Descifrando Bitcoin

El primer caso de uso de la Blockchain

Conceptos de base que sustentan la próxima revolución digital:
El internet del Valor y la Descentralización de la confianza

Gerardo Cifuentes

Descifrando

Bitcoin

El primer caso de uso de la

Blockchain

Gerardo Cifuentes

Contenido

Gerardo Cifuentes

Entusiasta de las nuevas tecnologías y de cómo éstas impactan a la sociedad. Su experiencia como académico y consultor lo motivan a contribuir en la educación de temáticas contingentes.

El autor es Ingeniero Constructor de la Universidad del Bío-Bío, Máster en Gestión Financiera de la

Universidad de Concepción y Especializado en Bolsa y Mercados Financieros de la Universidad de Alicante.

Prólogo

Mucho se habla de la revolución 4.0, pero ¿Qué entendemos realmente de este término? De alguna forma sabemos de qué se trata el internet, pero ¿Qué tiene que ver esta revolución con términos como la IA, el IOT, la *Blockchain* y las monedas digitales como el *bitcoin*, entre otros conceptos ligados a este ambiente? ¿Será solo una revolución conceptual lo que estamos viviendo y de la cual somos parte algunos de nosotros? ¿Por

qué me debería interesar saber más sobre la *Blockchain*? ¿Qué ganancia obtengo? ¿Podremos esperar que la revolución 4.0 sea tan o más relevante que la revolución industrial del siglo XVIII?

Muchas de las respuestas a estas interrogantes las podrás conocer en este libro, el cual pretende ser una guía práctica y amigable para que cualquier persona lo pueda entender y enriquecerse en el conocimiento sobre los cambios en términos digitales, de los cuales estamos siendo testigos o partícipes de manera pasiva o activa.

Esta obra no fue escrita por un experto informático, sino por un amante

de la innovación y de los avances tecnológicos, lo que facilita su lectura y el entendimiento de los conceptos que se explican.

En el mundo actual, el avance tecnológico y la aparición de nuevos cambios de paradigmas, están provocando una variación no solo conceptual, sino física. Desde hace un tiempo, se han estado escuchando términos tan "raros" y "complejos" como Bitcoin, *Blockchain*, Criptomonedas, *Smart Contracts*, ICO, entre otros. Por esta razón nace este libro, para ayudar al lector a entender qué es, cómo funciona, y sobre todo, cómo utilizar estos conceptos para crear

y generar nuevos productos y servicios, o simplemente, para estar preparados para el futuro próximo.

El mundo bancario es para muchas personas algo muy difícil de conocer y entender. Para realizar un pago o retirar dinero, hasta hace pocos años se tenía que obligatoriamente ir a un Banco a realizar dichas transacciones, hasta que apareció el internet y se empezó a masificar, y además irrumpieron en el mercado medios como los *smartphones*, los cuales posibilitan realizar distintas actividades desde cualquier lugar del mundo. Estos tipos de tecnologías innovadoras y disruptivas cambiaron lo que nuestros padres y

abuelos conocían como los movimientos bancarios. Hoy en día, y desde hace ya un par de años, una nueva tecnología innovadora se está posicionando disruptivamente para seguir cambiando a la Banca. Les hablo de la *Blockchain* y del *Bitcoin*.

Otro hecho importante de mencionar, y desconozco si solo será una casualidad, es que también en los últimos años, y en especial al menos en Chile, en los últimos 12 meses, han salido a la luz pública innumerables ataques de seguridad informática en grandes bancos de la plaza. Es posible que se deba a factores como la masividad de la internet, el amplio

conocimiento expuesto en esta, las nuevas tecnologías para desarrollar sistemas informáticos y que van mutando rápidamente, y por supuesto los ánimos por hacer daño que algunas personas tienen, ya sea para demostrar sus conocimientos avanzados en seguridad o solamente por robar. Todo estos fallos de seguridad han incrementado el descontento que se tiene con estas entidades financieras, y es precisamente en este punto donde la *Blockchain* junto a l *Bitcoin*, entre otras monedas digitales, llegan para ofrecer tranquilidad y seguridad en las transacciones.

Gerardo, el autor de este libro,

presenta de forma simple la complejidad de esta tecnología y el cambio de paradigma que está sucediendo, y del cual, afortunadamente, podemos ser parte importante ya sea creando y/o utilizando los productos en base a la *Blockchain*.

La *Blockchain* ya está siendo usada en temas empresariales y cotidianos, tales como en empresas de generación de energía, en área de la salud dado que la cadena en bloques permitirá que el historial médico de los pacientes posea mayor privacidad y seguridad, en aplicaciones para el transporte y logística, en sector inmobiliario, en *retail*, en los contratos legales, en la

identidad digital, en la banca, y obviamente en la creación de monedas digitales, entre otros muchos usos que nos podamos imaginar. Por lo anterior, se puede decir que está en todos lados, y si aún no lo está, pronto lo estará, al ser una tecnología de infinitos usos. Llegó para cambiar el mundo como lo conocemos, las interacciones entre las personas, empresas y el estado, todo va a cambiar y tú puedes decidir, si ser un actor activo o solo ver cómo otros cambian el mundo.

Con mis más de 12 años de experiencia trabajando en grandes y pequeñas empresas relacionadas al mundo TIC e Innovación, emprendiendo

y realizando clases en Universidad, estoy seguro que estos cambios están recién comenzando y que es una excelente oportunidad para sumarse. Los invito a conocer más de la *Blockchain* y del *Bitcoin* en este entretenido y amigable libro, escrito con un nivel de comprensión accesible, siendo un muy buen comienzo para aprender acerca de estas tecnologías, con ejemplos de los usos actuales y con referencias para que sigas aprendiendo.

Te invito además, que no solo te quedes con leer este maravilloso libro, sino trata de aplicarlo a lo que conoces; a tu negocio, a tus ideas, a tu vida. No te preocupes si al leerlo sientes que tu vida

tiembla, ¡más bien alégrate por el aporte que tú puedes generar para la vida de tod@s!

Juan Sepúlveda Fuentes

Ingeniero de Ejecución en Computación e Informática de la Universidad del Bío-Bío, Postítulo en Gestión Informática y Magister en Tecnologías de Información y Gestión de la Pontificia Universidad Católica de Chile, Scrum Master Certificado por la Scrum Alliance, Emprendedor y actual Presidente de la Asociación Gremial Informáticos de Ñuble A.G.

A Catalina Isidora que con su sonrisa
la vida cobra real sentido.

❋❋❋

Introducción

¿Es el *bitcoin* el nuevo oro? ¿Es una burbuja que acabó reventada? No son pocos los que creen en su potencial, pero a su vez una gran mayoría ve aún con desconfianza su usabilidad, no obstante, de lo que sí hay consenso es que para nadie es indiferente. A pesar de que el ecosistema que rodea el "Criptomundo" es aún joven y en etapa temprana, ya hemos sido testigos que las monedas digitales y la tecnología

disruptiva que sustenta esta innovación, llamada *Blockchain*, cambiará la forma en como intercambiamos valor en internet, abriendo una gran gama de aplicaciones de gestión descentralizada de datos, que trascienden a la transferencia de activos digitales, tales como: Expedientes médicos, logística, finanzas, internet de las cosas, propiedad intelectual, financiamiento de iniciativas, contratos inteligentes, sistemas eleccionarios, trazabilidad, entre muchas otras.

¡Internet nos cambió! Nos permite hacer cosas que poco tiempo atrás nos parecían inimaginables y casi de fantasía futurista; el internet de la

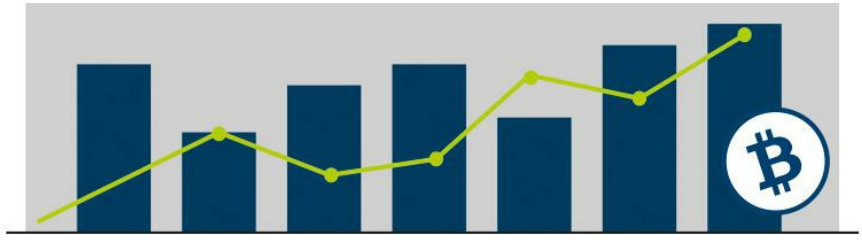
información está al alcance de nuestros *smartphones*, pero a pesar que consideremos que en este ámbito todo ha sido creado, fue precisamente con la creación del *Bitcoin* que recién surgió la función de enviar dinero digital sin intermediarios y eso ha significado comenzar a decir adiós al internet de la información y dar la bienvenida al Internet del Valor.

¿Quedarán obsoletos los sistemas de procesamientos de pago a causa de las Criptomonedas? ¿Se pondrá en entredicho la real necesidad de continuar con una autoridad monetaria? Interrogantes que solo el futuro inmediato dilucidará.

¿Qué es el *bitcoin* y la Criptoeconomía? ¿Qué usos prácticos permitirá la *Blockchain*? ¿Cómo invertir en una ICO? ¿Qué es un *Smart Contract*?

En un inicio pudiéramos pensar que el entendimiento del mundo del *Bitcoin* y de la *Blockchain* es solo atingente a profesionales del área informática y la programación, no obstante, en poco tiempo la usabilidad de aplicaciones descentralizadas tan cotidianas como *Google, WhatsApp* o *Facebook* hará que sea cotidiano interactuar y beneficiarse de las ventajas de la gestión segura y de bajo costo de datos y activos.

El presente libro tiene como principal objetivo dar a conocer, a no especialistas, tanto los conceptos fundamentales y básicos que explican la revolución de las Criptomonedas, como las características principales de la Criptoeconomía y la *Blockchain*. Todo lo anterior, en un lenguaje simple y directo, para cimentar una base que permitirá al lector introducirse posteriormente a aguas más profundas y ser un espectador privilegiado de un nuevo cambio de paradigma digital.



Criptoeconomía

¿Cripto que…? La nueva economía y su tecnología disruptiva

Si hay algo de lo cual se ha hablado en los medios estos últimos años, es del *Bitcoin* y como la escalada y posterior descenso en su valor no ha dejado indiferente a nadie. Términos un tanto lejanos empiezan a ser parte del vocabulario de publicaciones en prensa escrita y digital: *Criptomonedas*,

Blockchain, *Bitcoin*, *ICOs*, *Ethereum*, Protocolos, Minería, etc.

Expertos coinciden en que las últimas cinco décadas han marcado un antes y un después en cómo las personas nos relacionamos en todos los aspectos de la vida. Es así, como en la década del 70, se innovó en la confección de las Placas Madre, luego en los 80 irrumpieron los ordenadores personales. Ya en los 90 fuimos testigos de la irrupción de la Internet, para luego en los 2000 ver el boom de las redes sociales y los *smartphones*. Pues bien, ya existe consenso que la próxima gran revolución vendrá de la mano de la tecnología *Blockchain* y su uso en la

Criptoeconomía y el internet del valor, así como también en otras interesantes áreas que nos serán de mucho impacto en nuestro quehacer habitual.

Un concepto nuevo es precisamente la Criptoeconomía, término que ha sido acuñado por todo el ecosistema del *Bitcoin* y las Criptomonedas en general, pero lejos de ser, por lo menos hasta ahora, una especialidad de la economía, sí relaciona para sus aplicaciones prácticas a la criptografía y su uso para fines económicos, como son los pagos entre personas y empresas sin necesidad de intermediarios o terceros de confianza. Estamos ante una propuesta transgresora para la economía clásica y

el sistema financiero regular, que postulan en la necesidad de un ministro de fe y respaldo para las actividades en la economía real.

La génesis griega de la criptografía está dada por *Kryptos* que significa oculto y la *Graphia* que significa escritura y es definida como: el arte de escribir con clave secreta o de un modo enigmático, con el propósito de proteger la información de observadores no autorizados.

La funcionalidad de la *Criptoeconomía* se ve plasmada en las ventajas del *bitcoin* y las principales C*riptomonedas*:

Pagos entre personas y empresas sin intermediarios y sin barreras geográficas o políticas.

Inclusión financiera mundial, basta un *smartphone* para hacer transacciones, sin necesidad de que las personas estén bancarizadas o tengan que acudir a intermediarios tipo PayPal o Western Unión. Remesas y transferencias a bajo costo.

No se requiere, para su funcionamiento y preservación de valor, de una regulación y/o la confianza de un tercero.

Mantener, y muy

probablemente, aumentar el poder adquisitivo de las personas dada la cantidad finita de *bitcoin* a circular (21 millones).

Privacidad en las transacciones.

Factibilidad de realizar micro-pagos.

Imposibilidad de congelamiento de fondos.

Resuelve el problema del doble gasto o clon de dinero digital.

Crowdfunding en *Criptomonedas* con reglas

innovadoras de gestión para participantes y ejecutivos.

Transparencia y seguridad en las transacciones.

Intercambiar valor de una forma digital mediante contratos inteligentes.

La *Criptoeconomía* hace uso de la criptografía y de la distribución descentralizada de datos para elaborar formas y mecanismos para usos económicos. La combinación de sistemas distribuidos con la criptografía asimétrica da forma a los aspectos técnicos de lo que hoy conocemos como *Blockchain*, que es la tecnología bajo el

Bitcoin.

Un sistema distribuido, es aquel que está compuesto por varios ordenadores autónomos conectados mediante una red de comunicaciones y equipados con programas que les permiten coordinar actividades y compartir recursos.

La criptografía asimétrica o de clave pública, que es la usada en la *Criptoeconomía*, emplea una doble clave (una pública y otra privada) y tiene la ventaja que una de las claves puede hacerse pública sin que por ello la seguridad de la clave secreta se vea afectada; una aplicación es la firma digital que hoy conocemos. La clave privada permite al usuario firmar

transacciones, la clave pública permite a la red verificar las firmas y la dirección *Bitcoin* permite recibir transacciones.

La *Blockchain*, que es la tecnología que sustenta al *bitcoin*, es una base de datos compartida y descentralizada en miles de ordenadores, que funciona como un libro contable que registra transacciones, cantidades, fechas y participantes. Esta tecnología, al utilizar claves criptográficas y ser distribuida por muchos nodos (ordenadores), presenta ventajas en la seguridad frente a manipulaciones o fraudes (La *Blockchain* de *Bitcoin* jamás ha sido *hackeada*). Una modificación en una de

las copias no tendría efecto alguno, realizar un cambio fraudulento al mismo tiempo en todas las copias alojadas en los ordenadores, es prácticamente imposible, simplemente por el altísimo costo y poder de cómputo que se necesitaría para llevarla a cabo.

La Criptoeconomía está en proceso de cambiar al mundo y lo hará gracias al sustento de la *Blockchain* que interrelaciona tecnologías ya existentes, pero usadas de manera magistral, tales como ciencias informáticas, criptografía y teoría económica.

Descentralización

Si algo tenía en mente el anónimo creador del protocolo del *Bitcoin*, Satoshi Nakamoto, era el diseño de un sistema de pagos descentralizado entre personas, que estuviera gestionado por una comunidad sin la necesidad de un tercero de confianza centralizado. De esta forma, sacar del juego a la banca comercial y los bancos centrales que tanto daño hicieron a muchas personas

en la última mayor crisis financiera ocurrida hace una década, se presume, motivó al creador de la primera criptomoneda.

Bitcoin es tan solo el comienzo de cómo se puede descentralizar la sociedad. Gracias a la *Blockchain*, la tecnología bajo el *Bitcoin*, podemos hacer envíos de dinero sin cuenta bancaria, disponer de voto electrónico seguro, gestionar historiales médicos personales y de acceso privado, etc., y a un costo muy bajo. Al descentralizar la confianza, lo que estamos haciendo es poder hacer transacciones entre personas sin la necesidad de que se conozcan, ni de acudir a un

intermediario. Lo anterior es posible, a través d e mecanismos de consenso automatizados. La confianza no está en las personas o instituciones sino en un procedimiento de consenso informático.

Cuando hablamos de *Criptoeconomía* es necesario entender uno de sus sustentos, La Descentralización. Ésta consiste en realizar la validación y consenso de las transacciones o datos sin ningún tipo de autoridad central que imponga su criterio. La tecnología *Blockchain* o cadena de bloques, está dando lugar a un nuevo patrón económico basado en la descentralización de la confianza,

donde podremos intercambiar bienes y servicios sin necesidad de terceros o intermediarios. Este concepto abre la puerta a un abanico diverso de aplicaciones sin necesidad de un servidor central que haga de intermediario y use nuestra información y aumente los costos de uso, es así, como en un breve tiempo, veremos los clones de *Uber*, *Spotify, Airbnb, Google, YouTube, Facebook* y/o *WhatsApp* en su versión descentralizada, donde la comunidad será la propietaria/beneficiaria de sus bondades y será posible gracias a la descentralización de la gestión de datos. La transferencia de activos digitales y la descentralización en la gestión de

activos y/o datos hacen que la tecnología *Blockchain* cautive y convenza que su revolución nos hará ver y entender el mundo desde otra forma. Las empresas que no se adapten acabarán teniendo un impacto negativo o simplemente tendrán que cerrar operaciones.

Dependencia bancaria en entredicho

"Bitcoin le hará a los bancos lo que el correo electrónico le hizo a la industria postal". Rick Falkvinge

El *Bitcoin* y las *Criptomonedas* en general, dada su estructura de validación

y consenso de datos descentralizada, no requieren de la presencia de un banco o institución central en la ecuación, tanto en su monitoreo, regulación, emisión y control de la moneda. Lo anterior, hace que los bancos no estén del todo felices con la irrupción de la tecnología y miren la *Criptoeconomía* como un serio competidor a su modelo de negocio, toda vez que el *Bitcoin* permite realizar transacciones confiables, baratas, rápidas y libres del control de un gobierno o banco central.

La dependencia de la banca está en entredicho por las bondades del *Bitcoin*: No requieres cumplir requisitos para abrir una cuenta, no hay costos de

mantención, las comisiones de transacción son muy bajas, no hay límites en transferencias y lo puedes usar y transferir en cualquier parte del mundo.

Respaldo y dinero digital

El dinero tal como hoy lo conocemos, billetes y monedas, es lo que se denomina dinero fiduciario, dinero que es respaldado por la confianza de la sociedad, es decir, no tiene respaldo en metales preciosos como el oro, como alguna vez existió, sino más bien en el consenso general de las personas en que su dinero tiene valor. El dinero que tenemos en nuestra billetera, no es más

que papel impreso con una cifra y que una institución como un banco central hace su tarea de velar por la estabilidad de la moneda, y de esta forma, tratar que la inflación no merme el poder adquisitivo que ese billete tiene impreso.

Las funciones de un banco central permiten al dinero fiduciario gozar de aparente respaldo, regulando la cantidad de dinero en circulación, velando por la estabilidad de la moneda mediante una baja y estable inflación en el tiempo, logrando así un sistema financiero saludable.

Lo anterior ha quedado en entredicho para los libertarios defensores del

Bitcoin, dada la evidencia de la última crisis financiera que desestabilizó el sistema financiero mundial, que trajo consecuencias graves para la economía doméstica de millones de personas. Lo anterior no fue previsto a tiempo por la Reserva Federal de Estados Unidos, lo que habría motivado el descontento generalizado en las instituciones centralizadas encargadas de evitar crisis económicas. Este descontento permitió el surgimiento de la innovación de Satoshi Nakamoto, el de buscar un dinero digital como forma de intercambio de valor entre personas, que no esté bajo la supervisión de una institución, sino más bien, en el consenso de la comunidad y sea esta

quien dicte las directrices que requiera la criptomoneda.

El respaldo estaría dado no por un Estado y sus instituciones, sino por la confianza matemática de un poder de cómputo distribuido y descentralizado que validaría las transacciones y que por el diseño del código no tendría presiones inflacionarias, dado el aumento decreciente y predecible de la masa monetaria (21 millones de *Bitcoin* como tope máximo en circulación), lo que ayudaría a mantener y mejorar el poder adquisitivo de los poseedores de la moneda.

El *bitcoin* no se diferencia del todo al dinero fiduciario, toda vez que, su

respaldo está en la fe o confianza de las personas y no en la convertibilidad de un activo que posea valor intrínseco como los metales preciosos.

Si bien es cierto que aún no estamos habituados a los usos que brinda el *Bitcoin*, como sí lo estamos para el dinero convencional o para cualquier otro activo tangible, podemos inferir que si necesitamos hacer una transferencia de un lugar a otro y la hacemos en la red *Blockchain,* usando *bitcoin* u otra *Criptomoneda*, la operación tiene un costo más económico que un banco o una empresa de remesas, lo que supone una ventaja, lo anterior genera una demanda en el uso de la tecnología y eso

significa asignar valor a su aplicabilidad. No debemos olvidar que el *bitcoin* posee una cotización de precio, desde hace ya muchos años en los mercados, asignándole valor. Para muchos, el *bitcoin* soluciona los inconvenientes inherentes a la confianza en emisores e intermediarios que requiere el dinero tradicional.

Es visto como una desventaja para el *bitcoin* no tener un respaldo en algo tangible o en algún activo físico, no obstante, es justamente el no tener un respaldo físico centralizado lo que permite disponer de las ventajas en el uso de *bitcoin*, toda vez que su naturaleza es descentralizada. Disponer

por ejemplo de un respaldo en oro, que ni siquiera el dinero convencional lo tiene hoy en día, sería centralizar la confianza en alguna institución que pueda cuidar y hacer de custodio de ese respaldo y que por lo demás confiemos en que no nos defraudará.

La regulación deberá crear reglas que no solo piensen en evitar su uso delictivo, sino más bien, para respaldar a quienes de forma responsable utilizan la moneda virtual.

Startups y criptomonedas

A la fecha todo el mercado de

monedas digitales tiene una valorización de más de 240 mil millones de dólares, teniendo el *bitcoin* una participación de un 50% en todo el *criptomundo*. Existen más de 2.000 monedas digitales en el mercado y son miles los cruces entre ellas que se pueden intercambiar en casas de cambios o *Exchange*.

La *Criptoeconomía* nos trae nuevas formas de recaudar fondos para las empresas de reciente formación. El modelo es simple: Las empresas publican en internet toda la información de su proyecto y entregan una dirección electrónica donde los interesados puedan enviar su aporte, que en su mayoría son en *Criptomonedas* clásicas

como el *bitcoin* o *ether*. A cambio del aporte, los interesados o inversionistas reciben una criptomoneda o ficha digital (*Tokens*) propia del proyecto financiado. El objetivo de quien hizo un aporte, es vender las fichas digitales a un precio superior y así lograr beneficios importantes, lo anterior es cuando el proyecto se encuentre en etapa de operación.

En el año 2017 las ofertas iniciales de *Criptomonedas* o *ICOs* (*Initial Coin Offering*, acrónimo que evoca la expresión IPO o Initial Public Offering, utilizada en la apertura a bolsa), recaudaron miles de millones de dólares. Todas lo han hecho fuera de los

mercados de capitales formales, y en su mayoría, exentas de regulación ya que no poseen registro, autorización ni verificación por los organismos competentes de supervisión de valores. Lo anterior, no ha impedido que el interés por levantar financiamiento a iniciativas empresariales relacionadas a las *Criptomonedas* y la tecnología *Blockchain* siga creciendo.

Las *ICO,* como forma de financiar proyectos basados en la *Blockchain,* se asemeja al *crowdfunding* pero con la diferencia que con esta última se obtiene el producto que la empresa venderá, en cambio, en una *ICO* obtenemos *Tokens* o fichas digitales que permiten adquirir

los servicios de la plataforma de la *Startup,* o bien, según las características de cada *ICO* y con la incorporación de un contrato inteligente, ser parte de los beneficios que produzca la iniciativa ya en etapa de operación.

Los propietarios de los *Tokens* pueden negociarlos en las casas de cambio donde esté listado. La gran mayoría de quienes invierten en *ICO* lo hacen con montos menores, lo que supone una oportunidad de democratizar el acceso a alternativas de inversión y buena parte tiene la intención de que el *Tokens* se valorice con el tiempo y logren obtener una utilidad, dado el mayor precio respecto a la colocación

inicial.

Países como Suiza y Singapur han regulado las *ICOs,* y hoy en día, experimentan un incipiente volumen de iniciativas que favorecen su ecosistema. Los países que regulen adecuadamente las *ICOs,* se verán beneficiados de una buena parte del pastel que supone el potencial de la *Blockchain*.

Las tecnologías digitales están permitiendo la democratización de la economía, en un sentido colaborativo. Esto es posible, gracias a la combinación de la tecnología *Blockchain*, *Criptomonedas*, *Tokens*, *ICOs* y Contratos Inteligentes, todo lo anterior, dando forma a la

Criptoeconomía. El sustento de la revolución del internet del valor está en, ya no confiar en los Estados y bancos centrales para asegurar la estabilidad de nuestro dinero, sino más bien, en un algoritmo y en la criptografía, las cuales ofrecen una operación automática, inmutable, perpetua, global y descentralizada.

Para la autoridades, las *Criptomonedas* carecen de valor intrínseco, y su inversión es altamente riesgosa dado a su alto grado especulativo, advirtiendo a los inversores que podrían experimentar la pérdida total de su dinero, debido principalmente a que las *ICOs* serían

emprendimientos en fase inicial de desarrollo, y por consiguiente, existe total incertidumbre en su flujo de caja futuros.

Marco Regulatorio

A la fecha, en gran parte del mundo no existe un reconocimiento legal o reglamentario de las monedas digitales, y por lo pronto, no tienen pensado emitir normativa para permitir su uso, no obstante, las economías que han regulado algunas aristas del ecosistema son: Estados Unidos, Reino Unido, China, Japón, Alemania y Argentina. Por otro lado, quienes han prohibido el uso d e *bitcoin* son: Islandia, Vietnam,

Taiwán, Bangladesh, Bolivia y Ecuador.

El boom de *bitcoin*, la escalada y descenso abrupto en los precios de las *Criptomonedas*, su extrema volatilidad, el potencial uso criminal y los no pocos fraudes que se han dado en temas relacionados a las monedas digitales, han repercutido en que varios Estados han planteado regular la joven industria.

Los intereses por regular van, desde evitar la evasión de impuestos, el lavado de activos, el financiamiento terrorista y criminal, hasta la protección de los clientes bancarios ante posibles burbujas y estafas.

A la fecha, los pocos países que han

dado un marco regulatorio lo han hecho en específico a casas de cambio de *Criptomonedas* (*Exchange*), y a la Oferta Inicial de Monedas (*ICO*, en su sigla en inglés).

Generalmente, las regulaciones van más lento que los avances tecnológicos y es por eso que el desafío es que su redacción e implementación no detenga o entorpezca el desarrollo de la tecnología, la que necesita mucha holgura y flexibilidad para desarrollarse a un nivel que beneficie a la comunidad en el menor tiempo posible. Siempre es preferible la regulación y no la prohibición. La regulación sienta una base legal para la operación formal de

nuevos negocios, y a su vez, permite la competencia entre empresas similares.

Empresas y bancos han tomado medidas que han dificultado el camino para el *criptomundo*, argumentando que es una forma de proteger a los consumidores de posibles estafas y de los efectos de una potencial burbuja dada por la especulación acelerada de los precios del *bitcoin* y otras monedas.

Un caso reciente se dio en Chile, cuando la banca comercial decidió dejar de operar con los clientes que su unidad de negocio fuese el intercambio de monedas digitales, argumentando que estaban protegiendo a los usuarios finales de posibles fraudes y que las

compañías operaban en un marco fuera de la ley. Finalmente, el TDLC (Tribunal de Defensa de la Libre Competencia) de Chile determinó que la medida de cerrar las cuentas corrientes, por parte de los bancos comerciales a *Exchanges* que operan en el país, era arbitraria y ordenó reabrirlas.

Empresas como *Facebook*, han determinado prohibir publicidad relacionada a monedas digitales, y los principales bancos de Estados Unidos han prohibido comprar *bitcoin* con sus tarjetas de crédito. Países se suman a su intención de regular el uso de las *Criptomonedas* como medio de pago y a toda forma de financiar iniciativas

colectivas con *Tokens* (fichas digitales que permiten la transferencia de la titularidad de activos).

Cada vez existen más países con la intención de regular la industria de las *Criptomonedas,* con el objetivo de acabar con el anonimato en las transacciones, y así exigir documentos oficiales a quienes quieran participar del mercado mediante empresas que operan en el intercambio de monedas digitales.

Hay quienes ven con buenos ojos la regulación, ya que entrega certeza a las bondades del *bitcoin,* y por consiguiente, su posible mayor uso y valoración en el tiempo, no obstante, los

defensores del *bitcoin,* lo consideran contrario a la intención de la génesis de su creador, que es la libre circulación de dinero entre las personas sin las trabas impuestas por fronteras, gobiernos y leyes.

bitcoin y Criptomonedas

El bitcoin y su comienzo

El *bitcoin* es una moneda digital o electrónica descentralizada, creada por una o varias personas anónimas el año 2009, con el seudónimo Satoshi Nakamoto. Se ha definido al *bitcoin* como la evolución del dinero, tal como lo conocemos hoy, siendo su principal

característica que no se requiere confiar en una tercera parte para asegurar el intercambio, es decir, no requiere de un Banco Central que regule su emisión ni necesita de un banco comercial que intermedie en la transacción entre dos personas.

La cantidad total de *bitcoin* en circulación será de 21 millones. A la fecha, hay más de 16 millones, el año 2032 se crearán el 99% de ellos y su tope máximo será cumplido el 2140. El diseño del algoritmo no puede ser modificado, dada su naturaleza descentralizada, y su creador no tiene mayor poder ni control sobre el *bitcoin* que cualquier otro usuario del software.

Lo anterior, busca que el *bitcoin,* al igual que el oro, sea deflacionario, lo que quiere decir que mientras más escaso es un bien es mucho más probable que tenga valor.

El valor del *bitcoin* es definido por la oferta y demanda, y su respaldo, al igual que el dinero fiduciario de curso normal como dólares o euros, se basa en la confianza que las personas depositan en él.

Cada b*itcoin* se puede fraccionar en 8 decimales, la mínima expresión se le conoce como Satoshi y equivale a 0,00000001 *bitcoins*.

Cabe mencionar que *Bitcoin* - con B

mayúscula, se utiliza para describir el protocolo y/o concepto de red de *Bitcoin*. Por otro lado, *bitcoin* – con minúscula, se utiliza para describir la unidad monetaria del mismo.

¿Por qué utilizar bitcoin?

Algunas ventajas:

Transacciones muy económicas, anónimas y no rastreables

No requiere de un banco o cuenta bancaria.

No hay un organismo central que controle.

Permite pagos internacionales en minutos. Dos personas sin conocerse pueden intercambiar valor gracias a la descentralización de la confianza y validación de la operación, entre otras.

Las transacciones no son identificables con nombre y apellido, pero sus direcciones digitales sí son rastreables, debido al carácter público de la *Blockchain* detrás del *Bitcoin*.

El *bitcoin* y todas las *Criptomonedas* utilizan algoritmos matemáticos que permiten garantizar la seguridad, al no poder clonar o falsificar el dinero digital, y a su vez, verificar la autenticidad de una operación.

El *bitcoin,* que en sus comienzos se transaba en unos pocos centavos de dólar, ha experimentado un aumento en su valor de manera paulatina, el año 2017 tuvo una apreciación acelerada de su precio cotizando en valores cercanos a los 20.000 dólares, a fin de ese año. Al segundo semestre del año 2018, ha experimentado un descenso promedio en su valor en más de un 70%.

Breve cronología del bitcoin:

Noviembre 2008: Satoshi Nakamoto publica en un foro de criptografía el paper "*Bitcoin*: Un sistema de efectivo electrónico de "Peer-to-Peer".

Enero 2009: Satoshi Nakamoto registra el primer bloque en la red *Bitcoin* y la emisión de los primeros *bitcoin*, siendo la primera entrada en el registro de transacciones de la moneda digital.

Octubre 2009: Se crea el primer tipo de cambio a razón de 1.309 *bitcoin* por 1 dólar; el cual suponía el costo de crear o minar las monedas digitales.

Mayo 2010: Se intercambian 2 Pizzas por 10.000 *bitcoin*.

Junio / Julio 2010: Satoshi Nakamoto realiza su última contribución al código del *Bitcoin* y ya no se podría tener rastro de él.

Julio 2010: La empresa japonesa Mt. Gox inicia sus operaciones en el intercambio de *bitcoins*.

Agosto 2010: Se da lugar al único fallo de seguridad importante en la historia del protocolo *Bitcoin*. Se vulnera, se detecta y se soluciona en cosa de horas.

Febrero 2011: Se alcanza la paridad, 1 dólar por 1 *bitcoin*.

Junio 2011: Roban 600 cuentas de la empresa japonesa Mt. Gox, lo que conlleva una caída en el precio del *bitcoin* cotizándose en 1 centavo de dólar.

Septiembre 2012: Se crea la Fundación *Bitcoin* para acelerar el crecimiento global de *Bitcoin*.

Octubre 2012: El servicio de procesamiento de pagos *BitPay* dispone de más de 1000 comerciantes que aceptan *bitcoins*.

Marzo 2013: El *bitcoin* se aprecia fuertemente, dada la demanda como refugio de valor ante la crisis financiera griega.

Julio 2013: Se solicita la apertura del primer fondo de inversión en *bitcoin*.

Octubre 2013: Comienza a funcionar el primer cajero automático que

dispensa *bitcoin* en Vancouver, Canadá.

Noviembre 2013: El *bitcoin* logra la paridad con la onza de oro, cotizándose en 1.000 dólares americanos.

Diciembre 2013: China prohíbe el *bitcoin* como medio de pago en el comercio electrónico.

Enero 2014: La circulación de *bitcoin* ya supera las 14 millones de unidades.

Marzo 2014: El *Exchange* japonés Mt. Gox se declara en quiebra.

Septiembre 2014: Se solicita a la Comisión de Futuros de Estados Unidos, autorización para cotizar un producto en

el mercado extrabursátil basado en el precio del *bitcoin*.

Diciembre 2014: Microsoft acepta el pago en *bitcoin* en varios de sus productos.

Marzo 2015: La empresa relacionada con el *bitcoin* 21Inc logra recaudar 116 millones de dólares como capital de riesgo para sus operaciones.

Agosto 2015: Se estima que 160.000 comercios aceptan pagos en *bitcoins*.

Febrero 2016: Japón promueve una modificación de la normativa para considerar a *bitcoin* como una moneda corriente de curso legal.

Septiembre 2016: El número de cajeros automáticos que dispensan *bitcoin* supera las 770 unidades.

Abril 2017: Japón es el primer país en legalizar el *bitcoin* como forma de pago.

Junio 2017: El *bitcoin* se cotiza en 3.000 dólares.

Agosto 2017: Un desacuerdo dentro de la comunidad *Bitcoin* sobre la velocidad de las transacciones produce el nacimiento de una nueva moneda virtual: *bitcoin* Cash.

Diciembre 2017: El *bitcoin* se cotiza sobre los 20.000 dólares. *bitcoin* entra a

cotizar al mercado de futuros de Chicago.

Enero 2018: Diferentes Estados anuncian la regulación de las *Criptomonedas*. *Facebook* prohíbe la publicidad relacionada a las divisas digitales. Bancos prohíben la compra de *bitcoin* con sus tarjetas de crédito.

Febrero 2018: El precio del *bitcoin* baja a los 6.200 dólares, un 70% desde su máximo histórico para luego cotizar en valores cercanos a 10.000 dólares.

Agosto 2018: La SEC rechaza la apertura de ETFs en *bitcoin*.

Septiembre 2018: El *bitcoin* se cotiza

en 6.500 dólares.

La tecnología detrás del bitcoin

La tecnología que da sustento al *bitcoin* es la *Blockchain*, una mezcla magistral de tecnologías ya existentes antes de la creación de Nakamoto, las cuales son la criptografía y los sistemas distribuidos.

L a *Blockchain* es el protocolo que funciona por debajo de las *Criptomonedas* y que se caracteriza por ser global, descentralizada, inmutable, perpetua, segura y de acceso generalizado.

La *Blockchain* o cadena de bloques, es un registro único y no editable de transacciones que se encuentra y funciona en modo automático, de manera simultánea en una red de ordenadores.

L a *Blockchain* no solo sirve de soporte a las *Criptomonedas* sino a una serie de aplicaciones de distintos ámbitos. Basa su genialidad, en el proceso de validación de las transacciones o datos sin la necesidad de un agente centralizado de confianza, como un banco o una empresa intermediaria.

Cómo se crean los bitcoin

Los *bitcoin* no se emiten ni se fabrican, sino más bien, se crean o "minan" por la acción de los "mineros", a través de un proceso informático.

El algoritmo original *Bitcoin* diseñó un sistema de recompensa para los propietarios de los ordenadores, que con su poder de cómputo validarían las transacciones que se generan en la red *Bitcoin*. La recompensa por cada bloque de transacciones validado será en *bitcoin* de nueva creación, los cuales son creados de forma automática en la dirección digital del propietario del ordenador o red de ordenadores.

La minería consiste en realizar complejos cálculos mediante la acción

de ordenadores de gran poder computacional que compiten, sin intervención humana, para lograr resolver un problema matemático que deriva en la confirmación de las transacciones en la red *Bitcoin* y así dar seguridad a los intercambios.

Los mineros logran ingresos, aparte de los *bitcoin* de recompensa, a través de comisiones que son un costo de transacción para los interesados. La minería, hoy por hoy, es un mercado especializado y competitivo. La recompensa por cada bloque minado comenzó en 50 *bitcoins* y cada dos años se reduce a la mitad, hoy la recompensa es de 12.5 *bitcoins*.

Minería de bitcoin

Tal como comentábamos en el apartado anterior, la minería, a diferencia de la minería de metales preciosos, dispone de una recompensa a cambio de poder computacional que logre resolver y validar las transacciones, y de esta forma, permitir que la red de pago funcione de manera segura.

Para poder minar *bitcoins*, se

requiere ejecutar un software que el algoritmo *Bitcoin* desarrolló para que cada diez minutos se formara un bloque de operaciones, a la espera de ser validado para su posterior confirmación. El primer minero o grupo de mineros (pool) en encontrar la solución al problema criptográfico que presenta el bloque, es el que obtiene un nuevo lote de *bitcoin*.

En un principio era posible minar *bitcoins* con la CPU de los ordenadores de casa, pero con el correr del tiempo y el aumento en la dificultad, significó disponer de tarjetas gráficas de mayor cómputo como las GPU, para luego quedar obsoletas y ser reemplazados por

los ASIC de hoy. La industria del hardware continúa en su carrera meteórica por proveer de equipos con mayor poder de cómputo y menor gasto energético para los pool mineros, una actividad lucrativa a la fecha, dado los precios actuales del *bitcoin*.

Las comisiones o tarifas que los mineros reciben por las transacciones que validan, serán las que en el futuro mantenga la industria del minado (y por consiguiente la continuidad de operación de toda la red *Bitcoin*), ya que en algún momento se habrán minado cada uno de los 21millones de *bitcoins* y ya no existirá recompensa en *bitcoin* de nueva creación.

El negocio de la minería depende en buena parte de la inversión en ordenadores de gran poder de cómputo, bajos costos de electricidad y refrigeración y de espacio físico adecuado y accesible en precio.

Hoy en día las personas pueden acceder al negocio de la minería a través de tres formas: Una, es acceder a servicios de minería en la nube, la otra, es acudir a financiar una *ICO* que su actividad sea el minado y por último, instalar una granja de minado.

La primera opción consiste en adquirir poder computacional y recibir *bitcoin* o fracciones de estos en base a ese poder. Lo atractivo de esta

alternativa es que no necesitas la infraestructura, sino más bien, la "arriendas" o "compras" por un plazo determinado para tener ingresos. Las variables que influyen en la rentabilidad de la minería en la nube tienen que ver con la dificultad de minar (la cual se ajusta cada 14 días, de tal forma de lograr una cantidad de *bitcoin* minados a cierta velocidad), la cotización del *bitcoin* y el tiempo de arriendo del poder computacional.

En la segunda alternativa, al acudir a una *ICO,* el aportante recibe *Tokens* o ficha digital que en algunos casos le permitirá participar de las ganancias que logre el proceso de minado, y por otro,

liquidar esos *Tokens* a un mejor precio en el mercado, una vez que la iniciativa empresarial entre en operación.

Por último, armar una granja de minado requiere de una inversión mayor en equipos de minado, infraestructura, gastos de energía y refrigeración.

Oportunidades y riesgos

El creciente uso del bitcoin no ha hecho más que confirmar las ventajas para las personas y el comercio en general. Nos encontramos en una etapa que busca establecer al *bitcoin* y las Criptomonedas en general, como medio de pago seguro, rápido y barato. Los esfuerzos están centrados en posicionar

a las monedas digitales para lo que fueron creadas: Un medio de pago sin fronteras ni intermediarios. Sin horarios, bajas comisiones, sin bancos, sin límites de cantidad, seguridad criptográfica y privacidad en las operaciones son algunas de las ventajas.

La extrema volatilidad actual, el potencial uso delictivo, la posible regulación excesiva o prohibición, la falta de conocimiento y aceptación, el uso de esquemas Ponzi y estafas a personas sin mayor conocimiento, la irreversibilidad de las transacciones y las vulnerabilidades de una tecnología en proceso de maduración, ponderan los riesgo del *bitcoin*.

Wallet o Monedero

Un monedero o *wallet*, por su traducción en inglés, es una billetera virtual encriptada que da seguridad para guardar, recibir y enviar *Criptomonedas* o *Tokens*.

Una billetera digital entrega una dirección o clave pública para que podamos recibir *Criptomonedas*, generalmente en forma de código QR, y una dirección o clave privada para

poder firmar las transacciones para gastar o enviar esas *Criptomonedas*.

Podemos obtener un monedero en:

Sitios web tales como *Blockchain*.info, *MyEtherWallet* o *Coinbase*.

En nuestro ordenador a través de los programas como *Bitcoin* o *Waves*.

Y en nuestro *smartphone* con las app *Blockchain*.info o Waves.

Es recomendable mantener la clave pública y privada impresa en un lugar seguro, ya que el soporte papel protege ante la vulnerabilidad de tener tu

información de direcciones en algún dispositivo móvil, ordenador o en la web. Cabe mencionar, que el extravío o el olvido de las claves significará que perderemos para siempre nuestras *Criptomonedas,* ya que *Bitcoin* u otra plataforma no cuenta con la opción de recuperación de contraseñas.

Cómo adquirir bitcoin

Existen varias formas de adquirir *bitcoin*:

Obtener *bitcoin* mediante el proceso de minado:

Obtener la recompensa en *bitcoin* que el protocolo permite, como se explicó

en el apartado Minería del *Bitcoin*. Para ello, se requiere invertir en poder computacional capaz de verificar un bloque de transacciones. Existen tres formas: Armar una granja de minería invirtiendo equipos de minado; comprar poder de cómputo para minar a través de un servicio en la nube; y por último, participar de una *ICO* donde su actividad futura sea la minería de *Criptomonedas,* o bien, comprar *Tokens* de empresas ya en operación.

Comprar *bitcoins* en casas de intercambio:

Existen varias casas de cambio online o *Exchanges* disponibles para realizar

la compra de *bitcoin* y muchas otras *Criptomonedas*. Estos se pueden adquirir con moneda local, tarjetas de crédito o vía otras monedas digitales.

Abrir una cuenta es muy simple y breve. *Exchanges* como *Binance, OKEx, Bitfinex, Huobi* u *Orionx*, por nombrar algunos, permiten fondear las cuentas con dinero fiat (de curso legal) o en *Criptomonedas*. Muchos de estos intermediarios solicitan documentos de identidad por seguridad o regulación. Existen *Exchanges* que permiten realizar Trading de *Criptomonedas* pudiendo de esta forma también ganar o perder *bitcoins*.

Comprar *bitcoins* en un Cajero Automático

Existen en ciertos países red de cajeros que aceptan la compra de *bitcoin* con dinero en efectivo y se transfieren a tu dirección digital. También da la opción de imprimir un código QR con las claves respectivas.

Aceptar *bitcoins* como medio de pago

Permitir pagos de productos y servicios valorados en *bitcoins* es una de las formas más habituales de conseguirlos. Recibes pagos en tu monedero digital de forma directa o a través de aplicaciones que permiten el

procesamiento de pagos en las principales *Criptomonedas*.

Comprar bitcoins de forma directa entre personas

El intercambio se realiza transfiriendo *bitcoin* a la *Wallet* o monedero electrónico, previo pago con dinero fiat u otra moneda digital al vendedor. Existe la web *localbitcoins.com* que facilita la compra entre personas.

Las empresas que ofrecen servicios a los usuarios de *bitcoin* para facilitar su uso, tales como, casas de cambio o *Exchanges*, monederos virtuales, sistema de procesamiento de pagos,

cajeros automáticos y tarjetas de pago, benefician al ecosistema, no obstante, todas estas aplicaciones no son imprescindibles para realizar operaciones con *bitcoin*, ya que su red y código está hecho para proveer de aquella función básica.

bitcoin como medio de pago

La génesis del *bitcoin* se encuentra en la usabilidad de la moneda como medio de pago, fue la intención de Satoshi Nakamoto cuando publicó su *paper*.

Cada día aumenta de forma importante la cantidad de transacciones,

y con ello, la red de comercios que aceptan *bitcoin* y otras *Criptomonedas*.

Aún estamos en una etapa donde la mayor cantidad de transacciones son con intención especulativa, dado el alto y rápido crecimiento que experimentaron las monedas digitales en el año 2017, no obstante, ya son muchas las aplicaciones tecnológicas que están dando soporte a la red de negocios para hacer del pago e n *bitcoin*, *Ether, Litecoin, Ripple* o *IOTA* una forma simple, rápida y habitual.

El sitio Coinmaps.org nos informa de los comercios en el mundo donde se aceptan pagos en *Criptomonedas*. A la fecha en Latinoamérica, la red de

negocios es aún insuficiente, Buenos Aires, Santiago, Bogotá y México lideran la incorporación.

Hoy el *bitcoin* posee ciertas restricciones: Tiene una limitante operativa de 7 transacciones por segundo, la confirmación de la transacción por los mineros demora en promedio 10 minutos, y producto del aumento del precio del *bitcoin,* existe imposibilidad de realizar micropagos. Estas restricciones están siendo abordadas por dos iniciativas: *SegWit* y *Lightning Network*.

El aumento en el número de transacciones tiene una dificultad en la

red *Bitcoin: Es* incapaz de procesar todas las transacciones de forma rápida, lo que se conoce como el problema de escalabilidad del protocolo original del *Bitcoin*. Lo anterior, ya está siendo abordado por una serie de aplicaciones que ayudarán a mejorar la gestión de pagos con *Criptomonedas*, así tenemos por ejemplo a *SegWit* que busca aumentar la cantidad de transacciones, la velocidad de verificación y los recursos que emplea. Otra es *Lightning Network* que busca acelerar las *Blockchain*s, usando *Smart Contract*s, solucionando limitaciones técnicas tales como: pagos instantáneos sin problemas en los tiempos de confirmación, procesar millones de transacciones por

segundo a costos reducidos fuera de la cadena de bloques y permitir micro-pagos.

¿Y cómo realizo un pago en bitcoin?

La mayoría de los puntos de venta usan un teléfono móvil o Tablet para aceptar pagos en los smartphones de sus clientes. Así por ejemplo, en un comercio físico es tan simple como escanear el código QR con la dirección

del monedero digital del comercio, digitar la cantidad y pagar con un toque. No son necesarias firmas, tarjetas o digitar un PIN. Si lo que necesita es recibir pagos en *bitcoin*, es justamente lo contrario: Mostramos el código QR de nuestro monedero digital, el cliente lo escanea y procede a aceptar el pago por la cantidad requerida.

bitcoin como inversión especulativa / trading

El trading es la compra y venta de algún activo o mercancía en un mercado con el objetivo de obtener ganancias mediante la diferencia de precio. Si compramos a 100 y diez minutos

después vendemos a 105, hemos logrado una ganancia de 5. Si por el contrario el precio cotiza en 95 y decidimos vender, hemos perdido 5.

La mayor cantidad de transacciones d e *bitcoin*, hoy en día, es gracias al trading. La especulación es de vital importancia para dar liquidez al mercado de Criptomonedas.

Si hay un tipo de empresa que ha despegado en el ecosistema son los *Exchanges*, casas de intercambio que permiten comprar y vender Criptomonedas contra dólares, euros o moneda local.

A modo de ejemplo, en Chile existen

a la fecha cuatro Exchange y 50 comercios que aceptan *bitcoin*, pero es el primero el que mueve prácticamente todo el volumen transado en Criptomonedas.

¿Es el bitcoin una buena inversión?

A pesar de los detractores del *bitcoin,* el consenso de la mayoría es que en el mediano - largo plazo la apreciación será una realidad; desde sus inicios el *bitcoin* no ha hecho más que confirmar su aumento de precio a pesar de la gran volatilidad en su cotización. Pero también hay evidencia en el mundo

de la inversión, y es que la mayoría no siempre acierta a sus pronósticos.

Potencial futuro del bitcoin

El *bitcoin* llegó para quedarse, si bien es cierto que su potencial de uso como medio de pago aún está en fase temprana, no son pocos los esfuerzos del ecosistema en avanzar en su posicionamiento; cada día se observan nuevas aplicaciones y usos con la ayuda de una comunidad activa y comprometida.

Para algunos una burbuja reventada, para otros el nacimiento de una

tendencia mundial, pero de lo que sí hay certeza, es que habrá mayor regulación en el uso de las *Criptomonedas* y de las *ICOs*, sin embargo, lejos de entorpecer su crecimiento dará pie a una mayor confianza para los que aún desconfían en sus aplicaciones prácticas.

Siempre existe el riesgo de una regulación poco flexible y muy prohibitiva, que haría daño al ecosistema, en ese contexto, el peor de los escenarios lo tendríamos en el supuesto que las cinco mayores economías del mundo, de forma coordinada, prohibieran todo lo relacionado a las *Criptomonedas*. Pese a lo anterior, las tecnologías disruptivas

y los emprendedores detrás de ellas, buscarán los lugares y las redes para llevar a cabo la labor de beneficiar a la comunidad mundial.

No debemos confundir la moneda *bitcoin* con la *Blockchain*, esta última, trascenderá a miles de aplicaciones descentralizadas que ayudarán a la sociedad y que no harán más que confirmar que las *Criptomonedas* son una excelente aplicación sobre la confianza que entrega la cadena de bloques. La base de datos descentralizada es el futuro inmediato.

Respecto al precio del *bitcoin,* sin duda buscará un valor de equilibrio por un tiempo, luego de subidas y bajadas

abruptas, con alta volatilidad y movimientos de precios que asustarán a muchos, no obstante, el mediano y largo plazo dará la razón a una moneda deflacionaria como el *bitcoin*.

Otras Criptomonedas

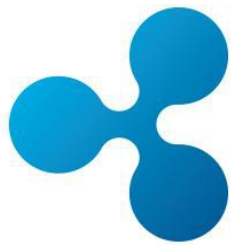
Entre monedas y *Tokens* existen más de 2.000, la cantidad no nos debe sorprender ya que es propia al boom que vive por estos días la tecnología *Blockchain*. Pero como ha ocurrido con otras innovaciones pasadas, luego de un tiempo, el universo se acota bastante y es probable que tan solo un puñado de ellas se ocupe para transacciones comerciales masivas.

Veamos algunas de ellas:

ETH Ethereum

Moneda descentralizada que es soportada en la red de código abierto *Ethereum*, red que permite ejecutar, una vez cumplidas las condiciones, códigos o programas autoejecutables llamados contratos inteligentes en el modelo *Blockchain* y es justamente la característica que da potencial de uso y crecimiento muy interesante. La red *Ethereum* es la preferida para realizar

ICOs que ofrecen *Tokens* a cambio. Ha tenido un crecimiento exponencial desde su aparición el año 2015, pasando de centavos, a un máximo en torno a los 1.380 dólares a principios del 2018. Actualmente (octubre 2018), posee el segundo lugar con una capitalización de mercado cercana a los 25 mil millones de dólares.



XRP Ripple

Conocida como la criptomoneda de los bancos. Basada en tecnología

Blockchain privada, provee de un sistema de pagos para los bancos y de esta forma realizar transacciones más rápidas, económicas y convertibles en multidivisas y *Criptomonedas*. A principios del 2018 logró un máximo de 3.8 dólares. Hoy (octubre 2018), posee el tercer lugar en capitalización de mercado con un valor cercano a los 23 mil millones de dólares.

BCH Bitcoin Cash

Esta moneda virtual nace en agosto del año 2017, como una alternativa al

bitcoin, luego de hacer un *fork* o bifurcación de la red *Bitcoin* para solucionar en parte la lentitud de ésta última en procesar las transacciones. En diciembre de 2017 logró un máximo de 4.300 dólares. Hoy posee el cuarto lugar en capitalización de mercado con un valor cercano a los 10 mil millones de dólares.

LTC Litecoin

Fue creada como alternativa al

bitcoin con rasgos diferenciadores tales como: su rapidez en la confirmación, un bloque se genera cada 2.5 minutos, a diferencia de los 10 que demora el *bitcoin*, la creación de moneda será de 84 millones y la minería requiere de menos sofisticación técnica en los equipos. En diciembre de 2017 logró un máximo cercano a los 370 dólares. Hoy (octubre 2018), posee el séptimo lugar en capitalización de mercado con un valor cercano a los 4 mil millones de dólares.

Smart Contract - Ethereum – NEM

"Imagina un automóvil auto-conducido, comprado en grupo, capaz de autogestionarse y alquilarse por sí solo pero sin una compañía tipo Uber detrás llevándose el 25%. Bienvenido al mundo de los contratos inteligentes". *www.bit2me.com*

Todo intercambio o transacción realizada se basa en la confianza, y para ello existen intermediarios, a través de los cuales se accede a rapidez y seguridad en la operación, pero a su vez, también a pérdida de privacidad y

engaños si el intermediario se comporta de forma cuestionable. La tecnología *Blockchain* detrás del *bitcoin*, *Ethereum* o NEM permite descentralizar estas relaciones de confianza. Trasladamos la confianza en empresas, gobiernos o personas, a un sistema autónomo, distribuido, descentralizado, con reglas transparentes preestablecidas que nadie puede modificar y todos pueden comprobar. Suena extraño y transgresor pero en la práctica pasamos de confiar en una persona a confiar en un código o algoritmo.

Los *Smart Contracts* o contratos inteligentes son códigos informáticos

que están soportados en la tecnología *Blockchain*. Permiten toda clase de innovación en lo que a contratos entre personas o empresas se refiere, sin la necesidad de un notario o intermediario de confianza externo.

Un *Smart Contract* es definido como un contrato entre dos o más partes, personas, empresas o maquinas, que es capaz de ejecutarse y hacerse cumplir por sí mismo, de manera autónoma y automática.

Como una forma de potenciar el uso de los *Smart Contracts* existen protocolos y plataformas sobre las cuales se pueden crear, veamos un par de ellas:

Ethereum

Es la plataforma de código abierto que evoluciona al *Bitcoin,* ya que si bien, ambas son tecnologías descentralizadas basadas en el modelo *Blockchain*, Ethereum permite la creación de contratos inteligentes entre pares. A modo de ejemplo, en *Ethereum* podemos ejecutar un código informático que puede transferir automáticamente la propiedad de una vivienda al comprador y los fondos monetarios al vendedor después de llegar a un acuerdo, sin necesidad de un tercero.

El *Ether* es la criptomoneda que usa la plataforma para ejecutar los contratos.

Ethereum es una de las *Blockchain más utilizada* por los desarrolladores de aplicaciones ya que además de poder diseñar *Smart Contracts,* es utilizada como soporte en la emisión de *Tokens* para levantar financiamiento vía *ICOs*.

Recordemos que los *Tokens* son fichas digitales creadas en una *Blockchain* como *Ethereum* que permiten la transferencia de la titularidad de activos, de una persona a otra o de una empresa a otra. Los *Tokens* ERC20 son un subconjunto de los *Tokens* de *Ethereum* que garantizan

su interoperabilidad, en simples palabras, permiten que los *Tokens* conversen entre sí en un mismo estándar y así intercambiar información y utilizarla.

Entre las principales diferencias de *Ethereum* respecto al protocolo *Bitcoin* podemos ver que: el tiempo de procesamiento de las transacciones es de 16 segundos en teoría versus los 10 minutos de *Bitcoin*; la cantidad de decimales que soporta la moneda de *Ethereum* es de 18 y *Bitcoin* 8; la recompensa por minar es constante en *Ethereum* a diferencia de *Bitcoin* que decrece en la mitad cada cuatro años aproximadamente; *Ethereum* no tiene

límite en la creación de monedas a diferencia de *Bitcoin* que tiene un tope máximo de 21 millones.

NEM

N E M *(New Economy Movement*) como plataforma basada en la *Blockchain* presenta una serie de características que la hacen muy atrayente para la comunidad interesada en el ecosistema, ya que tiene aspectos técnicos que facilitan su uso, tal como su poder de procesamiento de datos por la red descentralizada, de forma rápida y a muy bajo costo comparada con *Ethereum* y *Bitcoin*.

NEM, en su última versión, es capaz de procesar 4.000 transacciones por segundo, frente a las 20 de *Ethereum* o las 1.700 de Visa. Tiene una comunidad de desarrolladores y potencial de uso muy activo. XEM es la criptomoneda de NEM y agrega funcionalidades a las ya conocidas, tales como: Registrar *Smart Assets* o Activos Inteligentes, que pueden ser patentes, documentos notariales o títulos de propiedad que al incorporarlos a NEM pueden ser transferidos y registrados sin necesidad de notarios o registros de comercio o propiedad.

Al igual que *Ethereum*, la plataforma NEM te permite crear *Tokens* sin

conocimientos previos de programación y así poder crear y lanzar una *ICO*.

Una propiedad de gran potencial es que NEM tiene todo para realizar procesos eleccionarios o votaciones, proporcionando seguridad, siendo útil para las democracias participativas en el mundo ya que entrega automatización, velocidad, seguridad, transparencia y ninguna posibilidad de manipulación en los registros de votos.

ICOs

El constante crecimiento de las *Criptomonedas* en los últimos años, ha traído consigo una innovadora forma de

financiamiento sustentada en la tecnología *Blockchain*, las *ICOs* o Initial Coin Offering. Esta es una forma de levantar financiamiento colectivo o *Crowdfunding,* donde sin depender de intermediarios, un emprendedor anuncia su idea, crea una criptomoneda, o bien, un *Tokens* y lo vende para conseguir el dinero con el que hará realidad su negocio.

El último año hemos sido testigo de *ICOs* que han recaudado sus objetivos de financiamiento en horas e incluso segundos, así por ejemplo: *Bancor* recaudó 153 millones de dólares en tres horas; *Gnosis* captó 12 millones de dólares en 12 minutos; y *Brave*, en tan

solo 30 segundos, recaudó 35 millones de dólares. Lo que vemos aquí es una revolución por financiar innovaciones que se alojen en la tecnología *Blockchain*.

La plataforma preferida para lanzar una *ICO* es *Ethereum*, dado que su diseño permite la creación de contratos inteligentes junto a fichas digitales o *Tokens* que hacen de moneda de cambio a los aportes en moneda Fiat o digital de los inversionistas.

Existe una ventaja para las empresas o *Startup*s, a diferencia de una rueda de financiamiento privado, y es que quienes compren *Tokens* no reciben acciones de la empresa, por ende, no tiene propiedad

sobre ella, más bien los aportantes esperan una revalorización al alza de sus fichas digitales en un futuro y así acudir a los *Exchanges* para poder vender a mejor precio que el inicial, y por consiguiente, lograr un retorno importante y que recompense con creces el riesgo propio de una inversión de este tipo.

Las *ICO* en la mayoría de los países no son consideradas ilegales, no obstante, no están reguladas, situación que los inversionistas deben ponderar, ya que no existe ninguna protección a los aportes monetarios entregados, más que las propias que se derivan de las ventajas de la tecnología *Blockchain*.

Desde la primera *ICO,* allá por el año 2013 y su boom el año 2016 y 2017, las iniciativas financiadas son de las más variadas áreas, tales como finanzas, medicina, informática, redes sociales, juegos de azar, educación, inmobiliarias, cultura, etc.

Veamos algunos ejemplos de *ICOs* emblemáticas:

Mastercoin: Fue la primera *ICO* en obtener financiamiento en julio de 2013, recaudó 500.000 dólares. Su propuesta trataba sobre la creación de una plataforma descentralizada para crear y comercializar activos y

monedas digitales sobre la *Blockchain* del protocolo *Bitcoin*. Cambió de nombre a *Omni*.

Ethereum: Lanzó su *ICO* el año 2014 recaudando 18,4 millones de dólares. Su propuesta consistía en desarrollar una plataforma *Blockchain* descentralizada que tuviera como característica principal la creación de contratos inteligentes y el diseño de aplicaciones descentralizadas (Dapps). *Ethereum* marcaría un antes y un después en la evolución de las *ICOs,* ya que posterior a su

diseño, muchas *ICO* se crearon sobre su plataforma gracias a los contratos inteligentes y sus *Tokens* ERC20.

Augur: En el año 2015 lanzó su *ICO* logrando captar 5,1 millones de dólares. Su propuesta consistió en incorporar la tecnología *Blockchain* al mercado de apuestas y predicciones.

IOTA: Su *ICO* en el año 2015 levantó 440.000 dólares, pero lo impactante, es que a diciembre del año 2017 su valor de mercado ascendió a 1400

millones de dólares. La propuesta de *IOTA* es proveer una plataforma descentralizada que diera solución a la seguridad y gestión de los datos de IoT o Internet de las Cosas.

Iconomi: Su objetivo era diseñar una plataforma descentralizada de fondos de inversión, tanto indexados como hedge fund, en criptoactivos y *Criptomonedas*. Su *ICO* tuvo lugar el año 2016 y logro recaudar 10,5 millones de dólares.

The DAO: Fue concebida el año 2016 para crear un fondo de

inversión descentralizado que invertiría en criptoproyectos. Es tal vez la más criticada *ICO* que ha tenido lugar en el *criptomundo* y no es por la captación de fondos, pues logró la nada despreciable suma de 152 millones de dólares, todo un récord, sino por el ataque cibernético que sufrió unos meses después. Un hacker, a través de una vulnerabilidad en un contrato inteligente, retiró 60 millones de dólares.

Filecoin: En agosto de 2017 logró captar 252 millones de dólares y lo hizo en un plazo muy acotado,

superando las expectativas. Su propuesta consistía en una red de almacenamiento de archivos o datos en una *Blockchain*. Su *ICO* fue cerrada a inversores previamente acreditados para así cumplir con la regulación de los Estados Unidos.

¿Qué información debemos tener en cuenta al momento de analizar una ICO?

Estudiar su *Whitepaper*: El libro blanco es el documento donde las empresas presentan su proyecto, detallando su producto y su equipo detrás. Aquí vemos los aspectos técnicos, la problemática a resolver y cómo piensan desarrollar la solución. E l *Whitepaper* es la primera aproximación al proyecto, no obstante, debemos profundizar la investigación con fuentes

externas, tales como: Web de *rating*, estudios paralelos, comentarios en foros y el respaldo del equipo gestor.

Time Line u Hoja de Ruta: Aquí te informas del plan de la empresa a corto, mediano y largo plazo. Aquí debemos mirar con ojo técnico y crítico la factibilidad de llevar a cabo cada etapa en los tiempos que plantea la empresa.

Equipo de Gestión: Es importante analizar el currículo de los integrantes directos en la gestión de la empresa, sus perfiles históricos en *Linkedin*, su

experiencia en el sector donde operará la compañía. Aquí también se debe investigar al equipo asesor y cotejarlo si están en otras *ICOs* y que tal les ha ido al presente.

Capital Recaudado: La compañía debe informar cuánto dinero desea recaudar para financiar el proyecto, así como también, su *Soft Cap* o financiación mínima viable. Junto con lo anterior, es importante saber cómo distribuirán y administrarán esos fondos. Debemos analizar si la distribución es equitativa, o por el contrario, habrá muchos

recursos destinados a los gestores y a su contribución.

La criptomoneda o *Token*: La cantidad de *Tokens* a emitir y el cómo se distribuirán es un dato a tener en cuenta, así como también que otorgarán a cambio de tu inversión. Existen por un lado *Tokens,* que son capital o deuda a favor del inversor, y por otro, los que te entregan un derecho de uso para un servicio o producto de la futura compañía. Una pregunta a ser resuelta por el equipo gestor, con toda claridad, es si hubo una Pre*ICO* informando el precio y

cantidad de *Tokens* emitidos.

Comunidad: Debemos analizar si el proyecto ha generado una comunidad participativa en torno a la idea de negocio. Aquí debemos ver las redes sociales en torno a la idea y grupos de conversación como *Telegram*. Investigar si el equipo del proyecto aporta contenido, códigos o herramientas a su comunidad.

Autoría de Código: No siempre es bueno que la compañía diseñe todo el código desde cero, más bien, si reutilizan una *Blockchain* ya validada es una

ventaja para el proyecto.

Rating: Tener la opinión de un tercero sobre las características de una ICO la podemos ver en varias web de rating especializadas en estas iniciativas:

www.icorating.com

www.crushcrypto.com

www.icoindex.com

www.crytocompare.com

Viabilidad legal: Dada la insuficiente regulación de las *ICO* a nivel mundial, son pocas

las compañías que informan en su *Whitepaper* las aristas legales a la emisión de *Tokens,* tanto para los inversionistas como para la empresa. Si un proyecto tiene respaldo legal es una ventaja para el inversor, no obstante, muchas veces es a cambio de perder su anonimato y privacidad de sus datos personales.

¿Dónde puedo ver las próximas ICOs?

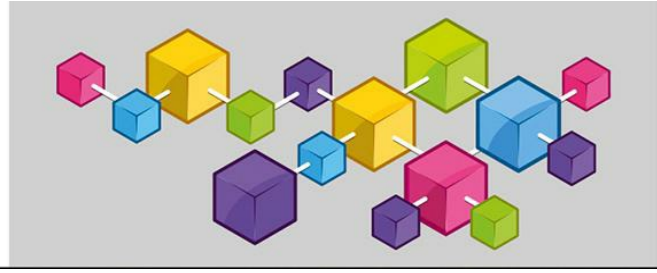
Las próximas *ICOs* se pueden ver en sitios web tales como:

www.ico-list.com

www.icoalert.com

www.icotracker.net

www.icocountdown.com



Blockchain

¿Qué es la Blockchain?

La *Blockchain* en términos simples es una base de datos compartida y descentralizada que opera como un libro contable registrando "en piedra" transacciones y/o datos. Su extrema seguridad es posible gracias a la utilización de claves criptográficas y a la distribución de su información de manera íntegra por muchos ordenadores

o nodos, lo que la convierte en una tecnología "Inhackeable" o no vulnerable a manipulaciones o fraudes. Una modificación o alteración en una copia de la información no tiene efecto alguno, ya que se tendría que hacer en todas las copias distribuidas en miles o millones de ordenadores al mismo tiempo para pretender hacer daño, lo que es prácticamente imposible. Lo que pasa en la *Blockchain* se queda en la *Blockchain*.

La *Blockchain* permite tener información guardada en ordenadores o nodos que están separados geográficamente, información que es compartida, descentralizada y protegida

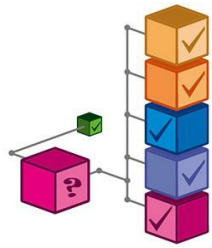
gracias a la criptografía. La *Blockchain* permite construir plataformas donde la información o datos son validados, seguros, de calidad, inviolables, verificables y no editables.

La *Blockchain* o Cadena de Bloques, por su traducción al español, promete ser la tecnología que transforme diversas industrias y es muy probable que lo haga en muy poco tiempo. Tal vez su uso más conocido ha sido el *Bitcoin,* pero su aplicabilidad es transversal a todo tipo de negocios y procesos, a nivel mundial ya vemos aplicaciones descentralizadas basadas en su filosofía.

La tecnología *Blockchain* se creó el año 2009 para crear dinero digital en

internet con la irrupción del protocolo del *Bitcoin*. Su creador anónimo, de forma magistral, hizo uso para su diseño de dos aspectos técnicos ya conocidos: La criptografía asimétrica y los sistemas distribuidos, dos conceptos descritos en el capítulo I del presente libro.

Si hay algo que hace a la *Blockchain* una tecnología confiable es el consenso, este es la piedra angular de la cadena de bloques, puesto que a través de él es posible que la comunidad de participantes pueda fiarse de los datos o información contenida en ella.



¿Cómo funciona Blockchain?

Los autores de territorioblockchain.es lo explican con un ejemplo: *"Imaginemos que estamos en una plaza repleta de gente en la que no conocemos a nadie, de pronto somos testigo de que alguien roba una bicicleta. Cuando nos preguntan a todos sobre lo ocurrido, lo más probable es que coincidamos en la versión de los hechos. Si alguien intenta dar otra versión, el resto de las*

personas la dejaremos en evidencia ya que todo el resto hemos visto lo ocurrido. Es prácticamente imposible poder mentir o hacer trampa. Todos comparten la misma versión de lo que ha pasado.

Así es cómo se valida la información en la Blockchain. Participantes que no se conocen y que no tiene por qué confiar los unos en los otros, validan lo que ha ocurrido porque han visto o comprobado los mismos datos que el resto de los participantes.

Una vez que la información se introduce en la red no puede ser borrada y queda distribuida en todos los ordenadores participantes. Todo

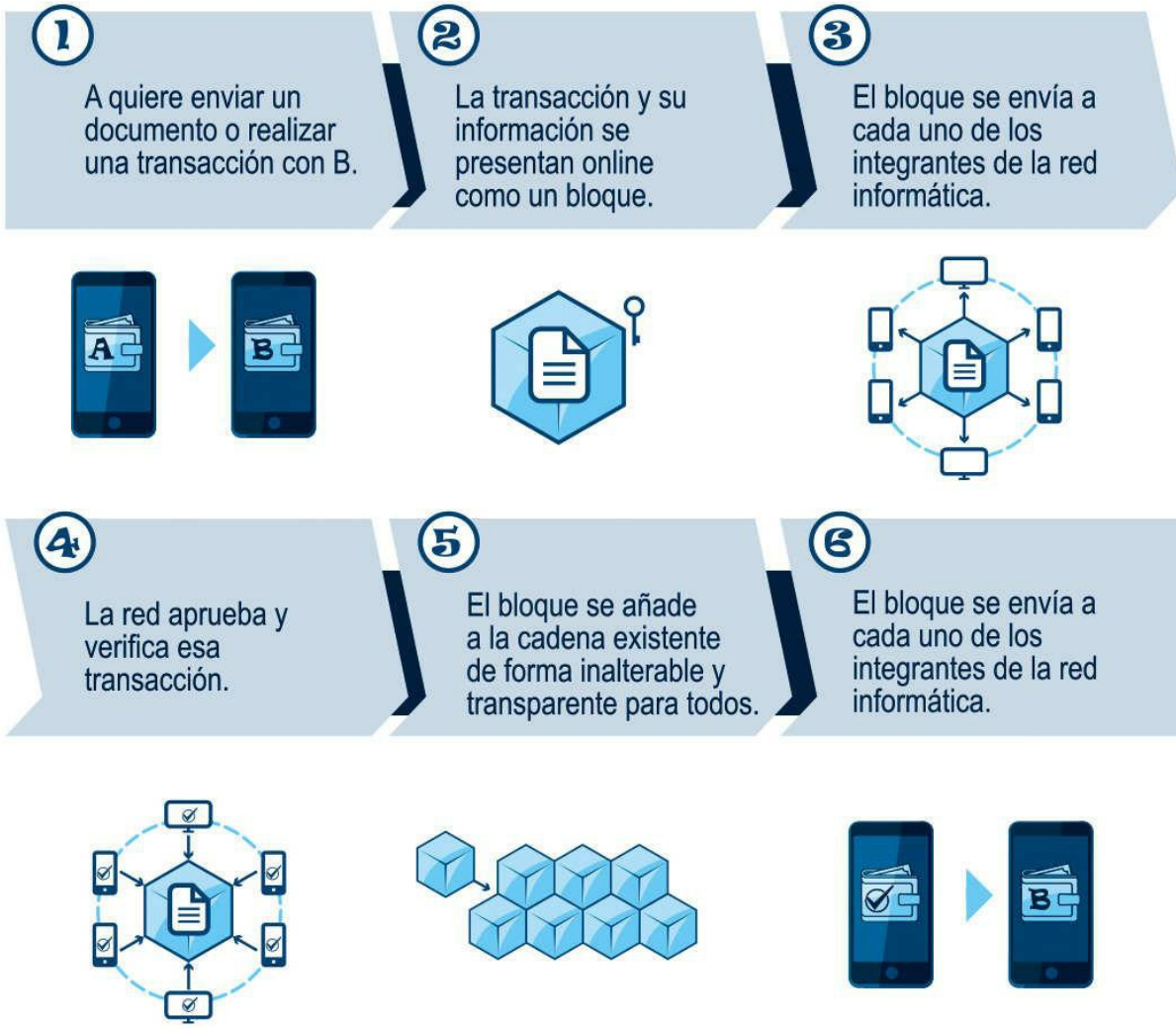
esto permite que desaparezcan los intermediarios, se reduzcan los costos en las transacciones y haya más seguridad y transparencia en determinados procesos".

Una forma simple de representar el funcionamiento de la *Blockchain* descrita por *Stock Logistic* la veremos a continuación:

1. A desea enviar un documento o realizar una transacción con B.
2. La transacción y su información se representan on-line como un bloque.
3. El bloque se envía a cada

uno de los integrantes de la red informática.

4. La red aprueba y verifica esa transacción.
5. El bloque se añade a la cadena existente de forma inalterable y transparente para todos.
6. La transacción se ha completado. B ha recibido la transacción de A.



El problema del Doble Gasto o Double Spending

Crear dinero digital y hacer transferencias con él tenía un problema no resuelto, hasta antes de la creación del protocolo *Bitcoin,* y es el Doble

Gasto.

En un contexto de dinero digital, sin la ayuda de un banco que haga de intermediario, surgen las siguientes interrogantes: ¿Cómo probamos que hemos pagado algo? ¿Cómo probar que disponemos del dinero para realizar una compra sin que un banco nos avale?

El problema del doble gasto es definido como una vulnerabilidad del dinero digital por el que una misma moneda pueda gastarse más de una vez, o dicho de otra forma, cómo evitamos falsificar o duplicar la moneda digital ya que es un archivo y los archivos son copiables o clonables fácilmente.

Satoshi Nakamoto solucionó el problema con su diseño del protocolo *Bitcoin* y lo hizo cimentado en el diseño de una red descentralizada que no permite gastar más de una vez los *bitcoins* disponibles.

Blockchain y el Internet del valor

La Internet nos permitió enviar información de una persona a otra, la *Blockchain* permite enviar valor o activos digitales de una persona a otra. No es sino con la irrupción de la *Blockchain,* cuando fue posible transferir dinero por internet de manera descentralizada, y con la creación del

Bitcoin, el primer ejemplo de esa particularidad.

El dinero que tenemos en una cuenta corriente, números en una pantalla respaldados por depósitos o líneas de crédito, está centralizado por un Banco, él hace de intermediario entre los fondos y a quienes son enviados. Confiamos en que el banco, una vez realizado un depósito, tendrá la capacidad de pagarnos el dinero cuando giremos de un cajero o lo usemos como medio de pago. Para ejercer esa labor, el banco tiene una infraestructura en donde lleva el registro del balance de las cuentas, entradas y salidas, es el banco el que hace de "tercero de confianza" entre las

transacciones entre dos personas: Valida que existan los fondos y que son transferidos a ese único destinatario, no pudiendo usar ese mismo dinero a dos destinatarios distintos al mismo tiempo y así "clonar" ilegalmente los fondos. Ese proceso y muchos otros tienen un costo para el cliente del banco.

La *Blockchain* elimina la confianza de la ecuación, la confianza en un tercero, en una persona, institución bancaria o gobierno y la sustituye por validación matemática a través de ordenadores descentralizados, inmutables, automáticos, de bajo costo, perpetuos y no arbitrarios al poder de unos pocos, ya que la información y/o

datos en la cadena de bloques es un registro que no tiene propiedad, nadie es dueño de ella ni tiene el poder para modificarla a su antojo. Alguien definió la *Blockchain* como el resurgimiento de la noción de comunidad.

El internet del valor basa su concepto en el consenso y validación. Para disponer de dinero digital a través de internet, algo impensado antes de la creación de Satoshi, se requiere de una base de datos, que registre todas las transacciones y el balance de las cuentas, pero al igual que el rol de un banco comercial, necesitamos un respaldo o un validador de confianza o ministro de fe y es aquí donde el autor

del protocolo *Bitcoin* ideó, de manera elegante, que todas las personas tengan en su ordenador una copia de esa base datos de transacciones y que al cambiar los saldos, dada las operaciones de salidas y entradas, todos estén de acuerdo o exista consenso. Con este mecanismo ideó la forma de crear dinero en internet.

Junto con lo anterior, era necesario diseñar un proceso seguro y no reversible o editable de forma maliciosa, y para aquello, Satoshi Nakamoto hizo uso de un mecanismo de consenso: La prueba de trabajo o *Proof of Work* en su traducción al inglés, lo que constituye la clave de la forma de

operar de la *Blockchain*. Esta prueba consiste en el uso de matemáticas complejas para descifrar, validar y confirmar las transacciones que han tenido lugar en la red, para lo cual se requiere de poder computacional elevado (Rol de los mineros).

Las transacciones verificadas forman un registro o libro contable, llamado cadena de bloques, cadena porque cada bloque está enlazado o referenciado al anterior. Resolver un bloque de transacciones pendientes es de una gran complejidad matemática, tratar de editar o "truquear" un dato significaría que tendríamos que modificar todos los bloques anteriores, lo cual es

prácticamente imposible por el poder de cómputo que se requiere, además de resultar carísimo, lo cual constituye una ventaja en la seguridad de la información.

Blockchain Privadas – Públicas

La *Blockchain,* en simples palabras, es una base de datos resguardada criptográficamente y que está distribuida o repartida entre muchos integrantes; se organiza en bloques de transacciones que están conectados en forma matemática. Cada usuario puede ver los datos y verificarlos utilizando algoritmos, los datos verificados se

introducen a un libro mayor como una colección de bloques, para luego ser almacenados en forma cronológica y asegurados vía criptografía.

La base de datos puede ser accesible por cualquiera que lo estime conveniente, lo que define a una *Blockchain* Pública, o bien, con acceso restringido, que es el caso de una *Blockchain* Privada. Los procesos de ambas siguen siendo validados de forma descentralizada, no debemos confundir *Blockchain* Privada con validaciones centralizadas.

Blockchain Públicas

El *Bitcoin* fue la primera base de datos pública y descentralizada que vio la luz. La *Blockchain* fue creada en su génesis para ser abierta, descentralizada y pseudoanónima, que es lo que define a una *Blockchain* pública. Cualquiera que así lo desee, tiene permiso para participar de ella de forma libre y consultar los datos que en ella se registran de forma inmutable. No hay participantes ni nodos que tengan más poder que otros dada su naturaleza descentralizada. Las *Blockchain* Públicas suelen ser pseudoanónimas, donde las transacciones no son registradas con datos personales, no así sus direcciones digitales que si son *trackeables* o de fácil identificación de

sus movimientos.

Blockchain Privadas

El sector financiero, sector público y cada vez más industrias, están haciendo uso de todas las bondades de una *Blockchain*, no obstante, producto de que su información debe ser confidencial, hace que la *Blockchain,* elegida para sus operaciones tenga la característica de Privada.

En este tipo de base de datos, si bien usa un código público, no está al alcance de todos, el usuario debe ser invitado. Existen varias formas de estructurar una cadena de bloques

privada: cerrada y con usuarios identificados o bien abierta y usuarios anónimos.

El ser distribuida, característica propia de una *Blockchain*, tiene la particularidad que el número de ordenadores o nodos que conforma la base de datos privada es limitado a la cantidad de usuarios o una parte de ellos.

Los datos escritos en "piedra" en este tipo de *Blockchain,* no pueden ser consultados por quien lo desee, tan solo los usuarios que posean el permiso.

Muchos defensores de las *Blockchain* Pública ven con recelo la apertura de su

versión Privada, ya que esgrimen que transgrede la intención original de su diseño, que es la descentralización de su operación. No obstante lo anterior, el uso de la *Blockchain* en todas sus versiones, públicas, privadas o híbridas, posicionan a la tecnología y la acercan a la economía real y a las actividades cotidianas de la sociedad.

El uso de *Blockchain* Privadas aporta a las organizaciones una base de datos con información inalterable, transparente, trazable, de reducido costo y con rapidez en sus procesos.

A modo de ejemplo, en Chile dentro del sector financiero y mercado de capitales, la Bolsa de Comercio de

Santiago tiene implementada una *Blockchain* Privada y dentro del Sector Público, la Comisión Nacional de Energía está haciendo uso de la tecnología *Blockchain,* como un notario digital, para certificar la calidad y certeza de los datos abiertos del sector energético.

Fuente de Verdad

Todos los usuarios de la Blockchain tienen acceso a una fuente compartida de verdad. La Blockchain no solo provee de una base de datos distribuida, cifrada y abierta, sino también, de una fuente de verdad para operaciones o transacciones entre personas, donde no es necesario

que se conozcan, ni que confíen mutuamente, ni de un notario físico que entregue la fuente de confianza. La confianza de una red descentralizada no está en un banco, institución, compañía o gobierno, sino en la misma red, en su verdad matemática y el consenso de sus usuarios que son la infraestructura de la Blockchain.

Automática

Todos los pasos que requiere el proceso de transacciones, validaciones y registros se hacen de manera automática gracias a la conexión en red, datos en tiempo real online, el software y los protocolos que sustentan la

columna vertebral de una Blockchain.

Inmutable

Cuando hablamos que la Blockchain asegura una base de datos escrita en piedra o inmutable, nos referimos a que la información incorporada no pueda modificarse, permanece inalterable, sin poder editarse. Lo anterior es posible, gracias a la seguridad que entregan los algoritmos criptográficos y la labor colectiva de la red. Esta característica promueve un gran potencial de uso, en una sociedad que demanda más transparencia y trazabilidad en la información, la cual debe ser inalterable.

Perpetua

La Blockchain asegura que los datos, transacciones o archivos que administre sean eternos, perduren por siempre, que sea posible conservarlos y mantenerlos para dar certeza a su uso.

Descentralizada – Distribuida

La Blockchain se ejecuta en miles, sino millones de ordenadores y está abierta a cualquier persona u organización, no es controlable quien participa. No está al arbitrio de un poder central que tenga dominio absoluto. No hay espacio a la manipulación o control a razón de un mayor poder de unos nodos sobre otros. Nadie es dueño de la información ni puede venderla a otros. En un sistema centralizado la información es controlada por un único organismo, a diferencia de la Blockchain, que basa su concepto en la descentralización donde

los nodos u ordenadores conectados e iguales entre sí controlan la red.

La base de datos que conforma la Blockchain no es almacenada en un solo lugar, sino que se distribuye a través de miles de ordenadores y dispositivos en todo el territorio global.

Proceso de Consenso – Validación

Los nodos que conforman la red a

través de la minería, verifican y confirman las transacciones pendientes, asegurando así la inalterabilidad de las operaciones, para luego formar un bloque que será parte de la base de datos irreversible y vigente.

El proceso se inicia con las *Wallet* que originan las transacciones, las firman y las envían a los nodos. Los nodos u ordenadores verifican las transacciones pendientes, luego esperan la acción de un minero. Los mineros toman las transacciones, las incluyen en un bloque y realizan la prueba de trabajo mediante un algoritmo matemático. Una vez resuelto, los mineros envían el bloque a los demás nodos, quienes lo

verifican y lo incorporan a la base de datos o cadena de bloques.

Usos potenciales de la Blockchain

La mayoría de las tecnologías que usamos de manera cotidiana, en los ordenadores personales o en nuestros *smartphones*, no las entendemos a cabalidad, su funcionamiento técnico es complejo de asimilar, no obstante, hacemos uso de ella de una forma práctica y nos beneficia en los más diversos ámbitos. Pasa lo mismo con la *Blockchain*, ésta no necesita ser comprendida sino aplicada en usos prácticos que beneficien a la sociedad.

La cadena de bloques puede ser utilizada en variados aspectos, uno de ellos es en los procesos, en donde diferentes empresas, que están en la misma cadena de distribución, pueden evitar procesos de conciliación de datos. Otro uso es en la tokenizacion en donde *startups* pueden financiarse contra la entrega de *tokens*, que son fichas digitales intercambiables por servicios futuros o bien representar con *tokens* algún activo físico o intangible para de esta forma facilitar su intercambio. Para diferentes sectores industriales la tecnología *Blockchain* es atractiva por la transparencia, precisión y velocidad con la que es posible disponer de los datos y/o transacciones,

sumado a sus características de inmutabilidad y descentralización.

Veamos algunos usos:

Remesas y transferencias a bajo costo

Con la creación del protocolo o red

Bitcoin se establece la primera *Blockchain* de uso público que permite transferir moneda digital *bitcoin* entre personas. Con la aparición de otras monedas digitales como ETH, LTC, NEO o ADA las opciones de transferir dinero digital se han ampliado.

Aplicaciones como BitPay, *Bitcoin Wallet* – Coinbase, *Blockchain Merchant*, *Blockchain*.info o *Xapo* son una muestra del uso de la *Blockchain* en el envío de remesas y/o transferencia de monedas digitales a bajo costo.

Recordar que los *Exchanges* de cada país nos dan la facilidad de hacer el cambio de moneda digital a dinero Fiat del país de destino. En Chile y

Latinoamérica existen *Exchanges* tales como *Buda.com, Orionx* y *Cryptomkt*, entre muchos otros.

Se estima que en un breve plazo de tiempo existirán teléfonos inteligentes a un precio de 5 dólares, lo que junto a la *Blockchain*, permitirá en un futuro cercano reducir la pobreza mundial, donde millones de personas podrán transferir valor de forma digital sin la necesidad de intermediarios o de estar bancarizados, y de igual manera, incrementar la inclusión financiera.

Certificar propiedad – Bienes Digitales

mediachain

VERISART™

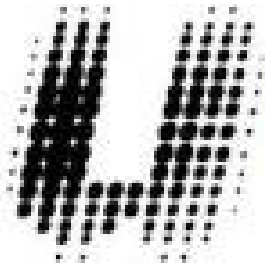
Con la *Blockchain* se podrán crear una serie de aplicaciones que permitan dar cabida a la gestión de servicios y activos digitales. Características propias de la *Blockchain*, tales como su descentralización e inmutabilidad facilitará la certificación de propiedad y transacción de activos y servicios tales como: música, obras de arte, literatura, inmuebles, dinero digital, energía,

vehículos, etc.

Una plataforma para certificar y verificar obras de arte es *Verisart* la cual usa la *Blockchain* de *Bitcoin* y viene a solucionar un problema antiguo en el mercado de las obras de arte, que es la verificación de la procedencia y así dar confianza a compradores y vendedores.

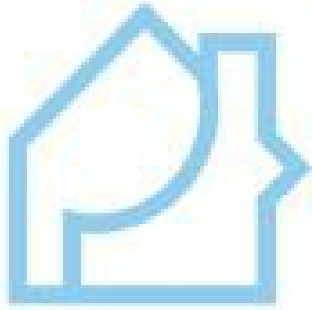
MediaChain es una empresa recientemente adquirida por *Spotify*, que permite resguardar la propiedad intelectual de creadores artísticos de tal forma que estos puedan registrar, identificar y realizar un seguimiento de su trabajo creativo en Internet.

Usos en el mercado inmobiliario



UBITQUITY

directhome



PROPY

FORT GALT

El mercado inmobiliario se

caracteriza por tener múltiples actores en su gestión, no son pocos los intermediarios que están en el proceso. Existen iniciativas empresariales que apuestan por digitalizar y automatizar el proceso de compra de un bien raíz; así es como ya podemos ver aplicaciones que a través de la red *Blockchain* distribuida de *Ethereum* y sus *Smart Contracts* es posible adquirir y registrar de manera descentralizada (sin la necesidad de notarios y archiveros y/o conservadores de bienes raíces) bienes inmuebles. Su uso tiene ventajas en transparencia, menor costo de transacción, menor plazo de compra y ampliar las fronteras de compra - venta.

Una plataforma para certificar y comprar bienes raíces es *DirectHome*, en donde compradores y vendedores de propiedades pueden realizar transacciones sin la necesidad de intermediarios, como son los corredores de propiedades o agentes de bienes raíces, a un costo nulo o extremadamente bajo.

Fort Galt es un proyecto inmobiliario comunitario cercano a la ciudad de Valdivia, Chile, fue uno de los primeros ejemplos en implementar el proceso de inversión a través de *Criptomonedas* y realizar todo el registro en una red *Blockchain*. Hoy, el proyecto ya se encuentra en etapa de construcción y

venta.

Plataformas como *Propy* y *Ubitquity* son otros ejemplos del uso de la *Blockchain* en el mercado inmobiliario.

Usos en el sector Seguros

El sector asegurador está trabajando en la implementación de la *Blockchain* y sus *Smart Contracts*, ya que su uso proporciona información veraz, reducción de costos por la disminución de trámites y una baja en la incertidumbre en las evaluaciones de riesgos. Lo anterior implica una rebaja en las primas de contratos con los

asegurados. Las aseguradoras *Liberty Mutual, Munich Re, Swiss Re, Allianz* y *Zurich* iniciaron un consorcio para estudiar las aplicaciones de la *Blockchain* en la industria.

Las aseguradoras de automóviles podrán, con el uso de la *Blockchain* y el

Internet de la Cosas, simplificar sus evaluaciones de riesgo y entregar pólizas personalizadas a cada cliente. Se podrá disponer de un historial de conducción veraz de un conductor y del estado del vehículo de forma automática escrita en la *Blockchain*. El cliente recibirá de forma automática, a través d e *Smart Contracts,* un abanico de ofertas de pólizas por todas las aseguradoras, decidirse por una y recién ahí mostrar su identidad y recibir su póliza de forma automática, no presencial y personalizada. Y ante un siniestro la activación y liquidación del seguro será rápida y automática.

Las aseguradoras prestadoras de

servicios de salud tienen ventajas de reducción de costos al usar la cadena de bloques, al poder gestionar los datos de forma descentralizada, segura y confiable, datos como contratos, prestadores, bonificaciones e historial médico; favoreciendo la interacción de centros de salud, usuarios, profesionales de la salud y aseguradoras. Lo anterior, tiene ventajas para la aseguradora al disponer de información verídica del historial médico de los asegurados. Los clientes se benefician al acceder a contratos a menor precio dada la reducción de incerteza por parte de las aseguradoras. Algunas compañías que usan la *Blockchain* en el sector seguros: ChainThat, AI Gang e InsureX.

Usos en el sistema electoral

El uso de la tecnología *Blockchain* aporta grandes ventajas a los sistemas actuales de elección democrática: Resultados irrebatibles y rápidos, sencillez en el proceso y bajo costo para el estado y la ciudadanía. Garantiza confidencialidad al ejercer el voto y que estos no puedan ser modificados.

Hoy en día existe el voto electrónico pero tiene limitaciones en transparencia y vulnerabilidad.

El uso de la *Blockchain* y sus características intrínsecas permiten el objetivo supremo de un sistema de elecciones: Resultados irrefutables. La cadena de bloques aporta de forma directa una base de datos descentralizada, transparente, con datos seguros, no editables, no hackeable, auditables, automatizados (sin intervención humana), anónimos, rápidos de procesar y eliminando la alteración o manipulación.

Las personas podrán votar desde sus casas a través de internet haciendo uso, por un lado, de una identidad entregada por la Unidad de Registro Civil de cada país, y por otro lado, la *Blockchain*

asegurando el voto anónimo. El registro del voto en la *Blockchain* queda de forma inmutable y protegido con criptografía. Los resultados estarían en tiempo real.

La Unión Europea se encuentra estudiando la implementación de la tecnología en sus sistemas de votaciones. A la fecha existen experiencias pilotos en elecciones estudiantiles en Latinoamérica.

Un ejemplo de esta funcionalidad de l a *Blockchain* es E-Vox, organización que busca fomentar una plataforma abierta de e- democracia, permitiendo procesos eleccionarios, tales como votaciones, plebiscitos y referendos

basados en la *Blockchain* de *Ethereum*.

Usos en el sector salud

MEDIBLOC

Ambrosus

HEALTH

wizz

El uso de la cadena de bloques en el sector salud ha sido una de las primeras incitativas y motivaciones que han gatillado a los entusiastas de la

Blockchain, y dadas sus características, la hacen especialmente aplicables al sector. Empresas como *MediBloc*, *Ambrosus, Health Wizz*, son algunos ejemplos del uso de la *Blockchain* en el área sanitaria. Así es como existen proyectos tales como: expedientes médicos o historia clínica con información consolidada e integrada, de tal forma de tener trazabilidad, inmediatez de datos y registro único e inmutable de exámenes, atenciones y tratamientos; la capacidad del paciente de tener el control de sus datos médicos, en uso y acceso, compartiendo su historial médico pero de forma confidencial. Lo anterior, viene a enfrentar un sistema de salud atomizado

en el que cada establecimiento de salud tiene una parte del historial médico de los pacientes, trayendo complicaciones en casos de urgencia médicas y en la duplicidad de exámenes y procedimientos que ya han sido descartados previamente.

Otra aplicación es en el consumo y producción de medicamentos; con la cadena de bloques se hace más eficiente, al poder cruzar en *Blockchain* los datos de medicamentos recetados por el médico a sus pacientes, así los laboratorios tendrían la cantidad a producir, y a su vez, el médico tendrá registro del consumo de medicamentos de su paciente.

Solo nueve de cada diez medicamentos que se venden son auténticos. Una forma de acreditar la trazabilidad y originalidad de los mismos, desde los laboratorios hasta el consumidor, es a través de las características propias de la base de datos única e inmutable que es la *Blockchain*.

Una aplicación interesante se desarrolló en la *Hackathon* de la *Blockchain Summit Latam* en Chile, donde un equipo de desarrolladores de nombre NoobChain plasmó a través de una aplicación web y móvil, una receta electrónica y de esta forma crear un mercado de remedios y/o medicamentos

donde las personas, con su consentimiento, publican la receta médica y reciben ofertas o cotizaciones de las farmacias (las cuales solo pueden visualizar los medicamentos y la prescripción), resguardando los datos personales del médico y del paciente a través de la encriptación que ofrece *la Blockchain.*

Uso en capital de riesgo y crowdfunding

BLOCKCHAIN CAPITAL

BANK TO THE FUTURE .com

godzillion

Iniciativas como *Blockchain Capital*, *BNK to the Future, Polychain Capital* y *Numerai* invierten activos digitales en proyectos que tienen como negocio central el uso de tecnologías disruptivas,

que promuevan la innovación a través de la *Blockchain*.

El capital de inversores es captado y administrado, quedando registro de la gestión activa o pasiva de los activos digitales en la red descentralizada y distribuida. Invertir a través del sistema tradicional en negocios de innovación requiere de conocimiento y un costo de administración alto, no obstante, hacerlo en proyectos *Blockchain,* vía tokenización y/o *Criptomonedas,* tiene las ventajas de acercar las inversiones al público inversionista no sofisticado, democratizando el acceso a productos de inversión.

Una nueva forma de *Crowdfunding* o

financiamiento colectivo se ha desarrollado en el ecosistema crypto, un ejemplo de ello es *Godzillion*, el cual funciona a través de una aplicación descentralizada (DApp), en la *Blockchain* de *Ethereum*, utilizando un *token* ERC-20 llamado *GODZ* relacionando a emprendedores e inversores. Los emprendedores acceden a financiamiento sin las barreras complejas que existen en la forma tradicional del *Crowdfunding* y los inversores pueden votar por las *Startup*s de su interés, invertir en sus proyectos y acceder a liquidez mediante la venta o compra de más *Tokens*.

Uso en logística y distribución

vechain

CargoX

origintrail

SHIPCHAIN

Si existe un mercado con crecimiento sostenido año a año es la logística y distribución de mercancías, y la *Blockchain* es una tecnología que puede ser de ayuda en todos los procesos necesarios en la gestión de transporte de carga y cadena de suministro.

Características como: la descentralización, encriptación, colaboración, interconexión e inmutabilidad, hacen de la cadena de bloques una tecnología aplicable a modelos de negocio que deben procesar gran cantidad de datos.

Existen usos que buscan aplicar la tecnología al sistema de tráfico de datos con el objeto de hacerlos seguros e

imposibles de manipular, toda vez que, en el comercio internacional de productos interviene una gran cantidad de agentes, y por consiguiente, no es poca la cantidad de documentos generados, los cuales mediante la *Blockchain* y *Smart Contracts* pueden ser autentificados de forma rápida prescindiendo de terceros que certifiquen y validen, reduciendo por un lado costos, plazos, duplicidad y errores, y por otro, aumentando la seguridad de la totalidad del proceso.

Otro uso es en el transporte de carga por carretera, donde sería posible hacer el encuentro de forma directa entre la demanda de carga con la oferta de

transporte, sin intermediarios, evitando viajes en vacío, y si sumamos el uso de contratos inteligentes, se podría incorporar la gestión de pago del servicio de forma automatizada.

Algunas empresas en distintas fases de desarrollo son *ShipChain, CargoX, Origintrail* y *Vechain*.

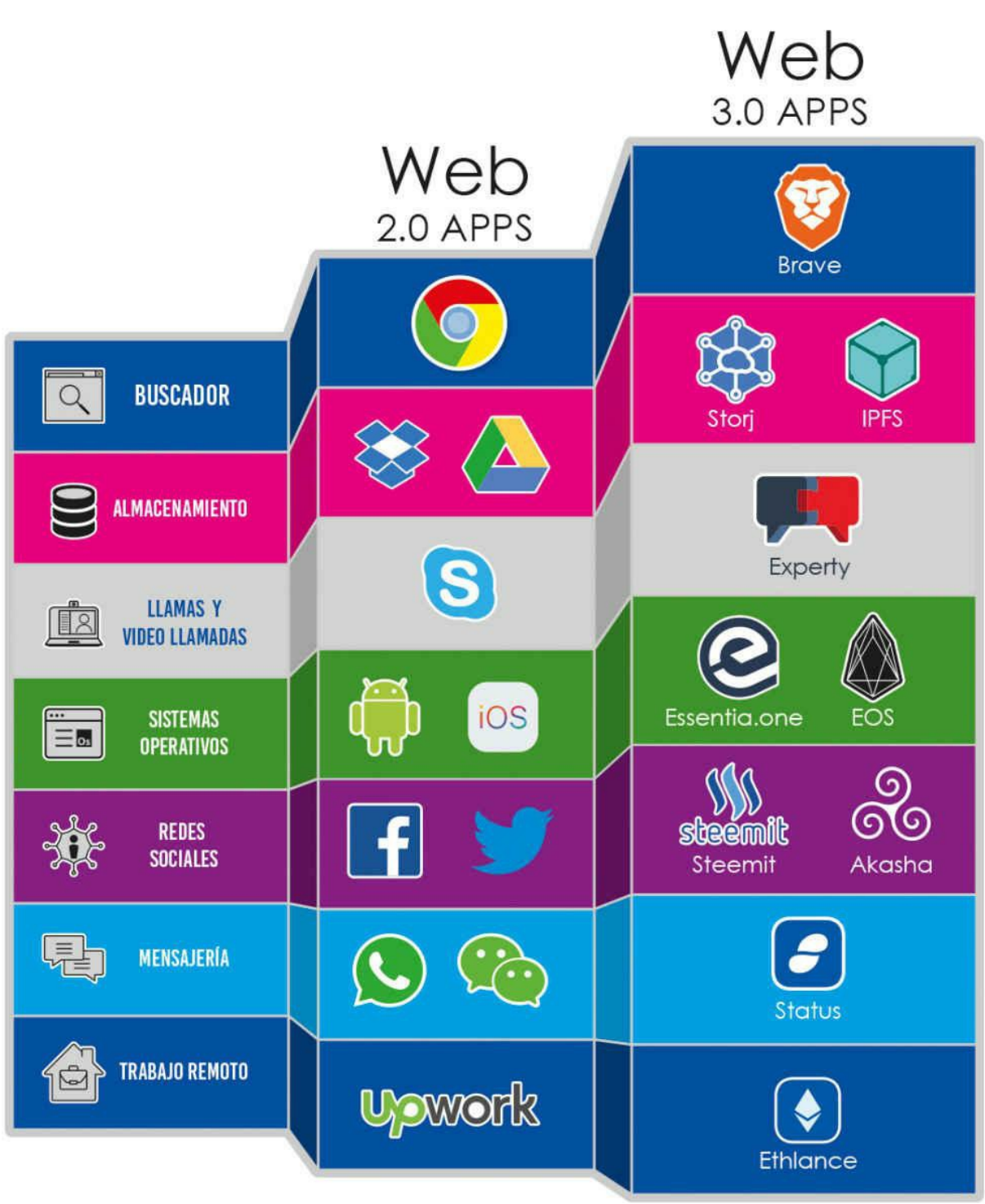
Modelos de negocios descentralizados

En los últimos dos años hemos visto los primeros pasos en la irrupción de los modelos descentralizados de negocios en las distintas áreas de la web. Estamos en transición de la Web 2.0 representada por las Apps hacia la Web 3.0 en donde son las aplicaciones descentralizas o DApps las que entregan servicios similares pero con las características de la *Blockchain*.

Una DApp es una aplicación de software que tiene su procesamiento de entrada de datos ejecutándose en una red de *Blockchain* como *Ethereum* o *NEO*.

Se diferencian de las Apps en que funcionan bajo un sistema descentralizado.

Así por ejemplo, veremos DApps en los servicios de mensajería instantánea (Status), música (Audius), video streaming (Flixxo, Viuly y Tribler), redes sociales (Steemit y Akasha), almacenamiento en la nube (Storj e IPFS), entre otras.



Usos en Internet de las cosas y la gestión de

datos

En los próximos años, millones de dispositivos estarán conectados a Internet, desde electrodomésticos, ropa, vehículos, viviendas y ciudades, siendo su objetivo la captura de información para así mejorar la calidad de vida de los usuarios y de paso nutrir de datos, vía Big Data, para el desarrollo de la inteligencia artificial.

La Blockchain, junto a otras tecnologías que aporten velocidad y eficiencia, traería escalabilidad y una red masiva de nodos para cumplir con las demandas de almacenamiento de datos de forma conveniente, segura y

rentable a través de la cadena de bloques.

Algunas iniciativas son IOTA, Hdac, IoT Chain, MOECO y Atonomi.

Limitaciones de la Blockchain

La Blockchain no es la solución para todos los problemas o desafíos que hoy tiene la sociedad. Es una tecnología relativamente nueva y su penetración y asimilación aún es lenta.

La falta de un conocimiento acabado por parte de las empresas y personas respecto a la tecnología, es una de sus

mayores trabas, impiden una mayor velocidad de implementación. Las aplicaciones sobre la *Blockchain* aún se encuentran en etapa de desarrollo más que en etapa de aplicación masiva.

Cuando una tecnología logra llegar a la fase de no ser entendida para ser usada, es cuando logra impactar a las masas. Por otro lado, el capital humano necesario para su desarrollo es aún escaso y requiere de una especialización alta.

La escalabilidad actual de la redes *Blockchain* es un problema, la demora y la baja cantidad de transacciones por segundo es uno de los mayores desafíos que la *Blockchain* debe superar, si

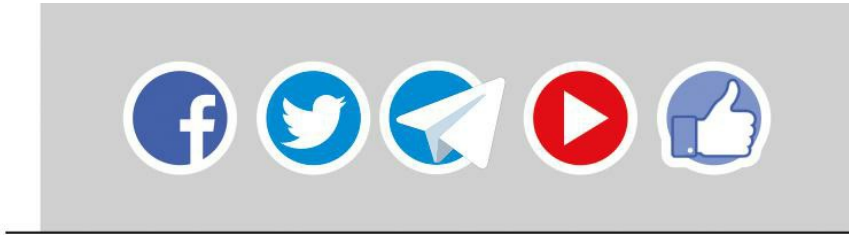
quiere lograr una real implementación global. La desventaja que existe respecto al número de transacciones en comparación a medios de pagos centralizados, ya se encuentra siendo abordada por iniciativas como *SegWit* y *Lightning Network*.

Para algunos procesos que requieren etapas de revisión y subsanación de errores u omisiones, la *Blockchain* no es la mejor base de datos para su implementación, dada la inmutabilidad de su contenido.

El *criptomundo* ha estado sometido a muchas estafas y engaños en el último tiempo, en especial en *Exchanges* e

ICOs. Buena parte ha sido producto de la falta de normativa legal que aplique al intercambio de activos digitales y la emisión de *Tokens*. Es de esperar que la regulación venga a reducir los miedos y desconfianzas en el despegue de la tecnología.

El alto gasto energético que requiere la confirmación de transacciones por parte de los mineros, para ciertas redes *Blockchain,* es una desventaja a la hora de medir la sustentabilidad de su implementación.



Influencers y fuentes de información

¿Dónde consultar información práctica en español y a su vez estar actualizados sobre la temática *Blockchain* y *Criptomonedas*?

Twitter

Cristobal Pereira @cristpereirag
Alberto G. Toribio @gotoalberto
Víctor Escudero @VEscudero
Santiago Márquez Solís
@smarquezsolis
Jorge Ordovás @joobid
Covadonga Fernández @CuadraLab
Cripto Noticias @CriptoNoticias
Cointelegraph @EsCointelegraph
CryptoChile @CryptoChile
Descentralizados @DCT2cl
Kawin @Kawin_io
Bitcoin Chile @BTChile

Telegram

Bitcoin Español @btces
Ethereum Español 2.0

@EthereumEspanol

Blockchain Español

@BitcoinBlockchainico

ICO Investors Spanish

@ICOSpanish

Trading Chile @tradingcl

Criptodivisas @criptodivisas

YouTube

Academia Blockchain

Nicolás Palacios

Leonardo Vera

David Battaglia

Web Sites

https://Bitcoin.org/es/

https://territorioBlockchain.es

https://www.blockchainmedia.es

https://agorachain.org

Terminología en el ecosistema

En el presente apartado se dará a conocer una descripción de los conceptos técnicos de base para el ecosistema del *criptomundo*, todo en un lenguaje sencillo para mejor comprensión del lector. Se ha tomado como referencia los recursos educativos de *bitcoin*.org/es, *criptonoticias.com* y *territorioblockchain.es*

Airdrop: Método de distribución de criptoactivos de manera gratuita a usuarios que cumplan determinados requisitos, por ejemplo mantener ciertos criptoactivos en su monedero.

Algoritmo: Conjunto de pasos y métodos lógicos que en una red informática sus participantes deben seguir para ejecutar un comando o resolver un problema. En el ámbito *blockchain*, se refiere a los métodos empleados por la minería para verificar transacciones. Algunos de ellos son SHA-256, *CryptoNight* y

Scrypy.

Altcoin: Término empleado para referirse a las criptomonedas o fichas de *blockchain* alternativas a *Bitcoin*; como Litecoin, *Ethereum*, *Dash, Monero, Zcash, Feathercoin* y *PPcoin*, entre otros.

Anoncoin: Término referido a criptomonedas cuyas transacciones son privadas y no pueden rastrearse, como *Zcash* y *Monero*.

ASIC: El Circuito Integrado de Aplicación Específica (ASIC) es un chip diseñado para cumplir

una tarea determinada. En el mundo de *Bitcoin* y las criptomonedas, es utilizado para resolver problemas de *hashing* y así generar nuevas criptomonedas, lo que se conoce como *"minería de criptomonedas"*.

Bifurcación: Versión de la cadena de bloques alternativa a la actual. Puede originarse de forma maliciosa si un minero obtiene demasiado poder de cómputo, de forma accidental en caso de un error en el sistema, o de forma intencional si se introduce una modificación del

protocolo, sin embargo, para que una bifurcación tenga éxito es necesario que cuente con el apoyo de suficientes mineros como para obtener la cadena más larga dentro de la cadena de bloques.

Bitcoin: con B mayúscula, se utiliza para describir el concepto de *Bitcoin*, o la totalidad de la red. Por ejemplo: "Hoy estuve aprendiendo sobre el protocolo *Bitcoin*". En cambio, *bitcoin* - sin mayúscula, se utiliza para describir una unidad del mismo. Por ejemplo: "Hoy he enviado diez *bitcoins*"; a menudo se

abrevia como BTC o XBT.

BitPay: Procesador de pagos con *bitcoins*. Permite a los comerciantes aceptar *bitcoins* como forma de pago, obteniendo, al final de la transacción, la criptomoneda o dinero fiduciario según su preferencia. También ofrece servicios de cartera de *bitcoins*.

Cadena de bloques o *Blockchain*: Es un registro público de las transacciones *Bitcoin* en orden cronológico. La cadena de bloques se comparte entre todos los usuarios de *Bitcoin*. Se

utiliza para verificar la estabilidad de las transacciones *Bitcoin* y para prevenir el doble gasto. Se trata de una base de datos descentralizada en distintos bloques en la que la información se encuentra distribuida en múltiples ordenadores (nodos). En cada bloque existen varios participantes que se encargan de certificar y verificar esa información sin que haya una confianza previa entre ellos, siendo necesario el consenso de la mayoría para validar esos datos.

Cartera fría: Dispositivo de hardware diseñado para almacenar criptoactivos de forma segura y aislada de internet.

Clave Pública: Texto alfanumérico del que se obtiene una dirección conocida por todos los usuarios. Al ser conocida, cualquiera puede enviar *bitcoins* a la dirección asociada, pero solo quien tenga la clave privada podrá acceder a ellos y moverlos.

Clave Privada: Texto alfanumérico asociado matemáticamente a una

dirección y que debe ser conocido solo por su dueño, permitiéndole así realizar transacciones *bitcoin*.

Consenso: Acuerdo alcanzado por la mayoría de nodos participantes de una red en cuanto al estado de esta y su protocolo.

Contrato Inteligente: Dirección de *blockchain* programada para ejecutar una tarea de acuerdo a las instrucciones previamente introducidas.

Confirmación: Verificación por parte de los nodos de la red de

que un bloque contiene únicamente transacciones válidas realizadas con criptomonedas que nunca antes habían sido usadas. El tiempo de confirmación en la red *Bitcoin* varía de 10 a 60 minutos, generalmente.

Criptoactivo: Ficha criptográfica que es emitida y comercializada en una plataforma *blockchain*. El término se acuña y populariza ante la expansión de las rondas de financiamiento y venta inicial de monedas (ICO) y el establecimiento de las nuevas dinámicas financieras en las

casas de cambio.

Criptografía: Conjunto de técnicas y métodos matemáticos que protegen la información de los datos registrados en la *blockchain*, dotándolos de seguridad y garantizando su inmutabilidad. El comercio en línea y los bancos ya utilizan criptografía. En el caso de *Bitcoin*, la criptografía se utiliza para hacer imposible que alguien pueda gastar los fondos del monedero de otro usuario o que se pueda corromper la cadena de bloques. También se utiliza para encriptar un monedero, de

manera que no se pueda utilizar sin una contraseña.

Criptomoneda: Moneda basada exclusivamente en la criptografía. A diferencia de las monedas emitidas por gobiernos y bancos centrales, se genera con la resolución de problemas matemáticos basados en criptografía. Su valor, no obstante, está sujeto a variación de precios dependiendo de la oferta y demanda en los mercados.

Dificultad: Número que determina la complejidad del acertijo hash

a resolver en cada bloque. Varía en función de la potencia de cálculo de los mineros en la red y se ajusta automáticamente cada cierta cantidad de bloques minados. En el caso de *Bitcoin*, se ajusta cada 2.016 bloques.

Dirección: Una dirección *Bitcoin* es parecida a una dirección física o correo electrónico. Es la única información que tiene que dar a alguien para recibir un pago en *bitcoin*. Sin embargo, hay una diferencia importante, y es que cada dirección solo debería usarse para una transacción.

Doble gasto: Acto de realizar dos pagos con una misma criptomoneda. Supone una operación fraudulenta, y aunque no resulta fácil de hacer en la red *Bitcoin*, se evita esperando al menos una confirmación de la red antes de dar por finalizada la transacción. La minería de *Bitcoin* y la cadena de bloques permiten crear un consenso en la red acerca de cuál de las dos transacciones es considerada válida.

Ethereum: Plataforma descentralizada desprendida desde la red de *Bitcoin* y que

permite la ejecución de contratos inteligentes. Su criptomoneda (*ether*) es una de las más populares y de mayor capitalización del mercado.

Firma: Una firma criptográfica es un mecanismo matemático que permite a alguien demostrar su propiedad. En el caso de *Bitcoin*, un monedero *Bitcoin* y su clave privada está vinculada por algún tipo de magia matemática. Cuando su programa de *Bitcoin* firma una transacción con la clave privada correspondiente, toda la red puede ver que la firma coincide

con los *bitcoins* gastados. Sin embargo, no hay forma de que el mundo descubra la clave privada para robar sus *bitcoins*.

FUD (Fear Uncertainly Doubt): Acrónimo angloparlante para Miedo, Incertidumbre y Duda, tres reacciones que algunas entidades buscan generar en los inversionistas para influenciar los mercados de criptoactivos.

Gigahashes / sec: El número de intentos de hash posible en un segundo dado, medido en miles de millones de hashes (miles de *Megahashes*).

GPU: Unidad de procesamiento gráfico. Chip de silicio diseñado específicamente para realizar cálculos matemáticos complejos necesarios para interpretar los gráficos visuales de juegos de ordenador. Son muy adecuadas para hacer cálculos criptográficos necesarios en la minería criptomoneda.

Halving: Término referente al evento en que se reduce por la mitad la recompensa recibida por los mineros al completar un bloque en una cadena distribuida, que funcione con Prueba-de-Trabajo (conocido en

inglés como *Proof-of-Work*). En *Bitcoin* sucede cada 210.000 bloques minados.

Hash: Función algorítmica que emite una dirección alfanumérica que resume y protege la información insertada a través de una entrada. Sirven también para garantizar la inmutabilidad de una unidad de información, ocultar una contraseña o servir como firma digital.

Hash de Firma: En *Bitcoin*, un hash que indica cuáles partes de la transacción son firmadas y por tanto, inmodificables. Por

defecto, se etiqueta una transacción con la señal SIGHASH ALL.

Llave Privada: Una clave privada es una pieza secreta de datos que acredita su derecho a gastar *bitcoin* de un monedero *Bitcoin* por medio de una firma criptográfica. Sus claves privadas se almacenan en su ordenador si utiliza un monedero de escritorio; mientras que si utiliza un monedero web serán almacenadas en servidores remotos del proveedor. Las claves privadas nunca deben ser compartidas ya que le permiten

gastar *bitcoins* desde su monedero correspondiente.

Minería: La minería en *Bitcoin* es el proceso de realizar cálculos matemáticos mediante computadoras para confirmar las transacciones en la red *Bitcoin* e incrementar la seguridad. Como recompensa por sus servicios, los mineros *Bitcoin* pueden cobrar los costos de transacción de las transacciones que confirman junto con *bitcoins* nuevos que se crean en cada bloque. La minería es un mercado especializado y competitivo en el que los

beneficios se reparten de acuerdo a la cantidad de cálculos que se hacen. No todos los usuarios de *Bitcoin* realizan minería y no es una manera fácil de hacer dinero.

Monedero: Un monedero *bitcoin* es aproximadamente equivalente a un monedero físico en la red *Bitcoin*. El monedero contiene su clave privada que le permite gastar los *bitcoins* asignados a la clave en la cadena de bloques. Cada monedero *Bitcoin* puede mostrarle la cantidad de *bitcoins* que contiene y le permite pagar una cantidad a una persona

específica.

Prueba de Trabajo, o PoW (por sus siglas en inglés): Es el algoritmo de consenso original en una red de *Blockchain*. En la *Blockchain*, este algoritmo se usa para confirmar transacciones y producir nuevos bloques en la cadena. Con PoW, los mineros compiten entre ellos para completar transacciones en la red y obtener recompensas.

P2P - Punto a Punto: Punto a punto se refiere a los sistemas que trabajan como una organización colectiva,

permitiendo.

Tasa de Hash (Hash rate): es la unidad de potencia de procesamiento de la red Bitcoin, es decir, que se relaciona con el número de valores hash que se pueden realizar en un periodo de tiempo dado. También se conoce como velocidad hash.

Velocidad Hash: La tasa de hash o "hash rate" es la unidad de medida de la potencia de procesamiento de la red Bitcoin. La red Bitcoin debe hacer intensivas operaciones matemáticas por razones de

seguridad. Cuando la red alcanza un hash rate de 10 TH/s significa que puede hacer 10 billones de cálculos por segundo.

DESCIFRANDO BITCOIN

El primer caso de uso de la Blockchain

Gerardo Cifuentes

2018