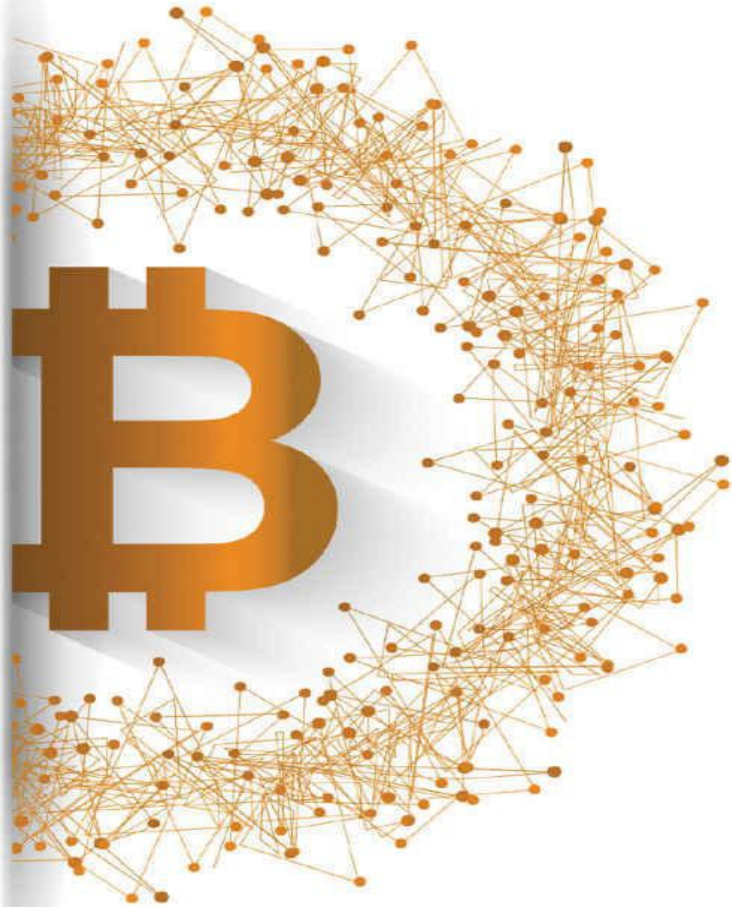
CRIPTOECONOMÍA

JUAN FRANCISCO BOLAÑOS
FRANK LUETTICKE
CARLOS GALARZA PONCE



Libro con realidad aumentada AR

Cómo el Bitcoin y Blockchain
están cambiando al mundo y tus finanzas

CRIPTOECONOMÍA

Cómo el Bitcoin y Blockchain están cambiando al mundo y tus finanzas

Juan Francisco Bolaños
Frank Luetticke
Carlos Galarza Ponce

Primera Edición

Categoría:
Economía, Finanzas,
Educación, Tecnologia.

Colaboradores:
Servicio ACE – ACCA

ISBN: 9781082212871
Imprint: Independently published

Juan Francisco Bolaños
Frank Luetticke
Carlos Galarza Ponce
www.librocriptoeconomia.com

Correo: info@bigmind360.com

A todas las personas que con
sus ideas,
esfuerzo y dedicación
trabajan a diario
para que la criptoeconomía
prospere y
avance. Este libro es nuestro
aporte al
gran trabajo que realizan.

REALIDAD AUMENTADA

En este libro podrás aprender de forma interactiva, ya que es el primer libro de su género en contar con material en Realidad Aumentada AR, tales como, animaciones, videos y juegos que te acompañarán durante este viaje.

Instrucciones

1) Si no tienes instalada la aplicación de Vinary VR/AR, descárgala en Google Play o Apple Store; encuéntrala también en www.vinarytech.com o escanea el código QR para su descarga y regístrate de forma gratuita.

2) Identifica las páginas que cuentan con Realidad Aumentada con este símbolo

3) Abre la App de Vinary, enfoca el target y disfruta del contenido interactivo.

4) Pulsa los botones en la realidad aumentada para ver todas las opciones.

AGRADECIMIENTO

Al inefable Satoshi Nakamoto por haber ideado y construido, hace diez años, Bitcoin, la cadena de bloques y la criptomoneda, que conforman el primer sistema de pagos descentralizado que permite transacciones globales, neutrales, confiables y resistentes a la censura, y que representan la base de la criptoeconomía.

A todas las personas que día a día trabajan con la misma determinación y visión que nosotros para educar y enseñar sobre las criptomonedas y la cadena de bloques. Ustedes son el motor que hace posible que cada vez más personas conozcan sobre la criptoeconomía y las tecnologías relacionadas con ésta.

Agradezco a mi familia: Mariela, Isabela, María, Veronika, Wolfgang, Peter, Judith y

David; quienes siempre me apoyan en mis decisiones, emprendimientos y proyectos. Sin el respaldo de la familia correr una milla extra no es posible.

A mi primera hija, para que este libro sea la base de enseñanza para poder vivir en un mundo mejor, libre de la dictadura de los bancos.

A las personas que han dado sus comentarios, opiniones y sugerencias para el desarrollo de este libro; en especial a Dany Ledesma, Jimmy Romero, Mónica Salazar y Marwen Chebbi.

A las personas que comparten la misma visión de una nueva economía y cada día realizan proyectos que permiten la inclusión de la criptoeconomía en todo el mundo. En especial a: MM, TG, MM, AY, CS, CG, CU, DJ, GW, PF.

FRANK LUETTICKE

A mi familia nuclear y extendida, Lorena, Samuel, Fátima, por su apoyo incondicional, son la fuente de mi inspiración y la razón de mi existencia. A Juan Fernando Carpio, por ser mi "knowledge sherpa" y por haberme introducido al fascinante mundo del libertarismo, de la economía austríaca y de la enteogenia. A Alejandro Veintimilla y Diego Saa de Academia Blockchain, por permitirme compartir mis conocimientos con la audiencia del criptomundo. A mi hermano del alma, Andrés Varhola, por estar siempre conmigo en los buenos y malos momentos.

Guardo en mi corazón una inmensa gratitud con todos ustedes, sin su respaldo, colaboración y paciencia esta obra no hubiese visto la luz.

JUAN FRANCISCO

Agradezco a mi padre, quien me enseñó el camino del emprendimiento; a mi madre

(QEPD), quien formó mis valores; a mis hermanas, quienes siempre me apoyan en mis proyectos; a mi hijo José Martín, por ser una inspiración para seguir adelante.

A mi socio Carlos Ugalde, por haber sido el primero en tener la visión y apostarle al mercado Cripto y Blockchain. Al Equipo de la empresa Vinary VR/AR, por todo su esmero en hacer de éste un proyecto innovador y el primero en su clase con Realidad Aumentada.

A las personas que me han apoyado en todo este camino con sus sugerencias, opiniones. Y todas las personas que forman parte del día a día… ¡Gracias!

CARLOS GALARZA

ÍNDICE

PRÓLOGO

Las criptomonedas como instrumentos financieros

Cuando bitcoin comenzó a cobrar eco dentro del mundo financiero, la industria y los gobiernos emitieron alarmas sobre un fenómeno que no podían explicarse y que, hasta 2019, todavía una gran parte de la población del planeta sigue sin comprender.

Como se ha documentado, bitcoin empezó a tener dos usos principales: instrumento de inversión y medio de pago. En 2014, empresas como Overstock no demoraron mucho en experimentar con el uso de bitcoin aceptando este criptoactivo para realizar

compras en su plataforma, basando su decisión en una cuestión mediática y una estrategia de mercadeo. Dentro de los foros de comunidades en internet, se hablaba de bitcoin como una moneda mundial, el "dinero del futuro" el cuál aumentaría su valor y llegaría a cifras exuberantes. Esto conllevó a un aumento sobre las expectativas, de tal manera que los efectos sobre su precio en comparación con el dólar estadounidense fueron inevitables.

El ecosistema de las criptomonedas o criptoactivos, se diversificó de manera acelerada originando la creación de múltiples billeteras digitales o wallets (en inglés), casas de cambio de bitcoin,

desarrollo de equipo de cómputo para realizar minería de bitcoin, incluso instrumentos derivados como los futuros de bitcoin emitidos en 2017 por la Bolsa de Chicago (CME, por sus siglas en inglés). El momento cumbre de bitcoin y por descontado de otros criptoactivos, tuvo lugar en 2017 cuando bitcoin alcanzó un precio máximo de alrededor de 20 mil dólares estadounidenses, es decir, un aumento de más de dos mil por ciento en dicho año. Sin embargo, en enero de 2018, el precio de bitcoin cayó abruptamente perdiendo más del ochenta por ciento de su valor en menos de un mes. Para algunos economistas y financieros, incluso premios nobel como Paul Krugman o Robert J. Shiller, no se

trataba más que de una gran burbuja económica la cual entre más pronto se quebrara, sería mejor.

Después de ese trago amargo que sacudió a muchos que decidieron ser parte de la euforia y comprar bitcoin cuando el precio tuvo máximos históricos, el mercado de criptoactivos se mantuvo con pérdidas a lo largo de diferentes semanas; no obstante, el interés por la tecnología no mermó, de hecho, fue uno de los aspectos que más se destacó, puesto que se tuvo un incremento en los casos de uso con la tecnología contable distribuida, mejor conocida como blockchain, como bien se describe en el presente libro.

El crecimiento del ecosistema de criptoactivos, ha permitido la creación de nuevos modelos de negocio principalmente para obtener financiamiento de una manera rápida. Algunos criptoactivos como ether o eos, lograron recaudar millones de dólares a través de las llamadas Ofertas Iniciales de Moneda (ICO, por sus siglas en inglés), que no fueron otra cosa más que proyectos publicados en internet, en donde se invitaba a la comunidad a fondear su idea de proyecto a través de una preventa del criptoactivo a desarrollar. Dichas recaudaciones tuvieron tal éxito que, nuevamente, generó euforia y, para 2017, una gran

cantidad de criptoactivos fueron ofrecidos bajo este modelo de financiación. Sin embargo, como era de esperarse, muchos proyectos resultaron ser un fraude, ya sea porque los sitios en internet desaparecieron de un día a otro o porque simplemente no se recaudaron los fondos en su totalidad. Posteriormente el modelo ICO evolucionó a las ofertas de token de valor (STO, por sus siglas en inglés) donde el objetivo consistió en realizar la venta de tokens, no obstante brindando garantías, es decir, otorgando el respaldo que las ICO no daban, pero a través de activos reales y con toda la instrumentación jurídica necesaria.

Hasta 2019, los instrumentos de inversión a través de criptoactivos ya no eran ajenos al ecosistema, por ejemplo: futuros de bitcoin, swaps, ETFs, fondos de inversión, opciones y stablecoins (criptomonedas estables). De esta forma, la existencia de los criptoactivos dio paso a un sector que comenzó la emisión de tokens respaldados por activos, bajo un concepto novedoso al que he llamado criptobursatilización y que requerirá una mayor profundidad probablemente a través de alguna otra obra.

La evolución del ecosistema a lo largo de los años ha generado reflexiones profundas en diferentes ámbitos:

financiero, legal, tecnológico, fiscal e incluso social. Estamos ante un fenómeno novedoso y "disruptor" que nos ha llevado a retomar y replantear múltiples conceptos, particularmente dentro del sistema financiero que, en apariencia, creíamos consolidados. Nociones sobre el dinero, su respaldo, su valor, entre otros, evidencian una brecha importante entre la forma en la que operan las instituciones y lo que el mundo había entendido, puesto que nos encontramos ante un fenómeno que demanda un cambio de paradigma dentro de la sociedad.

En el presente libro, se muestra un panorama general, con fundamentos

sólidos sobre las diferentes vertientes que han surgido en el ecosistema. La visión integral con el que está diseñado cada uno de los capítulos, resulta una excelente primera aproximación para los lectores puesto que contiene los elementos necesarios para aquellos quienes aún tienen ciertas reservas o cuentan con cierto temor y también para quienes desean ampliar y consolidar los conocimientos sobre criptoactivos.

Eloísa Cadenas

Doctorante en Ingeniería Financiera por la Universidad Nacional Autónoma de México. Investigadora sobre valuación financiera de criptoactivos en el ámbito empresarial y consultora de proyectos ICO y STO.

La importancia de la criptografía en blockchain y las criptomonedas

En enero del año 2009 se pone en funcionamiento Bitcoin, una tecnología que implementa un protocolo llamado Timechain, es lo que se conoce hoy en día como Blockchain. Este protocolo tiene como objetivo principal sincronizar bases de datos entre varias computadoras. En este caso, cuando hablamos de bases de datos en realidad estamos haciendo referencia a una serie de archivos binarios almacenados en el disco duro de nuestros ordenadores y que contienen la información de todo lo

que va sucediendo a lo largo del tiempo dentro de la red que conforman los nodos o computadoras en los que se está ejecutando este protocolo, es decir, transacciones, validaciones, firmas o pequeños programas que se pueden ejecutar dentro de las transacciones, también conocidos como scripts. Además, estos scripts se pueden programar de una forma muy particular para que ejerzan las funciones de un Smart Contract. Obviamente la información almacenada en estos archivos no se escribe en claro, no es legible para el ojo humano, o al menos no es nada fácil. En realidad, se trata de cadenas muy largas de ceros y unos, sistema en base 2 o binario, que

convertiremos en base 16 o hexadecimal para facilitar su tratamiento y lectura. Pero si ponemos la lupa en estos códigos hexadecimales seguiremos encontrando cadenas muy largas de bytes. Cuando Satoshi Nakamoto desarrollaba Bitcoin pensó en una estructura de datos muy compleja pero muy bien estructurada para almacenar toda esta información en bloques, de forma que estuviera meticulosamente ordenada y fácilmente comprobable por el protocolo Blockchain. Además pensó desde el principio en la escalabilidad del protocolo, de modo que a lo largo de estos 10 años que han pasado desde su creación se hayan podido incorporar una

serie de cambios que han garantizado una notable mejoría en muchos aspectos pero sobre todo, lo más importante, en el ámbito de la seguridad. En un protocolo como el de Bitcoin la seguridad se sostiene gracias a tres principios fundamentales, que son la confidencialidad, la integridad y la disponibilidad. La integridad y la confidencialidad solo se pueden alcanzar mediante el uso de técnicas criptográficas. La criptografía en Bitcoin está muy presente y aplicada de una manera brillante. Se pueden encontrar algunas funciones hash, esquemas de cifrado y algoritmos criptográficos como SHA-256, RIPEMD-160, Base58 o curvas

elípticas. La combinación de algunas de estas funciones o algoritmos tienen varios propósitos, desde la generación de claves privadas/públicas, generación de direcciones, validación de firmas, desbloqueos de algunos scripts o algo tan valioso y complejo como son las funciones de minería para intentar hallar un hash válido y así poder incorporar un bloque nuevo a la cadena de bloques.

Si Bitcoin no dispusiera de técnicas criptográficas simplemente no tendría uso que mereciera la pena, no tendría ningún sentido, pues se trata de una tecnología orientada a transacciones en las que se ha de garantizar cierto grado de confidencialidad, pero además debe

haber una prueba de trabajo (Proof of Work, PoW, por sus siglas en inglés) que añade dificultad a la hora de modificar el estado de la cadena, por ejemplo, añadiendo nueva información. Si no se aplicaran técnicas criptográficas la dificultad sería nula y cualquier persona podría manipular los datos de la cadena en cualquier punto del tiempo, lo que lo convertiría automáticamente en algo inservible y no serviría como medio de pago digital peer to peer, que es exactamente para lo que se creó.

Por otro lado, tener una gran cantidad de nodos que se encarguen de procesar, validar y distribuir toda la información

entre todos los participantes de la red es vital para garantizar otro grado más de seguridad. Este punto es especialmente importante, pues la cadena válida es la cadena más larga procesada y almacenada en la mayoría de los nodos, así pues, a mayor número de nodos menor probabilidad de sufrir un ataque al 51% de la red. Para que una tecnología que implemente un protocolo Blockchain sea lo más seguro y fiable posible es imprescindible que cumpla una serie de requisitos mínimos como que sea software libre, que su red de nodos sea descentralizada y que además la información esté distribuida en un gran número de computadoras, como no, implementando técnicas criptográficas,

pues la seguridad es el punto más importante de cualquier sistema que se precie.

Año 2008, Madrid (España), se celebró el congreso Día Internacional de la Seguridad de la Información (DISI). Entre los ponentes estaba la Dra. Radia Perlman, y dijo en la conferencia inaugural "Adventures in Network Security": "Tenemos que enseñar Criptografía, porque es importante que se conozca esta ciencia, pero muchas veces los educadores se centran en enseñar asuntos demasiado teóricos y matemáticos. No creo que sea esa la parte realmente interesante. No creo que el mundo necesite más criptógrafos, si

no más gente que entienda cómo usar la criptografía". Sabias palabras de una persona con un altísimo conocimiento en la ciencia de la Criptología. La criptografía existe desde hace miles de años, es casi tan antigua como la propia humanidad. Debemos aprender a usarla con el objetivo de incorporar seguridad a la información, a algo tan importante y primitivo como son las comunicaciones.

Debemos ser conscientes de que la seguridad en los sistemas computacionales depende principalmente de cuán fuertes y robustos son los elementos criptográficos que implementan, pero no olvidemos que en el pasado ha habido

sistemas criptográficos que han sido superados, rotos, vulnerados. Ante el avance de la ciencia y del conocimiento humano en campos como el de la computación binaria y cuántica, debemos hacer una reflexión y recordar la regla de oro de la seguridad operacional (OPSEC) que dice: "No existe una información mejor protegida que aquella que no se llega a generar". Hagamos uso de la tecnología, pero con responsabilidad y con los pies en la tierra.

Javier Domínguez Gómez
Profesor de Criptografía aplicada y programación en la Universidad Complutense de Madrid.
Ingeniero de software, especialista en

ciberseguridad
y análisis forense.

PREFACIO

La criptoeconomía es la economía del nuevo mundo, de la industria 4.0. Representa una novedosa y práctica manera de conectarnos e intercambiar valor directamente con todos los habitantes del planeta sin la necesidad de intermediarios.

Esta obra cuenta la historia del viaje que hemos realizado, cada uno a su debido tiempo y motivado por diferentes razones, a través de los emocionantes y sorpresivos caminos que tanto blockchain, bitcoin y las criptomonedas en general han abierto en nuestras vidas. Los autores compartimos el deseo de transmitir a los lectores lo que hemos

aprendido a lo largo de esta travesía y cómo estas tecnologías están transformando nuestros ámbitos personales y laborales. Desde que nos involucramos en el criptomundo decidimos dedicarnos por completo a él; sin duda alguna, ésta ha sido una de las decisiones más importantes de nuestras vidas.

La transformación que propone la cadena de bloques no sólo afecta al ámbito bancario y financiero; esta tecnología ofrece modificar y/o reemplazar muchos de los sistemas de organización social bajo los cuales nuestras vidas se desenvuelven y que ya han alcanzado su fecha de caducidad y

por tanto deben dar lugar al desarrollo y establecimiento de unos nuevos. En los próximos años seremos testigos de la migración del paradigma institucional centralizado –cerrado, discriminatorio, jerárquico, opaco y muchas veces corrupto, en donde el poder se encuentra concentrado en pocos individuos– hacia uno descentralizado –abierto, no discriminatorio, horizontal, transparente, autónomo y resistente a la censura, en donde el poder se encuentra disperso entre innumerables personas–.

El cambio de paradigma no será sencillo; va a enfrentar mucha resistencia por parte de quienes ostentan el poder y que por obvias razones no

quieren dejarlo escapar de sus manos. En este sentido, la mejor herramienta de la que disponemos los individuos es la autoeducación como una manera de fomentar la adopción de ésta y otras tecnologías. Este libro se propone alimentar a las mentes hambrientas de nuevos conocimientos que buscan entender y participar en este nuevo y fascinante mundo.

INTRODUCCIÓN

Es común que cuando aparece una nueva tecnología nos encontremos rodeados de nuevos términos sofisticados y difíciles de entender. “bitcoin”, “criptoeconomía”, “criptoactivos”, “criptomonedas”, “blockchain”, etc. En el fondo, más allá de todas estas palabras de moda, subyace el intento de los humanos por conectarse e intercambiar valor. Los individuos debemos conectarnos para comunicarnos, crear, producir e intercambiar valor en los diferentes mercados en los que participamos. Los mercados han existido desde el mismo momento en el que los humanos

empezamos a intercambiar cosas, han emergido como un proceso natural de coordinación social. La evolución de los mercados es constante, ocurre a través de una serie de desarrollos tecnológicos que los ayudan a ser más eficientes.

Sin la necesidad de entender lo que es una cadena de bloques y cómo funciona, pero aceptando que ésta es una tecnología que nos permite la transferencia de valor sin la participación de intermediarios, podemos afirmar sin temor a equivocarnos que ha llegado para quedarse y que ha permitido la creación de una red de mercados mucho más profunda y poderosa que la red de

información. La diferencia entre información y valor es la escasez: si entregamos información a alguien, aún la poseemos; pero si transferimos valor a otra persona, dejamos de ser sus propietarios. Blockchain y las criptomonedas permiten mover valor tan fácilmente como se mueve la información.

Con esta obra los lectores podrán aprender conceptos básicos, pero esenciales, sobre Bitcoin, las criptomonedas, blockchain y finanzas personales. para poder participar económicamente en esta revolución. Este libro está dividido en tres secciones principales: Criptomonedas,

Tecnología blockchain y Finanzas.

En la sección Criptomonedas abordamos la historia del dinero –fundamental para entender el fenómeno de Bitcoin– pasando por las criptomonedas o "altcoins" más importantes, de acuerdo con nuestro criterio, hasta la fecha. Del mismo modo, tratamos ciertos elementos importantes dentro del ecosistema, como las ICO (Initial Coin Offering), el uso adecuado de billeteras o monederos digitales y la manera de comprar, vender y usar criptodivisas con seguridad.

La segunda sección, Tecnologías Blockchain, trata sobre la tecnología subyacente que permite la existencia de

las criptomonedas: la cadena de bloques o blockchain. Qué problemas soluciona, cómo funciona, cuál es el nuevo paradigma de organización de los sistemas que propone, cuáles son sus aplicaciones en el mundo real y los desafíos que esta tecnología tendrá que enfrentar para trascender.

En la sección de Finanzas nos adentramos en temas relacionados con las finanzas personales y las posibilidades que el criptomundo ofrece a quienes inviertan en este mercado. Los lectores aprenderán cómo construir un portafolio de inversiones de criptomonedas basándose en una estrategia de inversión integral. Además

conocerán los diferentes mecanismos de inversión que están disponibles en la criptoeconomía y la importancia de saber cómo identificar oportunamente fraudes y pirámides financieras que se aprovechan de las expectativas que genera esta tendencia.

Hemos diseñado el libro de forma que pueda comenzarse a leer en cualquier punto. Esperamos que esta obra despierte en quienes lean sobre la criptoeconomía por primera vez, la misma pasión que ha despertado en nosotros, y que aporte nuevos conocimientos a quienes ya se infectaron con este virus del mundo descentralizado.

Al final del libro dispusimos un amplio glosario donde se incluyen explicaciones detalladas de términos con los que el lector pudiera no estar familiarizado.

Disclaimer

La información contenida en este libro es de carácter meramente informativa y no constituye ninguna recomendación de inversión, invitación, oferta, solicitud u obligación por parte de los autores. La misma no debe ser utilizada para la valoración de carteras o patrimonios, ni servir de base para recomendaciones de inversión. Los autores no serán responsables de ninguna pérdida financiera, ni de ninguna decisión tomada sobre la base de la información contenida en este libro. Los autores no asumen responsabilidad alguna en relación con dicha información, ni por cualquier uso no autorizado de la misma.

PARTE 1

CRIPTOMONEDAS

Historia del dinero y el nacimiento de bitcoin

> *La aparición de "cibermonedas" controladas por algoritmos matemáticos que no tienen jurisdicción, permitirá trasladar la riqueza de los ciudadanos a un entorno donde no está sujeta a la coacción de los gobiernos. Sólo los pobres serán víctimas de la inflación y deflación ocasionadas por las monedas fiduciarias.*
>
> JAMES DAVIDSON Y WILLIAM REES-MOGG

Para comprender a cabalidad el fenómeno de las criptomonedas en

general y del bitcoin en particular, primero es necesario entender qué es el dinero. El dinero por sí mismo no es ni bueno ni malo, es simplemente una herramienta neutral utilizada por todos nosotros diariamente; no obstante, muy pocas personas poseen un verdadero conocimiento de lo que realmente es.

El dinero es una ilusión

A pesar de que cueste aceptarlo, el dinero es una ilusión, forma parte de una de las tanta alucinaciones colectivas. Lo único real es su poder simbólico. El dinero no es más que un lenguaje de intercambio que nos permite dar valor a las cosas y confiar en los extraños; dicho de otra forma, nuestro

entendimiento e interpretación de un pedazo de papel impreso y teñido de diversos colores es todo lo que cuenta. En tal virtud, el valor de todo tipo de dinero es inestable, fluctuante y muchas veces volátil.

Características del dinero

Para que el dinero sea considerado como una herramienta adecuada para efectuar intercambios de valor debe cumplir con todas y cada una de las siguientes ocho características: debe ser escaso, de fácil almacenamiento y transporte, durable, difícil de falsificar, fácil de identificar, fungible (reemplazable), divisible y confiable. Si bien todas las características

enumeradas previamente son importantes, la fundamental es la número ocho; sin la confianza del usuario, por más que una moneda cumpla con las restantes siete, simplemente carece de valor. Ejemplos de la pérdida de confianza en una moneda ocurren con relativa frecuencia en países con una actividad política convulsa y problemática, la cual ha sido causante de grandes debacles económicas; Argentina, Bolivia, Brasil, Ecuador, Hungría, Perú, Venezuela, República Weimar, Zimbabue, son algunos ejemplos; todos estos países han cambiado de moneda una o varias veces debido a una hiperinflación causada por la pérdida de confianza en su dinero que

tiene como orígen la actuación de gobiernos irresponsables.

¿El dinero tiene un valor intrínseco?

Hoy en día la respuesta es no. El dinero es frágil y provisional. Aquel que cree que es real, sólido o respaldado por algo o por alguien es como creer en fantasmas. Y precisamente éste es el principal argumento que se emplea en contra del bitcoin y las otras criptomonedas: manifiestan que no valen nada porque “no tienen respaldo”. En pocas palabras, el dinero adquiere su valor por la confianza que los usuarios depositan en él. El bolívar venezolano no vale nada en este momento porque nadie confía en él ni en el gobierno que

lo emite soberanamente.

Funciones del dinero

Las funciones del dinero son tres: unidad contable, depósito de valor y medio de cambio. Cada una de las funciones mencionadas se explica por sí sola. Nos detenemos un momento en la número dos porque requiere de una explicación más detallada. Muchas de las monedas fiduciarias –emitidas por los bancos centrales– han perdido paulatinamente la propiedad de depósito de valor porque los gobiernos acuden a la impresión indiscriminada de dinero con el fin de cubrir sus abultados déficits fiscales, generando devaluación e inflación, las que se traducen en la

pérdida constante de la capacidad adquisitiva de los ciudadanos; es decir, el dinero ahorrado cada año vale menos. Ésta es una política monetaria común que comparten todos los Estados. Incluso la moneda de posguerra de mejor desempeño, el marco alemán, perdió el 71% de su valor desde 1949 hasta 1999, cuando Alemania adoptó el euro. En el mismo período, el dólar estadounidense perdió el 84% de su valor. Los casos actuales más evidentes son el bolívar venezolano y el dólar zimbabuense, monedas que han perdido millones de veces su valor, hasta el punto en que prácticamente nadie quiere tenerlas.

Bitcoin es la sexta transformación del dinero

En la historia del dinero han existido seis cambios o avances fundamentales:

- Trueque
- Abstracción de valor (conchas, piedras, granos, plumas, ganado, sal, tabaco…)
- Metales preciosos y gemas (oro, plata, cobre, bronce, diamante, esmeralda, rubí…)
- Dinero de papel
- Dinero plástico
- Dinero digital y criptomonedas

Trueque y abstracción de valor

El dinero es la tecnología más antigua creada por la humanidad, precediendo a la invención de la escritura. Se piensa que el dinero dio origen a la escritura como un mecanismo de registro de cuentas, ante las evidentes limitaciones de la tradición oral. Se estima que entre

15.000 y 9.000 a.n.e., ya se empleaban granos de trigo y cebada, rocas y ganado como medio de intercambio o trueque.

Para que un sistema de trueque funcione es fundamental que cada individuo quiera el bien de otro y que las cantidades deseadas coincidan con sus disponibilidades. Un individuo que posee cualquier excedente de un bien, ya sea una medida de grano, como trigo o cebada, o bien un cierto número de cabezas de ganado, podría intercambiarlos por algo que percibe como de valor similar o mayor utilidad, como herramientas, utensilios, alhajas, por ejemplo.

La capacidad para llevar a cabo

transacciones mediante trueque es limitada y se considera un mecanismo costoso en función de tiempo y esfuerzo, porque depende de una doble coincidencia de deseos. El vendedor de grano tiene que encontrar a alguien que quiera comprar grano, y que también pueda ofrecer a cambio algo que el vendedor quiera comprar.

Metales preciosos

La utilización de metales preciosos como el oro, la plata, el bronce y el cobre como dinero tuvo su origen en Mesopotamia alrededor de 2.500 a.n.e. Distintos códigos legales, entre ellos el famoso Código de Hammurabi (1760 a.n.e.), formalizaron el papel del dinero

en la sociedad civil, estableciendo pagos en cantidades fijas de pesos en plata para intereses de deudas, multas por delitos y compensación por diversas infracciones a la ley.

Acuñación de moneda y dinero de papel

Hasta ese momento se había utilizado varios metales y piedras preciosas como dinero por las ventajas que ofrecían en comparación con otros tipos de medios de intercambio, usándose estos metales y piedras por su peso. Las primeras acuñaciones de moneda se produjeron alrededor de 600 a.n.e. en tres lugares del planeta de manera independiente, en Lidia –actual Turquía–, en China y en

India. El metal se fracciona en pequeños trozos, se lo funde, se le da una forma determinada y se marca con una señal que lo identifica.

El papel moneda apareció en China en el siglo VII, pero su uso no fue oficial hasta el siglo IX, el año 812. Hubo tanto escepticismo por parte de los usuarios, quienes no podían entender por qué un trozo de papel valía lo mismo que un trozo de oro, que la aceptación generalizada del dinero de papel tardó 400 años.

En Europa, los primeros billetes de los que hay constancia aparecieron cuatro siglos más tarde en Suecia, específicamente en 1661, de la mano del

cambista Johan Palmstruch, quien los entregaba como comprobante o recibo para los depositantes de oro u otro metal precioso en el Banco de Estocolmo que él mismo había fundado. A la península Ibérica llegaron a finales del siglo XVIII durante el reinado de Carlos III, y su uso se popularizó rápidamente por ser mucho más cómodo de llevar que las bolsas llenas de monedas tan pesadas y llamativas.

Durante gran parte del siglo XX, en términos muy generales, la emisión monetaria estaba respaldada por el patrón oro; en otras palabras, cada emisión de dinero que hacían los bancos privados y más tarde los bancos

centrales, debía estar respaldada por una determinada cantidad de oro. Esto fue así hasta la década de 1970, cuando se dejó de utilizar el oro como respaldo de la moneda. De ahí en más, el valor de las monedas fiduciarias ya no está respaldado por oro sino por la confianza en el Estado que las emite.

Durante los Acuerdos de Bretton Woods en 1945, se decidió adoptar el dólar estadounidense como divisa internacional bajo la condición de que la Reserva Federal –el banco central de ese país– sostuviera el patrón oro, pero a partir de 1971, durante el gobierno de Richard Nixon, este respaldo de emisión se eliminó definitivamente, por lo que el

valor del dólar pasa a sostenerse exclusivamente en la confianza otorgada por sus poseedores. Puedes probar esta verdad leyendo lo que dicen los billetes de dólares americanos. Mientras antes indicaban que cada billete representaba monedas de oro, hoy dice la frase "IN GOD WE TRUST", ("En dios confiamos").

Dinero plástico

Junto con los cajeros automáticos, las tarjetas de crédito –inventadas por Frank McNamara, Ralph Schneider, Matty Simmons y Alfred Bloomingdale, fundadores de Diners Club– son las únicas innovaciones de la banca en más de sesenta años. Debido a que es un sector extremadamente regulado y

muchas veces intervenido por los gobiernos, la banca no ha tenido la libertad de innovar.

Es indiscutible que el dinero plástico es más cómodo, útil y seguro que el dinero en efectivo; sin embargo, su uso masivo representa una invasión absoluta a la privacidad de los usuarios. Tanto los bancos como los Estados tienen acceso casi inmediato a todas las transacciones realizadas por las personas que emplean este medio de pago. Los gobiernos se valen de esta útil herramienta para controlar la evasión fiscal. Ésta es la razón fundamental por la que los Estados, a lo largo y ancho del mundo, han declarado abiertamente

la guerra contra el dinero en efectivo que, junto con las criptomonedas, representan el último reducto de privacidad que tenemos los ciudadanos.

Dinero digital

El uso del dinero digital no es nuevo, empezó a utilizarse en la década de 1970 cuando la tecnología informática lo hizo posible. Se calcula que el 92% de los dólares estadounidenses en circulación son digitales –se mueven por medio de transacciones electrónicas entre los bancos–, el restante 8% se encuentra físicamente en la forma de billetes de papel y monedas.

Hoy el dinero está controlado por los gobiernos y los bancos centrales,

que en el caso de Estados Unidos es incluso una institución privada, que crea y presta el dinero que ellos imprimen al gobierno y otros bancos privados. Es decir, hay una administración centralizada en manos de pocos, con todas sus ventajas y desventajas. La pregunta es si con el invento del bitcoin como moneda descentralizada estamos llegando a un momento de grandes cambios en la historia monetaria. El ganador del Premio Nobel, Friedrich August von Hayek ya propuso en 1976 la introducción del mercado libre para las divisas, para que la gente pueda escoger cuál es el mejor dinero para ellos; de esa forma se evitaría el monopolio del Estado sobre el dinero. La obra "*The*

Sovereign Individual”, escrita hace veinte años por James Dale y William Rees-Mogg, profetiza la aparición de “cibermonedas” controladas por algoritmos matemáticos que no tienen jurisdicción y que por tanto trasladan la riqueza de los ciudadanos a un entorno donde no está sujeta a la coacción de los gobiernos. Con estos cambios los ciudadanos podrían recuperar nuevamente su soberanía sobre el dinero y no depender de horarios bancarios, requisitos de aperturas de cuentas o una exclusión del sistema financiero.

Bitcoin cumple 10 años

El totalitarismo financiero terminó el 3 de enero de 2009 con la invención de Bitcoin y el minado del "bloque génesis".

ANDREAS ANTONOPOULOS

Hace más de diez años, a finales de octubre de 2008, cuando el banco de inversiones Lehman Brothers se

declaraba en bancarrota y la economía mundial estaba cayendo en una grave crisis económica, la idea de una moneda digital alternativa se hacía realidad. En los últimos 10 años, Bitcoin se ha transformado de un juego de "geeks" y una declaración frontal contra lo establecido, a una herramienta muy familiar para casi todas las personas.

Quizás lo más atractivo y misterioso al mismo tiempo acerca de Bitcoin es su origen. Este sistema de pagos fue inventado por un criptógrafo anónimo que usaba el pseudónimo de "Satoshi Nakamoto". El 31 de octubre de 2008 Satoshi publica el libro blanco "whitepaper" de Bitcoin a través de una

lista de correos que trata temas de criptografía con el título: “Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario” (la version en español la encuentras aquí: https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf). Si bien es cierto que hasta ahora se desconoce su identidad real, se alega que obviamente se trata de alguien de origen japonés; no obstante, muchos especulan que su origen asiático es poco probable teniendo en cuenta el perfecto inglés con el que escribía y que el software de Bitcoin no se etiquetaba en japonés. Otros piensan que un código de software tan brillante e innovador no pudo ser escrito por una sino por varias personas.

A medida que Bitcoin comenzó a ganar popularidad, Satoshi dejó de tener actividad en el foro de desarrolladores en 2011; debido a esta situación Gavin Andresen, un ingeniero de software, fue el que asumió la batuta del desarrollo del software de código abierto de Bitcoin. Una de las razones del anonimato de Satoshi es su propia seguridad. Otros intentos de crear dinero virtual o privado terminaron con la encarcelación de sus inventores. Para que una persona pruebe que es Satoshi Nakamoto, sólo tendría que hacer una transacción de una de las direcciones de Bitcoin donde están guardadas las monedas que pertenecen a este creador

misterioso. En los primeros meses de existencia del bitcoin sólo Satoshi creaba nuevas monedas a través de la minería y por eso es fácil de saber cuáles direcciones deben estar en su poder. Si deseas conocer más detalles de la comunicación de Satoshi Nakamoto te recomendamos "*El Libro de Satoshi"* de Phil Champagne, que ofrece una amplia documentación sobre sus ideas.

El objetivo del bitcoin, según su libro blanco, es sencillo: "Una versión puramente electrónica de dinero entre pares que permite que los pagos en línea se envíen de persona a persona sin pasar por una institución financiera". Satoshi

había resuelto el problema del "doble gasto" que otras monedas digitales fallidas como e-Cash o DigiCash en los años 90 no lograron. Teniendo en cuenta que Bitcoin no es más que código de software, se debía encontrar la manera de impedir que pueda ser copiado indiscriminadamente. Para lograr este objetivo y de paso asegurarse de que las transacciones no necesiten de un tercero, Bitcoin emplea, entre otras tecnologías, la cadena de bloques (blockchain), que es en pocas palabras, un libro contable distribuido e inmutable que puede guardar cualquier tipo de datos. La red registra en tiempo real y públicamente las transacciones que ocurren, cada una de ellas se almacena en un bloque de la

cadena de bloques, creando un registro secuencial ordenado cronológicamente que no puede ser alterado o borrado y que al mismo tiempo se encuentra replicado en miles de nodos distribuidos alrededor del mundo. En un mundo centralizado los bancos se encargan en sus servidores de controlar que nadie gaste su dinero dos veces, para garantizar esta seguridad de forma descentralizada tuvimos que esperar al invento de Satoshi Nakamoto, que no requiere la confianza en un tercero, sino que permite realizar transacciones con plena confianza entre iguales Persona-a-Persona (Peer-to-Peer).

Hitos importantes de Bitcoin

El 3 de enero de 2009, Satoshi Nakamoto minó con éxito el "bloque génesis" dando la patada inicial a la cadena de bloques de Bitcoin que, una vez en funcionamiento, en términos prácticos, ya no puede ser detenida.

JUAN F. BOLAÑOS

La primera transacción de bitcoins se realizó el 12 de enero de 2009, entre Nakamoto y el fallecido Hal Finney, quien fue uno de los primeros contribuyentes de este proyecto. Nakamoto envió a Finney 10 BTC como prueba, mientras que el científico

informático comenzó a minar bloques por su cuenta.

Como todas las transacciones tienen su registro en la cadena de bloques puedes encontrar este primer bloque aquí:

https://www.blockchain.com/es/btc/block/0000 (https://bit.ly/2Mn3V9P)

Diez meses después, el 5 de octubre de 2009, el New Liberty Standard estableció el primer tipo de cambio del bitcoin frente al dólar estadounidense, 1 USD equivalía a 2.300 BTC. El 9 de febrero de 2011, el bitcoin alcanzó la paridad con el dólar estadounidense, a partir de ese entonces, tan sólo en cuatro meses, el valor del

bitcoin se disparó a 31,91 USD por unidad.

El 28 de noviembre de 2012 se produjo la primera reducción (halving) de la recompensa de minado (block reward), pasando de 50 a 25 BTC por cada bloque producido. El 9 de julio de 2016 ocurrió la segunda reducción de 25 a 12,5 BTC; la próxima reducción va a ocurrir en mayo de 2020 cuando la recompensa baje de 12,5 a 6,25 BTC. El precio de la criptodivisa continuó subiendo en 2013, superando los 200 dólares por primera vez el 9 de abril. Antes del quinto aniversario del libro blanco, el sitio web Silk Road cerró y se incautaron 26.000 BTC, bajando el

precio de 139 a 109 USD por unidad en pocas horas. En noviembre de 2013, el valor de un solo bitcoin alcanzó la paridad con el de una onza de oro; sin embargo, esta hazaña duró sólo pocos días, ya que al cabo de un mes el precio cayó a 600 dólares.

El año 2017 marcó el comienzo de lo que sería la carrera alcista más grande de la historia del bitcoin hasta el momento. Habiendo superado la marca de 1.000 USD tres años antes, el 2 de enero de 2017 volvió a hacerlo. El 11 de junio cruzó la marca de 3.000 USD por primera vez, en medio de un arduo debate que se hallaba en curso sobre las posibles medidas para solucionar los

serios problemas de escalabilidad que afectan a la blockchain de Bitcoin Como era de esperarse, parte de la comunidad no estuvo de acuerdo con los cambios propuestos, por lo que el 1 de agosto ocurrió la bifurcación dura de la cadena de bloques de Bitcoin, la cual dio origen a Bitcoin Cash. Aún así, su valor continuó incrementándose y superó la marca de los 5.000 USD el 2 de septiembre de 2017. A partir de octubre de ese año, luego de la corrección de rigor en su precio, el bitcoin emprendió una agresiva carrera alcista superando los 10.000 USD el 29 de noviembre. La criptomoneda continuó ganando valor a medida que los inversionistas se apresuraban a unirse a la acción.

Finalmente rompió la barrera de los 20.000 USD en diciembre de 2017. Para no alargar la historia, durante todo el año 2018 el bitcoin sufrió importantes correcciones en su precio, perdiendo más de cinco veces su valor en comparación con el máximo alcanzado en 2017. En el 2019 vimos como llego a 3.200 USD, el punto más bajo de la corrección de precio antes de entrar a la próxima carrera alcista que le hizo superar los 10.000 USD nuevamente.

El futuro del dinero

Cuando hablamos de Bitcoin no solamente hablamos de una moneda; estamos siendo testigos de la refundación de los sistemas sociales que

nos han fallado constantemente: los Estados y la banca. Estos sistemas jerárquicos basados en paradigmas del siglo XVIII están siendo reemplazados por sistemas abiertos, horizontales y descentralizados.

Durante más de dos décadas, después de la invención del automóvil, los medios de comunicación masiva seguían diciendo que estos eran unas máquinas ruidosas, sucias, que no podían llegar a cualquier lado, que se dañaban constantemente, que eran inferiores a los caballos, que sólo los raros los usaban y que eran peligrosos tanto para sus conductores como para los transeúntes. Lo mismo ocurrió con la

electricidad, se decía que era una tecnología sumamente peligrosa que incendiaba los hogares y que electrocutaba a sus usuarios, en lugar de decir que era un invento que estaba cambiando al mundo y mejorando la vida de la gente. Sus detractores dicen que Bitcoin es una tecnología extraña y complicada que da refugio a estafadores, terroristas, narcotraficantes, hackers, ladrones y lavadores de dinero.

La invención de la imprenta en el siglo XV terminó con el trabajo de los monjes escribanos y terminó con el monopolio de generación de conocimientos; los automóviles desplazaron a los caballos como un

medio de transporte más confiable y rápido; la electricidad reemplazó al uso de combustibles fósiles para iluminar los hogares de una forma más barata y segura; el correo electrónico terminó con el trabajo de los carteros. ¿Bitcoin dejará de lado a bancos y los Estados-nación al terminar con el monopolio de emisión monetaria?

La innovación detrás de Bitcoin

Bitcoin no es una organización ni una empresa, es un protocolo como el Internet. No tiene dueño, es una red distribuida de computadores que operan a través de un algoritmo matemático de consenso que establece las reglas del juego y procesa y valida las

transacciones. Bitcoin no es dinero, no es un sistema monetario, no es una compañía, no es un producto, no es un servicio al que te afilias. El dinero es su primera aplicación. Es el concepto de la descentralización aplicado a la comunicación de valor.

Aún quedan muchos desafíos por superar, pero lo importante ya ocurrió: se demostró que el dinero puede ser emitido por un sistema informático descentralizado que no depende de intermediarios ni de una autoridad central para su funcionamiento ni para generar confianza, esto quiere decir que las personas adquieren absoluta soberanía sobre su dinero.

¿Por qué el bitcoin tiene valor?

El bitcoin es una criptomoneda compuesta de bits, de código de software que carece de una representación física, no está respaldada por ningún Estado y prácticamente no está regulada en ningún país, salvo contadas excepciones. ¿Por qué una moneda intangible puede tener valor tangible? Existen diferentes puntos de vista que van desde su valor técnico –solución del problema de doble gasto–, pasando por el hecho de que facilita el comercio y el movimiento de capitales al ser una moneda global con bajos costos transaccionales, representa una

excelente alternativa a medios de pago tradicionales como las tarjetas de crédito tanto por seguridad como por costos, y es útil y aceptado. El término "aceptado" significa que existe una confianza por medio de sus usuarios en ello, caso contrario no lo aceptarían. La confianza es uno de los principales factores que da valor a una moneda o un activo. Algunos economistas sostienen que para que el dinero tenga valor éste debe estar respaldado por un gobierno que tenga autoridad fiscal y de gasto; dicho de otro modo, ese dinero debe servir para pagar impuestos y para que el gobierno lo gaste. Sin embargo, la historia nos mostró varios ejemplos en

los cuales el "respaldo" de una moneda por medio de un gobierno no ha sido muy útil. La República de Weimar (nombre que tuvo Alemania entre 1918 y 1933), tenía autoridad para cobrar impuestos y gastarlos, no obstante imprimió marcos alemanes indiscriminadamente, generando hiperinflación, lo que hizo que los ciudadanos y otros países dejaran de aceptarlos y exigieran oro o carbón en su lugar. El más reciente ejemplo latinoamericano de hiperinflación ocurre en Venezuela.

Otros factores como la escasez, la usabilidad y el trabajo que cuesta producir o conseguirlo juegan un rol

importante. En el caso del oro vemos que su valor se basa en la escasez, el esfuerzo que cuesta fabricarlo y el uso que se le puede dar, como por ejemplo en las joyas. El bitcoin hoy en día nos muestra características similares al oro que se desarrollaron en el tiempo.

Al inicio, en 2009, la moneda no tenía ningún valor para nadie. Nadie confiaba en ella y tampoco se le podía usar en ningún lugar; es decir, lo que tenía el bitcoin era un "costo de producción" que se basaba en el costo de la energía eléctrica y el desgaste en hardware que era necesario para minar un bitcoin. El costo en octubre de 2009 era de 0,000434 centavos de dólar; con

1 USD se podían comprar 2.300 unidades de bitcoin. Hoy el proceso de producción, la "minería" de bitcoin, es mucho más costoso. Minar un bitcoin cuesta varios miles de dólares en hardware y energía eléctrica y con eso el valor de un bitcoin es mayor que el del dinero en papel, cuya impresión cuesta centavos.

Un paso importante en la valorización de la moneda se dio el 22 de mayo de 2010, fecha que hoy millones de entusiastas de criptomonedas festejan como el Bitcoin Pizza-Day. Ese día Laszlo Hanyecz ofreció en un foro de bitcointalk.org pagar 10.000 monedas bitcoin a la

persona que le entrega 2 pizzas (puedes buscarlo en internet y vas a poder leer la comunicación original en inglés que es muy graciosa). Después de unas propuestas alguién compró las pizzas y se las entregó a Laszlo, quien después generó la transacción. La transacción quedó registrada en la blockchain para siempre y la puedes ver aquí:

https://www.blockchain.com/btc/tx/a1075db55c
(https://bit.ly/2Zkjwus)

Después de esa transacción las personas se dieron cuenta de que con bitcoins se pueden comprar productos físicos y se preguntaban si sería posible en un futuro comprar otros bienes también con bitcoins. Así empezó a crecer la confianza en la moneda, su

usabilidad, y con eso también su valor.

De la mano con la valoración va la cantidad de usuarios que empezaron a abrir una billetera y usar la moneda. Además creció la cantidad de comercios y personas que aceptan bitcoins como forma de pago. Mientras más crece el ecosistema, más valor va a tener la moneda.

Uno de los factores importantes en el ecosistema de Bitcoin es que la cantidad de monedas es limitada a un máximo de 21 millones de unidades. Eso quiere decir que la demanda por la moneda puede aumentar, sin embargo la oferta es limitada. Para crear un equilibrio entre oferta y demanda el

precio tiene que subir cuando sube la demanda.

Esta oferta limitada de monedas representa una gran diferencia con el sistema monetario manejado por los bancos centrales que pueden emitir la cantidad de nuevos billetes que ellos determinen; así surge una inflación en la que los billetes cada vez valen menos. Contrariamente, las criptomonedas tienen un sistema diferente, deflacionario, con reglas claras y abiertas y con límites definidos para la creación de nuevas monedas.

Las predicciones indican que un bitcoin puede valer 100.000 USD, 500.000 USD y más de 1 millón de USD

en un futuro. ¿Por qué un precio de más de 100.000 USD sí es posible? Proponemos que la capitalización del bitcoin alcanzará la del oro, que es de aproximadamente 7 billones de dólares. Con 18 millones de monedas minadas el precio estaría en 389.000 USD por bitcoin. Eso puede pasar en los próximos años, como puede no pasar. Hay muchísimos factores que hay que tener en cuenta.

La escasez, el costo de producción a través de la minería, su usabilidad para pagos y la confianza, son los principales factores que han llevado al bitcoin a tener un valor. Estos factores son parecidos a lo que le da

valor al oro

físico y esa es una de las razones por lo que se dice que el bitcoin es el “oro digital”.

¿Por qué deberías usar criptomonedas?

> *El progreso de la humanidade siempre involucró a una pequeña minoria que se desviaba de las ideas y costumbres de la mayoría, hasta que su ejemplo finalmente persuadió a otros a adoptar también sus innovaciones.*
>
> LUDWING VON MISES

Paul Krugman, premio Nobel de economía, es un abierto opositor a

bitcoin y las criptomonedas. Él manifiesta que el dinero fiduciario no existe por una razón arbitraria, sino que es la mejor solución que ha encontrado la humanidad para comerciar. Siguiendo esta premisa, explica que bitcoin y las criptomonedas son una tecnología cara de mantener, difícil de escalar y que no tiene razones para convivir en el mundo real dado que, en este sentido, no es tan útil. Por otro lado el austriaco Friedrich August von Hayek, también ganador del premio Nobel, es defensor de la idea de una libre competencia entre monedas tanto privadas como estatales. El bitcoin es la primera moneda global no hecha por un Estado y por ende nos encontramos en una competencia entre

diversas monedas en la que según Hayek va a resultar ganadora la mejor opción para el usuario. Como nadie está obligado a usar bitcoins la decisión de hacerlo depende de los beneficios que ofrece.

Vamos a ver a continuación algunos argumentos y ventajas que han atraído a millones de usuarios hacia el bitcoin y otras criptomonedas:

Transparencia

Cada transacción de bitcoins queda registrada en la cadena de bloques de forma abierta y para siempre.

Escasez

Existe una cantidad fija de monedas y no se puede crear más. Eso implica que con

un aumento de la demanda el valor va a subir en búsqueda del equilibrio de oferta y demanda. En el caso del dinero fiat, la cantidad que puede existir es infinita y con ello existe una inflación que quita valor al dinero.

Participación

Cada persona puede participar en el sistema de la creación de nuevas monedas y recibir una recompensa a través de la minería. La red informática de Bitcoin se basa en reglas de consenso respaldadas por algoritmos informáticos y funciona de usuario a usuario sin la participación de un intermediario bona fide. En cambio el dinero fiat es administrado por los bancos centrales y

sólo dejan participar a la gente común como usuarios, no como parte activa del sistema. El control de poder está en manos de pocos.

Acceso universal

Las criptomonedas representan una gran e innovadora alternativa para quienes no poseen acceso a la banca tradicional. De acuerdo a datos del Banco Mundial, 2.500 millones de personas y el 75% de los pobres no tienen acceso a servicios financieros formales por diversas razones. Las criptomonedas pueden hacer mucho más por la inclusión financiera que los bancos y los gobiernos y, lo más importante de todo, a una fracción del costo y del tiempo.

Para tener una billetera de bitcoins no se requiere de una autorización central; es decir, todas las personas con un dispositivo digital pueden tener acceso y no necesitan verificarse.

Globalidad

No pertenece a ningún Estado o banco. Puede operar como medio de pago en todo el mundo y evita la necesidad de cambio a monedas locales.

Funcionalidad sin interrupción

Las transacciones de bitcoins funcionan las 24/7 y no son sujetas a feriados, horarios bancarios o fines de semana.

Seguridad

La criptografía y un sistema

descentralizado a través de los nodos de la blockchain, permiten brindar un alto nivel de seguridad a los usuarios. Mientras que con el dinero fiat encontramos sistemas centralizados y vulnerables. Las tarjetas de crédito o débito, por ejemplo, son inseguras por defecto; cuando realizamos una compra y entregamos nuestra tarjeta al comerciante le estamos dando acceso completo a nuestra identidad y fondos. Un comerciante deshonesto o un pirata informático que ha accedido a las bases de datos centralizadas de los bancos, puede suplantar fácilmente nuestra identidad y robar nuestro dinero.

Falsificación y riesgo de fraude

Las criptomonedas no pueden ser falsificadas ni sus transacciones revertidas arbitrariamente por el remitente ni por la coacción de las autoridades, tal y como ocurre con las transacciones bancarias y las realizadas con tarjetas de crédito o débito. Además existen miles de billetes falsos del dinero fiat circulando en todo el mundo.

Libre en su uso

Nadie está obligado a usar bitcoin como medio de pago, contrariamente, los gobiernos definen su moneda de curso legal y con eso obligan su uso. Esta política puede causar problemas en una mala administración, como podemos observar con el bolívar en Venezuela u

otros países en crisis.

Rapidez

La latencia es un término que define la velocidad con la que una transacción es completada y liquidada; dicho de otro modo, ésta no puede ser detenida o revertida. La latencia de una transacción registrada en una cadena de bloques es de minutos. En cambio, transacciones internacionales del sistema bancario se demoran días en efectivizarse. Lo mismo pasa en el proceso de liquidación de pagos con tarjetas de crédito que retienen la liquidez del comercio durante días.

Tarifas más convenientes

El costo aproximado de una

transferencia bancaria internacional es de 50 dólares y, regularmente, tanto el banco emisor como el receptor y todos los bancos intermediarios que participan en la transacción se llevan una parte del pastel. Si hablamos de transferencias de dinero realizadas por servicios de pago como Western Union o MoneyGram, la comisión que ellos reciben puede llegar a ser de un 7% del monto total de la transacción. En contraste, las transacciones de bitcoins regularmente son de centavos, y hay monedas como stellar, donde el costo por transacción no llega a ser ni de un centavo.

Divisibilidad

Con ocho decimales el bitcoin es

altamente divisible. Eso permite realizar micropagos usando la unidad más pequeña, que es el satoshi.

Pseudo-anonimato

El anonimato o pseudo-anonimato de las monedas digitales, para unos es una ventaja y para las autoridades uno de los puntos más criticados de las criptomonedas. Los detractores de bitcoin indican que la tenencia anónima de una moneda incentiva su uso en actividades ilegales, como la evasión de impuestos, el narcotráfico, la corrupción política y el tráfico de armas y de personas.

Bitcoin no es una plataforma ideal para llevar a cabo actividades

delictivas que buscan el anonimato debido a la naturaleza transparente y pública de su cadena de bloques, en la que todas las transacciones se registran. El anonimato de Bitcoin es un mito, considerando que siempre se conoce tanto la dirección pública del emisor como la del receptor y el monto de las transacciones –a pesar de que la identidad de los participantes no se relaciona con aquellas–, por lo tanto es posible rastrear las direcciones IP involucradas en el proceso y lograr identificar quienes están por detrás. Adicionalmente, en ciertos casos, se requiere de la validación de la identidad personal, en cumplimiento con las normativas KYC y AML, para poder

usar algunas plataformas de intercambio de criptoactivos y billeteras digitales.

Un estudio del Centro de Sanciones y Finanzas Ilícitas de la Fundación para la Defensa de la Democracia, afirma que los bitcoins "sucios" que provienen de actividades ilícitas representan entre el 0,61 y 1,07% del volumen total de las transacciones. De hecho, el dinero fiat en efectivo, como el dólar o el euro, son la forma preferida para las transacciones ilegales porque una vez intercambiado el efectivo, éste no deja forma de rastrearlo. Esa es una de las razones que declaran los gobiernos para deshacerse del dinero en efectivo y en

algunos países, sobre todo europeos, están en buen camino de lograrlo en los próximos años. La razón real para deshacerse del dinero en efectivo es la falta de control sobre estas transacciones.

¿Alguna vez has pensado en cómo sería un mundo sin dinero en efectivo? Significaría que un tercero, en este caso el banco como entidad privada o el gobierno, puede decidir sobre tu inclusión en la sociedad. Sin dinero en efectivo tendríamos necesariamente que usar medios electrónicos de pagos, como tarjetas de débito/crédito o transferencias. En el momento de un cierre de cuentas no vamos a estar en la

capacidad ni de comprar pan y leche para el hogar; es decir, no vamos a poder participar en la vida económica y para sobrevivir tendríamos que regresar cientos de años de evolución, al trueque nuevamente, para conseguir los alimentos para la casa.

El atractivo futuro de las criptomonedas consiste en permitir a las personas el máximo control sobre su dinero con transacciones globales rápidas, seguras y con tarifas más bajas en comparación con el sistema financiero tradicional. Para los ciudadanos de los países del tercer mundo, quienes somos víctimas frecuentes de gobiernos populistas,

totalitarios y corruptos, las criptomonedas representan una gran oportunidad para alejar sus garras e injerencia de nuestras vidas.

Altcoins

Hasta ahora el libro se ha enfocado sobre todo en el bitcoin como la primera criptomoneda. Sin embargo, el año 2011, con Namecoin nace la primera "altcoin" o "moneda alternativa". La mayoría de las altcoins se basan en el código fuente de bitcoin y muestran unos cambios al código original. Es decir, estas monedas fueron creadas a través de un "hardfork" con el objetivo de ser una mejor versión que el original o permitir funciones adicionales o diferentes. Sin embargo sólo pocas monedas muestran innovaciones

importantes comparadas con el bitcoin. Otra forma de crear una nueva moneda es a través de un token como el ERC20 en la blockchain de Ethereum.

Las monedas listadas en casas de cambio "exchanges" las puedes encontrar en www.coinmarketcap.com. La mayoría de las monedas registradas en esta página son legítimas. Si quieres saber si una moneda es legítima o si tal vez forma parte de un sistema de fraude, puedes revisarlo en los capítulos de pirámides y scamcoins o shitcoins.

Durante mucho tiempo el bitcoin dominaba la criptoeconomía con una capitalización del 80 al 90% de todo el mercado. Sin embargo en el 2017 eso

cambió, los altcoins subieron de valor e importancia y el bitcoin bajó hasta menos del 50% de participación.

A continuación presentamos una serie de altcoins que nos parecen interesantes. No es una lista completa y sólo el hecho de que mencionemos una moneda aquí no es una garantía de que ésta tendrá éxito en el futuro.

Litecoin (LTC)

Litecoin es la plata digital;
bitcoin es el oro.

BILL BARHYDT

Litecoin (LTC) ha tomado al mundo por sorpresa, mientras bitcoin se usará para

adquirir una casa o un auto; litecoin será usado para gastos diarios como ir de compras o pagar por servicios de todo tipo.

Los orígenes de Litecoin

Si bien la identidad del creador de Bitcoin, Satoshi Nakamoto, está envuelta en un halo de misterio, el creador de Litecoin, Charlie Lee, es muy activo en las redes sociales y su blog. Charlie Lee es un exempleado de Google que tuvo la visión de crear una versión más ligera de Bitcoin. La cadena de bloques de Litecoin fue lanzada a través de un cliente de código abierto el 13 de octubre de 2011. Técnicamente es una bifurcación dura de Bitcoin Core.

Una de las diferencias esenciales entre Bitcoin y Litecoin es su proceso de minería. Ambos emplean el algoritmo de consenso conocido como Prueba de Trabajo. Bitcoin usa el algoritmo criptográfico SHA 256 para minar los bloques de su cadena. Los «hashes» generados por este algoritmo requieren de mucha potencia de procesamiento, lo que se traduce en un gran consumo de energía eléctrica. Con el surgimiento de hardware ASIC la minería de bitcoin se ha convertido en una actividad de escala industrial que se ha ido centralizando en contra de los deseos de Satoshi.

Litecoin ha encontrado una solución a los inconvenientes de

centralización y gasto de energía utilizando el algoritmo criptográfico conocido como Scrypt.

¿Qué es Scrypt?

Este algoritmo criptográfico de hecho utiliza el algoritmo SHA 256; sin embargo, los cálculos se realizan en serie en lugar de en paralelo como en Bitcoin. Supongamos que tenemos dos procesos: A y B. En Bitcoin, el hardware ASIC tiene la capacidad de efectuar los dos procesos en paralelo, al mismo tiempo. En Litecoin dichos procesos deben ser efectuados uno tras otro; es decir, en serie.

El tiempo de duración de un bloque en Litecoin es de 2,5 minutos, el

de Bitcoin es de 10 minutos. Siendo cuatro veces más rápido y también con una cantidad máxima de 84 millones de monedas, se van a crear cuatro veces más litecoins que bitcoins. Esta característica es extremadamente útil para los comerciantes, quienes usualmente procesan muchísimas transacciones pequeñas diariamente.

Si bien es cierto que el litecoin fue concebido como el hermano menor del bitcoin, ha tomado una y otra vez los riesgos necesarios para demostrar a las masas el verdadero alcance y el potencial de las criptomonedas. Litecoin fue el primero en implementar SegWit y también han probado con éxito los

Intercambios Atómicos (Atomic Swaps). Del mismo modo, se ha implementado Lightning Network en su red. Por ser una comunidad menos extensa que la de Bitcoin es más fácil llegar a un consenso para estas nuevas implementaciones tecnológicas.

Bitcoin Cash (BCH)

Todo lo que puede hacer Bitcoin (BTC), Bitcoin cash (BCH) puede hacerlo mejor.

ROGER VER

El hardfork más exitoso hasta el momento del Bitcoin es el Bitcoin Cash. Esta moneda nació el 1 de agosto de

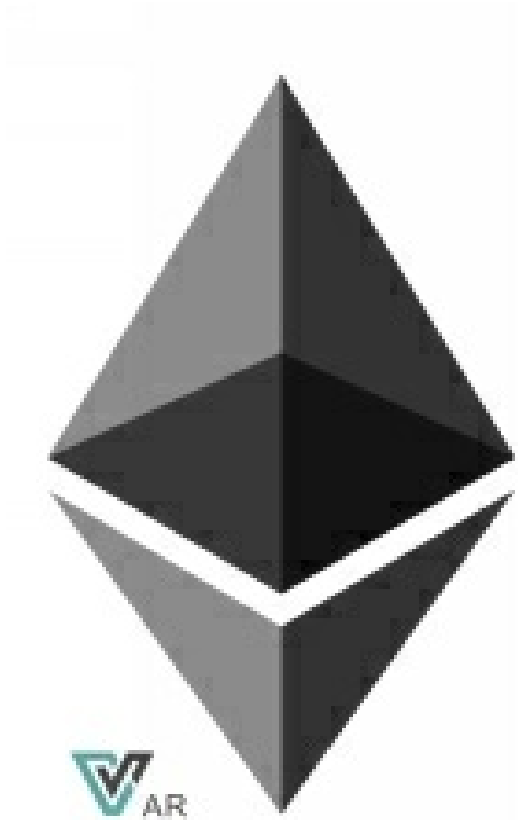
2017 y la razón número uno ha sido la disputa sobre SegWit (Segregated Witness). BCH decidió aumentar el tamaño de bloques de 1 MB de la blockchain de Bitcoin, a 8 MB. Eso significa que Bitcoin Cash puede realizar más transacciones en menor tiempo y a menor costo. Uno de los mayores inversores y promotores del BCH es Roger Ver, que está invertido en varios startups de Bitcoin y dice que el bitcoin cash es el verdadero bitcoin. Las visiones de ambas monedas se están alejando. Bitcoin apunta a ser el oro digital que no requiere tanta atención sobre la rapidez en transacciones sino más estabilidad, mientras que el BCH quiere convertirse en un medio de pago

masivo que requiere rapidez y bajos costos de transacción. El 15 de noviembre de 2018 el Bitcoin Cash nuevamente parte en dos monedas a través de un hardfork y nacen Bitcoin Cash ABC y Bitcoin Cash SV.

Ethereum (ETH)

Se supone que la principal ventaja de la tecnología blockchain es que es más segura, pero generalmente la gente no confía en las nuevas tecnologías, y esta paradoja no puede ser realmente evitada.

VITALIK BUTERIN



Ethereum es una plataforma abierta de software basada en la tecnología blockchain que permite desarrollar aplicaciones descentralizadas (DApps, por sus siglas en inglés), contratos inteligentes (smart contracts) y organizaciones autónomas descentralizadas (DAO, por sus siglas en inglés). Al igual que Bitcoin, Ethereum es una red de computadores que alojan una cadena de bloques abierta y distribuida. Ethereum es esencialmente un protocolo, al igual que BitTorrent, Bitcoin, TCP/IP, POP3, IMAP y SMTP.

De acuerdo a Vitalik Buterin, uno de sus creadores, Ethereum es una

plataforma universal con un lenguaje de programación interno (Solidity) para que cualquiera pueda desarrollar aplicaciones. Es descentralizada en el sentido en que nadie puede imponer sus decisiones a la comunidad. Ethereum no tiene dueños.

Básicamente, Ethereum ejecuta programas que no pueden ser detenidos, son incorruptibles y capaces de ejecutar pagos irreversibles, características ideales para hacer contratos que pueden ejecutarse a sí mismos sin la necesidad de bancos, notarías o abogados.

Aplicaciones de Ethereum

Por motivos de tiempo y espacio, nos limitamos a nombrar unas pocas de las

diversas aplicaciones que Ethereum puede tener:

- Fideicomisos
- Gobernanza experimental (democracia colaborativa)
- Sistemas de votación verificables en tiempo real
- Mercados P2P
- Servicios de pronóstico
- Redes sociales
- Transporte compartido distribuido
- Trazabilidad de productos
- Manejo descentralizado de salud, historias clínicas dinámicas
- Pólizas de seguros
- Plataformas de inversión y préstamos

- Sistemas de identidad, certificación y reputación
- Registros crediticios y de propiedad
- Creación de criptomonedas
- Servicios de contabilidad en tiempo real
- Elaboración de contratos inteligentes
- Plataformas de transmisión de audio y video
- Juegos de azar

Ether (ETH)

Ether es la criptomoneda nativa de Ethereum. Ethereum es el nombre de la tecnología, el software y el mainnet. Ether (ETH) es la criptomoneda con la

que se paga por utilizar los servicios de la red de Ethereum. En julio de 2014 la ICO de Ethereum recaudó 30.000 bitcoins, aproximadamente 14 millones de USD en ese tiempo y el ether inició su cotización en 0,30 USD en los exchanges. Ethereum es el ecosistema más usado hoy en día para la creación de tokens para ICOs.

¿Qué es un contrato inteligente?

Un contrato inteligente es un código de software que corre en la blockchain de Ethereum y facilita el intercambio de dinero, contenido, propiedad, acciones o cualquier cosa de valor. Un contrato inteligente se ejecuta automáticamente una vez que se cumplen determinadas

condiciones que fueron programadas previamente en éste. Debido a que los contratos inteligentes se ejecutan en una cadena de bloques no se pueden detener, modificar, revertir, cancelar o censurar. Un contrato inteligente no tiene ubicación geográfica, vive en el criptoespacio. Según Henning Diedrich, colaborador de IBM y autor del libro "*Ethereum*", un contrato inteligente es al mismo tiempo el acuerdo y la ejecución, la gobernanza y la ley.

¿Qué es una DApp?

Una DApp es una aplicación de código abierto y descentralizada que corre, en este caso, en la blockchain de Ethereum y que utiliza un protocolo o algoritmo de

consenso PoW o PoS como prueba de valor o de veracidad. Una DApp tiene partes que viven adentro y afuera de la cadena de bloques (aplicaciones móviles, sitios web, interfaces, bases de datos). Los contratos que "viven" en la cadena de bloques, son el backend de una Dapp, que a su vez puede ver, crear o ejecutar contratos inteligentes. Un contrato inteligente per se no tiene un "frontend". Ejemplos de DApps: Gnosis, CryptoKitties, Golem, Prism, Augur, Melonport, Status, Brave, Aragon, entre otras.

¿Qué es una DAO?

Una Organización Autónoma Descentralizada (DAO, por sus siglas en

inglés) consiste en una serie de contratos inteligentes que se ejecutan automática y transparentemente en función de las instrucciones que contienen sin la necesidad de la intervención humana. Es posible manejar toda una compañía o cualquier tipo de organización usando una cadena de bloques que ejecuta contratos inteligentes. La idea de una DAO es que se pueda crear una entidad completamente independiente, gobernada exclusivamente por la reglas programadas en una serie de contratos inteligentes, en lugar de las normas y estructuras de una organización tradicional basada en la jerarquía y el control centralizado.

Cómo podemos ver Ethereum, con su moneda, ether, es más que un sistema de pagos; es un protocolo y un nuevo ecosistema para desarrollar un sin fin de aplicaciones, contratos y organizaciones.

NEM (XEM)

La blockchain de NEM, por sus características técnicas de construcción, permite responsablemente proveer servicios que habilitan dinámicamente el progreso y crecimiento económico.

ADRIÁN NARANJO
Embajador de la Fundación NEM en Ecuador

NEM es la abreviatura para New Economy Movement, y eso quiere decir que no sólo es una moneda que en este caso se llama XEM, sino todo un movimiento que está creando una nueva plataforma económica. NEM se fundó a inicios de 2014 por desarrolladores que tenían como meta crear una moneda más justa que el bitcoin. En marzo de 2015

NEM publicó su primera versión y a los dos años se creó la Fundación NEM con sede en Singapur.

La cantidad máxima de XEMs es de 8.999.999.999 monedas que ya fueron creadas y están en circulación. Es decir, no hay un sistema de minería con el cual se aumenta la cantidad poco a poco. Los nuevos bloques en la blockchain de NEM se crean casi cada minuto y en operaciones de prueba se ha alcanzado hasta 10.000 transacciones por segundo.

NEM no aplica la minería para crear consenso; creó un nuevo sistema que se llama PoI (Proof of Importance). Este se parece al Proof of Stake en el

cual la probabilidad de generar el próximo bloque depende de la cantidad de monedas que se mantengan en la wallet. En el caso de PoI no sólo importa la cantidad de monedas que se tengan, sino también la cantidad de transacciones que se hacen desde una wallet; es decir, los usuarios de mayor actividad tienen más probabilidad de generar un bloque y ganar los costos de transacción generadas. Este proceso se llama "Harvesting" (Cosecha). A través de la Nano Wallet de NEM se puede participar en este proceso con un mínimo de 10.000 XEM.

NEM ofrece toda una plataforma para crear diferentes aplicaciones y

tokens. En comparación con Ethereum, ofrece la gran ventaja de que usa lenguajes de programación modernos, como JAVA-Script, que muchos de los desarrolladores en el mundo dominan; en cambio Ethereum tiene su propio lenguaje: Solidity, y éste sólo se puede usar para Ethereum. NEM ha creado una red global de embajadas y embajadores en la mayoría de los países del mundo con la que se quiere promover el conocimiento de esta criptomoneda y crear proyectos a nivel local y global que usen su ecosistema.

DASH

Nosotros queremos llegar a las personas que no están interesadas en criptos.

AMANDA B. JOHNSON
YouTuber de Dash: Detailed y
Dash School

En enero de 2014, Evan Duffield creó

XCoin, cuyo nombre después cambió a darkcoin, para mostrar el nivel de anonimato. Por razones de marketing y la confusión con la Darknet, en marzo de 2015 el nombre cambió nuevamente, esta vez por DASH (DigitalCash), como hoy lo conocemos. DASH funciona como Cash Digital; es decir, permite hacer transacciones anónimas y rápidas tal como lo hace el dinero en efectivo. Entre ZCash y Monero, DASH es la tercera moneda con un alto nivel de privacidad en las transacciones.

Según Ryan Tayler, del Core-Developer Team de DASH, la moneda tiene cuatro factores de diferenciación importantes:

1. Los pagos con DASH son tan rápidos como los pagos con tarjetas de crédito o con efectivo, gracias al InstaPay (pago instantáneo).

2. A través del CoinMix (mezcla de monedas) la privacidad de los usuarios está protegida.

3. Con el sistema de Masternodos (MN) se crea un sistema de gobernanza que decide sobre los desarrollos y el futuro de la moneda.

4. El 10% de las nuevas monedas minadas entran al fondo de marketing y desarrollo y asegura liquidez para pagos al equipo fuera de donaciones.

A través del algoritmo X11, que

combina 11 algoritmos diferentes, se va a minar un aproximado de 18 millones de monedas. La cantidad de nuevos DASH por bloque –cada 2,5 minutos– es flexible. Cuando se requiere un aumento de la cantidad de mineros la recompensa crece y cuando hay demasiados la recompensa baja. Además hay una deflación programada que indica que la cantidad de nuevas monedas creadas cada año decrece un 7,1%.

Una de las diferencias más grandes con respecto al sistema de Bitcoin, es que en Bitcoin los mineros reciben el 100% de las monedas minadas; DASH lo reparte de esta

forma: el 45% lo reciben los mineros, 45% va a los dueños de MN y el 10% es para el fondo de desarrollo y marketing.

Para operar un MN se requieren 1.000 DASH en la core wallet y conectarlos a un servidor. Por brindar este servicio a la red, el dueño del MN recibe su recompensa, igual a la de un minero. Los usuarios de DASH se benefician de pagos instantáneos y pagos privados que se permiten hacer por habilitar Masternodos. En la tercera parte de este libro (Finanzas), se incluye más información sobre el funcionamiento y la rentabilidad de los MNs.

La administración de DASH se

maneja a través de una DAO en la que cada dueño de MN tiene un voto. En una DAO todos mandan y no hay jefes. Cada mes se vota sobre las propuestas de la comunidad. Para ganar una propuesta se requieren más votos a favor que en contra y la cantidad neta de votos a favor tiene que ser mayor al 10% de todos los MNs activos. Es decir, si hay 5.000 MNs se requieren 500 votos más a favor que los votos en contra para ganar. Las propuestas de la comunidad se enfocan en nuevos desarrollos o proyectos de adaptación de DASH en el mercado para llegar a más establecimientos y usuarios.

Monero (XMR)

En los últimos 10 a 15 años ha habido un movimiento creciente de personas que valoran la privacidad, no porque sean raras y quieran esconderse en los bosques; son ciudadanos comunes que no están contentos con la cantidad de datos que entregan.

RICCARDO «FLUFFYPONY» SPAGNI

El sitio web oficial de este proyecto define a Monero como un sistema monetario seguro, privado e imposible de rastrear. Monero utiliza un tipo especial de criptografía para garantizar que todas sus transacciones no puedan ser vinculadas entre sí, ni tampoco rastreadas. En un mundo donde ya casi no quedan reductos de privacidad financiera, el uso de criptomonedas que aseguran el anonimato de las transacciones puede volverse deseable.

Los orígenes

Monero surgió en abril de 2014, de la bifurcación dura (Hardfork) de Bytecoin La nueva cadena de bloques que surgió a partir de esta bifurcación tomó el

nombre de Bitmonero, que luego fue reemplazado por Monero, término que significa moneda en el idioma "*esperanto*". El proyecto es de código abierto y financiado por la comunidad. Cinco de sus siete desarrolladores han decidido permanecer en el anonimato.

Propiedades que hacen único a Monero

Tu dinero es tuyo, sólo tuyo: el usuario tiene el control y la responsabilidad absoluta sobre las transacciones que realiza. Nadie puede ver el historial de las transacciones que los usuarios realizan. El usuario puede hacer que sus transacciones sean visibles a voluntad a través de la compartición de su clave de vista

privada. Esto hace que las transacciones sean auditables. El anonimato se logra a través de las Signaturas de Anillo (ring signatures) que mezclan y combinan las monedas de cada transacción de forma que después ya no se puede saber de dónde vinieron.

Escalabilidad dinámica: Monero no tiene un límite de tamaño de bloque predefinido; esto podría significar que mineros malintencionados congestionen el sistema introduciendo bloques demasiado grandes. Para evitar este problema, se implementó una penalización al "block reward", que se calcula tomando el tamaño medio de los últimos 100 bloques (M100) y

comparándolo con el tamaño del nuevo bloque (NBS). Un total de 18 millones de moneroj (plural de monero) serán minados hasta el año 2022. Después serán emitidos 0.6 monero nuevos por bloque (aproximadamente 2 minutos), para siempre.

Resistente a la minería ASIC: Monero no es resistente a la minería ASIC, sin embargo el costo de fabricación de hardware ASIC para minar Monero es muy elevado, ya que requiere chips con 2 MB de memoria rápida, los cuales son de costosa fabricación. El algoritmo Cryptonight, que es el que usa Monero, fue creado para construir un sistema monetario más

justo y descentralizado. Las criptomonedas que incorporan Cryptonight no se pueden extraer usando minadores ASIC. Se espera que esto evite la creación de grupos fuertes de minería para que la moneda se distribuya más uniformemente.

Llaves o claves múltiples: Bitcoin, Ethereum, Litecoin y otras cadenas de bloques utilizan un sistema de firmas digitales de criptografía asimétrica que consta de una clave privada y una clave pública. Monero utiliza claves múltiples: una clave de vista privada, una clave de vista pública, una clave de gasto pública y una clave de gasto privada. Una

dirección pública de Monero consta de 95 caracteres formados por una clave de vista pública y una clave de gasto pública. Aquí un ejemplo de una clave pública de Monero:

43TvKzzX3UpfNeVu5Reu7KfCsg72UnQpTTjy

Monero versus Bitcoin

Una de las principales características de Bitcoin es su cadena de bloques abierta, que puede ser verificada públicamente en tiempo real. Bitcoin es relativamente simple de almacenar y usar. En cambio Monero está construido para garantizar total y absoluta privacidad. Es complicado de entender, almacenar y usar, al menos para los principiantes.

No hay duda de que a medida

que el futuro se vuelva más abierto y descentralizado, las criptomonedas que garantizan el anonimato como Monero, serán cada vez más atractivas en virtud de la privacidad que ofrecen. Es particularmente significativo que monero sea una de las pocas criptomonedas que no está basada en Bitcoin. Si eres una persona que se preocupa considerablemente por su privacidad y seguridad, monero es la criptomoneda adecuada para ti.

Ripple (XRP) / Stellar (XLM)

Noventa por ciento de estos proyectos son una mierda. Espero que eso cambie.

JED MCCALEB
(sobre la gran cantidad de criptomonedas diferentes)

Las monedas Ripple y Stellar se están enfocando en las transacciones y

servicios bancarios y por eso las nombramos aquí juntas. Además, el fundador de Stellar, Jed McCaleb, es cofundador en Ripple, así que hay varias paralelas entre las dos monedas.

Ripple es una de las monedas más criticadas dentro de la comunidad cripto porque fue creada para servicios bancarios. Algo que va en contra de la idea inicial de Satoshi Nakamoto, quien nos quería liberar del sistema bancario. Ripple no usa una blockchain descentralizada para sus transacciones, sino más una base de datos que permite grandes transacciones de forma rápida y segura por todo el mundo a bajo costo. Es decir, elimina la gran debilidad de

las transacciones lentas de los bancos, que en el caso de transferencias internacionales puede demorar días.

Uno de los puntos más criticados de Ripple es que la compañía se mantuvo con el 100% de las monedas inicialmente emitidas; es decir, no se trata de una propuesta descentralizada. Actualmente la mitad de las monedas de Ripple siguen en manos de la misma empresa.

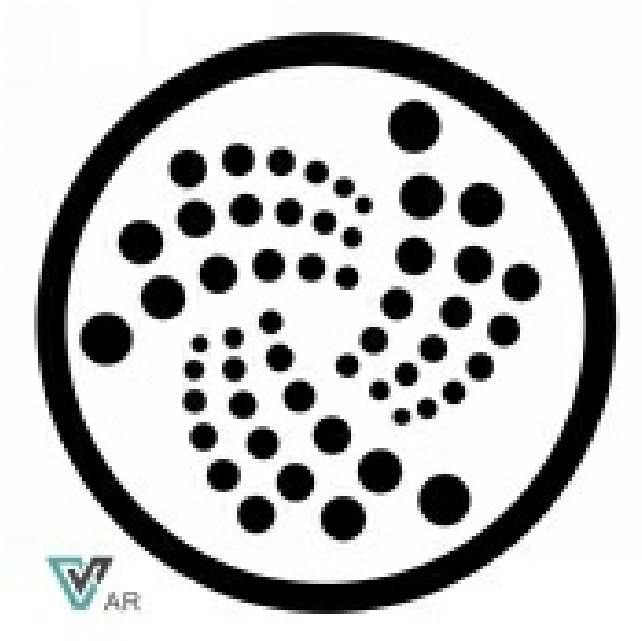
Stellar es un hardfork de Ripple y se emitieron 100 mil millones de

lumens en el año 2014; la misma cantidad que Ripple. La cantidad de lumens aumenta 1% anual y se distribuye según las votaciones de sus usuarios. Stellar quiere conectar a las personas a servicios financieros de bajo costo entre países desarrollados y subdesarrollados. Se usa la red de Stellar para transacciones de intercambio, entre el USD y el bitcoin o para pagos de remesas, por ejemplo. A diferencia de Ripple, Stellar tiene un enfoque menos corporativo y maneja un código abierto de su tecnología.

IOTA (MIOTA)

La ventaja de IOTA es que el proceso de validación requiere menos recursos que en el caso de Ethereum o Bitcoin.

DOMINIK SCHIENER, Co-fundador IOTA



IOTA es una base de datos distribuida que permite transacciones de valor o de datos entre personas o máquinas. Con una nueva tecnología llamada “Tangle”,

se busca eliminar las desventajas de la tecnología blockchain, principalmente el costo de transacciones (aunque es bajo) y el tiempo de confirmación. Para realizar una transacción en Tangle se tienen que confirmar dos transacciones anteriores. Este proceso requiere un mínimo de energía para que la red funcione. Con IOTA las transacciones no generan un costo, sino funcionan completamente gratis. Esta tecnología se construye sobre un gráfico acíclico dirigido (DAG), un sistema ordenado topológicamente en el que diferentes tipos de transacciones se ejecutan en diferentes cadenas de la red en forma simultánea.

Más que seres humanos IOTA quiere conectar máquinas para que se comuniquen entre ellas y puedan realizar pagos. Por ejemplo, la refrigeradora se comunica con el supermercado y ordena más leche porque hace falta y a la vez realiza el pago por el producto. En Tangle mientras más transacciones hay más rápido se realizan las confirmaciones.

IOTA está involucrado en varios desarrollos con gigantes industriales y tecnológicos como Bosch, Fujitsu y Volkswagen.

Stablecoins

Satoshi tenía una filosofía revolucionaria de lo que podría ser el dinero y las monedas estables están llevando la antorcha hacia adelante para esa visión. Bitcoin se ha convertido en un juego especulativo y es demasiado volátil para usarlo en el comercio.

RYAN KIM
Fundador y director ejecutivo del proyecto Xank

Las criptomonedas tienen varias ventajas sobre el dinero fiat, como ya hemos analizado; sin embargo, hay un factor que hace que sobre todo los

comercios que quieren usar criptomonedas no opten por este nuevo medio: la volatilidad de los precios. Para un negocio que cobra en criptomonedas es un factor de mucha incertidumbre si no se sabe cuánto valen los ingresos de hoy el día de mañana. Cambios en precios del 10, 20 o 30% en veinticuatro horas, han sido normales en el mercado de criptomonedas. Para mantener las ventajas de una criptomoneda, pero quitar el factor de la volatilidad se han creado los stablecoins (monedas estables). Estas monedas tienen un precio estable y se respaldan con activos, como dinero fiat, oro u otras criptomonedas.

Tokens respaldados en dinero fiat

En este caso hay una paridad 1 a 1 entre el token y una moneda fiat como el USD, EUR u otra. Es decir, la promesa es que siempre vas a poder cambiar el token con un cambio fijo a dinero fiat. Para que este sistema funcione se requiere de un gran fondo en dinero fiat en cuentas bancarias. Además es importante que haya auditorías constantes que certifiquen que existen realmente los fondos de respaldo. Es decir, los stablecoins necesitan crear confianza a través de terceros. Eso va en contra de las ideas iniciales de las criptomonedas, donde la criptografía es la que da confianza y no algo físico o de algún

Estado. Algunos ejemplos:

Tether (USDT): Fue creado en 2014 con el nombre Realcoin. Respaldado en pares de USDT/USD y USDT/EUR. Es uno de los primeros stablecoins y está vinculado a las operaciones del exchange Bitfinex.

TrueUSD (TUSD): Creado en 2018, ofrece el respaldo por el dólar estadounidense 1 a 1, y quiere ser más transparente que el Tether. Es parte de la plataforma de TrustToken que permite la tokenización de bienes y servicios. Funciona basado en un token ERC20 de Ethereum.

USD Coin (USDC): Creado en 2018 por la empresa Circle, filial

FinTech de Goldman Sachs. Es igual a un token ERC20 de Ethereum y es el stablecoin del exchange Poloniex.

Tokens respaldados en oro

Estos tokens representan cierta cantidad de oro físico. Para dar respaldo se guarda la cantidad en oro equivalente a la cantidad de tokens emitidos en las bóvedas de la compañía que opera este proyecto. Un ejemplo:

Digix Gold (DGX): Cada token representa 1 gramo de oro que se puede cambiar físicamente en la sede de DIGIX en Singapur. La compañía fue creada en 2014. DGX es un token ERC20 y se emite un token nuevo por cada gramo que se agregue a la custodia

de la empresa.

Tokens respaldados en otras criptomonedas

En este caso se mantiene como respaldo para un token cierta cantidad de otra criptomoneda. Eso implica que igual hay un riesgo por la volatilidad del mercado cripto, sin embargo se evita la dependencia del mercado fiat. Para dar mayor seguridad la paridad podría ser 2:1, el doble de respaldo en valor de criptomonedas para asegurar la estabilidad. Mientras el bitcoin sigue ganando confianza puede tener sentido respaldar un nuevo token en este criptoactivo, porque ya no es tan volátil y goza de mayor confianza.

DAI: Un stablecoin 1:1 con el USD respaldado en Ethereum a través de un Smart Contract. Es decir, para recibir DAIs se necesita depositar primero ETHs y a cambio se reciben DAIs prestados hasta que se devuelven y se obtienen de nuevo los ETH. La empresa lanzó su stablecoin a finales de 2017.

El uso de los stablecoins está en crecimiento. Mayormente se usa dentro de los exchanges para tener un par entre cripto y fiat y para guardar valor en el momento que se estima una baja en el mercado. Se espera un gran futuro para estas monedas porque ofrecen una estabilidad que la mayoría de las

personas en el mercado buscan y brindan las ventajas de una criptomoneda.

Facebook y su Criptmoneda Libra: 9 Datos importantes que debes saber

> *Todo el mundo entiende que el sistema de pago global es ineficiente en las transacciones transfronterizas, y no hay un mercado más grande que el dinero, es el mercado más grande del planeta.*
>
> NICHOLAS COLAS

Quince años después de haber fundado Facebook, la red social más famosa del mundo, Mark Zuckerberg está listo para una nueva revolución. No sabemos si Libra, la criptomoneda de Facebook tendrá el mismo impacto que la red social, pero sí que ésta es una de las

apuestas más notables de una empresa Fortune 100 en el naciente mercado de los criptoactivos.

Libra estará disponible en 2020 con el respaldo de bonos del gobierno y una serie de monedas fiduciárias –USD, GBP, EUR y JPY–. Esta criptodivisa es sólo la punta del iceberg de un ambicioso proyecto que pretende crear una infraestructura financiera global bajo la tutela de Facebook. Según David Marcus, ejecutivo de esta red social, el objetivo es "transformar la vida de billones de personas al proporcionarles acceso a un ecosistema financiero más abierto e inclusivo".

¿La competencia de bitcoin?

Siguiendo el modelo de Ethereum, Tezos e innumerables iniciativas del criptomundo, Libra Association, organización sin fines de lucro con sede en Ginebra, supervisa el desarrollo de la red y su criptomoneda. Los miembros fundadores de Libra, que pasaron estrictos filtros de selección y tendrán su propio nodo, son empresas reconocidas a nivel mundial como PayPal, Visa, Mastercard, Uber, Coinbase, Xapo, eBay, Spotify, Mercado Libre, Andreessen Horowitz y otras.

El libro blanco de Libra indica que se espera tener cien miembros cuando se lance la red. Por lo pronto, ni un solo banco es parte del consorcio,

pues sus ingresos podrían estar comprometidos si Libra tiene éxito. Además, las criptomonedas carecen de normativa en la mayoría de países, a diferencia del sector bancario que es uno de los más regulados e intervenidos en el mundo.

Libra funcionará en una cadena de bloques cerrada, por lo que únicamente sus miembros pueden ejecutar los nodos que participan en el consenso y en la validación de las transacciones. Lo mismo sucede con las blockchains privadas de R3 y Ripple, por ejemplo.

Facebook considera que los sistemas abiertos como Bitcoin todavía

no están listos para la adopción masiva por las limitaciones tecnológicas que les impide ser competitivos. En contraste, la red Libra tendrá un rendimiento de mil transacciones por segundo y una finalidad de diez segundos al momento de su operación inicial.

Al ser una cadena de bloques cerrada, pese a tener cierta descentralización por sus cien nodos de validación, existe la posibilidad de que el consorcio censure las transacciones a voluntad propia o de terceros vía judicial.

Con respecto a este riesgo, Andreas Antonopoulos, reconocido gurú del criptomundo, dijo que Libra será una

amenaza para el sistema financiero tradicional, no para bitcoin. Esta nueva criptomoneda carece de las principales características de una red distribuida –que Bitcoin sí posee–: apertura, descentralización, neutralidad, transnacionalidad y resistencia a la censura.

Otro aspecto de Libra que faculta la censura es que los desarrolladores la red pueden crear billeteras custodiales, y con esto los proveedores y dueños de la aplicación controlarían las claves privadas de los usuarios.

El modelo custodial deja abierta la posibilidad de que los usuarios

cuenten con servicio al cliente y seguros de protección contra robos y fraude. No obstante, al mismo tiempo, los usuarios no son los reales poseedores de Libra.

Lo que debes saber sobre la nueva criptodivisa de Facebook

1) Inclusión financiera

Libra Blockchain impulsará la criptomoneda Libra. Esta plataforma, diseñada para ser segura, escalable y confiable, busca resolver dos problemas que el sistema financiero tradicional no ha resuelto: las transferencias internacionales rápidas y a bajo costo y la inclusión financiera.

2) Inspirada en Ethereum

Libra Blockchain utiliza el modelo de cuentas, gas y contratos inteligentes de Ethereum. También será de código abierto bajo una licencia de Apache 2.0, lo que permitirá a

los desarrolladores leer, crear, comentar y participar en un programa de recompensas de identificación de bugs.

3) Transición a PoS

Libra planea migrar a una red basada en el algoritmo de consenso Prueba de Participación (PoS) durante los próximos cinco años. Aún no está claro qué tan sencilla será la transición, porque este proceso acarrea varios obstáculos técnicos y económicos, especialmente relacionados con la

gobernanza de la red, en lo que tiene que ver con escalabilidad versus rendimiento. Sabemos que la velocidad de procesamiento de datos tiene que ser sacrificada en beneficio de la autonomía, fenómeno que se ha visto en las cadenas de bloques abiertas como Bitcoin y Ethereum.

4) Transacciones pseudoanónimas

Al igual que las criptomonedas abiertas como bitcoin o ether, las transacciones no custodiales de libras serán pseudoanónimas; es decir, únicamente el monto de la transacción, sello de tiempo y la clave pública serán visibles para los miembros de la red, mas no la identidad del emisor y receptor de la

transacción.

Para distinguir adecuadamente entre privacidad y anonimato, podemos decir que deambular desnudo en tu departamento sin que nadie te vea es privacidad. Caminar desnudo por la calle sin que nadie sepa tu nombre es anonimato.

Libra Association ha manifestado que no almacenará los datos personales de las personas que usen su criptodivisa. Sin embargo, las billeteras custodiales que permitan efectuar transacciones fuera de la cadena podrían requerir que los usuarios cumplan con políticas Conozca a su Cliente (KYC).

5) La emisión

Las reservas que respaldan la emisión de libras consistirán en una colección de activos de baja volatilidad como depósitos bancarios y valores gubernamentales en divisas fuertes. Libra no está vinculada a ninguna moneda fiat en particular, por lo que no se consideraría como una moneda estable. Sin embargo, debido a su respaldo, podría esperarse que su precio goce de cierta estabilidad.

6) STO

Libra emitirá un token de seguridad llamado Libra Investment Token, como una forma de financiar programas de incentivos y cubrir costos operativos. Este token estará disponible

exclusivamente para inversionistas acreditados. Los tenedores obtendrían retornos a través de los intereses recibidos.

7) El costo de un nodo

Las empresas que tengan interés en operar un nodo de validación deberán efectuar una inversión mínima de diez millones de dólares en Libra Investment Tokens emitidos por Libra Association. Se ha previsto que las ONG, las organizaciones multilaterales, los socios de impacto social y las universidades no necesitan hacer una inversión para unirse a la asociación, pero sí tienen que correr con los costos operativos del nodo, que se estiman en 280 mil dólares

anuales.

8) Regulaciones

Los desarrolladores que utilicen el software de código abierto de Libra deben cumplir las leyes y regulaciones relacionadas con criptoactivos correspondientes a la jurisdicción donde residan. Libra no será regulada per se.

9) Lanzamiento

Libra y su cadena de bloques subyacente se lanzarán en 2020 en una fecha todavía no establecida. Los desarrolladores podrán leer, construir, proporcionar comentarios y participar en un programa de recompensas de errores.

¿Qué esperar en el futuro?

A pesar de que Libra será parte de los titulares durante un buen tiempo, el ambicioso proyecto de Facebook aún dista de ser ejecutado. De hecho, los miembros del consorcio ni siquiera están al tanto de cómo funciona el proyecto, como lo señala The Wall Street Journal.

En cuanto a las regulaciones, aún no se sabe a ciencia cierta cómo reaccionarán los gobiernos frente a la amenaza que una divisa no soberana representaría para su sistema de dinero fiduciario. Al respecto, el ministro de finanzas francés, Bruno Le Maire, hizo un llamado a las autoridades de los bancos centrales del Grupo de los Siete

–guardianes del sistema monetario mundial– para que preparen un informe sobre el proyecto de Facebook para su reunión de julio.

Tampoco se tienen claras las implicaciones fiscales. Libra Association ha manifestado que espera "trabajar con los responsables de la formulación de políticas mientras aclaran la aplicación de las leyes fiscales existentes a las criptomonedas o, en algunos casos, para actualizar esas leyes".

Para aquellos que estamos familiarizados con las criptomonedas, Libra podría ser la piedra angular de un profundo cambio del paradigma

financiero mundial iniciado y liderado por Bitcoin.

ICO

En una “Inicial Coin Offering” (Oferta Inicial de Monedas), una compañía ofrece una cantidad de tokens, fichas o vales a cambio de otras criptomonedas para recaudar un fondo para su proyecto. Este proceso de financiación colectiva es una forma del crowdfunding. En los últimos meses la ICO se ha convertido en una herramienta muy frecuentada por emprendimientos de la criptoeconomía para recibir fondos. En la economía tradicional se usa la herramienta de la IPO (Oferta Pública de Venta), en cuál una empresa privada ofrece sus acciones

a la venta en la bolsa de valores para que el público en general pueda adquirirlas. Para entrar a la bolsa de valores muchas veces las empresas ya están varios años en el mercado y tienen que cumplir regulaciones muy estrictas antes de poder vender participaciones a través de sus acciones. En cambio las ICOs son descentralizadas, no dependen de una autoridad que le permita funcionar. Sin embargo, ya existen los primeros países que han creado su regulación para la emisión de ICOs. Además, a diferencia de las compañías tradicionales, los ICOs se realizan sobre todo con empresas Start-Ups que tienen una idea o un proyecto que todavía no produce o está funcionando y por eso el

riesgo de inversión en una ICO es mucho mayor que en una empresa que emite acciones para entrar a la bolsa de valores.

Para una empresa la venta de tokens es muy interesante, porque puede recibir de forma fácil financiamiento de inversores pequeños y grandes de todo el mundo, y no tienen que vender una parte de su compañía, porque sólo emiten el token. El inversor a cambio no adquiere votos en la compañía, sino está motivado a adquirir un token a un precio bajo y especula que su valor subirá en el futuro.

Los términos “coin” y “token” a veces se usa de la misma forma y hay

confusiones. Se podría decir que un coin es una unidad de valor que tiene su propia blockchain, mientras que un token usa la blockchain de un sistema ya establecido, como los tokens de Ethereum. Los tokens en una blockchain representan un valor financiero o un activo digital.

Se puede distinguir entre varios tipos de tokens:

Token de Utilidad (Utility token)

Como el nombre lo indica, estos tokens tienen algún tipo de utilidad en el ecosistema para el que fueron creados. Por ejemplo, un token de una casa de cambio que permite pagar las comisiones que generan las

transacciones con este token en particular; o un token para videojuegos que permite comprar armas dentro del juego.

Token de Seguridad (Security token)

Los tokens de seguridad representan algo físico o digital que da un respaldo sobre su valor o un beneficio al dueño. Por ejemplo, un token que representa las acciones de una empresa y que genera un dividendo a los dueños; o un token que representa tierra u oro y que da un respaldo en el mundo físico.

Los ICOs se crean a veces con su propia blockchain, sin embargo la mayor cantidad usa una plataforma como Ethereum, NEM, Lisk, Waves o Stratis,

que permiten la creación de tokens en su ecosistema de una forma fácil. El sistema más usado son los tokens ERC20 (Ethereum Request for Comments No. 20) de Ethereum. La creación de un token ERC20 se puede realizar en un par de horas y no es necesario crear una blockchain propia que tiene que dar valor e incentivos a los mineros para que la apoyen. El ERC20 es un Smart Contract en la blockchain de Ethereum que define seis funciones:

1. Número de tokens
2. Cuantos tokens se registran en una dirección
3. De dónde se puede transferir

tokens

4. A dónde se puede transferir tokens
5. Qué está permitido y que no
6. Si existen opciones adicionales o no

Una desventaja en Ethereum, aunque tiene el mayor mercado, es el lenguaje de programación “Solidity”, que sólo se usa en el ecosistema de Ethereum. Otras plataformas como NEM usan lenguajes más conocidos, como Java Script, que facilitan el trabajo de los programadores.

Tanto para los creadores de ICOs como para los inversionistas, existe una serie de ventajas y también

problemas de los que hay que estar conscientes:

Ventajas de ICOs

Democratización de acceso: La participación se puede realizar desde cualquier parte del mundo realizando el aporte con criptomonedas.

Facilidad: Levantamiento de capital de una forma más fácil que en la economía tradicional, porque no existen muchas regulaciones.

Dar uso a las monedas: Como todavía no se puede usar las criptomonedas en todo el mundo, una forma de sacarle provecho es la inversión en nuevos proyectos.

Oportunidad de ganar dinero: Los

tokens de una ICO exitosa pueden subir de valor de forma exponencial y generar grandes ganancias.

Apoyo a la innovación: La mayoría de los ICOs se basan en ideas disruptivas e innovadoras y pueden recibir los fondos necesarios para su desarrollo a través de esta fuente de financiamiento.

Problemas

Regulaciones: En el caso de no tener regulaciones claras, cualquiera puede crear ICOs y con sólo una buena campaña de marketing atraer a inversionistas aunque no haya pruebas de que es un proyecto que va a funcionar. Una gran cantidad de ICOs terminan siendo SCAMs o Fraudes

porque después de recaudar los fondos los creadores desaparecen con las monedas o hay problemas en el desarrollo y nunca tendrán un proyecto funcional. Por otro lado, ya algunos gobiernos empezaron a regular los ICOs; esto tiene como ventaja la protección de los inversores, sin embargo una sobreregulación puede matar la innovación, teniendo en cuenta que quienes elaboran las regulaciones generalmente carecen de conocimientos suficientes acerca de las tecnologías emergentes.

Proyectos no operativos: La mayoría de las ICOs no han probado que su modelo de negocios puede funcionar en la

economía real. Son sólo ideas sobre un papel y tienen que pasar por muchas pruebas antes de saber si van a ser rentables en el futuro.

Falta de transparencia sobre el uso de fondos: Después de la fase de ICO los inversores no saben si el dinero será usado según lo antes acordado.

Riesgo de hackeos: Durante el proceso de la recaudación pueden surgir hackeos que roban los fondos, como fue el caso en la ICO de The DAO.

Las ICOs han sido una gran fuente de financiamiento para algunos de los proyectos más importantes de la criptoeconomía. El mismo Ethereum, que se lanzó como ICO en julio de 2014,

recaudó aproximadamente 30.000 bitcoins con un valor de 14 millones de dólares en ese entonces. Según las estadisticas de coinschedule.com estos son los valores recaudados por ICOs en los últimos años:

2013: 616.800 USD – 2 ICOs (Mastercoin y NXT)
2014: 29.924 Mio USD – 6 ICOs (incl Ethereum y MaidSafeCoin)
2015: 8.853 Mio USD – 7 ICOs (incl. Augur)
2016: 93.922 Mio USD – 51 ICOs (incl. Waves, Iconomi y Golem)
2017: 6.576 Mill Mio USD – 453 ICOs (incl. Filecoin, Tezos y Bancor)
2018: 21.483 Mill Mio USD – 1.072 ICOs (incl. EOS, Telegram, Bankera)

Fuente: www.coinschedule.com/stats.html
Más información sobre ICOs en las siguientes páginas:
www.smithandcrown.com/sale -
www.tokenmarket.net/ico-calendar
www.icocountdown.com/

Proceso de lanzamiento

El tiempo entre la idea inicial y el lanzamiento de una ICO puede durar de 6 a 12 meses. En este transcurso hay varias fases y muchos nuevos términos que tenemos que conocer si queremos entender en qué momento de la ICO nos encontramos y si la oferta pública está en buen camino. A continuación enumeramos los pasos más importantes de este proceso y explicamos los términos específicos.

Pasos importantes en el lanzamiento de una ICO

Primero: Creación del whitepaper que describe al detalle la idea del proyecto, qué problema resuelve el token, qué tipo de token se va a crear –de Utilidad o de Seguridad–, el equipo y sus habilidades, los asesores, el roadmap, la distribución de tokens, etc. El whitepaper es el resumen del trabajo previo a la creación y lanzamiento de la ICO y funciona como la tarjeta de presentación que los inversionistas leen antes de tomar la decisión de invertir.

Segundo: Creación de un Smart Contract para la administración y ejecución de la ICO. Eso se puede hacer a través de una

plataforma blockchain como Ethereum, Waves o Stratis.

Tercero: Lanzar los tokens parcialmente o en su totalidad a la venta. Se crea un plan con las diferentes rondas de inversión y se definen los precios de los tokens para cada una de estas fases en las que los inversionistas cambian sus criptomonedas por tokens. El precio del token suele subir mientras más se acerca la fecha final de la venta. Algunos términos que se usa en el proceso de venta:

- Venta privada: En esta venta se ofrecen los tokens a un precio muy especial a cierto grupo de personas que adquieren una

cantidad mínima definida de unidades para obtener algún beneficio, como un descuento o un bono en tokens adicionales. En este punto el inversor corre el mayor riesgo y por otro lado tiene la oportunidad más grande de vender los tokens después a un precio mayor.

- Venta pública: Todo el mundo puede comprar tokens a un precio que se estima que será menor que el precio con el que entrará al mercado. Para la adquisición el inversor abre una cuenta y verifica su identidad en la página de la ICO antes de

realizar su inversión.

- Pre-ICO: A veces se usa una Pre-ICO para recaudar fondos con los que después se puede financiar la campaña de marketing de la ICO, o para probar el mercado y ver si hay una buena respuesta a la oferta de valor. El valor que se pide por los tokens en esta fase normalmente es bajo o incluye un bono. La Pre-ICO puede realizarse a través de una venta privada dirigida a inversores grandes.
- Hard Cap: Es el monto máximo que va a recaudar una ICO y

después de alcanzarlo no va a recibir más dinero. Si una ICO alcanza el Hard Cap antes de lo planificado ya no recibirá más fondos. Si al proyecto llegan más fondos que los asignados en el Hard Cap, estos deben ser regresados a los inversionistas.

- Soft Cap: Es el monto mínimo a recaudar para que el proyecto se considere exitoso. Si no se alcanza el monto del Soft Cap los montos regresan a sus inversores y normalmente el proyecto se cierra.
- Uncapped ICOs: Hay ICOs que no tienen un límite en su

inversión; es decir, tratan de recaudar el máximo capital que puedan. Mientras más dinero entra durante el proceso de crowdfunding más puede el equipo invertir después en marketing, promoción y desarrollo.

Cuarto: Después de la fase de ICO el Smart Contract distribuye los tokens adquiridos a los inversionistas. Cuando la ICO empieza a cotizar en un exchange se va a ver por primera vez su precio real de mercado. Este precio puede variar mucho los primeros días y es muy especulativo. Sobre todo personas que adquirieron sus tokens a precios bajos y

con bonos tratan de venderlos con ganancia en los primeros días.

Quinto: La empresa usa los fondos recaudados para desarrollar su proyecto con el fin de que sea rentable.

Hay más etapas durante el desarrollo de una ICO que no son muy visibles para el público, sin embargo éstas son las principales.

Las cinco claves de éxito de una ICO

Que una ICO tenga o no éxito, depende de muchísimos factores internos y externos. A continuación una pequeña lista donde se puede ver qué han tenido en común los casos exitosos y en qué debemos enfocarnos cuando analizamos una ICO:

1. *Idea*: La ICO debe tener una buena idea que soluciona un problema real que otros proyectos no pueden solucionar.
2. *Whitepaper*: Tener un whitepaper que convence e informa bien a los posibles inversores es importante. Sólo si se logra explicar con claridad el fin del proyecto y plasmar cómo se va a realizar, los inversionistas van a tomar la decisión de invertir.
3. *Equipo*: El equipo debe conformarse por desarrolladores, ingenieros, legales, comerciales y

marketing. La transparencia y experiencia del equipo es importante, por eso debe ser visible en los medios de comunicación del proyecto y a través de redes sociales profesionales como LinkedIn.

4. *Estructura del token*: ¿Cuánto vale el token inicialmente? ¿Qué porcentaje de los tokens se va a vender? ¿Cuál es la función del token? ¿Desde qué país se realizará la venta? ¿Será un token de Utilidad o un token de Seguridad con respaldo? Las respuestas a estas preguntas deben ajustarse al volumen del

mercado que existe para el proyecto; es decir, la venta no debe ser sobredimensionada en relación al objetivo que quiere lograr.

5. *Comunicación*: El marketing y la comunicación son la llave al éxito para una ICO. Es importante revisar cuáles redes y foros se manejan y qué tan bien están administradas. Entre las redes más importantes están Bitcointalk, Slack, Twitter y los grupos de Telegram.

Que una ICO cumpla con las cinco claves mencionadas no representa una garantía de éxito y tampoco una

recomendación para invertir. En la tercera parte de este libro (Finanzas) se incluye información sobre ICOs como opción de inversión.

Cómo analizar una criptomoneda

El análisis de una ICO y de una criptomoneda coincide en algunos puntos. Ambos son proyectos que quieren posicionarse con éxito en la criptoeconomía. Por otro lado, hay diferentes fuentes de información y también factores de éxito a considerar cuando queremos saber si una criptomoneda tendrá o no éxito.

Fuentes de información

Una de las mejores fuentes para conocer a profundidad una criptomoneda es

analizar su whitepaper que regularmente se encuentra publicado en su página web. Este documento brinda información sobre la idea principal, los objetivos y la filosofía de la moneda. También presenta el plan de trabajo (Roadmap), el equipo que está trabajando en el proyecto, la distribución de la moneda y una explicación de cómo funciona la tecnología que se va a usar. Cada moneda seria cuenta con un whitepaper bien redactado que es su tarjeta de presentación para los posibles inversionistas.

Otras fuentes de información son las publicaciones online en páginas de

noticias o blogs. Muchas páginas se encuentran en inglés, sin embargo también hay buena información en español. Los sitios más importantes que tienen como enfoque temas relacionados con la criptoeconomía son:

En español:

- www.criptonoticias.com
- www.diariobitcoin.com
- es.cointelegraph.com
- www.criptotendencia.com

En inglés:

- www.reddit.com
- www.cointelegraph.com
- www.coindesk.com
- www.bitcoin.com
- http://www.bitcointalk.org

Los grupos de Telegram también

se han convertido en fuentes de información importantes y son usadas por los equipos de marketing de las monedas como una de las mejores opciones para estar en comunicación con su comunidad. Para conocer más acerca de un proyecto en específico recomendamos estar conectado a través de Telegram. También hay varios canales de noticias en Telegram que se dedican a enviar las novedades de la industria y son gratuitos. De la misma manera, algunas redes sociales como Twitter brindan información actual sobre las tendencias en el mercado; los canales y personalidades más importantes a seguir son: John McAffee, Roger Ver o Zhao Changpeng. Además

diversas monedas manejan este canal para difundir información.

Si ya sabes dónde encontrar la mejor información ahora tienes que saber qué marca la diferencia entre un proyecto con potencial de éxito y uno que está destinado al fracaso.

Los factores de éxito de una criptomoneda

Aparte de los factores de éxito como la idea principal, el whitepaper, el equipo y la comunicación que tienen en común los ICOs y criptomonedas, hay otros factores que hay que analizar si queremos saber si una criptomoneda aumentará su valor a mediano y largo plazo. Ya después de que se va la

euforia de un lanzamiento de una nueva moneda o ICO viene la realidad y se va a mostrar si el proyecto realmente tiene futuro.

Los factores de éxito más importantes de una criptomoneda a mediano y largo plazo son los siguientes:

Primero: Tamaño del mercado en el que se puede usar la moneda

Para poder ver el potencial de una moneda hay que analizar el tamaño del mercado que puede abarcar. Por ejemplo, si existe una moneda para el pago de remesas y este mercado mueve 1.000 millones de dólares y se estima que la moneda puede llegar a captar el

10% del mismo, entonces la capitalización del mercado puede ser de 100 millones de dólares. Si existen 100 millones de monedas entonces el valor puede llegar a 1 USD cada uno. Eso sería un cálculo simplificado para ver el potencial que tiene el precio de una moneda.

Segundo: Usabilidad de la moneda

Uno de los mayores factores de éxito de una moneda es si realmente la gente la está usando o la va a usar en un futuro. La cantidad de transacciones que se realiza cada cierto tiempo es el indicador que nos puede ayudar en este análisis. Para eso es importante separar el volumen de transacciones por los

exchanges y el volumen de transacciones entre billeteras, el uso real. También se puede tomar en cuenta la cantidad de direcciones usadas. Mientras más existen, mayor uso se está generando.

Otros factores técnicos que pueden influenciar en la usabilidad de una moneda son el tamaño y tiempo de bloque o los costos de transacción. Lo que buscan los usuarios para monedas de pagos, por ejemplo, es el mínimo costo y la máxima rapidez para las transacciones. Páginas que ayudan con este análisis son: https://chainz.cryptoid.info, o puedes usar los exploradores que muestra coinmarketcap.com en la información de

cada moneda.

Tercero: La comunidad

En principio, las criptomonedas son sistemas descentralizados que se basan en la participación de una comunidad que desarrolla, usa y hace conocer el proyecto o la moneda. Hoy en día la mayoría de monedas o tokens son proyectos centralizados para los cuales una empresa hace el marketing. De igual forma es importante para el futuro de una moneda que haya una comunidad detrás de ella. Los indicadores de si una comunidad está activa se obtienen respondiendo estas preguntas: ¿Cuántos seguidores tiene la moneda en redes sociales y chats como Telegram? ¿Son

seguidores activos o fueron comprados? ¿Cuántos artículos se están escribiendo sobre la moneda? ¿Quiénes redactan?, ¿siempre las mismas o diferentes personas? ¿Qué tanta participación hay en los chats en bitcointalk.org o reddit.com? ¿Hay actividades locales de miembros de la comunidad que educan a los ciudadanos sobre el uso de su moneda? Por ejemplo, podemos ver que Bitcoin tiene una comunidad inmensa que está formada por voluntarios; eso es un indicio de que esta moneda encontró su posición y justificación en el mercado con miles de usuarios y beneficiarios.

Cuarto: Estabilidad en su precio

Las monedas muy volátiles son

interesante para la especulación y el trading, sin embargo tendrán problemas para ser aceptadas en el mercado. El usuario, en vez del trader, busca estabilidad en el precio para poder usar una moneda con confianza. Sólo las monedas de baja volatilidad van a encontrar su posición en el mercado masivo a mediano plazo.

Quinto: La confianza

El factor confianza es esencial si se quiere lograr que el dinero fiat se reemplace por las criptomonedas. Sólo si pueden generar la confianza suficiente en sus usuarios van a tener éxito. Para crear confianza, la seguridad informática en las transacciones es importante. La

tecnología blockchain hoy en día es uno de los sistemas más seguros para transacciones. También las regulaciones y la aceptación de los gobiernos aumentan la confianza de las personas. Por último, la estabilidad de precio y la aceptación en establecimientos o negocios hacen que las personas confíen cada vez más en ciertas criptomonedas.

Lamentablemente todavía encontramos en el mercado monedas que no se enfocan en cumplir con estos factores de éxito para realmente dar un aporte a la criptoeconomía. Estas monedas las denominamos “Scamcoins” o “Shitcoins”, y fueron creadas para estafar a los incautos o desde el inicio

no tienen el potencial de crear valor.

Cómo detectar scamcoins o shitcoins

El mercado de criptomonedas brinda grandes oportunidades, la gente vio que una moneda como el bitcoin inicialmente se podía comprar a centavos y pocos años después llegó a tener un valor de hasta 20.000 USD y comenzó a buscarse el próximo "bitcoin" que repitiera la historia. Todos quisiéramos saber cuál es el "próximo bitcoin", para invertir a tiempo y aprovechar su gran rentabilidad. Sin embargo, si revisamos el mercado de cientos y miles de monedas digitales tenemos que llegar a la conclusión de que sólo unas pocas realmente van a valer algo en el futuro y

que hay más monedas en el mercado que no tienen ningún valor real, porque no hay un proyecto, una idea o el equipo correcto trabajando para su éxito.

Obviamente la gran pregunta es cómo distinguir las buenas de las malas monedas. Los siguientes cuatro puntos de análisis te van a ayudar a ubicar una moneda en el grupo de los proyectos con futuro o en el de los shitcoins.

Primero: ¿Está la moneda listada en coinmarketcap.com?

Aunque también en el listado de coinmarketcap.com se cuentran shitcoins, es un primer buen indicio que la moneda esté por lo menos listada en exchanges que permitan su compra y

venta; mientras en más casas de cambio se pueda negociar, mejor. Debes cuidarte cuando una moneda se puede comprar en un sólo exchange o en la misma plataforma de la compañía que la está ofreciendo; en esos casos no se tienen muchas opciones para adquirir o vender, y si la única casa de cambio la quitara de su lista se pierde la opción de intercambiar las monedas y eso puede causar que su precio caiga a cero.

Segundo: Revisa las redes sociales de la moneda

Puedes encontrar los enlaces en coinmarketcap.com en la sección "Social". Los canales como Twitter, Reddit, Telegram o Facebook te

permiten ver si existe una comunidad activa que interactúa y cómo están los ánimos. Si las redes están abandonadas y no se recibe respuestas a preguntas que se están haciendo a la comunidad, puede ser que ya no haya un equipo de desarrolladores detrás de la moneda y puede dudarse de su progreso en el futuro.

Tercero: Revisa la tecnología que usan

Unos "shitcoins" no usan una blockchain u otra tecnología innovadora para su funcionamiento, ni se basan en una plataforma como la de Ethereum, sólo se registran en una base de datos o hasta en una tabla de excel para ser administradas. Estas monedas se

manejan de forma centralizada. No puedes ver el código fuente, no puedes participar en la minería o hacer staking. A veces el argumento de los creadores es que no hay acceso a estos datos por seguridad, y eso es falso.

Cuarto: El whitepaper

También puedes revisar si la moneda tiene un whitepaper con la información relevante y transparente que debe ser pública para los usuarios. Una moneda sin whitepaper es una mala señal.

Ya hemos explicado qué caracteriza una buena moneda o un buen token; puedes usar estos factores de éxito también para ver si una moneda que estás analizando cumple con ellos.

Algunos shitcoins usan un sistema piramidal o ponzi para promocionarse; en el capítulo de Finanzas veremos cómo detectar estos sistemas.

Criptomonedas en la práctica

Billeteras de criptomonedas

Lo primero que necesitas si quieres usar criptomonedas es una billetera o wallet. Una billetera es una aplicación que te ayuda a recibir y a enviar monedas digitales. Hay diversos tipos de billeteras con sus ventajas y desventajas. En esta parte vamos a conocer su funcionamiento y vamos a analizar las mejores opciones que se adaptan a tus necesidades.

Claves privadas y públicas

Para entender el funcionamiento de una billetera de criptomonedas debes tener claro el concepto de las claves públicas y privadas. Una billetera no guarda en sí las monedas, es el lugar donde se guardan las claves privadas y públicas que dan acceso a las monedas que están vinculadas a las mismas. La clave privada, como su nombre indica, es secreta y no se debe compartir porque da acceso a las monedas; esta clave puede liberar las monedas que están vinculadas a la clave pública correspondiente. De una clave privada se pueden generar varias claves públicas, sin embargo cada clave pública sólo tiene una clave privada. Es

fácil de verificar si la clave pública viene de cierta clave privada, sin embargo no se puede revelar cuál es la clave privada teniendo la clave pública en mano.

Se podría comparar la clave privada con tu NIP o la contraseña de tu cuenta bancaria. Si alguien tiene tu número de cuenta (clave pública) y además la contraseña (clave privada), tendría acceso a tus fondos; lo mismo sucede con las criptomonedas y sus claves.

Un ejemplo para una clave privada de Bitcoin es:

5HwPmcxhTVrxSYar7zMQCGijDUf2Za

En un sistema descentralizado

nadie revisa si tu número de cuenta ya fue entregado a alguien más, por eso se crean los números de cuentas de forma aleatoria a través de la criptografía. En el caso de Bitcoin se pueden crear 2 potenciados por 256 direcciones diferentes. Eso es un 1 con 80 ceros, una cifra increíblemente grande. La posibilidad de generar dos veces la misma clave es matemáticamente casi imposible.

La mayoría de las wallets hoy en día son billeteras HD (hierarchical deterministic). En estas billeteras la creación de las claves privadas se basan en un SEED de Seguridad formado por 12, 18 ó 24 palabras que obviamente es

más fácil de guardar que una serie de letras y números. Si guardas estas palabras y pierdes el dispositivo con la billetera, por ejemplo tu celular, puedes recuperar tus monedas nuevamente. Lo importante es entender que la responsabilidad de guardar la clave privada es cien por ciento tuya. Si se pierde una clave privada no hay forma de recuperarla y con eso también pierdes el acceso a las monedas.

¡Aviso de seguridad! Cómo guardar las claves privadas

Uno de los lemas de Bitcoin es “Be your own bank” (Se tu propio banco). Entonces si somos nuestro propio banco también somos responsables de la

seguridad de nuestros fondos. Es imprescindible que tengas una estrategia para asegurar las claves privadas. Una estrategia puede ser: guardar las claves privadas de cuatro formas:

- Dos veces físicamente –impresas o escritas en dos papeles guardados en dos lugares diferentes, por ejemplo en tu casa y en la casa de tus papás–.
- Dos veces de forma digital –en una flash USB o disco duro externo y en un archivo encriptado en la nube–.

Pueden ocurrir muchas cosas, pero si lo manejas de esta forma siempre tendrás una manera de recuperar las claves y

con eso tus monedas.

La clave pública se necesita para recibir criptomonedas. No hay problema en compartirla porque es pública. Esta clave se podría comparar con un número de cuenta de la banca que puedes compartir con todo el mundo porque sólo sirve para recibir fondos. Cada moneda con blockchain propia tiene diferentes estilos de claves públicas; no se puede enviar DASH a una clave pública de bitcoin, por ejemplo.

Una clave pública de bitcoin se ve así:

1MF7mwMuvCLhqmvmxmAWYdhp9ckbTTPW

Una dirección de DASH empieza

con X:

Xy3AjU6CG8pTWgVssyfqvFsxcRPxicsUpw

En algunas billeteras, cada vez que se recibe monedas en una dirección pública ésta cambia para la próxima recepción. Es decir, para cada transacción la billetera genera una nueva clave pública. Esto se hace para que una persona que tenga una clave pública tuya no sepa cuántas monedas en total tienes en la billetera. Eso sería fácil de revisar en la blockchain, sólo copias la dirección y la pegas en el buscador de una página como www.blockchain.com o www.blockexplorer.com. Por otro lado, es importante saber que una clave pública generada en la billetera será

vinculada a ella para siempre; es decir, aunque ya no aparezca visible sigue ahí y siempre vas a poder recibir más monedas con la misma dirección.

Diferencia entre una billetera caliente y una fría

Dependiendo de donde se guarda la clave privada se habla de billeteras calientes o frías. Si las claves privadas se generan en un dispositivo que está conectado a internet siempre, como el celular, por ejemplo, o un online wallet, entonces se trata de una billetera caliente y hay un mayor riesgo de que alguien pueda hackearla. Mayor seguridad brindan las billeteras frías que no están conectadas a internet, como

un paper wallet o un hardware wallet. Las claves privadas están físicamente en la billetera que está en poder del dueño. No hay forma de hackearlas, sino se tendría que robarlas físicamente.

Billeteras móviles

Las billeteras móviles son una excelente opción para tener tus criptomonedas contigo en el celular o en una tablet. Hay billeteras para una o para varias monedas diferentes. Esos wallets son fáciles de usar porque puedes escanear la dirección a donde quieres enviar monedas con la cámara de tu dispositivo o mostrar el código QR de una dirección tuya a un cliente o amigo para que pueda enviarte criptomonedas. Por seguridad

debes guardar montos pequeños en estas billeteras, porque las llevas contigo siempre.

Existen varias opciones entre las que puedes escoger, aquí una breve descripción de las más recomendadas:

Mycelium (bitcoin y bitcoin cash). La billetera móvil de Mycelium es una buena opción y está disponible para Android e iOS. Para usarla primero debes seguir los pasos para apuntar la clave SEED en caso de que pierdas o te roben el dispositivo y necesites recuperar tus monedas. Su uso no requiere una verificación de usuario KYC, el manejo de los fondos es anónimo. Mycelium permite administrar

varias cuentas dentro de la misma aplicación y soporta en este momento bitcoin y bitcoin cash.

Pros:

- No requiere KYC
- Permite administrar diferentes cuentas dentro de la misma aplicación
- Se pueden restaurar los fondos de un paper wallet

Cons:

- Sólo soporta dos monedas: bitcoin y bitcoin cash

Enlaces:

Web: www.mycelium.com

DASH Wallet: La billetera móvil de

DASH permite recibir y enviar DASH desde tu teléfono Android o IPhone. Después de la instalación se hace el proceso de seguridad para apuntar la clave SEED o crear un archivo de seguridad para la recuperación de fondos. La billetera también permite restaurar monedas DASH desde un paper wallet escaneando el QR de la clave privada.

Pros:

- No requiere KYC
- Permite restaurar fondos de un paper wallet

Cons:

- Sólo soporta moneda DASH

Enlaces:

Web: www.dash.org/downloads

Coinomi (Billetera multimoneda): Coinomi es una excelente opción si quieres guardar varias criptomonedas en una sóla aplicación en tu celular o tablet. La billetera está disponible para Android e iOS. Las principales criptomonedas están soportadas: bitcoin, bitcoin cash, ethereum, litecoin, DASH, y una variedad de monedas menos conocidas. No se requiere hacer el proceso de KYC y la clave se guarda con un SEED. Una función interesante son los exchanges integrados que permiten cambiar monedas dentro de la misma billetera. Además Coinomi

ofrece su billetera para Windows, MAC y Linux para mantenerla sincronizada con el celular.

Pros:

- No requiere KYC
- Soporta aproximadamente quinientas monedas y tokens
- Permite el intercambio de monedas directamente en la billetera
- Permite sincronizar entre la billetera móvil y una PC

Cons:

- Se han publicado algunas críticas a la seguridad de la billetera.

Enlaces:

Web: www.coinomi.com/

Billeteras web

En una billetera web tienes acceso a tus monedas a través de un explorador en cualquier dispositivo con internet, como laptop o PC. Para usar este tipo de billetera debes revisar bien los estándares de seguridad del operador. En algunos casos ellos guardan la clave privada para ti. La ventaja es que tienes una opción de recuperar tu contraseña para entrar a tu cuenta y no eres el responsable de guardar la clave privada. Por otro lado puedes perder tus monedas en el caso de un hackeo en contra de la empresa que opera la billetera. Cuando las claves privadas están en manos del operador tienes que pasar por un

proceso KYC para poder abrir una billetera.

Coinbase (bitcoin, bitcoin cash, ethereum, ethereum classic, Tokens ERC20, litecoin): Coinbase es la empresa más grande de compra y venta de criptomonedas en EEUU. Después de abrir tu cuenta puedes comprar o vender monedas usando transferencias bancarias o una tarjeta de crédito. La billetera requiere una verificación KYC y la compra y venta no está disponible en todos los países. Si quieres usar este servicio primero revisa si hay disponibilidad para tu país. La billetera opera via web en coinbase.com o con una App para el celular.

Pros:

- Las monedas más usadas en una sola billetera
- Soporta Tokens ERC20
- Comprar y vender criptomonedas por transferencia bancaria o tarjeta de crédito
- Acceso desde la web o el celular

Cons:

- Requiere KYC
- El servicio de compra y venta sólo está habilitado para algunos países

Enlaces:

Web: www.coinbase.com

Blockchain.com (bitcoin, bitcoin cash, ethereum, stellar, USD PAX): Es una de

las billeteras más usadas. Puedes abrir una cuenta y usar la billetera Blockchain desde un explorador web o desde el celular. También permite intercambiar tus criptomonedas dentro de la misma wallet. Hay varios niveles de seguridad y es una de las mejores billeteras para iniciar con criptomonedas.

Pros:

- Las monedas más usadas en una sola billetera
- Opción de intercambio de monedas integrado

Cons:

- KYC opcional

Enlaces:

Web: www.blockchain.com/wallet

Core wallets

Las core wallets son normalmente las primeras billeteras de una criptomoneda cuando entra al mercado. Son necesarias para operar como nodo para minar, hacer staking u operar un masternodo. Estas billeteras requieren muchos recursos en almacenamiento y poder de procesamiento porque guardan la blockchain completa en la computadora y están en constante comunicación con la red.

Bitcoin Core Wallet: La primera billetera para almacenar y hacer transacciones con bitcoins fue la Bitcoin Core Wallet. La instalas como programa

en tu computadora y después empieza a sincronizarse con la blockchain completa que hoy en día supera los 200 gigabytes de tamaño. El proceso de sincronización la primera vez puede demorar horas o hasta días. La copia de seguridad se crea en un archivo wallet.dat donde están almacenadas las claves privadas y que se debe guardar en un dispositivo externo como una flash, disco duro o la nube.

Pros:

- No requiere KYC
- Forma segura de almacenar bitcoins
- Funciona para minar bitcoins

Cons:

- Es muy pesada y requiere muchos recursos
- Sólo se puede acceder a las monedas desde una laptop o PC

Enlaces:

Web: www.bitcoin.org/es/descargar

Desktop wallets

La desktop wallet también se instala como programa en una laptop o PC, como una core wallet; la diferencia es que la desktop wallet es como una versión light que no tiene que guardar toda la blockchain en el dispositivo. La clave privada se guarda a través de un código SEED, tú eres el dueño de las claves privadas y no dependes de la seguridad del operador. Para mantener

un portafolio de diferentes criptomonedas una desktop wallet puede ser una buena opción.

EXODUS (Billetera multimoneda): La billetera multimoneda Exodus se puede instalar en Windows, MAC o Linux. Las principales criptomonedas y una gran cantidad de tokens ERC20 están disponibles para recibir, guardar y enviar. Exodus se enfoca en un diseño muy atractivo y tiene funcionalidades como la recuperación de fondos a través de un código SEED. Además muestra el portafolio de criptomonedas que tienes guardado a primera vista e incluye el intercambio de tus monedas dentro del programa.

Pros:

- No requiere KYC
- Plataforma de intercambio integrado
- Diseño atractivo

Cons:

- No hay una versión para 32 BIT de Windows

Enlaces:

Web: www.exodus.io

Hardware wallets

Una de las formas más seguras de guardar grandes cantidades de criptomonedas es un hardware wallet donde las claves privadas se generan y guardan offline. La mayoría de los

hardware wallets se asemejan a una flash USB donde está instalado un software para el almacenamiento de las claves. En el momento de conectarlo con una laptop o PC tienes acceso a tus fondos. En el caso de pérdida del dispositivo puedes recuperar tus monedas con un SEED de veinticuatro palabras. Los hardware wallets permiten guardar múltiples monedas y tienen en sus versiones básicas un costo alrededor de los 100 USD.

Ledger: La compañía Ledger es una de las pioneras en hardware wallets en el mercado y tal vez la marca más reconocida en este momento. Ofrece diferentes modelos según funcionalidad

y diseño. Las claves privadas se guardan en el dispositivo y la recuperación se puede realizar con um SEED de veinticuatro palabras que se crea en el momento de la primera instalación. A través del software Ledger Live tienes acceso a tus fondos desde una laptop, PC o celular conectando tu dispositivo. Ledger permite guardar las monedas más reconocidas y gracias a la integración con MyEtherWallet también todos los tokens ERC20.

Pros:

- No requiere KYC
- Alto nivel de seguridad por la generación y custodia offline de las

claves privadas

- Se pueden guardar la mayoría de las criptomonedas y tokens

Cons:

- Alto costo por el dispositivo en comparación con otras billeteras gratuitas

Enlaces:

Web: www.ledgerwallet.com/

Trezor: Trezor es otra buena opción para un hardware wallet. Es un poco más económico que la competencia de Ledger y también ofrece varios modelos. Trezor permite manejar las principales monedas con su software Bridge a través de su página web y todos los

tokens ERC20 con la integración de MyEtherWallet. También es interesante la conexión con Dropbox que permite estructurar diferentes cuentas con nombres y descripciones.

Pros:

- No requiere KYC
- Alto nivel de seguridad por la generación y custodia offline de las claves privadas
- Se pueden guardar la mayoría de las criptomonedas y tokens

Cons:

- Alto costo por el dispositivo en comparación con otras billeteras gratuitas

Enlaces:

Web: www.trezor.io/

Paper wallets

La alternativa más económica para guardar las claves privadas offline son los paper wallets o billeteras de papel. En este caso se genera una clave privada y pública a través de una aplicación JAVA y se imprimen las claves en un papel. El único lugar donde están las claves es el papel, así que es imposible robar las monedas si no es con el papel en mano. Por otro lado, una pérdida del papel con las claves significa una pérdida de los fondos.

Consejos para el proceso de la creación de Paper Wallets: Sobre todo cuando se

trata de grandes montos de monedas, un paper wallet puede ser una buena opción. Primero hay que abrir la aplicación JAVA, esto se puede hacer a través de una de las páginas web mencionadas abajo. Es importante desconectar la computadora de internet para que durante la creación de las claves no haya forma de espiar lo que pasa en el dispositivo. Una vez creadas las claves es recomendable imprimir dos ejemplares, en una impresora que no esté conectada a ninguna red empresarial de computadoras. Las hojas pueden plastificarse para que estén protegidas contra la humedad u otro daño externo. Para recuperar las monedas de los paper wallets puedes

usar una billetera móvil y debes siempre vaciar la dirección completa. Si quieres mantener una parte de las monedas en un paper wallet es mejor crear una billetera nueva una vez importada la clave privada a una billetera caliente.

Pros:

- No requiere KYC
- Alto nivel de seguridad por la generación y custodia offline de las claves privadas
- Forma económica para guardar las monedas offline

Cons:

- El papel puede dañarse fácilmente si no se protege bien

Enlaces:

- www.bitaddress.org
- https//.paper.dash.org
- www.walletgenerator.net (cerca de cien monedas soportadas)

Exchanges

Una opción bastante fácil de manejar, sin embargo con mayores riesgos, es guardar las monedas en una casa de cambio o exchange, como Binance, Bittrex o Bitmex. En este caso la clave privada está en manos del operador. Eso significa que no tienes que responsabilizarte de cuidar esta parte sensible de una billetera, pero a cambio estás dejando el control sobre tus monedas a un tercero. Si por ejemplo

quieres guardar un portafolio de muchas monedas en pequeñas cantidades, un exchange definitivamente es lo más fácil y rápido de administrar. Cuando los valores crecen es recomendable sacarlos y guardarlos en billeteras más seguras, de las que hemos mencionado anteriormente.

¿Por qué se dice que los exchanges no son tan seguros? Obviamente las empresas que crean un exchange están manejando fondos de miles de usuarios y hacen todo lo posible para mantener su plataforma lo más segura posible con revisiones informáticas las veinticuatro horas del día. Por otro lado, un hacker tiene mucha

más recompensa al llegar a las claves privadas de billeteras de un exchange que a la de un sólo usuario, por eso los exchanges sufren ataques constantes, la mayoría de las veces sin éxito; sin embargo a veces logran sus objetivos, como fue el caso del mayor hackeo de un exchange: en el año 2014 fueron robadas 844.448 bitcoins de MTGox. Es importante entender que en este caso no es que alguien hackeó la blockchain, sino que lograron robar una clave privada (phishing) y de esta forma tuvieron acceso a las monedas. Los exchanges, más que para guardar criptomonedas fueron creados para tradearlas; es decir, hacer compra y venta de las mismas e intercambiarlas.

Pros:

- Fácil manejo para guardar una gran variedad de monedas en pequeñas cantidades

Cons:

- Requiere KYC para manejar diferentes montos
- Hay ataques de hackeo contra los exchanges

Enlaces:

- www.bittrex.com
- www.binance.com
- www.bitmex.com

Multi-Sig wallets

Las billeteras Multi-Sig requieren la confirmación o signatura de varias

personas para poder realizar una transacción. Por ejemplo, puede ser que tengan que firmar 2 de 3 personas, 4 de 5, 8 de 8, cualquier combinación es posible. Estas billeteras sirven si se manejan fondos en conjunto, por ejemplo en diversos proyectos o empresas donde tienen que firmar el contador y el gerente y dos socios para autorizar una transacción.

Pros:

- No se requiere KYC
- Mayor seguridad por tener varias claves privadas
- Manejo de fondos entre varias personas

Cons:

- Una cantidad específica de usuarios tienen que confirmar las transacciones

Enlaces:

Para bitcoin las billeteras Multi-Sig más conocidas son:

- www.copay.io
- www.greenaddress.it

Ya conoces una gran variedad de opciones para recibir, enviar y guardar criptomonedas. Busca la opción que más se adapte a tus necesidades. Como último consejo para el manejo de billeteras te recomendamos no guardar nunca todos tus fondos en un único lugar, sino diversificar entre varias billeteras y tomar el respaldo de las claves privadas

y el código SEED en serio para respaldar tus monedas.

¿Cómo y dónde comprar tu primera criptomoneda?

Ahora que conoces la forma de guardar criptomonedas es momento de llegar a la práctica y comprar tu primera moneda o las primeras fracciones. Si eres nuevo en la criptoeconomía lo más importante es empezar a adquirirlas y usarlas. Después de haber instalado una billetera, a lo mejor una billetera móvil en tu celular, la siguiente pregunta que surge es: "¿Dónde compro mis primeras criptomonedas?". A continuación algunas opciones para comprar bitcoins u otras criptomonedas.

Persona a Persona

En este caso contactas a una persona de la comunidad de criptomonedas que está vendiendo sus monedas. Mucho ojo aquí porque no todos los vendedores de bitcoins son confiables. Si compras por primera vez a alguien que no conoces, es importante que pidas referencias antes de hacerlo para asegurarte de que es una persona confiable. En las transacciones por lo general quien compra monedas primero hace el pago en moneda fiat al vendedor que puede ser por transferencia o en efectivo. Después el comprador comparte su dirección de billetera y el vendedor le transfiere la cantidad de monedas acordadas. En

estas negociaciones también es importante acordar a qué tasa se realiza el cambio, porque las diferentes casas de cambio tienen cotizaciones diferentes; como referencia de precio se usa bitstamp.com, coinmarketcap.com o blockchain.com, por ejemplo. Además se acuerda una comisión para el vendedor que es un porcentaje que se aumenta en el precio. La ventaja de estas transacciones es que si lo haces con efectivo no dejas ningún rastro y no tienes que registrarte en ninguna parte.

Plataforma de intermediación

Existen plataformas de intermediación como localbitcoins.com o paxful.com que te permiten comprar y vender

criptomonedas a otros usuarios registrados. Antes de poder usar la plataforma tienes que abrir una cuenta y verificarla. Las plataformas manejan algunas medidas de seguridad para que las transacciones se realicen con éxito. Por ejemplo, el vendedor tiene que tener la cantidad de bitcoins que ofrece ya almacenada en una billetera de la plataforma para poder ofrecerlas. Cómo en cada compra aquí también vas a encontrar diferentes precios porque los vendedores quieren ganar una comisión por la venta y por eso los precios en la mayoría de los casos superan la tasa actual de la moneda.

Exchanges

Algunos exchanges como bittrex.com, kraken.com o bitstamp.com ofrecen la compra de criptomonedas directamente a través de su plataforma. Para eso tienes que abrir tu cuenta, verificarla y a través de una transferencia bancaria o pago con tarjeta de crédito mandas USD o EUR que después puedes cambiar por bitcoins o altcoins. Dependiendo del país la opción de compra puede estar disponible o no, sobre todo en países de Latinoamérica esta opción de compra puede que no esté habilitada.

Broker

Mientras un exchange se enfoca en el servicio de trading entre criptomonedas, un broker ofrece la compra segura de

criptomonedas con dinero fiat. Algunos ofrecen también una billetera. Otros brokers no almacenan monedas sino que las envían directamente a la dirección indicada. En Latinoamérica existen las siguientes opciones: buda.com, capitalika.com, bitinka.com, bitso.com, satoshitango.com. Algunos brokers internacionales y de europa son: anycoindirect.eu, crypto.com, btcdirect.eu, bitpanda.com.

Cajero (ATM)

En todo el mundo existen ya varios miles de ATMs que te permiten comprar tu criptomoneda favorita directamente con dinero en efectivo. Hay dos tipos de cajeros: las de una sóla vía, que

permiten sólo comprar, y los de dos vías, que permiten comprar y vender las monedas. Para saber si te encuentras cerca de un cajero automático de criptomonedas puedes revisar la página www.coinatmradar.com, que maneja el registro más completo de ATMs de criptomonedas en el mundo. También con la App en tu celular puedes ubicar la máquina más cercana con geolocalización. Para comprar en un ATM la mayoría de las veces necesitas pasar por un proceso de KYC la primera vez que lo uses y luego quedas registrado en una base de datos. Después puedes colocar el dinero en efectivo y la máquina manda los bitcoins directamente a la billetera que indiques.

¿Cómo y dónde usar tus criptomonedas?

La idea principal de Satoshi Nakamoto era que el bitcoin se convirtiera en un medio de pagos, que permitiera a las personas vivir libres de los bancos tradicionales y del dinero fiat. Algunas monedas para pagos son bitcoin, bitcoin cash, litecoin y DASH. Ahora ya es fácil de aceptar monedas digitales como medio de pago en tiendas online o físicas. Se pueden usar operadores de pagos como bitpay.com, coinpayments.net o iQCashNow.com que permiten varias opciones de cobro en criptomonedas. También la simple impresión de un código QR de una

dirección bitcoin u otra moneda en una hoja puede ayudar para que la gente en un local pueda realizar sus pagos en criptomonedas. Además existen ATMs de monedas digitales que incluyen un POS –Point of Sales (Punto de Pago)– para que se pueda generar una factura que el cliente paga con sus monedas. El mismo sistema POS se puede operar desde un celular o un dispositivo especial que genera códigos QR de pagos.

Aparte de hacer la transacción directa con criptomonedas puedes usar el servicio de tarjetas de débito que varios operadores ofrecen. Estos servicios permiten cargar tus

criptomonedas a una tarjeta y usar el saldo cargado en USD o EUR en locales o en cajeros.

Para aceptar criptomonedas en tu negocio o local primero tienes que revisar la regulación en tu país para no tener problemas legales o fiscales. Sólo hay pocos países en los cuales realmente está prohibido el uso de criptomonedas, en algunos todavía no se las reconoce como medio de pago.

Ventajas para el negocio por aceptar criptomonedas

Publicidad gratuita

Mientras no se aceptan monedas digitales en todos los negocios es una novedad que la comunidad cripto

publique en redes sociales o grupos de chats para mostrar a otros donde se pueden usar las monedas para compras. Eso atrae nuevos clientes al establecimiento.

Cobro y liquidez instantánea

Los pagos en criptomonedas llegan en pocos minutos y tienes liquidez inmediata; en cambio un cobro con tarjeta de crédito, débito o cheques, requiere varios días para que el dinero esté acreditado en tu cuenta. Para cobrar un cheque necesitas ir al banco, pierdes tiempo haciendo filas y además puede que se demore en hacerse efectivo o que el fondo no esté cubierto.

Bajo costo de transacción

Sobre todo cuando se trata de ventas al exterior, las criptomonedas tienen una gran ventaja porque no hay que usar costosos servicios de transferencias internacionales como Western Union, MoneyGram o transacciones bancarias. Además, cobrar con tarjetas de débito o crédito genera una comisión del 2 al 8% que asume el que cobra. En el caso de cobro con criptomonedas el cliente asume la pequeña comisión de transacción.

Conversión de monedas

Si operas un negocio online que vende a varios países del mundo, el bitcoin puede ser la moneda universal y no tienes que aceptar las diferentes divisas

de cada país. De esta forma evitas las comisiones por conversión a tu moneda local.

Mayor protección para el negocio

Con servicios como PayPal o tarjetas de crédito pueden ocurrir problemas con los clientes que después de realizar el pago y recibir la mercadería piden la devolución de su dinero. Tanto los operadores de tarjetas como PayPal primero protegen al cliente. Eso puede causar grandes daños económicos al negocio si los clientes se abusan de esta opción e indican que no les ha llegado la mercadería aunque se les ha enviado. En cambio los pagos con criptomonedas son irreversibles, el cliente no puede

hacer una devolución de su transacción.

Ventajas para el cliente al pagar con criptomonedas

No sólo el operador del negocio tiene ventajas, sino también el cliente se puede beneficiar de usar sus criptomonedas para realizar pagos.

Moneda universal

El bitcoin se puede usar en todo el mundo, como cliente no tienes que manejar diferentes divisas para realizar compras. Eso puede beneficiarte sobre todo si estás de viaje por varios países con diferentes divisas.

Seguridad

Aunque las tarjetas de crédito tienen sus

sistemas de seguridad y anti fraude, es un hecho que cada año hay millones de robos de datos de tarjetas de crédito que perjudican al cliente. En cada transacción con tarjetas de crédito revelas los datos completos para poder usarlas y eso hace que se clonen las tarjetas y se roben fondos. Mientras que en una transacción de criptomonedas la clave privada queda sólo en las manos del dueño y con eso es difícil de robar los fondos.

Bajos costos de transacción

Como ya se ha mencionado antes, sobre todo en transacciones internacionales se puede ahorrar usando criptomonedas. Un ejemplo es el pago de remesas al

exterior que en algunos casos genera comisiones del 10 al 20% sobre el monto enviado. También hay muchas personas que trabajan online para compañías del exterior o con empresas internacionales que no tienen cuentas bancarias en el país donde radican. En ese caso recibir los pagos en criptomonedas es económico y rápido.

Anonimato

Tal vez quieres realizar un pago a una persona y no quieres que exista un registro de esta transacción vinculado a tus datos personales. Con criptomonedas como DASH o Monero puedes realizar pagos anónimos como si estuvieras usando cash y no queda un rastreo.

Te invitamos a que no sólo guardes tus monedas y las veas como objeto de especulación. Esta nueva economía va a crecer mientras más personas usen sus monedas en la vida diaria. Siempre que tengas la oportunidad de pagar algo con criptomonedas hazlo y muestra a los demás que estás apoyando este cambio en la economía global.

El sistema financiero del futuro

Las fuerzas del mercado, no las mayorías políticas, serán las que transformarán a las sociedades.

DAVIDSON Y REES-MOGG

El Foro Económico Mundial (World Economic Forum) –WEF– estima que en el 2025 el 10% del PIB mundial será guardado en cadenas de bloques en forma de criptomonedas. Eso haría que la capitalización de todas las criptomonedas llegue a 10,1 billones de dólares, tomando como referencia el

valor actual del PIB mundial[1]. En comparación con su mayor auge a inicios de enero de 2018, la capitalización de todas las monedas apenas superó los 800 mil millones. Las criptomonedas pueden lograr que el monopolio de los bancos centrales sobre el dinero caiga. Las personas a través de bitcoins ahora tienen una alternativa al dinero fiat. Existe una competencia entre los diversos tipos de dinero y cada uno puede escoger qué es lo que más le conviene. Un ejemplo de lo que eso significa es nuevamente el caso de Venezuela, donde el dinero del Estado tiene muchos problemas y pierde la confianza. Diez años antes las personas

no tenían buenas alternativas, hoy usan bitcoin y DASH para crear una economía que no depende de las decisiones gubernamentales y el manejo monetario centralizado. Eso quiere decir que bancos y Estados han perdido poder en el sector monetario. Ya no pueden congelar los fondos de cualquier ciudadano porque las criptomonedas están en manos de cada uno. Nosotros vemos tres posibles escenarios para nuestro futuro financiero con respecto a las criptomonedas:

- Primero: El dinero fiat va a desaparecer y vamos a tener sólo una criptoeconomía.
- Segundo: El dinero fiat y las

criptomonedas existen paralelamente.

- Tercero: La criptoeconomía desaparece y vamos a tener nuevamente sólo el dinero controlado por el Estado.

La más realista nos parece la opción de una coexistencia entre el dinero fiat del Estado y la criptoeconomía de forma regulada. Las ventajas que brindan las monedas digitales son grandes, una persona que ya se ha beneficiado por su uso querrá usarlas siempre. Además, la creación de infraestructura para el uso de las criptomonedas es un buen negocio, así que hay un gran incentivo para nuevos

emprendimientos y empresas dedicadas a la creación de soluciones para el mercado masivo. Mientras más fácil y seguro sea el uso del bitcoin y los altcoins, más usuarios va a atraer. Es probable que las criptomonedas primero dominen los mercados en donde más ventajas traen: transacciones internacionales, remesas, transacciones anónimas, negocios online que están operando a nivel internacional. Además serán usadas en los casos donde el Estado no logre ofrecer un sistema financiero estable y donde los ciudadanos requieran de una alternativa para guardar su patrimonio en un activo internacionalmente reconocido.

El sector que parece que si va a cambiar mucho es el de los bancos privados. No sólo las criptomonedas van a encontrar su espacio en la economía de las personas, también las empresas Fintech (Finance and Technology). Estas compañías no bancarias que se dedican al desarrollo de soluciones en el sector financiero, como PayPal, están ganando mercado y revolucionando el sistema bancario anticuado con sus productos y servicios innovadores. Es sorprendente que los usuarios se hayan acostumbrado a que una transferencia bancaria internacional se demore de dos a diez días hábiles y que incluya a varios intermediarios que

encarecen dichas transacciones. Esto en un momento en que la información puede enviarse al instante y casi sin costo a todo el mundo. Los "millennials" que hoy en día nacen con la tecnología en sus manos ya no van a aceptar servicios llenos de trabas y demoras. Ellos buscan lo que más les convenga y lo que está a la par con la tecnología que están usando todos los días. Un sistema bancario anticuado les a aparecerá poco funcional en comparación con las criptomonedas. Es decir, sin innovaciones importantes en el sector bancario, éste puede sufrir grandes pérdidas de clientela y de poder que mantienen todavía.

PARTE 2

LA TECNOLOGÍA BLOCKCHAIN

Problema y solución

> *Me encanta esta tecnología y la comunidad. Me ha parecido que tiene principios profundos, objetivos, inquietos y realmente extraños. ¡Al igual que el Internet primitivo! Estoy emocionado de aprender más directamente.*
>
> JACK DORSEY

La Tecnología Blockhain

Si hace 25 años te decíamos que las actividades que realizan las personas iban a depender en gran medida de una

red informática global, ¿qué hubieses pensado? Apuesto a que hubieses creído que padecemos de algún desorden mental. Más de dos décadas después, el Internet se ha convertido en un servicio tan necesario como la electricidad o el agua potable. Del mismo modo, es probable que pienses que estamos locos si digo que, en algunos años más, blockchain o la cadena de bloques, será tanto o más importante que el mismo Internet, muchas de las actividades que realizamos a diario funcionarán más transparente y eficientemente gracias a esta tecnología innovadora y disruptiva.

El nuevo modelo de organización de la sociedad que

propone blockchain afectará a todas las industrias; desde la agricultura, pasando por la salud, las finanzas, la banca y muchas otras. La cadena de bloques "impone" la honestidad, la transparencia, la confianza y la verdad, gracias a la gestión distribuida de la información. Las personas queremos conocer cada día más acerca de los bienes y servicios que consumimos, por tanto, presionamos a los fabricantes y proveedores para recibir oportunamente información más segura y transparente.

Así que comencemos con la definición más simple de lo que es una cadena de bloques o blockchain; hablaremos primero de los bloques que

forman la cadena de bloques.

¿Qué es un bloque?

Un bloque es un registro de transacciones digitales que pueden ser muchas cosas:

- Un registro de una transacción comercial
- Criptomonedas como bitcoin, ether o litecoin, por ejemplo
- Contratos inteligentes
- Archivos almacenados en la nube
- Registros de todo tipo: contables, de identidad, médicos, de propiedad, de consumo de energía, etc.

¿Qué es blockchain?

Existen tantas definiciones como cadenas de bloques, al momento de escribir estas palabras –13 de marzo de 2019–, de acuerdo a www.coincap.io, existen dos mil ciento cuatro. El desarrollo de esta tecnología es tan vertiginoso que a diario aparecen nuevas plataformas y desaparecen otras tantas que no lograron consolidar su propuesta de valor.

Henning Diedrich, autor y colaborador de IBM ha dicho que "Blockchain está usualmente asociada con transacciones de datos, activos digitales y criptografía. La esencia de una blockchain es la descentralización y la replicación de la información que

contiene. Para mantener dichas copias sincronizadas en todos los nodos se utiliza un protocolo de consenso".

"Blockchain es un libro público distribuido digitalmente con el potencial de impactar drásticamente en todas las industrias que dependen de la confianza o el mantenimiento de registros", dice Scot Cohen, CEO de Bitzumi.

Por su parte, Andreas Antonopoulos señala que "Blockchain es un sistema que sustituye a la autoridad por la autonomía, produce resultados predecibles sin la influencia de los caprichos de la autoridad".

Para nosotros, luego de rumiar y procesar algunas definiciones y

conceptos, **la cadena de bloques es una base de datos abierta, distribuida, transnacional, neutral y resistente a la censura que puede almacenar y transmitir todo tipo de datos incluyendo activos.** Pensemos en unas cajas de cartón que están ordenadas cronológicamente, una tras otra, formando una cadena, y que cada una contiene documentos. Cada caja es un bloque, los documentos son las transacciones, un conjunto de cajas es una cadena de bloques.

La información –registros de todo tipo, transacciones, contratos…– se registra en un nuevo bloque que se une al bloque anterior y así sucesivamente,

formando una cadena incorruptible que no deja de crecer en longitud. Cada bloque contiene un algoritmo o función matemática llamada "hash" que ayuda a garantizar la seguridad de la red.

¿Qué es la criptografía?

La palabra criptografía proviene del griego "cryptos" –que significa "oculto"– y "grafe" –que quiere decir "escritura"–. La criptografía es la ciencia que resguarda documentos y datos a través del uso de códigos que no se pueden descifrar fácilmente. La criptografía es tan antigua que los romanos la utilizaban para proteger sus ideas y proyectos de guerra de sus enemigos.

La cadena de bloques emplea sofisticadas técnicas criptográficas para cifrar las transacciones que se van registrando. ¿Cómo se descifran o decodifican estos mensajes cifrados? A través del uso de una clave o llave pública y una clave o llave privada. La clave pública es algo así como tu "dirección digital" en la cadena de bloques. Esta clave pública no contiene ningún tipo de información personal del usuario, simplemente es una forma segura de expresar las ubicaciones digitales en una cadena de bloques a las cuales el usuario tiene acceso. Por otro lado, una clave privada actúa como la combinación secreta de una caja fuerte;

es decir, permite al usuario acceder y utilizar la información almacenada en una ubicación específica en la cadena de bloques, siempre y cuando conozca la combinación correcta, obviamente.

Entonces, una clave pública te da una ubicación segura en la cadena de bloques; la clave privada te da acceso a dicha ubicación.

Almacenamiento distribuido de datos

La información almacenada en una cadena de bloques se encuentra replicada o copiada en múltiples computadores que forman parte de la red; cada computadora se llama nodo, un conjunto de nodos conforman una red entre pares o entre iguales (P2P, por sus

siglas en inglés). La característica fundamental de estas redes es que no tienen un administrador o autoridad central; son sistemas descentralizados o distribuidos.

Al comparar el paradigma de gestión centralizada de datos con uno descentralizado –el que propone la cadena de bloques– podemos destacar las siguientes diferencias:

Gestión Centralizada	**Gestión Descentralizada**
Centralizado	Distribuido
La criptografía es una opción –mínima seguridad–	Usa criptografía por defecto –máxima seguridad–
Con autoridad	Sin autoridad
Las decisiones se	Las decisiones se

toman por imposición	toman por consenso
Un solo punto de falla y ataque	Numerosos puntos de falla y ataque –si uno o varios nodos son atacados la red sigue funcionando–
Respaldos fragmentados de información	Cada nodo tiene una copia o réplica del estado de la red
Baja resiliencia	Alta resiliencia

Cuando ocurre una transacción todos y cada uno de estos nodos –que contienen una copia exacta de la información almacenada– se encargan de verificarla y validarla. Una vez que esta transacción es considerada como válida por todos los nodos participantes,

se registra permanentemente en un bloque que se añade a la cadena de bloques.

Ventajas de blockchain

1. Al funcionar en una red peer-to-peer, la información almacenada en una cadena de bloques se encuentra distribuida, por lo que no existe un único punto sensible de acceso para ataques informáticos, en comparación con una red centralizada en la que sí existe un único punto de acceso.
2. La información distribuida no puede ser controlada por un individuo o una organización.

3. Las transacciones que ocurren entre personas dentro de una cadena de bloques se realizan sin la participación de intermediarios –bancos, gobiernos, abogados, notarías–.
4. El registro de las transacciones que se almacenan en una blockchain es público, por lo que puede ser visto y auditado por cualquier persona.
5. El contenido de una cadena de bloques es muy seguro ya que para validarlo y almacenarlo se utilizan algoritmos criptográficos que son muy difícil de decodificar.

La tecnología blockchain es fascinante, pero desafortunadamente aún está rodeada de mucha incertidumbre y enterrada bajo muchos metros de jerga confusa. No obstante, estamos seguros de que en el futuro cercano, blockchain será una herramienta imprescindible para las industrias y los gobiernos que pretendan conferir a sus productos y servicios confianza, libertad, honestidad y transparencia.

La importancia de la descentralización

> *Si en 1989 se preguntaba a las personas qué es lo que necesitaban para mejorar su vida, era poco probable que hubiesen dicho una red*

descentralizada de nodos de información que están vinculados mediante el hipertexto.

FARMER & FARMER

El paradigma centralizado, como una manera de estructurar los sistemas de cualquier tipo, ha sido el dominante durante tanto tiempo que hemos olvidado casi por completo que existe una mejor manera de organización.

La descentralización no es nueva, los humanos han usado sistemas de organización persona-persona (cliente-cliente, en términos informáticos) desde que la sociedad existe. La descentralización es la forma

original y primordial de organización. En cambio, la centralización es un invento relativamente nuevo, surgió a partir de la economía agraria con el fin esencial de evitar la violencia y el robo. Antes de la revolución agrícola casi no había nada que robar porque las comunidades nómadas vivían estrictamente con lo necesario ante la gran dificultad de trasladar numerosas pertenencias. Actualmente, todas nuestras interacciones sociales están organizadas en torno a los designios de las autoridades y la burocracia –la gran mayoría de veces equivocados y motivados por intereses particulares o de grupos–.

Tanto la centralización como la descentralización tienen que ver con la forma de organizar el poder en una sociedad y establecer el rol que cada uno de los participantes realiza en ella. La centralización luce como una pirámide, es un sistema jerárquico de poder muy eficiente –no necesariamente legítimo y adecuado– porque permite que un reducido número de individuos tome e imponga las decisiones en nombre de millones de personas. La gran falla de un sistema centralizado es que a medida que crece se vuelve automáticamente más corrupto. El poder en la pirámide se concentra en su ápice; mientras más alta la pirámide más alta la

concentración de poder, por tanto la corrupción se incrementa. ¿Qué clase de personas son las que buscan estas posiciones de poder? Los megalómanos, los narcisistas, los misóginos, los psicópatas, quienes bajo un disfraz de "buenismo" y liderazgo eficiente construyen enormes redes de corrupción y abuso de poder. ¿Cuál es la verdad en un sistema piramidal? ¿Qué se debe hacer? Lo que diga el sujeto que está en el ápice de la pirámide.

La descentralización es un concepto comúnmente mal entendido, se piensa que este paradigma favorece al caos, a la anarquía, a la ausencia de normas y acuerdos, cuando en realidad

da cabida a la autonomía, a la innovación, a la evolución, a la transformación, a la colaboración en lugar de la competencia y el abuso. Una de las principales bondades de los sistemas distribuidos es que son resistentes a la censura –básicamente porque no tienen un solo punto de ataque–; éstas no son las únicas razones por las que la descentralización es importante.

En un sistema descentralizado o distribuido no existe una cúspide de poder. El problema de estos sistemas es que se les hace difícil escalar y al mismo tiempo seguir tomando decisiones eficientemente. Sin embargo,

aquí es donde interviene la tecnología como repositorio de confianza y consenso. Gracias a blockchain y Bitcoin hoy se puede lograr el escalamiento de estos sistemas y hacer que la toma de decisiones sea eficiente.

La esencia de un sistema descentralizado o distribuido no es ser más eficiente que uno centralizado; es dar más libertad, autonomía, independencia y empoderamiento a sus usuarios. Eventualmente es necesario sacrificar la toma rápida de decisiones en beneficio del consenso generalizado, dicho de otro modo, la descentralización nos permite reemplazar la autoridad por la autonomía.

El agujero en la represa

La centralización y descentralización no son arquitecturas similares. Si se descentraliza mínimamente un sistema de control centralizado, el control se evapora. Una gran represa que contiene millones de metros cúbicos de agua debe tener una integridad estructural del cien por ciento, si esa integridad se reduce un uno por ciento la estructura puede colapsar. Bitcoin representa un hoyo en la represa, señala Andreas Antonopoulos.

Los sistemas centralizados a pesar de su poder son frágiles por naturaleza, por esta razón deben depender de puntos de control que,

paradójicamente, son blancos fáciles de ataque. De ahí que los sistemas centralizados de poder deban atacar, perseguir, censurar, secuestrar y asesinar. ¿Qué pasa cuando alguien ofende al poder?

Tecnología disruptiva

Cada tres, cuatro o cinco décadas el statu quo debe ser perturbado, modificado y transformado con el objetivo de evitar la acumulación de poder, la centralización, el totalitarismo y la corrupción. La corrupción es inherente a los sistemas de poder. No hay poder más tiránico que el poder sobre el dinero.

A pesar de que durante los

últimos 15 años hemos sido beneficiados con el poder liberador de Internet, especialmente para la descentralización de la comunicación, no podemos decir lo mismo de la banca. Con la creciente intervención de los gobiernos en la banca privada, estamos viendo cómo la inclusión financiera decrece. Hace tan sólo una década era posible abrir una cuenta bancaria en casi todo el mundo con la copia del pasaporte. Hoy ya casi no es posible.

La arquitectura disruptiva de Bitcoin nos proporciona una nueva forma de organizar el mundo. Exactamente de la misma manera que en su momento Internet liberó las

comunicaciones, Bitcoin liberará el dinero y las finanzas. Quien tenga bitcoin se convierte en su propio banco. Bitcoin es la primera red financiera neutral y descentralizada. En una transacción de bitcoins, a la red que la procesa y valida no le interesa la fuente, el destino, el monto o el tipo de aplicación que la soporta; por tanto, cualquier transacción que ocurre dentro de esta red no puede ser bloqueada, censurada, revertida o congelada; a la red solo le interesa si ésta es válida o inválida, dicho de otro modo, si cumple o no con las reglas de consenso establecidas.

¿Por qué la descentralización

eventualmente va a ganar?

Una cosa es decir que las redes descentralizadas deberían ganar, y otra cosa es decir que ganarán. No obstante, existen algunas razones que nos permiten ser optimistas en cuanto a la victoria.

Tomando un ejemplo del ámbito informático, el cual podría aplicarse también a muchos otros ámbitos. Los desarrolladores construyen software de todo tipo, hay millones de estos individuos alrededor del mundo que se encuentran altamente capacitados. Únicamente una pequeña fracción de ellos trabaja en grandes compañías de tecnología y una pequeña fracción trabaja en el desarrollo de nuevos

productos y servicios. Muchos de los proyectos de software más importantes de la historia fueron creados por startups o por comunidades de desarrolladores independientes.

Otro ejemplo, ilustra la rivalidad entre Encarta y Wikipedia en la década de los 2000. Encarta, enciclopedia centralizada creada por Microsoft, fue un producto mucho mejor que Wikipedia porque en ese entonces se encontraba mejor estructurada y contaba con una mayor cantidad de temas. No obstante, Wikipedia –que se fundamenta en la generación descentralizada de información– mejoró a un ritmo muchísimo más rápido porque tenía una

comunidad activa de contribuyentes voluntarios que se sintieron atraídos por su modelo de negocio descentralizado y gobernado por la misma comunidad. En 2005, Wikipedia era el sitio de referencia más popular de la red. Encarta fue cerrada en 2009.

La moraleja de esta historia, según señala Chris Dixon, es que cuando comparas sistemas centralizados y descentralizados necesitas considerarlos dinámicamente, como procesos, en lugar de estáticamente, como productos rígidos. Los sistemas centralizados usualmente comienzan como muy buenas ideas que se encuentran respaldadas por grandes presupuestos, sin embargo,

tienen una importante limitación: se desarrollan en función de las aptitudes y prioridades de los empleados de las empresas que patrocinan los proyectos. En cambio, los sistemas descentralizados se inician a medias, eventualmente sin grandes recursos y empresas por detrás, aunque en las condiciones adecuadas crecen de manera exponencial a medida que atraen nuevos contribuyentes y usuarios.

La siguiente era de Internet

Las redes descentralizadas no son una panacea que solucionará todos los problemas que tiene la red de redes, pero es indiscutible que ofrecen un enfoque mucho mejor que los sistemas

centralizados.

Comparemos el problema del spam en Twitter con el spam en el correo electrónico. Desde que la empresa del pajarito cerró su red a desarrolladores externos, la única compañía que trabaja para crear soluciones para combatir el spam es la misma Twitter; es decir, las reglas del juego cambiaron radicalmente. En contraste, existen cientos de compañías financiadas por miles de millones de dólares de capital de riesgo que se volcaron a buscar soluciones para contrarrestar el spam en el correo electrónico. Si bien es cierto que este problema no se ha resuelto en su

totalidad porque, aunque con mucha menos frecuencia, aún seguimos recibiendo correo no deseado–, el correo electrónico, al ser un protocolo descentralizado (IMAP, SMTP y POP3), permite la participación y la creación de nuevos negocios sin la preocupación de que las reglas del juego cambien drásticamente en el futuro.

Podemos también considerar el problema de la gobernanza de la red. Actualmente las grandes plataformas centralizadas en línea deciden cómo se clasifica y filtra la información, cuáles usuarios obtienen promociones y cuáles son censurados. En las redes criptográficas distribuidas estas

decisiones son tomadas en consenso por la comunidad, empleando mecanismos transparentes, abiertos y públicos.

Descentralización, paradigma de libertad

Lo que blockchain y Bitcoin han permitido es la creación de un sistema descentralizado de poder, un paradigma de libertad que nos va a permitir cambiar las instituciones sociales. No es sólo una cuestión monetaria y de pagos, debemos entender que tenemos la oportunidad de cambiar los mecanismos de organización social a favor de sistemas igualitarios, autónomos, independientes y esperanzadores. Las tecnologías que permiten la

descentralización y la distribución de poder no son del agrado de quienes pretenden mantener el paradigma del poder centralizado.

La esencia de una blockchain es la descentralización y la replicación. No se puede hablar de una blockchain si copias idénticas de ella no están almacenadas en muchos computadores –llamados nodos– de manera descentralizada. Para mantener dichas copias sincronizadas en todos los nodos se utiliza un protocolo o algoritmo de consenso como PoW, PoS, DPoS, PoA, PoET, PoC, entre otros.

A continuación una breve explicación de los algoritmos de

consenso más comunes:

Algoritmo de consenso	Descripción
Proof of Work (PoW) – Prueba de trabajo	Las transacciones que realizan los usuarios son validadas por los mineros quienes deben resolver complejos problemas matemáticos (esta es la prueba de trabajo) por medio de hardware específico (que consume abundante energía eléctrica) para hacerse acreedores a escribir las transacciones en la cadena de bloques.
	Las transacciones

Proof of Stake (PoS) – Prueba de participación	realizadas por los usuarios son confirmadas por validadores que depositan un determinado monto de la criptomoneda nativa en un escrow (como prueba de participación). El monto depositado más una ganancia son devueltos al validador si ha llevado a cabo exitosamente la tarea encomendada, de lo contrario, pierde el depósito.
	Esencialmente funciona igual que PoS con la diferencia que se elige y delega a otros validadores (llamados

Delegated Proof of Stake (DPoS) – Prueba de participación delegada	testigos) el poder de voto sobre la confirmación de las transacciones. Las cadenas de bloques que usan DPoS tienen una mayor velocidad de procesamiento de transacciones.
Proof of Capacity	Los minadores (también llamados nodos) en lugar de aportar capacidad de procesamiento (que consume ingentes cantidades de energía eléctrica) para resolver complejos problemas matemáticos (como en PoW), contribuyen con capacidad de almacenamiento en disco

(PoC) – Prueba de capacidad	duro como una prueba de trabajo que les concede la atribución de confirmar las transacciones y registrarlas en una cadena de bloques. A mayor capacidad de almacenamiento, mayor capacidad de confirmación de las transacciones.

Las redes criptográficas son una forma poderosa de desarrollar redes que sean propiedad de la comunidad, también proporcionan un campo de juego equilibrado para desarrolladores, creadores y empresas. Tuvimos la

oportunidad de observar el valor de los sistemas descentralizados en la primera era de Internet. Esperemos que podamos verlo de nuevo en la próxima.

Estamos siendo testigos del desarrollo de una nueva forma de organizar la sociedad. La cadena de bloques y Bitcoin nos están dando la oportunidad de cambiar el balance de poder desde el sistema amo–esclavo, que es rígido, cerrado, autoritario, centralizado y corrupto, hacia otro fundamentalmente diferente, el persona–persona, que es flexible, abierto, horizontal, distribuido y autónomo.

Blockchain, el protocolo de confianza

[Blockchain] es la gran cadena de

estar seguros de las cosas.

THE ECONOMIST

[Extracto de la charla TEDx Quito, “Blockchain y la generación de confianza” de Juan Francisco Bolaños (La charla completa puede ser vista en https://youtu.be/bDo4-qiU8JQ)]

“La confianza es fundamental para establecer cualquier tipo de relaciones, gracias a ella se construyen los hogares, las empresas, las

sociedades. De acuerdo con la investigadora de la colaboración, Rachel Botsman, la confianza ha evolucionado en tres etapas: local, institucional y distribuida.

"Nos encontramos en un momento en que hemos dejado de confiar en las instituciones –que constantemente nos fallan– para confiar en los extraños...

"Cuando las sociedades eran más pequeñas, sus miembros podían intercambiar valor y llegar a acuerdos con relativa facilidad, porque se conocían entre sí; si alguno de ellos actuaba deshonestamente, era probable que el resto lo llegase a ver,

perjudicando seriamente su reputación. Conforme las sociedades crecieron y las distancias se hicieron más grandes, así también lo hizo la incertidumbre. Con la creación de instituciones, que son las llamadas a actuar como intermediarios de confianza entre las personas, se logró reducir esta incertidumbre a niveles tolerables. Sin embargo, estas instituciones tanto públicas como privadas [Estados, gobiernos, banca, corporaciones, iglesias], nos han venido fallando consistentemente, debido a su estructura rígida, jerárquica, centralizada y muchas veces obsoleta. La centralización y la acumulación de poder generan corrupción…

“**Lo fascinante de los nuevos inventos y paradigmas es que resulta extremadamente difícil pronosticar el impacto que los nuevos inventos y paradigmas tendrán en el futuro**; sus implicaciones se van descubriendo sobre la marcha, al cabo de décadas, muchas veces. Con el fin de predecir el impacto que un nuevo paradigma tendrá es necesario que nos hagamos la siguiente pregunta: ¿cuál es el espacio o el vacío que este nuevo paradigma ayuda a llenar?

“En el siglo XV, la invención de la imprenta llenó el vacío del conocimiento; puso a disposición de todos libros llenos de información que

antes estaba únicamente en manos de ciertos privilegiados. La máquina de vapor en el siglo XIX trasladó el trabajo manual hacia el mecánico, llenó el vacío de poder, en términos de energía y fuerza necesarias para la producción de bienes en serie… Ya en el siglo XX, en la década de 1970, apareció Internet, llenando el vacío de la distancia, reduciendo el tamaño del mundo, permitiendo que nos comuniquemos casi gratis e instantáneamente sin importar dónde nos encontremos.

"En 2009, nace una nueva propuesta tecnológica que ofrece llenar el vacío de la confianza. Así como Internet transformó radicalmente las

comunicaciones poniéndolas al alcance de todos, democratizándolas, la cadena de bloques hará lo mismo con las instituciones sociales, políticas y económicas.

"Blockchain es una base de datos abierta, sin fronteras, distribuida, neutral y resistente a la censura, que almacena y mueve todo tipo de datos, incluyendo activos –dinero, acciones, certificados, títulos, música, fotografía, etc.–. No es más que un gran libro contable, cuyos asientos o transacciones [codificados a través de un algoritmo criptográfico] se encuentran almacenados en una estructura secuencial de bloques ordenada

cronológicamente y relacionada entre sí matemáticamente… Estos datos contenidos en los bloques no pueden ser modificados o borrados sin el consenso de todos los participantes de la red informática –llamados nodos–…

"Cuando hacemos cualquier tipo de transacción partimos de la premisa de que no podemos confiar en la otra parte, por eso es necesaria la participación de intermediarios que verifiquen y certifiquen que lo que la otra parte nos dice es verdad. Los registros que actualmente utilizamos para verificar y respaldar las transacciones que realizamos, como por ejemplo, comprar una casa o un auto son

fácilmente manipulables, porque son gestionados centralizadamente…

"Blockchain puede ser utilizada para cualquier cosa que requiera de validación, certificación y garantía de ejecución sin la participación de un intermediario de confianza. Mi sueño es ver un mundo más libre, próspero, honesto y justo. Gracias a la cadena de bloques lo podemos lograr:

- Producción de alimentos limpia y honesta
- Agricultores que reciben un pago justo por sus productos
- Mercados sin intermediarios, que conectan directamente a productores con consumidores

- Consumidores que tienen información transparente y fiable de los productos que adquieren
- Creadores de contenido –escritores, músicos, fotógrafos– que reciben compensaciones adecuadas por su trabajo
- Elecciones transparentes, libres de fraude, auditables públicamente en tiempo real y resistentes a los apagones
- Gobiernos que gestionan las finanzas públicas con responsabilidad y transparencia
- Transferencias globales de dinero de manera rápida y con

costos razonables

- Servicios financieros para más de 2.000 millones de personas que no tienen cuentas bancarias
- Generación y venta persona a persona de energía eléctrica sustentable
- Inserta aquí tu idea. La imaginación no tiene límites…

"Para concluir, quiero decir que los paradigmas políticos, sociales y económicos tienen fecha de caducidad; funcionan bien durante un tiempo, luego empiezan a fallar, se los puede ajustar, pero tarde o temprano deben ser reemplazados por otros porque se vuelven obsoletos.

“Tengo la firme convicción de que la cadena de bloques es ese nuevo paradigma”.

Funcionamiento de la cadena de bloques

Explicación sobre las bifurcaciones de una cadena de bloques

Personalmente me gustan las bifurcaciones duras. En particular me gusta el hecho de que dan a los usuarios una medida de control, lo que les obliga a optar por los cambios de protocolo. Claro, pueden ser un poco más caóticos si son controvertidos, pero ése es el precio de la libertad.

VITALIK BUTERIN

Una bifurcación dura o “hard fork” es

una actualización significativa en el código de software que corre en los nodos de la red de una cadena de bloques que hace que las transacciones antes consideradas inválidas se consideren válidas y viceversa. Una bifurcación puede reescribir la historia de una cadena de bloques, por ejemplo, puede darse para revertir robos de dinero –como en el caso del hackeo a The DAO–, para reparar fallas de seguridad importantes o para introducir nuevas funcionalidades.

Una bifurcación es una condición por la cual el estado de la cadena de bloques se divide en cadenas donde una parte de la red tiene una perspectiva

diferente en el historial de las transacciones que la otra parte de la red. Dicho de otro modo, es una divergencia o desacuerdo en la perspectiva del estado de la cadena de bloques.

Para que ocurra una bifurcación dura los propietarios de los nodos deben decidir si aceptan los cambios propuestos o no. Con el objetivo de implementar los cambios, los nodos deben detenerse para recibir la actualización del código, que empezará a correr a partir de un número específico de bloque de una cadena de bloques.

Luego de la aplicación de una bifurcación dura la cadena de bloques

original se divide en dos, con la probabilidad de que la variante más antigua desaparezca tarde o temprano –dando origen a una bifurcación suave o "soft fork"–, caso que ocurre cuando ningún nodo la corre.

Diferencia entre hard fork y soft fork

Cada vez que una cadena de bloques debe actualizarse puede lograrlo a través de la implementación de uno de dos procesos: bifurcación dura o suave. En el primer caso, el software de la actualización no es compatible con versiones anteriores, por tanto los usuarios que no corran esta nueva versión ya no podrán interactuar con los nodos que corran la actualización. En el

segundo caso, el software de la actualización es compatible con las versiones anteriores, sin embargo todas las actualizaciones ya no serán visibles en las versiones anteriores. Por ejemplo, la bifurcación que dio origen a la cadena de bloques de Bitcoin Cash fue dura; la que permitió la implementación de SegWit en Bitcoin fue suave.

Ambos tipos de bifurcaciones dividen a la cadena de bloques original en dos cadenas, son esencialmente lo mismo, con la diferencia de que en una bifurcación suave, sólo una cadena de bloques seguirá siendo válida a medida que todos los nodos adopten la actualización de software, mientras que

la otra desaparecerá; en una bifurcación dura, en cambio, ambas cadenas pueden existir.

Andreas Antonopoulos describe la diferencia entre una bifurcación suave y dura de la siguiente forma:

> *Si un restaurante vegetariano escogiera agregar carne de cerdo a su menú, se consideraría una bifurcación dura. En cambio, si se decidiera agregar platos veganos, todos los vegetarianos podrían seguir comiendo en el restaurante; no es necesario que se hagan veganos para comer allí, los carnívoros también podrían* comer, así que sería una bifurcación suave.

El hackeo a The DAO

Una de las más famosas bifurcaciones duras es la que originó a Ethereum Classic (ETC). Luego del hackeo de The DAO y el cuasi saqueo de 150 millones de dólares en Ether (ETH), ocurrió un hard fork que dividió la cadena de bloques en dos, dando como resultado dos mainnets operativas: Ethereum y Ethereum Classic.

A principios de mayo de 2016, algunos miembros de la comunidad Ethereum anunciaron el inicio de The DAO, que también se conocía como Genesis DAO. Fue construido como un contrato inteligente en la cadena de bloques de Ethereum. El DAO tuvo un período de creación durante el cual a

cualquiera se le permitió enviar Ether (ETH) a una dirección de billetera especial a cambio de tokens DAO en una escala de 1-100. El período de creación fue un éxito imprevisto, ya que logró reunir el equivalente en ETH a 150 millones de dólares, siendo el crowdfunding más grande de la historia.

El 18 de junio de 2016, los miembros de la comunidad de Ethereum notaron que los fondos de The DAO estaban siendo sustraídos, y que el saldo total de Ether depositado en el contrato inteligente disminuía rápidamente.

Tras el pirateo a The DAO, la comunidad de Ethereum votó casi unánimemente: el 89% estuvo a favor de

una bifurcación dura con el fin de revertir las transacciones que desviaron decenas de millones de dólares en Ether por parte de un pirata informático anónimo. La bifurcación de la blockchain de Ethereum ocurrió el 20 de julio de 2016 en el bloque número 1.920.000.

Es importante comprender que este error no provino de Ethereum en sí, sino de The DAO, Organización Autónoma Descentralizada (DAO, por sus siglas inglés), que se creó en la plataforma de Ethereum. El código escrito para The DAO tenía varios errores. Otra forma de explicar esta situación es comparar Ethereum con

Internet y cualquier aplicación basada en Ethereum con un sitio web; si un sitio web no funciona no significa que Internet no funcione, simplemente significa que un sitio web tiene un problema.

Las bifurcaciones de Bitcoin

Las mayores bifurcaciones de la blockchain de Bitcoin hasta ahora, ocurrieron durante 2017 y 2018. la historia de las bifurcaciones no terminó con Bitcoin Cash (agosto 2017), Bitcoin Gold (octubre 2017); teniendo en cuenta que la cadena de bloques de Bitcoin funciona y se transforma gracias al consenso de sus participantes, es complicado pronosticar si es que en

futuro ocurrirán bifurcaciones duras, en cualquier caso, podemos estar seguros de afirmar que sí.

Las bifurcaciones realizadas a principios de 2018, llevan los nombres de: Super Bitcoin, Lightning Bitcoin, Bitcoin God, Bitcoin Uranium, Bitcoin Cash Plus, Bitcoin Silver y Bitcoin Atom. Algunas de estas bifurcaciones duras pudieron ser canceladas o bien, si efectivamente ocurrieron, las cadenas de bloques resultantes no tuvieron la suficiente acogida por parte de los usuarios y los mineros, y desaparecieron.

Es conveniente mencionar que antes de Bitcoin Cash, la blockchain de

Bitcoin sufrió tres bifurcaciones duras que dieron origen a Bitcoin XT (diciembre 2014), Bitcoin Unlimited (enero 2016) y Bitcoin Classic (febrero 2016), ninguna de las cuales funciona en este momento.

¿Por qué debería preocuparme por las bifurcaciones duras?

¡Es una gran pregunta! Hay varios motivos por los que debes preocuparte:

1. Al cambiar las reglas del juego, la nueva moneda resultante podría ser mejor que la original en cuanto a sus características, funcionalidades, aplicaciones, haciendo que la moneda original pierda su valor y eventualmente

desaparezca.

2. La bifurcación podría tener un importante impacto en la comunidad de usuarios y desarrolladores, afectando su adopción y valor.
3. Los poseedores de la moneda original, en la mayoría de los casos se hacen acreedores de la nueva moneda al momento de la bifurcación. Por ejemplo, si Juan tenía 1 BTC al momento de la bifurcación que dio origen a Bitcoin Cash, Juan se hacía acreedor de 1 BCH también.

Para terminar, quiero dejar al lector con esta idea, que tiene una

estrecha relación con las bifurcaciones como un mecanismo para lograr el consenso necesario para la implementación de los cambios o actualizaciones en una red distribuida:

La esencia de un sistema distribuido no es ser más eficiente que uno centralizado; es dar más libertad, autonomía, independencia y empoderamiento a sus usuarios. En un sistema distribuido, las decisiones se toman por todos los participantes con base en reglas de consenso definidas, en lugar de ser impuestas por una autoridad central que, en muchos de los casos, se aprovecha de su poder, tomando decisiones abusivas o poco

convenientes para los intereses de la mayoría.

La complejidad detrás de las actualizaciones de una blockchain

> *La escalabilidad es esta idea de crear una cadena de bloques que pueda desarrollarse mucho más que las cadenas existentes, esencialmente mediante el procesamiento de transacciones en paralelo. Y alejarse de este paradigma donde cada nodo en la red tiene que procesar cada transacción.*
>
> VITALIK BUTERIN

Las actualizaciones de una cadena de bloques pública como Bitcoin o Ethereum siempre representan fuertes

dolores de cabeza. La implementación de SegWit en la blockchain de Bitcoin tomó dos años de un serio y acalorado debate.

La primera pregunta que la mayoría de la gente normal se hace es: ¿cómo se planifican e implementan las actualizaciones en una organización descentralizada? Una de las características de estas organizaciones es la ausencia de una autoridad central que toma las decisiones a nombre de sus subordinados, esto quiere decir que nadie realmente decide cómo deben funcionar. Las cadenas de bloques tienen reglas establecidas a través de un protocolo o algoritmo de consenso, estas

reglas se definen en el código que establece su funcionamiento.

Los participantes de una blockchain –individuos, empresas, mineros– de hecho cumplen con las reglas de consenso, por tanto, están conscientes de que cualquier cambio en la red que se proponga requiere en teoría de una coordinación entre todos sus participantes, que en la mayoría de los casos no se conocen entre sí.

En las cadenas de bloques como Bitcoin y Ethereum, de las que se podría decir que son realmente descentralizadas, los cambios ocurren más o menos de la siguiente manera:

1. Si uno de los participantes tiene

una idea que quisiera implementar con el fin de mejorar las características de la red, habla con otros participantes al respecto y si su idea tiene aceptación escribe una propuesta formal, por ejemplo un BIP (Bitcoin Improvement Proposal) que es una propuesta de mejora de Bitcoin.

2. Dicha propuesta se comparte en los diferentes canales digitales, como listas de correo o foros en los que participan miembros de la comunidad.
3. Si se considera que la propuesta

es una buena idea el trabajo empieza, generalmente con planes para implementarla con otras mejoras similares. Las actualizaciones compatibles con versiones anteriores del software pueden implementarse muy lentamente, como una bifurcación suave (soft fork). Los cambios más grandes que no son compatibles con la versión actual, deben implementarse obligatoriamente a través de una bifurcación dura (hard fork). Usualmente la implementación de estos procesos es muy polémica y muchos usuarios que no están de acuerdo con ellos

deciden seguir usando la versión anterior del software y eventualmente crear una nueva cadena de bloques.

4. Cada implementación de software se actualiza por separado. Se anuncia la fecha de actualización con la debida anticipación para que todos los nodos tengan el tiempo suficiente de actualizar a la versión más reciente del software. Llegada la fecha de actualización, las nuevas características de la implementación se activan.

Por lo pronto, en Bitcoin, las

bifurcaciones duras son el último recurso. SegWit fue finalmente adoptado por la red después de que Peter Wuille, desarrollador primario de Bitcoin y cofundador de Blockstream, descubrió la manera de implementarlo a través de una bifurcación suave.

A mediados del mes de enero de 2019, Ethereum había planificado implementar su próxima gran actualización, Constantinopla. Esta no pudo llegar a buen término porque a último momento se descubrió un error importante en el código. Muchos de los nodos que ya se habían actualizado tuvieron que instalar nuevamente la versión anterior. Finalmente, una vez

superados los inconvenientes, la actualización de Ethereum se ejecutó el 28 de febrero de 2019 en el bloque 7.280.000.

Esta actualización considera muchas mejoras de rendimiento entre las que se destaca la modificación de la bomba de dificultad siendo la que más tiempo tardó en acordarse. Los desarrolladores de Ethereum quieren migrar de PoW a PoS, por este motivo buscan alentar a los participantes de la red a través de la implementación de una serie de bombas predefinidas que irán reduciendo el incentivo económico que los mineros reciben por cada bloque creado. Lo que se logrará finalmente es

la transición de PoW a PoS por medio de una actualización del software que gobierna a esta cadena de bloques.

Teniendo en cuenta que la investigación y desarrollo de PoS ha tardado más de lo esperado, los desarrolladores de Ethereum necesitaban impulsar la implementación de la bomba de dificultad y al mismo tiempo requerían que los mineros permanecieran a bordo y no abandonaran la red. Si bien casi el 50% de los nodos ya se había actualizado al nuevo software, una empresa independiente de auditoría de seguridad de contratos inteligentes, ChainSecurity, encontró una vulnerabilidad que obligó

a que la actualización se pospusiera hasta febrero.

Esta situación generó un debate entre los desarrolladores de Ethereum y los programadores de contratos inteligentes que, como no puede ser de otra manera, quieren que sus contratos sean inmutables tal y como lo ha garantizado Ethereum desde el principio, argumentando que los cambios en la manera en que se interpreta el código a través de las nuevas actualizaciones podrían afectar significativamente la inmutabilidad de los contratos inteligentes. Del mismo modo, este debate se ha extendió hacia la comunidad criptográfica, donde se ha

comentado que hacer cambios en una cadena de bloques es más parecido a la ciencia espacial que a la creación de una aplicación para compartir fotos. Los errores pueden ser fatales e incluso más difíciles de corregir luego de la ejecución de las implementaciones.

¿Qué garantías deben dar los desarrolladores de los protocolos a quienes crean aplicaciones en la parte superior de su cadena? ¿Es posible que un pequeño grupo de desarrolladores o algunas empresas tengan el control sobre la hoja de ruta de Ethereum?

Es indiscutible que las blockchains públicas enfrentan complejos problemas de escalabilidad

teniendo en cuenta que dependen del acuerdo entre sus participantes. Las cadenas de bloques públicas sacrifican la toma eficiente de decisiones en favor de la autonomía, libertad, independencia y empoderamiento que se logran a través del consenso generalizado. Aún estamos lejos de descubrir si esta visión que pretende modificar radicalmente el paradigma del orden social y modificar el balance de poder tendrá éxito.

Casos de uso de Blockchain

¿Blockchain es la tecnología que tu empresa necesita?

> *Las grandes empresas no están dispuestas a experimentar cambios radicales por sí mismas. Todo lo que quieren hacer es mejorar por sí mismas. Ven a la cadena de bloques como un proyecto más de IT: va a ahorrar dinero; va a mejorar un proceso aquí y allá; pero no va a transformar el negocio.*
>
> WILLIAM MOUGAYAR

La cadena de bloques está recibiendo mucha atención por su capacidad de modificar radicalmente los procesos

empresariales e industriales, debido a esto muchas organizaciones están tratando de aprender acerca de esta innovadora tecnología con el fin de incorporarla en sus actividades.

Con el fin de evitar que la implementación de blockchain sea un despilfarro de tiempo y dinero conviene siempre hacerse la pregunta planteada en el título de este acápite: ¿Blockchain es la tecnología que mi empresa necesita? Trataremos de responder si todas las empresas deberían utilizar esta aún muy costosa tecnología y cuáles son los aspectos que deberían tenerse en cuenta antes de tomar la decisión de adoptarla.

En una encuesta llevada a cabo por Juniper Research en agosto de 2017 en la que se preguntó a empresas de más de 20 mil empleados si buscaban implementar blockchain, se obtuvo que el 57% de los encuestados respondieron "sí", mientras que sólo el 9% respondieron "no", y el 34% "no lo sabe". Asimismo, el 76% de los empleados encuestados dijeron que blockchain podría ser "muy útil" o "bastante útil" para su empresa.

Esto es lo que la cadena de bloques puede ofrecer a las empresas e industrias:

1. La red informática de una cadena de bloques es

descentralizada o distribuida, esto quiere decir que ninguna entidad tienen el control absoluto sobre la información que almacena. Cada uno de los participantes –llamados nodos– posee una copia exacta de los datos almacenados.

2. Los datos que contienen los bloques se encuentran asegurados con sofisticadas técnicas criptográficas y con una marca de tiempo indeleble que proveen extrema seguridad ante posibles ataques.
3. La información que almacena una cadena de bloques es

inmutable, no puede ser alterada o borrada. Teniendo en cuenta que se trata de una red distribuida, nadie puede manipular los datos que contiene.

4. Los datos que almacena pueden ser auditados y rastreados públicamente y en tiempo real sin la necesidad de contar con la participación de un intermediario que actúa como validador o certificador de esa información.

Si funciona, no lo arregles

La idea de que todo debería estar descentralizado es errónea. Muchas

compañías que están desesperadas por adoptar blockchain poseen sistemas centralizados que de hecho funcionan a la perfección. ¿Por qué se debería implementar una tecnología con la cual no se tiene experiencia?

Si lo que se busca es incrementar la eficiencia de los procesos, la respuesta puede ser el rediseño de las soluciones existentes sin la necesidad de dar el gran salto tecnológico que la cadena de bloques significa. Usualmente, el cambio sistemático es mejor para la empresa que una transformación totalmente radical. En todo caso, no podemos dejar de mencionar que es indiscutible que

blockchain tiene muchos casos de uso significativos; no obstante, hay unos pocos casos de uso exitosos, muchos de ellos aún se encuentran en fase experimental y otros no han salido de la teoría.

Blockchains abiertas versus blockchains cerradas

En términos generales, existen dos tipos de cadenas de bloques en función de los permisos y privilegios que deben tener sus participantes para poder acceder a la red distribuida.

Blockchains abiertas

Son redes abiertas, no discriminatorias y resistentes a la censura, a las que cualquier participante puede unirse sin

la necesidad de contar con la autorización correspondiente. A pesar de que las cadenas de bloques públicas —(Bitcoin, Ethereum, NEO y NEM)— tienen un sinnúmero de cualidades que las hacen muy interesantes, no se puede negar el hecho de que aún tienen serios problemas de escalabilidad y, por tanto, no están listas para manejar volúmenes significativos de transacciones y datos.

Blockchains cerradas

Se trata de redes cerradas –a pesar de ser descentralizadas–, discriminatorias y no resistentes a la censura, en las que los nodos participantes deben contar con una autorización previa antes de formar parte de la red. Este tipo de cadenas de

bloques pueden ser controladas por una o varias entidades. Las blockchain privadas son las preferidas por los bancos y demás actores del sector financiero. Según los críticos de este tipo de estructuras, éstas no se diferencian en lo absoluto de las bases de datos compartidas. Entre las cadenas de bloques cerradas destacan Hyperledger. Multichain, Corda R3, Credits, Quorum, LACChain, entre otras.

¿Cuándo se debería considerar la adopción de la cadena de bloques?

Para contestar esta pregunta de la manera más clara, es necesario hacerse las siguientes:

1. ¿La organización depende de

terceros para gestionar sus operaciones?

2. ¿Estos intermediarios representan importantes egresos de recursos para la empresa?
3. ¿La eliminación de intermediarios significa un ahorro relevante de recursos?
4. ¿Se necesita una base de datos compartida entre los diferentes participantes de la cadena de suministro?
5. ¿La empresa está dispuesta a desenvolverse en un entorno en el que la confianza se traslade desde las instituciones ▌–que actúan como intermediarios– ▌

hacia la tecnología?

6. ¿Se requiere de soluciones tecnológicas contractuales?
7. ¿Existe la necesidad de trabajar con activos digitales?
8. ¿Es necesario tener un registro permanente, claro e inmutable de los diferentes procesos organizacionales para asegurarse de que todo funciona como debería?
9. ¿Existen procesos ineficientes que necesitan ser mejorados?
10. ¿Es posible destinar recursos para la educación y capacitación del personal de la empresa empezando por los ejecutivos?

11. ¿Es posible poner a todo el personal al día con el profundo cambio que significa adoptar una nueva tecnología?
12. ¿Es posible contratar consultores, asesores y desarrolladores blockchain a un precio accesible?
13. ¿Debería cambiar toda la infraestructura tecnológica de la empresa porque la actual posee muchas deficiencias?
14. ¿Se requiere una limitada capacidad de almacenamiento?
15. ¿Es necesaria una velocidad limitada en el procesamiento de los datos?

16. ¿La empresa está dispuesta a arriesgar tiempo y recursos para apostar por la implementación de una tecnología que promete mucho pero que aún se encuentra en una etapa temprana de desarrollo?

Si las respuestas a la mayoría de estas preguntas son afirmativas, la cadena de bloques es una excelente solución que debería implementarse en tu organización. Caso contrario, deberías pensar si realmente existe la necesidad y si hoy es el momento de hacerlo, teniendo en cuenta que esta tecnología se encuentra en una fase de desarrollo y su implementación todavía

puede ser costosa.

¿Conoces el origen y los ingredientes de los alimentos que consumes?

La tecnología "blockchain" ayuda a conocer el recorrido exacto que hacen los alimentos y los procesos que sufren. Los datos van a revolucionar las cadenas de suministro.

ELPAIS.COM

[Con extracto de la charla TEDx Quito, "Blockchain y la generación de confianza" de Juan Francisco Bolaños (La charla completa puede ser vista en https://youtu.be/bDo4-qiU8JQ)]

"… Me encontraba en Lima, asistiendo a una reunión con uno de los fundadores de la empresa italiana a la que

represento. Esta organización es una de las pioneras en el desarrollo e implementación de sistemas inmutables de trazabilidad basados en blockchain".

Un exquisito ceviche peruano

"Fuimos a un conocido restaurante y disfrutamos de un exquisito ceviche... Al momento de pagar, en efectivo, el cajero hizo el clásico gesto de alzar los billetes, ponerlos a contraluz y estirarlos casi hasta romperlos con el fin de comprobar su autenticidad. En respuesta a este ritual, uno de mis socios le dijo al cajero que quería ver el pescado con el que había sido preparado el ceviche; que quería conocer si era un producto nacional o extranjero; si había sido

pescado o criado en granja; en qué condiciones había sido almacenado y transportado, y cuál era la ruta que había seguido hasta llegar a nuestros platos… El cajero se quedó perplejo, fue a llamar al jefe de los meseros quien se acercó a nosotros muy amablemente y nos preguntó si había algún problema con la comida o con el servicio.

"Mi socio le hizo las mismas preguntas; el mesero nos dijo que era corvina fresca del día que había sido comprada al proveedor habitual. Mi socio le dijo: muy bien, tú nos estás diciendo que es así, pero quiero que me lo demuestres con pruebas, con evidencias, con documentos; porque si

el ceviche que he comido hoy me causa graves problemas estomacales no tengo a quién reclamar, no tengo a quién responsabilizar por los perjuicios ocasionados"…

¿Cuál fue la moraleja que esta historia nos dejó?

"Nos dimos cuenta de que existe un gran vacío de confianza a lo largo de la cadena de suministro; los consumidores estamos a merced de las buenas y malas decisiones que toman quienes producen, fabrican y nos venden los diferentes productos. La poca información a la que tenemos acceso no es transparente y desconocemos casi por completo los procesos involucrados en la fabricación

de los alimentos que nos llevamos a la boca".

Todo, absolutamente todo, se basa en la confianza que puede ser lesionada fácilmente ante la carencia de herramientas que permitan certificar su veracidad.

¿Conocemos el origen y los ingredientes de los alimentos que consumimos?

"¿Puedo estar seguro de que una lata de atún viene de Ecuador y que su pesca no proviene de áreas protegidas? ¿Cómo puedo saber si el pollo que estoy comiendo ha cumplido con las normativas sanitarias y de bienestar animal a lo largo de su crianza y

faenamiento? ¿Tengo la certeza de que los tomates que he comprado son orgánicos, tal y como dice en su etiqueta?"

Todos los alimentos que llevas a tu boca pasan por muchas manos antes de llegar a tu hogar. El gran problema, como dijimos antes, es que los procesos de las cadenas de producción y suministro resultan muy poco transparentes. Es realmente complicado conocer a ciencia cierta la procedencia de los alimentos que consumimos, así como saber cuáles son los ingredientes de los que están hechos y el impacto social y ambiental que causa su cultivo, transformación y transporte.

Falsificación y adulteración de alimentos

Se calcula que el fraude o la falsificación en la industria alimenticia representa 49 mil millones de dólares al año, de acuerdo a Food Safety Magazine. Lo mismo ocurre en otras importantes industrias: farmacéutica, cosmética, tecnológica, educativa, bienes raíces y automovilística. Las actividades de falsificación y la piratería que afectan a estos ámbitos es un negocio calculado en más de 500 mil millones de dólares al año.

"La globalización de los mercados ha hecho que las cadenas de suministro sean cada vez más largas. Y

mientras más largas, más complicado es controlarlas y asegurarlas, y hay más posibilidades de que se cometan errores de buena fe y también engaños y fraudes".

Existe toda una red internacional de falsificación de alimentos y otros productos en la que están involucradas mafias del narcotráfico y del lavado de activos que operan en muchos países del mundo y tienen cómplices en puertos, aduanas, empresas de transporte y puntos de distribución.

Para muestra un botón:

- El 20% del vino que se venden en el mundo es falsificado.
- Entre el 60 y el 90% del aceite

de oliva está adulterado con otros aceites.

- Pasta y arroz hechos de plástico y parafina.
- Cerveza mezclada con agua y jabón.
- Miel de abeja mezclada con azúcar.
- Leche mezclada con leche en polvo adulterada.
- Jugos de fruta de que no contienen fruta.
- Carne en estado de putrefacción que es "maquillada" con químicos cancerígenos para que parezca fresca.

Christiaan Sluijs, CFO de T-

mining, comenta que más de 30 diferentes actores –participantes de la cadena de suministro– tocan un contenedor, y sólo esperan que cada cual comunique la información que le corresponde. Añade también que muchas grandes corporaciones y organismos oficiales aún utilizan papel para registrar la información importante y sensible, como certificados de origen, facturas, pólizas de seguros y conocimientos de embarque. Este proceso resulta anacrónico teniendo en cuenta que se pueden utilizar medios digitales para transmitir ese tipo de información. IBM estima que todo ese papeleo representa el 20% de los costos totales del transporte.

¿Qué es la trazabilidad?

"La trazabilidad es una serie de procedimientos que permiten conocer el origen, la historia, la ubicación y la trayectoria de un producto a lo largo de la cadena de suministro a través del uso de ciertas herramientas tecnológicas".

La buena noticia es que la tecnología ya hace posible trazar o rastrear con exactitud la procedencia de los alimentos, conocer su lugar y fecha de producción y muchos otros datos más, como por ejemplo:

- Si son productos genéticamente modificados.
- Si son convencionales u

orgánicos.

- Cuáles son los ingredientes con que están elaborados.
- Cuál es el proceso de su fabricación.
- Cuánta agua se utilizó para su procesamiento.
- Si los animales han sido tratados conforme a las normativas de bienestar animal.
- Quién los transportó desde la fábrica hasta el supermercado.

Tecnología que permite la trazabilidad

La trazabilidad se ha ido perfeccionando gracias a la aplicación de tecnologías como las redes de comunicación, dispositivos móviles, software y

hardware, Sistema de Posicionamiento Global (GPS), sensores y oráculos, drones, Internet de las Cosas (IoT), Inteligencia Artificial (IA), códigos de respuesta rápida (QR) y de identificación por radiofrecuencia (RFID) y blockchain.

"Actualmente la trazabilidad se realiza con medios informáticos convencionales; es decir, gestionados centralizadamente, cerradamente, que carecen de la apertura y la transparencia de la cadena de bloques; Blockchain representa un factor disruptivo tanto en la trazabilidad como en muchos otros ámbitos.

"La cadena de bloques ayuda a

resolver este problema dotando a los datos de una dimensión de confianza *per se*. La información que se encuentra registrada en una cadena de bloques no puede ser borrada, modificada o censurada, por tanto, no se requiere de intermediarios que la certifiquen como auténtica.

Es un hecho que en el corto plazo las regulaciones tanto europeas como estadounidenses exigirán la implementación de sistemas inmutables de trazabilidad a quienes pretendan exportar sus productos a dichas regiones". Quienes no las tengan, simplemente no podrán vender sus productos ante el incumplimiento de las

normas de seguridad e inocuidad alimentaria establecidas.

Los productores y fabricantes de alimentos que son honestos no tienen nada que temer, al registrar sus procesos productivos en una cadena de bloques están dotando de legitimidad y confianza a su trabajo. Gracias a la cadena de bloques tenemos acceso a información que nos permitirá decidir qué alimentos consumimos en función de nuestros gustos y de nuestros valores o principios éticos. Por otro lado, los actores de la cadena de suministro se ven obligados a transparentar sus procesos y a ser honestos frente a las autoridades y al consumidor.

¿Te preocupa conocer con exactitud qué se están llevando a la boca tú y tu familia todos los días teniendo en cuenta que su salud y bienestar podrían estar en riesgo? A nosotros sí.

La cadena de bloques combate la corrupción

> El colapso de la moralidad y el incremento de la corrupción en la política no son casuales. Obedecen a la decadencia del modelo del Estado-nación».
>
> JAMES DALE DAVIDSON Y WILLIAM REES-MOGG

La corrupción es una enfermedad endémica de los sistemas de poder que devora los recursos públicos. Siempre se la ha considerado como un tema

político que se combate con más política, más leyes y más Estado; más de lo mismo, paradójicamente. Somos testigos frecuentes de campañas estatales en los medios de comunicación cuyo objetivo es crear conciencia en la burocracia y en la opinión pública; sin embargo, en términos reales no surten efecto alguno. En pocas ocasiones nos hemos detenido a investigar sus orígenes con el fin de entender sus efectos y combatirlos.

La gran falla de un sistema centralizado –como las instituciones estatales– es que a medida que crece se vuelve más corrupto. El poder en la pirámide se concentra en su ápice,

mientras más alta es la pirámide, la concentración de poder es más grande y también lo es la corrupción. ¿Qué clase de personas son las que buscan estas posiciones de poder? Los megalómanos, los narcisistas, los psicópatas, quienes bajo un disfraz de liderazgo eficiente construyen enormes redes de corrupción y abuso de poder.

¿Por qué nunca hemos podido combatir la corrupción eficazmente?

Usualmente pensamos que las instituciones, el sistema, la democracia y la ley no funcionan porque somos demasiado corruptos, cuando lo que ocurre es todo lo contrario. En nuestros países latinoamericanos, el Estado de

Derecho, que es el responsable del funcionamiento del sistema institucional, no existe o es incipiente, y la corrupción surge como una alternativa –obligatoria en muchas circunstancias– para que la gente pueda desarrollar sus actividades económicas.

Enrique Ghersi, académico de la Universidad de Lima, piensa que no hemos entendido la esencia de la corrupción, generalmente la consideramos como una causa cuando en realidad es un efecto. Es un efecto del alto costo de la legalidad; es decir, del hecho de creer que las leyes son gratuitas y neutrales. La ley tiene costos y beneficios, altera la forma en que las

personas se comportan. El costo de la ley no necesariamente se mide en términos de dinero, sino también de tiempo. ¿Cuánto tiempo toma realizar un trámite en alguna institución estatal? ¿Cuánto tiempo y dinero cuesta cumplir con una determinada ley? Cuando los legisladores elaboran una ley están comunicando implícitamente a los ciudadanos que se requiere de una cierta cantidad de tiempo, información y recursos económicos para obedecerla. Cuando una ley es demasiado costosa en los términos mencionados anteriormente, los ciudadanos eligen no acatarla y actuar en la ilegalidad. Por otro lado, si eligen respetarla porque no hay otra alternativa, la burocracia –que tiene el

poder de hacer cumplir la ley– es consciente del costo que esto significa y por tanto los funcionarios gozan de la atribución y la libertad de fijar "tarifas" para ayudar a obedecerla oportunamente.

La ley es más cara para los de poncho

Teniendo en cuenta que el cumplimiento de la ley está relacionado con costos de tiempo, información y dinero, resulta lógico afirmar que su cumplimiento es más costoso para los pobres que para los ricos. ¿Por qué? Porque los ricos tienen que utilizar menos de sus ingresos para cumplir con la ley; los pobres, en contraste, tienen que sacrificar más tiempo, dinero e información. Esto

quiere decir que la ley tiene efectos asimétricos, no existe la pregonada "igualdad ante la ley". Acertadamente, Enrique Ghersi señala que "sólo se cumplen las leyes cuyos beneficios son mayores que sus costos".

Existen dos puntos de vista en cuanto a la naturaleza de la corrupción. Unos dicen que es un impuesto ilegal o informal que se debe pagar para poder cumplir con la ley y salvarse del castigo producto de su inobservancia. Otros afirman que la corrupción actúa como una póliza de seguro cuya prima se paga en forma de coimas o sobornos a los funcionarios públicos, quienes actúan como agentes intermediarios brindando

protección frente a una ley costosa de acatar.

La cadena de bloques combate la corrupción

Los datos almacenados en una cadena de bloques no pueden ser borrados, modificados o falsificados. Ofrece un nivel sin precedentes de integridad, seguridad y fiabilidad a la información que administra. También permite el rastreo y auditoría en tiempo real de las transacciones. Estos atributos representan muy malas noticias para la corrupción.

En el sector público, los registros de todo tipo de transacciones y operaciones se encuentran almacenados

centralizadamente en cada una de las instituciones que se financian con el presupuesto estatal, quedando fuera del alcance del escrutinio de los ciudadanos y, en muchas ocasiones, de la Procuraduría y la Contraloría, instituciones fiscales llamadas a realizar auditorías del gasto público e investigaciones en caso de que se sospeche que se han cometido delitos de malversación de fondos públicos. Cualquier acción que pueden llevar a cabo estos organismos es *ex post* (después del hecho). Aplicada al control del gasto público, la cadena de bloques permitiría prevenir los actos de corrupción *ex ante* (antes de que ocurran).

La OCDE estima que la corrupción agrega hasta el 10% del costo total de hacer negocios a nivel mundial y hasta el 25% de los costos de los contratos en los países en desarrollo.

Aplicaciones de la cadena de bloques para combatir la corrupción

¿Qué pasaría si los organismos estatales de control y la ciudadanía en general tuvieran acceso en tiempo real a los registros públicos? Si los organismos de control y demás instituciones, tanto públicas como privadas, encargadas de velar por el correcto uso de los fondos públicos tuvieran a su disposición la tecnología de la cadena de bloques, sería posible identificar de primera

mano las irregularidades en las transacciones y realizar oportunamente las investigaciones pertinentes. De esta manera sería mucho más complicado que se utilicen los fondos públicos de manera irresponsable e indebida.

A continuación mencionaremos algunas aplicaciones de la cadena de bloques que permitirían mejorar y transparentar la gestión pública con el fin de reducir la corrupción:

- Registros públicos distribuidos (propiedad, mercantil, identidad, crédito, etc.).
- Elecciones de autoridades a través de mecanismos distribuidos y verificables

públicamente en tiempo real.

- Contratación pública distribuida y auditable en tiempo real.

El potencial de la cadena de bloques es inmenso. Si bien esta tecnología aún se encuentra en fase de desarrollo, promete contribuir de manera significativa con la tarea de combatir la corrupción, que es una de las grandes plagas que azota a la humanidad. Los países que gozan de mayores problemas institucionales son los primeros candidatos para corregir sus sistemas malogrados gracias a la implementación de esta tecnología.

Tres plataformas blockchain de almacenamiento distribuido de datos

Los medios digitales están sesgados hacia la replicación y el almacenamiento. Nuestras fotos digitales prácticamente se cargan y publican solas en Facebook, y nuestros correos electrónicos eliminados tienden a resurgir cuando menos lo esperamos. Sí, todo lo que haces en el reino digital también puede ser transmitido en la televisión en horario estelar y cincelado en el costado del Partenón.

DOUGLAS RUSHKOFF

Los datos se han convertido en el activo más valioso en la era de la información, muchas de las grandes compañías tecnológicas han construido sus exitosos modelos de negocios precisamente a

partir del análisis de la inconmensurable cantidad de datos que generan sus usuarios, poniendo en riesgo constante su seguridad y privacidad. No hace falta comentar los frecuentes casos de ataques y filtraciones de información de que son víctimas los sistemas centralizados. En este sentido, el ámbito de la gestión y almacenamiento de datos no ha podido permanecer ajeno al fenómeno de la cadena de bloques, el cual ofrece interesantes características de seguridad, integridad y privacidad.

El almacenamiento distribuido de datos no es un concepto nuevo. A partir de mediados de la década de 1990 e inicios de la de 2000, vimos el

surgimiento de plataformas descentralizadas de descargas de archivos digitales como BitTorrent y LimeWire. En lugar de que los usuarios descarguen la información de servidores centralizados, estas plataformas entre iguales (P2P, por sus siglas en inglés), permiten que un archivo sea alojado o #sembrado" en una sola computadora para luego ser dividido en fragmentos, y estos luego distribuirse a través de una red de ordenadores.

Esto permite que cada nodo de la red descargue de sus compañeros fragmentos del archivo, mientras que al mismo tiempo carga otros fragmentos del archivo a otros pares. Como nada es

perfecto, este modelo tiene algunas limitaciones, como por ejemplo:

- En el caso de que un nodo termine de descargar un archivo antes que los otros nodos, el propietario del primer nodo podría apagarlo al finalizar la descarga, haciendo que otros usuarios de la red nunca reciban una copia completa del archivo.
- No existen incentivos para sembrar archivos menos populares, haciendo que la descarga sea menos confiable y lenta. Teniendo en cuenta que la siembra ocupa ancho de banda, tampoco hay incentivos para

continuar alojando dichos archivos.

La solución es incentivar a los nodos para que alojen datos sin importar si estos son más o menos populares.

Como es de conocimiento generalizado, la escalabilidad no deja de ser una preocupación en el mundo de las cadenas de bloques. Actualmente se están empleando dos técnicas específicas para enfrentar este importante desafío:

- Fragmentación o sharding: es una técnica para dividir lógicamente los datos en una base de datos. Estos datos se dividen en fragmentos que

forman la base de datos original cuando se reconstruyen.

- Enjambre o swarming: es un proceso que almacena colectivamente fragmentos en un gran grupo de nodos –un enjambre– dentro de una red entre iguales. Los dispositivos conectados a esta red pueden recuperar los datos de los nodos más cercanos, lo que reduce la latencia y aumenta la confiabilidad y la escalabilidad.

La gestión descentralizada de datos garantiza que si un nodo falla y se desconecta de la red, los nodos restantes aún tienen la capacidad de restituir los

archivos de los fragmentos distribuidos por toda la red. Para aumentar la seguridad los archivos se encuentran cifrados, evitando que los nodos puedan conocer lo que contienen. Para recuperar un archivo se utiliza una tabla de hashes distribuida, una lista con las claves y los valores asociados que apuntan hacia la ubicación de cada uno de los fragmentos de los datos. La red emplea estos fragmentos para reconstruir el archivo antes de que su propietario use su clave privada para decodificarlo y usarlo.

Ventajas de blockchain para el almacenamiento de archivos

1. Es más difícil de intervenir un

servicio centralizado en la nube (AWS, Dropbox, Google Drive, OneDrive…) porque posee un punto único de falla y ataque. La naturaleza descentralizada del almacenamiento, junto con procesos como la fragmentación y la codificación, significa que los hackers que logren comprometer un nodo sólo podrán acceder a una pequeña porción cifrada de sus datos. Luego tendrían que ubicar y descifrar todos los demás fragmentos en los otros nodos para poder darles algún sentido.

2. El almacenamiento de archivos

descentralizado es más económico que las soluciones de almacenamiento centralizado en la nube o el mantenimiento de servidores in situ. Por ejemplo, en promedio, el almacenamiento descentralizado que ofrece la plataforma Sia cuesta un 90% menos que los servicios ofrecidos por los proveedores de soluciones centralizadas en la nube. Almacenar 1 TB de datos en Sia cuesta alrededor de dos dólares por mes, en contraste con los veintitrés dólares que cuesta el servicio S3 de Amazon Web Services.

3. El sistema de incentivos significa que si una persona tiene espacio de almacenamiento adicional, puede aportarlo a la red y ganar dinero a cambio. Es de esperar que si estos servicios descentralizados de almacenamiento llegan a sumar una cantidad interesante de usuarios, el valor del token debería apreciarse considerablemente.

A continuación vamos a analizar tres proyectos blockchain de almacenamiento distribuido de datos que podrían convertirse en el punto de quiebre del modelo centralizado que

actualmente acapara el mercado, dando origen a un nuevo modelo descentralizado basado en los incentivos económicos; dicho de otro modo, los participantes son recompensados con tokens o criptoactivos por la capacidad de almacenamiento que aportan a la red. Estos retornos monetarios harían que los participantes permanezcan conectados a la red y no apaguen sus nodos.

Storj

Esta plataforma se lanzó en 2014 y fue inicialmente un token desarrollado en la plataforma Counterparty construida en Bitcoin. Posteriormente, en el verano de 2017, migró a Ethereum y se convirtió en un token ERC20. Al mismo tiempo,

se completó exitosamente una nueva ICO que recaudó 30 millones de dólares.

El objetivo fundamental de Storj es ofrecer una alternativa al modelo tradicional y centralizado de almacenamiento de datos a través del empleo de su token nativo para incentivar a los usuarios –conocidos como granjeros– a alojar datos en la capacidad de almacenamiento ociosa de sus dispositivos. Los archivos de los usuarios de la plataforma se codifican, fragmentan y se envían a través de la red a los granjeros para su almacenamiento. Este proceso ocurre a través de la ejecución de contratos inteligentes de almacenamiento P2P que establecen los

términos y condiciones del servicio entre pares.

Storj emplea tablas de hashes distribuidas (DHT, por sus siglas en inglés). A través de esta tecnología los nodos de la red pueden transferir datos, verificar su integridad y disponibilidad y pagar a los nodos que contribuyen con su capacidad de almacenamiento a la red. Existe una herramienta llamada Storj Share que permite a los usuarios convertirse en granjeros, alquilar su capacidad de almacenamiento a la red. Como recompensa los granjeros reciben la criptomoneda STORJ.

Actualmente, tanto los nuevos usuarios como los nuevos granjeros se

encuentran en una lista de espera. Esta situación se debe principalmente a las limitaciones de escalabilidad que han surgido desde que la red alcanzó los 100 millones de GB de datos almacenados. A pesar de que esta capacidad de almacenamiento es considerable para el mundo de las cadenas de bloques, continúa siendo despreciable si la comparamos con las cifras de servicios centralizados como AWS. El equipo de desarrollo de Storj tiene como objetivo alcanzar una capacidad de 1 EB –10^18 bytes–, para esto está trabajando en la actualización denominada V3, que permitirá la transmisión de vídeos en búfer e integración con AWS. En febrero de 2019 se lanzó la version alfa

del explorador V3 de Storj.

Es importante mencionar que Storj no opera su propia cadena de bloques, sino que funciona como una aplicación descentralizada (DApp, por sus siglas en inglés) de Ethereum. Storj es el proyecto blockchain de almacenamiento más antiguo y más utilizado en términos de cantidad de datos almacenados.

Sia

Por el momento, Sia es la opción de almacenamiento descentralizado preferida por el mercado. Su funcionamiento es muy similar al de Storj con la diferencia de que Sia opera su propia cadena de bloques; esto no

sólo permite que el proceso de almacenamiento de datos se descentralice, sino que también la ejecución de contratos inteligentes entre usuarios y granjeros permiten, entre otras cosas, acordar la capacidad de almacenamiento y el valor a pagar en siacoins (SC) –criptodivisa nativa de la blockchain de Sia que interviene en los contratos de almacenamiento descentralizado–. Los tokens del usuario representan el pago a los granjeros una vez que se cumple el contrato; los tokens del granjero actúan como colateral en el caso de que éste no provea el alojamiento según lo acordado en el contrato. Esta garantía se puede perder si los granjeros se desconectan de la

red.

La cadena de bloques se emplea para almacenar el contrato y hacerlo público y auditable en tiempo real. También actúa como un servicio de depósito en garantía para ambas partes. Al finalizar el contrato, el granjero proporciona una prueba a la cadena de bloques de que el archivo se encuentra almacenado, luego la garantía es devuelta y el pago del usuario se transfiere al granjero. Tanto los usuarios como los granjeros utilizan siacoins para comprar y vender espacio de almacenamiento, por lo tanto tiene un precio flotante determinado por un mercado. Este criptoactivo también se

utiliza para pagar a los mineros que efectúan la Prueba de Trabajo (PoW, por sus siglas en inglés), mecanismo empleado para validar los bloques de la cadena.

En 2018 se lanzó la plataforma Goobox, que es un servicio descentralizado de transferencia de archivos que opera en la cadena de bloques de Sia. Permite cargar y transferir sin costo archivos de hasta 4 GB protegidos con contraseña y codificación punto a punto.

Goobox es la alternativa descentralizada basada en blockchain del popular servicio WeTransfer. En la primavera de 2019 se lanzó la versión

Pro de la plataforma, y en Verano del mismo año, se liberó la API que permite implementaciones e integraciones fáciles y económicas de en Sia.

Actualmente hay muchos usuarios que están interesados en intercambiar la criptomoneda siacoin, pero no tantos interesados en utilizar el servicio de almacenamiento. El incremento sostenido de su base de usuarios es el desafío más importante que debe superar esta plataforma. El crecimiento de usuarios está limitado por un par de situaciones clave. Primero, el software no es fácil de usar, requiere de algunas horas de configuración. Segundo, los nodos que

forman parte de la red sólo pueden almacenar hasta 5 TB de datos, lo que excluye del servicio a usuarios corporativos, por ejemplo.

Filecoin

En 2017, el ICO de Filecoin se convirtió en uno de los que más fondos ha recibido con 257 millones de dólares, manteniéndose fácilmente entre los diez primeros de mayor recaudación hasta el momento de escribir este libro. Filecoin es desarrollado por Protocol Labs, se basa en el Sistema de Archivos Interplanetario (IPFS, por sus siglas en inglés) que es un protocolo de código abierto y una red diseñada para crear un método de almacenamiento y uso

compartido de hipermedia en un sistema de archivos distribuido P2P. IPFS pretende transformar la manera en que los datos se transmiten en Internet. Tiene la asombrosa y fabulosa ambición de reemplazar al anacrónico protocolo HTTP. Esta tecnología ya ha sido adoptada por servicios de generación y distribución de contenido como Busy y DTube.

Además de IPFS, Filecoin agrega su token para crear un mercado que incentiva a los granjeros a almacenar archivos para los usuarios. Los mineros ganan la criptomoneda filecoin (FIL) al proporcionar espacio de almacenamiento ocioso a la red; los

usuarios gastan filecoin al pagar por el almacenamiento de sus archivos en la red descentralizada.

La red de Filecoin está compuesta por dos tipos de nodos:

1. Nodos de almacenamiento: similares a los granjeros de Storj que pueden alquilar sus discos duros para alojar datos.
2. Nodos de recuperación: localizan y recuperan los archivos de los usuarios. Estos nodos reciben una recompensa en filecoin en función de la rapidez con la que encuentran los archivos.

Al igual que Sia, pero a

diferencia de Storj, Filecoin operará en su propia cadena de bloques, lo que significa que procesos como la negociación de contratos y los pagos también pueden descentralizarse. Una capa será para el almacenamiento de archivos distribuidos mediante IPFS, y otra capa independiente mantendrá los contratos. En lugar de PoW, Filecoin emplea un nuevo algoritmo de consenso llamado Prueba de Almacenamiento (Proof of Storage) que implica dos componentes separados:

- Prueba de Replicación (PoRep): permite que el anfitrión (host) demuestre a los usuarios que sus datos se han replicado en un

almacenamiento físico determinado.

- Prueba de Espacio y Tiempo (PoST): proporciona una verificación de marca o sello de tiempo que indica de forma fehaciente que el anfitrión está alojando los datos.

Filecoin aún se encuentra en etapa de desarrollo, por lo pronto no existen actualizaciones más que una demo. Existe una creciente preocupación por parte de los inversionistas porque no conocen una fecha exacta de lanzamiento de la plataforma. Sin embargo, el proyecto ha recibido el respaldo de grandes nombres del capital

de riesgo, incluyendo Andreessen Horowitz y Winklevoss Capital. Esto haría que Filecoin se convierta, sin duda alguna, en un importante jugador del ecosistema del almacenamiento descentralizado de datos.

Legislación

La incertidumbre regulatoria está haciendo daño a la innovación de blockchain

¿Cómo desarrollamos un marco de referencia en el que nuestra economía, nuestro gobierno y nuestra gente puedan aprovechar esta tecnología [blockchain] de muchas maneras?

TOM JESSOP

Existe una constante y creciente preocupación por parte de los diversos actores que forman parte del ecosistema de la cadena de bloques, quienes

consideran que la incertidumbre regulatoria que se da a nivel global podría estar afectando el desarrollo de esta tecnología. Sin lugar a dudas, es necesario que existan marcos normativos que permitan el establecimiento de reglas de juego claras entre los participantes. Sin embargo, no podemos dejar de reconocer que las decisiones que toman las autoridades en su afán casi compulsivo de regular absolutamente todas las actividades que realizamos, afectan negativamente a la innovación debido a la promulgación prematura y sin criterio de regulaciones que, en los casos más extremos, pueden terminar por completo con una industria.

En este contexto, la pregunta que cabe hacerse es si los gobiernos deberían intervenir para ayudar a fomentar la tecnología blockchain. Unos piensan que sí. Por ejemplo, la Cámara de Comercio Digital de Estados Unidos ha publicado un llamado a la acción pidiendo a los responsables de la formulación de políticas federales que aborden y resuelvan el problema de la "falta de un entorno legal predecible" que está obstaculizando la experimentación e innovación de la cadena de bloques.

La situación en Latinoamérica

Asimismo, en los diferentes países de Latinoamérica han surgido movimientos

civiles que piden espacios para proponer leyes fintech que tomen en cuenta a blockchain y las criptomonedas. Los casos de México, Argentina y Venezuela son los más alentadores; estos tres países ya poseen cuerpos legales que regulan, desde diferentes perspectivas, las actividades del criptomundo.

En países como Paraguay, Uruguay, Costa Rica, Panamá, Guatemala y Nicaragua sus gobiernos han decidido abordar el tema con neutralidad; es decir, por lo pronto no han intervenido abiertamente en la regulación del ecosistema dejando que sus participantes actúen con relativa

libertad.

En Chile, Colombia y Brasil se han observado posiciones ambiguas; por un lado, los gobiernos hablan de apoyar el desarrollo de la tecnología de la cadena de bloques, pero por otro han ocurrido cierres de cuentas bancarias pertenecientes a plataformas de intercambio, y los bancos centrales han hecho declaraciones mencionando que las criptomonedas no pueden ser consideradas como monedas de curso legal.

El caso de Ecuador es muy particular teniendo en cuenta que este país no posee una política monetaria propia debido a que su economía se

encuentra dolarizada desde el año 2000. La Junta de la Política de Regulación Monetaria y Financiera no ha emitido disposición alguna que reconozca al bitcoin o a cualquier otra criptomoneda. De acuerdo al artículo 98, inciso 3, del Código Orgánico Monetario y Financiero, se prohíbe la circulación de especies monetarias sin el aval de la Junta. En términos sencillos, cualquier tipo de moneda diferente al dólar estadounidense no es admitida en Ecuador como instrumento para la compra y venta de bienes y servicios, salvo que goce de autorización por parte de la Junta, según el artículo 99 del mismo código. Lo que esta normativa no prevé es la prohibición explícita de

adquirir e intercambiar criptomonedas como instrumentos de inversión.

El gobierno boliviano prohibió el uso de bitcoin el 6 de mayo de 2014, convirtiéndose en la primera y única nación de la región en declarar frontalmente la ilegalidad de los criptoactivos.

La áspera relación con los Estados-nación

Era totalmente previsible que la relación entre el criptomundo y los Estados iba a ser incómoda, teniendo en cuenta que blockchain permite a los usuarios realizar transacciones persona a persona –eliminando la participación de intermediarios– fuera del sistema

financiero tradicional que se encuentra exageradamente intervenido y regulado por los Estados-nación.

En el transcurso de los años posteriores al surgimiento de bitcoin, los reguladores prestaron muy poca atención al mercado de los criptoactivos porque era muy pequeño y únicamente participaban los usuarios motivados por cuestiones técnicas. Esta situación empezó a cambiar a partir de 2017, cuando diferentes organizaciones empezaron a recaudar cientos o miles de millones de dólares mediante la venta de tokens basados en blockchain a través de las ICO. Invertir en todo tipo de iniciativas relacionadas con la cadena

de bloques y las criptomonedas se convirtió en una atractiva actividad relativamente generalizada, llamando la atención de los reguladores que buscaban proteger a los inversionistas de fraudes y estafas, que por cierto sí que ocurrieron.

En respuesta al frenesí que causaron las ICO, motivado por la agresiva revalorización del bitcoin y otros criptoactivos, la estadounidense SEC (Securities and Exchange Commission) empezó a citar y penalizar a varios proyectos ICO que no contaban con la licencia necesaria para vender valores. Esta situación hizo que muchas empresas del criptomundo se

trasladasen a otras jurisdicciones más amigables y que los ciudadanos estadounidenses quedaran al margen de estas iniciativas.

La incertidumbre regulatoria

En su declaración, la Cámara de Comercio Digital argumenta que las empresas y los consumidores se encuentran reacios a desarrollar y usar aplicaciones blockchain ante la incertidumbre que genera la eventual violación de leyes financieras obsoletas que ya han castigado a algunos con multas y prisión.

La posición que tanto reguladores como entusiastas y promotores de la tecnología blockchain

deberían asumir es la de cooperación y tolerancia. Los reguladores son esencialmente lentos, esto hace que sea prácticamente imposible que vayan al compás del vertiginoso desarrollo tecnológico. Si los participantes de esta nueva y pujante industria quieren que los procesos regulatorios ocurran a mayor velocidad, deberían estar en constante contacto y conversación con las autoridades. Esta estrategia puede rendir frutos muy positivos teniendo en cuenta que la llegada de regulaciones es inevitable, es fundamental que los interesados intervengan en su formulación en lugar de permanecer como meros observadores y dejarlas solamente en manos de la burocracia

que carece de criterio y de suficientes conocimientos en el ámbito como para tomar decisiones adecuadas que beneficien el desarrollo e innovación en este campo.

A pesar de la incertidumbre regulatoria, muchas empresas tecnológicas y financieras están invirtiendo activamente en el criptomundo; al mismo tiempo, hay muchas otras empresas que han preferido mantenerse al margen, precisamente por la desconfianza que genera la falta de regulaciones claras al respecto. La participación masiva de empresas de diferentes sectores ayudaría a que la industria blockchain

madure y se consolide.

Es indiscutible que las regulaciones son necesarias para una convivencia adecuada y sin contratiempos, no obstante, quienes pretendan que los Estados-nación asuman el rol de fomentar el desarrollo y la innovación vía decreto –en este caso de la cadena de bloques y las tecnologías relacionadas– estarían cometiendo un grave error porque existe la real posibilidad de que la intervención estatal produzca más daños que beneficios.

El futuro de la cadena de bloques

La lucha entre la sociedad industrial y la digital

En el mundo en que vivimos la libertad es una ilusión: nuestros cuerpos pertenecen a los gobiernos y nuestras mentes a las grandes corporaciones tecnológicas.

TIM REUTEMANN

Existen dos dominios políticos en este siglo XXI que poseen un inconmensurable poder; por un lado *la tierra*, que representa el modelo social y

económico actual basado en la supremacía de los Estados-nación y la revolución industrial surgida en el siglo XIX, donde los políticos monopolizan la violencia en jurisdicciones territoriales; por otro lado *la nube*, que representa a la revolución de la información que dio lugar a la aparición de las grandes corporaciones tecnológicas que monopolizan los datos de los usuarios con fines de mercadeo y publicidad.

Para algunos autores, incluyendo a James Dale Davidson y William Rees-Mog, quienes en 1997 publicaron el libro *The sovereign individual: mastering the transition to the Information Age*, la revolución de la

información está liberando a los individuos del anacrónico modelo del Estado-nación del siglo XX. Ellos afirman que la computación destruirá al Estado-nación, creando nuevas formas de organización en el proceso.

Con el fin de prepararnos para vivir en el mundo que está viniendo, debemos entender por qué será diferente de lo que la mayoría de los expertos dicen. Esto involucra ver más de cerca las causas del cambio que no son tan evidentes. Las causas más importantes del cambio no son propiciadas por manifiestos políticos o pronunciamientos de economistas muertos, sino por factores ocultos que

alteran las fronteras donde se ejerce el poder. Usualmente, modificaciones sutiles en el clima, la topografía, los microbios y la tecnología, alteran la lógica de la violencia. Aquellas transforman la manera en que la gente se organiza y defiende.

Pensadores convencionales observan que una de las premisas de un Estado-nación democrático es que los puntos de vista o los deseos de las personas determinan la manera en que el mundo cambia. Estos analistas explican, pronostican e interpretan los mayores desarrollos históricos como si fuesen exclusivamente un efecto de los deseos de las personas. Bajo esta misma óptica

muchos científicos sociales han vaticinado el final del Estado-nación para dar lugar a un gobierno global. Desde el punto de vista de un pensamiento más heterodoxo esta suposición es absurda, porque es una falacia el argumento de que una nueva forma de gobernanza surgirá porque otra ha fallado; si fuese así, nuestros países latinoamericanos, por citar un ejemplo, hace mucho tiempo tendrían mejores gobiernos simplemente porque los anteriores han venido fallando consistentemente. Dicho esto, cuando se toma en consideración a las tecnologías que están forjando el nuevo milenio, es mucho más probable que no veamos un gobierno global, en su lugar veremos

microgobiernos o incluso condiciones que se aproximan a la anarquía.

En nuestra región, quizás la batalla tierra vs. nube más notable está ocurriendo en Venezuela, donde la dictadura del chavista Nicolás Maduro está buscando y confiscando equipos de minería de criptomonedas –a pesar de que el régimen ha reconocido que la minería de criptodivisas es legal, lo que representa un claro abuso de autoridad–, mientras al mismo tiempo, se ha embarcado en la emisión del Petro, una criptomoneda emitida y controlada por el Estado venezolano, con la que esperan recaudar recursos frescos para que las arcas fiscales tengan mayor

liquidez, y así esquivar las sanciones internacionales que han hecho que se limite seriamente la posibilidad de acceder a créditos en el extranjero.

Blockchain como reducto de soberanía individual

De acuerdo a Democracy Earth, las empresas tecnológicas Google y Facebook son dueñas de las bases de datos de identidad más grandes del mundo, superando a las de los gobiernos de India y China. Teniendo en cuenta que el 97% de los ingresos de estas corporaciones provienen de la publicidad, resulta que gran parte de la población del mundo ve a través de los filtros de los embudos de venta de los

anunciantes que usan los servicios de dichas plataformas digitales. En otras palabras, esta inmensa acumulación de información ha hecho que los individuos perdamos nuestra privacidad y que estemos expuestos más que nunca al crimen organizado, al espionaje y a la coacción gubernamental.

Paradójicamente, el negocio de quienes son llamados a proteger nuestra identidad en línea depende casi exclusivamente de la cantidad de datos de sus usuarios que logren capturar y vender. Los servicios que ofrecen Facebook, Twitter y Google no son gratuitos a pesar de que así parezca. El uso de dichas plataformas no tiene costo

para los usuarios porque la información que estos generan es el producto que venden esas grandes corporaciones.

Es evidente que tanto al Estado-nación como a las grandes empresas tecnológicas no les interesa el surgimiento de la soberanía individual gracias a la aplicación de la tecnología de la cadena de bloques porque representa una grave amenaza para su supervivencia. Las redes informáticas distribuidas que operan en blockchain tienen la capacidad de mover todo tipo de activos sin la participación de un intermediario –llámese Estado, banco, notaría, registros públicos, etc.–, cuyo rol se haría irrelevante frente a esta

tecnología. El Estado-nación iría perdiendo su capacidad de cobrar impuestos y de coacción, conforme la riqueza de los individuos vaya trasladándose al ciberespacio.

La democratización de la información propiciada por el auge de Internet, y desde hace un par de años por el surgimiento de la cadena de bloques, hace posible una extensión dramática de los mercados alterando la forma en que los activos son creados, intercambiados y protegidos. Es posible que, gracias a blockchain, la era de la soberanía económica esté llegando; seremos testigos de la última forma de privatización: la desnacionalización del

individuo, tal y como se comenta en *The sovereign individual*…, "El individuo dejará de ser un activo estatal de facto para convertirse en un cliente".

La criptografía como un derecho humano

La criptografía, una de las tecnologías subyacentes de la cadena de bloques, desempeñará un papel cada vez más importante para proteger los derechos humanos de los ciudadanos digitales, en términos de su soberanía individual y económica, al liberarlos de la lucha que se lleva a cabo entre *la tierra y la nube*.

En lo que respecta a la gobernanza y a la democracia, el secreto es una propiedad fundamental de las

elecciones libres y justas: es un mecanismo que ayuda a evitar la coacción de los que están en el poder y, al mismo tiempo, evita el riesgo de que las elecciones se compren con demagogia, dádivas o dinero. La privacidad es la mejor garantía para que una mente consciente y libre pueda pensar por sí misma. Un sistema electoral distribuido basado en la cadena de bloques reduciría la probabilidad de fraude electoral casi a cero.

La tecnología nos ofrece un camino para escapar del control centralizado del que somos objeto por parte de *la tierra y la nube*,

ofreciéndonos una tercera vía: una manera de liberarnos de la tiranía de los "me gusta" y transformar nuestro voto en poder soberano y realmente representativo que nos permita crear las instituciones que necesitamos para el futuro. Hoy podemos considerar a la cadena de bloques como esa tercera vía, una herramienta adecuada para liberarnos, aunque sea parcialmente, de los poderes de *la tierra y la nube*.

Los intercambios atómicos explicados

> *¿Qué sucede cuando una red descentralizada de micropagos multidivisa se vuelve completamente automatizada e instantánea?*
>
> ANDREAS ANTONOPOULOS

De acuerdo a los entendidos, los intercambios atómicos (atomic swaps) podrían transformar radicalmente las transferencias de criptoactivos en un futuro cercano. Esta tecnología ha sido calificada como revolucionaria ya que tiene el potencial de cambiar los sistemas financieros. Estamos hablando de una nueva tecnología que permite a los usuarios hacer transacciones monetarias persona a persona (P2P), tanto dentro como fuera de la cadena de bloques sin involucrar a intermediarios.

En términos muy simples, un intercambio atómico es un contrato inteligente que permite el intercambio de una criptomoneda con otra entre dos o

más personas sin que un tercero participe en la transacción. Esto quiere decir que en el proceso no interviene un intermediario centralizado. El intercambio atómico ocurre entre dos cadenas de bloques diferentes que poseen diferentes monedas nativas, la transacción ocurre dentro o fuera de la cadena (on-chain y off-chain, respectivamente).

Algo de historia

A partir de la invención de blockchain y Bitcoin, se ha estado trabajando en el desarrollo del concepto de intercambio P2P de criptomonedas. El primer borrador del protocolo de intercambio sin confianza fue creado en 2012 por

Sergio Demián Lerner. No obstante, el protocolo no gozó de mucha popularidad en aquel momento. El escenario cambió en 2013 cuando Tier Nolan presentó la primera cuenta completa de intercambios atómicos y explicó su funcionamiento. A pesar de que el primer borrador del protocolo fue presentado por Lerner, a Nolan se le atribuye la creación de los intercambios atómicos.

El protocolo dejó de ser teoría en septiembre de 2017, cuando ocurrió el primer intercambio atómico exitoso entre Litecoin y Decred. Actualmente existe una serie de plataformas descentralizadas que permiten a sus

usuarios realizar intercambios atómicos, entre éstas se encuentran Lightning Labs, Altcoin.io, Komodo y 0x.

¿Por qué son necesarios los intercambios atómicos?

El proceso actual de intercambio de criptomonedas es frecuentemente complejo, requiere de mucho tiempo y de la participación de intermediarios, como los intercambios en línea — Digital Currency Exchanger (DCE). Se considera que esta situación es una de las barreras que impiden la adopción generalizada de las criptomonedas como medio masivo de pago. Hay más de doscientos DCE centralizados que permiten tanto a comerciantes como a

inversionistas comprar y vender criptoactivos.

A continuación vamos a enumerar ciertos problemas que surgen del uso de los DCE, los cuales se solucionarían gracias a los intercambios atómicos:

Barreras por regulaciones gubernamentales

Los DCE, al ser plataformas centralizadas, se encuentran registradas y domiciliadas en diferentes países, por tanto deben cumplir con las regulaciones establecidas en su jurisdicción de domicilio y con las de otros países en las que opera la plataforma. Cambios en las regulaciones pueden obligar a los

DCE a modificar sus políticas de uso, y en casos más extremos a trasladarse a otra jurisdicción o cerrar sus operaciones. El ejemplo más evidente ocurrió en 2017 en China, donde sucedió una situación similar a la que explicamos previamente.

Limitaciones de infraestructura

Cuando ocurre un aumento repentino en la demanda y el volumen de transacciones aumenta considerablemente, los DCE no tienen la capacidad de enfrentarlos y salir bien librados. En tales casos ocurren interrupciones del servicio, lo que ocasiona fluctuación en los precios de los criptoactivos y eventuales pérdidas a

los usuarios.

Mala gestión de los fondos y estafas

El aumento de interés en las criptomonedas ha hecho que los DCE sean el objetivo preferido de los piratas informáticos. Por un lado, casi a diario se reporta en los medios acerca de ataques y robos millonarios. Por otro, aparecen plataformas fraudulentas que captan el dinero de los usuarios y luego cierran y desaparecen misteriosamente de la noche a la mañana, quedándose con los fondos de sus clientes. De acuerdo a Reuters, en 2017 se perdieron alrededor de 1,2 billones de dólares por robo de criptodivisas.

En ciertos casos, a pesar de ser

empresas legalmente constituidas y que cumplen con las regulaciones, la mala gestión y administración ha causado graves pérdidas a los inversionistas.

Con el fin de evitar ser víctimas de estas situaciones, los usuarios pueden contar con una alternativa descentralizada mucho más segura y confiable: los intercambios atómicos.

¿Cómo funcionan los intercambios atómicos?

Los intercambios atómicos no se basan ni dependen de ninguna cadena de bloques. Como habíamos dicho, pueden ocurrir dentro o fuera de una blockchain con criptomonedas tanto similares como diferentes. Este protocolo se define

como “un proceso de intercambio de criptomonedas entre pares en el que intervienen dos o más partes sin la participación de un intermediario como un DCE”. Entonces, si no intervienen terceros en una transacción, ¿cómo los usuarios pueden realizar los intercambios? Se utilizan las claves privadas –que están bajo su control– durante el proceso de intercambio.

Para que el proceso sea seguro, ambas partes comparten un “secreto” que deben revelar en un momento dado durante la transacción. Teniendo en cuenta que sólo las partes involucradas conocen el “secreto”, un tercero no puede formar parte de la transacción.

Las partes intercambian sus criptomonedas únicamente si los "secretos" revelados coinciden. ¿Cómo se logra esto? Utilizando HTLC (Hashed Timelock Contracts). Esta propiedad permite la creación de canales de pago fuera de la cadena de bloques –como Lightning Network, por ejemplo– y que los participantes puedan realizar transacciones fuera de la cadena utilizando el canal de pago.

Los HTLC son un tipo de contratos inteligentes que se usan básicamente para eliminar el riesgo de contraparte. Esto permite transacciones con límite de tiempo entre las dos partes, por lo tanto los intercambios

atómicos poseen límite de tiempo. El receptor de la transacción debe proporcionar una prueba criptográfica –el concepto del "secreto" del que hemos hablado anteriormente– para reconocerla dentro de un marco de tiempo establecido, de lo contrario la transacción deja de ser válida.

¿Cómo funcionan los HTLC?

Los HTLC son un tipo de transacciones especiales que utilizan las cadenas de bloques que permiten el uso de varias firmas –claves privadas– que se utilizan para validar las transacciones. Los HTLC se diferencian de las transacciones regulares porque utilizan una propiedad llamada hashlock.

Cuando el emisor de la transacción establece el "secreto" criptográfico, el hashlock es una versión codificada de este mismo "secreto" que es utilizado por el receptor de la transacción para decodificar el hash y así demostrar que efectivamente es el destinatario de la transacción.

Los HTLC además de utilizar hashlock, emplean timelock, dos tipos diferentes para ser más específicos:

CheckLockTimeVerify (CLTV): Es una restricción de tiempo que se emplea para bloquear y liberar las criptomonedas en un intercambio atómico. Esta propiedad permite que las criptomonedas se liberen en un momento

específico durante la transacción, de no ser así, el canal se cierra al haber transcurrido un tiempo específico. Los participantes tienen la atribución de decidir el lapso de cierre de la transacción; por ejemplo, luego de tres horas.

CheckSequenceVerify (CSV): Este atributo no depende del tiempo sino de la cantidad de bloques generados para realizar un seguimiento y decidir en qué momento se liberan las criptomonedas, o bien, finalizar la transacción. Por ejemplo, las partes pueden decidir cerrar la transacción después de que se hayan realizado transacciones por un monto total de 0,5

BTC.

En general, HTLC permite el funcionamiento de un sistema de transacciones de firma múltiple que garantiza que ambas partes sean responsables de la transacción y que ésta sea segura.

¿Cómo se genera un hashlock?

Un hashlock se genera siguiendo estos sencillos pasos:

1. Se elige un número aleatorio bastante grande llamado “preimagen”. Para el emisor de la transacción éste es el “secreto”. Luego, se cifra o “hashea” esta preimagen para obtener otro número.

2. A continuación se crea un contrato inteligente que es enviado al receptor de la transacción. Este contrato está bloqueado con el hash creado a partir de la preimagen.
3. La otra parte sólo puede liberar las criptomonedas si es capaz de demostrar que conoce el "secreto" para decodificar la preimagen. Esto significa que para desbloquear la transacción, en el caso de los intercambios atómicos, el receptor requiere de una preimagen que sólo el emisor puede entregar.

Ejemplo de un intercambio atómico

Supongamos que Juan y Lorena quieren cambiar criptodivisas utilizando los intercambios atómicos en lugar de un intercambio descentralizado. Juan tiene unos bitcoins que quiere intercambiar con unos litecoins que posee Lorena. Estos son los pasos que se deben seguir:

- Paso 1: Juan genera un hash utilizando su clave privada y se lo envía a Lorena usando un canal de pagos abierto entre ambas partes. Juan también genera una preimagen del hash, ésta será utilizada posteriormente para validar y/o finalizar la transacción.
- Paso 2: Lorena, en respuesta,

genera su propio hash utilizando su clave privada y se lo envía a Juan. Del mismo modo, genera una preimagen tal y como lo hizo Juan en el primer paso.

- Paso 3: Tan pronto como Juan recibe la transacción de litecoins de Lorena, Juan la firma utilizando la misma clave original que tiene en forma de preimagen. El mismo proceso lo repite Lorena con la transacción de bitcoins de Juan.

Diferencia entre intercambios atómicos dentro y fuera de la cadena

Ya hemos mencionado antes que los intercambios atómicos pueden ocurrir

tanto dentro como fuera de la blockchain. Los que tienen lugar en la cadena se denominan on-chain, los que ocurren fuera de ella se llaman off-chain.

Para que un intercambio atómico pueda ocurrir on-chain, las cadenas de bloques deben ser compatibles con HTLC y las monedas deben tener el mismo algoritmo hash. Por otro lado, los intercambios atómicos off-chain se realizan utilizando la capa 2, que es un nombre para un canal abierto entre dos partes afuera de la cadena. Un ejemplo de esto es el primer intercambio atómico que tuvo lugar entre Litecoin y Bitcoin y empleó Lightning Network de Bitcoin en

lugar de la cadena de bloques.

Beneficios de los intercambios atómicos

Se ha mencionado previamente que los intercambios atómicos son una excelente alternativa a los DCE. A continuación mencionaremos algunos de los beneficios más importantes de este protocolo.

- Solución efectiva al problema de la interoperabilidad entre diferentes criptoactivos.
- Ahorro de dinero al evitar el pago de los cargos y comisiones que cobran los DCE.
- Se puede intercambiar directamente todo tipo de criptomonedas –incluso las

menos conocidas– sin utilizar BTC o ETH como tokens intermediarios.

- Intercambio de persona a persona más rápido, barato y seguro si lo comparamos con el servicio que ofrecen los DCE en los que es necesario crear una cuenta de usuario, identificarse debidamente y cumplir con las regulaciones KYC y AML antes de poder empezar a utilizar las plataformas. Para realizar un intercambio atómico no es necesario proporcionar ningún tipo de información personal ni pasar por engorrosos procesos

de verificación.

- A menudo los DCE son vulnerables a ataques informáticos al representar un solo punto de ataque. En contraste, al no haber un intermediario de confianza en los intercambios atómicos no hay riesgo de ataques y robos de dinero.

Podemos resumir los beneficios de los intercambios atómicos en cuatro aspectos:

1. Transacciones instantáneas
2. Costos más bajos
3. Total seguridad y transparencia
4. Transacciones persona a

persona sin intermediarios

Limitaciones de los intercambios atómicos

Los intercambios atómicos se encuentran dando sus primeros pasos, sin embargo éste es un protocolo que está en constante evolución. A continuación algunas de las limitaciones que esta tecnología enfrenta:

Adaptabilidad: Aún no es posible hacer intercambios atómicos entre todas las criptomonedas. Las condiciones que se deben cumplir para poder realizar un intercambio atómico son:

1. Las criptomonedas deben tener el mismo algoritmo hash

2. Ambas criptodivisas deben soportar HTLC
3. Las cadenas de bloques deben tener la capacidad de ejecutar contratos inteligentes

Hoy por hoy, no existen muchas criptomonedas que cumplan las tres condiciones previas, esto limita la cantidad de criptoactivos que pueden emplear intercambios atómicos.

Volumen de transacciones: A pesar de que una de las ventajas de los intercambios atómicos es la velocidad de las transacciones, aún existen serias limitaciones en cuanto al intercambio de montos grandes. Aún se requieren muchas mejoras para que este tipo de

transacciones puedan darse sin contratiempos.

Compatibilidad: La gran mayoría de billeteras aún no son compatibles con intercambios atómicos; las que ofrecen la opción de intercambios generalmente utilizan servicios centralizados como ShapeShift o Changelly. Atomic Wallet es una billetera multidivisa no custodial que ofrece intercambios atómicos.

El futuro de los intercambios atómicos

Por lo pronto, los intercambios atómicos son una excelente solución para aquellos usuarios que desean intercambiar criptomonedas de una forma descentralizada, sin la participación de

un intermediario. Se espera que este protocolo juegue un papel fundamental en la evolución de la tecnología blockchain.

Los intercambios atómicos son una tecnología prometedora que ofrece muchos beneficios a sus usuarios en comparación con las plataformas centralizadas, estas ventajas se traducen en ahorro de costos, mayor seguridad y más velocidad. En todo caso, todavía existen algunas limitaciones importantes por lo que es posible que sea necesario esperar algún tiempo antes de que esta tecnología prevalezca.

MimbleWimble: la privacidad que blockchain necesita

La privacidad de la sociedad abierta es necesaria en la era de la información. No podemos esperar que los gobiernos, corporaciones u otras organizaciones sin rostro nos garanticen la privacidad. Nosotros debemos defenderla si esperamos tenerla.

ERIC HUGHES

MimbleWimble es un protocolo de blockchain que se basa en la fungibilidad, privacidad y escalabilidad, lanzado en julio de 2016 en el canal de IRC Bitcoin-wizards por el seudónimo "Tom Elvis Jedusor". El documento propuso una nueva e interesante forma de combinar o mezclar transacciones para mejorar las características de

privacidad en una cadena de bloques pública; es decir, evitar que la información pueda ser vista por ojos no autorizados. Su nombre se debe a un hechizo de Harry Potter que evita que las personas se cuenten secretos.

El documento de Tom Elvis Jedusor se inspiró en un artículo publicado anónimamente en 2013, y en dos propuestas de privacidad, Confidential Transactions y CoinJoin, elaboradas por Gregory Maxwell, desarrollador de Bitcoin Core.

La publicación original de MimbleWimble hace referencia a la misma criptografía de curva elíptica (ECDSA, por sus siglas en inglés) que

usa Bitcoin, lo que despertó la atención de algunos investigadores de Bitcoin, entre los que se encuentra Andrew Poelstra, criptógrafo y matemático de Blockstream, quien hizo mejoras al documento original de MimbleWimble y lanzó una versión mejorada en octubre de 2016.

La privacidad de Bitcoin

El libro blanco de Bitcoin publicado por Satoshi Nakamoto posee una sección titulada "Privacidad", en la que Nakamoto reconoce las limitaciones que tiene Bitcoin respecto a la privacidad de las transacciones. Estos inconvenientes se han hecho cada vez más evidentes a medida que las transacciones de bitcoins

pueden ser rastreadas por medio del análisis de datos hasta identificar, con relativa facilidad, a sus emisores y receptores. Los días en que se pensaba que las transacciones de bitcoins eran anónimas quedaron atrás.

¿Cuáles son los datos que revelan las transacciones de bitcoins? Bitcoin muestra tres "secretos" en cada una de las transacciones que se realizan en su red de pagos:

1. Dirección del emisor
2. Monto de la transacción
3. Dirección del receptor

Al igual que cualquier sistema monetario –oro, efectivo, trueque–, Bitcoin debe cumplir con dos requisitos

fundamentales para considerarse seguro y confiable:

1. Tener la capacidad de verificar fehacientemente que la cantidad recibida equivale a la cantidad enviada, de lo contrario se crearía dinero de la nada. Si Juan entrega 5 dólares a Lorena, estos tienen que seguir siendo 5 al llegar a su bolsillo, ni uno más, ni uno menos; algo similar ocurre en una transacción de bitcoins.
2. Una transacción sólo puede ser realizada por el dueño del activo, no es posible hacer una transferencia bancaria desde una

cuenta ajena. Es imprescindible verificar que la transacción fue enviada efectivamente por el titular a través de una firma, PIN o contraseña, en el caso de haber hecho la transacción vía bancaria; en las criptomonedas, esta función es cumplida por la clave o llave privada.

Entonces, Bitcoin cumple estos dos requisitos al revelar los tres datos mencionados previamente. Una transacción de BTC contiene la cantidad y las direcciones del emisor y receptor, de esta manera se cumple con el primer requisito. Para cumplir con el segundo requerimiento, Bitcoin usa direcciones

públicas con sus claves privadas correspondientes. El emisor firma la transacción con su clave privada y libera esos BTC que se encuentran en su dirección pública. Todos los participantes de la red pueden verificar que la firma proviene de la clave privada detrás de la dirección que contiene los BTC. De esta forma se sabe que la firma proviene del individuo que tiene autoridad para iniciar la transacción.

El propósito de MimbleWimble es garantizar que las transacciones cumplen con los dos requisitos mencionados previamente, pero sin revelar los tres “secretos” de Bitcoin.

La primera implementación de MimbleWimble

La primera implementación, Grin, que prácticamente se ha convertido en sinónimo de MimbleWimble, se lanzó pocos días después del documento publicado por Poelstra. El seudónimo "Ignotus Peverell" –el propietario original de la capa de invisibilidad de Harry Potter–, creó el proyecto ignopeverell/grin en GitHub, donde proveyó una implementación parcial del protocolo escrito en Rust, además de publicar su visión del espíritu del proyecto.

En marzo de 2017, "Peverell" publicó una introducción técnica a Grin

y MimbleWimble, que sirve como referencia principal a la especificación del protocolo actual. Hasta la fecha, el proyecto aún es mantenido por un grupo de desarrolladores en su mayoría anónimos, varios de los cuales han tomado sus seudónimos de los personajes de Harry Potter –"Luna Lovegood", "Seamus Finnigan" y "Percy Weasley"–.

La segunda implementación de MimbleWimble

La segunda implementación, BEAM, es un proyecto que comenzó en marzo de 2018 y se anunció formalmente en el primer aniversario de la publicación original de MimbleWimble. BEAM se

presentó en un documento técnico separado –junto con un nodo minero funcional y una billetera– adquiriendo una estructura más formal, similar a la de Zcash, en contraste con el carácter anárquico y abierto de Grin. El equipo de BEAM está dirigido por Alexander Zaidelson, un empresario israelí.

Con un equipo de administración e ingeniería definido y una constitución formal, BEAM adoptó un enfoque muy diferente para presentar una alternativa a Grin en el mercado. Además de crear la estructura formal en torno al proyecto, el equipo de BEAM hizo diferentes elecciones técnicas a Grin, incluidas las decisiones relacionadas con la política

monetaria y el algoritmo de consenso. Este proyecto se lanzó a principios de enero de 2019.

En un mundo donde los sistemas de vigilancia, tanto a nivel estatal como privado, vienen haciéndose cada vez más intrusivos y sofisticados gracias a la implementación de tecnologías como la inteligencia artificial (IA), es indiscutible que la privacidad es importante a la hora de diseñar los sistemas monetarios del futuro. A pesar de que el uso de sistemas transaccionales privados no son del agrado de las autoridades –por obvias razones– y de que eventualmente su

utilización podría "manchar" la reputación de los que cumplen con la ley, el desarrollo de criptomonedas que ofrecen transacciones anónimas y privadas no deja de ser importante, ya que del mismo modo, los usuarios honestos que no tienen nada que esconder tienen a su disposición una herramienta tecnológica para proteger su patrimonio de los deshonestos. Se espera que este 2019 sea un año interesante para la privacidad.

Explicación de la tecnología MimbleWimble

Desde los primeros días de Bitcoin, la privacidad y la fungibilidad han sido las preocupaciones centrales de sus

usuarios. Bitcoin ha visto muchos intentos de eliminar el pseudoanonimato a sus transacciones, del mismo modo han surgido criptomonedas –Zcash, Monero, Grin, por ejemplo–. Por su parte, Bitcoin también ha visto mejoras significativas en cuanto a la privacidad y fungibilidad tanto en la capa de protocolo como en la capa de transacción. Tanto Grin como BEAM utilizan el mismo modelo de salida de transacción no gastada (UTXO, por sus siglas en inglés) que utiliza Bitcoin, en contraste con otras cadenas de bloques basadas en cuentas, como Ethereum.

Como habíamos visto anteriormente, Bitcoin revela tres

“secretos” sobre cada una de las transacciones: dirección del remitente (input), monto de la transacción y dirección del destinatario (output). En contraste, MimbleWimble realiza varios cambios en el modelo UTXO de Bitcoin para permitir transacciones privadas –que no muestran esos tres datos–, basados en Confidential Transactions y CoinJoin, como veremos a continuación.

Las mejoras en la privacidad de las transacciones propuestas por MimbleWimble, se fundamentan en tres propiedades:

1. Inexistencia de direcciones públicas (ConfidentialTransactions)

2. Ausencia de montos de las transacciones (ConfidentialTransactions)
3. Dos o más transacciones se combinan en un bloque para formar una sola (CoinJoin)

Las dos primeras propiedades hacen que las transacciones no puedan distinguirse unas de otras; dicho de otro modo, todas las entradas y salidas parecen fragmentos de datos aleatorios. Adicionalmente, los bloques en la blockchain no enumeran transacciones separadas, sino que se agregan en una sola transacción con entradas y salidas mixtas. Ver un bloque no proporciona información sobre una transacción

específica; en otras palabras, un bloque luce como una única transacción grande, perdiéndose toda pista de las transacciones. Los nodos pueden verificar la autenticidad de las transacciones sin revelar los valores que se transfieren; es decir, no hay direcciones ni información identificable en una transacción.

ConfidentialTransactions

Las primeras dos propiedades de MimbleWimble se basan en el uso de ConfidentialTransactions, una propuesta implementada en Blockstream Liquid, que es una cadena lateral de Bitcoin en producción que utiliza una técnica criptográfica llamada Esquema de

compromiso de Pederson para mejorar el modelo UTXO de Bitcoin. Gracias a ConfidentialTransactions, sólo los participantes de una transacción pueden ver el monto de la misma.

El compromiso de Pederson se puede explicar de esta manera: “Estoy probando que sabía algo antes de ‘hashearlo’ porque no puedo revertir el hash para revelar lo que sabía”.

Inexistencia de direcciones: Efectivamente, no hay direcciones. Todas las salidas son únicas y no comparten datos comunes con ninguna salida anterior. En lugar de usar una dirección para enviar criptomonedas, las transacciones deben ser construidas

interactivamente con dos o más billeteras que intercambian datos entre sí; esta interacción no requiere que ambas partes estén en línea al mismo tiempo. Sólo los participantes pueden ver estos datos y la información no puede ser reutilizada por terceros.

Ausencia de montos de las transacciones: El concepto de validación de transacciones sin conocer ninguno de los valores negociados se asemeja a las Pruebas de Cero Conocimiento (ZKP, por sus siglas en inglés) y RingCT empleados por Zcash y Monero, respectivamente.

En Bitcoin, donde se utilizan funciones hash criptográficas simples

para realizar compromisos de transacciones, la entrada, la salida y los montos de transacción son esenciales, como vimos previamente. Un compromiso de Pederson mejora esto al garantizar que la suma de las entradas y la suma de las salidas sean iguales. Las pruebas criptográficas que permiten esta certeza están más allá del alcance de este texto, sin embargo, se nos revela una idea clave: las entradas y las salidas pueden permanecer en secreto mientras la seguridad del sistema –que puede ser verificada *ipso facto*– permanece intacta.

Todas las implementaciones de MimbleWimble utilizan

ConfidentialTransactions para garantizar que no haya direcciones o cantidades visibles en el sistema.

CoinJoin

En cuanto a la tercera propiedad –combinación de transacciones–, ésta se explica mediante el uso de CoinJoin, también creado por Gregory Maxwell. El historial de una transacción contiene una importante cantidad de información que permite que alguien con suficientes recursos computacionales pueda visualizar gráficamente e inferir con relativa facilidad las relaciones entre diferentes transacciones en una misma red. Empresas como Elliptic y Chainalysis utilizan esta forma de

análisis forense para detectar fraudes y transacciones ilícitas –lavado de dinero, actividad en el mercado negro, por ejemplo–. En este sentido, debido a la trazabilidad de las transacciones de bitcoins a través del análisis de sus gráficos, es una pésima idea lavar activos utilizando esta criptomoneda. A través del uso de CoinJoin, las entradas de múltiples usuarios se combinan en lo que se llama conjunto de anonimato y se mezclan para garantizar que el gráfico de las transacciones sea más difícil de rastrear.

Wasabi, una billetera de bitcoins, ha implementado CoinJoin para ofrecer privacidad a las transacciones

de esta criptodivisa. Sin embargo, este intento no ha sido satisfactorio teniendo en cuenta que el conjunto de anonimato suele ser muy pequeño, por los pocos participantes en cada transacción, siendo fácil rastrear y descubrir a los participantes.

Las implementaciones de MimbleWimble resuelven este problema haciendo de CoinJoin una parte central del protocolo, en lugar de una mejora de la privacidad de la capa de transacción implementada por billeteras y servicios de terceros; en MimbleWimble todas las transacciones en cada bloque se contraen automáticamente en una sola transacción y la información intermedia

se oculta.

Dandelion

¿Hay alguna otra manera de descubrir o rastrear el origen y destino de las transacciones? La respuesta es sí.

Puede haber un punto de falla cuando los nodos de la red revelan las direcciones IP de origen. Cuando se realiza una transacción de bitcoins desde una billetera, ésta se transmite a un conjunto de nodos, los cuales a su vez la transmiten rápidamente a otros nodos, estableciéndose una "red de chismes". Antes de que una transacción se consolide en un bloque, es posible rastrear las direcciones IP de las que se origina, teniendo en cuenta que las

transacciones se transmiten por partes.

MimbleWimble propone una solución a este inconveniente llamada Dandelion, originalmente diseñada para Bitcoin, concebida por un equipo de investigadores de la Universidad de Illinois en Urbana-Champaign. Ha estado en discusión desde 2017 como una propuesta pública de mejora de Bitcoin.

El objetivo de Dandelion es "oscurecer" u "ofuscar" las direcciones IP de las transacciones de bitcoins. Los pétalos de una flor de diente de león (Taraxacum officinale) poseen un solo tallo hasta que florecen completamente. De manera similar, con Dandelion una

transacción de Bitcoin se transmite a la red en dos fases: la fase “raíz”, donde se oscurece u ofusca, y la fase de “encrespado”, donde se transmite. En primer lugar, la transacción se transmite a un solo nodo, luego se transmite a otro igual, y así hasta que haya suficientes saltos desde el interlocutor original; en ese momento la transacción se transmite al resto de la “red de chismes”.

La combinación de mejoras como ConfidentialTransactions, CoinJoin y Dandelion permite que las implementaciones de MimbleWimble eliminen las ideas tradicionales como las direcciones. Los compromisos criptográficos admitidos por los

individuos que generan una transacción asumen el propósito de las claves públicas y privadas utilizadas en Bitcoin para realizar una transacción.

PARTE 3

FINANZAS PERSONALES

Las finanzas tomadas desde un punto de vista personal han sido relegadas en el mundo y es una de las áreas más importantes en la vida de las personas y las familias. El dinero forma parte de nuestra vida diaria y es importante para lo que es importante y no es importante para lo que no lo es. Hay muchas personas en el mundo que piensan que el dinero no es importante, ¿pero a la hora de pagar la renta o querer comprarse un auto nuevo lo puede hacer con buenas intenciones? Pues, nosotros no lo hemos

visto, aun así hay personas que repiten frases como “el es tan pobre que lo único que tiene es dinero”, y eso en parte puede ser verdad; sin embargo lo importantes es siempre llegar a un equilibrio.

¿Te has preguntado por qué si el dinero forma parte de la vida diaria de las personas y es una constante en la sociedad no se toma en cuenta en los planes de educación para tener unas finanzas saludables y desarrollar nuestra inteligencia financiera? Pues se enseñan muchas cosas inservibles, pero hay temas importantes en la vida que no se incluyen, como educación financiera y alimentación. Existen varias teorías de

conspiración que dicen que un mundo educado derrumbaría al mundo actual como lo conocemos. A las grandes élites que controlan el mundo y las finanzas no les conviene que la masa esté educada en este campo. Hoy en día la deuda es la nueva forma de esclavitud que han instaurado en el mundo, es ahora la única forma de quitarles la libertad a las personas, ya que las personas libres son peligrosas para el *status quo*.

Vivimos actualmente en un mundo en el que utilizamos dinero, cualquiera sea su forma o denominación, para hacer intercambio para todo; por lo tanto, es importante que entendamos cómo funciona este juego. La mayoría de

las personas no conoce las reglas del juego del dinero y pasa la vida jugando por jugar. Si estamos obligados a jugar al menos debemos conocer como jugar a ganar.

Desarrollar una inteligencia y aprender sobre finanzas personales tiene un impacto directo sobre la vida de las personas. Existen millones de personas en el mundo que han empezado a vivir su vida no en automático, sino por diseño, creando su estilo de vida deseado y han empezado a jugar el juego del dinero a otro nivel.

Hoy en día lo que necesitas para jugar el juego del dinero es el conocimiento, y si estás leyendo este

libro es justamente porque estás buscando crear conocimiento sobre el futuro del dinero y el fascinante mundo de la criptoeconomía. Estás conociendo una de las mejores oportunidades de generar riqueza desde el auge de las empresas punto com en los años 90. Las criptomonedas no sólo brindan ventajas, como su rapidez en transacciones internacionales o su fácil manejo, también ofrecen una verdadera alternativa a un sistema financiero que cada vez parece estar más enfermo. Las deudas de los países industrializados son más grandes que nunca antes. Cada vez se les hace más difícil a los bancos centrales mantener sus divisas estables, y en la actualidad podemos observar que

en algunos países en crisis, como Venezuela, las criptomonedas ganan popularidad porque ofrecen una alternativa a los ciudadanos que ya no confían en su moneda local que pierde valor cada día. Mientras la infraestructura de las criptomonedas crece en el mundo, más personas en diferentes países buscan refugio en la criptoeconomía, ya que se enfrentan a fenómenos económicos que generan mucha inestabilidad.

En los últimos años, sobre todo durante su último boom en el año 2017, las criptomonedas se han convertido en un instrumento interesante de inversión. Muchas veces se compara el desarrollo

de la tecnología blockchain con el surgimiento de Internet. El 99% de las empresas que se crearon con el fin de ser una compañía de internet en la década de los 90 quebraron; sin embargo, los que invirtieron en empresas que verdaderamente tenían una utilidad real, como google.com, amazon.com o e-bay.com, son los grandes ganadores. Se predice lo mismo para las criptomonedas, aquellas que tengan una utilidad real y estén acompañadas por tecnología que solucione problemas reales de la sociedad, serán las grandes ganadoras. El Foro Económico Mundial proyecta que el mercado de criptomonedas llegará a una capitalización de 7

trillones de dólares hasta el año 2025, lo que implica un gran crecimiento en los próximos meses y años.

Si quieres invertir en criptomonedas debes estar consciente de los riesgos y oportunidades de este mercado. Las criptomonedas se negocian de la misma manera que acciones o divisas. La diferencia es que son digitales, no están vinculadas a un Estado y son descentralizadas. Un mercado tan jóven como la criptoeconomía tiene un gran potencial y por otro lado también conlleva un alto riesgo de inversión; hay que aprender a encontrar estos “diamantes” que pueden generar grandes ganancias. Mientras las

criptomonedas están en proceso de ser aceptadas en todo el mundo, también son objeto de especulación. Una de las reglas de los negocios e inversiones, es no ingresar en ningún mercado que no se conozca a profundidad, y esta regla también aplica para la criptoeconomía; sin embargo, el mercado de criptomonedas permite aprender en el proceso.

Cada cierto tiempo existe una revolución tecnológica. En los años 90 fue el Internet; en el 2000 fueron las redes sociales y los smartphones. Nosotros los autores de este libro estamos convencidos de que la siguiente gran revolución son las criptomonedas y

la tecnología blockchain. La economía del futuro se basará en las criptomonedas y creemos también que eso va a brindar ventajas a los usuarios que confiaron en sus inicios, más conocidos como “early adopters”. En este momento estamos entrando a una fase en la que se está creando un nuevo ecosistema alrededor de las criptomonedas y se están realizando grandes inversiones en la infraestructura que permite al usuario decidir qué sistema o moneda quiere usar. Él mismo escogerá el sistema que más se ajuste a sus necesidades y pueda brindarle mayor probabilidad de ganar en una valorización en el tiempo.

En los próximos capítulos proporcionaremos una guía para que conozcas las opciones de inversión que te ofrece la criptoeconomía y puedas crear tu estrategia de inversión, basándote en tu personalidad financiera. Antes de entrar en este campo primero analizaremos tus finanzas personales.

Tus Finanzas Personales

Estado financiero personal

El que no sabe en dónde está, cualquier camino le sirve.

JUAN CARLOS PALACIOS ELJURI

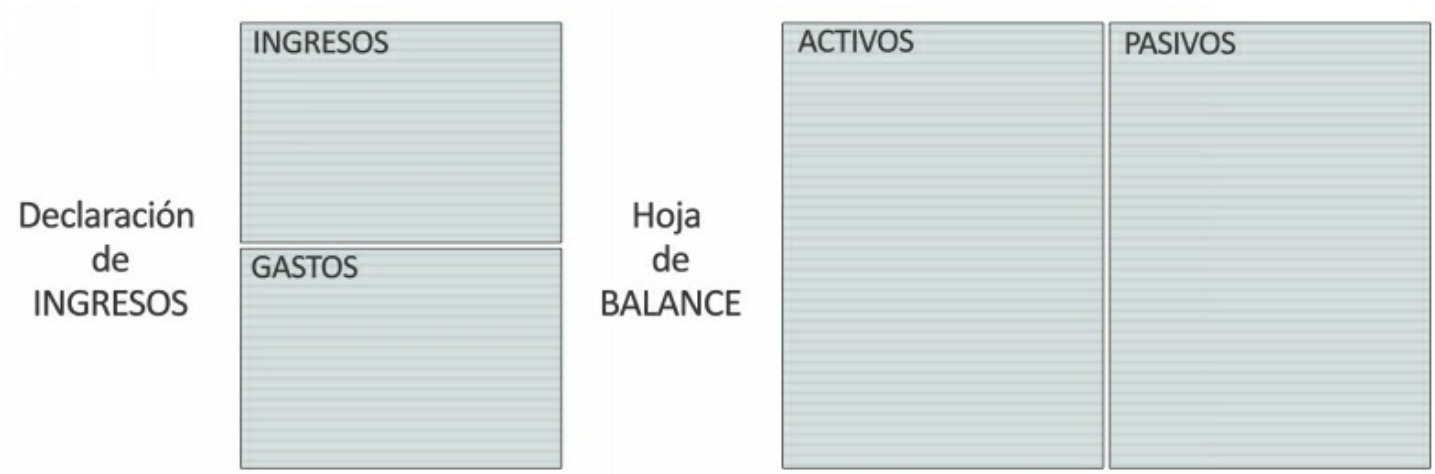
No es recomendable invertir en negocios, acciones, criptomonedas o cualquier otro tipo de inversión, si no

tienes claridad sobre tus finanzas personales primero. Es decir, debes estar consciente de dónde y cómo se encuentran tus finanzas personales. Imagina que tienes el mapa de un tesoro, y no sabes dónde estás situado en ese mapa; pues no te sirve de nada.

La forma más sencilla de saber en dónde te encuentras, financieramente hablando, es poner las cifras sobre la mesa usando el modelo del Estado Financiero Personal (EFP). Si sabes que no te va bien con tus finanzas este paso te puede costar cierto esfuerzo, pero es el primer paso para tomar el control sobre tu futuro financiero.

El EFP consiste en cuatro

elementos: ingresos, gastos, activos y pasivos, como muestra el ejemplo. Puedes desarrollarlo en una tabla de excel o en papel.



En el primer paso apunta ingresos y gastos. En la parte de ingresos registra todo ingreso de dinero por tu trabajo, negocio o tiempo que le dedicas a una actividad o ingresos pasivos por inversiones realizadas. Estos pueden ser ingresos por un "sueldo", si tienes un trabajo fijo; "comisiones", si trabajas en ventas; u

“honorarios”, en el caso de que trabajes de forma independiente, por ejemplo como coach o abogado. También puedes apuntar en esta parte “rendimientos o rentas”, si haz realizado inversiones o tienes un bien inmueble arrendado. Suma todo y sabrás cuál es tu flujo mensual de ingresos que generas a través de tu esfuerzo, trabajo e inversiones.

En el cuadro de gastos detalla todo aquello hacia donde va tu dinero, por ejemplo: arriendo, seguros, comida, ropa, servicios básicos, educación, comunicación, diversión, gimnasio, etc.

Si comparas ingresos y gastos podrás identificar cómo está tu flujo financiero mensual. Si los gastos son

mayores que los ingresos, no es hora de invertir todavía sino de arreglar tus finanzas buscando formas de simplificar; es decir, gastar menos y también de generar otras fuentes de ingreso y ganar más. Una vez que hagas un plan para administrar tus finanzas inteligentemente recuerda destinar un 10% de tus ingresos a una cuenta de inversion. No es importante el monto, lo que realmente es importante es el hábito. Cuando tu nivel de ingresos supere los gastos y tengas un potencial de ahorro podrás empezar con las inversiones.

En la segunda parte del cuadro analiza tus activos y pasivos. Un activo es cualquier bien que te da dinero sin

tener que trabajar o invertir tu tiempo. Por ejemplo, arrendar una casa genera una renta que recibes sin la necesidad de tener que trabajar. En el sistema financiero tradicional se considera un activo el dinero en la cuenta de ahorros con intereses, dinero a plazo fijo, pólizas, inversiones en acciones, fondos o ETF (Exchange Traded Funds). También la propiedad intelectual de canciones, libros o infoproductos digitales, ya que generan regalías y el trabajo de creación se realiza una sola vez. En esta parte de tu EFP también entran las criptomonedas y sus diferentes formas de inversión que vamos a analizar más adelante, ya que pueden generar una ganancia en valor o

flujo de efectivo sin tener que trabajar por ello.

La primera meta financiera de las personas no es ser rica, sino alcanzar la libertad financiera: "La libertad financiera se alcanza cuando los INGRESOS PASIVOS que vienen de las inversiones en ACTIVOS son mayores que los GASTOS FIJOS mensuales". Es decir, que los ingresos generados por el portafolio de activos generan el monto necesario para vivir el estilo de vida deseado. Para alcanzar esta meta es importante que definas una cifra exacta de cuánto es el valor que te permitirá vivir en libertad financiera y lo apuntes. Mientras más claridad tengas sobre tu

meta, mayor probabilidad tendrás de alcanzarla. El valor que define tu libertad financiera debe incluir gastos básicos, como vivienda, movilización, seguros, gas, agua, teléfono, luz, internet, ropa, comida y educación. Si el flujo de ingresos que generan tus activos cubre todos estos egresos entonces alcanzaste la libertad financiera y no tienes la necesidad u obligación de trabajar para cubrir tus gastos.

Una vez que no tengas que preocuparte por generar para vivir mes a mes, podrás fijar un valor que te permita vivir un estilo de vida con lujos y gustos extras, como el carro de tus sueños, una casa de lujo o viajes por el

mundo. Al vivir con libertad financiera el valor que te propongas en tu próxima meta seguro será más alto, pero es muy probable que te tome menos tiempo alcanzarlo, ya que al no preocuparte por producir lo que necesitas para vivir, tienes disponible todo tu tiempo y energía para crear nuevas fuentes de ingresos que te permitirán alcanzar tus nuevas metas.

La última parte en el EFP son los pasivos. Un pasivo es algo que posees y que te quita dinero, es decir que te genera gastos. Por ejemplo: si vives en casa propia ésta te genera gastos a través de impuestos o mantenimiento. Un carro propio genera gastos por el

seguro, mantenimiento, combustible y depreciación. Todo lo que es deuda también forma parte del pasivo, como créditos, deuda de la tarjeta de crédito, etc. Debes tener un equilibrio en los pasivos para manejar una economía sana. Evitar la deuda mala, conocida como deuda de consumo, y ser inteligente al usar la deuda buena para generar activos y nuevas fuentes de ingresos.

Cuando hayas desarrollado tu EFP podrás ver claramente el punto de partida en el mapa, y responder a la pregunta de dónde y cómo se encuentran tus finanzas personales.

A continuación te presentamos el

“Plan financiero de cuatro pasos”; una guía práctica y sencilla para administrar tu dinero y crear un plan de inversión que te permita adquirir criptomonedas y otros activos.

Los cuatro pasos a seguir son:

Primero: Crea una Cuenta de Inversiones que te permita alcanzar la libertad financiera con 10% de tus ingresos.

Segundo: Simplifica, elimina gastos innecesarios, pon tu vida en un período de construcción.

Tercero: Elimina la deuda mala y genera un sistema de compras programadas.

Cuarto: Crea múltiples fuentes de ingresos.

Vamos a ver cada paso más al detalle:

Primer paso: crea una Cuenta de Inversiones

En esta cuenta deberás depositar el 10% del total de tu ingreso mensual, esta cuenta es a largo plazo y la que te permitirá adquirir activos que te generen ingresos pasivos a lo largo del tiempo. Los fondos en esta cuenta no se pueden usar por ningún motivo que no sea el propósito para el que fue abierta. Como sugerencia: abre esta cuenta en un fondo de ahorro que no te de acceso libremente para evitar que se convierta en gasto corriente en algún momento. Más bien, cuando vayas a utilizar este

fondo que sea una decisión bien pensada que requiera tu firma o ir al banco.

Segundo paso: simplifica

> *No es más rico quien más tiene sino el que menos necesita.*
>
> BUDHA GAUTAMA

Simplificar va más allá de simplemente dejar de gastar en cosas que no necesitas. Se trata de recortar los excesos. Por ejemplo, muchas personas poseen una pila de diferentes tarjetas de crédito. ¿Pero sabías que cerrar las tarjetas que no usas puede ayudarte a mejorar tu crédito? Tener menos cuentas y tarjetas también puede ayudarte a mantenerte organizado para que ningún pago se pierda. Es muy probable que

tengas un refrigerador repleto de cosas que no vas a comer antes de que se echen a perder. Al final del mes, una gran parte de la comida se irá a la basura, y tendrás que regresar al supermercado y llenar tu carrito de compras con más productos para reabastecer tu refrigerador entero. Simplificar es priorizar tus gastos y eliminar los que realmente no son necesarios o no aportan nada en tu vida. Te sorprenderás al ver cuánto estás gastando en cosas innecesarias, que no utilizas o que no te hacen feliz. Elimina en lo posible los gastos fijos y automáticos, trata que todos tus gastos sean por consumo. Esta cultura ya se está implementando en varias partes del

mundo, incluso con los pagos recurrentes como seguros. Existen compañías de seguros que te permiten activar y desactivar el seguro del auto según tu requerimiento. Por ejemplo, si no vas a sacar el auto de casa todo el fin de semana desactivas el seguro, pero si sales de viaje lo vuelves a activar, así podrás disfrutar de una economía real.

Tercer paso: elimina la deuda mala

El eliminar deudas es un paso importante en este plan y se refiere sobre todo a las malas deudas, las que sólo te generan gastos y no traen beneficios económicos. Existen dos fórmulas para eliminar las deudas. Lo que siempre tienes que hacer primero es

apuntarlas todas en papel para tener claridad, saber montos y porcentajes de interés que generan. Después puedes optar por uno de los siguientes planes para eliminarlas:

Opción 1: Ordenar la lista de las deudas desde la más pequeña hasta la más grande y empezar a eliminar las pequeñas deudas primero y después las grandes. De esta forma te vas a motivar cuando ves que la lista al inicio se disminuye rápido y después te quedan sólo unas pocas, como por ejemplo la hipoteca de la casa que no tiene tanta urgencia en eliminarse.

Opción 2: Pagar las deudas que mayor interés generan primero. Si tienes dos

deudas en tu lista de 5.000 USD cada una y una es la de la tarjeta de crédito donde te cobran un 25% de interés anual y la otra es con tu hermano que te prestó el mismo monto, pero no te cobra interés, entonces primero eliges pagar la tarjeta de crédito.

No todas las deudas tienen que ser eliminadas de la lista, sólo las malas, las que no te traen beneficios. Suena raro, sin embargo existen también buenas deudas y no hay problema en mantenerlas. Aquí hay dos ejemplos:

Buena deuda 1

La que te genera más de lo que te cuesta pagarla. Este tipo de deuda se genera cuando te prestan dinero para un

negocio. Por ejemplo: estás vendiendo ropa y adquieres un crédito de 10.000 USD al 15% anual; con este dinero compras ropa y la vendes en 20.000 USD; en un año devuelves el capital y 1.500 USD en intereses y te quedan 8.500 USD en ganancias. De esta forma te estás apalancando con dinero ajeno para tu negocio y generas una rentabilidad mayor.

Buena deuda 2

La que la paga otra persona. Esta deuda funciona sobre todo en los bienes raíces. De la forma que adquieres un departamento con una hipoteca que te cuesta pagar 500 USD al mes. Al mismo tiempo alquilas el departamento en 500

USD mensuales. Así puedes usar el dinero del arriendo para pagar la hipoteca y te quedas al final con el bien.

Al eliminar la deuda mala puedes crear un fondo de compra programado. Consiste en comprar un bién, viaje o servicio cuando se tiene suficiente dinero ahorrado para poder pagarlo de contado. De esta forma se evita pagar altos costos de financiamiento en las tarjetas de crédito y se puede disfrutar de descuentos extras por el pago en efectivo. Esta práctica te puede ahorrar un 40% en las compras.

Cuarto paso: crea múltiples fuentes de ingresos

El último paso consiste en usar el dinero

ahorrado en la Cuenta de Inversiones para adquirir nuevos activos y de esa forma aumentar tu portafolio de activos que te llevarán a la libertad financiera. Ese dinero debe usarse sólo para comprar algo que después produzca más dinero de forma automática, sin tener que invertir tiempo y esfuerzo. Adicionalmente puedes empezar a crear negocios inteligentes que se conviertan en negocios pasivos en cierto momento del proceso y así aumentar tus ingresos en el tiempo.

La clave para alcanzar la libertad financiera más rápida es generar más ingresos mientras gastas menos y automatizas el ahorro. Recuerda

que “si no controlas tu dinero, el dinero te controlará a ti”.

La mentalidad del inversionista

> *Gran parte del éxito se puede atribuir a la inactividad. La mayoría de los inversores no pueden oponerse a la tentación de comprar y vender constantemente.*
>
> WARREN BUFFETT

Ahora que has aprendido cómo analizar tu situación financiera y con qué plan puedes acercarte a la libertad financiera, hay que empezar a adquirir activos, y eso en la mayoría de los casos significa que debes convertirte en inversionista.

Tal vez ya has hecho tus

primeras inversiones o tal vez formas parte de la mayoría de las personas que no lo ha hecho aún. La principal razón de por qué la mayoría no hace inversiones es el factor emocional; es decir, el miedo a perder o al fracaso que nos impide tomar acción. Las personas que aún no han desarrollado una mentalidad de inversionista se preguntan antes de hacer una inversión: "¿Y qué pasa si pierdo?", mientras el inversor experimentado se pregunta: "¿Cuánto puedo ganar?".

Existen ciertas creencias limitantes que pueden frenarte al momento de hacer inversiones para alcanzar la libertad financiera, como

pensar que el dinero es algo malo, que la gente que tiene mucho dinero son personas malas o pensar que no mereces vivir en abundancia. Aunque la mayoría de las personas dicen que quieren tener libertad financiera, estando en el camino se frenan y quedan atrás de sus posibilidades, liquidan sus inversiones antes de explotar el pleno potencial y se estancan a medio camino porque sienten que es una gran responsabilidad manejar mucho dinero. El tope máximo de su mentalidad y su termostato financiero no les permite pasar de cierta cantidad de dinero o patrimonio; es decir, tienen un tope en los montos que pueden ganar, manejar o poseer.

Para tener éxito en las inversiones tenemos que entrenar nuestro pensamiento y nuestro ser. Sólo con creencias empoderantes y una visión clara podemos llegar a nuestras metas financieras. El acomodarse en un estilo de vida a medias siempre será el peor enemigo. Tú te mereces lo mejor y toda la abundancia, ése es el estado natural del ser humano, recuerda que existen recursos ilimitados en el mundo, lo único que tienes que descifrar es cómo acceder a ellos en el momento que los requieras, esto es conocido como abundancia. ¿Crees que puedes ser tú el próximo millonario de criptomonedas? ¿Por qué tienen que ser otros? Definir

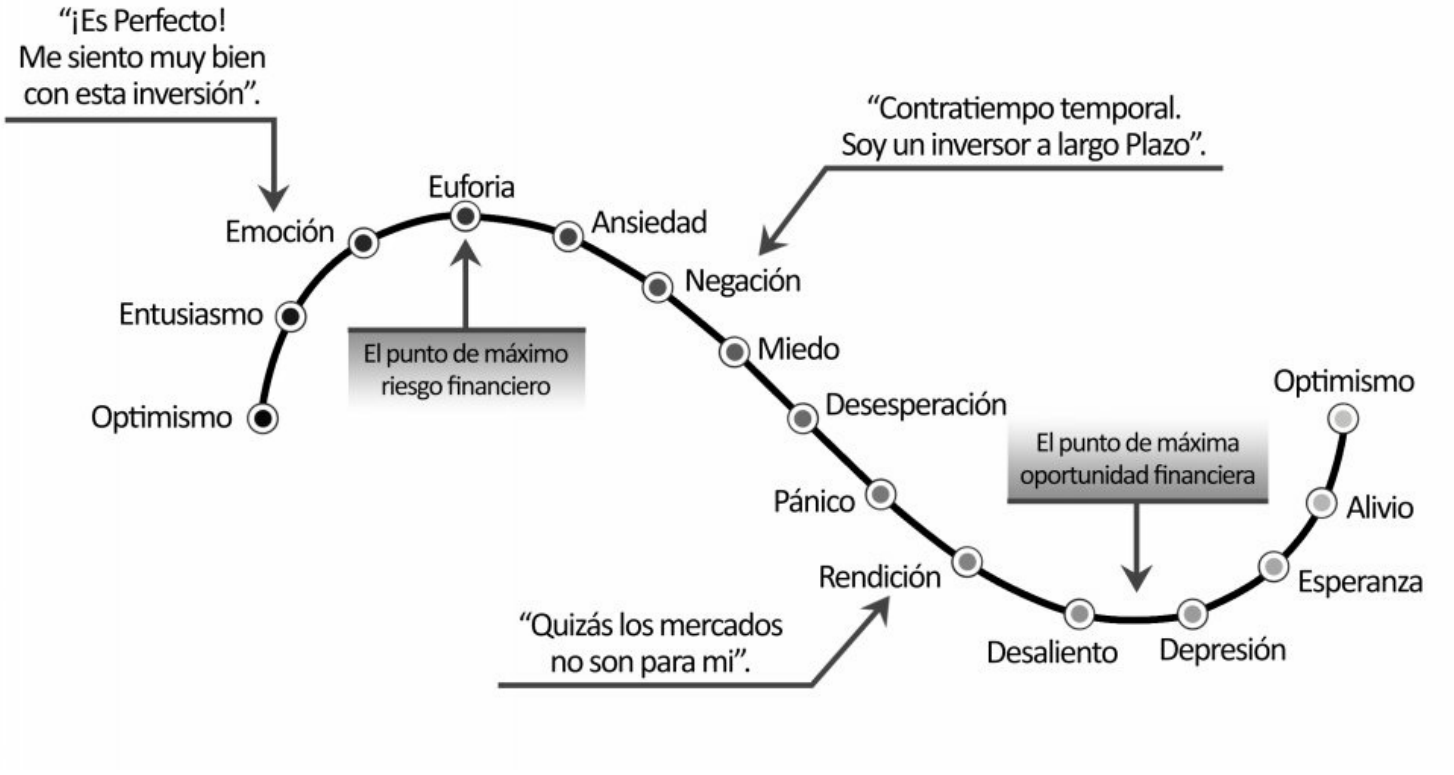
tus metas y un plan de trabajo específico te llevará hacia ellas y lo lograrás.

Una herramienta que te puede ayudar a superar los miedos a las inversiones son las "autopreguntas", hacerte a ti mismo ciertas preguntas. En el caso de sentir miedo a las inversiones pueden ser éstas:

1. ¿Qué es lo peor que puede pasar? ¿Puedo manejar la pérdida?
2. ¿Qué es lo mejor que puede pasar? ¿Vale la pena hacerlo?
3. ¿Qué pasará si no lo hago? ¿Nada? Entonces, si quiero mejorar mis finanzas tengo que tomar acción.

Responder estas preguntas te ayudarán a manejar el miedo y tomar una decisión acertada basada en un análisis objetivo y no en la emoción del momento.

Los mejores inversionistas saben manejar muy bien sus emociones para que no influyan en la forma de tomar sus decisiones. En los mercados financieros hay ciertos ciclos que se repiten y tienen gran influencia en el comportamiento de los inversionistas experimentados y de los novatos. Al conocer estos ciclos podrás ajustar las estrategias de inversión según el ciclo en el que se encuentre el mercado y tomar decisiones como los grandes inversionistas.



Fuente: esBolsa.com

Lo que podemos observar en el gráfico es que los ciclos en los mercados pasan del optimismo a la euforia, llegando al pánico y después a la depresión. Este proceso es cíclico y siempre se repite, los inversionistas lo conocen y ajustan sus estrategias basados en el momento del ciclo en el que se encuentre el mercado. Los

inversionistas con pocos conocimientos creen que los momentos de emoción y euforia nunca terminan y que el mercado siempre va a seguir al alza, por eso no venden sus inversiones a tiempo y recién al llegar a la zona de pánico empiezan a vender con pérdida. El secreto es actuar en contra de los ciclos y emociones del mercado; es decir, vender en momentos de emoción y euforia cuando los demás dirán que estás loco porque piensan que el mercado seguirá subiendo y comprar cuando "la sangre corre por las calles", como dijo el barón Rothschild ya en el siglo XVII. En los momentos de crisis y pánico hay las mejores oportunidades de entrar, se puede ganar mucho dinero esperando sin hacer movimiento alguno,

manteniendo una buena reserva en efectivo hasta que llegue el momento oportuno. Eso implica que hay que tener calma y paciencia para no hacer nada en los momentos en los que no hay buenas oportunidades. A la mayoría de los inversionistas les gana la desesperación y empiezan a tomar decisiones por emoción.

Hay una frase que se pudo corroborar en dos ocasiones al hacerse realidad. Tanto en el auge de las empresas punto.com a finales de los años 90, como en el auge de las criptomonedas a finales de 2017. La frase dice: “Cuando tu abuela empieza a invertir en este mercado es tiempo de

vender". A finales del 2017 los precios de criptomonedas llegaron a nuevos récords día tras día, se sentía una gran euforia en el mercado que parecía que nunca iba a parar, todo el mundo quería entrar al mercado y comprar criptomonedas, aunque no sabían nada sobre el mismo. Los medios crearon un hype y eso es justo el momento para vender. Por el FOMO —el miedo de quedarse fuera de esta gran oportunidad —, muchos pequeños inversores no vendieron, sino compraron y perdieron el 80, 90 o más por ciento del valor de su portafolio de monedas durante el 2018. El tiempo en cual se debe invertir empieza en la fase de pesimismo, se desarrolla en la época de escepticismos,

madura en los tiempos del optimismo y termina en los momentos de euforia.

Antes de mostrarte una guía para crear un portafolio propio de inversión te queremos compartir cuatro principios que aplican los inversionistas más grandes del mundo:

Primer principio: Evitar pérdidas de todas maneras. Todos quieren generar grandes rentabilidades. Aún más importante es asegurar las ganancias generadas y no perderlas nuevamente.

Segundo principio: Generar una buena rentabilidad mientras el riesgo sea lo más bajo posible. Buscar la mejor relación entre oportunidad y riesgo.

Tercer principio: Anticipar y

diversificar. La diversificación es fundamental en una estrategia de inversión porque te va a proteger en contra de posibles equivocaciones.

Cuarto principio: Nunca ponerse cómodo, sino mantenerse hambriento.

Crear un portafolio de inversiones

> *¿Cuántos millonarios conoces que se hayan enriquecido invirtiendo en una cuenta de ahorro?*
>
> ROBERT G. ALLEN

Una de las claves más importantes para llegar al éxito financiero y alcanzar la libertad financiera es la estructuración de un portafolio de inversiones. La mayoría de las personas que han

desarrollado su inteligencia financiera diversifican sus activos. Poner todo en una sola canasta es una estrategia de suicidio financiero, quiere decir que manejar el 100% de tu capital de inversión en criptomonedas es demasiado arriesgado. Para crear una estructura equilibrada en tu portafolio, vamos a revisar las opciones que tienes tanto en la economía tradicional como en la criptoeconomía. Aquí creamos dos grupos: inversiones con más seguridad e inversiones de mayor oportunidad.

Ejemplos de inversiones con más seguridad

- Dinero en efectivo: no es una inversión para generar

rentabilidad, sólo si especulas que una divisa ganará valor sobre otra, por ejemplo USD vs. EUR. El dinero en efectivo te sirve más bien para tener rápido acceso a liquidez con la que puedas aprovechar oportunidades de inversión. También ten en cuenta que el dinero fiat pierde valor adquisitivo por la inflación.

- Bonos del Estado.
- Dinero a plazo fijo o pólizas en los bancos.
- Casa propia: aunque no genera rentabilidad puede ser una forma de protección del patrimonio.

- Metales (oro, plata…): no son para generar rentabilidad sino para guardar valor o ganar en una revalorización.
- Seguro de Vida.

Ejemplos de inversiones de mayor oportunidad

- Bienes Inmuebles o REITs (Real Estate Investment Trusts).
- Objetos de colección: arte, monedas físicas, vinos etc.
- ETFs o fondos de inversión.
- Acciones.
- Criptomonedas.

Como regla general, existe la creencia en que se debe tener tanto porcentaje en inversiones con más

seguridad como años de edad se tengan, y el resto en inversiones de mayor oportunidad. Quiere decir que si tienes ahora 35 años, entonces el 35% de tu capital debe estar en inversiones de mayor seguridad y el 65% en inversiones de mayor oportunidad. Este 65% podrías dividirlo de la siguiente forma:

- 20% Inmuebles.
- 15% ETF.
- 15% Acciones.
- 15% Criptomonedas.

La estructuración de un portafolio es muy importante, porque hay oportunidades de ganar mucho dinero de forma rápida; sin embargo, la correcta

estructura asegurará la riqueza alcanzada para no perderla en un movimiento negativo del mercado. Lo más importante en la diversificación de las inversiones es generar tranquilidad y paz mental en el inversor. Para la consolidación de un portafolio una de las mejores estrategias es aumentarlo en el tiempo con compras periódicas; por ejemplo, comprar 100 USD en bitcoin cada mes, así evitarás la duda de cuándo es el mejor momento para comprar, y aprovechas un precio promedio del mercado.

Al encontrar una diversificación entre seguridad y oportunidad es importante que cada cierto tiempo realices una reestructuración, ya que puede ser que los fondos de mayor oportunidad crezcan con mayor velocidad que los de seguridad. Esto quiere decir que la diversificación porcentual cambia y requiere que la ajustes nuevamente. Es importante

revisar cada seis o doce meses el comportamiento de las inversiones y reestructurarlas de ser necesario para mantener el equilibrio inicial. Las emociones pueden inclinarte a no hacerlo, ya que esto puede implicar, por ejemplo, vender criptomonedas que se encuentren al alza y con potencial de aumentar su valor todavía más y transferir estos valores a una inversión de seguridad que genere un rendimiento menor. Sin embargo, son justamente estos ajustes los que aseguran un crecimiento saludable de tu portafolio a largo plazo, se maximiza la rentabilidad y se minimizan las pérdidas. Ray Dalio, uno de los inversionistas más importantes en la actualidad, dice que

toda inversión tiene su tiempo de ganar y también su tiempo de perder. La clave del portafolio es estructurarlo de forma que siempre se generen ganancias con una parte de las inversiones. Hay épocas de inflación en las que los metales como el oro y la plata, los bonos del Estado con protección contra la inflación o los bienes raíces son una buena opción de generar una rentabilidad, mientras el dinero en efectivo pierde su valor. Por otro lado, al existir una crisis en los mercados tradicionales podemos usar el dinero en efectivo, pólizas con rendimientos fijos o criptomonedas como opción de protección de capital.

Una vez que hayas encontrado la

forma de tener tu portafolio en equilibrio, basado en tu personalidad financiera, en cualquier situación economica vas a ganar.

Aunque este libro se encuentra enfocado en las criptomonedas y la tecnología blockchain, hemos mencionado ahora algunos conceptos de inversión y opciones de la economía tradicional. Mientras la criptoeconomía no está bien establecida en las mayores economías del mundo, no sería responsable hacer únicamente inversiones en criptos. Dada su baja liquidez y alta volatilidad en la actualidad están consideradas como una de las opciones más especulativas de

inversión y así como puedes ganar mucho dinero también se debe estar dispuesto a perder en esta parte del portafolio. Si existe desconocimiento sobre los activos financieros que hemos mencionado en este capítulo hay que tener en cuenta que se debe invertir con base en los conocimientos y la información que se tengan sobre ellos. Al estudiar este libro podrás adquirir conocimientos muy valiosos acerca del mercado de criptomonedas y podrás empezar a realizar inversiones en este mercado. Si lo que se pretende es invertir en ETFs, acciones o inmuebles, lo primero que hay que hacer es estudiar estos mercados antes de hacer cualquier tipo de inversión.

Inversión en criptomonedas

Mis más sinceros agradecimientos al gobierno de Estados Unidos, senador McCain y senador Lieberman por impulsar Visa, MasterCard, Paypal, AmEx, Mooneybookers y et al en un ascendiente bloqueo bancario ilegal contra WikiLeaks, empezando en 2010. Esto causó que invirtieramos en Bitcoin y generamos un retorno de 50.000%.

JULIAN ASSANGE

Después de haber aprendido mucho en este libro sobre las criptomonedas, la tecnología blockchain y finanzas personales, ahora es momento de tomar acción. Puede generarse la interrogante:

¿cuándo es el mejor momento de empezar a invertir en criptomonedas? La respuesta es: ahora. Casi seguro que perdiste la oportunidad de haber comprado tus primeros Bitcoins en 2009 a centavos, cuando nadie confiaba en esta nueva tecnología; desde ese momento ha habido crecimientos impresionantes y también caídas y nadie sabe con certeza cómo será el futuro. Por eso es importante tomar acción en este momento y aplicar una o varias de las opciones de inversión en criptomonedas que vamos a explicar en este capítulo. Antes de ver las opciones concretas hay ciertos factores y términos que hay que conocer.

La diferencia entre inversión y especulación

Inversión

Adquisición de bienes o productos financieros a mediano o largo plazo para generar una rentabilidad.

Especulación

Generación rápida de ganancias por la volatilidad en precios de bienes o productos financieros; por ejemplo el trading intradiario, la compra y venta dentro de pocas horas en los exchanges, es una especulación.

Relación entre riesgo y oportunidad de las inversiones en criptomonedas

Tomando en cuenta las proyecciones y

análisis de varios inversionistas, hay una gran oportunidad de que la criptomoneda crezca veinte veces su valor en los próximos diez años. Esto quiere decir que por cada dólar que inviertes tendrás una oportunidad de ganar veinte; por otro lado, el máximo riesgo que existe en una inversión es perder el 100%. La pérdida total en las criptomonedas definitivamente es posible, sobre todo si sólo invertimos en una moneda específica; que todo el mercado desaparezca ya no es un escenario tan probable. Es decir, que la mejor forma de realizar una inversión y bajar el riesgo es diversificar nuestro capital en varias monedas y formas de inversión.

Si ponemos el riesgo en una balanza podemos ver que con las proyecciones nombradas tenemos una oportunidad de ganancias del 2.000% y un riesgo de pérdida del 100%. Al poner estas cifras en relación con su probabilidad realizamos la pregunta: ¿Qué tan probable es cada uno de los dos casos? Digamos que el crecimiento del 2.000% tiene una probabilidad del 30%, que resultaría en un 600% de beneficio neto. Por otro lado la pérdida del 100% tiene una probabilidad del 10%, que significa que hay un 10% de probabilidad de pérdida total. Teniendo estas cifras en cuenta podemos ver que la relación entre oportunidad y riesgo

está a favor de la oportunidad.

¿Cuánto invertir en criptomonedas?

Como hemos descrito en el capítulo sobre la creación de un portafolio de inversiones, no debemos poner todos los huevos en una canasta. Principalmente en las inversiones de mayor oportunidad hay que tener en cuenta el riesgo para definir qué porcentaje de nuestro capital queremos invertir. Un portafolio de inversión en criptomonedas bien diversificado contiene de diez a treinta monedas diferentes.

La regla básica es: "No inviertas más de lo que estás dispuesto a perder". En el portafolio de inversión se puede destinar entre un 5 y un 20% al mercado

de criptomonedas. Para principiantes lo más recomendable es iniciar con un 5% y según aumentan experiencia y confianza llegar a un 20%.

Pump y Dump

El Pump y Dump es una forma muy común de manipulación de precios en el mercado de criptomonedas. Pump significa la manipulación hacia arriba; un pump puede aumentar el precio de una moneda 1.000% o más en pocas horas o días. Cuando la moneda tiene la atención en el mercado y sobre todo los inversores novatos empiezan a comprar por emoción, sin tener en cuenta las razones de la subida, empiezan a vender los grandes inversores y se quedan con

la ganancia, mientras los inversores nuevos entran en pánico cuando miran la cotización cayendo (Dump) y venden a cualquier precio con pérdida. Estos movimientos también se los conoce como intervención de las "ballenas", que son grandes inversores que mantienen en su poder un número significativo de estas criptomonedas. Mientras aumenta la capitalización de una moneda es más difícil manipular su precio; sin embargo, en las monedas con poca capitalización los Pumps y Dumps ocurren frecuentemente. Los exchanges o casas de cambio están poniendo atención a estos movimientos y tomando acciones, y pueden llegar a cerrar una cuenta de usuario cuando detectan que

está participando en esta manipulación riesgosa del mercado.

¿Cómo medir tus resultados de inversión en criptomonedas?

Existen dos formas de medir el éxito o la rentabilidad de las inversiones en criptomonedas. Una es realizar el cálculo basado en cuánto se ha ganado o perdido en USD/EUR; en moneda fiat, y la otro es hacer la medición en bitcoins. Sobre todo cuando inviertes en altcoins, donde el riesgo y la volatilidad son mayores, puede ser una buena idea medir tus ganancias en bitcoins y no en dinero fiat. En la mayoría de los exchanges existen los pares de BTC y altcoin de forma que se puede ver

cuántos satoshis cuesta una altcoin, si sube la cantidad de satoshis significa que se ha ganado más bitcoin, si al mismo momento el precio del bitcoin también ha subido en comparación con el dólar, adicionalmente se han ganado más dólares. En este caso se gana dos veces, en bitcoin y en dinero fiat. Por otro lado, puede bajar el precio del bitcoin y con esto puede pasar que con la altcoin se gane más bitcoins; sin embargo, al hacer cuentas en dinero fiat se tendrá menos al final.

¿Cuándo efectivizar las ganancias en criptomonedas?

La pregunta de cuándo se debe efectivizar las ganancias generadas en

criptomonedas o cuándo venderlas es tan compleja de responder como la pregunta de cuándo debes comprarlas. Finalmente, no podemos predecir hasta qué punto las monedas van a subir o bajar y puede pasar que una moneda que adquiriste subió un 100% y pensando que es un buen momento de venderla, se vende y después quintuplica su valor; por eso lo mejor sería hacer ventas parciales y guardar la otra parte. Es importante tener claro cuál es el objetivo con las inversiones en criptomonedas y tener una meta de cuánto se quiere generar. Una meta puede ser la compra de un auto o crear tu patrimonio a largo plazo en la criptoeconomía. Es importante basar las

acciones en las metas planteadas y mantenerse pendiente de las subidas y bajadas. Debes vender cuando ya alcanzaste el porcentaje de utilidad que te has propuesto o el valor en dinero fiat que quieres alcanzar. Con la ganancia realizada hay que cerrar operacional y mentalmente esa transacción, de igual manera dejar de lado lo que sucede después con el valor de la moneda. Es muy complejo hacer una compra o venta en los momentos más bajos o más altos de una moneda, aunque el análisis técnico nos da una referencia. Una estrategia útil cuando no se está seguro de vender o no alguna moneda, es vender el 50% de lo que tienes de esa

moneda. Si después baja puedes estar satisfecho porque has realizado ya una ganancia y si sube sigues participando en la revalorización. En ambos casos ganas. Consejo: nunca vendas el 100% de una moneda, si la quieres vender quédate con unas pocas o con una pequeña fracción porque nunca sabes qué va a pasar en un futuro con la misma.

Formas de invertir en Criptomonedas

Buy and Hold (HODL)

I AM HODLING.

GAMEKYUUBI (sinónimo),
18 de diciembre 2013 en
bitcointalk.org

La estrategia de Buy and Hold (Comprar y Guardar) implica comprar una o varias criptomonedas y guardarlas en una billetera segura y esperar a que suba el precio. En la comunidad cripto esta estrategia también se llama HODL (Hold On to Dear Life). El HODL nace de una conversación en Bitcoin-Talk

donde un participante escribió mal la palabra HOLD (mantener) y este error se hizo famoso. El Buy and Hold es una de las estrategias más simples, porque lo único que necesitas es una billetera y comprar monedas. Además, si usas una billetera que maneja claves privadas es una opción muy segura porque eres el dueño de las monedas y no dependes de un tercero. Otra ventaja es que puedes empezar con montos de inversión muy bajos, como por ejemplo 50 USD que compras en cripto, lo guardas y esperas. Aunque parece muy simple, esta forma de invertir ha generado grandes beneficios a mediano y largo plazo. La clave es tener una visión a un plazo más largo y no dejarse llevar por la

volatilidad del mercado que puede asustar a los inversores y hacerle cambiar la estrategia a cada rato.

Para mostrar el poder de esta estrategia aquí un ejemplo: supongamos que hubieses comprado 100 USD en cada una de las monedas del top 5 en coinmarketcap a inicios de enero de 2016 (Bitcoin, Ripple, Litecoin, Ethereum y DASH). Tu inversión hubiese sido de 500 USD. ¿Cuanto valdría este portafolio tres años después, a inicios del 2019? La respuesta es alrededor de 27.000 USD; una rentabilidad del 5.400% en tres años. Muchos traders que tratan a diario de ganar al mercado a través de la

especulación no llegaron a esta rentabilidad en el mismo tiempo.

Para aplicar el Buy and Hold puedes usar una de estas tres estrategias:

Estrategia 1: Compra única

En la compra única realizas una sola compra de monedas al precio del momento y después las guardas. Cómo se invierte a mediano o largo plazo no importa tanto el día y la cotización porque no se está especulando, sino se espera que la cotización se desarrolle en positivo durante los próximos meses o años.

Estrategia 2: Compra única diversificada

Puedes también diversificar la compra a

corto plazo. Quiere decir que si tienes 1.500 USD para comprar criptomonedas y no sabes si es un buen momento para comprar puedes dividirlo en tres compras. Los primeros 500 USD al inicio, otros 500 USD cuando el mercado esté bajando y los últimos 500 USD cuando exista otra bajada posterior. De esta forma se realiza una compra a un precio promedio y se disminuye el riesgo de comprar en un momento en que la moneda se encuentra a un valor muy alto. También puedes dividir la compra en tres fechas fijas; por ejemplo, cada 5 del mes durante los próximos 3 meses, así no tienes que especular cuándo será un buen momento para la próxima compra sino que sólo

sigues el plan.

Estrategia 3: Compras periódicas (ahorro acumulado)

Esta estrategia es de las más recomendadas para iniciar inversiones en criptomonedas. Se trata de comprar una cantidad cada cierto tiempo –por ejemplo, cada mes–, no importa a qué precio esté la moneda. Al realizar esta acción durante un año se obtiene una compra a un precio promedio minimizando así el riesgo. Esta estrategia conviene más en mercados bajistas que en mercados alcistas. Al final las compras periódicas son una estrategia que protege la salud emocional del inversor, ya que se puede

estar contento tanto cuando sube la moneda, ya que el valor de ahorro total sube, como cuando baja, porque se compran más monedas a menor costo.

Para que veas cómo funciona esta estrategia vamos a ver la diferencia en resultados en un mercado alcista y en uno bajista, comparando la compra única de 1.200 USD en bitcoins el 1 de enero o doce compras de 100 USD durante un año el primer día de cada mes.

Año alcista 2017: Con una compra única de 1.200 USD el 1 de enero hubieras recibido 1,247 bitcoins que el 1 de enero de 2018 hubieran valido 16.604 USD. Comprando 100

USD cada primero de mes hubieras acumulado 0,64 bitcoins que el 1 de enero 2018 valían 8.528 USD.

Año bajista 2018: Con una compra única de 1.200 USD el 1 de enero hubieses recibido 0,09 bitcoins, que el 1
de enero de 2019 valían 337 USD. Comprando 100 USD cada primero de mes hubieras acumulado 0,164 bitcoins que el 1 de enero 2019 valían 615 USD.

Ahora, si durante los dos años hubieses comprado 100 USD cada primero de mes tu inversión total hubiese sido de 2.400 USD. El 1 de enero de 2019 hubieses tenido 0,805 bitcoins que valían 3.012 USD y una

rentabilidad del 25,5% en dos años.

En resumen, podemos notar claramente que esta estrategia funciona mejor en mercados bajistas, pero a largo plazo proporciona la mejor opción para generar ganancias, suba o baje el mercado.

Diversificación

Aplicando la estrategia de Buy and Hold se recomienda diversificar entre varias monedas para crear un portafolio de criptomonedas y así evitar poner todos los huevos en la misma canasta. La página web coinmarketcap.com puede ser una gran ayuda en la selección de monedas a comprar, ya que ordena las criptomonedas según su capitalización

en el mercado; mientras mayor sea la capitalización, menor riesgo existirá al adquirir una moneda. Una estrategia en general puede ser tener las top 3, top 5, top 10 o hasta top 20 de criptomonedas en ciertos porcentajes en el portafolio. Mientras más monedas de menor capitalización tengas en el portafolio, mayor riesgo estarás asumiendo. Por otro lado, existe mayor oportunidad si éstas crecen y multiplican su precio varias veces. En la página web www.iconomi.net puedes encontrar ejemplos de portafolios, ahí puedes comprar participaciones en portafolios ya estructurados e incluso crear y publicar tu propio fondo de criptomonedas al público y así generar

ingresos a través de las comisiones que paguen los inversionistas de tu fondo.

En la estrategia de Buy and Hold se recomienda tener tiempo y no depender en el corto plazo del dinero invertido; debido a la volatilidad del mercado el portafolio de monedas que adquieras puede perder valor en poco tiempo y tendrías que esperar hasta que el mercado se recupere para no vender con pérdida. Hay personas que compraron bitcoins en 1.000 USD a finales del 2013, después la moneda bajó a 200 USD, y cuatro años después, en 2017, pasó otra vez los 1.000 USD para llegar a 20.000 USD. Las personas que invirtieron a largo plazo obtuvieron

ganancias a pesar de la caída.

Minería (POW)

La minería ha sido una de las primeras opciones para generar ingresos con criptomonedas y la rentabilidad que genera es parte esencial para que funcione su sistema descentralizado. Mientras este proceso genere un beneficio económico, más personas invertirán en hardware y energía, de esta forma la red de blockchain se mantiene activa y segura. En este capítulo analizaremos la rentabilidad de la minería como inversión.

Principalmente existen tres opciones para minar: minería propia, pools de minería o cloud mining

(minería en la nube).

Minería propia

En la minería propia el inversor adquiere y administra sus equipos personalmente, en su casa o en un espacio preparado para ese fin. Para calcular la rentabilidad de este tipo de minería hay que analizar el costo de los equipos y sobre todo el costo de la energía eléctrica que se consume. También hay que tener en cuenta que la minería con equipos ASIC genera ruido y calor, por lo que no es conveniente ubicarlos en la sala de la casa, sino en un lugar adecuado para ello. Factores como el costo de la energía eléctrica y el calor que genera la minería, hacen

que los mineros se enfoquen en armar sus granjas en países con costos de energía y temperaturas bajas para ahorrar el consumo de energía en el enfriamiento de las máquinas. Además de los equipos también se requieren conocimientos técnicos para poder operar la granja.

Existen tres equipos con cuales se puede minar criptomonedas:

CPU (PC o laptop)

En los primeros meses desde la creación de Bitcoin los mineros usaron sus computadoras caseras para minar y ganar la recompensa por bloques resueltos. Al no existir mucha competencia, de vez en cuando cada uno

de los participantes encontraba un bloque y ganaba 50 monedas bitcoin. Hoy en día lo más probable es que nunca logres resolver un bloque y generar la recompensa usando la capacidad computacional de un CPU, ya que el algoritmo de Bitcoin se está haciendo cada vez más complejo y la competencia se multiplicó, por esto los equipos que se usan actualmente tienen mayor capacidad computacional.

GPU (Tarjetas gráficas)

El uso de tarjetas gráficas para la minería de criptomonedas puede ser rentable en algunos casos. Las tarjetas son muchas veces más rápidas que un CPU. Minar bitcoins de esta forma ya no

es rentable, sin embargo hay varios altcoins que vale la pena minar con GPUs. Es importante que en el momento de la compra adquieras los modelos más recientes y rápidos para que puedan trabajar durante unos meses con ventaja sobre otros mineros que usan modelos anteriores.

ASIC (Application-Specific Integrated Circuits)

Las máquinas de minería ASIC (circuito integrado para aplicaciones específicas) se desarrollan especialmente para la minería de criptomonedas y no pueden hacer otra cosa más que minar, generar hashes. Los ASIC miners más nuevos logran generar giga y hasta terahashes;

es decir, mil millones de hashes por segundo. En el caso de Bitcoin es la única forma de minar rentablemente.

Mining pool

Actualmente, minando desde la casa con sólo algunas máquinas es casi imposible que encuentres un bloque con la capacidad de minería que se puede instalar en el hogar. Por eso existen los "pools de minería" en los cuales puedes conectar tus máquinas a un grupo –pool– de otras máquinas y juntos resolver los bloques. En el momento de tener éxito, recibes la parte de recompensa que corresponde a la participación que tienen tus máquinas en el pool.

Cloud mining

El cloud mining (minería en la nube) brinda la opción de adquirir máquinas de minería GPUs o ASIC sin instalarlas en tu propio hogar y manejarlas por tu cuenta, invirtiendo en el hardware y la infraestructura que una empresa está manejando en sus propias instalaciones. Estas empresas buscan por lo general países en cuales el costo de energía es bajo y las condiciones climáticas no requieren gastos altos en enfriamiento. Islandia es uno de los países, aparte de China, en donde más operaciones de minería hay. Se dice que la mitad de la energía que produce Islandia se usa en operaciones de minería.

Las empresas de cloud mining

permiten hacer la compra de cierta cantidad de poder de minería y de esta forma participar en sus resultados. De las monedas que ganan ellos descuentan el costo de energía, mantenimiento, espacio y un fee por manejar esta operación. La diferencia va a la cuenta del inversor. Al comprar equipos en grandes cantidades consiguen buenos descuentos con los productores, lo que puede favorecer la rentabilidad.

Los modelos de cloud mining se distinguen en los diferentes contratos que ofrecen. Una forma es ofrecer rentabilidad por un número de días y una cantidad de hash-power determinado. Otra opción son contratos de por vida,

que se refieren a la vida útil de las máquinas contratadas, no a la vida del comprador. Todas las empresas serias tienen una cláusula en sus contratos que indica que la minería deja de pagar rendimientos al comprador cuando ya no es rentable; es decir, cuando el costo de mantenimiento y energía supera los rendimientos obtenidos. Si eso ocurre la minería deja de producir y se termina el contrato automáticamente. Esto significa que tienes que confiar en la compañía para que no corten los pagos mientras ellos siguen minando con el hardware pagado por ti para su propio beneficio.

¿Es rentable invertir en minería?

Para saber si la minería es una inversión

rentable existen muchas variables que juegan un rol importante en los cálculos. La rentabilidad de la minería se calcula sumando la recompensa de nuevas monedas y costos de transacción que recibe el minero, descontando la inversión en hardware, energía, mantenimiento y arriendo de espacios. La fórmula sería: Ganancia = (Monedas minadas X precio de moneda) - costo de hardware - costo de energía, mantenimiento y espacio.

Aunque a muchas personas les fascina la idea de invertir en minería y la promueven como una forma de "imprimir" tu propio dinero en casa, la realidad muestra que no se han cumplido

siempre las expectativas. Claro, si en 2009 y 2010 hubieras puesto tu PC de 1.000 USD a minar y hubieras minado unos 1.000 bitcoins que vendiéndolos siete años después en 20.000 USD cada moneda, hubieras generado 20 millones de dólares con una inversión de 1.000 USD en hardware y algo de electricidad. ¿Suena genial verdad? Ahora, ¿qué pasa si en el mismo tiempo hubieras comprado bitcoins con 1.000 USD? El mismo valor que ha costado la compra del hardware. Los bitcoins costaron un promedio de 10 centavos y hubieras adquirido 10.000 bitcoins con la misma inversión. Vendiéndolos en 2017 en 20.000 USD hubieras generado 200 millones de USD. ¿La minería ha sido

rentable en este caso? Claro que sí. Sin embargo, comprar bitcoins directamente hubiera generado mayor rentabilidad aún. La verdad es que comprar criptomonedas y guardarlas durante algunos meses o años en muchos casos te hubiera generado una mayor rentabilidad a través de la revalorización que invertir en equipos de hardware para minar. La meta de un inversor en minería es que la minería genere más monedas de lo que tuvo que invertir. Es decir, si hoy se invierte un bitcoin en máquinas, se espera que la máquina produzca más de un bitcoin en rentabilidad a lo largo de su vida útil.

La minería de criptomonedas

desde el punto de vista financiero tiene dos grandes retos y varios componentes que juegan un rol importante para dictaminar si es rentable o no:

Primero: el tiempo de recuperación

Actualmente hacen falta meses y hasta años para recuperar el valor invertido y llegar al punto en que realmente se genere una rentabilidad. Ejemplo: si inviertes 1.000 USD en hardware y generas un 10% de rentabilidad mensual, necesitas ganar durante diez meses para llegar al punto en que recuperas la inversión y realmente obtienes una rentabilidad neta, y eso si hacemos el cálculo en moneda fiat; muchas veces es peor si calculamos en

criptomonedas. Por ejemplo, si invertiste 1 bitcoin en minería en enero de 2017, cuando equivalía aproximadamente a 1.000 USD, y obtuviste el 10% de rendimiento mensual (100 USD), al final del año 2017 hubieras generado 1.200 USD; recuperando los 1.000 USD invertidos y obteniendo una ganancia de 200 USD. Pero si hubieras comprado un bitcoin en enero 2017, en 1.000 USD, hubieras tenido una moneda a finales de 2017 en casi 20.000 USD. La ganancia hubiera sido de 19.000 USD, en vez de los 200 USD que hubieses obtenido con la minería. También si hubieras generado 100 USD mensuales en bitcoins y las hubieras guardado hasta finales del año,

hubieras tenido una muy pequeña fracción de bitcoin y no hubieras ni siquiera recuperado la moneda entera invertida inicialmente.

Segundo: el avance tecnológico

La tecnología avanza constantemente, sobre todo en el caso de la minería, en donde el hardware produce dinero y se genera un negocio de billones de dólares para los productores de equipos. El hash-power de la red –Difficulty– sube con pasos gigantes y casi cada semestre entra una nueva generación de equipos de minería ASIC o tarjetas gráficas al mercado –más potente que la versión anterior, que consume menos energía y cuesta menos dinero. Eso quiere decir

que si compras hoy un minero ASIC, probablemente durante los primeros meses te va a dar buenos resultados, pero cada mes la cantidad de monedas producidas se reduce y cuando entren las nuevas versiones de hardware al mercado la máquina dejará de ser rentable y tendrás que apagarla. La única forma de ganar esta guerra de hardware es seguir comprando los nuevos modelos y seguir aumentando el poder de minería, guerra difícil de ganar minando en casa o aportando a un pool.

Si quieres calcular la rentabilidad de minería con tus propios números puedes hacerlo en las siguientes páginas web:

www.bitcoinx.com/profit/
www.cryptocompare.com/mining/calcu

La conclusión es que se debe analizar muy bien y contemplar varios factores para saber si una inversión en minería es rentable. Si se realizan cálculos en moneda fiat se puede obtener una ganancia al final, dependiendo también de la valorización de la moneda. Sin embargo, haciendo cálculos basados en cifras de años pasados, la valorización de las criptomonedas hizo que comprar y mantenerlas en una billetera, el Buy and Hold, haya sido la mejor opción.

Staking (PoS)

El staking, o PoS (Proof of Stake), es

una forma de crear consenso en una cadena de bloques. En esta parte analizaremos qué tan rentable es el staking como forma de generar ingresos pasivos con criptomonedas. Para hacer staking sólo se necesita cierta cantidad de monedas en una core wallet que trabaje con este algoritmo para crear consenso. Mientras más monedas se tienen, mayor rentabilidad se puede generar. Lo interesante del staking es que la única inversión que tienes que hacer es la compra de las monedas y no se requiere de hardware en especial, como es el caso de la minería. Eso quiere decir que no hay tiempo de recuperación de la inversión ya que siempre se tendrán las monedas

adquiridas y en cualquier momento se pueden vender.

Existen 3 opciones para participar en el staking:

Primero: staking en tu propia billetera

Para hacer staking en tu propia billetera tienes que descargar la core wallet de la moneda, instalarla en la PC o laptop, tenerla sincronizada –descargar toda la blockchain–, transferir las monedas a la wallet y ponerla en modo staking. Hay que tener en cuenta que la wallet debe estar conectada a internet las 24/7. Lo bueno es que este proceso no requiere de muchos recursos en energía o internet; puedes usar una computadora antigua que siempre esté encendida.

Sólo tienes que esperar que lleguen las nuevas monedas. Este proceso, dependiendo de la moneda y la cantidad que se tengan, puede demorarse horas, días hasta semanas.

Segundo: staking en un pool

Como el staking trae mayores beneficios mientras más monedas están en una billetera, se han creado pools de staking en los que se unen las monedas de varias personas en una sola dirección y después se reparte la ganancia entre todos según la cantidad aportada. La ventaja es una rentabilidad mayor dada la alta cantidad de monedas que participan en la billetera común. Por otro lado, el servicio tiene un costo que

debes considerar, y mientras participas en el pool las monedas están en manos de un tercero y no en tu poder. Algunos pools de staking son: www.cryptostakingpool.com o www.stakinglab.io (¡Enviar monedas a estas plataformas es bajo tu entera responsabilidad!)

Tercero: staking en un exchange

Hay ciertos exchanges que reparten las monedas que fueron generadas a través del staking mientras las tienes en un exchange. Si quieres tener este beneficio tienes que investigar que exchange ofrece esta participación y con qué monedas. Un ejemplo es NEO. Si tienes NEO el staking te genera GAS, puede

ser en la billetera propia de NEO o en los exchanges binance.com o kucoin.com; si tienes NEO en estos exchanges te acreditan GAS por mantenerlos ahí.

¿Es rentable el staking?

La pregunta ahora es qué tan rentable es hacer staking con las criptomonedas. Unas monedas conocidas para hacer staking son: NEO, PIVX, ReddCoin, Lisk, Tron, Stellar, Stratis... etc. Existen muchas más, la mayoría entra en el grupo de las shitcoins; algunas prometen una rentabilidad del staking de más de 1.000% anual, sin embargo sus precios están bajos y caen cada vez más porque no tienen un proyecto que les de un

sentido que no sea la generación de más monedas que no tienen uso. Las monedas que sí tienen proyectos, como las nombradas anteriormente, generan dependiendo de la cantidad de monedas que uno mantenga, una rentabilidad alrededor del 5% anual (NEO, PIVX, ReddCoin, Lisk, Tron); Stratis 1,5%; Stellar 1%.

El staking es una inversión interesante, sobre todo cuando el mercado sube, porque aparte de ganar por el aumento en valor de las monedas, también se ganan monedas. Por otro lado, las monedas que ofrecen rentabilidades muy altas por el staking son en su mayoría shitcoins, y mientras

duplicas su cantidad en la billetera éstas pierden valor. Si tienes algunas monedas que usan PoS en tu portafolio aprovecha la rentabilidad que puedes generar en nuevas monedas haciendo stacking en una billetera propia o en un exchange. En esta página web puedes revisar los niveles de riesgo y las rentabilidades de monedas PoS: www.stakingrewards.com.

Algunas monedas interesantes que actualmente usan el algoritmo de PoW tienen planificado cambiarse a PoS. Mantente al tanto de las noticias sobre esta forma de generar consenso y rentabilidad.

Masternodos (MN)

Los MNs son una forma de staking.

Técnicamente un MN brinda a sus usuarios la oportunidad de ofrecer pagos instantáneos y anónimos, como en el caso de DASH, la primera moneda que implementó este sistema. Un dueño de MN tiene que vincular cierta cantidad fija de monedas desde la core wallet a un servidor y ponerlas a disposición de la red, a cambio recibe nuevas monedas de recompensa, como un minero. Hoy no sólo DASH usa este sistema, sino varias monedas más.

Requerimientos técnicos

Para hostear un MN, en primera instancia se debe averiguar cuántas monedas se requieren para hacerlo. En el caso de DASH son 1.000 monedas

que deben estar en la core wallet. Después tienes que vincular la cantidad de monedas que requiere el MN a un servidor. Las monedas no salen de la billetera y siempre están 100% bajo el poder del propietario. Puedes usar un servicio de hosting como www.vultr.com para alquilar un espacio en un servidor en la nube que está conectado 24/7. El proceso exacto para activar un MN puedes encontrarlo en la página web de la moneda, a través de tutoriales en Youtube o descripciones en foros. Una vez montado el MN en tu core wallet empiezas a generar rendimientos.

Rentabilidad

La rentabilidad que puede generar un

MN depende de dos factores. Uno es la cantidad de monedas que reciben los dueños del MN por bloque y el otro es el desarrollo del precio de la moneda. En DASH se requieren 1.000 monedas para el MN; a un precio de 100 USD por moneda se deben invertir 100.000 USD para adquirir la cantidad necesaria. A un precio de 1.000 USD por moneda ya sería un millón de USD. El monto a invertir depende entonces del precio de la moneda y la cantidad requerida. Existen otras monedas que requieren inversiones de entre 1.000 y 10.000 USD para adquirir la cantidad suficiente para ser dueño de un MN. Cada moneda con MN define el porcentaje de la recompensa por bloque que corresponde

a sus dueños, en el caso de DASH es el 45%. Por ejemplo, si la recompensa son 3 DASH por bloque el dueño del MN recibe 1,35 monedas cada vez que le corresponde. El tiempo para recibir la recompensa depende de la cantidad total de MNs activos; con 5.000 nodos activos y un tiempo de bloque de aproximadamente 2,5 minutos, ganarías una recompensa cada 8 ó 9 días. En el caso de DASH eso equivale a una rentabilidad anual de más o menos un 6%.

Ventajas

Una de las ventajas de los MNs está en el bajo costo de mantenimiento mensual, ya que un servidor en la nube cuesta de

3 a 10 USD por mes y no es necesario tener el equipo encendido las 24/7 como en el staking. Además tienes siempre todo el control sobre tus fondos y puedes vender las monedas en cualquier momento y dejar de operar como MN. Tampoco corres el riesgo de que tu hardware vaya a ser obsoleto o se requiera de un tiempo de recuperación de la inversión, ya que siempre tendrás las monedas adquiridas inicialmente; es decir, la rentabilidad empieza con el primer pago que recibes. Otra ventaja es que puedes generar rentabilidad tanto por nuevas monedas como por la valorización. Por ejemplo: si compraste 1.000 DASH a inicios de 2017 a un precio de 12 USD por moneda, tuviste

que invertir un total de 12.000 USD para completar un MN; a un precio máximo de 1.500 USD en diciembre del mismo año, el MN valía 1,5 millones de USD. Una increíble revalorización.

Desventajas

El costo inicial por la compra de monedas puede ser muy alto, no todos tienen el capital para comprar la cantidad de monedas necesarias. Si sólo se tiene una parte de las monedas requeridas existe la opción de participar en un pool. En este caso se pierde el control sobre los fondos, porque alguien más va a montar el MN en su billetera. Lo que también se debe tener en mente al escoger una moneda para un MN es

que la gran mayoría de las que ofrecen esta opción son shitcoins, no tienen ninguna función fuera de ser una moneda de MN y eso obviamente no contribuye para que el precio sea estable y gane valor. Se pueden encontrar MNs que ofrecen varios cientos por ciento de rentabilidad al año, sin embargo el precio en los exchanges puede caer drásticamente al intentarse vender la moneda, porque hay bajo volumen y poca demanda; de esa forma se podría perder mucho dinero si no se logra vender a tiempo.

Para más información de inversiones en MNs recomendamos revisar estas páginas informativas sobre

los rendimientos y estadísticas (hay que revisar varias fuentes porque no siempre están actualizadas):

www.masternodes.pro (ingl.)
www.masternodes.com (ingl.)
www.masternodes.online (ingl.)
www.masternodo.com (esp.)

Trading

El trading es la compra y venta de acciones, futuros, commodities, divisas o criptomonedas en una casa de cambio o exchange. En el mercado de criptomonedas se ha puesto de moda tradear bitcoins o altcoins para generar una rentabilidad y ganarle al mercado. Una de las razones de que el trading de criptomonedas se haya vuelto popular incluso entre traders de mercados

financieros tradicionales, es la volatilidad del mercado, ya que una alta volatilidad genera una mejor oportunidad para el trader que un mercado lateral; es decir, un mercado sin mucho movimiento.

Aunque el trading se incluya aquí, en la parte de las inversiones en criptomonedas, más que inversión se trata de especulación. Un inversionista invierte en una criptomoneda a través del Buy and Hold por razones fundamentales, y lo hace por lo general a mediano o largo plazo. Por otro lado, un trader basa sus decisiones de compra y venta en la especulación, realizando un análisis técnico de los charts de

movimiento de las monedas. El trading tiene como meta generar rentabilidad sin tener que trabajar físicamente, aunque es una actividad o un trabajo que requiere la atención diaria del trader, y su conocimiento. Dependiendo del tipo de trading los plazos de especulación son diferentes:

Position trader: Operaciones de semanas a meses.

Swing trader: Operaciones de días a una o dos semanas.

Day trader: Operaciones de pocas horas a pocos días.

Scalp trader: Operaciones de minutos a una o dos horas.

Para hacer trading necesitas una

cuenta habilitada en uno de los exchanges de criptomonedas como Bitmex, Binance, Bitfinex, Bittrex etc., y unos satoshis de bitcoin. Como ya hemos mencionado, es importante tener en cuenta que la mayoría de las casas de cambio son instituciones centralizadas que manejan tu clave privada de las monedas. Por eso debes pensar muy bien cuánto capital quieres mantener en cada una de estas plataformas para manejar tu riesgo.

Manejo de riesgo

Existen algunas medidas que puedes aplicar para disminuir el riesgo de pérdida de los fondos al hacer trading. Una de ellas es la diversificación en

varias operaciones y monedas; es decir, usar sólo una pequeña parte del capital en cada operación. Otra medida es trabajar con varias plataformas de trading y guardar los fondos diversificados entre ellos. Ya hemos mencionado varias veces la seguridad de los exchanges y que si hay un ataque contra uno, no pierdes todo el capital – como ha pasado en el caso de Mt. Gox, si lo tienes diversificado. Es recomendable activar el uso de seguridad de autenticación con el Segundo Faktor (2FA) para acceder a las cuentas en exchanges o hacer retiros. Todas las plataformas serias de trading ofrecen esta opción y lo más recomendable es usarla, si no quieres

estar expuesto a que terceros accedan a la cuenta y puedan robar los fondos.

Dos recomendaciones con respecto al uso del 2FA: primero, siempre respaldar el QR de acceso al autenticador de forma impresa junto con el MasterKey para poder recuperarlo en caso de pérdida del dispositivo móvil; segundo, usar un dispositivo móvil sólo para guardar la APP del autenticador y no conectarlo a la red con chip o wifi. Una vez instalado el autenticador funciona sin internet.

Como éste no es un libro sobre trading no vamos a profundizar demasiado, sin embargo queremos compartir contigo algunos

conocimientos básicos sobre trading que t e ayudarán a realizar las primeras transacciones para aprender. Un trader basa las decisiones de operación en la especulación y en el análisis técnico del chart. Un chart muestra en sus dos ejes el tiempo y el valor de un activo. El valor es representado por las "velas japonesas" en verde y rojo que permiten identificar el precio al que se apertura un intervalo de tiempo (1 minuto, 10 minutos, 1 hora, 1 día…) y a qué precio se cierra. Dependiendo del color que tiene sabemos si el intervalo se cerró a un precio mayor (verde) o menor (rojo) que el intervalo anterior.

Diferentes tipos de análisis

Análisis técnico

El análisis técnico se basa en el análisis de los movimientos de la cotización de una moneda; es decir, en los movimientos en el chart o las velas. Hay muchos indicadores y análisis estadísticos y gráficos que se pueden aplicar para analizar las probabilidades de subir o bajar de una moneda. Para un trader ésta es la herramienta de análisis más importante para realizar su trabajo.

Análisis fundamental

El análisis fundamental se concentra en los datos técnicos y económicos de una moneda que pueden brindar información sobre su futuro. Lo que se busca es identificar un valor real de la moneda en

el futuro con todos los desarrollos y proyectos planificados. El análisis fundamental es mayormente utilizado por los inversionistas para tomar decisiones sobre la adquisición de una moneda. Las mayores fuentes de información para este análisis son el whitepaper, la página web de la moneda, las redes sociales y páginas de noticias.

Formas de trading

Long position

El long trading es la forma más común del trading y significa que un trader compra una moneda porque piensa que su valor sube. Es decir, la compra a un valor bajo y la vende a un valor más alto, quedándose con una rentabilidad.

El tiempo entre la compra y la venta puede ser de unos pocos minutos, horas, días, semanas o meses, dependiendo del estilo de trading que se aplique, como vimos anteriormente.

Short position

En un "short" el trader especula que un activo va a perder valor. Por eso lo pide prestado a cierto precio con la intención de recomprarlo más barato. La ganancia se genera con la depreciación del activo. Por ejemplo el trader abre un short de bitcoin a un precio de 10.000 USD y lo cierra cuando baja a 9.000 USD. En este caso genera una ganancia de 1.000 USD. Eso quiere decir que un trader puede ganar en mercados alcistas

–Long position– y bajistas –Short position–.

Margin trading

En el Margin trading el trader puede pedir prestados fondos a otros usuarios o al exchange mismo, que maneja grupos de inversión que prestan su dinero a cambio de intereses, y con eso generar mayores ganancias. En español se habla de "palanca" o "apalancamiento" (Leverage). En casas de cambio como Bitfinex, Deribit o Bitmex se permite el apalancamiento hasta cierto factor. Por ejemplo, si se elige el factor 10 entonces las ganancias y también las pérdidas se multiplican por este factor; si el mercado sube 1%, el trader gana 10%,

si baja 1% hay una pérdida del 10%. El Margin trading es una herramienta para traders experimentados ya que el riesgo aumenta.

Arbitraje

El Arbitraje es una forma de trading en el que se aprovecha una diferencia en el precio de un mismo producto, acción o moneda entre diferentes exchanges. Mientras en los mercados tradicionales el arbitraje se ha vuelto muy difícil debido a que los robots y el trading automatizado casi no permiten que se creen diferencias en los precios, en el mercado de criptomonedas aún existen estas diferencias. Sobre todo cuando hay un día con muchos movimientos en el

mercado, lo que se hace es vender una moneda a un precio alto en un exchange y pasar los dólares a otro exchange donde la misma moneda cotiza más bajo para recomprarla. Esta transacción tiene que realizarse rápido y con un volumen de monedas considerable para que se asuman los fees de venta y de compra, más el costo de traspaso. Existen bots en el mercado que pueden hacer estas transacciones y si son bien programados también obtienen buenos rendimientos. Lo que hay que analizar son las cantidades que se requieren para que sea rentable, ya que los márgenes de diferencia en precio pueden ser muy pequeños.

Después de conocer las diferentes opciones de trading, a continuación vas a conocer unos términos importantes que se usan dentro del ambiente de trading:

Los toros y osos

En la bolsa existen dos animales que caracterizan un mercado alcista –mercado a la subida– o un mercado bajista –precios a la baja–. El oso (bear) caracteriza el mercado a la baja porque jala con sus garras los precios hacia abajo; el toro (bull) representa un mercado alcista en el que los precios suben porque el toro alza el mercado con sus cuernos.

Stop loss

El Stop loss es una herramienta del trading con la que se puede programar un valor para el cierre de una operación. De esta forma se pueden evitar pérdidas grandes. Por ejemplo: haces un trade con una Long position –esperas que la moneda suba–, y al mismo tiempo colocas un Stop loss para el caso de que baje un 5%. De esta forma puedes estar tranquilo de que cuando tu análisis no te lleve al resultado esperado, no vas a perder más del 5% de tu inversión.

Lending

Si prestas monedas a otros traders puedes generar una rentabilidad por el préstamo. Este proceso se llama "Lending", y está disponible en Bitfinex

o Poloniex. Lo que se debe hacer es definir el interés que se quiere cobrar y el tiempo que se está dispuesto a prestar las monedas. Ésta es una forma muy segura de generar rentabilidad, el único riesgo que existe es que las monedas están en un exchange en manos de terceros y si ocurre un hackeo se podrían perder.

Exchanges descentralizados

Las casas de cambio que hemos nombrado arriba, como Bittrex, Binance o Bitmex, tienen algo en común: son centralizadas. Las claves privadas están en sus manos y eso implica un riesgo para tus monedas, aunque a un nivel bajo, debido a la confianza generada por

esas empresas. Hoy ya existen los primeros exchanges descentralizados "DEX" en los cuales nunca se entregan las monedas a un tercero, sino que las transacciones se realizan directamente Peer-to-Peer, de persona a persona. Aunque todavía no son muy conocidos, creemos que ahí está el futuro. Algunos ejemplos de DEX son:

www.bitshares.org
www.nxtplatform.org
www.ddex.io

Trading bots

En los mercados tradicionales como Forex, existen ya bots que automatizan los procesos de compra-venta. Estos bots trabajan con ciertos algoritmos y

son más rápidos que los seres humanos, de forma que se hace difícil ganarles en los mercados. En el mercado de criptomonedas también existen bots que prometen generar ciertos rendimientos en automático. Lo que hay que tener en cuenta al trabajar con bots son principalmente dos cosas: primero hay que cubrir un costo mensual para pagar el software, esto significa que la ganancia se reduce por el servicio; y segundo se debe analizar la seriedad y la constancia. Muchos funcionan bien cuando el mercado sube pero ponen en riesgo tu capital cuando el mercado está a la baja. A fin de cuentas estás poniendo tu capital en manos de un tercero y puede pasar que se "queme" tu

cuenta y el capital vaya a cero si el mercado no ha sido tan previsible para el bot. Los bots usan algoritmos que pueden funcionar durante un tiempo y puede suceder que después de cierto tiempo de uso estos ya no funcionen.

También debemos preguntarnos por qué una persona que desarrolla un bot que trabaja bien lo quiere alquilar, arriesgándose a que demasiadas personas usen el mismo algoritmo para realizar trading y bajen las ganancias para todos; es decir, los mejores bots normalmente no entran al mercado público para que cualquier persona los pueda adquirir.

Dentro de las opciones de

inversión en criptomonedas el trading es una de las que más riesgo implica, ya que estamos hablando más de especulación que de inversión. También el trading requiere un trabajo de muchas horas en la ejecución y aún más en el aprendizaje; el tiempo que hay que dedicar para convertirse en trader profesional es mucho y hay que tenerlo en cuenta si realmente queremos alcanzar buenos resultados. Con menos riesgo y menos inversión de tu tiempo puedes hacer otros tipos de inversión que ya hemos explicado anteriormente.

Otras opciones de inversión en criptomonedas

ICOs

Si tienes interés en invertir en ICOs como parte de un portafolio, debes tener en cuenta que es la forma más especulativa de invertir en la criptoeconomía. Existe un alto riesgo y por otro lado también una gran oportunidad de generar una alta rentabilidad. Para bajar el riesgo es recomendable hacer varias inversiones pequeñas en diversos proyectos y no una inversión grande en uno sólo; si quieres invertir el equivalente a 1.000 USD

mejor es buscar 10 ICOs y colocar 100 USD en cada una que invertir la cantidad completa en una sola. Entre todas tus inversiones en criptomonedas no más del 20% debería estar en ICOs. Finalmente debes tener claro que estás invirtiendo en un proyecto que en la mayoría de los casos todavía no es rentable y cuyo éxito depende de muchos factores internos y externos. El valor real de un token ofrecido durante la fase de la ICO, sólo se puede ver cuándo empieza a cotizar en los exchanges y la oferta y demanda del mercado fija un precio. Muchos ICOs entraron al mercado y después de un PUMP en las primeras horas sus precios cayeron porque muchos inversores vendieron sus

tokens comprados inicialmente a precios bajos para realizar ganancias. Esto sucede cuando hay muchos beneficios al comprar los tokens durante la ICO con descuentos altos y bonos extras. La tentación de vender es muy alta en este caso, pues el precio del mercado es mucho mayor que el precio de compra inicial.

Como inversor en una ICO debes estudiar bien el whitepaper del proyecto y analizar su potencial de éxito basándote en las cinco claves de éxito de una ICO, descritas en un capítulo anterior. Si inviertes en etapas tempranas en una ICO, recibes más tokens a menor precio; por esto es

importante revisar las diferentes rondas de inversión, como la Pre-ICO o venta privada que permite recibir más beneficios.

En resumen, se puede decir que las ICO van a continuar siendo parte fundamental del mundo blockchain, no se puede subestimar el impacto que han tenido en cuanto a la posibilidad que están dando para financiar fácilmente proyectos realmente innovadores y disruptivos. Dicho esto, no hay duda de que las ICOs pueden ser una alternativa de inversión muy interesante que brindan la oportunidad de generar importantes retornos en un futuro, sin embargo en la mayoría de los casos los resultados son

inciertos. Si decides invertir en una ICO, es vital actuar responsablemente –dejando de lado la avaricia– y estudiar a profundidad el proyecto.

Futuros, ETFs, Fondos de inversión

Hasta el momento muchas personas no han invertido en criptomonedas directamente porque no entienden la tecnología y no tienen el conocimiento de cómo y dónde comprarlos. Los inversionistas pequeños están acostumbrados a que sus inversiones se manejen a través de un asesor en un banco o un broker que se encarga de todo y por eso cobra una comisión. Cuando escuchan que en las criptomonedas hay que manejar claves

privadas y que la pérdida de las mismas significa la pérdida de fondos, o las noticias de plataformas de trading hackeadas, se asustan y prefieren no invertir. La creación de productos financieros tradicionales para el mercado de criptomonedas puede ser el próximo gran paso para la adaptación masiva y la apertura al mercado financiero global. A muchos entusiastas de primera hora de la criptoeconomía no les gusta la idea de que las monedas se vinculen al mercado financiero global. La idea inicial de Satoshi Nakamoto ha sido la de crear un nuevo ecosistema fuera de la manipulación y el poder de los grandes actores de la economía global, sin embargo es muy probable

que estos mismos actores de la economía tradicional creen sus productos propios relacionados con criptomonedas, lo que de hecho ya está pasando.

Los primeros futuros de Bitcoin entraron a la Bolsa de Chicago a finales de 2017 y se vencieron en enero de 2018. Este primer producto tradicional en la bolsa seguro tuvo un efecto en el desarrollo del alza del precio del bitcoin a finales de 2017 y también en la corrección que empezó en enero de 2018.

¿Cómo funcionan los futuros?

En los futuros se crea un contrato en el cual una persona A se compromete con

una persona B a comprarle o venderle bitcoins a un precio fijo en el futuro. Si la persona A quiere comprar la moneda a un precio acordado en el futuro, la persona B tiene una ganancia cuando el mercado baja y según el contrato vende sus monedas al precio más alto establecido. En el otro caso, si sube la moneda, la persona A gana porque compra el bitcoin más económico al momento del vencimiento del contrato.

Otro producto del mercado tradicional que se quiere desarrollar para las criptomonedas son los ETF (Exchange Traded Funds). En los años 2017 y 2018 había mucha especulación y varios intentos de crear el primer ETF

para bitcoin y las criptomonedas. Un ETF es un fondo de inversión que se negocia en la bolsa y que refleja el precio de un índice, como por ejemplo el S&P 500 (Standard & Poor's 500: las 500 empresas más grandes de EE.UU.), de forma pasiva. En el caso del bitcoin, un ETF podría reflejar el precio bitcoin vs. dólar. Técnicamente eso no es un problema, sin embargo autoridades como la SEC (la autoridad que regula las actividades en las bolsas de valores en EE.UU.), como respuesta a varios intentos de crear un ETF, indicaron que faltan regulaciones y que el mercado no está listo todavía. Un ETF atraería grandes sumas de capital, y con el volumen del mercado de criptomonedas

muy bajo todavía, esta atracción de capitales podría causar la creación de una burbuja que no tendría nada que ver con el desarrollo real de este mercado sino que sería sólo especulación. A diferencia de un fondo de inversión, los ETFs no requieren de managers que los administren activamente, y eso significa que las comisiones que cobran los brokers por mantener un ETF en tu portafolio son más bajas y por ende el comprador queda con más rentabilidad. Mientras que un fondo de inversión cobra alrededor del 3% anual en comisión para sus administradores, los ETFs sólo cuestan alrededor del 1%, o menos; esta diferencia, con una

estrategia a mediano y largo plazo puede significar grandes cambios en el resultado final de la inversión.

Aunque tiene un costo mayor, un fondo de inversión puede ser una buena opción para invertir en criptomonedas. Ya existen fondos de inversión que incluyen al bitcoin y otras criptomonedas en su portafolio. La idea es que el administrador del fondo siga cierta estrategia de inversión en diferentes activos y a través de su manejo logre obtener mejores resultados que el mercado, que no siempre funciona. Una ventaja de los fondos es la diversificación, pueden incluir diversas criptomonedas u otros activos y de esta

forma obtener un crecimiento más estable que no depende del valor de un sólo activo y su volatilidad.

Actualmente podemos observar la entrada de las instituciones de finanzas tradicionales a la criptoeconomía y eso significa que las inversiones en criptomonedas a través de futuros, fondos y ETFs van a estar al alcance de muchas personas, lo que traerá más liquidez y también especulación.

Si tienes interés en una de estas formas indirectas de inversión en criptomonedas, en primera instancia debes buscar un broker o un banco que ofrezca inversiones en futuros, ETFs o

fondos, y analizar los requisitos necesarios para invertir. También es importante analizar comisiones y calcular la rentabilidad real que se puede obtener.

Pirámides y Sistemas Ponzi

Al buscar diferentes formas de inversión en criptomonedas, seguro te encontrarás con propuestas y plataformas que ofrecen una inversión en este mercado a cambio de rentabilidades fijas o variables. Los participantes pueden generar ingresos con su propio capital o también invitando a otros inversionistas. Recomendamos analizar con mucho cuidado estas propuestas ya que muchas

veces al entregar tus monedas a un tercero para obtener rentabilidades altas a través de un plan de compensación, suelen resultar sistemas ponzi o pirámides.

Los sistemas ponzi y pirámides

El sistema Ponzi toma su nombre del italiano Carlo Ponzi, quien en los años 20 del siglo pasado inventó un sistema que ofrecía una rentabilidad de hasta el 100% en 90 días sobre el capital de sus inversionistas. Los inversionistas supuestamente invertían en cupones de respuesta internacional de correos, que eran raras después de la Primera Guerra Mundial y se podían vender dentro de EE.UU. más caros que en el exterior. Lo

que realmente hizo fue pagar a los inversionistas antiguos con el dinero de los inversionistas nuevos. El sistema se mantiene mientras cada vez más personas se unen al negocio. Cuando el crecimiento de nuevos inversionistas baja, no hay dinero para pagar y el sistema se cae dejando muchas personas sin sus ahorros. Hoy en día conocemos también el nombre de pirámides financieras, en las cuales las personas son incentivadas a involucrar a más personas en el sistema fraudulento, pagando altas comisiones por cada nuevo inversor vinculado a la pirámide. Al final ambos sistemas terminan con muchas personas perdiendo dinero, con amenazas y demandas, amistades rotas y

hasta muertos.

Para que evites ser estafado en uno de estos sistemas te nombramos aquí diez características que tienen en común la mayoría de estos sistemas y que te ayudarán a identificarlas:

1. Ganancias fijas

La propuesta de pagar una rentabilidad fija a diario, semanal o mensualmente por medio de inversiones en minería o trading es muy arriesgada, porque el mercado de criptomonedas es muy volátil en sus rendimientos y es difícil poder predecir cuáles serán las rentabilidades exactas. Comprometerse a pagar ciertos valores fijos puede causar que la compañía no genere lo que

esperaba y se quede sin fondos para poder seguir pagando. Esto no quiere decir que el mercado de criptomonedas no puede generar rentabilidades superiores al mercado financiero tradicional, aunque garantizar pagos fijos crea grandes riesgos.

2. Falta de evidencia

Es importante que la empresa pueda dar evidencias de sus actividades, aunque no es necesario revelar todas las operaciones que hace. Si una compañía dice que tradea o mina debe estar en la capacidad de mostrar que eso es cierto. Por ejemplo, en la parte de minería pueden ser granjas físicas que se puedan visitar o mostrar registros con su

nombre en la blockchain, con los bloques que han minado.

3. Ni dueños, ni oficinas

Ten cuidado cuando en la información pública de la empresa, como en la página web, no aparece el lugar donde está constituida o donde está operando. Aunque en la era digital no es necesario tener infraestructura corporativa física en grande, tener un país de constitución sí lo es, porque muestra que se está cumpliendo con cierta regulación. Hay una diferencia entre una compañía que está regulada bajo las leyes estadounidenses y una compañía constituida en la República de Vanuatu. También las compañías serias no tienen

problema en mostrar quiénes son los dueños y las personas legalmente responsables del proyecto.

4. Criptomonedas no públicas

El tener su propia criptomoneda que no es pública es una forma de engañar a muchas personas. Si la compañía dice que tiene su propia criptomoneda y ésta no es pública, no tiene whitepaper, no la puede minar cualquiera o no cotiza en un exchange público, ni tiene una blockchain, entonces no cumple con las principales características de una criptomoneda real. Recuerda que una de las mayores ventajas de la criptoeconomía es la descentralización y el protocolo abierto (open source). Si la

moneda no cumple estas características debes tener dudas sobre la seriedad del proyecto y la compañía que la promueve.

5. Monedas preminadas

Cuando las monedas que usa y promueve la empresa son preminadas y la mayoría –más del 50%– la poseen los creadores, existe un gran riesgo de manipulación del mercado. Hay excepciones, sin embargo es un punto importante de analizar.

6. Monedas sin idea ni plan

Cuando una empresa promueve una moneda que no tiene otro uso o proyecto que pagar rentabilidades dentro del mismo sistema, hay que tener cuidado.

El valor de una moneda finalmente se va a crear a través del uso que se le pueda dar. Muchas monedas que incluso encontramos hoy en coinmarketcap.com no tienen función, ni equipo de desarrolladores detrás. Son monedas abandonadas que a mediano plazo van a ir hacia cero en su valor y van a desaparecer. Pagar rentabilidades en una moneda propia que sólo existe dentro del propio ecosistema de la empresa, pero que afuera de ella no tiene ningún uso, puede ser un indicio de un sistema fraudulento.

7. Aceptan dinero fiat como pago

Algunas compañías que dicen que trabajan con criptomonedas, sólo

aceptan pagos en dinero fiat para adquirir sus planes de inversión. Una compañía seria de criptomonedas acepta y paga en criptomonedas que están listadas en exchanges que permiten el intercambio en el mercado abierto. Lo peor es cuando una empresa tiene su propia moneda y ni ellos la aceptan como forma de pago.

8. Varios códigos a tu nombre

Otro indicio de que se trata de una pirámide es cuando puedes abrir varios códigos de inversión a tu nombre y armar tu estructura binaria o matricial en la red con tu propio capital. El fin de una red de mercadeo es que puedas distribuir servicios o productos a

clientes y de esa forma generar una comisión. Si con tu propio dinero creas códigos que te empiezan a pagar comisiones por tus propias compras, ten cuidado, es probable que estés en un sistema fraudulento que no va a sobrevivir en el tiempo, como muchos casos lo han demostrado.

9. 80/20 en reclutar

Cuando presentan la oportunidad y el 80% de la presentación la dedican a explicar cómo uno va a ganar dinero invitando a más personas al sistema y en la menor parte de la presentación explican los productos, servicios o el funcionamiento de la criptoeconomía, entonces puedes darte cuenta de que el

enfoque no son los productos o servicios que ofrece la compañía, sino la atracción de nuevos inversores con cuyos aportes pagan a los ya existentes. Recuerda que la mayoría de las personas no conocen las criptomonedas y una empresa que trabaja para el bien de sus inversionistas primero debe enfocarse en enseñarles sobre esta nueva tecnología en la cual se está invirtiendo.

10. Saldos internos

Algunas de las plataformas piramidales o ponzis manejan "saldos" en su sistema. De esa forma la empresa evita tener que pagar a sus inversores directamente, sólo acreditan "puntos" en

el backoffice que llevan un símbolo de $ y dicen que eso es la ganancia generada. Para cobrarlo la empresa no paga este valor al inversor, sino que para efectivizar hay que venderlo a un nuevo socio que quiere invertir; de esta forma el inversor antiguo sólo puede efectivizar su ganancia involucrando a otro incauto al sistema. Si no quieres invitar a más personas, no puedes cobrar. Esta herramienta se usa en muchas ocasiones para alargar la vida del sistema porque el pago y cobro es responsabilidad de cada socio. En este caso la empresa no requiere de liquidez para realizar los pagos.

Con estos diez puntos tienes una

buena referencia para analizar si una empresa es real o forma parte de la lista de sistemas ponzi o pirámides que están en circulación. Los negocios de Network Marketing o Redes de Mercadeo son una forma de distribuir servicios y productos, y seguro que hay empresas serias que trabajan en la criptoeconomìa y ofrecen una propuesta real. Vale la pena tomarse el tiempo para investigar antes de invertir. También existen páginas web que revelan malas empresas, monedas falsas y fraudes que puedes consultar durante tu investigación. Unas de ellas son www.behindmlm.com o www.badbitcoin.org.

Criptomonedas e impuestos

Las criptomonedas son relativamente nuevas y muchos países todavía no han definido claramente qué son y cómo declarar los beneficios económicos que se pueden obtener con ellas. Casi cada semana hay noticias nuevas sobre las formas de tributación en ciertos países. Por la rapidez de cambios y actualizaciones en esta parte y la sensibilidad del tema tributario decidimos no entrar en detalles en este libro.

Lo que primero tiene que suceder, paso a paso, en cada país o región, es lograr una definición clara de lo que es una criptomoneda, y con base en esta definición encontrar la forma de

tributación. Dos ejemplos de cómo se ha definido las criptomonedas son: Servicio Federal de Inspección Bancaria Europea (EBA): Bitcoin es un «reflejo digital de valor» o Internal Revenue Service (IRS) USA: «valor de capital».

Con criptomonedas se pueden generar rentabilidades de varias formas, como hemos analizado en capítulos anteriores. Por eso pueden darse diferentes tipos de impuestos dependiendo de cómo el inversor ha generado sus ganancias. Comisionar por gestionar una compra y venta, "comisión por servicio"; generar utilidad al comprar a precio bajo y vender a un precio mayor, "ganancias por capital";

estar involucrado en el proceso de la minería, “venta de producto generado”. Realmente depende de las definiciones de cada uno de los países y en este punto no hay nada generalizado. Lo que sí recomendamos es que te dejes asesorar por un experto en esta área en el país donde vives, porque no tributar e ignorar las normas fiscales te causará problemas legales.

Crea tu plan de inversión ahora

El éxito en las finanzas sólo se puede alcanzar cuando tienes metas claras y desarrollas un plan que conduzca hacia ellos. En este libro aprendiste sobre la

tecnología blockchain, las criptomonedas y cómo invertir en ellas. Si ahora puedes ver con claridad que esta nueva economía puede jugar un rol importante para llevarte a cumplir tus metas financieras, es momento de fijarlas y poner acción sobre los pasos del plan de trabajo que ayuda a cumplirlas. Queremos compartir dos herramientas de coaching que pueden ayudarte en este camino.

Primero: definir metas

Para definir tus metas usa el modelo SMART que indica que tu meta debe ser: Específica (**S**pecific), **M**edible, **A**lcanzable, **R**ealista y con fecha (**T**ime).

Por ejemplo: el 31 de diciembre de 2020 tengo un patrimonio equivalente a 250.000 USD en criptomonedas en mis billeteras. Esta meta cumple con los cinco elementos del modelo SMART.

También puedes proyectarte a tu Libertad Financiera. Por ejemplo: hasta el 31 de diciembre de 2021 tengo un portafolio creado de ocho diferentes activos que me producen ingresos pasivos de 5.000 USD mensuales y soy financieramente libre.

Escribe tu meta en un papel y revisa varias veces si realmente está cumpliendo con todos los elementos del modelo SMART, si no es así ajústala hasta que estés seguro de que es la meta

que quieres alcanzar. Después colócala en un lugar visible para que varias veces al día te recuerde a dónde quieres llegar.

Segundo: desarrollar un plan de trabajo

Una vez definida la meta el próximo paso es tener claridad de cómo alcanzarla. Para el desarrollo de tu plan te pueden ayudar esta serie de preguntas:

¿Que tan importantes es esta meta para ti? - (*Importancia 10 sobre 10, eso quiere decir que voy a dejar de hacer otras actividades menos importantes para enfocarme más en el cumplimiento de esta meta.)*

¿Dónde y con quién la vas a

lograr? - *(En la ciudad donde vivo junto con mi pareja.)*

¿Qué herramientas necesitas para poder lograrla? - *(Un plan bien estructurado, una billetera en frío para guardar de forma segura mis monedas, etc.)*

¿En quién te tienes que convertir para alcanzarla? - *(En una persona responsable, constante, disciplinada, etc.)*

¿Quién se beneficiará si logras la meta? - *(La familia, pareja, hijos, etc.)*

¿En qué momento sabes que la has alcanzado? - *(Al ver el valor que quiero alcanzar reflejado en la*

billetera.)

¿Cuáles son los pasos a seguir para lograrla?, ¿Qué tienes que hacer, hoy, cada día, cada semana, cada mes?

Con estas preguntas puedes definir tu plan paso a paso que te llevará a la meta. Mientras más minucioso lo desarrolles, más probabilidad de éxito tendrás. Ahora es tu momento de arrancar. Recuerda que el conocimiento no aplicado no te va a llevar a ninguna parte. Para recibir recompensas tienes que aplicar lo que aprendiste.

Para finalizar la parte de las finanzas es importante dejarte un descubrimiento que todas las personas que alcanzaron un alto nivel de riqueza

obtuvieron. El dinero en sí no crea la felicidad y la satisfacción, es más lo que puedes hacer con ello. El DAR tu dinero o invertirlo en alguien crea un alto nivel de felicidad y de satisfacción. Ten en mente que para recibir primero hay que DAR, y este hábito se aplica ganando 1.000 USD o 100.000 USD. Al DAR, el universo te regresa lo que has sembrado. La clave hacia una vida plena es la generosidad, pero también debes aprender a ser un buen recibidor de todos los regalos que este maravilloso universo te da; uno de los principales escollos para alcanzar las metas propuestas es no saber recibirlos y es muy común que la mayoría sienta malestar o incomodidad ante un regalo.

Ahora te pregunto: ¿si haces un regalo a alguien y éste no lo acepta, le darías nuevamente un regalo en un futuro? ¿No, verdad? Lo mismo pasa en la vida cuando bloqueas los canales para recibir toda la abundancia en tu vida; recíbela y disfrútala. Recuerda que la mejor forma de agradecer es vivir en plenitud.

Desde ya te deseamos éxito en el camino hacia tus metas financieras y esperamos que este libro sea la guía para lograrlas.

EPÍLOGO

¿Cuántas veces en tu vida tienes la oportunidad de participar en algo realmente grande que cambiará el mundo para siempre? La criptoeconomía tiene el potencial de marcar un antes y un después en la economía mundial y en la vida de las personas. Lo interesante es que desde el inicio el Bitcoin ha sido impulsado por una comunidad y no por grandes instituciones. El éxito que tenga y el cambio que pueda marcar la criptoeconomía para las personas dependen de la comunidad que la impulsa.

El Bitcoin es una red de pagos persona a persona. No depende

de instituciones centralizadas y puede crear confianza y consenso a través de la tecnología blockchain sin un tercero.

SATOSHI NAKAMOTO

Mientras más personas entiendan este concepto y qué implica para su economía personal, más va a crecer la criptoeconomía. Eso quiere decir que el éxito de la critoeconomía y la forma en que las criptomonedas lleguen a la vida de muchas personas, también depende de ti, atento lector de este libro.

En esta obra conociste el orígen del dinero y cómo ha llegado a su sexta evolución que son las criptomonedas. Ya sabes como comprarlas y usarlas.

También explicamos su funcionamiento basado en la tecnología blockchain. Además pudiste ampliar tus conocimientos sobre las diferentes formas de uso de esta tecnología, que va mucho más allá de monedas digitales y que tendrá un gran impacto en varios ambientes de nuestras vidas. Finalmente aprendiste estrategias de inversión en la criptoeconomía que te ayudarán a generar ingresos y mejorar tus finanzas personales.

Tres temarios que para nosotros: Juan Francisco Bolaños, Carlos Galarza y Frank Luetticke, componen lo que llamamos la CRIPTOECONOMÍA. Nuestro trabajo empezó aquí y ahora con

este libro, sin embargo queremos dar los próximos pasos contigo para enseñar a más personas lo que es la criptoeconomía. Pasos pequeños, como ayudar a abrir una billetera de Bitcoin y pasar los primeros satoshis, son el inicio. ¿Crees en las criptomonedas? Entonces es hora de que otras personas también las pueden conocer. Te invitamos a que formes parte activa de esta revolución. Enseña sobre el uso del bitcoin y otras monedas. Comparte, recomienda o regala este libro a las personas que te importan. Esperemos que con este trabajo te hayamos ayudado a entender mejor la criptoeconomía. Ahora depende de ti lo que hagas con estos nuevos conocimientos; tú decides

si quieres ser un usuario, un profesional o un inversor.

No dejes pasar esta gran oportunidad sin formar parte activa de ella. ¿Contamos contigo?

GLOSARIO

Ataque del 51%

Situación en que la mayoría de los mineros en una cadena de bloques lanzan un ataque a los nodos restantes con el fin de realizar doble gasto o cambiar las reglas de consenso de la plataforma.

Altcoin

Abreviatura de "moneda alternativa". Una parte importante de las altcoins surgieron como bifurcaciones duras –hardforks– de la cadena de bloques de Bitcoin; por ejemplo, Litecoin (LTC), Bitcoin Cash (BCH), Bitcoin Gold (BCG), PeerCoin (PPC), etc.

AML

El AML es la abreviatura para "Anti Money Laundry" y se refiere a la investigación en contra del lavado de dinero.

ASIC

Un "circuito integrado de aplicación específica" (Application Specific Integrated Circuit), es un chip de silicio específicamente diseñado para realizar una única tarea. En el caso de Bitcoin, estos circuitos están diseñados para resolver las funciones hash SHA 256 con el fin de minar nuevos bitcoins.

Bitcoin

La primera y más popular criptomoneda, creada en 2009, que está basada en un registro distribuido llamado "cadena de bloques" y una red informática cliente-cliente (P2P). Se escribe Bitcoin con "B", en mayúscula, para referirse a todo el sistema de software de Bitcoin; se escribe con "b", en minúscula, para referirse a la unidad de moneda bitcoin.

Bloque génesis

El bloque inicial o bloque 0 de una cadena de bloques. El "genesis block" de Bitcoin fue minado el 3 de enero de 2009 a las 18:15 UTC

y se puede ver en este hash:
https://www.blockchain.com/es/btc/block/0000
-
(http://bit.ly/2Mn3V9P)

Cadena de bloques (blockchain)

Libro contable distribuido que almacena y mueve todo tipo de datos, incluyendo activos, en una estructura secuencial de bloques ordenados cronológicamente y relacionados matemáticamente entre sí. Los datos que contiene una cadena de bloques no pueden ser modificados, borrados o censurados sin el consenso de todos los participantes –nodos– de la red informática.

Consenso

Cuando una mayoría de participantes de una red informática distribuida decide acerca de la validez de las transacciones. Un proceso, codificado en software, mediante el cual las computadoras en una red, llamadas nodos,

llegan a un acuerdo sobre un conjunto de datos.

Contrato inteligente (Smart Contract)

Un contrato inteligente es un código de software descentralizado, almacenado y ejecutado en una blockchain que mueve todo tipo de datos, incluyendo activos, basado en una o varias condiciones. Es, al mismo tiempo, el acuerdo y la ejecución, la gobernanza y la ley.

Criptoeconomía

Economía que se basa en la criptografía. La criptoeconomía permite transferir activos y valores a través de redes descentralizadas y encriptadas alrededor del mundo confiando en la tecnología criptográfica.

DAO

DAO significa "Decentralized Autonomous Organization", o en español "Organización Descentralizada Autónoma", e indica una organización en cual nadie es el jefe y el consenso se crea a través de todos los usuarios.

Las reglas se encuentran programadas en un contrato inteligente.

DApps

DApp es una aplicación descentralizada que usa código descentralizado. Ethereum fue creado precisamente para correr DApps. Una DApp tiene un "backend" descentralizado y un "frontend" centralizado. El backend está almacenado en la cadena de bloques que no puede ser alterada retroactivamente. El frontend usa aplicaciones móviles, gráficos o sitios web gestionados centralizadamente.

Dificultad de minería (Dificulty)

Mide qué tan difícil es encontrar el siguiente bloque de una cadena de bloques. Dependiendo de cuántos mineros se unan a la red, la dificultad puede aumentar o disminuir. El objetivo de la dificultad es mantener constante el tiempo de generación o producción de bloques. Por ejemplo, en Bitcoin se crea un

nuevo bloque cada 10 minutos; en Litecoin cada 2,5 minutos.

Dinero fiat

Cualquier dinero declarado como de curso legal por un gobierno, el cual es válido para cumplir con obligaciones financieras tanto públicas como privadas. Ejemplos: dólares, euros, pesos colombianos, soles peruanos, etc.

Dirección (Clave pública)

Las direcciones o "claves públicas" de criptomonedas se utilizan para enviar o recibir transacciones en la red. Las direcciones pueden ser representadas por códigos QR o de forma escrita. Una dirección generalmente se presenta como una cadena de caracteres alfanuméricos. Por ejemplo: Bitcoin:

1MUc7xuPKdbX7hkqxgBNURMMskKfkiuJoE

DLT

"Distributed Ledger Technology". Sistema de

contabilidad distribuida comúnmente usado en una cadena de bloques para crear una base de datos compartida y protegida criptográficamente.

Explorador de bloques

Herramienta en línea de acceso público para explorar la cadena de bloques de una criptodivisa particular en la que se puede seguir en tiempo real todas las transacciones que suceden en la cadena de bloques.

Firma digital

Esquema matemático usado para verificar la autenticidad de activos digitales. Las claves privadas se usan para firmar transacciones. Cada vez que se envía una transacción a través de una cadena de bloques, se firma con la clave privada del usuario. La transacción firmada se transmite por la red junto con la clave pública correspondiente.

FOMO

El FOMO es la abreviatura para “Fear Of Missing Out”. Se trata de crear miedo de perder una oportunidad. Con esta estrategia se logró una gran subida de valores en el mercado de criptomonedas a finales de 2017 porque nadie quería perderse la oportunidad de ganar dinero rápido.

FUD

FUD es la abreviatura para “Fear, Uncertainty and Doubt”. Es una estrategia con la cual se trata de crear inseguridad sobre un producto, en el caso de criptomonedas sobre una moneda, a través de información falsa y negativa. De esta forma la competencia trata de destruir la reputación de monedas.

Función hash criptográfica

Función matemática que produce como resultado una cadena única de caracteres de una longitud definida. Esta cadena de caracteres es única para cada una de las entradas de datos.

Estas funciones son usadas para crear identificaciones o huellas digitales.

Hardfork

Una bifurcación dura o "hardfork" es una actualización significativa en el código de software –que corre en los nodos de la red– de una cadena de bloques. Una bifurcación puede reescribir la historia de una cadena de bloques; por ejemplo, puede darse para revertir robos de dinero, para reparar fallas de seguridad importantes o para introducir nuevas funcionalidades.

HODL

En la comunidad cripto, en vez de "HOLD", que significa "no cambiar una criptomoneda por dinero fiat", se dice "HODL". El "HODL" nace en una conversación de Bitcoin-Talk donde un participante escribió mal la palabra "HOLD" y este error se hizo famoso en la comunidad.

ICO

Una ICO (Inicial Coin Offering) es una mezcla de una oferta pública inicial (IPO) y un "crowd funding" y se refiere en el ambiento cripto a la primera oferta de tokens.

IPFS

El "InterPlanetary File System" es un protocolo de distribución de medios, dirigido por contenido e identidades. IPFS permite la creación de aplicaciones completamente distribuidas. Su objetivo es hacer que la web sea más rápida, más segura y más abierta. Es un sistema de archivos distribuidos punto a punto que busca conectar todos los dispositivos informáticos con el mismo sistema de archivos. La característica principal de IPFS es que no tiene un solo punto de falla o de ataque.

KYC

"Know Your Customer"; en español: "Conoce a tu cliente", es un proceso de verificación de identidad de un usuario de una plataforma a

través de su documento de identidad, número de teléfono y documentos oficiales que indican la dirección en donde vive. La necesidad de un KYC va en contra de la idea inicial de Satoshi Nakamoto de que las criptomonedas sean anónimas.

Lightning Network

Red descentralizada que utiliza contratos inteligentes para permitir pagos instantáneos a través de una red de participantes. Lightning Network permite que las transacciones ocurran de inmediato, sin preocuparse por los tiempos de confirmación de los bloques. Permite millones de transacciones por segundo, a bajo costo, incluso entre diferentes cadenas de bloques, siempre que ambas cadenas usen la misma función hash criptográfica. Este protocolo pretende resolver el problema de escalabilidad de Bitcoin.

Minería

La minería es una intensa competencia entre computadores por encontrar el siguiente bloque de la cadena de bloques de Bitcoin u otras criptomonedas. A través de equipos de hardware como CPU, GPU o ASIC se procesan datos para la validación de transacciones que ocurren en la blockchain.

Nodo

Cualquier computadora que se conecte a una cadena de bloques se llama nodo.

PoS

“Proof of Stake”; en español: “Prueba de Fondos”, crea consenso sobre las transacciones a través de la cantidad de monedas que poseen los usuarios. Mientras más monedas se guardan en la billetera, más poder se tiene sobre las decisiones si una transacción es verídica o no.

PoW

“Proof of Work”; en español: “Prueba de

Trabajo", es un sistema de creación de consenso a través de un trabajo que hay que realizar. En el mundo cripto, PoW también se refiere a la minería para confirmar transacciones.

Oráculo

Los oráculos alimentan a los contratos inteligentes con información externa a la cadena de bloques. Los oráculos son interfaces del mundo real hacia el mundo digital. Un oráculo puede ser un sensor de un dispositivo IoT o servicios web que proveen información para los contratos inteligentes.

Red centralizada

Red cerrada de computadores o nodos que se encuentran administrados por una autoridad central y jerárquica, que se encuentra en una determinada ubicación geográfica.

Red distribuida

Red abierta de computadores o nodos que se encuentran dispersos o distribuidos alrededor del mundo que pueden procesar transacciones sin la participación de intermediarios o redes gestionadas centralizadamente.

Satoshi

La unidad más pequeña de Bitcoin, igual a BTC 0,00000001. En otras palabras, un satoshi es la cienmillonésima parte de un bitcoin.

Satoshi Nakamoto

Pseudónimo para la persona o grupo de personas que creó el protocolo de Bitcoin y el software de referencia Bitcoin Core.

SegWit (Segregated Witness)

El SegWit es una propuesta para encontrar una solución al debate sobre el tamaño de bloques de la red de Bitcoin que sólo permite transaccionar con una cantidad limitada de transacciones. La empresa Blockstream y el

equipo de Bitcoin Core lo propusieron y fue activado el 24 de agosto de 2017. Con SegWit la red de Bitcoin consume menos recursos y permite realizar transacciones más rápidas.

Softfork

Tanto las bifurcaciones duras como las suaves separan a la cadena de bloques original en dos cadenas, con la diferencia de que en una bifurcación suave o "softfork", sólo una cadena de bloques seguirá siendo válida a medida que todos los nodos adopten la actualización de software, mientras que la otra desaparecerá.

Tainted Coins (Monedas pintadas)

Se refiere a monedas que han estado en contacto con transacciones ilegales y quedaron marcadas.

To the moon

El "To the moon" es una expresión que usa la comunidad de criptos para decir que el precio de una moneda sube en gran escala, "hasta la

luna”.

Token

Un activo digital escaso definido por un protocolo de consenso e intercambiado a través de una cadena de bloques. Son una unidad de valor, emitida por una entidad privada, que tiene el valor que se le otorga dentro de una comunidad o un mercado.

BIBLIOGRAFÍA

1. Antonopoulos, A. (2016). The Internet of Money, Volume I. Merkle Bloom LLC.
2. Antonopoulos, A. (2017). The Internet of Money, Volume II. Merkle Bloom LLC.
3. BTC-ECHO; de Boer, D.; Giese, Dr. P.; Kops, M.; Preuss, M.; Wagenknecht, S. (2016). Die Bitcoin Bibel: Das Buch zur digitalen Währung (German Edition). Kleve, Alemania. BTC-ECHO. Edición de Kindle.
4. BTC-ECHO; Kops, M.; Wagenknecht, S.; de Boer, D.; Giese, Dr. P., Preuss, M. (2017). Investieren in Kryptowährungen: Dein Weg zum erfolgreichen Blockchain-Investment (German Edition). Kleve, Alemania. BTC-ECHO. Edición de Kindle.
5. BTC-ECHO; Kops, M.; Wagenknecht, S.; de Boer, D.; Giese, Dr. P. (2016). Die Blockchain Bibel: DNA einer revolutionären Technologie (German

Edition). Kleve, Alemania. BTC-ECHO. Edición de Kindle.

6. Davidson, J.; Rees-Mogg, W. (1997). The Sovereign Individual: Mastering the Transition to the Information Age. New York, NY: Touchstone.
7. Diedrich, H. (2016). Ethereum. London, UK: Wildfire Publishing.
8. Eker, T. Harv (2005). Los secretos de la mente millonaria. Cómo dominar el juego interior de la riqueza. Título original: Secrets of the millionaire mind, traducción: Anna Renau Bahima. Buenos Aires, Argentina. Ed. Sirio Argentina.
9. Hosp, Dr. J. (2017). Kryptowährungen - Bitcoin, Ethereum, Blockchain, ICOs & Co. einfach erklärt. (German Edition). Edición de Kindle.
0. Hosp, Dr. J. (2018). Blockchain 2.0 - einfach erklärt - weit mehr als nur Bitcoin (German Edition). München, Alemania.

FinanzBuch Verlag. Edición de Kindle.

1. Koenig, A. (2015). BITCOIN – Geld ohne Staat: Die digitale Währung aus Sicht der Wiener Schule der Volkswirtschaft (German Edition). München, Alemania. FinanzBuch Verlag. Edición de Kindle.
2. Koenig, A. (2017). Cryptocoins: Investieren in digitale Währungen (German Edition). München, Alemania. FinanzBuch Verlag. Edición de Kindle.
3. Márquez Solís, S. (2016). Bitcoin – Guía completa de la moneda del futuro. Bogotá, Colombia. Ediciones de la U.
4. Nachtigall, P. (2016). Inteligencia Emocional Financiera. 39 consejos para atraer la prosperidad que mereces. Bogotá, Colombia. Planeta Colombiana S.A.
5. Preukschat, A., et. al. (2017). Blockchain: La revolución industrial de Internet. Barcelona, España: Grupo Planeta.

6. Robbins, T. (2018). Money – Die 7 einfachen Schritte zur finanziellen Freiheit. (German Edition). München, Alemania. FinanzBuch Verlag.
7. Tapscott, D. & Tapscott, A. (2017). La revolución blockchain. (Primera edición electrónica). Barcelona, España: Grupo Planeta.

WEB

kbar, K. (6 abril 2018). What is Cosmos Blockchain? The Most Comprehensive Guide. Recuperado de http://bit.ly/2JTayRP

lam, I. (4 diciembre 2018). What Are Atomic Swaps? The Future of Blockchain Technology. Recuperado de http://bit.ly/2ShRgcD

lex de Coinstaker. (s.f.). Initial Coin Offering. Recuperado (20 febrero 2019) de

http://bit.ly/2HsJDJb

lvarez, R. (4 octubre 2018). 7 Curiosidades de las Stablecoins. El Criptógrafo. Recuperado de http://bit.ly/2HsJZiZ

ntonopoulos, A. (2016). Mastering Bitcoin. Recuperado de http://bit.ly/2HsKlWR

nwar, H. (4 octubre 2018). Do You Need a Blockchain? The Ultimate Blockchain Decision Tree. Recuperado de http://bit.ly/2Ftjquf

solo, B. (18 diciembre 2018). Mimblewimble Explained. Recuperado de http://bit.ly/2FuRkix

alaji, A. (9 enero 2019). MimbleWimble: History, Technology, and the Mining Industry. Recuperado de http://bit.ly/2FynGce

ancayNegocios.com. (18 diciembre 2017). Claves del éxito o fracaso de una criptomoneda. Recuperado de

http://bit.ly/2HrHYUc

it2me (19 septiembre 2018). Todo sobre las ICO dentro de las criptomonedas – Explicación completa. Recuperado de http://bit.ly/2Ht0sUA

lock, The. (20 enero 2019). Special Edition—Money 2.0 Stuff: Upgrading Blockchains Is Like Cleaning a Pig. [Correo electrónico al autor].

BlockchainHub. (s.f.). Blockchain Glossary. Recuperado (20 febrero 2019) de http://bit.ly/2N2M59r

Bolaños, J.F. (s.f.). La importancia de leer un "white paper" antes de invertir en una criptomoneda o ICO – Steemit. Recuperado (20 febrero 2019) de http://bit.ly/2G8Fjz0

Bolotin, N., & Nolascow, P. (18 enero 2018). What is Litecoin? The Most Comprehensive Guide Ever! Recuperado de http://bit.ly/2FReTj0

orman, D. (s.f.). Jed McCaleb calls 90% of crypto projects “B.S.” in new interview. Recuperado de http://bit.ly/2HsT0Zp

otsman, R. (Junio 2016). We've stopped trusting institutions and started trusting strangers – TED Summit. Recuperado de http://bit.ly/2GajQoZ

uchman, E., & Kwon, J. (s.f.). Cosmos: A Network of Distributed Ledgers. Recuperado (1 abril 2019) de http://bit.ly/2uCxES3

ustillos, M. (30 noviembre 2017). You Don’t Understand Bitcoin Because You Think Money Is Real. Recuperado de http://bit.ly/2R7mz4N

alderón, G. (1 diciembre 2017). La guerra contra el efectivo. Recuperado de http://bit.ly/2ALXWGB

arrino, I. (20 noviembre 2015). El origen del dinero, de Carl Menger. Recuperado de http://bit.ly/2FTeJte

ermak, L. (18 junio 2019). Let's stop the Libra FUD. Recuperado de http://bit.ly/2MXDRUL

han, J. (11 septiembre 2018). Blockchain and Data Storage: 3 Promising Projects. Recuperado de http://bit.ly/2TJS9ex

han, J. (5 septiembre 2018). Blockchain and Data Storage: A Perfect Match? Recuperado de http://bit.ly/2TNhTab

haparro, F. (18 junio 2019). Facebook releases plan for its Libra cryptocurrency to 'meet the daily financial needs of billions of people'. Recuperado de http://bit.ly/2MVl50n

hibber, K. (15 septiembre 2014). Here are all the countries that don't have a currency of their own. Recuperado de http://bit.ly/2FWuUpL

oinlist.me. (s.f.). Qué es Stellar y cómo funciona – la mejor guía sobre Lumens (XLM). Recuperado (20 febrero 2019)

de http://bit.ly/2HrHlu2

urran, B. (16 enero 2019). What is Grin Coin & MimbleWimble? Complete Beginner's Guide. Recuperado de http://bit.ly/2FxmplE

urran, B. (5 diciembre 2018). Guide to Cosmos: The Tendermint-Based Blockchain Ecosystem. Recuperado de http://bit.ly/2JTtjEE

el Castillo, C. (30 octubre 2018). La próxima revolución política será por el control de los algoritmos – WEF. Recuperado de http://bit.ly/2F8Wu45

íaz, G. (25 septiembre 2018). Aprende las diferencias entre bitcoin y el dinero fiduciario. Recuperado de http://bit.ly/2qazSGm

ixon, C. (26 octubre 2018). Why Decentralization Matters – Medium. Recuperado de http://bit.ly/2FH1RrA

udas, M. (18 junio 2019). Facebook's Libra cryptocurrency: Where are the banks? Recuperado de http://bit.ly/2MU90sh

conomiasimple.net. (s.f.). Ripple ¿Qué es el Ripple? ¿Cómo funciona el Ripple? Recuperado 20 febrero 2019 de http://bit.ly/2Htryec

l Telégrafo. (14 febrero 2018). Junta Monetaria no autoriza el uso de criptomonedas. Recuperado de http://bit.ly/2EUOnES

squema Ponzi (7 enero 2019). Recuperado de http://bit.ly/2HsTcb5

anusie, Y.J., & Robinson, T. (12 enero 2018). Bitcoin Laundering: An Analysis of Illicit Flows Into Digital Currency Services. Washington D.C.: Center of Sanctions & Illicit Finance & Elliptic. Recuperado de http://bit.ly/2FZr7J4

hersi, E. (6 enero 2015). La corrupción es efecto, no causa. Recuperado de

http://bit.ly/2LIFvnW

ómez, R. (9 enero 2019). Chilenos comenzarán a declarar impuestos por canje de criptomonedas en abril. Recuperado de http://bit.ly/2HtP6Q4

onzález, G. (15 septiembre 2018). Un vistazo a la regulación de las criptomonedas en América Latina. Recuperado de http://bit.ly/2EPQBFB

onzález, G. (21 mayo 2018). Conoce los stablecoins, los criptoactivos de precio estable. Recuperado de http://bit.ly/2Htgn4Y

arper, C. (21 marzo 2018). What are Atomic Swaps? A Beginner's Guide. Recuperado de http://bit.ly/2Dql9wW

errera, C. (17 mayo 2018). ¿Qué son los stablecoins o monedas estables? Recuperado de http://bit.ly/2HukoGB

istoria del dinero – Wikipedia. (8 enero 2019).

Recuperado (25 enero 2019) de http://bit.ly/2FWTS8b

uang, Z. (6 noviembre 2018). Bitcoin: How everything started with creator's nine-page paper. Recuperado de http://bit.ly/2F0nm5L

uillet, M. (13 noviembre 2018). Gigante de electrónica Bosch se asocia con IOTA para lanzar nuevo dispositivo para recolección de datos de IoT. Recuperado de http://bit.ly/2HrLazk

üls, J. (11 enero 2018). Interview mit IOTA-Mitbegründer Dominik Schiener. Recuperado de http://bit.ly/2HrZKGZ

)TA. (s.f.). What is IOTA? Recuperado (20 febrero 2019) de http://bit.ly/2HtPaiM

enkinson, G. (2 enero 2019). A Brief History of Bitcoin: 10 Years of Highs and Lows. Recuperado de http://bit.ly/2F51YfA

im, C. (15 marzo 2019). A Blockchain to

Connect All Blockchains, Cosmos Is Officially Live. Recuperado de http://bit.ly/2JWrtTD

hatri, Y. (18 junio 2019). The 10 most important things you need to know about Facebook's new cryptocurrency, Libra. Recuperado de http://bit.ly/2MW8H0a

ópez, G. (12 abril 2018). La tecnología del Bitcoin (Blockchain) contra la corrupción. Recuperado de http://bit.ly/2LIJZuA

ópez, T. (20 junio 2018). ¿De dónde viene lo que comes? Los pasaportes digitales pronto te lo dirán – El País. Recuperado de http://bit.ly/2lr7Js7

u, J. (17 octubre 2018). The Importance of Blockchain Interoperability. Recuperado de http://bit.ly/2UbjUNr

Iarchena, P. (7 diciembre 2018). Bitwise lanza fondos de inversión para Bitcoin y Ethereum. Recuperado de

http://bit.ly/2Ht6RPk

Martínez, A. (8 septiembre 2018). Estudio revela que los millennials están dispuestos a usar Bitcoin. Recuperado de http://bit.ly/2HuZlno

Matsakis, L. (22 mayo 2017). Following a Tuna from Fiji to Brooklyn–on the Blockchain. Recuperado de http://bit.ly/2MhRxEO

MIT Technology Review Editors. (23 abril 2018). A glossary of blockchain jargon. Recuperado de http://bit.ly/2MYMLwA

Nakamoto, Satoshi (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Recuperado de http://bit.ly/2YEMLYa

Nuevo Financiero (21 mayo 2018). ICO, el boom de ofertas iniciales de monedas. Tipos, ventajas e inconvenientes. Recuperado de http://bit.ly/2HrIscY

O'Higgins, C. (18 septiembre 2018). Mimblewimble explained like you're 12 –

Medium. Recuperado de http://bit.ly/2FHIX2b

rcutt, M. (8 marzo 2019). Blockchain boosters warn that regulatory uncertainty is harming innovation. MIT Technology Review. Recuperado de http://bit.ly/2ESYCtD

atiño, D. (15 marzo 2018). Se abre camino para cobrar impuestos a bitcoins. Recuperado de http://bit.ly/2HrM1Qy

attekar, S. (26 mayo 2018). Do I really need blockchain? 4 important factors to consider. Recuperado de http://bit.ly/2FtG5H6

eereboom, C. (11 diciembre 2018). What Are Atomic Swaps? The Most Comprehensive Guide Ever! Recuperado de http://bit.ly/2Do1CgV

imentel, P. (Marzo 2014). Trends and Solutions in Combating Global Food Fraud – Food Safety Magazine. Recuperado de

http://bit.ly/2Mgambf

urlev, P. (7 junio 2018). What is an ICO presale or Pre-ICO? Recuperado de http://bit.ly/2Hs06gN

urlev, P. (21 septiembre 2018). What is the difference between an ICO hard cap and soft cap? Recuperado de http://bit.ly/2Hs06NP

eutemann, T. (2018). The First Major Battle Between the Land and the Cloud – Democracy Earth. Recuperado de http://bit.ly/2KantOU

ooney, K. (3 noviembre 2018). Happy 10th birthday bitcoin: Here's what's changed since the cryptocurrency grew into a $100B market. Recuperado de https://cnb.cx/2F3cYdc

osic, A. (11 noviembre 2016). What is Ethereum? The Most Comprehensive Beginners Guide. Recuperado de http://bit.ly/2Kjk29k

osic, A. (s.f.). Comprehensive Blockchain Glossary: From A-Z. Recuperado (20 febrero 2019) de http://bit.ly/2MXsqaT

osic, A. (12 septiembre 2017). What is Monero? Most Comprehensive Guide. Recuperado de http://bit.ly/2UC6ZmY

antiso, C. (2018). ¿La cadena de bloques frenará la corrupción? Recuperado de http://bit.ly/2LNsQAb

chmidt, K. (Abril 2018). Bitcoin Forks: Fully Comprehensive Blockgeeks Guide. Recuperado de http://bit.ly/2N0Rlvr

in autor. (s.f.). Blockchain? Is this the technology your business needs? Recuperado de http://bit.ly/2FrOEC1

putnik (1 noviembre 2018). La minería de criptomonedas se suma a la lista de amenazas para el clima. Recuperado de http://bit.ly/2HsL0aN

tanley, A. (18 abril 2018). Quebec Chief

Scientist: Bitcoin 'Not A Magnet For Illicit Transactions' – Forbes. Recuperado de http://bit.ly/2FZ869F

okens24 Team (12 marzo 2018). Definición de los 3 tipos de tokens – Tokens24. Recuperado de http://bit.ly/2HrIyBm

rustToken: Tokenization you can Trust. (s.f.). Recuperado (7 enero 2019) de http://bit.ly/2HrM8eW

an Altsyne, M. (Mayo 2014). Why Bitcoin Has Value – Research Gate (Communications of the ACM, Vol. 52, No. 5). Recuperado de http://bit.ly/2FZtDy2

iele, J. (1 octubre 2010). Mt.Gox y el mayor hackeo de criptomonedas. Recuperado de http://bit.ly/2Hx35EZ

ite, J. (27 enero 2018). El uso de criptomonedas en el Ecuador no está autorizado, según Banco Central. Recuperado de http://bit.ly/2EQkJ3V

/orld Economic Forum (Septiembre 2015). Deep Shift Technology Tipping Points and Societal Impact. [archivo PDF] Recuperado de http://bit.ly/2We07gt

uckerman, M. J. (18 enero 2019). El primer contrato de futuros de Bitcoin expira a $10 900; una 'victoria para la bajas'. Recuperado de http://bit.ly/2HrIrpE

SOBRE LOS AUTORES

Juan Francisco Bolaños es consultor, capacitador y desarrollador de negocios blockchain desde 2017. Su actividad laboral abarca un período de veinte años en diversos ámbitos, como el comercio exterior de alimentos, cooperación agrícola internacional, sanidad agropecuaria e inocuidad de alimentos, emprendimiento, administración de PYMES y servicios legales, comerciales y financieros internacionales.

Actualmente ejerce las funciones de CEO de BuenBlock S.A., Blockchain Business Developer en Kruger Corporation, consultor de

AcademiaBlockchain.com y embajador de 101Blockchains.com. Todas estas iniciativas tienen que ver con el desarrollo e implementación de soluciones blockchain para diferentes sectores (banca, seguros, salud, agroindustria, gobierno…) y con la educación y generación de conocimientos relacionados con la tecnología de la cadena de bloques y las criptomonedas.

Ha participado como conferencista y promotor de la tecnología blockchain en importantes escenarios internacionales de la talla de TEDx y LaBitConf. Asimismo, ha dictado conferencias y seminarios sobre esta tecnología en las

universidades San Francisco de Quito, Politécnica Salesiana, Central y Escuela Superior Politécnica del Chimborazo en Ecuador, San Martín de Porres y San Ignacio de Loyola en Perú, así como en eventos privados organizados por la Cámara de Comercio de Quito, Sociedad Nacional de Industrias del Perú, Programa Al Invest 5.0 de la Unión Europea, Liberty Rail, ExpoCryptoBlockchain, Ouishare, Hult Prize On Campus 2019 y Grupo Creex.

Frank Luetticke es economista graduado en Alemania y Ecuador. Desde el año 2011 radica en Quito y se dedica al desarrollo personal, negocios e

inversiones. En 2014 se certificó como Life Coach y Coach en Network Marketing en la ACCA (Academia de Coaching y Capacitación Americana de Miami). Desde 2015 es Mentor Coach Educativo con la especialización en Finanzas Personales e imparte las mentorías de Coaching Financiero en la academia. Durante dos años fue director encargado de la certificación de Coach Ejecutivo Empresarial.

Desde 2016 estudia y trabaja con tecnología blockchain y criptomonedas. Ha dictado conferencias y seminarios con el tema de criptomonedas y finanzas en Ecuador, Colombia y EE.UU. En 2017 culminó con éxito la primera

certificación de criptomonedas y blockchain a nivel universitario, en la Universidad de Nicosia de Grecia. Ese mismo año nace la marca CriptoAsesores, con la cual Frank y sus socios ofrecen un amplio portafolio de servicios alrededor de inversiones y asesorías en la criptoeconomía. Desde sus inicios forma parte de los Embajadores de la marca CAPITALIKA, una de las principales casas de cambio de criptomonedas para Latinoamérica. En 2018 fue cofundador de la marca CripTec, la primera compañía en producir ATMs para criptomonedas en Latinoamérica. Hoy Frank trabaja en varios proyectos relacionados con la criptoeconomía y

ofrece un amplio portafolio de productos y servicios en esta área, como asesorías, seminarios, talleres, conferencias, ATMs y sistemas de pagos POS.

Carlos Galarza Ponce es ingeniero comercial, Master en Desarrollo Emprendedor e Innovación por la Universidad de Salamanca. Cuenta con una certificación de Coaching Ejecutivo Nivel Excelente de la Escuela de Coaching EFIC en Barcelona, España.

Lider Coach y Facilitador en Inteligencia Financiera con estudios en

la academia Peak Potentials Training en EE.UU. Además es Conferencista Internacional en Inteligencia Financiera y Liderazgo.

Lleva quince años dedicado con éxito a los negocios. Es promotor de nuevas tecnologías, principalmente Blockchain, Realidad Virtual y Realidad Aumentada. Forma parte del Grupo Empresarial Gala, vinculado a varias empresas en diversos sectores productivos. Desde cero desarrolló proyectos en el ámbito de las importaciones, comercio mayorista, minorista y de servicios. Inversionista de riesgo; en varios proyectos participa activamente en la capacitación y asesoría de

emprendedores e inversores como Advisor y Business Developer.

Actualmente enfocado en el mundo de las Startups. Inversionista y Representante para la región de Nodalblock, empresa que ha salido a bolsa en Canadá y ha sido reconocida como una de las suministradoras líderes a nivel mundial de ID Digital en Blockchain, según Research N Reports.

En 2018 ideó y cofundó una de las principales wallets de criptomonedas en Latinoamérica llamada CAPITALIKA, impulsando así el uso de las mismas. En 2019, también como cofundador, lanzó al mercado una de las Startups pioneras en desarrollo de Realidad Virtual y

Realidad Aumentada en la región, llamada VINARY VR/AR.

CONTACTOS

Para más detalles o información adicional sobre el tema puedes visitar la página web:

www.librocriptoeconomia.com

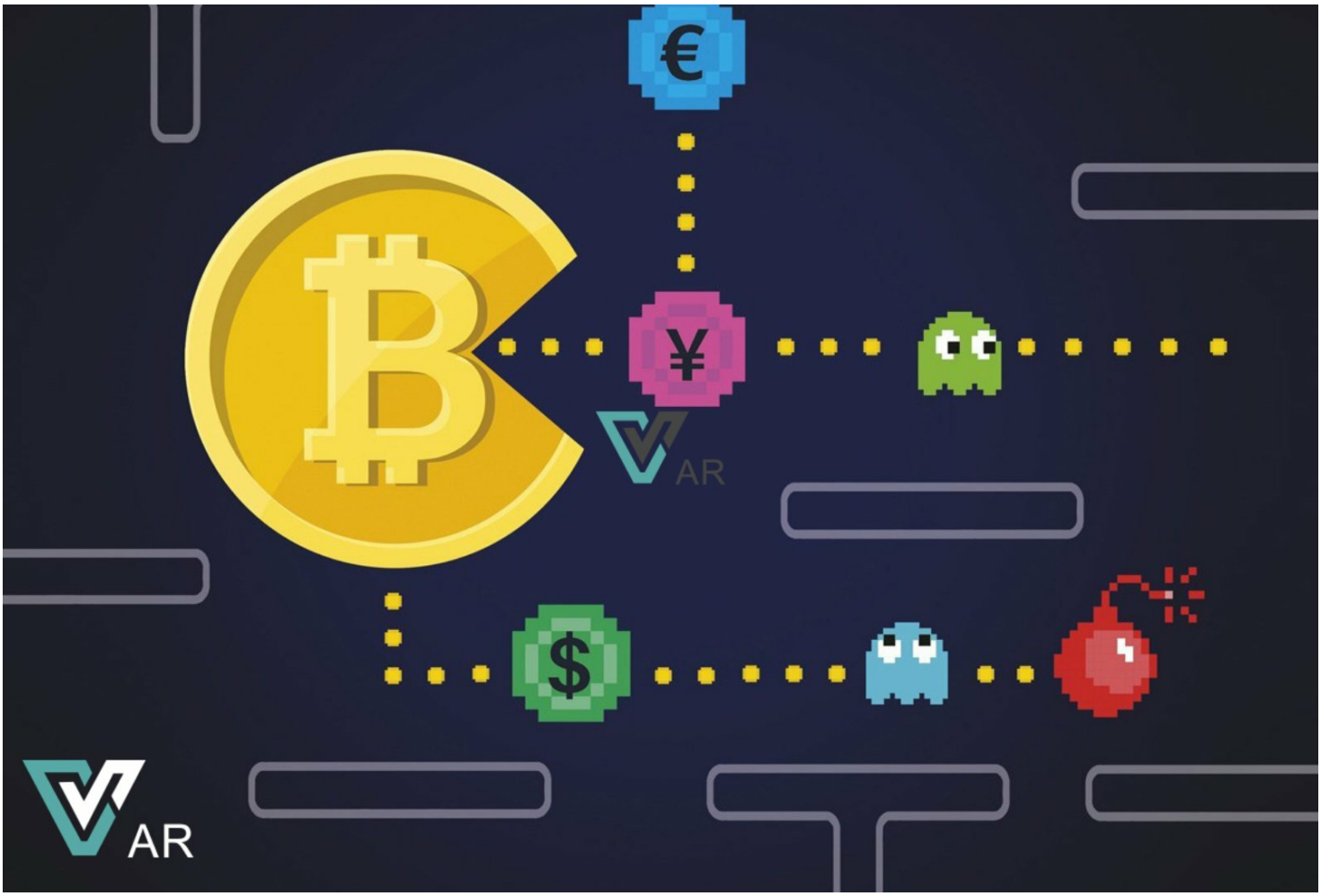
Contactos directos:

Frank Luetticke	Correo: Frank.Luetticke@gmail.com Celular: +593 99 838 6586 (Ecuador)
Juan Francisco Bolaños	Correo: jfbt@pm.me Celular: +51 932 03 0404 (Peru) +593 99 248 5870 (Ecuador)
Carlos	Correo:

Galarza cgalarza@capitalika.com
Celular: +593 99 850 2427
(Ecuador)

Si estas interesado en adquirir copias en cantidad de este libro con un descuento para tus clientes o tu empresa puedes escribir a: info@bigmind360.com

JUEGO CON REALIDAD AUMENTADA



Disfruta de esta experiencia lúdica en Realidad Aumentada

REFERENCIAS

[1] World Economic Forum. (2015) Deep Shift Technology Tipping Points and Societal Impact Survey Report, Septiembre 2015. REF 310815. Recuperado de: http://bit.ly/2We07gt