"No es que todo el mundo confía mucho en el bitcoin. Es que

dejaron de confiar en ustedes (bancos) ".

Miko Matsumara, fundador de la bolsa

de criptomonedas

Evercoin, hablando a una platea de banqueros.

Si los bancos, operadores de tarjetas y otras empresas de

servicios financieros no están preocupados por la expansión

de las criptomonedas y blockchain, es porque sus

administradores son demasiado perezosos para tratar de

entender lo que es. O tal vez esos administradores sean de

una generación no familiarizada con informática y la

revolución digital.

Lo que vemos ahora es algo análogo a la invención de

Internet, pero en una escala que aún no es posible predecir.

Puede ser que el blockchain y las criptomonedas no causen

cambios tan grandes en la sociedad como la Internet hizo,

pero con el tiempo deben afectar la vida de la mayor parte de

la población del planeta, haciendo excluidas a las personas

que no tienen acceso a los medios de pago digital. No será un

cambio repentino, de la misma manera que Internet no lo fue.

Tal vez demore algunos años o décadas, pero las ventajas de

las criptomonedas sobre el sistema financiero mundial de hoy

son incuestionables. Basta que un número mínimo de

personas consiga entender o al menos

aceptar el

funcionamiento de ese sistema.

Es por eso que las instituciones financieras clásicas

como bancos critican tanto las criptomonedas y todavía se

niegan a realizar operaciones con ellas. La amplia aceptación

de las criptomonedas como medio de pago corriente en un

país traería la legitimidad necesaria para que ellas sustituian a

los bancos en gran parte de sus actividades. No sería más

necesario pagar tasas de transferencias, tarifas de

mantenimiento de cuenta, algunas tasas de administración y

de financiación también podrían ser eliminadas. Los bancos

perderían buena parte de su capacidad de apalancamiento, es

decir, de prestar el dinero de un correntista a otro cobrando

intereses. Esto haría más difícil vender

otros productos como

planes de previsión y certificados de depósito bancario.

Hay implicaciones acerca de las criptomonedas y la

blockchain que aún no se explotan y muchas que todavía

surgirán en el futuro. Una aplicación prometedora para el

blockchain es el registro de cualquier tipo de propiedad,

como inmuebles, vehículos y otros objetivos que necesitan un

documento probando la propiedad. Esta puede ser una gran

amenaza

a

los

notarios,

especialmente

en

países

extremadamente burocráticos, como los de América Latina.

No es exagerado decir que en un futuro próximo, las notarías

serán tan importantes como los periódicos impresos son hoy.

Un número creciente de abogados se interesa por

blockchain en asuntos relacionados con la propiedad en

general y, más específicamente, propiedad intelectual. Ya

existen, en diversos países, empresas especializadas en

ofrecer registros de propiedad para

obras de músicos,

escritores y pintores. Algunos de estos servicios son gratuitos

y capaces de identificar el uso no autorizado de material

protegido por derechos de autor en plataformas como

Youtube. La tecnología del blockchain ya está siendo

utilizada para proteger esos derechos y registro de obras

diversas. Las instituciones locales de cada país que registran

libros y musicas para protección de derechos de autor ya

están obsoletas y sus servicios son innecesarios. Basta ahora

que el gobierno lo reconozca y libere escritores y músicos del

costo de registro de obras, una burocracia que sólo existe para

mantener empleos de funcionarios públicos.

El Anarquista Bitcoin

Sus profesiones aparecen en Wikipedia como

programador, hacker y revolucionario. Exactamente,

profesión revolucionario. Amir Taaki es un anarquista

bitcoin o cripto-anarquista nacido en Londres, con doble

nacionalidad iraní, que quedó conocido mundialmente

por ser uno de los primeros promotores

y

emprendedores de tecnología para comercialización de

Bitcoin.

Difícilmente usted oirá hablar de él en la televisión,

pero Amir Taaki se convirtió en una especie de celebridad

digital contra lo que considera opresión y control sobre la

vida privada. Trabajó durante años para desarrollar y

promover plataformas gratuitas de software, creó una de

las primeras bolsas de transacción de bitcoins del mundo

y desapareció de los medios entre 2015 y 2017, cuando

se trasladó a Siria, donde participó en combates armados

contra el Estado Islámico.

Taaki se define como un activista defensor de la

libertad y del acceso gratuito a datos. Él participó en la

creación de sistemas open source para diversos fines,

como juegos electrónicos y compartir bases de datos. En

2014, creó, junto con Cody Wilson, la Dark Wallet, una

plataforma digital para negociación anónima de bitcoins.

Algunos miembros de la comunidad de desarrollo de

criptomonedas criticaron la invención por tratarse de un

medio facilitador de pagos de

operaciones ilegales, como

tráfico de drogas y armas.

El "anarquismo digital" defendido por Taaki es un

concepto vago, cada cripto-anarquista tiene un objetivo

personal, no existe consenso. Mientras unos quieren dar

poder de elección al público, otros quieren facilitar el

acceso a armas por cuestiones ideológicas y aún hay

quienes creen en la necesidad de reducir el poder de

control de los gobiernos. Ninguno, sin embargo, habla en

Democracia. Ellos quieren cambiar la situación del

mundo, pero no tienen propuestas muy claras de lo que

podría ser usado en su lugar.

Las criptomonedas posibilitan algo hasta entonces

impensable: quedarse independiente del sistema de emisión

de monedas de bancos centrales. Los gobiernos a menudo

generan inflación intencionalmente a través de la emisión de

moneda y aumento de gasto público por encima del valor de

la recaudación con impuestos. En la década de 1930, el

economista británico John Maynard Keynes propuso un

conjunto de ideas que dio origen a la Escuela Keynesiana,

basada en la proposición de que la

economía debería ser

regulada y conducida activamente por los gobiernos para

llevar el país al pleno empleo. Estas ideas se popularizaron en

el período entre la I y II Guerras Mundiales y llevaron

gobiernos de varios países a intervenir en la economía. Una

de las formas de intervención es por medio de la política

monetaria, o sea, de la gestión de la moneda del país.

Keynes defendía que cuando un país está en situación

de crisis o retracción económica, el gobierno debe expandir

gastos con obras públicas, contratación de personas, oferta de

crédito para consumo entre otras medidas para estimular la

economía. Estos gastos llevarían la economía a un nivel de

actividad del pleno empleo, algo deseable según la teoría.

Esta expansión de gastos debería ser

financiada con emisión

de moneda y endeudamiento público, lo que aumenta la

inflación, pero que sería compensado posteriormente con

crecimiento económico y aumento de recaudación de

impuestos.

Hay mucha discusión sobre la eficacia de este tipo de

política, muchos economistas afirman que la expansión del

gasto público no funciona a largo plazo y que el esfuerzo

necesario para pagar la deuda del aumento de gastos no llega

a ser compensado por el crecimiento generado por el gasto

público.

Aparte de las controversias, es un hecho que cuando

un gobierno emite moneda a ritmo más rápido que el

crecimiento de la economía real, el resultado es el aumento

de la inflación. Fue exactamente lo que sucedió con algunos

países latinoamericanos en la década de 1980, que vivieron

crisis severas de hiperinflación, o con la Venezuela de

Nicolás Maduro. El aumento de la inflación impone

automáticamente una pérdida de riqueza para la población,

pues la mayoría de las personas no tienen suficiente dinero en

inversiones para protegerse contra el

aumento de precios. Por

regla general, los salarios se reajustan más lentamente que los

precios, lo que genera un empobrecimiento de la población en

virtud del aumento de los gastos del gobierno. Esta dinámica

se llama impuesto inflacionario.

Las criptomonedas permiten una forma de protección

contra el impuesto inflacionario. Suponiendo un caso extremo

en el que una persona utilice todos los bienes que posee para

comprar criptomonedas, no será afectada por la política

monetaria de los gobiernos que generan inflación, pues nadie

puede simplemente emitir más criptomonedas, como un

Banco Central haría. Los criterios de emisión de

criptomonedas son conocidos y abiertos, cualquier persona

puede participar y el volumen total

emitido es totalmente

conocido.

Naturalmente, las transacciones corrientes del día a día

todavía se deben hacer en moneda normal, pero imagínese

que un individuo convenza su empleador a recibir salario en

criptomonedas y encuentre tiendas que vendan productos con

bitcoins. Él sería capaz de librarse de las oscilaciones

inflacionarias que afectan a la economía del país y tener su

patrimonio protegido de los riesgos locales. En muchos

países, tiendas normales como supermercados ya prueban

aceptar pagos en criptomoneda y hasta Microsoft acepta

bitcoins como forma de compra de algunos productos. Debe

ser una cuestión de tiempo hasta que la papelería de su barrio

esté aceptando bitcoins, aunque de

forma indirecta. Puede ser

que en algún momento ella acepte sin saberlo, por medio de

empresas tercerizadas de pago.

Para la mayoría de la población la idea de migrar

definitivamente a las criptomonedas puede parecer arriesgada

y demasiado laboriosa para valer la pena, pero hay personas

en todo el mundo que valoran mucho la oportunidad de no

depender de dinero de los Bancos Centrales y que

transforman el máximo que pueden de sus bienes en

criptomonedas. Estos radicales comenzaron a ser llamados de

cripto-anarquistas. Son personas que no concuerdan con el

sistema político y económico de los países, no apoyan a

gobiernos o partidos políticos y usan las criptomonedas para

alejarse del poder de influencia de las

autoridades públicas.

Además de la cuestión política, el uso de

criptomonedas reduce considerablemente los costos de

transacción entre países, pues si empresas de varios sectores

aceptan criptomonedas como forma de pago, no es necesario

comprar moneda extranjera para hacer pagos internacionales,

usar bancos, pagar tasas de envío, esperar días para que haya

compensación, declarar las transferencias al fisco y al banco

central, entre tantas otras burocracias que existen. Esto

favorece la globalización, la integración de los mercados,

reduce las barreras que protegen los privilegios.

Con criptomonedas es posible hacer pagos en países

que no tienen relaciones diplomáticas entre sí, que están bajo

embargo económico o hasta que estén en

guerra. Las

criptomonedas reducen la capacidad que los gobiernos tienen

que intervenir en la vida privada de las personas y empresas,

y eso es una idea muy atractiva para los libertarios. Muchas

empresas y personas sueñan en trabajar en ambientes menos

controlados, con menos burocracia, más libres, y las

criptomonedas se hacen para que esto suceda.

Bitcoin Como Alternativa A Los Intereses Negativos

En varios países, las tasas de interés pagadas por los bancos

privados a sus depositarios son negativas. Para un

latinoamericano eso parece algo totalmente raro, pues

estamos acostumbrados a altas tasas de interés derivadas de

los sucesivos déficits de cuentas de los gobiernos.

Lo que ocurre en algunos países ricos,

en que gran

parte de la población tiene ahorros, es un exceso de reserva

de dinero en bancos y falta de demanda de préstamos para

consumo. Para estimular el consumo y no el ahorro, los

gobiernos cobran tasa de interés negativa, o sea, el correntista

no recibe ningún interés por dejar el dinero en el banco, y aún

paga tarifas, lo que torna su rendimiento negativo. En ese

caso, sería más ventajoso para la persona mantener todo su

dinero en billetes en una maleta guardada en casa que dejarlo

en un banco. Sabemos que mantener maletas de dinero en

casa puede traer problemas, entonces ¿de qué forma es

posible guardar dinero sin perder un poco cada mes? Si usted

pensó en criptomonedas, está pensando igual a los inversores.

Criptomonedas sirven como reserva de

valor, es decir,

una alternativa a las monedas que tienen una tasa de interés

negativo. Entre los países que tienen un tipo de interés cero o

negativo, están Japón, Suiza, Suecia, Dinamarca y

prácticamente todos los países de la zona del euro. En estos

países, una moneda simplemente no pierde valor ya es una

ventaja para los inversores. Las criptomonedas se presentan

como alternativa para huir de la pérdida de valor de dinero en

bancos.

Criptomonedas Como Forma De Incrementar El

Beneficio De Las Pequeñas Empresas

Estamos totalmente acostumbrados a comprar con tarjetas de

crédito y débito, usamos cada vez menos dinero en papel.

Esta ha sido una tendencia mundial y esto genera costos

significativos para pequeños comerciantes, que se ocupan

constantemente de las tarifas de los operadores de tarjetas.

Las tasas cobradas por las empresas pueden variar. Algunas

no cobran mensualidad, pero invariablemente presentan algún

aumento de costo para los comerciantes.

Si consideramos que los márgenes de beneficio de las

empresas de comercio son cada vez más pequeños, cualquier

economía es significativa. En muchos comercios el margen

de beneficio promedio se sitúa entre el 5% y el 7% de los

ingresos totales. Algunos operadores de tarjetas cobran un

2% o un 3% sobre el valor total de ventas como tarifa,

además de tardar un mes o más para pagar a los vendedores.

Si los comerciantes pudieran eliminar esta tarifa de las

empresas de cartón, podrían aumentar su

margen de beneficio

significativamente, además de repasar parte de ese descuento

para los clientes.

Las criptomonedas pueden facilitar este tipo de

reducción de costos, facilitando la vida de comerciantes y

consumidores. Si pensamos en las tiendas en línea,

especialmente las pequeñas, la reducción de tarifas de los

operadores de tarjetas sería una excelente noticia y esto

representa un incentivo para que acepten criptomonedas

como forma de pago.

Microtransacciones: Forma de Reducción de Pobreza

Otra ventaja importante de las criptomonedas es la viabilidad

de microtransaciones. Hoy, es imposible vender algo a través

de tarjeta de crédito que cueste menos de aproximadamente 1

dólar. Pequeños comerciantes prefieren no vender a usar las

tarjetas para recibir pequeños valores, porque la mayoría de

las veces pagan tarifas fijas por transacción. Si no hubiera

tarifa fija, cualquier transacción podría ser viable, incluso las

muy chicas.

Con transacciones directas entre las personas sin

atravesadores, sería posible vender productos o servicios que

cuestan céntimos por internet. Esto puede generar empleos

que hoy son imposibles debido a los costos de transacción.

Esta es la lógica del microcrédito, una iniciativa que rindió a

Muhammad Yunus el premio Nobel de la paz, por ayudar a

micro emprendedores de países pobres a desarrollar una

fuente de ingresos. Con las criptomonedas esta lógica puede

expandirse por Internet y ayudar a

reducir la pobreza en el

mundo.

¿Habrá Regulación De Las Criptomonedas?

Otro tema controvertido sobre las criptomonedas es la

regulación. En el momento, hay poca regulación de los

gobiernos y el fisco de la mayoría de ellos trata las

criptomonedas como un activo a ser declarado en el impuesto

de renta, como se hace con el oro, por ejemplo. Sin embargo,

sabemos que una vez que el dinero se transforma en

criptomoneda, ya no existe la forma en que los gobiernos

monitorean lo que sucede. El dueño de la cartera puede

comprar criptomonedas diferentes, venderlas en países

extranjeros, intercambiarlas por servicios y sólo debe declarar

ganancia de capital si vende las

criptomonedas con ganancias

en algún momento en el futuro.

Una vez más, la falta de regulación puede ser una

ventaja o un factor inhibidor. Muchos serán atraídos por

poder hacer transacciones sin burocracia y por evitar la

supervisión de gobiernos. Otros inversores, sin embargo,

nunca se sentirán lo suficientemente seguros para comprar

criptomonedas como inversión o utilizarlas como medio de

transacción mientras no haya una seguridad institucional

garantizada por organismos gubernamentales o empresas de

control.

Algunos expertos en blockchain y criptomonedas

creen que para que el mercado se expanda y alcance una

madurez, es necesario que los gobiernos creen algún tipo de

regulación para que el ciudadano común se sienta seguro para

usarlas. Otros, sin embargo, son contrarios a la regulación

precisamente por no querer que el gobierno controle sus

actividades.

Al parecer, los gobiernos no entrarán tan pronto en el

complicado campo de la regulación de las criptomonedas por

varios motivos, entre ellos:

1) Pocos países tienen profesionales con competencia técnica

suficiente para elaborar una regulación eficiente del mercado

de criptomonedas;

2) La regulación va a favorecer que surjan medios más

sofisticados de proteger el anonimato, mientras no existan

reglas eso no es una preocupación tan fuerte;

3) Es posible controlar empresas, pero prácticamente

imposible controlar a las personas físicas, y eso puede crear

una informalización del mercado;

4) El volumen transaccional de criptomonedas sigue siendo

pequeño para justificar la inversión estatal en una estructura

de control;

5) La mayoría de los políticos no entiende lo que es

criptomoneda y tendría gran dificultad en discutir y votar

leyes sobre ese tema;

6) No existe consenso entre los países sobre cómo tratar el

tema.

Lo más probable es que los gobiernos todavía esperan

algunos años antes de comenzar a hacer leyes para regular el

comercio de criptomonedas. Cuando la regulación empezar a

ser discutida e implantada, podemos esperar que haya una

división entre monedas reguladas por los gobiernos y

monedas no reguladas, siendo que esa diferencia debe afectar

la liquidez y demanda de ellas.

Podemos esperar también que algunos países empiecen

a prohibir, o al menos a crear restricciones burocráticas sobre

el comercio de criptomonedas, principalmente por la

preocupación de perder recaudación.

Países Que No Tienen Moneda Propia

Por más extraño que pueda parecer, existen varios

países que no poseen una moneda nacional propia, o sea,

usan una moneda emitida por otro país como medio

corriente de cambio. Los casos más notorios de América

Latina son Ecuador y El Salvador. Estos países pasaron por

grandes problemas de inflación en las décadas de 1980 y

1990, de gobiernos que gastaban más de lo que

recaudaban y acabaron devaluando la moneda debido al

endeudamiento público. En Brasil y Argentina, algo

similar ocurrió durante la década de 1980 con la

hiperinflación.

La manera en que los economistas y políticos

responsables del mantenimiento de la estabilidad de la

moneda han encontrado para reducir ese riesgo ha sido

extinguir la moneda local y utilizar una moneda

extranjera estable. En los casos latinoamericanos, se

eligió el dólar norteamericano. Al principio era una

estrategia pasajera, pero los beneficios de la estabilidad

monetaria derivados de la adopción del dolar acabaron

convirtiéndola en una práctica

permanente. Ninguno de

los dos países tiene planes de volver a usar una moneda

propia.

Varios países están en bloques de unión

monetaria, como la zona del euro y los países de Gran

Bretaña, pero otros usan monedas extranjeras como

forma de solucionar problemas económicos internos.

Zimbabue es un caso extremo en el que

el dinero local

fue tan devaluado con la inflación que el país dejó de

emitirlo y pasó a considerar ocho monedas extranjeras

como oficiales.

Además, países pequeños, como grupos de islas en

el pacífico y caribe, también participan en bloques

monetarios o vinculan sus monedas directamente a

monedas extranjeras. Como son países demasiado

pequeños para tener una política monetaria propia (algo

que frecuentemente resulta en aumento del

endeudamiento público o inflación), prefieren vincular

sus economías a una moneda relativamente estable de

un país con una política monetaria más fiable.

Las criptomonedas tienen algo en común

con las

monedas extranjeras aceptadas en países que no las

emiten. Las criptomonedas no pueden ser emitidas de

forma discrecional, es decir, en cualquier momento que

la autoridad monetaria desee. Ellas no sirven para crear

inflación (algo que los gobiernos hacen

intencionalmente), tiene una oferta finita, con criterios

de emisión conocidos y disponibles para el público en

general. El uso de criptomonedas crea una referencia de

valor fijo, independiente de la voluntad de los gobiernos,

como si fuera una moneda extranjera que no es

controlada por ningún país.

La Adopción De Blockchain Por Instituciones

Financieras

Hasta las instituciones financieras que tienen gran potencial

de pérdida con la tecnología de blockchain están estudiando

ese mercado y aprendiendo cómo pueden beneficiarse de él.

Los bancos de todo el mundo están haciendo experimentos

con blockchain para registrar transacciones y reducir costos

de control.

El Banco Central de Gran Bretaña ya probó el uso de

blockchain para transferir valores con otros bancos centrales

y bancos globales como Santander también están probando la

tecnología como forma de transferencia de recursos entre sus

unidades en varios países.

En Brasil, algunos bancos grandes comenzaron a

probar esta tecnología para compartir información de

catastros sobre clientes. En el caso de las instituciones

financieras, la ventaja inmediata sería la rápida divulgación

de información en el caso de ofrecer crédito, préstamo u otros

servicios financieros.

Aunque amenazados por la tecnología detrás de las

criptomonedas, los bancos estarán obligados a aprender sobre

ella si no quieren caer en la obsolescencia. Muchos de ellos

ya están tratando de prepararse para ello, pero aún lejos de

encontrar medios de competir con las ventajas de la

blockchain.

Las Criptomedas de Venezuela y Rusia

En 2017 y Rusia anunció la creación de una criptomoeda

gestionada por el gobierno, el criptorublo. La idea del país es

transformar parte de la emisión monetaria física en digital,

pero sin garantizar la privacidad de las partes ni permitir que

agentes no estatales puedan minar. En la práctica sólo sería la

digitalización del dinero que ya existe.

Es una iniciativa innovadora, pero que no adopta los

conceptos de descentralización y anonimato que definen las

criptonedas en general. En la práctica, el gobierno controlaría

todo de la misma forma y ese medio de pago no estaría en

manos de un banco o operador de tarjeta. Para una persona

que no confía en el gobierno, el criptorublo no trae ventajas.

El caso de Venezuela es más crítico, por diversos

factores. En enero de 2018, Nicolás Maduro anunció en una

red nacional de televisión la creación de una criptomoeda

estatal llamada "Petro", que tendría lastre en petróleo, gas

natural, oro y diamante. El objetivo es

insertar el país en el

contexto mundial tecnológico, pero la realidad es que esta

iniciativa intenta controlar de alguna forma la hiperinflación

en el país, estimada en el 2.300% en el 2017. Las notas de

bolívar, moneda venezolana, no tienen casi ningún valor y la

economía perdió las referencias monetarias. Oficialmente 1

unidad de esa criptomoeda correspondería a 1 barril de

petróleo y podría traer nuevamente algún referencial, pero no

resuelve el problema de confianza. Nadie explicó si sería

posible cambiar "Petros" por petróleo físico, lo que tal vez

diera algún nivel de credibilidad a la moneda.

¿Es posible confiar en que el gobierno de Maduro

estaría aún almacenando petróleo proporcional a la

criptomoeda emitida? Y si fuera capaz

de aumentar la

producción y vincularla a la moneda, porque necesita una

moneda digital y no una moneda normal, o incluso un título

de deuda pública ? Con el histórico del gobierno venezolano

de medidas económicas desastrosas, es difícil que los

acreedores e inversores internacionales confíen en la

existencia de un sistema eficiente de control del lastre de esa

moneda.

Venezuela tiene deudas con varios países, incluso los

vecinos sudamericanos, y ya está retrasando pagos de

parcelas de esos préstamos. Fue alejada del Mercosur por los

países miembros del bloque y vive un tipo de aislamiento

diplomático en función de medidas antidemocráticas del

gobierno actual. Todo indica que se trata de un intento de

volver a tener acceso a crédito internacional y reducir el caos

financiero que vive el país.

Consideraciones Finales

Invitamos a todos los que han leído este libro a participar en

los grupos de discusión en nuestra página web:

www.livroguiabitcoin.com

Las publicaciones son hechas mayoritariamente en

portugués, pero alentamos a todos los lectores de este libro a

participar escribiendo sus opiniones y dudas en castellano.

Así, podemos compartir experiencias con la comunidad de

traders, desarrolladores y invertidores de Brasil y todo

latinoamerica.

Nuestra intención es unir personas interesadas en

criptomoedas para compartir informaciones, mejorando el

conocimiento disponible sobre el tema en castellano y

portugués. Creemos que criptomoedas y blockchain son

tecnologías que vinieron para quedar, aunque en el futuro

haya una desaceleración del mercado. Cuanto más

información

disponible

haya

para

inversores

latinoamericanos, más desarrollado será nuestro mercado y

más podremos insertarnos de forma estable y lucrativa en los

mercados financieros internacionales.

Queremos alentar que la comunidad de desarrolladores

e inversores converse entre sí. Somos inversores y estudiosos

de las criptomedas y tenemos interés en contribuir con la

formación de una comunidad activa, que sepa sacar provecho

de las oscilaciones de precios y generar liquidez de mercado.

Nuevas Fronteras

Ahora que entendemos donde estamos dentro del mundo de

la tecnología en el momento, podemos tener bases para

analizar las tendencias del futuro. Lo que está sucediendo en

el momento es la posibilidad de que el individuo tenga los

medios de producción de vuelta en su poder. Lo que sucede

es que estamos en una transición social

hacia una economía

compartida. Existirán dos sociedades: aquella que tiene como

base grandes autoridades centrales como monopolios y

gobiernos, donde existirá gran concentración de poder y

renta, y otra que tendrá como base la economía distribuida y

compartida.

La primera de ellas es nuestra actual sociedad y

economía. La llamaremos de economía "legado", y sociedad

"legado". Legado, pues es exactamente esto, una herencia del

pasado que debe ser compatibilizada de alguna forma con los

modelos actuales. La tecnología está llevando una opción al

individuo. Cada uno puede optar por no hacer más parte de la

sociedad legado, donde no tiene control sobre medios de

producción, o puede participar de la

nueva economía y nueva

organización social donde es proporcionalmente responsable

y recompensando por su nivel de participación.

Un ejemplo de eso son las nuevas tecnologías de

organización en red incipientes que tienen un enorme

potencial disruptivo, las llamadas *mesh networks*. Estas redes

permiten a todos conectarse sin depender de los proveedores

de Internet. Hoy en día el sistema de telecomunicaciones

depende de grandes empresas que poseen enrutadores

centrales estratégicamente y jerárquicamente posicionados

para manejar la alta carga de tráfico de datos. Las empresas, a

su vez, compran el derecho de uso, incluso del espectro de

radio, del gobierno, que licencia esos grandes medios de

telecomunicación. Con el avance en la

tecnología tanto de

radio y de software, ya no es necesario mantener la estructura

actual. El costo de producción de hardwares que funcionan

como antenas potentes, pero que caben en la palma de su

mano, los llamados SDR (*software de radios*), cayeron a

niveles que cualquier persona puede montar su propia

estación de celular.

En el campo del software, aún hablando sobre *mesh*

networks, existen grupos proporcionando código abierto para

programar un protocolo de torre de celular en el SDR, como

el OpenBTS, y el YateBTS. También existen iniciativas de

empresas

que

están

implementando

softwares

que

funcionarán en cualquier celular, o sea, todos pueden usar el

celular para acceder a internet. Si un usuario genera más

tráfico que consume, puede optar por vender su capacidad de

transmisión, esencialmente transformando al individuo en su

propio proveedor de Internet, lo que elimina la necesidad de

grandes centros corporativos.

En el campo de la energía, hoy cualquiera puede

producir su propia electricidad, a través de la evolución de la

tecnología de paneles solares y su continua caída en el costo

de producción, principalmente donde existe gran incidencia

de sol. Hoy, en la mayoría de los lugares, ya es más barato, a

largo plazo, instalar paneles solares que consumir energía

eléctrica de la concesionaria distribuidora. Esto significa que

es sólo una cuestión de tiempo hasta que este movimiento de

transición de la matriz energética gane fuerza y no

necesitamos más de grandes empresas de energía. Aún asi, es

importante resaltar que con la tecnología actual, todavía es

necesario tener la infraestructura de transmisión, pues la

energía eléctrica extra producida no

puede ser almacenada

eficientemente. La industria todavía necesita avanzar en la

parte de la tecnología de baterías para que tengamos una

sociedad totalmente fuera de la red.

En el campo urbano, coches automáticos y

compartidos serán la base de la movilidad. Probablemente, en

algunas décadas, nadie deseará tener la propiedad privada de

un coche. La persona simplemente saldrá en la calle y entrará

en un taxi, sin conductor, y en pocos minutos de espera. Las

calles no tendrán más semáforos, y puede ser que tengamos

un tráfico automatizado tridimensional, en lugar de

bidimensional, lo que significa que probablemente tendremos

drones para el transporte humano también. En este contexto,

es posible que aún existan grandes

corporaciones, dueñas de

las flotas de vehículos, pero el beneficio de ellas vendría por

la prestación de un servicio, en lugar de la venta de coches. Y

el costo del servicio sería mucho más bajo para el pasajero

que para los taxis actuales. Probablemente existirá un

mercado de coches de lujo, donde individuos súper ricos

desearán conducir su propio coche, pero probablemente será

en una pista de tráfico separada del resto de los coches

automáticos. La lección para sacar de aquí es que todos estos

autos serán automáticos e integrados en Internet, y podrán

usar criptomonedas para hacer transacciones, por ejemplo.

En el campo de la agricultura, ya existen personas

organizándose en ecoaldeas y produciendo su propio

alimentando, librándose de la

dependencia de grandes

hacendados. Estas ecoaldeas también tienden a producir su

propia energía. Además, tenemos avances en el desarrollo de

carnes sintéticas, a partir de células madre, disminuyendo la

necesidad de grandes granjas de ganado, que acaban por

generar un impacto enorme en el medio ambiente.

Todos estos cambios nos hacen creer que el mundo

está caminando hacia una sociedad en la que las personas se

organizarán en grupos más pequeños, como los antiguos

clanes o tribus, libres de una autoridad central, y estas tribus

serán integradas unas a otras por la tecnología y por acuerdos

hechos entre ellos. Todo ese cambio parece converger hacia

lo que las criptomonedas están proponiendo.

Si miramos el cambio que Amazon trajo

al mercado de

libros, por ejemplo, donde pasó a ser viable a las personas

comprar cualquier libro que quieran, y no sólo unos pocos

vendidos en masa, debido al costo extremadamente bajo de

almacenamiento, podemos ver características de consumo de

nicho, o tribu.

En Internet, en el mundo digital, ya estamos en esta

etapa en que cientos de miles de foros agregan a personas de

todo el mundo en torno a una afinidad, aunque esta reunión

sea virtual. Hay una anarquía digital real en nuestro mundo

contemporáneo. Con esas bases fundadas, tal vez la propia

institución familiar comience a cambiar nuevamente. La

noción de familia en la Grecia Antigua, en el Imperio

Romano, en China, o en el Oriente

Medio eran diferentes

entre sí. La tecnología está cambiando este concepto

nuevamente, y su tribu puede terminar siendo sinónimo de su

familia.

Por último, las criptomonedas van más allá de encajar

perfectamente en estos nuevos paradigmas de mundo que se

han lanzado, que forman una de las bases esenciales para que

todas estas previsiones del futuro puedan suceder.

Agradecimientos

Agradecemos a nuestras familias por el apoyo en nuestra

formación académica y por el incentivo en escribir ese libro.

Agradecemos también a nuestros amigos, colegas y

profesores de la Facultad de Economía y Administración de

la Universidad de São Paulo y de la Fundación Getulio

Vargas - EAESP.