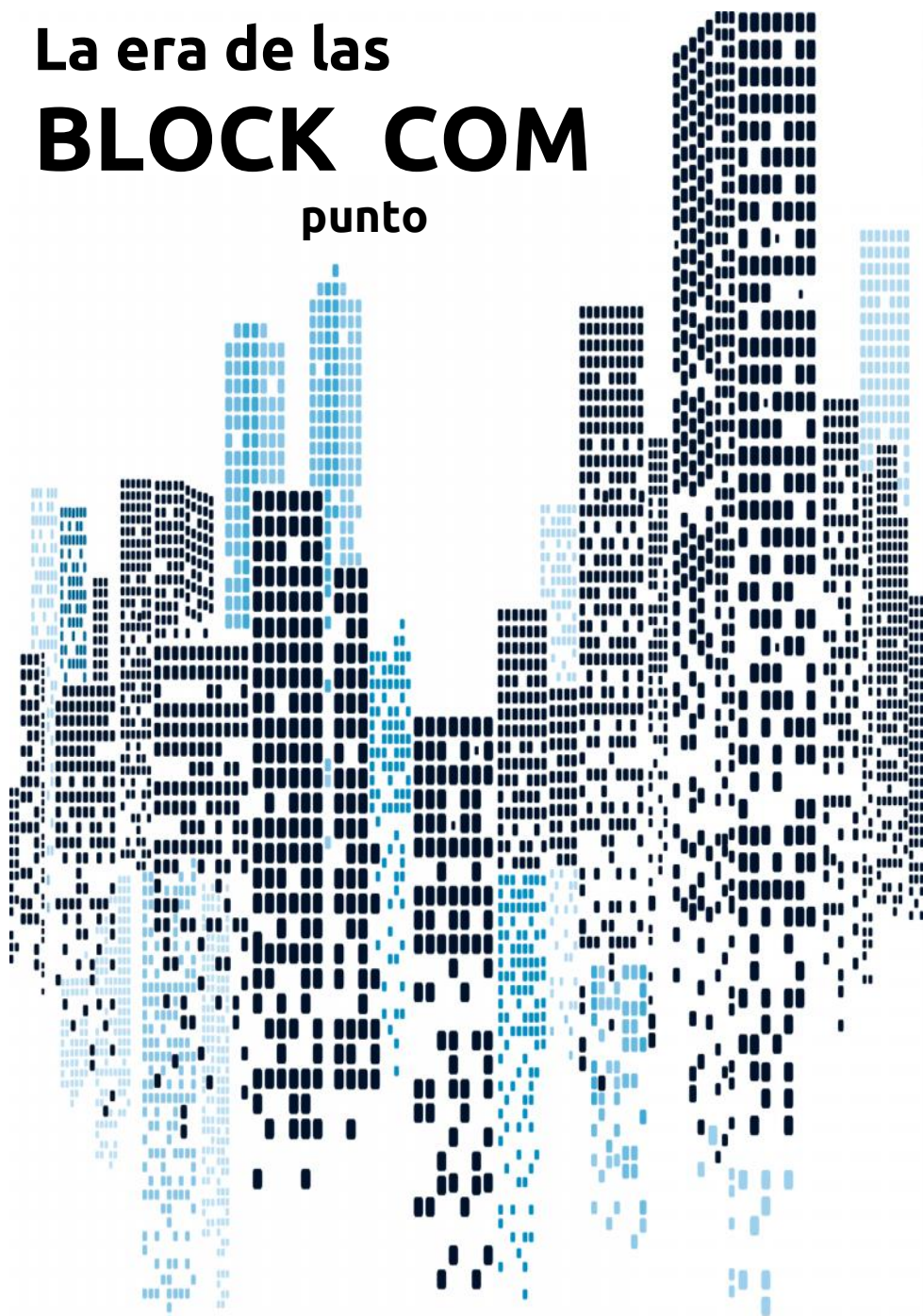


La era de las **BLOCK COM** punto



José Felip Darás

La era de las BLOCK punto COM

JOSÉ FELIP DARÁS

A lo largo del libro se han utilizado varios nombres que corresponden a marcas registradas por organizaciones o personas, por claridad en el texto se ha eliminado el símbolo ®, aunque el autor reconoce que son marcas registradas y usadas por sus propietarios, así como la intención de no infringirlas.

Para la elaboración del contenido de este libro, los autores han tomado especial cuidado para asegurar la veracidad y corrección de todo el material expuesto. El autor, no asumen ninguna responsabilidad sobre los daños o perjuicios que el uso o mal uso de la información y opiniones contenidas en este libro pueda ocasionar.

Este libro está publicado bajo licencia Creative Commons



Reconocimiento – No Comercial – Compartir Igual

En cualquier explotación de la obra autorizada por la licencia hará falta reconocer la autoría. La explotación de la obra queda limitada a usos no comerciales. La explotación autorizada incluye la creación de obras derivadas siempre que mantengan la misma licencia al ser divulgadas.

No está permitida la reproducción total o parcial de este libro, ni su tratamiento informático, ni la transmisión de ninguna forma o por cualquier medio, sin el permiso previo y por escrito del autor.

La era de las BLOCK punto COM

Primera edición v1.0: Junio 2017

Revisión de la Primera edición v1.0.1: Julio 2017

<http://www.laeradelasblock.com>

ISBN-13: 978-84-697-4062-0

CC 2017 – España

Lo difícil no es aprender, lo difícil es saber enseñar.

A mi padre, allí donde esté, quien supo enseñar.

Sumario

Sobre el autor, uno de muchos	7
Prologo (Jaime Sánchez)	10
Introducción (Jose Felip)	13
Capítulo 1: “Hype Cycle”: ciclo de sobre expectación	15
Capítulo 2: Blockchain, la evolución	18
Capítulo 3: Tokens y monedas, la revolución	25
3.1. Bitcoin, bitcoin y blockchain	26
3.2. Tokens, fichas y monedas	29
3.3. El valor	30
3.4. Smart Contracts y Ethereum	36
Capítulo 4: Qué puede hacer una blockchain	39
4.1. Pensar en frío: Usuario, empresa y emprendedor	40
4.2. Bancos y entidades financieras	42
4.3. Propiedad intelectual y catastral	47
4.4. Trazabilidad y verificación de productos originales	49
4.5. Transparencia: Entidades públicas	50
4.6. Transparencia: Entidades privadas	51
4.7. Loterías, rifas y otros sorteos transparentes	52
4.8. Gestión real de Identidad y reputación	55
4.9. Votaciones	59
4.10. Inteligencia Artificial e “Industria 4.0”	60

4.11. Aseguradoras	64
4.12. Seguridad	65
4.13. La imaginación	66
Capítulo 5: Mi blockchain	69
Capítulo 6: Estafas e inversiones	73
6.1. Monedas y tokens	75
6.2. El riesgo: ICOs	76
6.3. Pumps and Dumps	78
Capítulo 7: Legalidad	79
Capítulo 8: “Blockchain Hype Cycle”: Especulación	81
8.1. El “valor” de bitcoin	82
8.2. El “valor” de otras criptomonedas	85
Capítulo 9: Donaciones en la cadena de bloques	86
Capítulo 10: Las opiniones: Oscar Domínguez, Territoriobitcoin.com	101
10.1. Daniela Caro, Cointelegraph España	105
10.2. Jordi Carrera, “minero digital”	106
10.3. Santiago Márquez Solís, Z-Games	107
10.4. Alex Preukchat, autor de #libroblockchain	109
10.5. y muchas más	113
Capítulo 11: Continuará	115

Sobre el autor, uno de muchos

Hola,

Soy un humilde informático, desde hace más de 30 años, mi vida ha girado siempre alrededor de un ordenador desde que mi padre introdujo en casa un ZX Spectrum, y desde entonces, no tengo suficiente tiempo para intentar aprender todo lo que puedo y transmitirlo a quien lo necesita.

Soy una persona altamente inquieta, y en una época en que la crisis azotaba fuertemente a todo el mundo y, en concreto, a los seres que más quería, empecé a preparar un proyecto al que llamé sin pensarlo “moneda universal” (allá por 2011, no en 2008, no me confunda el lector con Satoshi Nakamoto). Investigando y leyendo mucho, me crucé en mi camino con el bitcoin, y a su vez, con la tecnología asociada blockchain (cadena de bloques).

Hablaré de especulación, de economía, de los exchanges (casas de cambio de valor), de movimientos sociales, evolución y revolución económica, pero sobre todo, de la tecnología blockchain en sus diversas funcionalidades posibles conocidas y futuras, orientada a empresas, emprendedores y a las personas. No hablaré de bitcoin en profundidad, ni de otras criptomonedas, puede encontrar amplia información sobre esos temas en la red y en las librerías.

No me gustan los exchanges, aunque parecen ser necesarios, es algo que aprendí mientras preparaba mi “moneda universal”: *no podemos dar valor del mismo modo erróneo que el actual dinero* (lo veremos más adelante).

El momento de escribir este libro fue perfecto, 2017, las ganas inmensas, pero sobre todo, el concepto de ser un libro “descentralizado”, fue lo que más fuerzas me dio para llevarlo a cabo, hablar con la gente, pedir su opinión, sus experiencias positivas y negativas, sus visiones a presente y a futuro, ver cómo ha evolucionado el mundo de las criptomonedas y de la tecnología blockchain y sus aplicativos, apoyado y rodeado de cientos de mensajes y contactos, lejanos y próximos, que mostraban su afecto y su apoyo por un mismo ideal, un mismo fin y una misma idea: la descentralización en muchos de sus ámbitos y el ansia por compartir y divulgar los conocimientos adquiridos.

“ I’m happiest when I’m working on One Big Thing. I think I’ve found my next Big Thing, and I’m excited!”



“Soy más feliz cuando estoy trabajando en Una Gran Cosa. ¡Creo que he encontrado mi próxima gran cosa, y estoy emocionado!”

Gavin Andresen, desarrollador de Bitcoin Core

*El único modo de hacer un gran trabajo, es amar lo que haces.
¡No olvides perseguir siempre tus sueños!*



Group BTC

Por ello, tengo que agradecer a muchos, no sólo a los que han colaborado de manera desinteresada en este libro, sino también a otros que ya de una manera u otra han compartido su conocimiento, mediante libros, artículos, blogs o simplemente con un mensaje, empezando por Ramón Quesada, al cual creo, le formulé la

pregunta más difícil de todo el libro y que entenderán su respuesta a través de los siguientes capítulos:



¿Qué cadena de bloques necesita tu hija, Ramón?

Me parece muy buena pregunta, teniendo en cuenta que todos mis esfuerzos van orientados a dejarle lo mejor de mí, a mi hija, para cuando yo ya no esté, en ese sentido espero dejarle algo tan intangible como necesario, además de intentar darle cariño, amor y la mejor educación posible, tarea que comparto con mi mujer y que ella hace mucho mejor que yo, también me preocupo de dejarle algo de lo que pueda estar orgullosa y es por eso que la mejor cadena de bloques que ella necesita es:

HUMANA, LIBRE, COLABORATIVA, DESCENTRALIZADA, PARTICIPATIVA, ABIERTA A TODOS, ROBUSTA, VIRAL, AMIGABLE, OPEN SOURCE, VOLUNTARIA, TRANSPARENTE, JUSTA y RESPONSABLE.

Si logro unificar todos esos ingredientes en una cadena de bloques, creo que será mi mejor legado y en ello estoy trabajando activamente, espero este verano ver un primer Esbozo.

Dado que todos estos conceptos son difíciles de articular en una cadena de bloques, por la propia naturaleza de la tecnología, y la manera en que ésta se transforma, a medida que las personas interactúan con ella, creo que la mejor manera de combinarlos es a través de un token y una plataforma, que permita una forma nueva de generación de beneficios con un MODO DE PRODUCCION DESCENTRALIZADO (P2P) e inclusivo, donde el ser humano pueda ser capaz de hacer uso de sus facultades de producción sin tener intermediarios y utilizando una tecnología que se lo permita de forma: LIBRE, RÁPIDA y GLOBAL

Muchas gracias Jose Felip

Ramón Quesada, padre, Avalbit.org y Bitcoin Valencia.

“La base de avalBit son la gente, la filosofía y los principios”

avalBit.org



PRÓLOGO

Bienvenido al futuro, aunque todavía no lo sepas. Estás en el lugar y en el momento adecuado para asistir a la mayor revolución de lo digital, de las interacciones entre dispositivos, de cómo el mundo procesa los datos, gestiona personas, toma decisiones, la banca, las administraciones, el dinero, el sector empresarial, los gobiernos, en definitiva, TODO. Todo cambia todo pasa como diría Bob Dylan, pero lo que no sabía Bob es que lo único que no cambia es aquello que pongas en la Blockchain. Sí, eso de lo que todo el mundo habla, pero te es difícil de entender, aquí te lo vamos a poner fácil, no te asustes, sigue leyendo.

Nos interesa que lo entiendas, pero que pongas patas arriba todas tus creencias, lo que te han enseñado, lo que te han contado que así debe ser siempre. Esto va de hacerte pensar, de sembrar la semilla de lo que vendrá, de que vuele tu imaginación y veas y comprendas que la Blockchain será un estándar algo que usaremos cada día por inercia, como lo es la electricidad, el agua que sale de tu grifo o la cobertura de tu móvil. ¡Pero eh! no todo es de color de rosas, cada cosa a su debido tiempo más adelante lo iremos viendo.

Detrás de este libro hay personas, porque éste es un libro con trozos de personas, muchas, con vivencias, con aventuras, con anécdotas, personas que han vivido el nacimiento de algo en lo que han creído después de entenderlo y por eso su estilo de vida se ha convertido en una especie de religión, de ganas, de fuerza, de cambiar a un mundo más igualitario, equitativo, porque con la blockchain es posible. Éste no es un libro cualquiera, es una guía, es un big bang

de ideas, es un comienzo, es un escrito en constante desarrollo, que evoluciona que se adapta y que nos cuenta la parte humana de la Blockchain.

Cada 35 años se produce una fuerte innovación que hace cambiar el sistema económico global, (o eso dicen) que hace replantearse las estructuras sociales y nos trae a su vez un salto de evolución, pues bien, desde el nacimiento de internet no había habido otra innovación de similar envergadura hasta que en 2008 surgió algo llamado Bitcoin, el cual nos traía de la mano (escondida silenciosamente) la tecnología Blockchain. Ya te va sonando algo ¿verdad?. Y como toda tecnología lleva su tiempo de maduración parece que el árbol ya ha crecido algo en estos años y ahora vemos los primeros brotes.

Éste es un libro para todos los públicos, ¡arriba esa curiosidad! tampoco hace falta que vengas con un doctorado tras la manga para entender todo lo que te vamos a contar, esto va de ser ameno una lectura curiosa y sobre todo que te quedes con la idea de que todo esto está pasando y seguirá pasando. Vamos a hablar del impacto económico, de burbujas ¿dónde? de cómo se fundamenta técnicamente esta tecnología, pero siempre con un punto ágil. Y lo mejor, que algún día editaremos estas mismas líneas para seguir contándote el futuro del futuro.

Mientras aprendes a entender qué es Blockchain, la dichosa palabra, te vas a ir encontrando con paradigmas económicos, términos digitales, la banca, las empresas, los gobiernos...un largo etcétera

A todos nos suena la famosa “economía colaborativa”, lo colaborativo está de moda, pero no todo lo colaborativo lo es propiamente dicho, algo puede ser colaborativo, pero estar centralizado en su toma de decisiones y al fin y al cabo monopolizado. Sea un negocio, nuestros datos en internet o mismamente el sistema económico global (casi nada).

Para entender Blockchain hay que separar, “colaborativo” de “centralizado” y crear una nueva concepción de cómo funcionan las cosas. Romper con la centralización y democratizar el reparto de la importancia de cualquier cosa y de la información en el tiempo.

Pensando en Blockchain pensaríamos como los 3 mosqueteros, todos para uno y uno para todos.

Adelante, empezamos...

Jaime Sánchez
CEO bitcoinadvisor.es y COO [Octopocket](#)



Introducción

Ya hace 20 años, en 1997, cuando Internet estaba en pleno crecimiento en el auge del comercio electrónico, las empresas vieron un filón potencial de crecimiento y especulación al añadir a su producción habitual servicios en red, apareciendo filiales, nuevas empresas y sub-departamentos que enfocan sus servicios y productos en Internet.

En 2001, la gran mayoría de estas empresas o inversiones realizadas se perdieron, por mera especulación (salidas a Bolsa con alto crecimiento de valor inicial), o simplemente por ser proyectos inviables (alimentadas por el exceso de financiación que existió en esa época).

A estas empresas, se les denominó “punto com”, ya que lo único que hacían era añadir a su nombre comercial la extensión “.com” para poder aparecer y ser localizadas en red y ofrecer sus supuestos productos y servicios de valor ultra mejorado.

Al desastre provocado por su crecimiento desmesurado e irreal, con trágico final se le denominó “burbuja punto com”, donde desaparecieron la gran mayoría y las que sobrevivieron, eliminaron la coletilla “punto com” para volver a ser lo que realmente eran.

Entonces, esa época, ¿Qué fue? ¿Una evolución de los mercados empresariales o una revolución empresarial?

[...no conteste todavía...]

Internet acercó a las empresas los clientes, la forma de llegar hasta ellos, de consultar sus artículos, sus servicios, pero no supieron gestionarlo debidamente, hasta apenas hace unos pocos años, con las tecnologías de bigdata (recopilación de gran cantidad de datos para luego su análisis y sacar conclusiones muy precisas de perfiles de clientes, tipo consumo, tendencias, etc...).

Hubo una revolución visto del modo de marketing, pero las empresas no supieron evolucionar a la par. Fue una evolución en el modo que las personas adquirirían productos (no debían desplazarse a tiendas físicas).

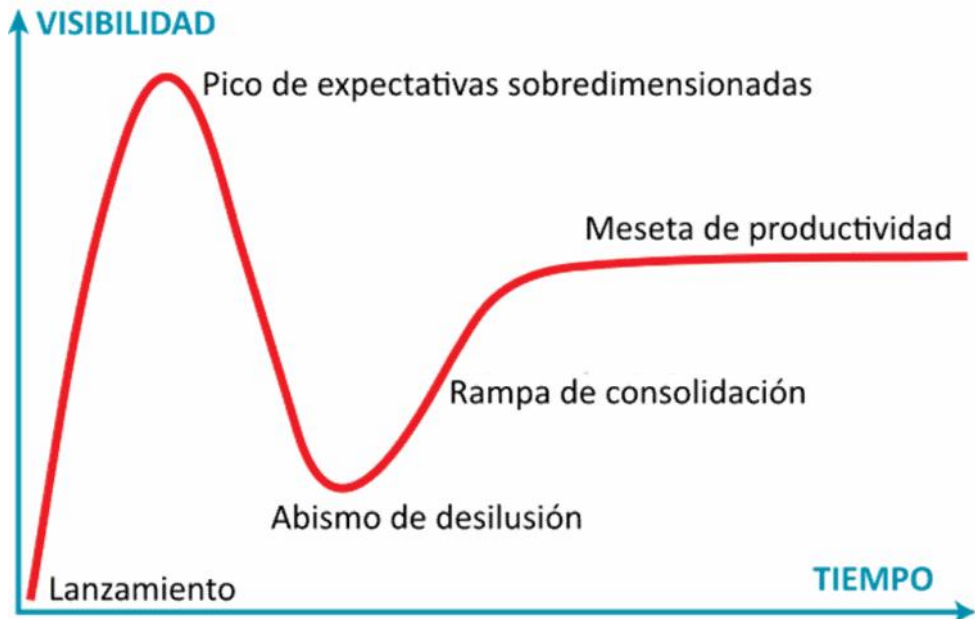
Fue muchas cosas, pero ninguna comparada con las que nos viene ahora, la era de las *block punto com*. La tecnología blockchain nos ofrece entre otras muchas cosas, soluciones y mejoras a problemas reales. Muchas empresas van a conseguir ahorrar costes, agilizar producciones, conocer mejor a los clientes y, sobre todo, de manera más rápida y transparente.

Pero antes de seguir y desvelar algunos de los grandes acontecimientos que nos deparan permítame lector, recordarle si no lo conoce, que es, como funciona y qué relación tiene un ciclo de sobre expectación (Hype Cycle) para entender de mejor manera como serán las empresas dentro de poco tiempo.

Capítulo 1

***“Hype Cycle”*: ciclo de sobre expectativa**

Los ciclos Hype, o ciclos de sobreexpectación, son *una representación gráfica de la madurez, adopción y aplicación comercial de una tecnología específica*¹.



1. Definición de Wikipedia.org: Ciclo de sobre expectativa

El término fue acuñado por Gartner, una casa de análisis/investigación, basada en los EE.UU., que proporciona opiniones, consejos y datos sobre la industria de las tecnologías de la información mundial².

Desde 1995, Gartner ha utilizado el ciclo de sobre expectativa para caracterizar el entusiasmo sobredimensionado y la subsiguiente decepción que ocurre habitualmente en la introducción de nuevas tecnologías².

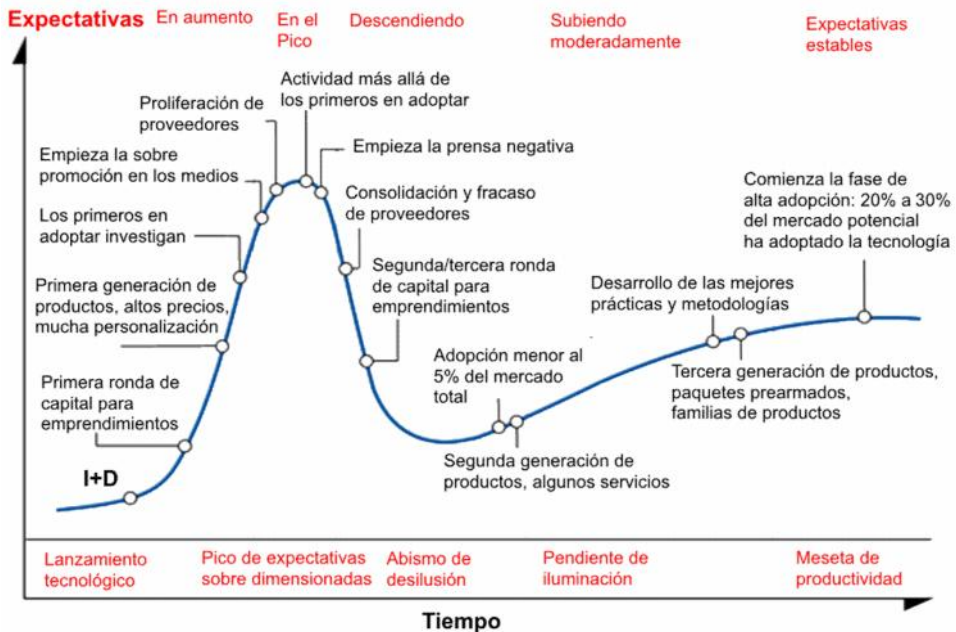
Este ciclo se compone de cinco fases:

1. "Lanzamiento" - La primera fase de un ciclo es el "lanzamiento", una presentación del producto o cualquier otro evento genera interés y presencia en los medios.
2. "Pico de expectativas sobredimensionadas" - En la siguiente fase, el impacto en los medios genera normalmente un entusiasmo y expectativas poco realistas. Es posible que algunas experiencias pioneras se lleven a cabo con éxito, pero habitualmente hay más fracasos.
3. "Abismo de desilusión" - Las tecnologías entran en el abismo de desilusión porque no se cumplen las expectativas. Estas tecnologías dejan de estar de moda y, en consecuencia, por lo general la prensa abandona el tema.
4. "Rampa de consolidación" - Aunque la prensa haya dejado de cubrir la tecnología, algunas empresas siguen, a través de la "pendiente de la iluminación", experimentando para entender los beneficios que puede proporcionar la aplicación práctica de la tecnología.
5. "Meseta de productividad" - Una tecnología llega a la "meseta de productividad", cuando sus beneficios están ampliamente demostrados y aceptados. La tecnología se vuelve cada vez más estable y evoluciona en segunda y tercera generación. La altura final de la meseta varía en función de si la tecnología es ampliamente aplicable o sólo beneficia a un nicho de mercado.

El término se utiliza ahora de forma generalizada en el marketing de las TIC.

2. Explicación de Wikipedia.org: Ciclo de sobre expectativa

El detalle de las fases aplicado a un producto o servicio se plasma gráficamente aquí:



Aplicando estos ciclos a la época de las “punto com”, vemos como claramente el impulso se perdió totalmente en el punto 3, *Abismo de desilusión*, ya que no se supo aprovechar internet o no se disponía de medios suficientes para que el cliente final adoptara esta innovación.

Ahora parece que sí es el momento, de una evolución en las empresas, de una revolución por parte de las personas de realizar lo mismo que hacen ahora, pero de manera estructurada, clara y libre, más rápida, más económica y más fiable: la tecnología Blockchain (la cadena de bloques) se encuentra “supuestamente” en su 1º ciclo.

Capítulo 2,

Blockchain: la evolución

La tecnología blockchain o cadena de bloques, se define en Wikipedia³ como *“una base de datos distribuida, formada por cadenas de bloques diseñadas para evitar su modificación una vez que un dato ha sido publicado usando un sellado de tiempo confiable y enlazando a un bloque anterior. Por esta razón es especialmente adecuada para almacenar de forma creciente datos ordenados en el tiempo y sin posibilidad de modificación ni revisión.”*

Desde el BBVA Research⁴ lo definen como *“una contabilidad pública entre pares que se mantiene mediante una red distribuida de ordenadores y que no requiere ninguna autoridad central ni terceras partes que actúen como intermediarios.”*

En las últimas décadas, hemos vivido la internet de la información. Cuando enviamos un correo electrónico, una foto no se envía el original, se envía una copia (datos).

3. Definición de Wikipedia.org: Cadena de Bloques

4. https://www.centrodeinnovacionbbva.com/sites/default/files/ebook-cibbv-tecnologia_blockchain-es.pdf

Ahora, internet dejará de transmitir datos para transmitir valor, transmitir cosas como dinero, activos financieros como acciones y bonos, contratos, propiedad intelectual, música, arte, un voto, de manera única y demostrable matemáticamente, concretamente con criptografía de alto nivel, resolviendo lo que los criptógrafos denominan el problema del "doble gasto", que hace que cuando yo le envié a usted por ejemplo 10€, no pueda volver a usar esos 10€ para realizar otro envío u compra.

Podemos encontrar muchos ejemplos y definiciones de la cadena de bloques, según en el contexto en el que se aplique, por ello, en vez de definir exactamente que es, primero veremos las cualidades y características que tiene.

1. Descentralización

A diferencia de las actuales bases de datos que almacenan sus registros en un solo lugar, la cadena de bloques se encuentra “en todos los sitios”, debido a que usa una red de tipo P2P para gestionar y almacenar de manera descentralizada y redundante un **registro distribuido y sincronizado** de datos.

En la actualidad hay unos 5000 nodos fijos que contienen todos ellos la misma información, sincronizados, lo que permite que, si uno o varios nodos falla, la red y la información continúe fluyendo, sin interrupciones. Cualquiera con un ordenador conectado a Internet puede ser un nodo instalando un software específico.

En la economía real, hoy nos basamos en grandes intermediarios como los bancos, el gobierno, grandes compañías, tarjetas de crédito, etc. para establecer la confianza en nuestra economía. Estos intermediarios realizan la función de autenticación e identificación de personas, y compensan y liquidan registros de valor, pero de manera centralizada, quedando expuesto a ataques, robos de información y, lo peor de todo, a excluir a cualquier persona que no cumpla determinados requisitos a entrar en este ciclo económico.

2. Velocidad

En un segundo un correo electrónico da la vuelta al mundo, pero en el caso de activos, como el dinero, tarda días o semanas.

Mediante las conexiones que ofrece la tecnología blockchain entre nodos, bajo protocolo de comunicaciones P2P, el dinero puede moverse en apenas unos minutos o demorar como mucho unas pocas horas, y siempre evitando el “doble gasto”.

3. Bajas comisiones

Si usted es o ha sido inmigrante, o simplemente ha enviado dinero fuera de su país, se puede haber encontrado con unas comisiones entre el 5% y el 20 % solo por la acción de enviar dinero a otro país.

Si lo hubiese transmitido por la blockchain de bitcoin, se le habría aplicado un 0,001% de comisión básica.

En otros tipos de cadenas de bloques puede variar entre gratis y el 1% el envío de cualquier “cosa” que desee enviar.

4. Pseudo-anónima

La información que se almacena en esta gran base de datos distribuida se realiza mediante transacciones, las cuales son pseudo-anónimas, es decir, conservan la privacidad hasta que el individuo decida relacionar los registros con una identidad.

En las entidades bancarias actuales, toman nuestros datos, los revisan, los transmiten incluso a gobiernos o terceros en algunos casos, evitando así que cualquier transacción se pueda considerar privada.

Las criptodivisas, (o *tokens*, como veremos más adelante), junto con su correspondiente cadena de bloques, permiten establecer confianza y hacer transacciones sin una tercera parte, y son el

elemento que transporta el valor de manera intrínseca y, además, carece de un control central como un gobierno, un estado o una nación que la emita o la controle.

5. Segura

La estructura de bloques de la que se compone, certifica que la información almacenada no puede ser alterada en el tiempo y, dependiendo del tipo de cadena de bloques, los niveles de seguridad criptográficos garantizan estos datos. Cada bloque se vincula con el bloque anterior, y ese con su bloque anterior, para crear una cadena de bloques. Y todos reciben una marca de tiempo, algo así como un sello digital. Si se quisiera piratear un bloque, se tendría que piratear ese bloque, y todos los bloques anteriores, toda la historia comercial de esa cadena de bloques, y no solo en un ordenador (nodo) sino en miles de computadoras, de forma simultánea. Es infinitamente más seguro que los sistemas informáticos que tenemos hoy en día.

6. Es libre, de código abierto (Open Source)

Cualquiera puede revisar su estructura y su código fuente, y por supuesto, colaborar de manera desinteresada para su mejora o revisión, y también puede consultar todos los registros almacenados (transacciones) de manera gratuita y pública. Intente hacer esto con su entidad bancaria actual, con su notario, el resultado de las últimas votaciones, etc...

"En Bitcoin no estamos interesados. En Blockchain, sí. Es el sueño de cualquier supervisor: poder ir a un sitio y mirar todas las nuevas operaciones de forma transparente y centralizada".



Carlos Kuchkovsky, responsable del Kickstart Team en BBVA

7. Transparente y auditable

La consulta de los registros generados por una cadena de bloques es transparente, desde el primero de los registros hasta el último, no se puede bloquear la lectura de unos registros en concretos, o todos o ninguno.

Es muy curioso que conceptos tan dispares como descentralización y unión se lleven tan bien, y esto solo es posible en la blockchain.



Es como si encontrásemos un recipiente donde el aceite y el agua se mezclarán a la perfección. Para mí, la cadena de bloques y bitcoin tratan de dar una oportunidad al mundo de ser justo, creando un sistema donde nadie es discriminado ni rechazado y donde cualquiera puede entrar a formar parte del sistema. No importa raza, sexo, política o religión, todo el mundo es bienvenido. Todas las decisiones se toman por consenso de la mayoría y esto es lo revolucionario que creo está cambiando las reglas del sistema actual.

Si tengo que destacar algo en lo personal, me quedo con la gente que está empujando en la comunidad para hacer de esto algo muy grande. Nos llaman locos, frikis... ¡que digan lo que quieran! Solo tratamos de hacer del mundo un sitio mejor y más justo.

Luís Vaello,
ex DJ y productor musical, vicepresidente de Avalbit, COO en Bitnovo

8. Escalable por consenso

El consenso de toda o de una parte muy elevada de los nodos que componen la red permite una “democracia real” frente a problemas, mejoras o cualquier característica que la afecte. Esta característica la hace tan **fuerte**, que hace que nadie pueda controlarla individualmente o que pueda apropiarse de ella; si un nodo o un grupo de nodos no actúa de manera correcta o no suman un consenso total establecido, son expulsados de la red y dejan de recibir transacciones para su almacenamiento y gestión.

9. Única

La estructura de bloques, uno tras de otro, unidos mediante una prueba matemática y criptográfica de trabajo, hacen que la cadena de bloques sea única, inmodificable, conformada y sellada con una marca de tiempo.

En el caso de que una cadena se dividiese en 2 partes debido a un consenso en el que una minoría no quisiera seguir sin el consenso de la mayoría, tendríamos otra cadena de bloques distinta y ambas seguirían existiendo, pero por caminos diferentes (a esto se le denomina “fork”).

Estas son las principales características que componen una blockchain, pero a su vez, una cadena de bloques puede ser:

A) Pública (permisiva)

Una blockchain pública es accesible por cualquier usuario en el mundo. Lo único que se necesita es un ordenador y una conexión a Internet. Sólo es necesario que se componga de un **protocolo**, la **unidad de cuenta o token** y la propia **blockchain** (la base de datos en la que se registran las transacciones).

Ejemplos de blockchains públicas son bitcoin, litecoin y ethereum.

B) Privada (no permisiva)

Una blockchain privada, no está abierta al público, sino que solo se puede acceder a ella por invitación. Pueden ser incluso muy diferentes las unas a las otras en cuestiones de características base y, en algunos casos, es incluso cuestionable que se puedan clasificar de Blockchains.

Algunas de las más famosas son Hyperledger (de la Fundación Linux), R3 (un consorcio de bancos internacionales para desarrollar

soluciones bancarias de blockchain privada) o Ripple (un protocolo para facilitar las transferencias internacionales de dinero).

C) Mixtas o híbridas (también llamadas “federadas”)

Las blockchain híbridas son una combinación de las públicas y privadas. En una blockchain híbrida los nodos participantes son invitados por lo que se mantiene un control de ellos, pero todas las transacciones son públicas.

Algunos ejemplos de blockchains híbridas son BigchainDB (un proveedor de tecnología blockchain) o Evernym, una blockchain híbrida que quiere facilitar la gestión de la Identidad Digital Soberana.



Unido al concepto “distributed ledger technologies” (tecnologías de registro distribuido), blockchain se presenta como un conjunto de tecnologías (P2P, sellado de tiempo, criptografía, etc.) que combinadas hacen posible que computadoras y otros dispositivos puedan gestionar su información compartiendo un registro distribuido, descentralizado y sincronizado entre todos ellos, en vez de utilizar las tradicionales bases de datos.

Pero no es solo eso, sino que la información se transmite y guarda de un modo extremadamente seguro, respetando la identidad y privacidad, gracias al uso de claves criptográficas. Además es un registro que no permite su alteración, es decir, no permite deshacer o reescribir lo ya registrado, que además es visible para cualquier participante de la red (si ésta es pública, como Bitcoin), añadiendo una gran transparencia.

Como analogía podemos asemejar el blockchain a un libro de cuentas, donde en cada página se registran las operaciones para un cálculo que parte del resultado obtenido en la página anterior.

Fundación CTIC, fundacionctic.org

Capítulo 3, Tokens y monedas: la revolución

La revolución no será televisada, será “tokenizada”



fluonecosystem.org White Paper

En una blockchain se almacenan transacciones, registros de actividad, con una huella de tiempo (sellado). Lo que contienen estas transacciones son movimientos de una “ficha” o “token” que es única y que sirve como referencia y justificación del contenido de la transacción. Por ello, toda blockchain necesita de una “ficha” o “token” para poder gestionar las transacciones y registrarlas, transacciones que contienen la información relevante.

Una blockchain sin un “token” es una base de datos descentralizada, no una blockchain. Es como el yin y el yang, no puede existir por separado.

El “token” o “ficha”, se les llama también “moneda”, por ser la que transmite el valor en la blockchain que se utiliza. La moneda más conocida es el bitcoin (en minúsculas para referirse a la moneda, en mayúsculas para referirse a red y a la cadena de bloques), por haber sido el primero en crearse. Entonces, **¿Qué fue antes, el huevo o la gallina?, ¿La blockchain o el token?** En este caso, fueron ambas a la vez. Repasemos por encima la historia del bitcoin:

3.1. Bitcoin, bitcoin y blockchain

La finalidad única de la creación y aparición del bitcoin fue el poder transmitir valor a través de internet de manera segura, libre (sin intermediación de terceros) y rápida.

Para ello, su autor, Satoshi Nakamoto, necesitó cubrir una serie de problemas básicos, como el doble gasto, la descentralización y la rapidez de las comunicaciones seguras, apoyándose para ello, de la creación de una tecnología basada en P2P (red entre iguales) y en la criptografía, a la que en base a su estructura de bloques denominó blockchain (cadena de bloques).

Cada 10 minutos aproximadamente, la red Bitcoin, recopila todas las transacciones confirmadas, junta todas las que puede en un bloque (actualmente los bloques tienen un tamaño limitado) y mediante un algoritmo, las verifica para acuñar de manera firme en el tiempo un bloque.

Esto genera un proceso llamado minado, que produce una recompensa, pero no entraremos en tema ahora, porque lo que nos interesa es la robustez de la unión de cada bloque, uno detrás de otro con dependencia del anterior, quedando, por tanto, la información contenida en cada bloque inmodificable.

Ya digo que no entraremos en más detalles de Bitcoin, porque la esencia que se generó, la cadena de bloques, es lo realmente disruptivo y revolucionario. Veamos algunas opiniones:

"Bitcoin es, en esencia, un libro de contabilidad distribuido, en busca de un protocolo informático que proteja el valor que ahí reside."



Jose Jorge Guardiola Piqueras, miembro de Avalbit.org

Cuando descubrí bitcoin me quedé enamorado del ideal y del objetivo que persigue, deshacernos de los bancos y de intermediarios con comisiones abusivas que manejan a su antojo los ahorros, el dinero y la deuda de la gente corriente... pero esto no era nada más que la punta del iceberg. ¡Realmente el gran potencial es la tecnología en la que se basa bitcoin, la blockchain!



La blockchain es una tecnología necesaria para hacer un ejercicio de transparencia en una era donde grandes corporaciones y gobiernos manipulan los datos para su propio interés.

El día que los gobiernos descubran el gran potencial de la blockchain y nos obliguen a utilizar esta tecnología habremos dado un gran paso para la sociedad, aunque el comienzo de una nueva era, será cuando nosotros obliguemos a los gobiernos y corporaciones a utilizar dicha tecnología para el bien del pueblo.

Gonzalo Borrás . Consultor Odoo ERP en bisnesmart,
Miembro y tesorero de Avalbit

Bitcoin es una tecnología, una aplicación monetaria y una forma única y diferente de concebir el mundo. Todo aquel que quiera sustraer o limitar cualquiera de estas partes estará olvidando la esencia de lo que es realmente importante.



Toni del Moral, CEO de tokens.com



Acercar la cadena de bloques a la sociedad.

El bitcoin es mucho más que una moneda digital; la cadena de bloques en la que se basa el bitcoin, es la revolución de la confianza.

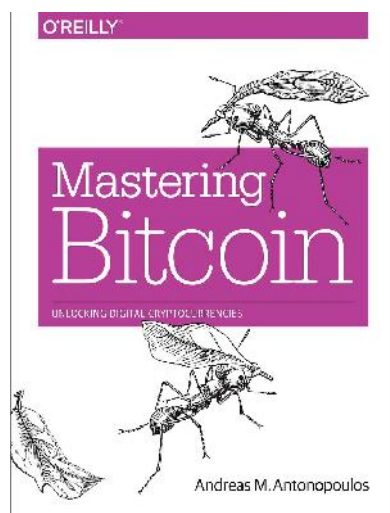
La cadena de bloques trae el cambio de paradigma de un mundo centralizado a otro descentralizado y colaborativo. Los que estamos viviendo y participando en este mundo apasionante, vemos como se ha pasado de los datos (saldos de direcciones bitcoin) al código (smart contracts) descentralizado

Es decir, la revolución de bitcoin trae nuevas revoluciones 2.0 que van a cambiar la manera en la interactuamos y nos relacionamos en nuestra sociedad.

Sin embargo la mayor parte de la gente desconoce su potencial; por ello, el principal objetivo de la gente que trabajamos con la cadena de bloques es hacer esta tecnología se aplique en el día a día en forma de aplicaciones útiles para la sociedad y fáciles de usar.

Así la blockchain tendrá el mismo rol para la descentralización y la confianza que el TCP/IP ha tenido para internet.

Manuel Sales, CEO de Octopocket,
CTO & Founder en New Finance LTD



Si el lector quiere profundizar más sobre Bitcoin o bitcoin, le recomiendo el libro "Mastering Bitcoin: Unlocking Digital Cryptocurrencies" de Andreas Antonopoulos.

3.2. Tokens, fichas y monedas

Ya hemos visto que una blockchain sin un “token” no puede existir, ya que es como en medio de transporte que lleva la información que se desea gestionar, verificar y almacenar.

Dependiendo del ámbito, tipología y naturaleza de la cadena de bloques que se use, un token puede ser una moneda (o criptomoneda), o puede ser una “ficha” de cambio por dicha moneda (lo veremos más a fondo con en el capítulo que se habla sobre Ethereum).

En el mundo real en el que usted todavía se encuentra (más adelante le ofreceré elegir entre la “*pastilla roja y azul*”), la diferencia fundamental entre un token y una moneda es que una moneda es emitida por una autoridad local o nacional, mientras que un token tiene un uso mucho más limitado y es a menudo emitido por una empresa privada, institución, grupo, asociación o persona, por lo que no son dinero de curso legal (lo que resumiría entonces, que las criptomonedas no son legales...lo discutiremos en el capítulo de Legalidad).

En el mundo de las criptomonedas no hay una entidad central que controle o emita las monedas y, por tanto, que las respalde.... son los “mineros” quienes las emiten en las cantidades y tiempo establecidos por la cadena de bloques a la que son gestionables, y pueden estar limitadas o no su emisión.

Pero para no liarle tanto, por ahora nos quedamos con el concepto de 1 token= 1 moneda, que contiene valor transmisible, el cual no existe o carece de ese valor si no está asociado a una cadena de bloques activa.

3.3. El valor

El valor de cualquier cosa va en relación al trabajo que conlleva crear esa determina cosa, por ejemplo, una obra de arte cuesta 1 mes en pintar, por lo que su valor podría ser el equivalente en monedas a un mes de trabajo. Pero el mundo en el que sigue creyendo no parece funcionar así, ya que, el gran pintor Pablo Picasso tiene muchos cuadros que le costaron un mes de trabajo, pero si usted quiere adquirir una obra de este autor no creo que la consiga por el equivalente a un mes de trabajo, le van a pedir seguramente cantidades de como mínimo 5 dígitos, ¿verdad?

Visto este ejemplo, ¿Quién le otorga valor a las criptomonedas, a los tokens, a las fichas? Centrándonos en la cadena bitcoin y, sabiendo que no hay una entidad central que emite los bitcoins, ¿cómo es posible que hoy en día (Junio de 2017) el “valor” de 1 bitcoin ronde los 2600\$?

Muy fácil, la suma de muchos factores en su conjunto:

- La característica de edición limita a 21 millones sólo.
- La usabilidad: cuanta más gente lo use, más valor tendrá.
- Transacciones en la red con bitcoin: va en aumento.
- “La moda”: Si él lo usa, yo también. (Realimentamos su uso).
- Ideológico y político: Libre, rápido y global.
- Especulación nivel 1: invertir en algo limitado, tipo coleccionista.
- Especulación nivel 2: invertir a corto plazo, para luego revenderlo más caro.
- Especulación nivel Dios: Apalancamiento de futuros con valores irreales de apalancamiento x2, x5 x10, x20 y hasta x50 veces el valor
- Huida de la economía real hacia un nuevo tipo de inversión **de riesgo** (crisis, guerras, conflictos, etc...)

Y muchos más que sería temas técnicos como la seguridad criptográfica, la descentralización, etc...

Y, ¿...es esto correcto? ¿El valor de algo en concreto se puede medir así de fácilmente?

*La **píldora roja** y su opuesta, la **píldora azul**, son símbolos de la cultura popular que representan la elección entre abrazar la a veces dolorosa verdad de la realidad (roja) y la dichosa ignorancia de la ilusión (azul).*

Los términos, popularizados en la cultura de ciencia ficción, provienen de la película The Matrix (1999)

[Wikipedia](#)

Si señor lector, EN EL MUNDO EN QUE VIVE SI, pero ¿y si hubiese otra manera de gestionar el valor?, ¿y si le dijera que tome “la pastilla roja”?

Le recuerdo que no soy economista, soy un humilde informático, y tengo mi punto de vista y mis ideales, pero le recomiendo que se apoye en este capítulo con el libro otro gran gurú: **Santiago Márquez Solís**.



Bitcoin. ¿Jaque mate al Sistema Financiero?

Libro 1. Enseñando criptomonedas a la abuela Pepa.

Autor: Santiago Márquez Solís

Además de ver la economía desde otro punto vista, se encontrará el lector con 2 grandes deducciones principalmente:

1. El valor que se le ha dado a bitcoin, ha sido igual e equivalente al valor del dinero que usamos actualmente, perdiendo por tanto, toda su esencia real y de su finalidad de creación original (recordar “Especulación nivel Dios”).
2. El principio de Gresham: aun habiendo gestionado mal la asignación del valor la cadena de bloques bitcoin (e incluso de otras), prevalece el principio de Gresham, donde el bitcoin y otras criptomonedas se han convertido en el valor moneda “bueno” mientras el fiat (dinero de uso corriente) en el “malo”.

El principio de Gresham se debe a un comerciante y financiero inglés del siglo XVI, cuyo nombre completo era (Sir) Thomas Gresham. Como comerciante y financiero que era, se fijó en una cosa curiosa, que si en un determinado país existían dos monedas de curso legal, y una era percibida por el pueblo como “buena” y la otra era percibida como “mala”, la gente prefería pagar con la moneda considerada como mala, para deshacerse de ella, y guardar la buena.

Por lo tanto:

¿Qué hace falta para que una cadena de bloques tenga un valor real? ¿Es necesario algo semi-centralizado que lo semi-controle?
¿Demasiada libertad e falta de control hacen que sea convertida en controlable? (Revise el lector en internet los problemas de consenso con la red Bitcoin con el tamaño de bloque y los mineros, por ejemplo).

Si tan buenos son los bitcoins, las cadenas de bloques, las criptomonedas, la descentralización, ¿por qué no se están usando ya masivamente?, ¿por qué no hay empresas y gobiernos que lo tendrían que tener en los primeros puntos de estudio e implantación?

La respuesta a todas esas preguntas, desde mi humilde punto de vista, **es la humanidad**. Las políticas de los países, los intereses, las economías como el petróleo, las armas, y sobre todo, las fronteras entre países, las divisas, la riqueza y la pobreza, hacen que el factor humano falte en esta ecuación.

Mientras las personas, desde el punto de vista humano, no se impliquen al 200% en ello, no podremos tener una o varias cadenas de bloques que realmente transmitan un valor real, de bienes, servicios o equivalente que haga funcionar esta ecuación de efectividad y confianza.



El mercado se revuelve

*Nuestras relaciones como humanos se basan en la **confianza**, y ahora la tecnología nos ofrece una nueva manera de establecerla, desplazando a las tradicionales entidades centrales de confianza, desde bancos, hasta gobiernos, pasando por aseguradoras o multinacionales de todo tipo.*

Y esto no es un típico discurso anarcohippyantisistema, es el propio mercado quien desplazará la forma de establecer confianza entendida como la prestación de un servicio, igual que ha “disroto” (estoy un poco cansado ya de la disrupción, y esto es “disromper”) otras actividades.

Hoy la tecnología es mucho más eficiente, barata, rápida y confiable en la prestación de servicios de establecimiento de confianza (para transacciones económicas, registro de propiedades, de actividades, y de todo lo que requiera confianza para funcionar, o sea todo...) que las entidades que tradicionalmente nos venían prestando estos servicios. El propio mercado se revuelve. Wellcome to the blockchain!

[Alex Casas](#), [Shelpin](#)

Pero bueno, sigamos, no seamos tan pesimistas, que el mundo no se hizo en 9 años... (2008 publicación del bitcoin paper). Le daremos la vuelta positiva al tema del valor más adelante.



El camino de la Blockchain, un camino que deja huella.

< Cuando conoces la verdad no puedes seguir viviendo en la mentira >

Como experiencia personal desde que me topé con Bitcoin a finales de 2012 no he podido desenamorarme de la tecnología subyacente, cuando conoces y comprendes qué es la cadena de bloques y te das cuenta de su potencial abres tu mente a un nuevo mundo.

< Porque comprender algo, es quedar libre de ello >

Blockchain o cadena de bloques no solo es la revolución de cómo concebimos las estructuras sociales administrativas y financieras entre las personas, sino que siembra un cambio de mentalidad y replantea todo aquello que damos por sentado y nunca nos hemos detenido a plantearnos.

<La desintermediación hace aumentar la prosperidad y las oportunidades>

Cada vez que hagas cola en un banco o en una administración para cumplimentar un documento cierra los ojos y piensa en Blockchain, esa compañera que trabajará para ti en el futuro.

Desde el punto de vista monetario: Bitcoin nos hace replantear que el sistema monetario centralizado el cual se ha sostenido con cierta ilusión a lo largo de la historia no sea el más correcto. Ahora cada uno puede ser soberano monetario utilizando unidades de cuenta basadas en criptografía imposibles de falsificar.

Asistimos a una revolución silenciosa, una revolución que comenzó en 2008 en plena crisis bancaria (¿casualidad?). Empezando con Bitcoin y siguiendo con la multitud de proyectos descentralizados que han ido apareciendo. Si, si estás pensando en dinero, hay y mucho, los bancos comerciales, grandes aseguradoras y todo el sector financiero está dentro de este camino Blockchain pues no se quieren perder esta fiesta. TÚ que vienes aquí en busca de información y curiosidad, lee y fórmate para comprender las oportunidades que puedes aprovechar.

Con el paso del tiempo me he dado cuenta que toda revolución comienza por una minoría de “locos” esos locos que nos hemos ido encontrando en el camino, con unos mismos valores y ganas de cambiar cosas, de no conformarnos con lo que se nos ha dado y sobre todo dejar huella. Gracias a este camino Blockchain, puedo decir que he aprendido, he perdido, he ganado, he pensado y reflexionado y sobretodo he evolucionado.

Nadie hubiera dicho que encabezaríamos el ecosistema Bitcoin aquella tarde en Valencia cuando fundábamos la asociación del Bitcoin Avalbit.org, cuando de ésta salía Octopocket, nuestra primera Startup, premiada internacionalmente, desde Valencia, Albacete, Castellón con dedicación y creencia firme en todo lo que hacemos trabajando para divulgar el conocimiento.

Coged asiento en este camino que ya ha comenzado y lo mejor es que nos toca escribir la historia con este libro y con todo lo que venga, no solo somos partícipes sino descubridores.

*[Jaime Sánchez](#), Bitcoin & Blockchain Analyst,
[Octopocket](#), Consultor en [Bitcoinadvisor.es](#)
Socio en [Avalbit.org](#) y ciudadano del mundo.*

El lector puede revisar también, la naturaleza criptoanarquista del bitcoin en un artículo publicado en [Cointelegraph España](#) (o en diversos sitios de la red), lo que demuestra a su vez, esa limitación humana por ideales políticos:



[La fortaleza básica del bitcoin](#)

3.4. Smart Contracts y Ethereum

Como ya hemos visto, cadenas de bloques hay muchas, con sus correspondientes tokens, todas ellas únicas (bitcoin, litecoin). Profundizaremos en el siguiente capítulo, pero ahora veamos una en concreto: Ethereum.

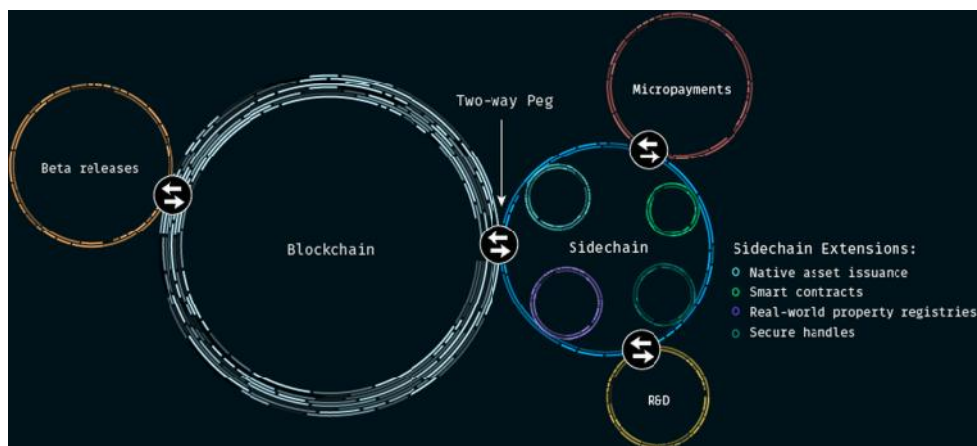
El canadiense Vitalik Buterin desarrolló la cadena de bloques Ethereum. Tiene 22 años, y esta cadena de bloques tiene algunas capacidades extraordinarias, en diferencia a sus principales predecesoras (bitcoin, litecoin y otras que ya ni existen o apenas tienen actividad).

La principal y diferente característica es que el software de su cadena de bloques puede realizar “Turing completo” mientras que bitcoin por ejemplo no. Con ello Ethereum permite realizar los llamados “Smart Contracts” de manera cíclica hasta que algo delimite su finalización.

Pero **ATENCIÓN**, y lo voy a poner mayúsculas y en negrita para que quede súper clarito: **BITCOIN TAMBIÉN PUEDE HACER SMART CONTRACTS**, pero no de manera cíclica (su lenguaje “no es Turing completo”) ni de manera tan sencilla como Ethereum. Para que Bitcoin pueda hacer un “Turing completo” en formato Smart Contract debe de recurrir a las llamadas SideChains (o ColoredCoins, términos que no voy a tratar por ahora). Si el lector quiere ampliar la información puede visitar [Blockstream](#), o la cadena de bloques [Lisk](#), o un artículo correspondiente:



[5 claves para visualizar mejor el potencial de Lisk](#)



Sidechains interactuando con blockchain. Blockstream explica en su paper como, a las sidechains, se les añade una nueva pieza llamada two-way peg. Two-way peg es “el conector” entre ambas cadenas y se encarga de hacer la “magia” para que los bitcoins “salten” a la otra cadena. Juntando ambas cosas obtenemos las pegged sidechain: cadenas laterales conectadas en todo momento. En la imagen puedes observar cómo, incluso, las sidechain pueden interactuar entre ellas. ¿Llegaremos a un escenario de blockchains interactuando con aspecto fractal?

Un Smart Contract es un Contrato Inteligente, es un contrato que se auto ejecuta. El propio contrato, programado dentro de la cadena bloques de ethereum, se encarga de ejecutarse, gestionarse, emitir o recibir pagos en base a premisas y condiciones, y puede hacerlo entre personas, entre entidades o simplemente entre máquinas (contratos contra contratos). Con ello, imagine querido lector, las infinitas posibilidades que podemos hacer en una cadena de bloques.

No vamos a menospreciar a bitcoin, ni a alabar a ethereum (y viceversa), cada cadena de bloques tiene sus finalidades y sus objetivos, sus condiciones y características, pero si destacaremos que mientras bitcoin creció y se expandió de manera libre, ethereum tiene el respaldo de grandes empresas como Microsoft.

Si quiere saber más sobre Ethereum: <https://www.ethereum.org/>



Desde que conocí Ethereum a finales de 2014, comprendí el potencial de esta tecnología y la capacidad que tenía para cambiar por completo los paradigmas sociales del momento. Di un giro a mi vida profesional de investigación, y decidí dedicar la totalidad de mi tiempo a lo que entendía como la revolución más grande construida desde el nacimiento de Internet. Desde entonces, comencé a trabajar como profesional, sumergido en un “bucle infinito” de nuevas oportunidades y proyectos, que terminaron por llevarme al proyecto en el que actualmente trabajo como responsable tecnológico, el Fluon Ecosystem.

Mi pasión por esta tecnología no es algo que pudiese predecir en aquel momento, así como mi absoluta dedicación a una sola materia. Y es que, a diferencia la irrupción de otras tecnologías, Blockchain no es solo un cambio tecnológico, o económico. Blockchain cambia por completo toda nuestra manera de interactuar y razonar, y con el tiempo modificará todas las estructuras políticas y sociales, pudiendo ser considerada su aparición como la principal innovación del siglo XXI.

Carlos Buendía, Head of Technology Fluon Ecosystem

Capítulo 4, Qué puede hacer una blockchain

Vayamos a los negocios, a mejorar problemas, al futuro, veamos que puede hacer la cadena de bloques por usted, por su empresa y por todos.

Hemos visto algunas de las características de cadena de bloques, que, a su vez, son soluciones a problemas o mejoras:

rapidez, en el caso de transacciones,

transparencia, en el caso de registros de consulta públicos

seguridad, criptografía de alto nivel

descentralizada, base de datos distribuida en cualquier punto del planeta con conexión a internet y comunicada a tiempo real entre los nodos

baja en comisiones, en el caso de transmitir valor

etc. no vamos a repetirlas todas.

Veamos primero si usted realmente necesita una blockchain, a nivel de implementación o de usabilidad, tanto en su día a día como usuario o como si es una empresa. ¿Tiene algún problema? ¿Desconoce que lo tenga? ¿Puede hacer las cosas mejor, más rápidas, más seguras, más económicas? Veámoslo.

4.1. Pensando en frío: usuario, empresa y emprendedor

Es una calurosa mañana de verano, usted tiene sed, decide acercarse a un bar y pedir un refresco, y el camarero le dice:

“puede pagar en bitcoins o en moneda (€, \$)”

Usted decide pagar en bitcoins, porque cree en ellos y por algún motivo más, pero su wallet (cartera) de bitcoins está vacía. Decide recargarla con su teléfono móvil, operación que se realiza casi al instante, mientras el camarero sigue esperando. Procede a pagar al camarero con bitcoins, pide el código QR del bar para hacer la transacción a la dirección bitcoin del bar, pero como usted es un poco tacaño, pone la comisión mínima de transacción. La red de bitcoin está actualmente saturada de transacciones, y demora en efectuarse 30 minutos.

Como puede apreciar el lector, en este caso NO es conveniente ni el uso de la blockchain como valor (bitcoin), ni le es rentable al bar, y mucho menos a la paciencia del camarero. Por rápida que hubiese sido la transacción en la red Bitcoin, hubiese sido más rápido y efectivo otros métodos de pago tradicionales (imagine que además de sed hubiese tenido prisa también).

Bueno, una solución al tiempo de confirmación de la transacción hubiese sido pagar con otra “criptomoneda” como por ejemplo *litecoin* que tiene un tiempo menor, pero ya hemos escuchado al camarero que solo efectivo o bitcoins, encontrando con ello un problema añadido, el bar no acepta la cadena de bloques *litecoin*.

En el caso del uso de una blockchain que transmita valor, SI es efectivo por ejemplo en transferencias internacionales, donde 30 minutos si son un tiempo considerado rápido y la comisión mínima (1x1000 en la red Bitcoin) también se considera muy baja en comparación de los medios habituales como bancos o empresas de envió de dinero.

Vaya... parece que “no todo el monte es orégano” en mundo de las blockchains.

Pretendo llevar al lector a que piense: muchas veces, el concepto “estar de moda” no significa que usted o su empresa necesite de esa moda. En informática, muchas cosas que usted puede pensar que deberían de ser ya una cadena de bloques se pueden gestionar y manejar de manera más eficiente con una simple base de datos distribuida o centralizada.

La cadena de bloques se diseñó para otros usos más específicos, algunos todavía ni los conocemos. Por ello y, a continuación, va a encontrarse el siguiente símbolo:



Este símbolo indicará una idea, una mejora, ya creada o por crear, que usted lector, si tiene madera de emprendedor, debería de estudiarla y tenerla en cuenta, usted también como usuario, debe valorar si esa idea le aporta una mejora real, y usted empresario revisar si es conveniente implementarlo en su empresa o negocio y que beneficios o mejoras le aportaría.

Recuerde, aunque pronto verá y usará sin darse cuenta cadenas de bloques, no todo tiene que ser blockchain, debe de aprender a **diferenciar lo que es blockchain y de lo que NO ES blockchain.**

“Gracias a la tecnología financiera como el blockchain, las empresas se convierten en su propio banco, y a un coste casi cero” (Periódico Expansión)



*Alberto Gómez Toribio,
especialista en tecnología Blockchain, Coinffeine*

4.2. Bancos y entidades financieras

Ya hemos visto como por medio de la blockchain, por ejemplo, de bitcoin o litecoin, podemos transmitir valor a través de la red con una serie de características que nos aseguran su transmisión.

La cadena de bloques funciona como un libro mayor de contabilidad en tiempo real, elimina el tiempo de liquidación entre entidades financieras, es decir, acelera, verifica y conforma una transacción casi al instante.

Reduce las comisiones a niveles muy bajos para el cliente o la propia entidad, no son posibles las cancelaciones (gran problema que ocurre por ejemplo con las tarjetas de crédito y débito), y evita el doble gasto de una misma unidad monetaria.

Evolucionar o morir, los bancos tal y como los conoce ahora pueden ser reemplazados por tecnología blockchain. ¿por qué?

Porque la tecnología blockchain permite:



- Acceso a personas al ciclo económico financiero que hasta ahora no se les permitía por su localización geográficas, políticas de su país o situación social.



- Pagos globales desde cualquier entidad o persona sin intermediación

- Micro finanzas y prestamos entre personas, empresas o entidades

*"El blockchain hace viables los **micro pagos** porque elimina las comisiones"* (Periódico Expansión)



Roberto Fernández Hergueta, director del área Digital de Everis

Todo esto y mucho más, y si entramos en el sector financiero puro y duro, el gran **Víctor Escudero Rubio** nos explica con sumo detalle en uno de sus artículos muchas más características:

Cada vez son más las personas que me preguntan por las posibles implicaciones que Blockchain podría tener en su sector.



Atendiendo a esta petición, comenzaré este artículo indicando algunos los usos actuales y futuros de esta tecnología en Banca y en el sector financiero en general.

Establecimiento de acuerdos y ejecución de contratos

Tan pronto como el registro de un activo digital se ha registrado en una cadena de bloques, su transmisión posterior automáticamente desencadena las operaciones de conciliación y apunte de asientos contables asociados. Es más, como no es posible disociar las operaciones de transmisión y registro, al actuar ambas como si de una sola instrucción atómica se tratase, se garantiza en todo momento la consistencia de la información.

Los usuarios que hubiesen recibido un token digital, que representara, por ejemplo, la propiedad sobre los títulos de una compañía cotizada en el mercado continuo, estarían en disposición de poder recibir automáticamente los dividendos y los derechos a voto a los que diera lugar la posesión de las acciones de esa compañía.

Procesos de reconciliación y auditoría

Con el uso de cadenas de bloques, las organizaciones pueden eliminar la hasta ahora imprescindible, pero costosa contabilidad de doble entrada, simplemente conectando el Back-office que realiza el procesamiento de una transacción con quien la genera.

Así, en lugar de tener que realizar periódicamente informes y auditorías para los reguladores, será posible comunicar datos en tiempo real, lo cual permite una mejor monitorización de riesgos por parte de los reguladores y supone menores costes de implementación de los requisitos regulatorios para las instituciones financieras.

Firma de mensajes en representación de un tercero

Hasta ahora, una empresa cuya actividad principal fuese la importación/exportación de mercancías, con frecuencia se veía obligada a

solicitar una carta de su banco para probar que disponía de suficientes fondos en su cuenta antes de realizar una gran operación. Gracias a la tecnología Blockchain, la simple firma de un mensaje sobre la cadena de bloques bastaría para probar el acceso a dichos fondos.

Conexión con dispositivos IoT (Internet of Things)

Al permitir que los sistemas de una organización se conecten con los datos generados por miles de pequeños dispositivos, las organizaciones pueden obtener datos en tiempo real de infinidad de asuntos, tales como condiciones meteorológicas muy destructivas (para aseguradoras), localización de clientes (prevención de fraude), estado de las instalaciones de producción (valoración de activos), etc.

Facilitar la transferencia de activos

Un libro mayor distribuido permitiría que los títulos de propiedad puedan ser intercambiados libremente en el mercado y, además, estar asociados a un objeto inteligente. Por ejemplo, una cerradura electrónica que tan sólo se abriría con una determinada clave.

Automatización de los procesos de cumplimiento regulatorio

Si todas las transacciones de compra-venta de activos se realizasen sobre una cadena de bloques, donde las operaciones estuviesen cifradas con las claves de cada una de las contrapartes, más la del regulador, éste último podría conocer casi en tiempo real la posición financiera de cada uno de los intervinientes en la operación. Asimismo, podría saber si las transacciones adicionales podrían exceder el nivel de riesgo o los requerimientos de capital necesarios. En situaciones donde estos umbrales se superasen, el regulador podría automáticamente cerrar el acceso a mercados específicos o imponer sanciones.

Una blockchain privada (permissioned ledger) podría contener todas las reglas de operación, regulación, auditoría y controles internos embebidos en su propio código de ejecución, haciendo innecesaria gran parte de las atribuciones actuales que hoy en día tienen ciertas instituciones centrales y organismos supervisores y reguladores.

Identidad portable

La ventaja de las cadenas de bloques es que al estar basadas en criptografía no es necesario requerir credenciales a los usuarios. Esto significa que los participantes en una Blockchain pueden construir su propia identidad, simplemente, generando una llave privada a la que solo ellos tengan acceso. La entidad, ya se trate de un individuo o un negocio, puede portar su identidad a lo largo de diferentes servicios siempre y cuando mantenga la misma dirección.

La identidad se puede mantener a salvo mediante el uso de una clave maestra y algún otro factor de autenticación adicional como podría ser la huella, o un código de Google authenticator, mientras que se puede generar un nuevo token por cada nueva identidad que se quiera crear para un servicio en particular, siendo decisión del usuario relacionar ambos perfiles entre sí o mantenerlos totalmente separados.

Compañías automatizadas y nuevos vehículos de inversión

Como los activos y los fondos pueden interaccionar directamente entre sí a través de una cadena de bloques, nuevos vehículos de inversión basados en la ejecución de contratos inteligentes podrían determinar con precisión las propiedades de un negocio con total transparencia.

La cadena de bloques puede registrar tanto la emisión de nuevas acciones como la negociación de las ya existentes. Las instituciones financieras pueden elegir comerciar dentro de sus propios pools de liquidez, utilizando por ejemplo sidechains, pero sus acuerdos con terceros, necesariamente deben poder enlazarse en la cadena de bloques principal a través de un proceso de reconciliación automático.

Blog del Víctor Escudero

Víctor Escudero Rubio

Y efectivamente, los bancos y entidades financieras no se están durmiendo. A nivel internacional existe ya el [consorcio R3](#), que es una empresa de innovación centrada en la construcción y autorización de la próxima generación de tecnología de servicios financieros globales, la cual, reúne a los principales bancos y entidades financiera de todo el mundo.



En España se ha creado por ejemplo la [RedLyra](#), la red blockchain española multisectorial de referencia en el mundo, que también reúne a grandes bancos y empresas:



la tecnología blockchain alterará de raíz el modo en el que las instituciones financieras hacen negocios y acabará por convertirse en el “corazón” del sistema financiero internacional.

World Economic Forum (WEF)

4.3. Propiedad intelectual y catastral

Usted puede ser un cantante, un artista, un pintor, un escultor, un escritor. La obra que realiza hoy en día tiene un reconocimiento difícilmente demostrable si no interfiere un tercero que certifica que esa obra o producción es suya: por ejemplo, un notario. La figura del notario parece peligrar también al igual que los bancos, la tecnología blockchain permite registrar de manera inequívoca y en el tiempo cualquier cosa que quiera.

Por ejemplo, este libro que está leyendo, si se le aplica una técnica llamada *Hash*, devuelve un número muy grande único. Sólo con que modifique una simple coma o un punto del texto, el *Hash* que se generaría sería totalmente diferente, demostrando así mi autoría.

Por medio de esta técnica, podemos registrar en la cadena de bloques cualquier cosa, ya sea digitalmente como este libro, o por otros procesos un poco más complicados para cosas físicas.

Y cuando digo cualquier cosa me refiero a cualquier cosa, como por ejemplo una propiedad como su vivienda o un terreno.



Ya existen empresas *BLOCK punto COM* que se encargan de realizar una verificación única de la originalidad de un diamante, por ejemplo, y otras están preparando modelos de registro de propiedades y terrenos en los países en los que la política y la dictadura no es muy de fiar.



Del mismo modo que lo identifica como suyo, también podría asignar un Contrato Inteligente (Smart Contract) por su uso, alquiler o explotación, y recibir por alguna cadena de bloques el valor expresado en dicho contrato (Bitcoin o Ethereum, por ejemplo).

Profundicemos un poco más con un ejemplo, como la blockchain puede ser una buena tecnología para la distribución de la música y retribución a sus autores:

(del artículo original <http://tecnologia12.com/como-blockchain-puede-cambiar-la-industria-de-la-musica/>)



Hemos visto y repito, que la blockchain es como un libro distribuido que puede validar y registrar las transacciones sin necesidad de una autoridad central. Nadie posee el control, se extiende a través de los nodos que constituyen su red y está públicamente disponible para todo el mundo. La información almacenada, se interrelacionan a través de hashes criptográficos, que hacen prácticamente irreversible y a prueba de manipulaciones. En pocas palabras, significa que las partes pueden hacer entre iguales intercambio de datos, dinero o cualquier otra cosa de valor en cualquier cantidad y de forma segura.

En la industria de la música, podría transformar la edición, la monetización y la relación de los artistas con sus comunidades de fans.

En primer lugar, música puede ser publicada una cadena de bloques con un ID único y sello de tiempo de una manera eficaz e inalterable. Esto puede solucionar el problema histórico de contenido digital descargado, copiado y modificado para el ocio de los usuarios. Cada registro puede almacenar metadatos que contengan propiedad e información de los derechos de una manera inmutable y transparente para que todos puedan verla y comprobarla. Esto asegurará que pagarán a las personas adecuadas por el uso de los contenidos.

Una infraestructura basada en contratos inteligentes, podría reportar los pagos directamente al autor o a la discográfica. Los fans podrían incluso donar cantidades muy pequeñas como donativos, adquirir productos añadidos como entradas a conciertos, relacionados directamente con el autor.



En el artículo original puede encontrar más detalles.
<http://tecnologia12.com/como-blockchain-puede-cambiar-la-industria-de-la-musica/>
o visitar un ejemplo en <http://dotblockchainmusic.com/>

4.4. Trazabilidad y verificación de productos originales

He comentado anteriormente que ya existe una empresa que usa la tecnología blockchain para verificar la autenticidad de los diamantes que sus distribuidores registran para luego venderlos. El proceso es realmente sencillo: el diamante tiene grabado un código, y el cliente cuando lo compra se le entrega otro código (sobre cerrado opaco). Cuando el cliente llega a casa registra mediante ese código y el pre-registrado por la empresa en la blockchain su compra, siendo desde ese momento suyo para siempre, con su número único de identificación del diamante. Con esto, el cliente puede demostrar siempre que quiera su calidad, su veracidad como diamante, de donde se compró, y en caso de robo, un ID único como prueba de que es suyo. También en caso de venta a un tercero (casa de empeño, por ejemplo) se puede hacer un proceso inverso de verificación.

La empresa que realiza este proceso es <https://www.everledger.io/>



Imaginemos ahora todo lo que se trazar de forma fiable a través de tecnologías asociadas a blockchain:

- Comida y bebidas
- Fármacos originales (hay muchas copias ilegales)
- Materiales de cualquier tipo (construcción, tierras, colas, ...)
- Aparatos electrónicos, máquinas, vehículos ...
- Juguetes, herramientas, utensilios....

Y además les podríamos añadir en su registro el Origen, fecha de elaboración o recogida, país de origen, lugar de fabricación... y cualquier característica que se nos ocurra.

Esto aportaría al consumidor una mayor confianza a la hora de adquirir un producto, ya podría confirmar casi al instante la transparencia y fiabilidad de esos datos, llegando a la confianza total de un producto - una marca; y son ello evitaríamos copias ilegales, suplantaciones, controles alimenticios, etc., etc., etc....

4.5. Transparencia: Entidades públicas

La política y los gobiernos siempre han pecado de falta de transparencia. No voy a entrar en acusaciones, lo que sí puedo aportar son todos los “supuestamente” que leemos en los periódicos continuamente.

Pues parece que la blockchain podría ser una solución a la transparencia de los entes públicos, siempre y cuando ese gobierno quiera ser transparente claro ;)

Imaginemos los presupuestos económicos de un país de este año, junto con un balance de caja a fecha de hoy. En los presupuestos se detalla cómo va a usarse el dinero recaudado más el remanente en caja pero, ¿Dónde se refleja esto? En bases de datos internas que luego “se hacen públicas”, ¿un doble trabajo no cree? ¿no sería mejor añadir cada movimiento de libro mayor a una cadena de bloques a tiempo real donde se pudiese consultar los apuntes y con ello comprobar si se siguen o no los presupuestos económicos pactados?. Además, siendo pública, se podría consultar si el gasto realizado es correcto o no (existen algunos ejemplos de gastos que multiplican x10 su coste en comparación si usted lo hubiese gestionado, hablamos facturas de obras, facturas de luz en donde podríamos preguntar por qué se usa tanta energía en determinados edificios públicos y aportar soluciones, costes publicitarios, etc...)

Pero no hace falta apuntar tan alto, bajemos a colectivos sociales llamados agrupaciones políticas, esas que prometen en elecciones un montón de cosas. Si registrásemos esas cosas en una cadena de bloques, también conseguiríamos que los políticos cumpliesen con sus palabras mediante hechos, hechos que también quedarían registrados públicamente.

En resumen, la **transparencia** y la **confianza** si no la tienen, es por qué no quieren.

4.6. Transparencia: Entidades privadas

Si se puede hacer en un organismo público, también se puede en uno privado. Mediante cadenas de públicas, o mixtas (parte pública y parte privada) las empresas podrían ser auditadas en todo momento por quien quisiera, reduciendo costes, y creando confianza, consiguiendo nuevas ISOs de calidad, de trazabilidad de productos, controles sanitarios, de fabricación y muchos beneficios más.

Aunque claro, está la competencia, estos datos quedarían expuestos a su vez a la competencia, factor que desde el ámbito privado podría ser un problema para por ejemplo lanzar un nuevo producto.



Pero podríamos dar una clave pública para lo general, una privada para proyectos internos y controles de la empresa, y una clave “temporal” que se activaría en un determinado momento del tiempo... ¿no?

Todavía quedan muchas cosas por inventar...sobre todo en el ámbito de las blockchain ;)

4.7. Loterías, rifas y otros sorteos transparentes:

Como hemos visto, la cadena de bloques añade cada bloque en base a unos cálculos basados en el bloque anterior, generando un hash ÚNICO para ese grupo de transacciones que contiene.

Este Hash, nos puede servir como elemento de aleatoriedad, ya que es muy difícil saber el hash que tendrá el siguiente bloque o un bloque futuro.



Mediante esta característica, podemos hacer loterías o sorteos basados en ese número Hash desconocido. Con ello volvemos a recalcar la característica principal de las cadenas de bloques públicas: la **transparencia**.

Veámoslo con un ejemplo sobre la blockchain de *bitcoin*:

Supongamos que tenemos que hacer un sorteo de un único acertante a un número. El número acertante está dentro del rango 0-4095 (en hexadecimal entre el 000-fff). Asignamos un número a cada participante entre el 0 y el 4095 inclusive.

Elegimos un bloque de blockchain futuro, por ejemplo, uno que sepamos que se minará un sábado de la semana próxima que es cuando se daría a conocer el resultado del sorteo. Para ello tenemos que hacer un cálculo estimado del bloque que este momento se ha minado y sumar tantos bloques a ese número como bloques se minan cada 10 minutos aproximadamente hasta ese día:

Si estamos en el bloque 461000, el sábado siguiente en una semana exacta sería aproximadamente el 462024.

Ahora disponemos de una semana para repartir los números entre los participantes.

Cuando llegue el sábado siguiente, y el proceso de minado de la blockchain llegue al bloque 462024 tendremos un único ganador.

¿Cómo sabemos quién es el ganador y como se hace público y transparente para todos?

Lo hace la blockchain en el proceso de minado: cogemos el hash generado por el bloque 462024 de la cadena de bloques de bitcoin:

0000000000000000013329c6ab777cd3545196bda9346eba4ff28c0100ff977d

Seleccionamos sólo las últimas cifras del hash de ese bloque: *77d*

Tener en cuenta que el hash está en Hexadecimal por lo que hay que transformar estos 3 dígitos hexadecimales a un número decimal: 1917. Por lo que nuestro ganador será aquel que su número coincida con las 3 últimas cifras del hash del bloque 462024 pasado a decimal: el número 1917.

Con esto hemos realizado un sorteo totalmente aleatorio (es técnicamente imposible predecir que hash tendrá un bloque a futuro de más de 2000 bloques de diferencia, y que transacciones contendrá para su minado), y transparente (se ha publicado en la cadena de bloques).

También podemos hacer más variantes de sorteo por este sistema:

- Si queremos varios acertantes solo habría que elegir más bloques, por ejemplo, 3 acertantes se elegirían los bloques 462024, 462025 y 462025.
- Si nuestro sorteo necesita menos números, reduciríamos los dígitos de hash últimos a elegir: 1 nos daría entre 0 y 15, 2 nos daría entre 0 y 255 (recordamos que está en hexadecimal).
- Si queremos más números para el sorteo aumentaríamos los dígitos de hash últimos a elegir: 4 nos daría entre 0 y 65355, 5 entre 0 y 1048575, etc...

Si no conseguimos vender todos los boletos de una serie, se puede añadir en las condiciones del sorteo que en el caso de que el bloque número X no coincida con ningún boleto vendido, el número del premio pasaría a ser el del siguiente bloque minado, por ejemplo, retrasando apenas 10 minutos el resultado final del sorteo.

Como vemos, no hace falta un complejo sistema de azar...el propio bloque es el azar, la propia blockchain es la que reparte la suerte y de manera matemáticamente comprobable y transparente.

4.8. Gestión real de Identidad y reputación

La **confianza** es algo muy difícil de conseguir, tanto en las empresas con sus clientes, como entre personas o entidades de cualquier tipo.

La cadena de bloques puede generar un identificador único para cada persona y, además asociarlo a unas acciones, buenas o malas, que se quedarían registradas para siempre y de manera inmodificable.

Esto suena bastante “ilegal”, porque nos saltaríamos leyes como “el derecho al olvido”, incluso determinados puntos de privacidad personal.



Bueno, busquemos una solución a la par, tanto para lo bueno como para lo malo, y respetando siempre la privacidad y a las personas: ¿Por qué no creamos DOS BLOCKCHAINS, una “buena” y otra “mala”?

En la buena y pública, un futbolista podría agregar todos sus partidos jugados, todos sus goles, con un ID único.

En la mala y privada, las empresas de seguros podrían asignar a un ID en concreto, los partes de accidentes que ha tenido, para que, en futuro calcular el riesgo de esa ID única y poder ofrecerle o no alguno de sus servicios, bonificaciones o incrementos de precio justificados.

Con ello crearíamos una reputación universal de un individuo, centralizada en una cadena de bloques única, sin contradicciones entre diferentes fuentes de datos como ocurre ahora.



Imagínese como si su currículum público fuese visible por todo el mundo, un médico, un fontanero, un humilde informático ... todos se mostrarían reales y transparentes.

¿No le daría esa reputación a usted más confianza con sus iguales?

Diego León Ullauri, nos cuenta una historia real relacionada con este punto de identidad digital:



La siguiente es una historia real. Vivo en Ecuador con mi novia que es de Argentina. Tenemos planes para casarnos, y con eso en mente viajamos a Argentina para obtener algunos documentos.

Cuando estuvimos en la oficina de Registro Civil de Salta, Argentina, nos dijeron que (aunque parezca extraño) no tienen base de datos, así que toda solicitud la envían para la capital, Buenos Aires. El papeleo, según nos explicaron, tarda un mes. Y eso no es todo, luego de que llegue el documento a la ciudad de Salta es necesario hacerlo apostillar (Apostilla de la Haya) y para eso hay que enviar de regreso el documento a Buenos Aires. Toda una odisea.

Como no teníamos ese tiempo regresamos a Ecuador (el viaje lo habíamos hecho por tierra) y dejamos encargando a una amiga de mi novia que nos ayude con las gestiones.

A nuestro regreso, la parte que yo quería evitar (o al menos pasar muy de prisa) era Bolivia, un país que al ingreso, en las oficinas de migración, nos pidieron una coima de 50 dólares a cada uno. Fue la primera mala experiencia y aún no había ni entrado a territorio Boliviano. Bolivia además es el único país de Sudamérica que otorga sólo 30 días de permiso cuando el resto de países otorga 90 días. Y los “gringos” la tienen peor; necesitan Visa y un pago para entrar a Bolivia.

En fin, llegamos a Tarija (la ciudad al sur de Bolivia) sin novedad y casi al instante salimos rumbo a La Paz. Al llegar a la capital, luego de más de 15 horas de viaje, pedí a mi novia que me ayudara a echar una mirada al equipaje mientras yo buscaba boletos para Puno (Perú). En ese momento una persona (luego nos enteramos de que fueron 5) hurtó el pequeño morral en donde teníamos todos nuestros documentos: DNI, Cédula, Pasaporte y Licencia de conducir. Nos sentimos morir. Pedimos a la policía que nos ayude a ver en las cámaras de seguridad lo que había sucedido, pudimos corroborar que efectivamente 5 personas actuaron en complicidad (1 persona hizo preguntas a mi novia, 2 personas taparon parcialmente las cámaras, 1 persona tomó el morral y la última persona salió de la terminal

a toda prisa con el morral). ¿Qué hacer ahora? por suerte mi novia contaba con un primo que vivía en La Paz y decidió llamarlo. Nos hospedó en su departamento en donde vivía con su esposa. Las autoridades nos habían dicho que debíamos ir al Consulado tanto de Ecuador como de Argentina para obtener nuevos documentos y continuar el viaje.

El proceso para obtener los documentos nos tomó tres días y dinero. En la embajada de Ecuador me otorgaron un Salvoconducto ya que para pedir un Pasaporte de Emergencia debía esperar un mes hasta que llegue el Pasaporte desde Ecuador. Por suerte el trámite me tomó solo 40 minutos y no tuvo costo alguno. Sin embargo, en el Consulado Argentino las cosas fueron diferentes, solicitaron un pago de 50 dólares y el boleto de viaje para Perú como requisito para emitir un Pasaporte de Emergencia. Y no podíamos comprar ningún boleto porque no estaba claro cuando nos iban a entregar dicho Pasaporte de Emergencia. Si nos lo entregaban luego de la fecha del viaje íbamos a perder el dinero usado en la compra del pasaje. Finalmente, luego de varios intentos, logramos obtener el Pasaporte de Emergencia unas horas antes del viaje.

Ir a los Consulados de nuestros países no nos aportó ninguna tranquilidad. En primer lugar, no trabajaban allí personas de nuestro país, estaban personas locales. El Cónsul seguramente estaba al fondo del edificio haciendo algún tipo de papeleo. El poco personal de nuestros países trabajando en el Consulado fue reducido y no prestaban la ayuda necesaria. Sentimos que no les importó si perdimos todo el dinero y los papeles. Ellos únicamente seguían procesos (burocráticos). No hay un lado humano. En segundo lugar, los Consulados únicamente trabajan de 8 am a 1 pm. Si se presenta alguna emergencia por la tarde, no hay nadie a quien pedir ayuda. El trato en los consulados de Ecuador y Argentina nos dejaron con un sabor amargo en la boca. Éramos solo un número más en sus trámites burocráticos.

Al cuarto día pudimos iniciar nuestro retorno a Ecuador. Y mientras viajaba cruzaba por mi mente que un día en el futuro seremos libres de viajar por el mundo sin que oficinas de migración o consulados se interpongan en el camino enlenteciendo algún proceso o echándolo todo a perder. Con tan solo una lectura de nuestro iris, nuestras huellas digitales,

reconocimiento de voz y (probablemente) lectura de ADN in situ; podremos viajar de manera rápida y segura, pero ¿Cómo podría suceder?

Soy un apasionado de las criptomonedas desde el año 2015 y desde entonces había escuchado que la tecnología que sostiene a Bitcoin, llamada Blockchain, iba a cambiar el mundo en muchas formas, una de ellas era la descentralización de la información y de cómo esta información iba a ser verificable e inalterable. Esto me llevó a investigar si actualmente hay proyectos basados en Blockchain que permitan a las personas administrar su identidad en la Blockchain y descubrí dos interesantes proyectos:



*uPort(https://twitter.com/uport_me)
y Civic (<https://twitter.com/CivicKey>)*

La idea es que cuando una persona necesite mostrar su identidad a otras personas (o instituciones), éstas podrán verificar la información en la Blockchain sin que se lleguen a apoderar de dicha información evitando que vaya a parar a alguna base de datos centralizada. Toda la información se quedará con el usuario siempre. Con la tecnología Blockchain el dueño de los datos y de toda la información será siempre el usuario final.

La identidad basada en Blockchain abre también la posibilidad para que millones de personas alrededor del mundo, que no poseen ningún documento de identificación, puedan tener una identidad, su propia identidad, almacenada de forma inalterable en la Blockchain. Con esta tecnología podrían entrar al sistema financiero y ser sujetos de crédito, podrían también recibir remesas, etc. Esta tecnología ofrecerá ventajas que ahora mismo son impensables...

Por cierto, ¿Y si registro mi matrimonio en la Blockchain sin tener que pedir permiso a ningún gobierno?

Diego León Ullauri

<https://twitter.com/DiegoLeonU>

“El disponer de un ID es libre, no tiene por qué aceptarlo ni usarlo, usted sigue siendo libre, la tecnología blockchain no ha venido a restarle derechos de privacidad ni le obliga a nada, al contrario, la tecnología blockchain ha venido para mejorar muchas cosas.” - José Felip Darás

4.9. Votaciones

Acabamos de ver en el anterior punto que se podría crear de algún modo un ID único para cada persona, empresa o entidad.

¿Y para que podemos usar ese ID único?

Ahora ya existe algo igual, lo llamamos “documento nacional de identidad” o “pasaporte” pero, de buena tinta sabemos, que son falsificables.

Un ID gestionado y creado en una cadena de bloques tiene un nivel de seguridad y veracidad que no le voy a explicar de manera técnica, pero si le diré que es muy muy alto, incluso me atrevería a decir que es “infalsificable”.



Si tan alta es la seguridad e “infalsificable”, imagine todo lo que se podría hacer a nivel de verificación y uso con ese ID: votaciones de forma transparente y segura.

Proyectos como <https://followmyvote.com/> ya permiten realizar votaciones online, de manera segura con la blockchain. Aquí por ejemplo se detalla el concepto y la implementación en un *paper*: <https://www.economist.com/sites/default/files/plymouth.pdf>

incluso los gobiernos apoyan la iniciativa:

<http://www.govtech.com/security/Will-Blockchain-Based-Election-Systems-Make-E-Voting-Possible.html>

y aquí un resumen presentación:

http://bitcoin-class.org/presentations/Blockchain_Voting.pdf

4.10. Inteligencia Artificial e “Industria 4.0”

Algunos puntos que hemos visto ya, los podríamos unir entre ellos y hacer que, mediante contratos inteligentes, cadenas de bloques mixtas y aparatos, se comunicasen entre ellos, que se auto gestionaran, se auto repararan, hiciesen pedidos cuando les faltase algo, todo dentro de un entorno seguro y verificado.



En este punto, me ha permitir el lector que no me pronuncie, no por desconocimiento, si no porqué el siguiente artículo detalla de suficiente manera y de manos de todo un experto el contenido que quiero transmitirles:

Oscar Lage, responsable de ciberseguridad de Tecnia, el centro privado de investigación más grande de España y responsable del Tecnia Blockchain innovation Center, coautor del libro *Blockchain: la revolución industrial de internet*



Blockchain, la columna vertebral de la Industria 4.0

Desde que se inventaran las bases algorítmicas de la tecnología blockchain, el interés por la misma no ha parado de aumentar. Lo demuestra el hecho de que empresas de todo el mundo estén realizando inversiones millonarias para desarrollarla y tomar una posición privilegiada en la que será la próxima revolución industrial.

El sector financiero fue el primero en analizar y estudiar blockchain. El sector industrial en general, y más concretamente la fabricación avanzada es uno de los sectores que ofrece un mayor potencial disruptivo a día de hoy. Actualmente la comunidad científica y tecnológica trata de imaginar las posibilidades, usos y modelos de negocio que habilitará esta tecnología.

Aplicaciones potenciales de blockchain

La digitalización y coordinación cooperativa de las unidades productivas van a suponer un nuevo hito en el desarrollo industrial. En la actualidad, la demanda es cada vez más sofisticada y requiere de productos más

inteligentes y personalizados. Al mismo tiempo, la industria manufacturera deberá ser capaz de adaptar el actual sistema de fabricación, concebido para la fabricación masiva. El objetivo de la cuarta revolución industrial, de hecho, viene definido por nuevas fábricas inteligentes, capaces de producir miles de configuraciones diferentes de un producto y de fabricar series cortas o incluso miles de configuraciones diferentes de un mismo producto a precios muy competitivos.

La digitalización es la base de esta revolución industrial: dará como resultado la denominada “industria inteligente”, sustentada en tecnologías facilitadoras como son el internet de las cosas (IoT), las comunicaciones Machine to Machine (M2M), las plataformas en la nube, etc.

Los datos, además, tendrán un mayor valor en el negocio, de modo que no serán un mero resultado del proceso de fabricación, sino la base del producto o servicio, o incluso el propio producto en sí mismo. Por esta razón se están lanzando diferentes iniciativas denominadas Industrial Data Platform dirigidas a gestionar la soberanía y explotación de los datos industriales. Algunas de las plataformas emergentes en este ámbito son Industrial Data Space, BOIP (Basque Open Industry Platform), Mindsphere de SIEMENS o Digital Manufacturing Commons (DMC), liderada por GE y UI Labs.

Blockchain se postula como la tecnología facilitadora de dicha revolución industrial. Ofrece un mecanismo de gestión de la soberanía del dato confiable y seguro para habilitar la automatización avanzada y colaborativa tanto entre las propias fábricas inteligentes como a un nivel inferior entre sus propias máquinas de fabricación avanzada.

La fábrica inteligente del futuro estará compuesta por dispositivos IIoT (Industrial Internet of Things) y por módulos de fabricación conectados entre sí que funcionarán de forma auto gestionada y/o autosuficiente. De esta forma, y mediante el uso de tecnologías como blockchain, surgirá una nueva economía de las cosas en la que los propios dispositivos, mediante transacciones M2M serán capaces de llegar a acuerdos de suministro de materias primas, piezas, mantenimiento, energía y delegación/coordinación de la producción, e incluso también logísticos. Quedarán reflejados en

Smart Contracts y su pago se ejecutará automáticamente cuando se cumplan las condiciones establecidas en el contrato.

Automatizar y agilizar ciertos procesos actuales es la condición esencial para que la fabricación inteligente pueda llegar a producir series cortas a precios competitivos. De no ser así, los costes indirectos que se amortizarán por cada lote unitario podrían superar el coste de fabricación del propio producto, como ocurre en la actualidad.

Según el paradigma de la Industria 4.0, la solución pasa por la desintermediación del proceso productivo, de forma que las empresas puedan recibir las peticiones desde un portal descentralizado y fabricar series cortas de forma automática. Así se facilita que la fabricación pueda ser realizada por pequeñas PYMEs locales, que cooperan de forma coordinada para ofrecer este servicio de fabricación integral. Esa plataforma descentralizada es posible gracias a blockchain. Un Smart Contract cerrará automáticamente el acuerdo con la mejor oferta sin necesidad de intervención de ninguna de las partes.

A su vez la trazabilidad de cada uno de los productos/bienes producidos y sus componentes desde el inicio de su producción hasta su obsolescencia o fin de su vida útil en una blockchain privada en conjunción con estrategias de intercambio de información en la cadena de suministro como las anteriormente mencionadas Industrial Data Platform, y la automatización de la Fabricación avanzada y futuros Marketplaces industriales son una nueva vía de conocimiento sobre sus productos y bienes a lo largo de su vida útil.

Cabe resaltar que la trazabilidad utilizando RFID u otras tecnologías se presuponen ya implantadas y lo relevante en esta fase es que el productor pueda disponer de información más allá de su ciclo productivo o intervenciones propias y de que el ensamblador o productor del bien final pueda tener la trazabilidad unívoca de cada pieza ensamblada en su componente; llegando ambas partes a poder evaluar el resultado de las innovaciones y pequeños cambios de producción/diseño incorporados en el proceso de fabricación que puedan influir positiva o negativamente en la vida útil del bien/producto.

En este sentido Airbus o Mercedes (Daimler AG) son de las primeras multinacionales que han anunciado su involucración en las tecnologías blockchain, y más concretamente ambos podrían estar trabajando en la trazabilidad de cada pieza/componente de sus productos como una línea prioritaria dentro del proyecto Hyperledger de la Linux Foundation desde su incorporación hace tan solo unos meses.

En el medio plazo ambas compañías podrían ofrecer a toda su cadena de valor una blockchain privada en la que compartan los datos de forma bidireccional con cada uno de sus proveedores e incluso clientes/usuarios. De hecho, Airbus además ha comenzado con una iniciativa divulgativa para poder explicar a todo el grupo y sus proveedores la relevancia de blockchain para Airbus en su estrategia tras un análisis exhaustivo sobre las ventajas de Blockchain en el grupo.

Oscar Lage
Tecnalia

Si mides el éxito de bitcoin con los éxitos de la industria actual y la obsoleta que reemplaza, lo estás haciendo mal.



Andreas M. Antonopoulos,
autor de “Mastering Bitcoin” y “The Internet of Money”

4.11. Aseguradoras

Al igual que hemos visto ejemplo de los bancos y las entidades financieras, las aseguradoras llevan el mismo camino, subirse al tren de la tecnología blockchain o dejar de prestar algunos de sus servicios.

Y parece que tampoco se han dormido, ya se ha creado el primer grupo de asegurados denominado *Blockchain Insurance Industry Initiative* (B3i), con compañías como Aegon, Allianz, Munich Re y Zurich.



Con una cadena de bloques que pudiese gestionar contratos inteligentes, las aseguradoras podrían ahorrarse mucho dinero.

Y no solo ahorrar en costes, sino auto gestionar partes de siniestros con otros contratos inteligentes entidades directamente como pagos, primas de seguros, reclamaciones, peritajes, ofertas, etc...

Estamos estudiando el uso de los contratos inteligentes para agilizar la venta de los reaseguros y la tramitación de reclamaciones.

*Alessandro Spadoni
Zurich*



4.12. Seguridad

La seguridad es una de las características principales que contiene una cadena de bloques, la cual, puede ser desde muy segura hasta técnicamente infranqueable.

El modelo de seguridad de las blockchains se basa en la criptografía y en unos algoritmos matemáticos que certifican su seguridad por su elevado número de posibilidades.

La cadena de bloques bitcoin se considera hoy en día segura, pero hay otras que todavía tienen mayores niveles de seguridad.

No voy a entrar en detalles de que protocolos o algoritmos usan las cadenas de bloques, pero si le voy a decir que son totalmente seguros a nivel de pruebas de fuerza bruta (metodología usada para romper sistemas de seguridad).



No obstante, a más seguridad, mayor tiempo de verificación de dicha seguridad, tenga en cuenta este factor a la hora de implantar o usar una blockchain.

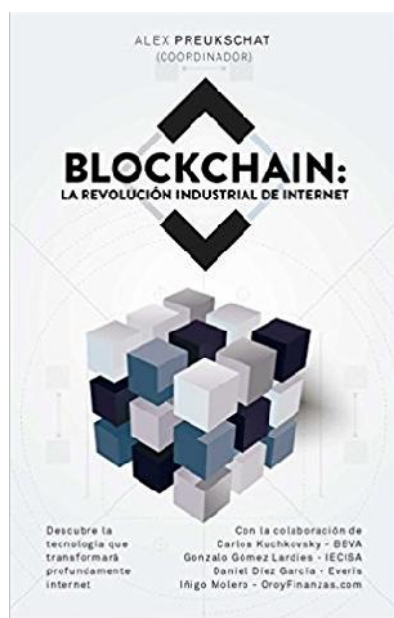
Nada es inquebrantable, los sistemas operativos, cualquier software que use, incluso cerraduras físicas de puertas, tienen “bugs” que se descubren con el tiempo, y no por falta de diseño, si no a veces, por coincidencias o por evolución normal de la potencia tecnológica (consulte el lector en internet como se ha llegado ya a romper la seguridad del protocolo seguro SHA1).

4.13. La imaginación



Vistos estos pocos ejemplos, invito ahora al lector a que desarrolle mentalmente todo lo que realmente podría solucionarse o mejorarse mediante la tecnología blockchain.

Me dejo muchos ejemplos, por ello le invito a revisar el siguiente libro de Alexander Preukschat, el cual, contiene principalmente ejemplos más extensos de tecnología blockchain, explicados por auténticos expertos en la materia:



Blockchain: La revolución industrial de internet

Autor y coordinador:
Alexander Preukschat

<http://libroblockchain.com/>

¿Pero se puede hacer algo más para aplicar o encontrar estas mejoras y soluciones?



Si claro, fíjese, puede escribir un libro como este, por ejemplo, o un artículo, o comentarlo con sus amigos (a esto en nuestro entorno friki le llamamos “evangelizar”), o algo mucho más potente, más interesante:

Podríamos EDUCAR para que la gente entienda, aplique y use la tecnología blockchain.



No es fácil para muchos comprender que la cadena de bloques (Blockchain) llegó para cambiar el mundo, y más allá de lo que podemos imaginar.

Para la mayoría de los países de Latino América la implementación de la cadena de bloques se ha dificultado por múltiples factores, la resistencia al cambio, miedo a lo desconocido o temor de salir de nuestra zona de comodidad, ...y porque muchas entidades bancarias exigen una serie de condiciones que la población no tiene (pobreza, agricultores) y no les permite llegar al gran ciclo que es la economía, sin darnos cuenta que podemos avanzar más eficientemente, eficaz y con un gran nivel de seguridad.

La educación juega un papel fundamental para el entendimiento y comprensión de la cadena de bloques, no es un software malicioso, no representa un peligro para la banca, industrias ni gobiernos, todo lo contrario, la misma se caracteriza porque es ciencia, tecnología e innovación y se puede describir de la siguiente forma:

Ciencia: porque su seguridad criptográfica y forma de trabajar están soportadas en las matemáticas, la cual es verificable.

Tecnología: porque todo este proceso matemático realizado por la cadena de bloques se ejecuta por medio de un Circuito Integrado para Aplicaciones Específicas (ASIC, por sus siglas en inglés) o un equipo (computador) que podemos obtener y armar en nuestra propia casa.

Innovación: porque crea un nuevo concepto en el mundo financiero, distinto a los conceptos del dinero soportado en metales nobles, dinero fiat o fiduciario, en los seguros, en las donaciones, en los contratos, en la veracidad de noticias, identidades digitales, trazabilidad de productos, juegos online y un largo etc. Tal innovación revolucionaria establece la

descentralización del dinero, pero esta nueva creación va más allá de las finanzas y puede formar parte de algo específico o de todo.

Podemos concluir diciendo con toda certeza que la cadena de bloques (Blockchain) puede ser verificada y comprobada porque está fundamentada en la ciencia y en la tecnología (criptografía y matemáticas), sin olvidar que es innovador. Por tal motivo cualquier país lo puede estudiar, desarrollar e implementar en su sistema gubernamental, en la educación, en lo comercial, industrial o salud, no existen límites para el beneficio de los pueblos.

Arit Alexander Rodríguez

Director de "VTEC", Industria Venezolana de Tecnología, C.A.

Capítulo 5,

Mi blockchain

Vistos los ejemplos, puede que ya se le haya ocurrido alguna genial idea de cómo asociar la tecnología blockchain a su empresa, a su día a día, o haya descubierto alguno de los usos y mejoras que todavía nadie conoce.

Perfecto, mi objetivo se ha cumplido, le he hecho pensar, y tranquilo, si no le ha surgido nada todavía no sea impaciente, poco a poco irá viendo parte del futuro.

Pero cuidado, le repito que no todo tiene porqué convertirse en blockchain, algunas cosas ya están bien como están, evalúe con personas experimentadas si realmente está aportando una mejora o una solución, no cometa el error básico de un emprendedor.

Para ello, y para seguir comprendiendo aún más todo, le mostrare dos artículos que, a mi parecer, se redactaron de manera muy amena, de forma muy comprensible, y sobre todo comparados con la vida real:

Mi cadena de bloques, del artículo original de <https://cointelegraph.es/news/mi-cadena-de-bloques/es>

Muchos me han preguntado que es la blockchain (cadena de bloques), su relación con bitcoin y los pagos digitales y, de entre todas las explicaciones que he dado, me quedo con esta:



*Hola, me llamo **Bob** y os voy a presentar a una parte de mi “cadena de bloques”:*

*En la vida real, tengo una familia, cada miembro lo considero un **nodo** que trabaja por separado para formar una única cadena de bloques, a todas horas, todos los días del año.*

También tengo amigos, conocidos, compañeros de trabajo que se comportan también como nodos dentro esta red natural (la vida). Si un nodo se cae, los otros siguen trabajando y le ayudan a volver a estar online.

*No importa la diferencia de potencia que tenga cada nodo, desde el más pequeño **Dave** (6 GHash/años), hasta yo con 39 GHash/años, contribuimos a la red en lo que podemos, añadiendo cada poco tiempo nuevos bloques a nuestra historia de la vida, con hechos buenos y malos, a lo que llamamos “**transacciones**”.*

*Tampoco importa la distancia, mi hermana **Alice** a una esquina de mi casa, mi primo **Charlie** desde Alemania y **Frank** desde Valencia, siempre estamos comunicados entre nosotros, sino de manera inmediata, más tarde, fluyendo la información hasta que todos la conocemos. Recibimos la energía de nodos más fuertes, los padres (mis tíos y mi madre), los cuales desconocemos como gestionan algunas acciones (programadores), simplemente las evaluamos y aceptamos dentro de nuestra red (consenso).*

Transmitimos y mantenemos la red siempre online, para que la cadena de bloques (la familia y la vida) siga creciendo, de manera segura, verificando cada transacción que se realiza y añadiéndola, inmodificables por el tiempo.

*Si las cosas se complican, llamamos a otros nodos de la red para pedir apoyo y verificación de nuestros actos, como amigos y familiares, para que todo siga siempre funcionando con la misma felicidad y exactitud del primer nodo... como cuando mi primo **Chuck** empezó a acepar bloques inválidos y tuvimos que hacer un fork a sus amigos, demasiadas fiestas...*

*Mi padre **Walter**, tuvo problemas técnicos graves de funcionamiento, y ha dejado de añadir bloques nuevos, pero no por ello los demás seguimos manteniendo viva la red, y realizando ahora sus funciones como nodos menos potentes, transmitiendo toda su experiencia pasada en la gran cadena de bloques.*

Mi tía Eva, estuvo haciendo negocios en Japón el otro día, tuvo que buscar una cadena de bloques alternativa para conformar sus contratos, y nosotros desde España, usando unos "colores" le dimos conformidad a sus negociaciones (Ethereum, Smart Contracts, colored coins).

Estos son los últimos bloques minados ayer y añadidos a la cadena de bloques junto con otras muchas transacciones de todos los nodos que componen la red, y hasta hoy éramos pseudoanónimos, encantados de conoceros, bienvenidos a mi cadena de bloques, también la tuya ;)

José Felip Darás
Editor en Cointelegraph España

Y con esta otra, cuando Oscar me pregunto en Territorio Bitcoin:

¿Qué es Bitcoin?



El bitcoin es algo necesario, como moneda complementaria o principal de pago, y como protocolo, es una evolución tecnológica obligada, que conlleva la adaptación del mercado y de las empresas a su metodología y, a los usuarios su uso. (Como los SMS y Whatsapp para Telefónica)

La adaptación a nivel mundial está siendo lenta, y debería de agilizarse y crear formas para llegar a los usuarios, a nivel político, gubernamental y social (Si Coca-Cola incluyese en sus anuncios a un chico comprando una Coca-Cola con bitcoin, veríamos que pronto se pondría de "moda"). Si en vez de aparecer en 2009, hubiese aparecido en 2004, ahora estaríamos todos usando bitcoins como forma principal de pago o alternativa, y los grandes sistemas informáticos estarían basados en tecnología y estructuras descentralizadas, con niveles de seguridad criptográficos más elevados.

Algunas grandes empresas empiezan a meterse, pero más que ayudar, parece que se estén preparando el trozo de pastel que le tocará a cada una. Las startups ligadas a bitcoin reciben mucha financiación, pero pocas están despegando por diversos motivos, uno de los cuales es la falta de conocimiento de los usuarios finales.

Desde Castellón (España), junto con AvalBit (Valencia-España), intentamos llevar a cabo esta metodología de aceleración y adopción, mostrando las cualidades positivas y negativas del bitcoin, y diré que no es tarea fácil. Lo que no sale en la "TV" como publicidad, reportaje o noticia, no le interesa a la gente, aunque le demuestres sus cualidades positivas.

Por todo ello, el bitcoin es, desde mi humilde opinión, el sistema Beta frente al VHS, el Linux contra Windows, la Pepsi a la Coca-Cola, y el tiempo dirá realmente que es bitcoin.

Mientras tanto, yo apuesto positivamente por él.

José Felip Darás

Entrevista en Territorio Bitcoin, por Oscar Domínguez

Con ellos intento ya, de una forma más técnica, que vaya comprendiendo los entresijos que componen la tecnología blockchain, una definición más exacta y algunas funcionalidades.

Definición de Blockchain:



Blockchain es una tecnología que permite interactuar y transmitir valor entre dos o más intervinientes sin necesidad de confianza ni de intermediarios.

Definición de Smart Contracts:

Los Smart Contracts son herramientas que permiten la ejecución automática e independiente de aquellos términos de un contrato que sean objetivables mediante lógica matemática.

Alejandro Gómez de la Cruz,

abogado especializado en blockchain y smart contracts,

Blockchain Lab de Grant Thornton,

fundador y Responsable de Cumplimiento Normativo (CCO) de Octopocket,

Law & Bitcoin, Icofunding.com

Capítulo 6,

Estafas e inversiones

Cuando hablamos del valor de una cadena de bloques, este puede ser muy alto (como hemos visto en mayo de 2017 con bitcoin, alcanzando más de 2900\$ por bitcoin), y con ello y como en la vida real pueden ofrecerle multitud de productos y promesas, historias de gente que se ha hecho rica, con el valor que transmite el token de alguna blockchain.

Cuando algo comienza a despegar, se pone de moda, y empieza a recibir cantidades masivas de gente como modelo de adopción, aparecen las estafas, y en el mundo de las criptomonedas y la blockchain no es una excepción.

Nos lo cuenta Antonio Andrés, en una de las muchas opiniones recibidas:

¡Nos quieren robar!!!

Cada vez que sale una nueva Tecnología como es el caso de Blockchain y que a su vez es factible de general un valor sobre la misma, siempre aparecerán los que nos quieran robar todo lo que puedan y más. Yo mismo he sufrido todo esto en mis propias carnes y es por lo que trato de ayudar a todos para que esquiven a estos impresentables.

Con la llegada de esta apasionante tecnología, también han surgido multitud de timos casi todos desarrollados en internet, ya sean los más sencillos como webs en la que prometen duplicar tus Criptomonedas en 48/72 horas, los que usan un interés simple o incluso compuesto en el que si reinviertes tus "propias ganancias", generas aún más beneficio, las simples web de apuestas y juegos en el que la banca siempre gana y no

olvidarnos de los que pretenden ganar dinero “Minando” usando un software específico o conectando con un “pool” que prometen 0% de comisión e incluso un % por ser de los primeros en registrarse, las webs de inversión prometiendo un % diario, semanal y mensual, las webs que venden equipos de minería nuevos con alto poder de minado y bajo consumo o simplemente una copia de la web original cambiando alguna letra en el dominio y por último los Exchange donde tradear o convertir a FIAT tus Criptodivisas.

*Todos cumplen unos mismos patrones, sitios de nueva creación y uso de “REFERIDOS”. Estos sitios te dan un pequeño porcentaje porque tu traigas a nuevos incautos y lo más seguro es que desaparezcan de la noche a la mañana, y si no lo hacen, el soporte técnico nunca contestara a tus tickets o lo harán con alusiones de que tienen un problema, o les han hackeado o simplemente te mandarán algo al principio para que creas que son de fiar y les envíes más y más criptomonedas. Esto es lo que se llaman un sistema **PONZI** y **SCAM**.*

Una vez que se descubre el timo/engaño, la persona se pone a buscar y escribir en FOROS, o grupos de chat en aplicación de mensajería y tratan de que les ayudes y poniendo mal a toda esta tecnología sin importar lo que le sucediera.

*Por tanto, al igual que uno mismo trata de evitar los robos, ya sea en la calle, en tu casa, procura ser precavido en internet, no des tus datos personales a cualquiera que te los pida, usa los buscadores antes de luego llevarte las manos a la cabeza y mira con cautela lo que te ofrezcan, si es algo con posible beneficio rápido hacia tu persona, algo irá mal en un futuro, y recordar el dicho, **nadie da duros a 4 pesetas**.*

Antonio Andrés
“antuan”

Por ello, voy a intentar enseñarle a diferenciar entre inversiones y estafas en criptomonedas y cadenas de bloque, siempre bajo su responsabilidad de inversión y sin ofrecerle por mi parte ningún tipo de garantía.

6.1. Monedas y tokens

Lo primero que tiene que diferenciar el lector es entre una “moneda” y “token”, ya lo introducimos en el capítulo 3.2. *Tokens, fichas y monedas*:

“Dependiendo del ámbito, tipología y naturaleza de la cadena de bloques que se use, un token puede ser una moneda (o criptomoneda), o puede ser una “ficha” de cambio por dicha moneda”

Vamos a ver si podemos especificar un poquito más:

- Una criptomoneda: es un token con valor (en este caso económico)
- Un Token: es un medio por el que se transmite un valor en concreto (como puede ser también el económico).

En el caso de la cadena bloques bitcoin, está claro que el bitcoin es a su vez una moneda y su token. Pero en la cadena de bloques de Ethereum por ejemplo, existe una diferencia entre estos dos conceptos, ya que, la moneda de valor sería el Ether, y los tokens tiene un uso mucho más limitado, emitido por una empresa privada, institución, grupo, asociación o persona, para conformar un Contrato Inteligente (Smart Contract) o más técnicamente como nos definió Alejandro Gómez de la Cruz *“son herramientas que permiten la ejecución automática e independiente de aquellos términos de un contrato que sean objetivables mediante lógica matemática.”*

Por ello, a lo hora de invertir, debería de tener claro que es lo que está comprando o intercambiando, si una moneda o un token, ya que puede quedarse “sin valor” en cualquier momento, o dispararse a nivel especulativo.

El que compró bitcoins en 2009 y los mantuvo hasta 2017 ha multiplicado por 25000 su inversión...

6.2. El riesgo: ICOs

Visto el concepto de token, vamos a revisar el concepto de ICO (del inglés *Initial Coin Offering*, Oferta inicial de “monedas”)

Antiguamente, si una startup o una empresa necesitaba dinero para crear o ampliar un proyecto, o acudía al banco o a inversores privados para que le prestaran el dinero a cambio de intereses y otros bienes como acciones.

Luego, apareció el concepto de crowdsourcing, en el que se hacía público el proyecto y gente normal y corriente podía apoyarlo con contribuciones económicas bajas, teniendo así cientos o miles de inversores en un proyecto pero cumpliendo la finalidad que buscaba la empresa: conseguir el dinero a muy bajo coste y de manera segura y rápida (el ejemplo más famoso es Kickstarter).

En el universo blockchain ha aparecido una nueva manera de recaudar dinero para proyectos, es hacer ICOs sobre un producto o un proyecto basado en un Contrato Inteligente, el cual intercambia valor por tokens (fichas participativas, que a su vez tiene valor en exchanges, pero no son monedas), todo sobre la cadena de bloques de Ethereum.

(si, puede volver a leer este último párrafo, incluso le invito a que lo haga, lo puede sorprender todo lo que se puede hacer con una cadena de bloques y costarle entenderlo)

Entonces, puede invertir en una startup, que normalmente solo dispone de un “White Paper” (documento que explica la finalidad del producto que van a ofrecer y de la empresa, componentes, cantidad de tokens que van a emitir, y largo etc. de detalles técnicos), de una página web, y de un Smart Contract dentro de la red Ethereum.

Vaya, pues si antiguamente, los bancos ya tenían un determinado riesgo en invertir y financiar empresas o proyectos, los business

angels todavía arriesgaban más, el crowdfunding solo le ofrecía una plataforma web donde enviar el dinero con apenas garantías de éxito del proyecto y legislación dependiente del país o de las cláusulas del creador del proyecto, ahora va a invertir en unas “fichas” cuyo valor depende de muchos factores, la mayoría especulativos, siendo el principal que tenga éxito el proyecto, sino sus “fichas” no van a servir para nada.

Pero bueno, no todas las ICOs, tienen ese elevado riesgo, la cadena de bloques Ethereum empezó así, y ahora es una red fuerte, pero nadie le quita el factor riesgo asumido por sus inversores.

Lo que quiero decir, es que hay proyectos muy interesantes, y algunos como en la vida real, sin fundamento ninguno o futuro, pero que especulativamente, consiguen un alto valor.

Usted es quien asume el riesgo.

“Las nuevas tecnologías, traen maravillosas aplicaciones, pero también nuevos delitos. El invento del dinero de papel trajo los atracos y robos, pero otras enormes ventajas. Lo importante es entender las nuevas tecnologías y protegerse contra los nuevos riesgos y delitos.”

Alfredo Blasco,
CEO en LED Y SPA, S.L.,
Fundador de AvalBit

6.3. Pumps and Dumps

En una época fui *trader* (que es aquel que especula con acciones y derivados, y digo especular porque lo de ganar dinero no era mi fuerte, yo simplemente programaba “robots” de código para compraran o vendieran según unas condiciones del mercado).

Fue una época en la que aprendí mucho sobre economía, no obstante, mi fuerte siempre fue la informática, por lo que me alejé de ese mundo tras observar varias características específicas de ese mundo con las que mi moral no se sentía muy tranquila.

Una de ellas es la conocida vulgarmente como el “pump” y el “dump”, que consiste nada más y nada menos que en hacer que algo suba muy rápidamente de valor (pump) o baje muy bruscamente de valor (dump). Estos movimientos de valor tan bruscos hacia que mucha gente ganara dinero o lo perdiese en minutos, y no voy a especificar exactamente como se hacía, pero si uno tiene una gran cantidad de dinero, puede casi llegar a manejar el mercado como quiera.

Esto, está ocurriendo ahora con el valor de moneda de algunas cadenas de bloques y, sobre todo, en tokens referenciados a ICOs.

Por lo que, tenga en cuenta también a la hora de invertir, que puede encontrarse por el camino tanto “pumps” como “dumps”, que por más que le busque explicación o sentido, no lo encontrará, ni podrá justificar tan si quiera con una noticia buena o mala.

Muchas criptomonedas y muchos tokens se han revalorizado x10 en solo una semana, incluso por x1000, y a su vez en un día han perdido casi todo su valor.

Recuerde, usted es quien asume el riesgo.

Capítulo 7,

Legalidad

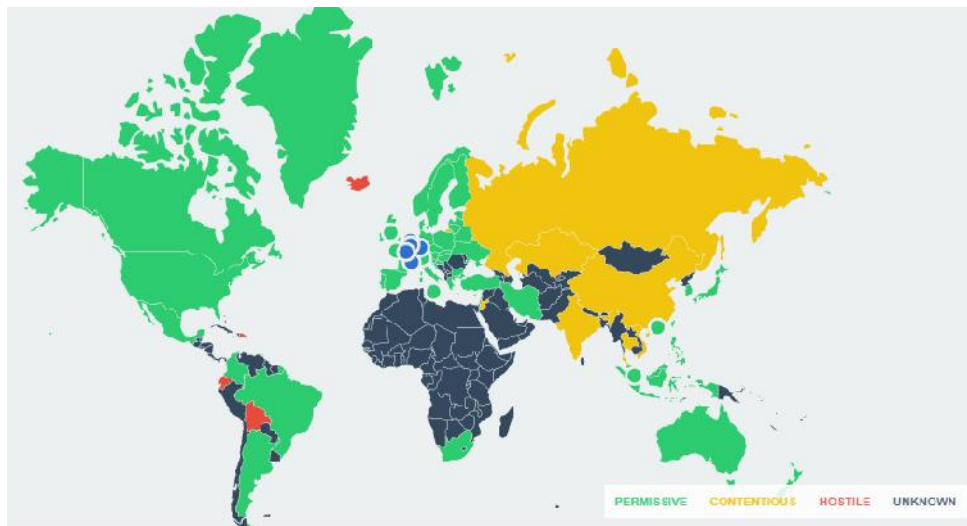
Las cadenas de bloques no necesitan de manera directa una legislación, a no ser que lo que almacenen esté prohibido o legislado por algún motivo.

Cualquiera puede montar una cadena de bloques, tanto pública como privada, sería como montar una base de datos. Pero lo que si necesita legislación y control son el valor que se transmite en la cadena de bloques, su valor económico, su valor de datos personales, su valor catastral, etc...

Y esto es tarea complicada por la estructura descentralizada que tiene una cadena de bloques, algo disperso por el mundo, en miles de nodos replicado y comunicados entre sí.

Cada país está aplicando su propia normativa para cada cadena de bloques y eso les quita por completo muchas de sus principales características. En la siguiente dirección puede ver como se encuentra la legislación ligada principalmente a cadena de bloques de bitcoin (de valor económico): <http://bitlegal.io/> en la que puede comprobar si está permitido, que tipos de impuestos se aplica y la regulación, clasificando cada país en Permitido, Contencioso, Hostil o Desconocido.

...vaya pues, todo al garete, porque si yo aquí en España hago una cadena de bloques pública que solucione un problema, mis amigos de china no sé si podrán aprovecharla....



(fuente: <http://bitlegal.io/> - Junio 2017)

Tampoco es así, ya hemos comentado que los gobiernos están trabajando en devolver la esencia completa a la blockchain, legalizar su usabilidad, su libertad, siempre cumpliendo con la legislación vigente y sin solapar normas. Por ahora diremos eso, que están trabajando en ello.

El lector puede encontrar leyes ya pronunciadas por países en la red, incluso empresas y abogados especializados en valor de monedas y tokens, y gestorías especializadas en tributación de criptomonedas, como por ejemplo:

<http://lawandbitcoin.com/>

<http://bitcoinadvisor.es/>

“Blockchain posibilita un cambio de paradigma, pero necesitamos la participación del regulador”

Luís Pastor,
Consultoría Grant Thornton

Capítulo 8,

“Blockchain Hype Cycle”: Especulación

Se olvida decirle que para usar los tokens o monedas de las cadenas de bloques tiene que adquirirlas, **comprarlas** en este caso, cambiar su dinero real por estas fichas con valor. En 2017 ya es bastante fácil adquirirlas, pero hace unos años la única manera era comprándolas en un exchange o mediante el intercambio persona a persona (localbitcoins).

Volviendo a mi época de trader y metiéndome con los exchanges, le diré que este capítulo voy a sacar mi bola de cristal, al igual que hacen muchos, e intentar adivinar el futuro (de eso se trata la especulación).

No voy a divagar en porque una cosa vale lo que vale, o porque una persona quiere pagar por ella más por ella o menos, o si los mercados se han unido para crear una burbuja, simplemente expondré unos gráficos, los cuales interpretaré a mi manera, luego usted lector, ya pensará en la lógica real o disparará su imaginación más allá de un simple dibujo. Y por supuesto, no asumo ninguna responsabilidad.

6.2. El “valor” de bitcoin

Vimos en el primer capítulo que las blockchains se encontraban supuestamente en la fase 1 de un Hype Cycle.



Pero las monedas, los tokens y las fichas, ¿En qué fase se encuentran?

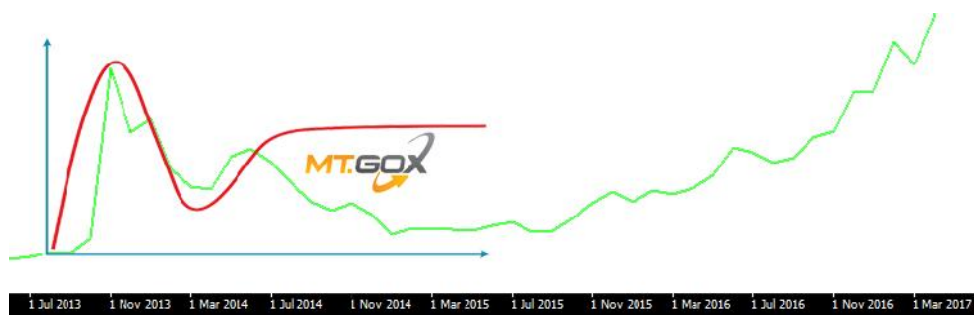
El proceso de maduración y experiencia de una cadena de bloques no tiene porqué ir ligado a su token, la cadena puede llevar un ritmo, y su token (valor) otro muy distinto.

En el caso de bitcoin, vamos a ver su valor económico a lo largo del tiempo y superponerlo en una gráfica de ciclo de sobre expectativa:



Si este gráfico fuese cierto, el bitcoin ya se encontraría en la fase 5.

No obstante, las líneas no tienen por qué coincidir exactas, además en bitcoin en concreto tenemos un hecho bastante relevante que fue la caída del exchange Mt. Gox, por lo que la gráfica se justificaría de la siguiente manera:



Vemos como antes de llegar a la **fase 5**, hubo una caída más “alargada”, y vuelvo a repetir, que las líneas no tienen que ser exactas: *“La altura final de la meseta varía en función de si la tecnología es ampliamente aplicable o sólo beneficia a un nicho de mercado.*

Esto sería mi visión más que optimista de que bitcoin está estabilizado como valor, porque ya se ha aceptado su uso y se está implementando en el mercado.

Pero claro, ahora es cuando su imaginación puede dibujar otras fases si yo le digo, por ejemplo, que el valor máximo de ese gráfico (con máximos dibujados de valor de 2900\$) es 125.000\$; entonces, ¿estaríamos en la **fase 1**? Piense, piense....



Alberto GomezToribio
@gotcalberto

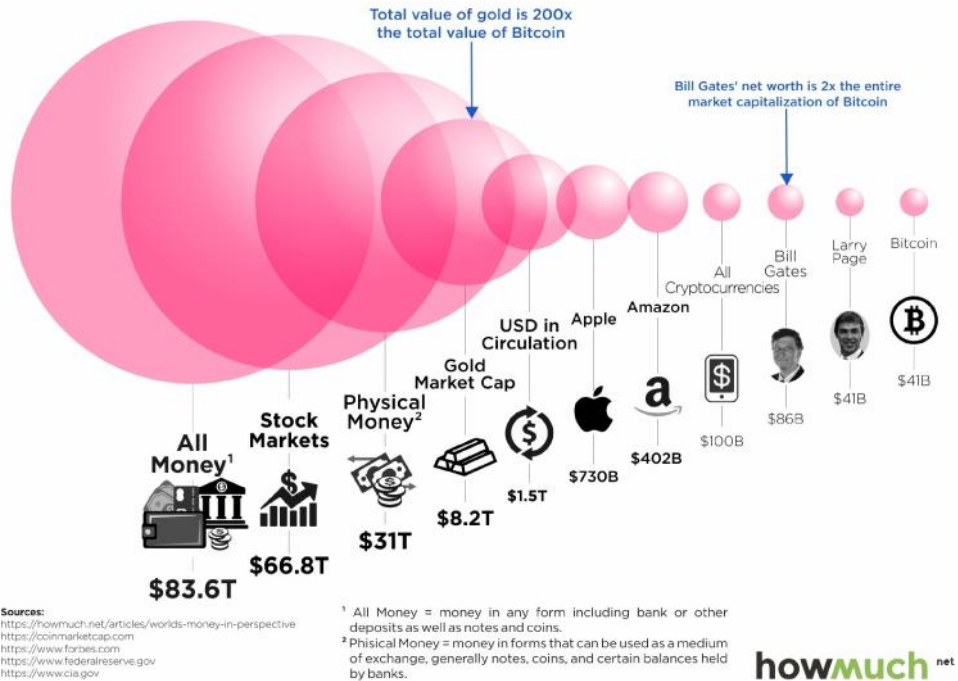
Siguiendo

La capitalización del mercado de Bitcoin esta a punto de alcanzar los 30.000MMS. Más capitalización que más del 70% de las monedas del mundo



Con ese tweet de Alberto Gómez Toribio llegamos al siguiente gráfico:

Putting the World's Money into Perspective



(fuente: <https://howmuch.net/articles/worlds-money-in-perspective>)

Con estos datos, el valor hoy en día de bitcoin es relativamente insignificante a nivel global, a nivel de otros países tal y como explica Alberto no.

Entonces, ¿sabe ya en qué fase estamos? ;)

"Bitcoin es una realidad, y está aquí para quedarse"

Varios autores, personas y empresas citan esta frase, considerada ya de carácter público.

"¿Pero puede el Bitcoin unirse al grupo selecto del verdadero dinero? Solo el tiempo lo dirá."











Diego León Ullauri, gestor de publicidad.

6.2. El “valor” de otras criptomonedas

En base al anterior punto, ahora vamos a ver lo mismo pero para el conjunto de todas las criptomonedas que todavía siguen vivas en el mercado (le puedo decir que se han llegado a ser casi 2000 cadenas de bloques con sus respectivas monedas, quedando ahora unas 800 vivas...y las que se crearán y morirán).

Desde la web <https://coinmarketcap.com/> podemos ver la capitalización de muchas de las monedas, tokens y tokens ICO que tiene las cadenas de bloques.

All Currencies

All ▾	Currencies ▾	Assets ▾	USD ▾		
#	Name	Symbol	Market Cap	Price	Circulating Supply
1	 Bitcoin	BTC	\$45,310,398,702	\$2761.64	16,407,062
2	 Ethereum	ETH	\$31,995,366,409	\$345.05	92,727,829
3	 Ripple	XRP	\$11,746,649,032	\$0.306770	38,291,387,790 *
4	 Litecoin	LTC	\$2,485,722,928	\$48.10	51,681,132
5	 Ethereum Classic	ETC	\$1,980,844,487	\$21.33	92,880,530
6	 NEM	XEM	\$1,775,907,000	\$0.197323	8,999,999,999 *
7	 Dash	DASH	\$1,427,767,592	\$193.47	7,379,864
8	 IOTA	MIOTA	\$1,259,271,754	\$0.453052	2,779,530,283 *
9	 BitShares	BTS	\$863,978,942	\$0.332777	2,596,270,000 *
10	 Stratis	STRAT	\$774,887,345	\$7.87	98,435,767 *

En ella en junio de 2017, nos indicaba una capitalización total de unos 140 millones, frente a los 41 millones solo de bitcoin.

Le va a tocar volver a pensar que significa ese dato y deducir en qué fase se encuentran cada una de esas monedas y cada una de esas cadenas de bloque... mi bola de cristal se acaba de romper. ;)

9. Donaciones en la cadena de bloques

Ya hemos visto cómo se puede transmitir valor a través de la blockchain y, aunque este capítulo estaría dentro de *“que puede hacer una blockchain”*, me va a permitir el lector que se lo muestre de manera independiente debido a su importancia y su relación con fines de carácter benéfico.

Hemos llegado al final del libro, pero antes de terminar, le mostraré como puede y donde puede hacer donaciones para organizaciones benéficas, sin ánimo de lucro u ONGs. ¿Por qué donaciones con criptomonedas y no mediante cuenta bancaria u otro medio tradicional?

Por la transparencia: Su donación se quedará registrada para siempre en la cadena de bloques, demostrando así su colaboración. Además, usted siempre podrá solicitar o ver en la cadena de bloques el uso que se dio a dicha donación.

Por la velocidad: en casos extremos, como desastres naturales, la rapidez es un factor clave en las ayudas humanitarias.

Global: Desde cualquier punto del planeta, a cualquier hora, puede realizar una donación directamente al destino.

Y por muchos otros factores que no voy a repetir y se han abordado en este libro.

Desde la fundación [BitGive](https://bitgivefoundation.org/) (<https://bitgivefoundation.org/>), han creado su propia blockchain (GiveTrack) para gestionar y distribuir entre diferentes asociaciones y ONGs las donaciones que reciben.

Ahora, si lo desea, y quiere contribuir con una donación al esfuerzo de muchos en la elaboración de este libro, no nos envíe nada a nosotros, done a una de las siguientes entidades o, a la que crea conveniente, en criptomonedas, tokens o con “dinero antiguo”: lo necesitan más que nosotros. Muchas gracias.

Jose Felip Darás, “La era de las BLOCK punto COM”

Puede encontrar la lista actualizada en:

<http://bitcoinforcharity.com/>
<https://bitgivefoundation.org/>

Aquí puede revisar de manera transparente las gestiones de las asociaciones y ONGs:

<https://www.charitynavigator.org/>

Generador de códigos QR:

<http://bitcoinqr.com/>

The Water Project

El proyecto del Agua

El Proyecto de Agua se basa en desbloquear el potencial humano, proporcionando proyectos sostenibles de agua a las comunidades en el África subsahariana que sufren innecesariamente de una falta de acceso a agua limpia y saneamiento adecuado. El acceso al agua desbloquea potencial. Elimina los obstáculos que dificultan una comunidad creciente de salir de la pobreza.



dirección bitcoin:

1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R

thewaterproject.com

Omni nano

Omni Nano es una organización de beneficio público dedicada a la educación en la nanotecnología. Nuestro plan de estudios está diseñado para estudiantes de secundaria y universitarios y se centra en las aplicaciones prácticas de la nanotecnología para promover el desarrollo profesional y las oportunidades en la carrera.



dirección bitcoin:

16Sy8mvjyNgCRYS14m1Rtca3UfrFPzz9eJ

<https://omninano.org/>

Outpost seans

El puesto avanzado de Seans es el mayor proveedor de comidas a las personas sin hogar en el condado de Escambia, Florida. Tenemos la distinción única sola en el mundo de ayudar a los sin hogar financiado principalmente por criptomoneda.

“Estamos muy agradecidos por todos los Satoshi que hemos recibido.”



dirección bitcoin:

1M72Sfpbz1BPpXFHz9m3CdqATR44Jvaydd

<http://www.seansoutpost.com/>

Save The Children

Save the Children invierte en la infancia - todos los días - en tiempos de crisis y para nuestro futuro. En los Estados Unidos y en todo el mundo - damos a los niños un comienzo saludable - la oportunidad de aprender y su protección.



dirección bitcoin:

Para donar en bitcoin, debe contactar con la asociación, aunque recuerde que también puede hacerlo por medios tradicionales.

<http://www.savethechildren.org>

Songs Of Love

Las canciones de la Fundación Amor es una organización nacional sin fines de lucro que crea gratuitamente canciones originales personalizadas para animar a los niños y adolescentes que se enfrentan actualmente a desafíos físicos o emocionales médicos difíciles. Cada CD es producido profesionalmente con letras que contengan el nombre y las referencias del niño para todas sus actividades favoritas cosas que las personas y los animales domésticos. Las canciones son escritas e interpretadas en cualquier idioma en el estilo musical que más le gusta al niño por una variedad de profesionales cualificados. Pueden escucharse en [Spotify](https://www.spotify.com).



dirección bitcoin:

1946W6LDsEYF9B5sPYDKfwLw6YBZuHns4L

<https://www.songsoflove.org/>

Free Software Foundation

Sus donaciones nos apoyan como defensores de las libertades y derechos de todos los usuarios de ordenadores, consolidando el proyecto GNU, que certifican la libertad y el, y que luchan contra la práctica de la Gestión Digital de Restricciones (DRM).



dirección bitcoin:

1PC9aZC4hNX2rmmrt7uHTfYAS3hRbph4UN

dirección litecoin:

LPttYC3GoXNrBqGfLT7tTbNHm8SiUpBwYz

<https://my.fsf.org/donate/>

Watsi

Watsi es una plataforma de crowdfunding global para la salud que permite a cualquier persona donar tan poco como 5\$ para financiar directamente la atención médica que cambia la vida de las personas necesitadas. El 100% de cada donación financia la atención médica.



dirección bitcoin:

1PA5oKQGBRigFDY6fB2WgQTtQJNzFyTDr

<https://watsi.org/>

Proyecto Tor

La red Tor es un grupo de servidores voluntarios que permite a las personas mejorar su privacidad y seguridad en Internet. Los usuarios de Tor emplean esta red mediante la conexión a través de una serie de túneles virtuales en lugar de hacer una conexión directa, lo que permite a las organizaciones y a los individuos compartir información a través de redes públicas sin comprometer su privacidad.



dirección bitcoin:

1NgiUwkhYVYMy3eoMC9dHcvdHejGxcuaWm

<https://www.torproject.org/>

AntiWar

Antiwar.com es la principal fuente de noticias contra la guerra y análisis en todo el imperio estadounidense. Desde 1995 ha sido el sitio de noticias de los últimos planes y maquinaciones del partido de la guerra. Nosotros hemos expuesto sus mentiras una y otra vez, movilizando a nuestros lectores en todo el mundo a luchar por la paz.



dirección bitcoin:

1M87hiTAa49enJKVeT9gzLjYmJoYh9V98

<http://www.antiwar.com/>

TunaPanda

El Instituto Tunapanda hace el entrenamiento de la habilidad profesional en la era digital en lugares de bajos ingresos de África oriental. La organización se centra en habilidades como el diseño web y la programación informática, y edición de vídeo que pueden ayudar a las personas obtener un ingreso, a mejorar sus comunidades y participar en el sentido auto-expresión. Despliegan redes informáticas de software de código abierto y (Libre) de contenido de vídeo libre educativo.



dirección bitcoin:

1CU5YgiquupDw6UeXEyA9VEBH34R7fZ19b

<http://www.tunapanda.org/>

Chicago Wish

Wish Chicago es la fundación que concede deseos en el área de Chicago dedicada a animar las familias con la esperanza y la alegría por la concesión de los deseos de los niños y adultos jóvenes locales - desde el nacimiento hasta los 20 años - que han sido diagnosticados con enfermedades que amenazan la vida. Están incondicionalmente comprometidos con la creación de recuerdos especiales a través de los niños que conectan con los corazones tiernos y donaciones de individuos y patrocinadores corporativos en la comunidad de Chicago.



dirección bitcoin:

16DEzKc9fX4XfgGzEvQUJmoYeUrbRNXqxe

<http://www.aswchicago.org/bitcoin-donation/>

Run2Rescue

Ejecutar 2 Rescate es una organización cristiana sin fines de lucro dedicada a la restauración de las víctimas de tráfico sexual.



dirección bitcoin:

1AS3TiTqgJZK6CfNfqcbPXSx4PTFvfghvF

<http://run2rescue.com/bitcoin.html>

y muchas, muchas organizaciones más que ya aceptan donaciones con bitcoins y otras criptomonedas, como la ONU que envía ethers (Ethereum) a sus colaboradores, como **Wikipedia** (Enciclopedia libre de Internet), partidos políticos, empresas como Starbucks, usuarios de compra venta de segunda mano, y un largo etc.

Le invito a que pregunte si aceptan bitcoin o mediante otra criptomoneda allí donde desee pagar alguna compra o servicio, fíjese además, si encuentra una pegatina como estas en el establecimiento:



Capítulo 10,

Las opiniones

A lo largo este pequeño libro, se ha ido encontrando enmarcado en cuadros, opiniones diversas de diferentes personas que han querido colaborar de manera desinteresada.

Agradecer a todos ellos su aporte, ya que ha sido muy importante tanto para mí como creo si no me equivoco, para usted querido lector.

He ido posicionando entre página y página algunas, pero la verdad, es que han sido muchas las recibidas, por ello quiero, aunque no estén en contexto, se aprecien de igual manera, porque son todas igual de importantes por su contenido.

En especial, quiero agradecer a Oscar Domínguez, la recopilación espectacular de opiniones recibidas de gente que ha pasado por su página web Territoriobitcoin.com, con las cuales empezamos:

Cuando en septiembre de 2014 por casualidad leí en prensa un artículo que hablaba de Bitcoin, nunca pensé que me iba a involucrar tanto en algo tan extraño. Pasé más de 14 horas diarias intentando descifrar que era ya no solo Bitcoin, sino Blockchain, palabra que ahora está en boca de todos.

En noviembre de ese mismo año y sin apenas conocimientos decidí aventurarme en un proyecto (Territorio Bitcoin) que serviría para divulgar sobre estas tecnologías a la par que me ayudaba a aprender y conocer la opinión de otras muchas personas.

Hoy mi experiencia se la debo a todas las personas que de una manera u otra hacen día a día Territorio Bitcoin. Aprovecho esta ocasión para rendirles un pequeño homenaje con las frases que ellos mismos nos transmitieron en su día.

Mientras que Víctor García Pastor asegura que Bitcoin debería ser algo del día a día “Queremos que el Bitcoin no sea tan frío, sino que sea algo del día a día”, Ofir Beigel apunta a las reglas de Bitcoin “Bitcoin se rige por un conjunto de reglas que ninguna persona puede doblar” Ramón Quesada y Gonzalo Borrás opinan lo importante de mantener una buena base para toda asociación “La base de avalBit son la gente, la filosofía y los principios”

Josep Rovira, Nuria Calzada y Fernando Caudevilla eligen Bitcoin por sus características “Bitcoin por sus características y anonimato es un medio de pago adecuado para nuestro servicio”

Para Adrián Grau los videojuegos van de la mano de Bitcoin “Ha llegado el momento de Bitcoin al sector de los videojuegos” mientras que Thomas Bertani hace hincapié en el experimento social que supone esta tecnología distribuida “Bitcoin es la red más grande distribuida en el mundo, un experimento social, una tecnología revolucionaria” Asumin Richmond y Sika Boatening expusieron las virtudes de Bitcoin y Blockchain para las poblaciones marginales “Bitcoin y Blockchain podrían ayudar a la población marginal de África”

Nacho Artax y Javi Andreu quisieron dejar claro la revelación que supone “Bitcoin y Blockchain, toda una revelación. Un medio de pago mundial, inmediato y sin comisiones”

Los juristas Fernando Ramos y Pablo Fernández Burgueño expertos y especialistas opinan que “La unión europea no se ha posicionado. Considera que Bitcoin no es ni dinero electrónico ni un medio de pago” y que “España está impulsando un marco de legalidad absoluta para Bitcoin y otras criptomonedas” respectivamente.

Alejandro de La Torre emprendedor ve en Blockchain una zona ideal “Bitcoin y Blockchain una zona ideal para emprendedores creativos donde pueden ver desarrollar sus ideas” mientras que Matías Bari apunta a la forma de entender las finanzas “Bitcoin es una tecnología que está cambiando la forma de entender las finanzas, el dinero y los pagos online”

José Luis Várez busca dar soluciones siempre por adelantado "AvatarBTC busca dar soluciones o alternativas que la gente se planteará cuando llegue alguien de fuera de España" y Alex Preuskchat participa en la economía descentralizada "BlockLift, es el instrumento que hemos creado para participar en la economía descentralizada"

Miguel Ortuño y Jaime Sánchez siempre preocupados en facilitar el acceso a Bitcoin opinan "Queremos ser la empresa número uno mundial en cajeros automáticos de Bitcoin" y "Hacemos que la complejidad de comprar o vender Bitcoin se reduzca a la facilidad de estar hablando con un amigo"

Mientras que Tatiana Moroz encuentra la inspiración "Encuentro la inspiración creativa en el poder de Bitcoin y otras criptomonedas" Covertress desde el punto de vista de una desarrolladora considera que "El mercado de las criptomonedas seguirá perfeccionándose a través de nuevos usos del mundo real y las nuevas tecnologías"

Radoslav Albretch apunta una de las virtudes de los sistemas P2P y de qué manera pueden ayudar a emprendedores "Los préstamos P2P son, sin duda, la mejor manera para que emprendedores y pequeñas empresas obtengan la financiación que necesitan para crecer" Joshua Scigala por su lado muestra la transparencia manteniendo la privacidad "Quiero mostrar al mundo lo extremadamente transparente que un Exchange puede ser manteniendo la privacidad de los usuarios"

Para David Albela y José Basalo su objetivo se basa en transparencia, seguridad y legalidad "Nuestro objetivo, una empresa enfocada en la transparencia, la seguridad y la legalidad en todo momento" Carlos Zehr apuesta por un negocio tradicional y transparente "Hemos apostado en nuestro modelo de negocio por una plataforma transparente y tradicional"

Javier González Granado, desde el punto de vista notarial afirma que "Blockchain no va a acabar con el notariado. Es un instrumento

que tenemos que poner a nuestro servicio” Daniel Lipshitz por el contrario piensa que “Bitcoin no se trata de tecnología, sino de dinero”

Gracias a esta tecnología y al igual que veíamos que puede ayudar a las poblaciones marginales, en la India está ayudando a su crecimiento económico según Akash Gaurav “La economía de la India sigue estando entre las economías de más rápido crecimiento del mundo” Estas son solo algunas de las frases que definen estas tecnologías disruptivas, como podéis ver cada uno tiene su propia opinión.

Para mi Blockchain no tiene fronteras tal y como la imaginación. Blockchain puede ser cualquier cosa que imagines.

Oscar Domínguez,
CEO & Founder Territorio Bitcoin

La Blockchain entró en mi vida una tarde de principios 2016 de manos del Bitcoin. Por años, los conceptos que rodean estas palabras me rodeaban a mí por mis amigos, conocidos y compañeros de trabajo. Pero fue esa tarde cuando por fin me atreví a preguntar en un programa de radio al que llamamos "Bitcoin desde Cero" los invitados: José Felip y Ramón Quesada. Los conductores, Enric Martí y yo.

Cada cuatro palabras debía interrumpir y preguntar "Minería", "Blockchain", "Altcoins", "Bitcoin" y otros términos me resultaron algo chinoscos. Mas debo reconocer la paciencia de mis dos invitados que respondían con paciencia infinita. Esa misma tarde Ramón me invitó a escribir en Cointelegraph, lo cual me pareció una locura, pero acepté. Y escribiendo, preguntando, respondiendo, fue como me di cuenta de lo más importante de la Blockchain: La Blockchain no es solo una tecnología, es una forma de vida.

De pronto me convertí en receptáculo de palabras, números, anglicismos, acrónimos sin sentido. Pero siempre he encontrado a alguien que me desvele un concepto, un simple concepto que decodifique todo lo demás y es así como se cierra un bloque...y comienza otro, siempre un poco más complejo. En toda esta aventura he podido entrevistar a escritores, desarrolladores, mineros, abogados, técnicos, empresarios y todos tienen algo en común: Su generosidad al ayudarme a cerrar el bloque que tocaba, seguramente, porque cuando elijen vivir en el lado blockchain "alguien" ya ha sido generoso con ellos.

Pero así se avanza en una comunidad o en la vida propia, yo ayudo a otros para que decodifiquen sus propios bloques explicándoles de redes sociales o simplemente como se utiliza un móvil. Lo importante es ser generoso y autentico.

Y si, existen diferentes Blockchain en el mundo de las cripto, como en mi propia vida, sin embargo, tengo y tenemos la posibilidad de elegir nuestras cadenas, nuestros bloques y yo siempre busco aquella de la que me hablaron en un principio, esa con identidad de libertad, cooperación y descentralización. Por lo que me alejo del Bitcoin y acerco a la blockchain.

Daniela Caro,
redactora en Cointelegraph España

“Desde que me inicié en esta emocionante tecnología descentralizada allá a finales del año 2012 vi por primera vez cómo cambiaría nuestra forma de vivir y nuestra forma de trabajar. La minería al principio se realizaba desde cualquier ordenador equipado con un mínimo de prestaciones que irían poco a poco descifrando los bloques Bitcoin de la cadena de bloques “blockchain” y premiando con bitcoins. Pasado unos años la dificultad de descifrar los bloques subió y tuvimos que usar las comúnmente tarjetas gráficas o “GPUs”, pudiendo estas calcular más rápido y mejor. Todo parecía ir bien hasta que empezó a popularizarse esta manera de transferir fondos punto-punto y notemos que ya tenía muchos adeptos y empezaba a verse el potencial de los tremendos cálculos generados por miles de computadoras trabajando y descifrando bloques. Principalmente los Geeks o conocedores de Bitcoin usaban esta tecnología como prueba de que realmente no necesitamos la confianza de otra persona o fiarnos de tal para transferir fondos, sino que esta confianza se basa en la cadena de bloques y potencia de cálculo, es así como la red crece y la confianza no la dejamos en manos de sólo unos cuantos.

Problemas resueltos y ganando confianza hemos llegado a un punto que la minería se ha vuelto tan complicada y la dificultad para calcular los bloques está subiendo que tenemos que echar mano de los últimos chips especializados y dedicados solamente a minería digital. Este es el punto de que ya no hay vuelta atrás, es tal la potencia mundial que ya de largo se supera al pentágono y otras instituciones gigantescas. El ser “Minero Digital” conlleva a construir máquinas capaces de llenar salas, naves incluso fábricas, dedicadas a ir descifrando y generando nuevos bloques y apoyando la red Bitcoin. Para mi pensar, pronto veremos máquinas más potentes que transformarán la vida y la manera de trabajar de muchos jóvenes que hoy en día no tienen manera de introducirse en una economía que todavía vive del siglo pasado.

Creo firmemente que muchas personas se beneficiarán y mejorará su vida con esta tecnología libre y descentralizada pudiendo crear trabajos menos sacrificados y más dedicados a la familia o a otras actividades. Actualmente la manera de trabajar está obsoleta y antigua, todavía no se regula eficientemente ningún gobierno. Las ventajas en la vida usando Blockchain son infinitas y mejor distribuidas. La minería digital sigue siendo necesaria para apoyar a todos los proyectos basados en esta tecnología, incluso creando nodos y dejando una computadora con la cartera de una moneda en abierto, podemos confiar en que nuestras transacciones no se vean afectadas por problemas de confianza de terceros. El futuro es hoy y es nuestro.”

Jordi Carrera, “minero digital”

Todos sabemos cómo empieza la película de “El Hobbit: Un viaje inesperado”. Bilbo un hobbit normal, con una vida corriente y aunque con antepasados gloriosos, lleva una existencia plácida y tranquila, y no gusta demasiado de sobresaltos. La llegada de los enanos a su casa a instancias de Gandalf, supone un giro en su vida, que hace que tenga que abandonar su plácido hogar y ponerse en camino para ayudar a la compañía de enanos en su lucha contra el malvado Smaug.

Lo que en un principio parece una secuencia de casualidades sin mayores consecuencias, iniciadas con el deseo de vencer al malvado dragón y recuperar el reino perdido, hace que ocurran por el camino una serie de hechos, que demuestran que el pretexto inicial, era solamente el punto de partida de una historia mucho mayor y que tiene su continuación con Frodo, en “El Señor de los Anillos”.

La moraleja que sacamos de estas obras maestras de Tolkien es que nada sucede por casualidad y todo de un modo u otro, sigue un plan precisamente trazado que, aunque escapa a nuestra comprensión inicial, no por eso deja de existir y estar fina y sutilmente definido. Destino lo llaman muchos a esto.

¿Qué tiene todo esto que ver con la Blockchain? Mucho me temo. Hace unos años, un desconocido Satoshi Nakamoto publicó en un foro ciberpunk el manifiesto fundacional de Bitcoin. Durante un tiempo, pasó desapercibido para muchos, yo soy uno de ellos, porque aunque incluso nos acercamos a él y llegamos a leerlo y vimos que era algo muy interesante, al igual que Bilbo en “El Hobbit”, llevábamos una vida plácida y tranquila que no estábamos dispuestos a dejar de lado. Los fundamentos de Bitcoin, aunque sólidos, presentaban a este humilde lector, unas barreras de entrada tan enormes y un cambio tan disruptivo no solo para el modelo de medios de pagos dominante, sino para el sistema económico mundial, que directamente lo dejé apartado en el mundo de las entelequias, otra gran idea que nunca llegaría a materializarse en la realidad, o quedaría como vaporware, ese software que parece se está desarrollando pero que nunca nadie llega a ver realmente.

Sin embargo, me equivoqué, y Nakamoto fue capaz de movilizar a una pequeña comunidad para que se pusieran en marcha, no sólo desarrollando

el cliente original, sino creando el germen de algo muchísimo mayor. Ideado como un sistema para resolver el problema del doble gasto en un entorno inseguro y entre actores que no confían entre ellos, la idea de la cadena de bloques y la prueba de trabajo, emergía como una solución a un problema hasta la fecha irresoluble. Satoshi había derrotado a Smaug y se alzaba como una opción real y alternativa para dinamizar los flujos de dinero tal y como estaban definidos.

Pero, la cadena de bloques es mucho más, y al igual que sucede en las novelas de Tolkien, nada sucede por casualidad. Gandalf lo sabía y por eso mandó a los enanos a casa de Bilbo, y Satoshi estoy seguro que también lo sabía. La Caja de Pandora se había abierto y ya nada podría ser lo mismo, porque la revolución de la Blockchain aunque había comenzado con uno de los elementos más importante, la eliminación del secuestro de la Entidad Moneda por parte de los Estados, permitía a partir de ahora, crear un nuevo abanico de aplicaciones y servicios, que es capaz de cambiar el funcionamiento de la Sociedad desde sus cimientos más básicos. Yo creo que en la mente de Satoshi estaba esto como objetivo, no solo conseguir que la moneda fuera libre, sino conseguir por primera vez en toda nuestra Historia, que seamos las propias personas las que se encuentren anonimizadas completamente, que sean libres y puedan relacionarse sin estar secuestradas por ninguna clase de Estado o Nación, y hacer realidad el Manifiesto Criptoanarquista de Timothy C. May.

Puedo que todo esto solo sea una ida de olla mía, pero al igual que Gollum con el Anillo, al ver la Blockchain solamente puedo decir “miiiiii tesssssooorrrrooooo”.

Artículo en LinkedIn.

Santiago Márquez Solís,
CEO & Founder z-games ltd,
Bitcoin and Blockchain Specialist

El internet del valor

La apuesta de futuro de los inversores en criptomonedas o tokens de protocolos abiertos descentralizados es la confianza en que puedan disrumpir el actual modelo de negocio de las empresas establecidas del Internet de la Información o en la forma de operar de otras muchas industrias asentadas.

El reparto de valor, en este contexto, hace referencia a la figura que se va a llevar el beneficio en esta nueva estructura económica descentralizada. En el actual Internet de la Información ha sido la capa de aplicaciones -y empresas como Google, Facebook o Twitter, entre otras-, la que ha logrado crear valor, comercializando los datos de sus usuarios, a expensas de los protocolos que han permitido su nacimiento y desarrollo (como son TCP/IP, HTTP, SMTP). En muchos casos estas empresas eran de los pocos que tenían los recursos para innovar en la capa de protocolos, destinando parte de sus abultados beneficios a esta financiación.

Sin embargo, ahora, la apuesta de algunas grandes empresas de capital riesgo -como Union Square Ventures (USV) en EEUU que ya invirtieron en las grandes empresas de tecnología de éxito como Google-, es que en la nueva economía descentralizada podrían ser los protocolos los principales ganadores, tal y como explica Joel Monegro.

La apuesta es que en una economía descentralizada del Internet del Valor los tokens que permiten utilizar los protocolos abiertos acapararán el valor a expensas de las aplicaciones. Esta previsión toma forma con la expresión “Fat protocols” (Protocolos gordos) vs. “Thin apps” (capas de aplicaciones delgadas) como concepto para explicar la futura redistribución desde la capa de aplicaciones hasta la capa de protocolo.

¿Cómo funciona la economía descentralizada del Internet del Valor con la tecnología Blockchain?

Para que la economía descentralizada del Internet del Valor sea posible han tenido que pasar dos cosas. Por una parte, la creación de la tecnología Blockchain, que es una base de datos descentralizada que no necesita de un administrador central, como son Bitcoin o Ethereum, y el segundo

elemento es la criptomoneda o token criptográfico que hace falta para poder utilizar la Blockchain.

La ventaja de una base de datos abierta al público, descentralizada y pública -accesible a todo el mundo-, es que replica y almacena información de usuarios en una red abierta y descentralizada en vez de hacerlo de forma centralizada, tal como sucede hoy en día en la mayoría de las aplicaciones del Internet de la Información.

Las casas de cambio como aplicaciones del Internet del Valor de la tecnología Blockchain

Esto crea un ecosistema a nivel de aplicaciones mucho más rico, dinámico y competitivo. El ejemplo más gráfico que tenemos de esta situación es la facilidad con la que se puede cambiar de una casa de cambios de bitcoins -o cualquiera otra criptomoneda- a otra. La razón de que eso sea posible, a diferencia del sistema bancario tradicional, es que todas las casas de cambio tienen acceso a la misma información de transacciones y registros en la Blockchain y además de forma gratuita y actualizada.

El mundo de las casas de cambio de criptomonedas podría ser una muestra del futuro, en el que servicios y aplicaciones, que compiten entre ellos, son compatibles al construirse sobre los mismos protocolos, tal y como tuvo lugar en el Internet de la Información. Pero esta vez harán falta tokens para poder utilizar el Internet del Valor, circunstancia que podría provocar una redistribución del valor nueva y original.

Los inversores están acostumbrados a invertir en la capa de aplicaciones porque han aprendido que es ahí donde se concentra el valor, pero el futuro podría ser diferente en un mercado de aplicaciones, en el Internet del Valor, más competitivo, incluso, que en el actual Internet de la Información. Especulación e innovación como parte del Internet del Valor con la Blockchain

Cuando un token o una criptomoneda se revaloriza atrae la atención de curiosos, especuladores, desarrolladores y emprendedores. Al invertir su tiempo o dinero en el protocolo se convierten en accionistas del mismo y lo promueven.

Algunos de esos inversores invierten parte de los beneficios o de sus propios recursos para desarrollar servicios sobre el protocolo porque, en caso de que alguno de estos servicios tenga éxito, hará también que se revaloricen sus criptomonedas. Algunos de esos servicios tendrán éxito y atraerán más inversiones.

En fases más avanzadas, como la actual, los inversores de capital riesgo o inversores institucionales también empiezan a invertir en redes descentralizadas, lo que a su vez eleva el interés y curiosidad de más desarrolladores, inversores y emprendedores.

La especulación -palabra que en muchas ocasiones tiene connotaciones negativas en la sociedad, - es la que hace posible todo este ciclo virtuoso de innovación tecnológica, además de generar liquidez en el mercado. El protocolo Bitcoin y la mayoría de protocolos serios de éxito intentan mantener la emisión de nuevas criptomonedas previsible y limitada para recompensar a sus inversores iniciales y a veces la demanda y las expectativas de futuro son tan grandes que los precios se disparan como en una gran burbuja financiera.

En ese sentido el ciclo de especulación frenética y explosión de burbujas en el mundo de las criptomonedas y los protocolos descentralizados puede ser considerado un aspecto positivo para fomentar la innovación.

Lo interesante es que cuando empiezan a nacer aplicaciones de éxito se atraen nuevos usuarios al protocolo y los inversores que ya tomaron posiciones las mantienen a la espera de revalorizaciones de sus participaciones en forma de tokens o criptomonedas, reduciendo así la oferta de criptomonedas. El efecto es que el aumento de la capitalización de mercado del protocolo (número de criptomonedas emitidas x el precio de mercado por unidad) atrae a nuevos inversores y desarrolladores.

USV defiende que el efecto es la redistribución del valor en el Internet del Valor. Si se cumple esta previsión la capitalización de un protocolo crece más rápido que todas las aplicaciones juntas que hacen uso del protocolo, ya que el éxito de las aplicaciones acelera la popularidad del protocolo y fomenta la competencia en la capa de aplicaciones.

El resultado es un mercado altamente competitivo de aplicaciones en el que el valor podría concentrarse en la capa de protocolo. Así podrían convertirse los protocolos en acaparadores gordos del valor y las aplicaciones en víctimas de este hecho, porque comparten todas la misma base -hiper competitiva- pudiendo beneficiarse quizás de una parte más pequeña del valor en el futuro.

La apuesta es que de estas nuevas estructuras económicas nacerán las futuras “empresas”, basadas en protocolos, con un potencial económico como las grandes compañías que operan en el Internet de la Información. Una de las diferencias importantes es que todos podremos invertir o especular desde el principio en ese nuevo ecosistema, a diferencia el Internet de la Información que lo limitaba a los grandes inversores institucionales hasta la salida a bolsa.

Una de las acciones de USV y Andreessen Horowitz derivado de este pensamiento ha sido invertir 10 millones de dólares en un fondo especializado únicamente en criptomonedas para participar en el ecosistema de los protocolos gordos.

Por otra parte, USV ha sido de los más activos invirtiendo en protocolos que operan encima de Bitcoin o Ethereum con nuevas funcionalidades como Blockstack (para crear un Internet más descentralizado y renovado), Mediachain (para etiquetar activos digitales como fotografías en Internet) o OB1 (que desarrolla en protocolo Open Bazaar para crear un protocolo de comercio electrónico descentralizado).

Artículo en Oro y Finanzas

Alex Preukschat,
autor de #libroblockchain

Blockchain es una gran área de concentración debido al potencial que la tecnología ofrece. Para nosotros, las áreas más importantes son SWIFT, manejo de activos y manejo de identidad. Hemos construido algunos prototipos, hecho demos, y estamos en el proceso de implementar algunos casos de uso interno para nuestros clientes.

(entrevista 12 Septiembre 2016)

K.R. Sanjiv,

Jefe de Tecnología de la Información de Wipro

“Blockchain permitirá a Pymes locales fabricar productos únicos a precios competitivos”

Artículo en Criptonoticias

Oscar Lage Serrano,

responsable de ciberseguridad en TecNALIA

“Creo que nuestra opinión sobre el mercado ha cambiado en la Reserva Federal. Diría que es notorio que en la sabiduría popular se maneja que ahora, probablemente, es esa contabilidad distribuida, y la tecnología debajo de ella, mucho más interesante y potencial de lo que es bitcoin actualmente.”

Neel Kashkari,

Presidente del Banco de la Reserva Federal en Minnesota

“Blockchain permitirá donar a ONGs céntimos de euro de forma instantánea”

Iñigo Molero, *consultor en comunicación.*

El primer sistema de alertas de emergencias validado con Blockchain.

Alertry

Será mejor que empecemos a tomar al sistema de Bitcoin en consideración, ya que nos ofrece una oportunidad para mejorar, entre otras cosas, nuestra economía y nos provee las herramientas necesarias para empezar a tomar el control de nuestra vida, un paso necesario para la evolución de la Consciencia del ser humano.

Javier Martín

“El principal reto del sector eléctrico en el siglo XXI es integrar más energía renovable en la red de manera rentable en un contexto de demanda en gran medida plana o en disminución. La única forma de saber cómo hacerlo es automatizando el lado de la demanda, permitiendo a muchos más participantes en la red. Estamos entusiasmados por el potencial de la tecnología blockchain como un habilitador para realizar esa visión. Blockchain no será el único elemento fundamental de la red del siglo XXI, pero es muy probable que sea un elemento fundamental. También proporciona niveles mucho más altos de ciberseguridad esencialmente de forma gratuita, lo que aborda, como subproducto, una de las principales preocupaciones de los ejecutivos de servicios públicos cuando se trata de recursos energéticos distribuidos.”

Entrevista en Infocoin.net

Hervé Touati,
*director general de RMI (Rocky Mountain Institute)
y presidente de EWF (Energy Web Foundation)*

Sin duda alguna pienso en Blockchain como el genoma del conocimiento, una cadena de ADN que acumulará código y experiencia, y será la génesis de una inteligencia global. Su potencial dista aún de nuestra imaginación.

Sergio Sebastián

Capítulo 11,

Continuará...

Hemos visto la v1.0 de esta recopilación informativa de datos, definiciones, experiencias, opiniones, y de sueños cumplidos, los cuales, seguro que son necesarios modificar, ampliar o incluso corregir, ya que, por ahora, no tenemos “algo” que nos muestre el futuro, y por supuesto, ni somos perfectos ni nuestras palabras son las únicas.

Pretendo que este libro sea solo el inicio de un libro de referencia que este siempre, lo más actualizado posible, y que se actualice de manera colaborativa, descentralizada, aunque siempre bajo mi supervisión.

No he negado a nadie su colaboración, he añadido todos y cada uno de los comentarios, opiniones y experiencias recibidas, sin discriminar si son correctas o no, porque para eso el propio contenido del libro lo verifica o desmiente.

La edición de la versión 1.0 queda cerrada, pero ya está abierta la siguiente edición para seguir recopilando, de manera amena, real y profesional, todo aquello que sea relevante, interesante, innovador, disruptivo y especial en esta nueva era de la transmisión de valor, basada en la tecnología BLOCKCHAIN: la era de las BLOCK punto COM.

*Creo que el libro nunca debería de estar terminado.
Me encanta la idea de un libro que se autoalimente con el aporte
de sus lectores y el consenso del autor
Así serán los libros del futuro.*



Alfredo Blasco,
CEO en LED Y SPA, S.L.,
Fundador de AvalBit

Me he dejado a mucha gente por añadir en el libro y muchas opiniones, algunos por desconocimiento del proyecto, otros por qué todavía no me he cruzado en su camino, la mayoría por falta de tiempo o de momentos de inspiración, pero a todos, tanto los que están en esta primera edición como los que no están, muchas muchísimas GRACIAS.

La blockchain solo es el primer paso hacia la integración de nuestro planeta y de nosotros mismos, con el resto del universo.



Jose Alfonso Hernando Abejón (Valdeande Mágico),
teoría del todo IFotonica.

Un saludo,

Jose Felip Darás

<http://laeradelasblock.com>