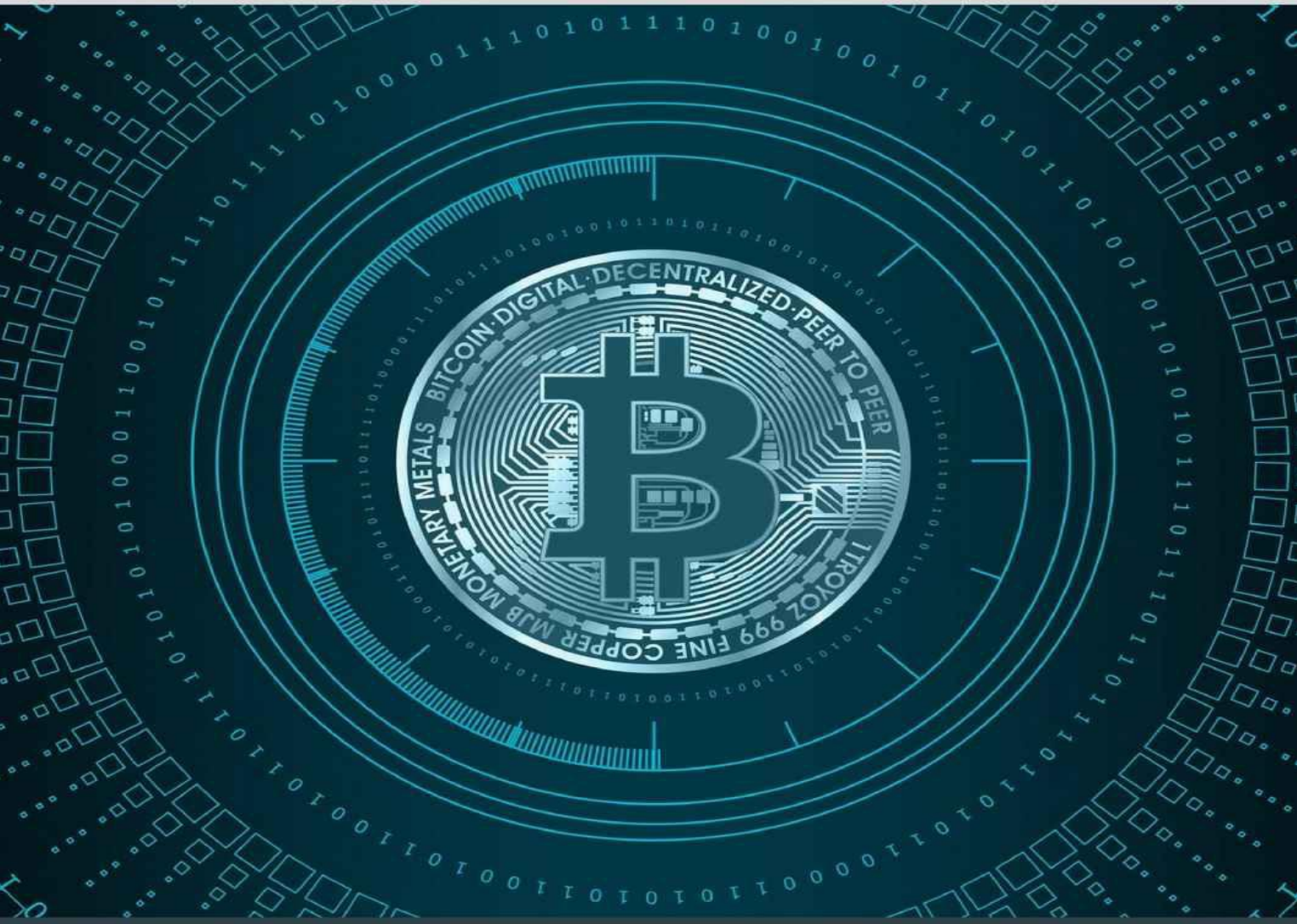
La mayor revolución en Tecnologías de la Información después de Internet

LOS 5 PILARES DEL BITCOIN

UNA INTRODUCCIÓN A LA TECNOLOGÍA BLOCKCHAIN



JOSÉ G. MOISÉS

Los 5 Pilares del Bitcoin: una introducción a la tecnología blockchain.
José G. Moisés

Revisores:
Yazmín Delgado, Edgar Jiménez, Eduardo Lavín, Nataly Moisés, Gustavo Sánchez.

Imagen de Portada:
Pete Linforth (TheDigitalArtist)

Primera Edición Digital.
Publicada el 21 de Octubre de 2018.
Segunda Edición Digital - 1ro de Diciembre de 2018.

Envío de comentarios a:
los5pilares@josemoises.com

Sitio Web complementario:
http://josemoises.com/los5pilares

Software usado para esta edición:
EbookGen 0.7 (Perl), Sigil 0.9.9,
Calibre 3.23, Kindlegen 2.9

Contenido

Prólogo

Se considera que la tecnología blockchain producirá una revolución mundial de dimensiones similares o mayores a la aparición de Internet[1]. La red Bitcoin fue el primer caso de uso global en aplicar esta tecnología, por lo cual su entendimiento es clave para comprender el funcionamiento y las derivaciones que tiene. Este libro tiene como objetivo que puedas adquirir ese conocimiento de una forma rápida y amena sin entrar en los detalles más técnicos.

Durante la evolución histórica de esta

tecnología blockchain, el impulso por parte de los participantes se ha dirigido fuertemente a desarrollar cada vez mejor la plataforma y las herramientas, proveer seguridad, permitir intercambios del dinero digital por dinero fiat, o bien recaudar fondos para continuar haciendo lo anterior. En definitiva, mucha experimentación y mucha acción. Durante ese tiempo, han quedado postergados la capacitación y el buscar medios para facilitar el aprendizaje[2]. La tecnología detrás del Bitcoin es difícil de entender a la primera, y además está impregnada de tabús por situaciones relacionadas con su origen, como el propio Bitcoin y su uso para actividades ilegales.

En este libro podrás encontrar un modelo sencillo de cinco pilares que serán los puntos de partida para comprender una tecnología que es en realidad la suma de muchas tecnologías combinadas adecuadamente para obtener casos de aplicación que antes no existían, entre ellos el dinero digital cuyo ejemplo más conocido es el Bitcoin.

Para leer este libro no requieres entrenamiento técnico: pretende ser entendible para cualquier persona con un nivel de educación preparatoria, bachillerato o superior. Pero también es provisto como una herramienta para los

conocedores del tema que, se enfrenten al dilema de tener que explicar qué es blockchain a sus conocidos, amigos y alumnos en una forma amena.

Formalmente, la **tecnología blockchain** se le denomina DLT, por las siglas en inglés de **Tecnologías de Libro Distribuido**, la cual abarca más que blockchain, ya que pueden usarse otras estructuras diferentes a la cadena de bloques para almacenar los registros. Actualmente la base de conocimiento de las DLTs está en una expansión exponencial. Continuamente se plantean nuevas ideas, formas novedosas de resolver los problemas, se forman comunidades de desarrolladores para

resolver situaciones de maneras impensadas. De hecho, como puede ocurrirte (o te ocurrirá), no es extraño para quien está involucrado en este nuevo mundo cada descubra un término nuevo semana o incluso cada día.

Por lo anterior, es de esperarse que este libro se limite a desarrollar los conceptos más básicos, de una manera informal. Un problema tradicional de la ciencia es que, al pasar de sus modelos formales a lo informal, pueden introducirse errores y confusiones. Hemos tratado de reducirlas al mínimo, buscando priorizar la comprensión general. De todas formas, se incluye al final del libro una forma de reportarnos cualquier error o comentario, que nos

pueda servir para futuras ediciones.
Se identifica a Bitcoin como caso histórico y porque es natural utilizarlo para explicar blockchain, aunque existen muchas otras aplicaciones de las DLTs, pero no se busca favorecer a esta "criptomoneda" sobre otros activos virtuales a través de este libro. Bitcoin es sin duda es el ejemplo más didáctico de blockchain, bastante más simple en sus bases que otras redes blockchain[3].

Mucho menos este libro está pensado para incentivar o desalentar la compra o venta de este u otros activos virtuales, dado que se concentra en la tecnología en sí, no en el valor que un mercado determina dependiendo de una infinidad

de factores. Por el contrario, debes considerar que las operaciones con cualquiera de los activos virtuales implican riesgos, probablemente altos pero seguramente difíciles de estimar "a priori", por lo cual es un factor que debe ser considerado si planea experimentar con su adquisición.

Es probable que si ya tienes experiencia en blockchain identifiques que en este libro que faltó esto o aquello, por eso es importante aclarar que el objetivo no es explicar todo el funcionamiento a detalle, sino por el contrario presentar los elementos mínimos comunes que permitan facilitar la comprensión general de las DLTs.

Aunque para generar el libro se ha tomado como base en una variedad de bibliografía, artículos y contenidos de diferentes fuentes, se ha puesto especial atención en comentar pasajes del artículo inicial de Satoshi Nakamoto, ya que es el fundacional del Bitcoin y el primero que integra las tecnologías base de blockchain. Encontrarás algunos cuadros informativos tienen el título "Citando a Satoshi" justamente porque es un momento oportuno en el libro para repasar algún fragmento de la publicación original[4] de Bitcoin. Eso ayuda a que si luego de leer este libro, vuelves a leer la publicación, entonces podrás comprender mejor muchos de los

conceptos allí vertidos. Probablemente ya me has descubierto, busco una forma motivadora de llevarte a leer la publicación original y no quedarte solo con este libro, ya que solamente es un comienzo.

El libro está organizado en dos partes. En la primera se trata el modelo general de los cinco pilares, donde poco a poco vamos construyendo mentalmente una red blockchain con sus elementos hasta poder comprenderla en forma general.

En la segunda parte se busca responder de una forma simple y partiendo del modelo, a las preguntas frecuentes acerca de las DLTs que surgen en todo

tipo de situaciones: con amigos, en mesas de discusión, foros, etc. Algunas muy evidentes y otras más disparatadas, unas muy simples y otras relativamente complejas de responder. De todas formas, siempre quedarán preguntas pendientes para futuros libros, más aún en una tecnología tan dinámica.

Incluso para personas que conocen sobre temas tecnológicos y de programación, lanzarse a aprender por primera vez sobre la tecnología blockchain es un viaje que lleva mucho tiempo: horas de navegación en Internet saltando de un artículo a otro, revisar una y otra vez conceptos, tratar de encontrar algún sitio donde las cosas se

expliquen en forma más didáctica.

Cuando se buscan noticias de Bitcoin y "criptomonedas" aparecen en Internet infinidad de artículos, muchos con errores, otros usando metáforas que a veces confunden más que ayudan. Recuerdo que, en mi época de estudiante de secundaria, al comenzar en el mundo de la programación, me encontré con un libro sobre el lenguaje de programación Pascal que comenzaba de forma irónica: algo así como "Solamente se puede aprender Pascal, si se sabe Pascal". Así me sentí cuando me fui internando en el mundo de Blockchain. Este libro tiene como objetivo, que se pueda aprender sobre la tecnología blockchain sin que

se tenga que saber previamente... blockchain.

Notas:

[1] - Dado que implica un cambio de paradigma en muchos aspectos, especialmente en temas de seguridad, la tecnología se encuentra aún en fase de maduración, pero ya ha generado soluciones altamente disruptivas. Adicional al universo de las "criptomonedas" algunos ejemplos corporativos de esa disrupción ya existen: Everledger es una compañía que utiliza blockchain para dar trazabilidad de diamantes, la empresa Walmart está usando la tecnología para dar

trazabilidad a la calidad de la comida, el Gobierno de Estonia está incluyendo blockchain en varios de sus programas, haciéndose este país famoso por su identidad digital y la disponibilidad de la residencia digital (e-Residency). IBM e Intel son participantes activos de la Fundación Linux proporcionando plataformas para desarrollos blockchain, y en esa institución bajo el nombre de Hyperledger se incuban diez proyectos diferentes para habilitar masivamente esta tecnología.

[2] - Durante el año 2018 han aumentado considerablemente las ofertas educativas y varias universidades han incorporado programas para el aprendizaje de

blockchain. Además de la Universidad de Nicosia en Chipre que fue la primera en ofrecer un posgrado en criptoactivos, se han incorporado también la Universidad de Princeton, la de Duke y la de California en Berkeley. Adicionalmente varios programas privados.

[3] - Aunque con el tiempo se ha ido modificando incluyendo mayor complejidad.

[4] - La versión original en inglés la puedes encontrar en: https://bitcoin.org/bitcoin.pdf y la traducción al español en https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf

Plan de la obra

El desarrollo de este libro está planeado en tres ediciones, con el objetivo de incluir en cada versión los ajustes dados por la retroalimentación de los lectores. Es una gran ventaja que nos permiten las ediciones digitales. De esta forma el libro va a estar mejorando en calidad y revisión con cada edición. En la siguiente sección comentamos el procedimiento para que pueda obtener una actualización a las diferentes ediciones sin costo adicional.

La versión inicial fue la primera edición, basada en una revisión realizada por un grupo reducido de

colegas. Tiene como base un conjunto de presentaciones preparadas y realizadas durante los años 2016 y 2017 acerca de las DLTs y en particular el caso del Bitcoin, donde explicaba de una forma lo más comprensible posible el funcionamiento de la tecnología, incluyendo las similitudes que tiene con la Facturación Electrónica en México, un área de mi experiencia laboral durante más de diez años. Esto también abre una ventana muy interesante de posibilidades para implementaciones en este país.

La edición que lees es la segunda. Esta edición tiene varias correcciones y ajustes en función de dichos

comentarios. Aunque hemos puesto mucho esfuerzo para evitar cometer errores, el mundo de la cadena de bloques sin duda es de alta complejidad, y la terminología aún no se encuentra totalmente estandarizada. Por lo cual pueden existir casos en los cuales las percepciones o los textos puedan ser expresados mejor de una manera que de otra. Optimizar estas expresiones es lo que buscaremos al generar cada nueva edición.

Adicionalmente, una nueva edición con ajustes se realizará en enero de 2019, que es cuando la red del Bitcoin cumplirá sus 10 años de vida (considerando la fecha en que se generó el bloque génesis). En ese caso

estaremos incluyendo una serie nuevos textos y citas a nivel histórico, considerando los diferentes sucesos que hayan ocurrido durante el cierre del año 2018.

En paralelo a este plan de ediciones digitales a través de Kindle Publishing de Amazon se buscará también generar una versión en forma impresa la cual probablemente coincida con la tercera edición digital lo cual dependerá de lo que se acuerde con las la editora seleccionada para la publicación del libro impreso.

Obtener nuevas ediciones

Debido a que las aplicaciones y dispositivos de Kindle permiten el registro de notas y comentarios, el proceso para actualizar a la nueva edición no es automático. Tampoco tendrás un aviso, debes hacer el proceso manualmente.

La forma más práctica es ingresar a su cuenta de Amazon Kindle, buscar la opción "Mi cuenta" y en ella "Gestionar contenido y dispositivos". Si hay una versión nueva disponible, debajo del título aparecerá un botón naranja con el texto "Actualización disponible", al pulsarlo aparece una advertencia "Se encuentra disponible una versión actualizada de este libro. La versión

actualizada reemplazará la versión anterior." Se requiere pulsar el botón actualizar para contar con la nueva edición.

Para más información sobre las ediciones visitar: https://josemoises.com/los5pilares, donde se incluirá información de referencia y recursos relacionados con el libro. Adicionalmente, si cambiaran los pasos descritos anteriormente por actualizaciones de la plataforma web de Amazon, en esa página estaremos publicando el nuevo procedimiento.

Comentarios u

observaciones

Si tienes comentarios, errores que me quieras reportar u observaciones, escríbeme al siguiente correo electrónico:
los5pilares@josemoises.com
También estaré publicando notas posteriores a la publicación así como herramientas en el sitio:
https://josemoises.com/los5pilares
Debido a que esta es la primer edición, espero contar con comentarios de los lectores para mejorar en lo que sea posible la calidad del libro, siempre recordando que las nuevas ediciones o revisiones las pueden descargar usando el método descrito anteriormente.

Aviso Legal

La información contenida en este libro tiene únicamente propósitos informativos y de educación, promoviendo la reflexión y el análisis.

Ningún contenido de este libro puede considerarse un aviso o recomendación. Toda acción que el lector pretenda tomar en relación a los temas tratados en el contenido, siempre deberá realizarse de manera informada a través de su propia investigación independiente o en su caso obteniendo asesoramiento de profesionales debidamente facultados en las áreas correspondientes, como la legal, la financiera o la fiscal, entre

otras. No utilice este libro para tomar ningún tipo de decisión relacionada con inversión. En ningún caso utilice este libro como su única referencia de información.

La obra tiene foco en el aspecto tecnológico de la red Bitcoin y su funcionamiento como parte de una red de computadoras, y en este sentido el contenido del libro debe tomarse únicamente como un acercamiento a un conocimiento más profundo de estas tecnologías.

El autor y los editores no asumen ningún tipo de responsabilidad derivada de errores u omisiones, o cualquier daño

que pueda resultar del uso aislado o combinado del contenido aquí presentado.

Los sitios web y los paquetes de software citados en este libro deben ser usados con total responsabilidad del lector, ya que el autor no puede garantizar el adecuado mantenimiento del contenido de los mismos.

Las referencias de cualquier tipo que aparecen en este libro en ningún caso significan un respaldo o adhesión a cualquiera de los elementos mencionados, incluyendo personas y organizaciones.

Parte I - Los 5 Pilares del Bitcoin

Introducción

Bitcoin y **blockchain** se confunden frecuentemente, pero no son la misma cosa. Podemos afirmar que nacen juntos en cuanto a caso de aplicación real, aunque las tecnologías sobre las que se basa blockchain son anteriores, y en la creación de la red Bitcoin es cuando se reúnen adecuadamente. De hecho, veremos que la sola palabra Bitcoin se puede referir a tres conceptos diferentes y que además hay "muchos Bitcoins".

Estas confusiones no son casuales, son causadas por la esencia de las DLTs [5]: la descentralización. Es por ello que no encontraremos una entidad central que defina todos estos términos, aunque hay varios consensos generales sobre su significado que son los que exploraremos en este libro.

Pero al menos podemos resaltar sus diferencias: Bitcoin se refiere a una red, una implementación concreta, y blockchain es un conjunto de tecnologías, justamente usadas por Bitcoin. Existen otras redes de blockchain, de hecho tú mismo podrías crear una con relativamente poco

esfuerzo[6].

Una gran barrera para ingresar al mundo blockchain es la dificultad para encontrar por dónde empezar. La mayoría de quienes he conocido han comenzado con noticias publicadas en Internet, un camino escabroso porque está lleno de trampas: noticias escritas por personas no suficientemente informadas, mucha confusión en los propios autores y la existencia de "bandos" a favor y en contra del mundo de las criptomonedas, aunque no se necesite que exista una criptomoneda para que exista una red blockchain.

Justamente una de las esperanzas para

este año y los siguientes, es el desarrollo de un movimiento de formación y educación en el mundo blockchain, incorporándose en universidades y en el entorno corporativo. Ya existen varias iniciativas al respecto, aunque todas ellas bastante recientes. Con este libro se espera contribuir a ese objetivo a través de una explicación más profunda pero no altamente técnica de blockchain.

Por lo anterior, en este libro se presenta un modelo didáctico, ya que aunque es muy común actualmente escuchar sobre Bitcoin y blockchain (parece ser hasta una moda), las explicaciones se limitan a metáforas que finalmente no hablan

mucho de la tecnología que está detrás.

Para fundamentar frases como que "la tecnología blockchain es revolucionaria" o bien que "el valor de algunas de las criptomonedas reside en su tecnología", es necesario que el público en general conozca más sobre el funcionamiento de las DLTs y en particular de las características que las hacen diferentes.

Con Internet ocurrió algo similar, y si bien en un principio estaba reservada únicamente para tecnólogos, hoy otras disciplinas la están usando ampliamente involucrándose también en muchos de los aspectos técnicos. Como ejemplo,

podemos citar el amplio desarrollo del Marketing Digital, donde la terminología es mayormente tecnológica y aunque en la teoría los principios son los mismos del marketing tradicional, en la práctica es una disciplina totalmente nueva.

Incluso, para mi asombro, muchos profesionales de tecnologías de la información y en particular programadores, presentan resistencia para conocer y aprender sobre DLTs, quizás por los elementos que combina, o bien por la dificultad que aparenta tener comenzar a programar en la tecnología.

Esto último es algo paradójico ya que casi la totalidad del código de los

proyectos blockchain es abierto, y visible por todos. En realidad se puede crear una "criptomoneda" a nivel únicamente tecnológico en una tarde solamente bajando ciertos componentes ya hechos. Evidentemente el reto es conceptual.

Bitcoin y la mayoría de las criptomonedas son descentralizadas, esto es que no existe una entidad central a la cual se le pueda exigir algo en relación al funcionamiento de la red.

Veremos que el tema de la descentralización no es algo de blanco y negro, existen escalas de grises, sin embargo al compararlo con las

entidades que han existido en el mundo hasta la actualidad podríamos afirmar que las DLTs, y muy particularmente las que están basadas en prueba de trabajo, proporcionan por primera vez en la historia mecanismos altamente descentralizados para mantener registros y procesar transacciones. La comprensión de esto no vendrá sino hasta revisar el cuarto pilar.

A continuación se presenta en forma breve la historia del Bitcoin, de forma de tener un contexto para conocer más sobre la tecnología blockchain. La extensión sobre el tema será breve: lo suficiente para tener la información necesaria para poder pasar al modelo de

los 5 pilares.

Notas:

[5] - Por las siglas en inglés de "Tecnologías de Libro Distribuido"

[6] - Solamente nos referimos a crear la red y ponerla en funcionamiento. Si estabas pensando en crear tu propia "criptomoneda" y que tenga valor, eso no es tan fácil, y de hecho quizás no sea tampoco conveniente si no va acompañada de una idea muy original.

Origen de la Red Bitcoin

Cuando usamos la palabra "Bitcoin" podemos referirnos a tres cosas:

1. el **Bitcoin** como concepto fundamentado en la publicación de Satoshi Nakamoto de 2008 (en particular, el protocolo que de esa publicación se deriva) al cual nos referimos en mayúscula
2. la **red Bitcoin**, conjunto de nodos que dan vida a lo expresado en la publicación anterior, a la cual una parte de su comunidad aporta computadoras y hardware para

mantener su funcionamiento.

3. la "criptomoneda" que es unidad de medida en las transacciones de la red anterior, que para diferenciarla suele referirse usando su símbolo: **BTC** o bien expresarla en minúscula: "tengo 2 **bitcoins**"

Adicionalmente es relevante comentar que la red de Bitcoin se ha bifurcado varias veces, originando otros pares red-criptomoneda, como Bitcoin Cash, Bitcoin Gold, Bitcoin Diamond, que suelen llamarse componiendo la palabra Bitcoin y alguna palabra adicional para caracterizar sus diferencias con la red

original. En la segunda parte del libro se trata el concepto de las bifurcaciones, pero para comprenderlo primero debes conocer los cinco pilares y los elementos que se desprenden de ellos.

El documento considerado fundacional de Bitcoin es el "libro blanco"[7] publicado en el año 2008 por una persona de nombre Satoshi Nakamoto, cuyo paradero es aún desconocido, y que podría haber sido un grupo de personas. Ese documento tiene solamente nueve páginas, y puede descargarse de Internet.

Se trata de un documento bastante técnico, aunque inicialmente en los

ambientes universitarios simplemente pasó como una investigación más, aparentemente sin relevancia.

Sin embargo, el documento logró reunir una serie de tecnologías que ya existían en el pasado, para proponer un mecanismo que permitiera crear dinero digital. No debe confundirse dinero digital con los medios de pago existentes previamente, como los pagos por tarjeta de crédito, las transacciones electrónicas entre cuentas bancarias o bien el uso de empresas intermediarias como Paypal[8].

Cuando hablamos de dinero digital nos referimos a una clase nueva de activo

con características sobre las cuales podrás profundizar más adelante en este libro, como la resistencia al doble gasto y la independencia de una entidad centralizada.

Al año siguiente a la publicación del documento ya se encontraba funcionando la primer implementación del sistema propuesto, existiendo entonces una pequeña red en la cual se podían transferir los Bitcoins. Desde el punto de vista técnico lo correcto es afirmar que en ese año ocurrió lo que se denomina generación del bloque génesis, que es el primero de una cadena de bloques relacionados que tienen la información de las transacciones. Este

bloque fue creado el 3 de Enero de 2009.

Es generalmente aceptado que una de las razones de la creación del Bitcoin fue la crisis global del año 2008, desencadenada por la crisis inmobiliaria en Estados Unidos de América, sobre la cual se ha documentado la existencia de un sinnúmero de irregularidades y se identificaron fallas en la aplicación adecuada de diferentes regulaciones, resultando en planes de rescate financiero en muchos países debido a la afectación global. La búsqueda de un "dinero independiente" de los gobiernos y las organizaciones tradicionales, donde éstos no pudieran interferir,

resultó en la creación del Bitcoin. Para septiembre del año 2018 existen más de 2000 activos virtuales que presumen tener características similares al Bitcoin[9], cada uno de los cuales podría, utilizando diferentes enfoques, llegar a convertirse en ese nuevo "dinero independiente". Desarrollaremos más sobre estas alternativas en la segunda parte del libro.

Durante un tiempo el Bitcoin fue intercambiado por intangibles, por lo cual no funcionó realmente como dinero en el sentido usual, como poder realizar una compra en algún establecimiento. Fue hasta el año 2010 donde ocurre la

primera compra de un tangible: dos pizzas compradas por un total de 10,000 (diez mil) bitcoins[10]. A partir de allí poco a poco fueron apareciendo lugares donde se permitió la compra de mercadería aceptando bitcoins, eso ocurrió sobre todo en los sitios en línea para aprovechar un nuevo mercado de compradores que ya poseía el activo virtual.

En el año 2012 se crea una organización denominada Bitcoin Foundation para desarrollar más activamente la tecnología y poner de acuerdo a la comunidad creciente. En el año 2013 el precio hace un nuevo pico de más de 250 dólares regresando a 100 dólares a

mediados de año y volviendo a saltar a más de 1,200 dólares en Diciembre. En ese mes un comunicado en China anuncia que el BTC no puede tratarse como moneda en circulación, lo cual desata pánico y vuelve a caer a 500 dólares.

En el año 2014 se produce una crisis adicional, dado que había una única casa de cambio que en todo el mundo que concentraba casi el 70% de las transacciones relacionadas con Bitcoin: Mt. Gox con sede en Japón. Tiene un problema muy serio y cierra sus puertas. Según algunos fue un robo por parte de cibercriminales, según otros una mala administración con gasto desmedido que

no permitía respaldar un precio a la baja. Por esa causa se dan por robados o desaparecidos 850,000 Bitcoins, una gran cantidad de usuarios se queda sin el dinero invertido en el criptoactivo debido a que los registros se encontraban en realidad en la casa de cambio, no en sus billeteras digitales[11].

En los años siguientes se mantiene con cierta estabilidad entre los 400 y 600 dólares, hasta que en 2017 Japón regula los activos virtuales permitiendo su uso como moneda de pago, siendo así el primer país que emite una regulación, eso dispara los precios de la mayor parte de los criptoactivos.

El precio crece durante todo ese año, hasta que en el mes de noviembre el BTC sobrepasa en precio de mercado a los 10,000 dólares americanos, después de subir varias veces, lo cual hizo que tuviera una fuerte repercusión en los medios. Considerando que muchos medios habían previamente anunciado que el Bitcoin ya había muerto, toda la difusión hizo que ya muchos ciudadanos en el mundo, y en particular en Estados Unidos, pasaran a estar muy interesados en comprar criptoactivos, aún sin conocer de qué se trataba.

Es en diciembre de 2017 cuando el aumento del precio del Bitcoin pasa a ser continuo hasta el día 17, alcanzando

un valor de alrededor de 20,000 dólares, pero cayendo fuertemente en los primeros meses del año 2018. Esta situación se suele identificar como una burbuja económica, y algunos señalan su causa en la incorporación al mercado de muchas personas con pocos conocimientos en el tema, únicamente con la esperanza de hacerse ricos al duplicar o triplicar el precio de la moneda. Al momento de escribir este libro, el precio del Bitcoin se encuentra alrededor de los 7,000 dólares.

Notas:

[7] - Del inglés "white paper", manuscrito que presenta una idea o investigación usualmente en ámbitos

académicos

[8] - Estas empresas mantienen registros de pagos, similares a cuentas bancarias, en bases de datos tradicionales. La propuesta de Bitcoin fue algo original y diferente.

[9] - Esta afirmación es discutible y por eso uso la palabra "presumen". Quizás los comparables al Bitcoin en lo tecnológico sean unas pocas decenas. En tamaño de la red y valor teórico de mercado actualmente (2018) ninguno es comparable.

[10] - El programador Laszlo Hanyecz recibió el 22 de Mayo de 2010 dos pizzas de valor 41 dólares americanos, pagando por ellas 10,000 bitcoins.

[11] - Se profundiza sobre este tema en la parte II, ¿Qué es una casa de cambio de Bitcoin?

Los 5 Pilares

¿Qué es blockchain? Si eres alguien que ya está involucrado en el mundo blockchain ¿Cuántas veces te han preguntado que es blockchain y te ha costado explicarlo? Este libro está pensado para permitir dar una explicación algo más profunda que una metáfora, pero sin entrar en las complicaciones altamente técnicas y partiendo del primer caso existente: Bitcoin.

Existen muchas diferentes definiciones de blockchain, que incluso terminan especificando diferentes conceptos, sin

existir una definición estándar[12] hasta el momento. La definición que proporciono aquí se ajusta más al modelo didáctico, para ser su punto de partida, pero otras definiciones pueden ser más amplias (abarcar más casos) o bien más restrictivas

"Un libro distribuido de registros inalterables almacenados en bloques encadenados que incluyen transacciones firmadas digitalmente, cumpliendo un conjunto de reglas de consenso distribuido y asegurando su funcionamiento en un código [abierto] común."

La definición reúne los siguientes

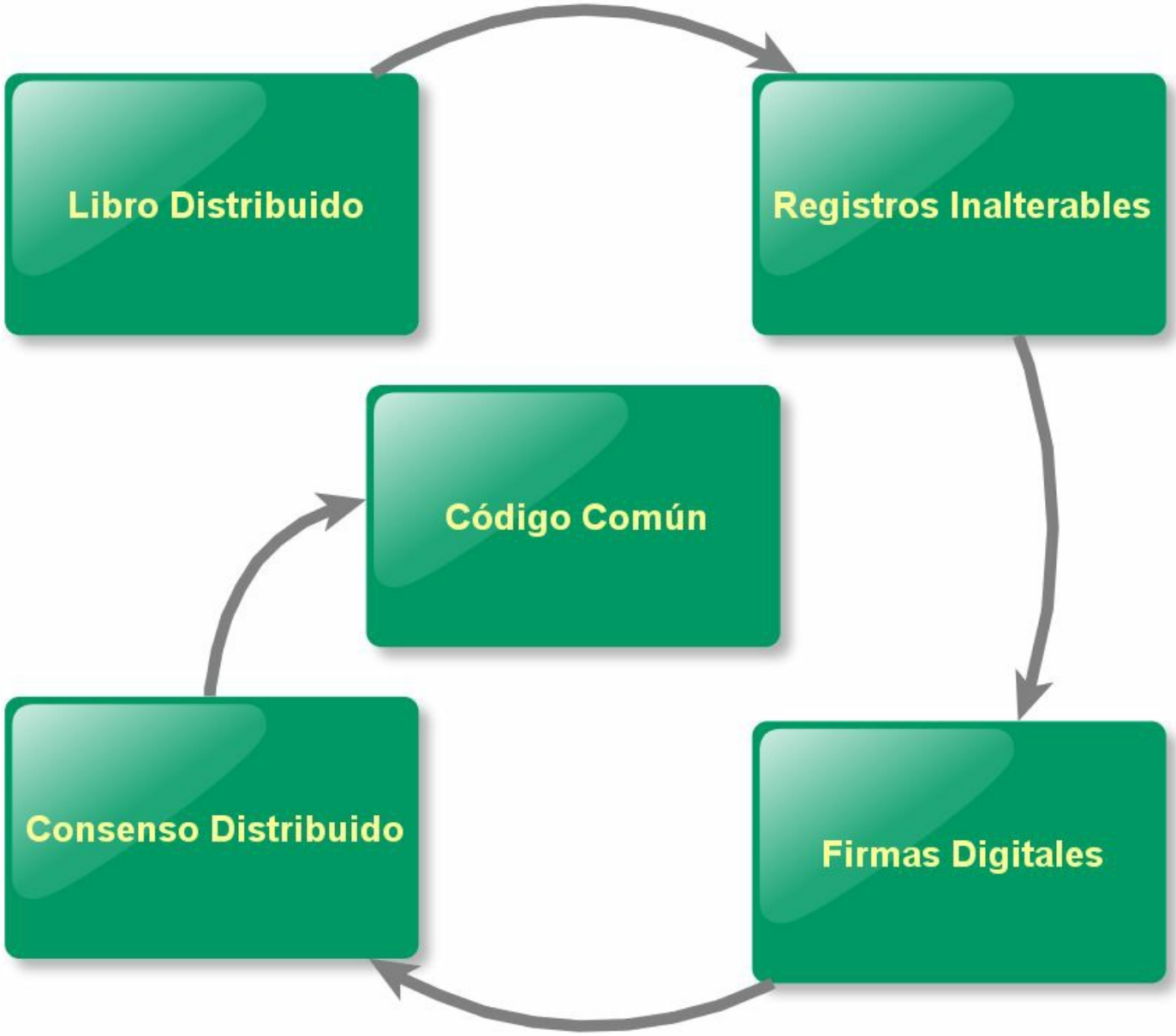
elementos, que son los 5 pilares del Bitcoin y en general de la mayoría de las redes blockchain:

1. libro distribuido
2. registros inalterables
3. firmas digitales
4. consenso distribuido
5. código [abierto] común

La palabra "abierto" está entre corchetes porque aquellos más puristas podrán afirmar que el código no debería ser necesariamente abierto, es suficiente que sea compartido por todos los miembros de la comunidad, no por todo el mundo. Por otra parte, los defensores de las redes públicas exigirán que sea abierto, por lo cual la palabra debe aparecer en

la definición. Hecha la aclaración, el título del quinto pilar en este libro es solamente "código común" sobreentendiendo que la mayoría de las veces será código abierto, lo cual se desarrolla en esa sección.

Los registros inalterables se encuentran almacenados en bloques encadenados, sin embargo podría usarse una estructura diferente, como un grafo acíclico dirigido u otras estructuras. En este caso ya no se trataría de una blockchain, pero seguiría siendo una DLT. La definición anterior, quitando el texto "almacenados en bloques encadenados" sería la definición de una red DLT genérica (incluyendo blockchain).


Libro Distribuido
Registros Inalterables
Código Común
Consenso Distribuido
Firmas Digitales

Primer pilar: Libro Distribuido

¿Qué es un libro distribuido? Supongamos que tenemos una información que queremos proteger de un evento catastrófico, lo más natural es pensar en copiarla a diferentes computadoras. Durante mucho tiempo las empresas que utilizaban información excesivamente centralizada y tenían débiles procesos de respaldo pensaron si era conveniente tener toda su información replicada en diferentes lugares. Esta preocupación se avivó tras los atentados del 11 de Septiembre de 2001 en Estados Unidos. Sin embargo,

recuperar un respaldo puede ser algo muy lento, y en todo ese tiempo la operación de la empresa puede quedar totalmente comprometida.

Por esta razón, la información replicada en forma dinámica, esto es, bases de datos que se encuentran conectadas a través de una red y que aseguran que los registros realizados transaccionalmente se mantienen en todas las copias, pasaron a ser esenciales en toda aplicación de misión crítica.

En los tiempos actuales el manejo de información distribuida y réplicas se utiliza ampliamente. Hay un motivo adicional al de la fiabilidad de la

información. La información en Internet se mueve a la velocidad de la luz, 300 mil kilómetros por segundo. Pero esta velocidad, aunque muy rápida, es finita y solamente se produce en el vacío. Las trasmisiones por cobre o fibra óptica son algo más lentas. Todo lo anterior hace que sea más rápido acceder a un servidor que se encuentra cercano que a uno que se encuentra otra parte del mundo. Para un habitante de México, es mejor conectarse a un servidor de Estados Unidos o Canadá, que a un servidor en Singapur. Por ello se replican los datos, imágenes, videos, e incluso aplicativos.

Aunque el concepto de libro distribuido

es el más fácil de comprender de los pilares, de él derivan varios elementos esenciales de una red blockchain. Se trata justamente, de ubicar la información en diferentes puntos, denominados nodos por ser parte de una red, donde cada uno tiene una copia exacta (al menos del pasado no muy reciente) de las transacciones realizadas en la red.

Un ***libro distribuido*** *consiste en un conjunto de computadoras (o hardware) que almacenan el mismo conjunto de registros (usualmente transacciones) sincronizándose entre sí a través de una red donde cada máquina participa como un nodo.*

Reiteramos, aunque generalmente se usa el término "tecnología blockchain", el nombre formal y más amplio es Tecnologías de Libro Distribuido (DLT por sus siglas en inglés). Prefiero usar el nombre de libro distribuido y no base de datos distribuida, porque este último concepto es muy utilizado en el mundo de bases de datos y suele referirse a otras tecnologías que incluyen medios de replicación. La traducción literal debería ser "libro mayor" o "libro contable"[13], pero considero más general la palabra libro dado que como veremos más adelante los registros que pueden hacerse no están limitados a transacciones contables.

El tamaño de la Red

Un libro distribuido funciona manteniendo en forma sincronizada entre cada nodo (que puede estar ubicado en cualquier parte del mundo) una copia de un conjunto de información. El conjunto de todos los nodos conforma la **red**. Puede considerarse como una base de datos, como un gran archivo de registros, los cuales son copiados en el almacenamiento de cada máquina. La red de Bitcoin es la primera en su tipo en entrar en funcionamiento. En momentos que se comenzó a escribir este libro a fines de 2017, existían más

de 12,000 nodos de Bitcoin, mas de 17,000 nodos de Ethereum y unos 2,000 nodos de Bitcoin Cash, sin contar aquellos que se conectan como billeteras en forma temporal.

La siguiente tabla muestra un mapa con la lista de los veinte países con más cantidad de nodos visibles de la red Bitcoin, proporcionado por el sitio bitnodes.earn.com a comienzos de 2018:

Posición	**País**	**Num. Nodos**
1	Estados Unidos	2508
2	Alemania	1963
3	China	807

4	Francia	659
5	Paises Bajos	496
6	Canada	375
7	Reino Unido	373
8	Federacion Rusa	357
9	Japón	188
10	Singapur	176
11	Hong Kong	159
12	Corea del Sur	157
13	Suiza	146
14	Suecia	121
15	Australia	116
16	Ucrania	104

17	Italia	76
18	España	72
19	Lituania	72
20	Irlanda	71

Esos números son variables con el tiempo, ya que cualquiera de nosotros puede encender su computadora con el software adecuado y poner en funcionamiento un nodo adicional de Bitcoin, esto debido a que es una blockchain pública. Al tratar el cuarto pilar, conoceremos también sobre las redes privadas y permisionadas, otra forma de crear una blockchain diferente a como funciona la red Bitcoin.

Redes P2P

Implementar réplicas en diferentes nodos de una red es relativamente fácil si la información no cambia. Sin embargo, cuando la información va modificándose, necesitamos mantener a esas computadoras conectadas en red para pasarse los datos entre ellas.

Afortunadamente existen protocolos para lograr eso. El software Napster que fue muy popular a comienzos de siglo, significó una disrupción en el mundo de la música, permitiendo que las personas compartieran archivos en formato mp3 entre ellas y ocasionando protestas respecto a la protección de derechos de

autor, con un impacto muy fuerte a las casas productoras.

La familia de protocolos usados en ese tipo de software se denomina Par a Par (P2P, por sus siglas en inglés) y significa que las computadoras pueden conectarse directamente entre ellas, sin la necesidad de que exista un servidor central. Esto es totalmente opuesto a lo que ocurre con los sistemas de redes sociales como Facebook y Twitter, donde la conexión se realiza a muchos servidores propiedad de estas empresas.

*Una **red P2P** es un conjunto de computadoras que no dependen de un servidor central, dado que los nodos*

se comportan como iguales y en general cualquier nodo puede contactar a cualquier otro nodo.

Semillas DNS

Para que los nodos de la red Bitcoin funcionen adecuadamente, cuando se inicializa deben buscarse otros nodos. Existen dos opciones para esto, una es proporcionar un nodo conocido y de confianza que ya esté conectado a la red Bitcoin, el cual conocerá ya a muchos otros nodos y nos pasará la información correspondiente. La otra opción es conectarse a una lista predefinida de computadoras conocidas como **semillas**

DNS[14] las cuales funcionan como las páginas amarillas telefónicas: contienen un listado de direcciones de nodos que están funcionando y a los cuales pueden conectarse. De esta forma cada nodo comienza contando con esa lista de semillas DNS, por lo cual al inicializarse buscará una de ellas para obtener datos de otros nodos de la red. Si no encontrara información, buscará a la siguiente semilla y así sucesivamente. Finalmente, el nodo habrá contactado varios otros nodos, y comenzará a realizar un proceso de sincronización con esos nodos.

Funciones dentro de los nodos

Cada nodo de la red puede cumplir diferentes funciones. Como se indica en la siguiente tabla, el funcionamiento de la red está relacionado con los 5 pilares propuestos en este libro[15]:

Funcionalidad	**Descripción**
Nodo de red	Descubrir otros nodos y comunicarse con ellos para trasmitir información (transacciones y sincronización de la estructura de cadena de bloques)
	Guardar en forma parcial o completa la estructura de la

Almacenamiento	cadena de bloques (ver en el Segundo Pilar: Registros inalterables)
Billetera	Permitir guardar y enviar unidades del blockain (ej. bitcoins) a otros nodos (ver en el Tercer Pilar: Firmas digitales)
Generación de Bloques	Crear nuevos bloques para agregarlos a la estructura de la cadena (ver en el Cuarto Pilar: Consenso Distribuido)

Beneficios del libro distribuido

¿Para qué nos sirve que un libro sea distribuido? Tener la información en un libro distribuido permite:

- En caso de que uno de los nodos deje de funcionar, acceder a otro nodo
- Poder elegir a que nodo conectarnos, lo cual puede tener efectos de rendimiento
- Contar con copias alternativas de

la información, en caso de que dudáramos de la integridad en el nodo que estamos accediendo (por ejemplo si un extraño intentara modificar la información y solo lograra hacerlo en uno o pocos nodos)

En un libro distribuido con un buen número de nodos, si uno aparece diferente contrasta con el resto de los nodos. Poder descubrir inconsistencias es fundamental. Este asunto es importante, debido a que al tener muchas copias que están indicando cuanto valor tenemos en dinero, si alguien realiza un cambio en forma unilateral podremos descubrir la alteración. La forma más

adecuada para hacerlo se verá en el segundo pilar. Así que si en todos los nodos dice que Juan tiene 100 dólares, pero en el nodo de Juan el libro dice que tiene mil dólares, podríamos presumir que Juan hizo alguna modificación. La red simplemente ignorará su nodo.

La comunidad

El mantenimiento de la red de nodos y el software que deriva en el libro distribuido, implica la necesidad de una comunidad. Aunque una empresa o varias empresas podrían mantener un buen número de nodos de esta red, en el caso de Bitcoin y muchas redes

blockchain públicas el mantenimiento ocurre a través de una comunidad con integrantes distribuidos en diferentes países en todo el mundo. Todos los miembros de la comunidad deben comprender mínimamente el funcionamiento y los requerimientos para participar con uno o más nodos dentro de la red. También deben cumplir con una serie de reglas, como veremos más adelante, para asegurar que toda la red subsista en forma integral y no se divida o subdivida en varias redes menores.

Generalmente la comunidad se convierte en el respaldo de la red. En la red Bitcoin esa comunidad está compuesta

de:

- Participantes con nodos completos, que guardan una copia más del libro distribuido, en ocasiones buscando recompensa (a ellos se les denomina mineros)
- Desarrolladores de software, que apoyan al mantenimiento del código necesario para que un nodo pueda funcionar
- Usuarios, personas que buscan intercambiar valor dentro de la red (en algunos casos usando la unidad como medio de pago)
- Intermediarios, como las casas de cambio, que buscan crear mercados donde se pueda

intercambiar bitcoins por moneda fiat u otros criptoactivos
- Promotores de la tecnología, que pueden utilizarla para otros fines

Adicionalmente forman parte de la comunidad aquellos que creen en la filosofía que esa comunidad tiene. En el caso de Bitcoin esta podría ser la filosofía de búsqueda del "dinero alternativo" o "dinero de la gente" que ha sido mencionada al comienzo del libro.

El tamaño de la comunidad es importante, ya que se convierte en lo más cercano a la garantía de que la red se mantendrá siempre en

funcionamiento, lo cual a su vez impacta en la fortaleza de todo el ecosistema Bitcoin, y suele reflejarse en su mantenimiento de precio o su volatilidad. Según la opinión generalizada, cuando la comunidad recibe noticias negativas o tiende a dividirse, el precio suele bajar; por el contrario cuando se percibe sólida y se generan mejoras en la tecnología, el precio tiende a subir.

Evitando conciliaciones

¿Acaso no es suficiente contar con un libro distribuido para tener las ventajas de blockchain? La opción de distribuir

la información existe desde hace mucho tiempo, pero no es suficiente para crear una red blockchain.

Si se tratara de un respaldo, una información que permanecerá inamovible, la solución es sencilla. Pero para generar dinero digital, necesitamos registrar transacciones. Cabe preguntarse qué ocurre cuando uno de los actores en la red quiere registrar una transacción y hacer un cambio.

Por ejemplo, sería sencillo que Juan avisara a la red algo así como "quiero transferir 10 bitcoins de mi cuenta a la de Ana". Y todos podrían registrar esa solicitud. Si estuviera garantizado que

todos los participantes se comportaran adecuadamente, sin trampas, se tendrían que descontar 10 Bitcoins de la cuenta de Juan en el registro de cada nodo. El problema es que no todos los participantes jugarán un juego limpio. Si no hay una entidad central ¿cómo asegurarnos que realmente se descuente en el libro que Juan ya no tiene esos 10 bitcoins?

Además, ese movimiento puede ser pequeño en monto en relación al resto de los movimientos. A fines del año 2017 se movían diariamente más de un millón de bitcoins en la red, un equivalente a más de diez mil millones de dólares por día. En un movimiento

así, una trampa de 10 bitcoins es insignificante. En un sistema contable tradicional será difícil encontrarla.

Si tenemos múltiples copias de estos libros y hay varias personas que hacen modificaciones, no tendremos forma de saber quién tiene el libro contable correcto. Una forma sería indicar que un nodo tiene toda la autoridad. Esa es la solución tradicional, se crea un intermediario. Ese intermediario resuelve las disputas y todos acatan lo que finalmente decida.

En definitiva, al parecer deberíamos estar haciendo conciliaciones, contactándose un nodo con otro, similar

a lo que ocurre con las empresas. Y hasta tendríamos que tener auditorías. Pero esta alternativa no parece ser muy práctica, y definitivamente no es lo que se hace en una red blockchain.

Hay otra solución, y esa está basada en funciones matemáticas que permiten asegurar que muy pocas diferencias sean altamente visibles. Con ello hemos llegado a la necesidad del segundo pilar: los registros inalterables.

Notas:

[12] - Existen esfuerzos liderados por la Asociación Australiana de Estándares para definir los términos en relación a las DLTs, los cuales buscan llevarse a

la Asociación Internacionla de Estándares (ISO, por sus siglas en inglés). Ver la referencia en ingés: Roadmap for Blockchain Standards en el sitio https://www.standards.org.au

[13] - Del inglés "distributed legder".

[14] - Por las siglas en inglés de Sistema de Nombres de Dominio, el cual permite traducir las direcciones IP en Internet por nombres de dominio legibles.

[15] - Esta relación la descubrí mucho después de mis primeras presentaciones sobre los cinco pilares al crear una tabla informativa con base en el libro "Mastering Bitcoin" de Andreas Antonopoulos.

Segundo pilar: Registros Inalterables

El Doble Gasto

¿Qué pasaría si pudiera usar mi billete de 100 dólares sin jamás gastarlo?

En un mundo digital, si poseo un archivo binario este puede ser copiado en forma idéntica a otro archivo. Algo muy conveniente para la distribución de medios o de software. Sin embargo, cuando se trata de implementar dinero

digital se convierte en un problema. Porque funcionaría como un billete que se usa pero jamás se gasta. Esa opción de usar dos veces el mismo valor es lo que se denomina doble gasto, y en un sistema de dinero digital debe asegurarse su inexistencia.

Llevar un registro de transacciones exacto que nos indique quien gastó y quien recibió, lo cual es finalmente un libro contable, comienza a asegurar que no haya doble gasto: esto es lo que registra la red Bitcoin en cada copia de su libro distribuido.

El problema aún no se resuelve, si tenemos muchas copias de estos libros y

hay muchas personas que hacen modificaciones, no tendremos forma de saber quién tiene el libro contable correcto. Una forma sería indicar que un nodo tiene toda la autoridad. Esa es la solución tradicional, se crea un intermediario. Ese intermediario resuelve las disputas y todos acatan lo que finalmente decida.

Pero otra forma de hacerlo es que todos puedan tener un número verificador, que aunque sea muy largo, permita darte cuenta de que tu copia se encuentra en el mismo estado que las copias de los demás nodos. Para ello requerirás echar un vistazo a una de las aplicaciones de la criptografía que se usan en

blockchain.

> ***Citando a Satoshi**:*
> *"En este trabajo, proponemos una solución al problema del doble gasto utilizando un servidor de marcas de tiempo P2P distribuido para generar una prueba computacional del orden cronológico de las transacciones."*
> *Satoshi Nakamoto, 2008.*

Un poco de criptografía

Lo que vas a leer sobre criptografía es en la práctica relativamente simple, no deberías asustarte por el título. Como

comentábamos al inicio del libro, muchas partes de mayor dificultad técnica de las DLTs serán ocultadas o no mencionadas en este libro para facilitar la comprensión. Los dominios de la criptografía son enormes, hay muchas funciones criptográficas, un mundo con demostraciones de complejos teoremas y corolarios, una ciencia de la mano de las matemáticas más avanzadas. Son muchos estudios profundos que debe realizar un criptógrafo.

Aquí no encontrarás un tratamiento a esa profundidad, no vamos a colocar comandos de ejecución o código de programas de cómputo ni mucho menos

formulación de teoremas. Sin embargo, hay dos asuntos relacionados con la criptografía que son de vital importancia para entender el funcionamiento de las DLTs: si no se explican, podríamos afirmar que no se ha entendido realmente qué son estas tecnologías.

Las funciones de resumen son el primero de esos elementos. Si ya conoces el concepto de función hash, puedes saltarte esta sección hasta el título "Propiedades de las funciones Hash". Si prefieres hacer un repaso de conceptos o conocer más sobre este tema, quédate en este capítulo donde veremos qué significan estos términos: función, número hexadecimal, función hash y

colisión.

Función

Cuando hablamos de una función, nos referimos a una función matemática, similar a las que conocimos en la secundaria, por ejemplo consideremos un polinomio de primer grado:

$f(x) = x *5 + 120$

Se trata de una función donde a cada valor de x da como resultado un valor de f(x), por ejemplo para x=1, el resultado es 125. Una función es una relación que asigna a un valor de los

posibles de x, un único valor diferente de potenciales resultados.

Sin embargo, el conjunto de partida no necesariamente debe ser un número a primera vista, si consideramos que una serie de bytes representan un número, podemos aplicar también una función a esa serie de bytes. Por ejemplo, podríamos considerar la función OrdenaBytesCreciente, que ordene los bytes en forma creciente. De esta forma si tenemos un archivo misbytes.dat con este contenido:

misbytes.dat
73

02
48
21

el resultado de aplicar la función será:

OrdenaBytesCreciente(misbytes.dat)
02
21
48
73

Número Hexadecimal

En las funciones hash, los valores resultantes usualmente no se representan con diez símbolos (notación decimal) sino que se usa la notación **hexadecimal** la cual considera un total de 16 símbolos. El resultado 125 en hexadecimal es 7D. Curiosamente para convertir 7D a decimal podemos usar otra función de primer grado. La letra D representa el 13 decimal y el 7 debe multiplicarse por 16 porque se encuentra en la segunda posición. Entonces al convertir 7D a decimal tenemos:

$7*16+13 = 125$

La función de primer grado que usamos fue:

f(x) = primer_digito * 16 + segundo_digito

En la siguiente tabla mostramos los números decimales del 0 al 29 y sus representaciones en hexadecimal.

Dec.	Hex.	Dec.	Hex.
0	0	15	0F
1	1	16	10
2	2	17	11
3	3	18	12
4	4	19	13
5	5	20	14
6	6	21	15

7	7	22	16
8	8	23	17
9	9	24	18
10	0A	25	19
11	0B	26	20
12	0C	27	21
13	0D	28	22
14	0E	29	23

Como comentábamos, las funciones hash usualmente se representan con un resultado en hexadecimal. En este libro estaremos representando las series de bytes como números hexadecimales pero en grupos de 4 caracteres (2 bytes)

separados por un espacio, esto para facilitar la lectura en dispositivos móviles. De esta forma el hexadecimal AC415983BB72 se representará en este libro como AC41 5983 BB72.

Huellas digitales de los datos

Aunque el nombre en español es función de resumen, lo más común es que se encuentre el nombre de función hash por la estructura de datos que se utiliza para realizar el cálculo. También se le suele llamar hash a secas a un resultado concreto de una función hash.

Para ilustrar fácilmente como se aplica

una función hash, podemos partir del concepto denominado dígito verificador. Es un valor de un dígito usado para muchos códigos corporativos, números de identificación y cuentas bancarias.
Por ejemplo en México si se tiene una cuenta bancaria correspondiente al banco 014, sucursal 180 y número de cuenta 12344556677 se crea la CLABE[16] interbancaria juntando los dígitos así: 014180123445566 77 pero adicionalmente se hace una operación usando esos dígitos para obtener un dígito adicional, por ejemplo el 2, quedando como resultado una CLABE: 014180123445566772

Si por alguna razón uno de los dígitos

anteriores se escribiera mal al intentar realizar una transferencia por Internet, el último digito no coincidirá (porque se calculó en función de los números correctos) y eso nos ayudará a darnos cuenta de nuestro error.

Básicamente el dígito 2 es un "resumen" de todos los dígitos anteriores. Aunque conviene advertir: si nos equivocamos por varios dígitos quizás vuelva a coincidir que el dígito verificador es 2. El diseño está preparado para resistir un error, no múltiples errores.

El dígito verificador da una idea simplificada de la forma en que funciona un algoritmo de función hash. Estas

funciones son mucho más complejas, reciben muchos más datos en forma variable. Realizan un tamizado de la información mezclándola de muchas formas en su proceso interno y resultan en una serie de bytes de largo fijo: siempre la misma cantidad de caracteres.

Las funciones hash más conocidas son bastante más largas que un dígito y tienen nombres algo extraños, las más conocidas son md5, sha1, sha2-256, sha2-512. La siguiente tabla muestra los largos de cada función hash.

Función	Largo Bytes	Largo Hexadecimal

MD5	16	32
SHA-1	20	40
SHA-256	32	64
SHA-384	48	96
SHA-512	64	128

La tabla de más abajo muestra ejemplos del hash de "HOLA MUNDO" en mayúsculas.

Función	**Resultado Hash de "HOLA MUNDO"**
	68E4 B955 1869 BCE5 B170

MD5	E873 F5AB E1F7
SHA-1	76AE 569A 40BC F30E 79A6 1699 20ED 616F 85B3 FEAA
SHA-256	FE66 F29E 4AE4 3F0B DE57 1567 BDCA 37C9 360F 1448 1739 C012 69F1 1923 F54F 5575
SHA-384	3816 CEB3 FFE2 EBBD 1EE7 89A6 3103 C825 FAF7 0BA7 BDFD A54A FAE8 AA30 7CBB 7446 AC8D 603E 0541 10AE D9E7 D4B7 C715 8FDA
SHA-	02B8 85D9 84DE 653F D42E 6895 1638 D24D 4E5E AAF4 5C10 82E7 01F5 ABAA

512	DBA0 7CEB 0273 BF8A 1FF6 49F7 92D0 1602 8C69 63A7 FF06 29B9 3241 74EA 7089 0903 4CC1 F4B3

Una función hash puede ser aplicada a un archivo muy grande, por ejemplo una base de datos o un video. Sin embargo generalmente es más adecuado aplicarlas en bloques o bien sobre archivos comprimidos.

Funcionamiento

¿Cómo funciona una función hash? Se trata de un algoritmo que toma la entrada, en este caso el x y hace cálculos

sobre ella hasta obtener un resultado que es un "resumen" de su contenido.

Veamos por ejemplo una de las funciones hash muy conocidas llamada md5. Si tomamos la cadena de caracteres "HOLA MUNDO"
y le aplicamos la función md5 tendremos:

md5(HOLA MUNDO) = 68E4 B955 1869 BCE5 B170 E873 F5AB E1F7

Siempre dará ese resultado en cualquier computadora que calcule la función md5, no importa en qué lenguaje de programación este implementada la función. Sin embargo, la función si nota

diferencia si se pone el texto en minúsculas o en mayúsculas.

De esta forma tenemos

md5(hola mundo) = 0AD0 66A5 D29F 3F2A 2A1C 7C17 DD08 2A79

Ahora si se considera la función SHA-256 y la aplicamos a pequeñas variaciones de la frase "Hola Mundo", veamos los resultados:

Texto	**Resultado SHA-256**
HOLA MUNDO	FE66 F29E 4AE4 3F0B DE57 1567 BDCA 37C9 360F 1448 1739 C012 69F1 1923 F54F 5575

hola mundo	0B89 4166 D333 6435 C800 BEA3 6FF2 1B29 EAA8 01A5 2F58 4C00 6C49 289A 0DCF 6E2F
hola mundo. (punto al final)	4668 A116 DC25 7A09 8E24 1E57 BEEE 8B5B C1BD 8F53 A8D7 53F2 990D 7D8A 4B4E 34DE
Hola mundo	CA8F 60B2 CC7F 0583 7D98 B208 B57F B648 1553 FC5F 1219 D596 18FD 0250 02A6 6F5C

Lo que observamos en la tabla anterior es que:

Un pequeño cambio en los datos de

entrada de una función hash provoca un cambio radical en el hash resultante.

Aplicaciones prácticas

Las funciones hash pueden aplicarse también a archivos enteros, incluso archivos de video.

Por ejemplo, si aplicamos la función SHA-256 al archivo PDF del documento de https://bitcoin.org/bitcoin.pdf nos dará el siguiente hash:

B167 4191 A88E C5CD D733 E424 0A81 8031

05DC 412D 6C67 08D5 3AB9 4FC2 48F4 F553

Si alguien cambiara ese archivo desde el momento que se descargó, ese valor cambiará radicalmente, aunque se cambie un solo byte del archivo.
¿Eso qué significa? Que podemos identificar un cambio en el contenido solamente con ver el resultado de la función hash. Y que además puedo comparar dos archivos usando las funciones hash, en lugar de estar revisando manualmente byte a byte si es diferente.

Esta propiedad de las funciones hash es muy usada en Internet para verificar la

autenticidad de los archivos que se descargan. Si un ejecutable fuera modificado con malas intenciones, su valor de hash cambiaría.

Por ejemplo en la página del motor de bases de datos SQLLite, se proporcionan los valores de SHA1 para cada archivo de descarga. Una vez descargado el archivo se puede verificar que su SHA1 coincide con el que está publicado. De esta forma se puede determinar si el archivo está alterado o no al recibirlo.

Colisiones

Podríamos decir que el valor de hash es una "huella digital" de la cadena de texto. Sin embargo, ¿podría ocurrir que dos cadenas de texto produjeran el mismo valor? Esto se denomina una "colisión" y efectivamente, si la función hash no tiene un resultado suficientemente largo en caracteres, esto puede ocurrir. Ya se han descubierto colisiones para funciones md5 y sha1. Veamos por ejemplo estas dos cadenas escritas en hexadecimal que se parecen mucho, pero tienen algunos caracteres diferentes, por ejemplo a mitad de la secuencia una contiene en AFBF A200 y la otra AFBF A202:

CADENA 1:

4DC9 68FF 0EE3 5C20 9572 D477 7B72 1587 D36F A7B2 1BDC 56B7 4A3D C078 3E7B 9518 AFBF A200 A828 4BF3 6E8E 4B55 B35F 4275 93D8 4967 6DA0 D155 5D83 60FB 5F07 FEA2

CADENA 2:
4DC9 68FF 0EE3 5C20 9572 D477 7B72 1587 D36F A7B2 1BDC 56B7 4A3D C078 3E7B 9518 AFBF A202 A828 4BF3 6E8E 4B55 B35F 4275 93D8 4967 6DA0 D1D5 5D83 60FB 5F07 FEA2

Cuando se calcula el md5, ambas dan el mismo resultado:

008E E33A 9D58 B51C FEB4 25B0 9591 21C9

Este es un caso conocido de colisión para la función MD5.

La primer colisión para la función MD5 fue hallada el 17 de Agosto de 2004 por Xiaoyun Wang y sus colaboradores, al encontrarse con un caso de dos juegos de datos binarios produciendo la colisión. El MD5 resultante fue:

A4C0 D35C 95A6 3A80 5915 367D CFE6 B751

Posteriormente Xiaoyun Wang y Hongbo Yu publicaron "Cómo romper MD5 y

otras funciones hash" en la publicación Avances en Criptología, en la Conferencia Internacional de Teoría y Aplicaciones Criptográficas en Dinamarca, celebrado en Mayo de 2005.

Esto no se cumple para la función SHA2-256 y las de mayor longitud como SHA2-358 o SHA2-512 (no han existido casos) por la tan baja probabilidad de una colisión. Podría decirse que no existirán colisiones de esas funciones en un futuro que nuestra especie conocerá. Como siempre, esto queda sujeto a un potencial cambio por algún descubrimiento matemático que sería notable, pero que no solamente afectaría a la tecnología blockchain, sino

probablemente a buena parte de los mecanismos de seguridad actualmente utilizados para proteger a los sistemas de empresas y gobiernos conectados a Internet.

Propiedades de las funciones hash

Las funciones hash tienen varias propiedades, una de ellas es que su uso es **irreversible**. Esto significa que puedo obtener fácilmente el hash de la frase "hola mundo", pero si conozco el hash y quiero conocer la frase que lo produce, no existe algoritmo que lo permita.

Es más, si quiero obtener un archivo que

me produzca un SHA-256 que contenga una serie de bytes específicos, la única manera de hacerlo es utilizando lo que se denomina fuerza bruta: probando una y otra vez con una cadena, aplicándole el SHA-256 y verificando si el resultado coincide con la serie de bytes que buscamos[17]. Incluso si solamente buscáramos que comenzara con ciertos bytes, también se debería seguir el mismo procedimiento.

Además las funciones hash tienen las siguientes propiedades:

1. Su largo siempre es fijo (para la misma función)
2. Siempre que se aplican a la

misma entrada se obtiene el mismo resultado

3. No existe función inversa que permita obtener el mensaje a partir del hash resultante: deben probarse continuamente las entradas hasta que coincida el hash
4. Para generar su resultado tienen en cuenta todos los bytes de la información de entrada
5. Un pequeño cambio en la entrada genera un cambio radical en el hash resultante
6. En la práctica no puede encontrarse dos entradas que den el mismo valor hash (colisión)

En relación a la segunda propiedad, es importante observar que el hash resultante siempre es el mismo cuando se aplica a una entrada, no importando en que lenguaje de programación se implemente el algoritmo de la función. Debido a su popularidad, existen implementaciones de las funciones hash en prácticamente todos los lenguajes de programación de propósito general, por lo cual si un programador quiere implementar una solución en su lenguaje favorito, puede hacerlo contando con la biblioteca adecuada.

Las funciones hash, junto con otros algoritmos de propósito similar usados en otras redes diferentes a la de Bitcoin,

se hacen ideales para resolver el primer problema derivado de tener un libro distribuido: detectar rápidamente potenciales modificaciones a la información. Para ello se utiliza una estructura denominada cadena de bloques, que le da nombre a la tecnología blockchain[18].

La cadena de bloques

Denominamos **cadena de bloques** a una estructura de datos organizada en fragmentos de información denominados bloques relacionados entre ellos. Cada bloque contiene una serie de propiedades, entre ellas registros de

transacciones y un vínculo a un bloque anterior.

Por ejemplo, esta sería una representación del bloque 150 de una cadena de bloques que usaremos como ejemplo didáctico:

Número de bloque	**150**
Nonce	0
Datos	Ana paga 100 Bitcoins a Juan Pedro paga 150 Bitcoins a Mario
	7ED9 3D2B 7C62 AB8E DDBD 8A23 6B23 809D

HashPrevio	4173 7502 415B 5FC1 126E 72CC 2194 09BE
Hash	4549 F33D 0110 4BD9 BD73 FF71 9C34 023D 3316 2220 B244 6AD9 208E 4A94 F61A C72B

Las propiedades que podemos ver en el ejemplo son el número de bloque (suele denominarse altura de bloque, lo cual tiene sentido si representamos los bloques todos apilados), los datos de las transacciones, un dato denominado Hash-Previo y al final un Hash, que se calcula en función de todos los datos anteriores. Hay un dato variable que se denomina nonce que no lo trataremos sino hasta el cuarto pilar.

La cadena de boques de Bitcoin tiene varias diferencias y complejidades adicionales, sin embargo lo que estamos representando aquí es a efectos exclusivamente de comprensión. Así, para formar una cadena de bloques, el siguiente bloque se construye así:

Número de bloque	**151**
Nonce	0
Datos	Juan paga 25 Bitcoins a Mariana Mario paga 120 Bitcoins a Luisa Ana paga 20 Bitcoins a

	Santiago
HashPrevio	4549 F33D 0110 4BD9 BD73 FF71 9C34 023D 3316 2220 B244 6AD9 208E 4A94 F61A C72B
Hash	9CCD E7E3 E4DC 3ABD 7413 6AB2 C8FE FBBD 8A74 F0A0 D8F2 1C40 2BF8 8CB5 13DA F808

Aquí agregamos usando la imaginación otras transacciones, para representar el funcionamiento de la cadena. Podemos observar que el campo de HashPrevio que comienza con 4549F3 coincide totalmente con el Hash del bloque 150. Esta es la forma en que los bloques

quedan "encadenados" y la propiedad que le da nombre a la cadena de bloques. Como el lector podrá suponer, un siguiente bloque, se formaría de esta manera:

Número de bloque	**152**
Nonce	0
Datos	Juan paga 7 Bitcoins Santiago
HashPrevio	9CCD E7E3 E4DC 3ABD 7413 6AB2 C8FE FBBD 8A74 F0A0 D8F2 1C40 2BF8 8CB5 13DA F808
	6F56 2EBF 875E 230B D4A4 184A 949B FAC7

Hash	16D5 7978 846C 1271 4963 CE60 427D D25A

Y nuestro bloque siguiente sería:

Número de bloque	**153**
Nonce	0
Datos	Santiago paga 10 Bitcoins Mario Mariana paga 5 Bitcoins a Mario
HashPrevio	6F56 2EBF 875E 230B D4A4 184A 949B FAC7 16D5 7978 846C 1271 4963 CE60 427D D25A
	357D 2F60 E1D0 E2FB

Hash	27BF AD90 14FC B4E0 DC35 0C1B 7DD2 E63A D31C DEDA E082 D35A

De esta forma hemos creado un fragmento de una cadena de bloques que podría representarse así:

Bloque 150	**Bloque 151**	**Bloque 152**	**Bloque 153**
(2 registros)	(3 registros)	(1 registro)	(2 registros)
Prev: 7ED9...	Prev: 4549...	Prev: 9CCD...	Prev: 6F56...
Hash: 4549...	Hash: 9CCD...	Hash: 6F56...	Hash: 357D...

Aunque se usa como traducción de "blockchain", este término en inglés se utiliza para representar algo que va más allá, debido a que abarca el funcionamiento completo de la red. En realidad, no hay actualmente consenso respecto al uso del término blockchain, sin embargo en este libro usamos la definición proporcionada en la introducción. La cadena de bloques en cambio, en español, se refiere aquí a la estructura de datos utilizada para soportar el libro de registros inalterable (también llamados registros inmutables).

En ocasiones también se refiere a la estructura de la cadena de bloques como un libro inalterable, sin embargo no es

inalterable en el sentido estricto de la palabra (que nada puede alterarse). Un libro inalterable implica que lo que ya se escribió, ya no puede borrarse. Pueden agregarse nuevos registros, pero las páginas ya escritas no pueden modificarse. Una vez que volteas la página, básicamente está escrito en piedra, o mejor aún, está escrito en la blockchain. En general, la piedra es más fácil de destruir, en cambio una blockchain requeriría no solamente apagar Internet, sino hacer que los nodos queden incomunicados incluso por otros medios.

Explorando la cadena

Para ver las páginas de estos registros podemos usar herramientas de software llamadas **exploradores**. Muchas de ellas están publicadas en la propia web para uso general. Prácticamente toda blockchain tiene al menos un sitio disponible con un explorador, y si no es así, quizás no exista la propia blockchain (muchos fraudes pueden detectarse al preguntar por el explorador de la cadena).

Lo que hacen los exploradores es conectarse a un nodo propio que a su vez está conectado a toda la red blockchain (es un nodo más de la red). Por esta razón cuenta con toda la información disponible, ya que como

recordamos cada nodo debe tener el total de registros históricos de la cadena de bloques.

Descargando el software apropiado, y poniendo a funcionar un nodo de la red Bitcoin, tú podrías también tener tu propio explorador. No hay que pedir ningún permiso, solamente conectarse a la red.

Los exploradores permiten buscar información en la cadena de bloques, puede ser a partir del número de bloque (más comúnmente llamado altura de bloque), de una dirección de Bitcoin, o de un identificador de transacción.

Busquemos por ejemplo el bloque número 111999 de la cadena de bloques de Bitcoin en blockexplorer.com, uno de estos sitios de exploración de la cadena:

Altura de bloque	**111999**	
Marca de tiempo	2011-03-05 08:17:25	
Nonce	627311872	
Hash	0000 0000 0000 65e3 af34 797f e53f 6f35 5c2b f40a c13b 2778 4e68 76c0 c078 8117	
	0000 0000	

Bloque previo	0000 eb59 6a34 c7e3 4fb4 32e2 fb05 49ab 9557 77dd 580f b742 5dae cc0e	
Total de transacciones	2	
Transacciones:		
Emisor:	Receptor:	Monto
	17TX iCLE 9bMz HrHL ufBg 1s5V FE5e sA5c qH	50.01 BTC
1ETa CryF NDy7 2qMw EJwi Czjy SkCU Aqgt 8o	1CAm vuiz VuAN avWS vAYq xypf TKFx z2cS Pg	79.29 BTC

1ETa CryF NDy7 2qMw EJwi Czjy SkCU Aqgt 8o	18Cw G39r Hcge VQ4T 8JXz XVMT Bvy8 x8Rw Sh	0.05 BTC

Este es un bloque real, a diferencia de los bloques de ejemplo del principio de este capítulo. La información se ha resumido y se le ha dado forma para presentarla en el capítulo, verás más detalles en los sitios de los exploradores.

Puedes observar varias cosas, en primer la altura de bloque (que es el número del bloque en la cadena). En segundo lugar que tiene una **marca de tiempo** la cual se realiza considerando que todos

los nodos tienen sus relojes sincronizados gracias a un protocolo de tiempo en la red, permitiendo así tener certeza de cuando se registra el bloque en la cadena. De hecho, si algún nodo no estuviera sincronizado, generalmente el conjunto de la red lo rechaza hasta que ajuste su reloj.

***Citando a Satoshi**:*
"Servidor de marcas de tiempo: La solución que proponemos comienza con un servidor de marcas de tiempo. Un servidor de marcas de tiempo funciona al tomar un hash de un bloque de elementos a ser fechados y publicando ampliamente el hash, tal como en un periódico..." Satoshi

Nakamoto, 2008.

Adicionalmente puedes ver un parámetro denominado nonce, del cual aprenderás su razón de ser en el capítulo correspondiente al consenso distribuido.

Podemos ver además el hash, que no por casualidad comienza con doce ceros. Hay razones para esto, ya las podrás conocer. El bloque contiene solamente dos transacciones, en una de ellas parece crearse de la nada unos 50 bitcoins (abreviatura BTC), y en la otra transacción el dinero de un poseedor de bitcoins pasa a dos nuevos poseedores diferentes.

Ahora veamos el siguiente bloque, el 112000:

Altura de bloque	**112000**	
Marca de tiempo	2011-03-05 14:17:53	
Nonce	2809263700	
Hash	0000 0000 0000 1d69 b389 9a49 f377 99c3 75a7 4718 2995 3d54 70f4 68f4 8ff7 0432	
	0000 0000 0000 65e3 af34 797f e53f 6f35	

Bloque previo	5c2b f40a c13b 2778 4e68 76c0 c078 8117	
Total de transacciones	1	
Transacciones:		
Emisor:	Receptor:	Monto
	175o XHhj JgQC ewec UyYQ A9UY 5g8o VK2p gk	50 BTC

Aquí podemos verificar que este bloque tiene como hash previo el del bloque 111999, como era de esperarse. Sin embargo este bloque tiene solamente una transacción, donde solamente aparecen

de la nada 50 BTC.

Sí, efectivamente en la red Bitcoin existe un mecanismo similar a un banco central, que permite emitir unidades de la cadena de bloques. Necesitarás algo de paciencia, ya que antes de ver la razón, vamos a explorar el tercer pilar: las firmas digitales.

Notas:

[16] - Se denomina CLABE por las siglas de Clave Bancaria Estandarizada.

[17] - Quizás ya lo hayas escuchado: esto es lo que se utiliza por ciertos participandes de la red denominados "mineros" a quienes te vamos a

presentar cuando tratemos el cuarto pilar.

[18] - Por la traducción del inglés, "block": bloque, "chain": cadena.

Tercer pilar: Firmas Digitales

¿Cómo se crea una cuenta Bitcoin?. Y una vez creada ¿Cómo se transfieren los bitcoins de una cuenta a otra?

En una red como la de Bitcoin, cada transacción que se realiza debe ser firmada por el emisor de una forma que todos los demás participantes puedan validar quien la ha firmado. Para que pueda realizarse, se utiliza criptografía. Esto permite que los usuarios firmen sus transacciones de una forma que solamente ellos pueden hacer, y que esa firma pueda ser validada por todos los

demás en la red.

Además se requiere una unidad de medida para que esa transacción. Podrían ser 10 pesos, o 10 dólares, pero en la práctica eso no es posible, ya que no se puede controlar el valor de esos pesos o dólares (veremos más adelante que es necesario crear esas unidades de medida, y crear pesos o dólares sería emitirlos, actividad reservada a los bancos centrales).

En definitiva, dentro de la blockchain se requiere usar una unidad propia. Esa unidad es lo que se suele denominar "criptomoneda", pero eso no significa que realmente sea una moneda. En el

caso de la red Bitcoin, la unidad también se llama Bitcoin, o BTC. Así cuando se transfieren diez unidades se dice que se transfieren 10 BTC. ¿Cuánto vale en dólares cada BTC? Ese es otro tema, que incluso escapa del propio concepto de blockchain, por eso será tratado en la parte 2.

Las transacciones se envían a una lista de transacciones pendientes, que quedan en cada nodo de la red Bitcoin. Cada nodo deberá validar que la transacción está correctamente firmada, si no es así rechazará la transacción. Si pasa la validación, se considerará la transacción para ser incluida en un nuevo bloque, como se podrá ver en las

secciones que siguen. Para que esto funcione, se utiliza criptografía.

Criptografía Asimétrica

Para que las transacciones puedan ser firmadas se utiliza una tecnología de criptografía que abarca toda una familia de métodos y algoritmos: la criptografía de llave pública y privada también denominada criptografía asimétrica.

Se llama criptografía asimétrica debido a que a diferencia de la criptografía simétrica, no se utiliza la misma clave para encriptar y desencriptar un contenido. Por ejemplo, usando el

algoritmo de criptografía simétrica llamado Blowfish, el resultado de encriptar la frase "HOLA MUNDO" con la contraseña "abracadabra" es el siguiente código: EBE441B97AA5EBEEF631AA2BF88C

Si a ese código le aplicamos desencriptación con la misma contraseña "abracadabra", nos vuelve a regresar el resultado "HOLA MUNDO".

En la criptografía asimétrica, se requiere una clave para encriptar y otra para desencriptar. Esto significa que si enviamos la llave que solamente desencripta, podríamos ver perfectamente el resultado de un

mensaje y si este es válido, pero nunca podríamos encriptarlo con esa clave, a menos que la conozcamos. Eso hace que una llave pública y otra privada se den en pares. Una llave pública siempre va asociada a determinada llave privada.

Esta tecnología existe desde los años 70, no se trata de una novedad su uso en Blockchain, sin embargo se encontró que podían aplicarse a Blockchain, y que en particular un tipo de algoritmo basado en curvas elípticas, era el más adecuado para la implementación.

Facturas Electrónicas

Como ejemplo, en México, se usan diariamente las direcciones basadas en criptografía para firmar las facturas electrónicas, un sistema que ya tiene más de 10 años de antigüedad.

Cuando una persona concurre a una oficina del Servicio de Administración Tributaria (el nombre que tiene el departamento de hacienda en México) para solicitar la firma electrónica (denominada e-Firma) a través de la cual se puede generar las autorizaciones y firmas junto con esa autoridad, se entrega al contribuyente un archivo denominado "llave" con una extensión "key" conjuntamente con una contraseña elegida por el usuario.

Conjuntamente el archivo "key" y la contraseña conforman una llave privada. Un archivo de extensión "cer" se proporciona como el componente de llave pública. En facturación electrónica, el uso de esta criptografía es en la generación de una factura, ya que esta debe firmarse. Solamente la llave privada sirve para firmar. Sin embargo, la llave pública permite validar que la firma se ha realizado correctamente y es válida. Esto permite determinar si la factura es verdadera o es apócrifa, permitiendo tener certeza a la hora del cálculo de los impuestos a partir de la facturación.

Pagos en Bitcoin

En el caso de las transacciones de Bitcoin ocurre un proceso similar, se utiliza la llave privada para firmar la transacción, firma que será fácilmente verificable por cada nodo de la red.

Debido a estas características, las llaves siempre se generan en pares, pública y privada. Puede resultar evidente que la llave privada debe mantenerse en absoluto secreto, porque quien la posea podrá generar transacciones.

En el capítulo referido a registros inalterables tratamos los números hexadecimales, los cuales consisten en

16 símbolos posibles: 0 1 2 3 4 5 6 7 8 9 A B C D E y F. En Bitcoin, debido al largo que implicaría presentar las llaves pública y privada, se decidió usar otro sistema denominado Base58, el cual permite generar un número más corto, agrupando los bits y usando mayor cantidad de símbolos. Siendo algo más puristas, las direcciones usan una ligera variación del algoritmo Base58 estándar, denominada Base58Check, la cual incluye bytes de código de comprobación así como información de la versión de la dirección.

También en este caso, y exclusivamente en este libro, agrupamos el texto cada cuatro caracteres para una mejor lectura

en dispositivos móviles.

Direcciones Bitcoin

Por ejemplo la siguiente tabla se muestra una dirección de Bitcoin (generada a partir de la llave pública) junto con la llave privada correspondiente (transformada en un formato legible).

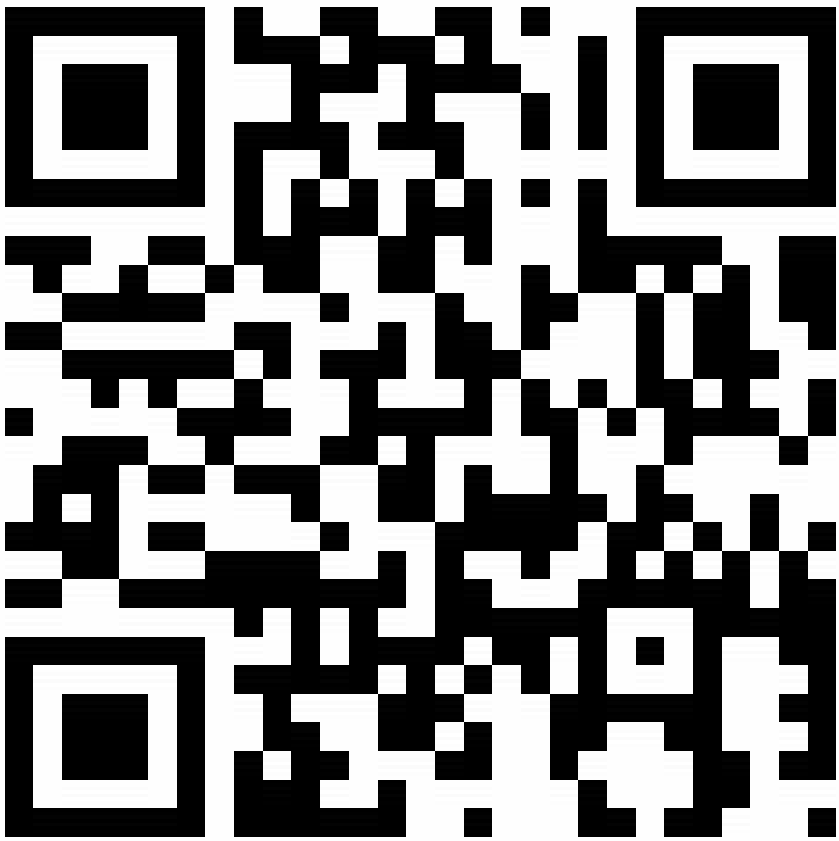
Dirección Bitcoin:	**12q7 HJP6 LFwM HFWC ogVz jq7B sHt8 tqWf ur**
Llave Privada:	B94D 27B9 934D 3E08 A52E 52D7 DA7D ABFA C484 EFE3 7A53 80EE

	9088 F7AC E2EF CDE9

Esto significa que si alguien recibe dinero a la dirección anterior puede transferirlo usando la llave privada correspondiente. Advertencia: asegúrate de no transferir nada a esa dirección, como cualquiera que lea este libro tiene acceso a la llave privada, podrá transferir el dinero a una cuenta propia. Lo mismo ocurre con cualquier llave privada generada con una semilla que no sea aleatoria[19].

Para que sea más fácil de leer estas llaves, suelen usarse códigos bidimensionales que se pueden escanear con un dispositivo móvil.

La representación bidimensional de la dirección pública anterior es la siguiente:



Únicamente el poseedor de la llave privada puede hacer movimientos. Esto significa que si alguien solamente conoce una llave pública no tiene información suficiente para "retirar"

dinero de la cuenta. De hecho, en las una red blockchain no existe el retiro, esto es, que un tercero diferente del propietario pueda hacer una transacción y decrementar el total de la cuenta. Esto es diferente de lo que ocurre con las cuentas bancarias, donde el propio banco puede retirar dinero para el cobro de su mensualidad al cuentahabiente, o bien para el pago a empresas a través de las cuales el cuentahabiente suscribió un servicio de domiciliación (agua, energía eléctrica).

Creando tu cuenta Bitcoin

¿Qué necesito para poder "abrir una

cuenta" de Bitcoin?
La realidad es que no necesitas nada más que un programa de computación que sea capaz de generar el par de llave pública y privada a partir de un número aleatorio muy grande (denominado **semilla**). Siempre que le solicitamos a un programa que genere una llave pública y privada se genera un par diferente. Puede parecer extraño, pero no se necesita más que una computadora, incluso sin conexión a Internet, para generar un par de estas llaves.

Como son tantas las posibles combinaciones de direcciones la cuenta que vas a generar con seguridad será nueva y tendrá cero en su balance

inicial. De lo contrario se hubiera producido una colisión.

¿Qué probabilidad hay de que se dé una colisión así?
Para que exista una colisión, que se vuelva a generar una llave pública y privada igual a alguna que ya tenga saldo en bitcoins, se tiene una probabilidad menor a una en un octillón. Muchos eventos apocalípticos se estiman en probabilidades muy superiores a ese valor, por lo cual se considera uno de los sistemas más seguros de generación de cuentas, siempre y cuando se parta de una semilla suficientemente aleatoria. Algunos programas como el del sitio

bitaddress.org usan la posición del ratón sobre la pantalla para generar valores aleatorios, y cuando tienen suficiente cantidad generan el par de llaves necesarias.

Cuando comenzó el funcionamiento de la red de Bitcoin el monto total que existía era de cero bitcoins. Posteriormente, a través de ciertas reglas se fueron produciendo nuevos bitcoins, ya conocerás dichas reglas cuando lleguemos al concepto de consenso distribuido.

Como puedes ver, una "cuenta en Bitcoin" es muy diferente a una cuenta bancaria. La tabla que sigue presenta las

diferencias existentes:

Cuenta Bancaria	**Cuenta Bitcoin**
Contraseñas centralizadas	Llaves privadas basadas en algoritmo
Recuperación de contraseña a través de la entidad central	No hay recuperación de llave privada en caso de extravío
Usualmente única cuenta	Posibilidad de generar pares de llaves prácticamente ilimitados (un octillón de direcciones)
Transacciones	Transacciones públicas

privadas y protegidas	y rastrables con exploradores

***Citando a Satoshi**:*

"Definimos una moneda electrónica como una cadena de firmas digitales. Cada dueño transfiere la moneda al próximo al firmar digitalmente un hash de la transacción previa y la clave publica del próximo dueño y agregando estos al final de la moneda. Un beneficiario puede verificar las firmas para verificar la cadena de propiedad." Satoshi Nakamoto, 2008.

Transacciones

Ahora ya tienes tu dirección Bitcoin pero tu balance es cero. No tienes bitcoins. Pero tienes una amiga, Ana, que sí tiene. Ella necesariamente tiene otra dirección Bitcoin y una llave privada asociada. Puede hacerte un envío.

¿Cómo funciona? Supongamos que Ana usa una billetera Bitcoin que funciona en su dispositivo móvil. Esto es lo que hará para enviarte bitcoins:

1. Ella indica en la aplicación de billetera que quiere transferirte 0.5 bitcoins

2. Da aceptar al mensje de confirmación que le aparece (en ocasiones le pide un pin de confirmación)
3. La aplicación de billetera firma digitalmente un mensaje dentro de su dispositivo (puede hacerlo porque tiene internamente la llave privada)
4. La aplicación ahora se comunica con un nodo de la red, y envía el mensaje
5. El mensaje de ese nodo se propaga entre los demás nodos de la red
6. Los nodos tienen capacidad para validar el mensaje, si es válido, lo colocan en una lista propia de

transacciones pendientes

Alguien tiene que encargarse de procesar esas transacciones, de lo contrario no habrá manera de que la red funcione y tu recibas tus bitcoins.

Esto es lo que se ve en el cuarto Pilar qué consiste en el consenso distribuidor. Básicamente veremos Cómo hacer para que se genere un nuevo bloque del blockchain.

***Citando a Satoshi**:*
"Aunque sería posible manipular monedas individualmente, sería difícil de manejar el hacer una transacción por cada centavo en una

transferencia. Para permitir que el valor se divida y se combine, las transacciones contienen múltiples entradas y salidas. Normalmente habrán o una sola entrada de una transacción previa más grande o múltiples entradas combinando cantidades más pequeñas, y al menos dos salidas: una para el pago, y una para devolver el cambio, si es que hay algún cambio, de vuelta al emisor." Satoshi Nakamoto, 2008.

Resguardando las llaves privadas

Un gran problema que se presenta es que teniendo la llave privada es suficiente para hacer las transacciones. Por lo cual si alguien roba ese número será suficiente para que tenga el poder de mover nuestros bitcoins. Y aquí hay un problema importante: en Bitcoin una vez que se realiza una transacción esta no se puede cancelar ni existe una institución a la que podamos reclamar.

Si usáramos la llave privada en una computadora conectada a Internet que estuviera siendo espiada para conocer las teclas presionadas alguien podría hacerse de nuestra llave privada y apropiarse de todo nuestro balance en bitcoins.

Billeteras de Hardware

Por lo anterior, para la generación de este tipo de llaves se sugiere utilizar equipos desconectados de Internet, pero aún así tenemos un problema adicional cuando tenemos que enviar una transacción debemos hacerlo a través de una computadora que esté conectada.

Son así populares las denominadas **billeteras de hardware** que en esencia permiten realizar las firmas de las transacciones dentro de su hardware, sin permitir jamás acceso al software de la computadora donde están conectadas. Lo

que surge del hardware es una transacción ya firmada y la computadora solamente realiza el envío de la transacción, siendo imposible que un agente externo pueda extraer la llave privada.

Algunas de estas herramientas son:

- Trezor
- Ledger Nano S
- Keepkey

Claro que cabe preguntarse que pasa si pierdes el dispositivo y cómo hacer para recuperar los bitcoins[20].
Para recuperar las llaves existe un procedimiento que se basa en la frase semilla.

La frase semilla

La mayoría de las billeteras criptoactivos utilizan una frase semilla acompañada de una contraseña para poder generar la llave privada. Esta frase se compone de una serie de palabras en inglés que pueden ser recordadas, como por ejemplo:

> *main priority hole reject trophy private crystal option vendor three creek chase cabbage throw similar*

Usando criptografía de una forma que

escapa a lo que buscamos explicar en este libro, se puede derivar en llaves privada y dirección pública de Bitcoin (existen varios pares que pueden generarse desde una frase semilla, dependiendo de la técnica usada por la billetera). Por lo tanto la frase semilla es un sustituto más fácilmente legible (y recordable) que una clave privada. La misma frase semilla usada en el mismo tipo de billetera permitirá acceder a los bitcoins guardados, aunque la billetera original se haya destruido.

Resguardar la frase semilla implica los mismos problemas que resguardar la llave privada, sin embargo en algunos casos puede aprenderse de memoria:

aunque si la llegáramos a olvidar, no tendríamos acceso nuevamente a los bitcoins de esa dirección[21].

Multifirma

Un problema que existe con el manejo de las firmas de Bitcoin es que si en lugar de ser personas son organizaciones las que quieren manejar las cuentas, un requerimiento frecuente será que para realizar una transacción sean necesarias en forma obligatoria dos o más personas (dos o más firmas). Por esta razón se creó un mecanismo para realizar transacciones requiriendo multifirma.

Bitcoin permite transacciones multifirma, que pueden requerir del total de las llaves existentes, o de una parte de esas llaves. Por ejemplo tú, tu hermana y tu padre pueden tener cada uno diferentes llaves, pero usando dos cualesquiera de esas llaves en forma simultánea será suficiente para firmar una transacción y por lo tanto transferir Bitcoins.

El transcurso del tiempo

Si lo has notado, hasta ahora todo lo que hemos descrito de la blockchain es prácticamente estático. El tiempo no ha transcurrido en nuestros ejemplos con la

excepción de que en ocasiones hemos hablado de dos o tres bloques sucesivos, pero nunca hemos explicado como aparecen dichos bloques en la cadena. En lo que sigue vamos a meternos en el motor que hace que la blockchain funcione: el consenso distribuido.

Notas:

[19] - Ver acerca de la "semilla" más adelante en ¿Qué necesito para poder "abrir una cuenta" de Bitcoin?

[20] - Algunas personas creen que el dinero se almacena en la billetera de hardware. Recordemos que los bitcoins que tienes son solamente un balance en la blockchain. La billetera en realidad es un llavero: guarda llaves y ayuda a

firmar transacciones.

[21] - La probabilidad de volver a lograr encontrar esa dirección es de una en un octillón, a menos que recordáramos buena parte de la frase semilla, pero de todas formas estaríamos en problemas y solamente la suerte podría ayudarnos.

Cuarto Pilar: Consenso Distribuido

Leído hasta este punto del libro ya sabes qué es el libro [contable] distribuido. Has aprendido que las funciones hash se usan para que no puedan alterarse los registros que se dejan en ese libro. También conoces que para realizar pagos se tienen que realizar firmas digitales. Pero aún nos quedan muchas interrogantes. En este capítulo vas a terminar de descubrir las cuestiones que han ido surgiendo al visitar los pilares anteriores. Eso te enfrentará a nuevos conceptos, porque en particular este capítulo incluye muchos detalles clave

del funcionamiento de la red Bitcoin y la forma en que cambia su cadena de bloques.

Las reglas del juego

El funcionamiento de la red blockchain de Bitcoin es como un juego. Puedes imaginarlo como un juego de mesa, un juego virtual colaborativo o incluso un deporte como el fútbol. Hasta ahora, solamente hemos presentado a los participantes. Para que el juego comience todos debemos tener claras las reglas. Cuando el juego avanza entre los participantes realmente comienza a sentirse el transcurso el tiempo. En

algunos juegos, este avance ocurre por turnos de cada jugador. En otros ocurre cuando alguien desplaza la pelota a través del campo. En uno y otro caso hay reglas que todos deben cumplir. Para asegurar el cumplimiento, en los deportes profesionales existe también un árbitro. En Bitcoin ese árbitro no existe en forma de una persona u organización, es el software, cuyo código ha sido acordado en forma colectiva, el que hace que las reglas se cumplan. Esto se desarrolla en el quinto pilar. Ahora veamos como ocurre el transcurso del tiempo en una cadena de bloques.

Agregando Bloques

¿Quién agrega los bloques a la cadena? Una solución muy sencilla es elegir un ente centralizado que los agregue, en definitiva, un árbitro. Sin embargo, al ser centralizado el sistema, podría perder muchas ventajas que ofrece blockchain. Pero aún así, se considera una opción válida para ciertos casos de aplicación. Este tipo de reglas de consenso se denominan prueba de autoridad, ya que hay una autoridad central que gobierna la creación de bloques. Por ejemplo, algunas redes blockchain tienen sus ambientes de prueba funcionando de esa forma.

Bitcoin no funciona de esa manera. En Bitcoin, a cualquier nodo se le permite

crear bloques. Pero para hacerlo, tiene que ganarse el derecho de agregar un nuevo bloque. Eso es parte de las reglas de este juego del Bitcoin. Estas reglas se denominan **consenso distribuido**, que es el conjunto de criterios utilizados para que todos los participantes, los nodos, estén de acuerdo en cual es el estado actual de la cadena de bloques. De alguna forma se debe llegar a un consenso, porque todos tienen que tener claro cuál es el estado actual. En un deporte, las reglas del juego aseguran que todos tengamos claro cual es el marcador actual. Si en el baloncesto un partido va 75 a 59, ese es el estado actual del partido. Todos lo aceptamos, tanto porque vemos el marcador en el

estadio como porque entendemos que el árbitro ha aceptado que ese estado es correcto. Es un consenso.

En Bitcoin se busca también el consenso respecto al estado de la cadena, pero en este caso el concepto probablemente sea bastante más complejo. Se han propuesto varias formas de establecer ese consenso pero en particular la que usa Bitcoin es una de las que se consideran más creativas. Y aunque tiene muchas ventajas también tiene inconvenientes[22].

Una forma de establecer los criterios es a través de los atributos de cada bloque. El objetivo principal de crear nuevos

bloques es agrupar transacciones. En el capítulo sobre las firmas digitales aprendiste que cuando haces un pago con Bitcoin, envías a toda la red Bitcoin una transacción firmada con tu llave privada, la cual se coloca en un listado de transacciones pendientes.

Si tienes un nodo de Bitcoin y quieres crear un nuevo bloque, buscarás algunas transacciones de esa lista, las que quieras, y las agregarás a tu bloque candidato. Recuerda que ese bloque candidato debe contener el hash del bloque previo, por lo cual debes conocer perfectamente cuál es el estado actual de la blockchain y en particular cual es el último bloque y su hash.

El reloj de tu nodo está sincronizado con toda la red, por lo cual no tendrás problema en incluir la marca de tiempo al bloque. Agregas los demás atributos y calculas el hash de todo el bloque y tienes un bloque que, considerando otros criterios que en un momento veremos, puedes agregar a la blockchain. Pero has gastado tiempo y dinero para hacer esto. ¿por qué lo harías? Se requiere que tengas un incentivo.

Prueba de Trabajo

¿Por qué alguien estaría interesado en agregar bloques a la cadena de Bitcoin?.

Se requiere una motivación, algo que provoque ese dinamismo para generar los bloques, de lo contrario todo nuestro mapa de miles de nodos podría quedarse estático, sin producir. Se requiere un incentivo. Ese incentivo es la creación de nuevas unidades de bitcoins, que se asignan al que genera un bloque válido en la cadena. Sí, al agregar un nuevo bloque, por un momento te conviertes es una especie de banco central de la blockchain, emitiendo tus propios bitcoins que serán considerados por todos los miembros de la cadena como válidos.

Bloques válidos

Eso nos lleva a otro problema, ¿quién agrega el bloque? Todos querrán llevarse el premio. Una forma de solucionar quien gana este premio, es aprovechando el hecho de que cada bloque de la cadena tiene un hash, y poniendo alguna regla especial sobre ese hash. Por ejemplo imaginemos tenemos el bloque 150 de la siguiente forma (simplificado para su comprensión):

Número de bloque	**150**
Nonce:	0
	Ana envía 100 Bitcoins a Juan

Datos	Pedro envía 150 Bitcoins a Mario
HashPrevio	7ed9 3d2b 7c62 ab8e ddbd 8a23 6b23 809d
Hash	C14A 09C2 97D4 F6DC AF00 843C 4399 19DD C50C 0A53 BBAC 91F6 C6B7 86E3 11AE A4E1

Pero exigimos a quien vaya a crear el bloque, que debe hacerlo cumpliendo la regla de que el hash comience con cuatro ceros[23]. La forma para lograrlo implica cambiar algún dato que aparezca dentro del bloque. No podremos modificar valores en cada transacción, ni el hash previo, pero el

parámetro denominado nonce si lo podemos cambiar. En lugar de cero le ponemos el valor 1, y nos queda este bloque:

Número de bloque	**150**
Nonce	1
Datos	Ana envía 100 Bitcoins a Juan Pedro envía 150 Bitcoins a Mario
HashPrevio	7ed9 3d2b 7c62 ab8e ddbd 8a23 6b23 809d
Hash	07D9 97FF C4B8 03EF 259D A642 3A29 2D8B CFCD 582D 0B24 5C95

pero todavía el hash resultante no comienza con cuatro ceros.

Entonces se nos ocurre una gran idea, buscar a un excelente criptógrafo que nos dé una fórmula matemática para que, partiendo del hash resultado y el resto de la información, nos detecte que número es necesario poner en el campo nonce para que nos dé el hash correcto, en forma similar a como se resuelve una ecuación matemática.

¿Qué nos dirá este criptógrafo experto? Sencillamente que no es posible. El cálculo de un hash está realizado por un

algoritmo de una sola vía, solamente podemos calcular y obtener el resultado, no existe una función inversa a un hash. Lo cual es bastante razonable, al considerar que cuando se obtiene el hash se reduce toda la información a una cadena de unos pocos bytes. El pasaje de los datos a través de intrincadas tablas que transforman la información, hace que no pueda hacerse el proceso reversible. Así fueron diseñadas las funciones hash. En definitiva, solamente se puede usar lo que se denomina "fuerza bruta", intentar una y otra vez, como hace un ciberdelincuente que quiere descubrir una contraseña de un sistema.

Sin embargo, nos da una sugerencia: automatizar el cambio del valor del nonce para que una computadora lo vaya incrementando, hasta que llegue al valor correcto en el cual el hash comienza con cuatro ceros. Y lo hacemos, la computadora comienza a calcular y luego de un tiempo nos arroja este resultado:

Número	**150**
Nonce	136652
Datos	Ana envía 100 Bitcoins a Juan Pedro envía 50 Bitcoins a Mario
	7ed9 3d2b 7c62 ab8e

HashPrevio	ddbd 8a23 6b23 809d 4173 7502 415b 5fc1 126e 72cc 2194 09be
Hash	0000 f141 0ba7 914f 08b4 1ae0 e095 3b37 5598 dbe5 d8dd e8b3 64d4 31c0 7c42 e588

Lo logramos, después de iterar hasta el número 136652, al final hemos generado un bloque que comienza con el número de ceros definido en la regla. Como todos estamos de acuerdo con las reglas desde el inicio, tenemos consenso. Esta forma de llagar a ese consenso se llama prueba de trabajo (PoW, por sus siglas en inglés).

***Citando a Satoshi**:*
"La prueba de trabajo envuelve la exploración de un valor que al calcular un hash, tal como SHA-256, el hash empiece con un número de bits en cero." Satoshi Nakamoto, 2008.

Esto es justamente lo que se le pide a cada nodo, lo cual obliga a gastar en procesamiento intensivo para llegar primero al cálculo. Esta operación de estar buscando el hash que cumpla con la regla se le llama **minería**, porque consiste en buscar el hash correcto una y otra vez de la misma forma en que una

mina se pica la piedra para encontrar oro. Se les llama mineros a las personas que operan estos nodos[24].

Se denomina minería en Bitcoin al proceso de buscar la generación un bloque de transacciones cuyo valor hash resultante cumpla con la regla de dificultad válida en ese momento, lo cual implica que el hash debe comenzar con determinada cantidad de ceros.

De esta forma un **bloque válido** es aquel que incluyendo el hash previo y una serie de transacciones tiene un hash que comienza con cierta cantidad de ceros.

Avisar lo antes posible

Cuando un minero encuentra el hash que cumple las condiciones, lo comunica al resto de la red. Esto debe ser lo antes posible, ya que de lo contrario otro minero podrá encontrar otro hash que cumpla el criterio de dificultad y la mayoría de los nodos comenzará a colocar sus bloques sobre ese bloque alterno. Si llegas tarde, tu bloque no será ni siquiera considerado.

Si se producen dos bloques casi en simultáneo, usualmente existe uno de los dos que se lleva el apoyo de la mayoría

de los nodos consigo y generan un bloque o dos siguientes antes que los nodos anteriores. En definitiva una de las dos ramas pasa a formar una **cadena más larga** y esa es la válida. Si eres minero y generaste bloques en la cadena que quedó más corta, entonces esos bloques no se considerarán como parte de la cadena más larga y por lo tanto tu balance no es válido: el balance válido de bitcoins es el que está en la cadena más larga.

En Bitcoin los balances válidos son los que pertenecen a la cadena más larga. Las demás cadenas en algún momento dejarán de recibir bloques y quedarán huérfanas.

Los premios tienen nombre

¿Por qué razón no podría otra persona copiar ese bloque y reclamarlo como suyo? Cada nodo de un minero tiene una dirección propia asociada. Cuando genera el bloque, pone esa dirección en un atributo del bloque denominado **coinbase**. Esa dirección es la que gana el premio de los bitcoins generados.

Cuando el minero calcula el hash del bloque lo hace incluyendo en los datos ese campo, por lo cual si un segundo minero quisiera generar un bloque idéntico, tendría que poner en ese campo

la dirección del primer minero: lo cual estaría diciendo que es el primer minero el que gana los bitcoins, no él mismo. Su alternativa es cambiar ese campo por la dirección propia, pero el hash cambiará, entonces tendrá que volver a minar el bloque, para lo cual ya es tarde porque ha habido un ganador antes: el primer minero.

***Citando a Satoshi**:*
"Incentivo: Por convención, la primera transacción en el bloque es una transacción especial que genera dinero nuevo cuyo dueño es el creador del bloque. Esto agrega un incentivo para que los nodos apoyen a la red, y provee una forma inicial

de distribuir monedas en circulación, dado que no hay una autoridad para crearlas. Esta adición estable de una cantidad constante de monedas nuevas es análoga a mineros de oro gastando recursos para agregar oro a la circulación. En nuestro caso, es el tiempo del CPU y la electricidad que se gasta." Satoshi Nakamoto, 2008.

El valor del incentivo

Cuando nació Bitcoin, el pago a cada minero consistía en 50 bitcoins. Sin embargo la regla establece que cada 210,000 bloques el pago se divide entre

dos. Podemos verlo en los exploradores, herramienta que ya usamos previamente:

Altura de bloque	**209999**
Marca de tiempo	2012-11-28 15:01:40
Nonce	282240624
Hash	0000 0000 0000 00f3 8191 6464 5360 294b 5dee 7f2e 8460 01ac 9f41 a70b 7a9a 3de1
Bloque previo	0000 0000 0000 00c6 d9b5 7b9d b3f3 18d9 a308 0a61 82af a437 18f4 5cdf 9624 48ac

Total de transacciones	543
Premio de Bloque	50 BTC

Vemos que se generó para el minero un total de 50 BTC (premio de bloque). Ahora veamos el siguiente bloque:

Altura de bloque	**210000**
Marca de tiempo	2012-11-28 15:24:38
Nonce	4069828196
Hash	0000 0000 0000 048b 9534 7e83 192f 69cf 0366 0763 36c6 39f9

	b722 8e9b a171 342e
Bloque previo	0000 0000 0000 00f3 8191 6464 5360 294b 5dee 7f2e 8460 01ac 9f41 a70b 7a9a 3de1
Total de transacciones	457
Premio de Bloque	25 BTC

Avancemos otros 210,000 bloques (casi cuatro años) para encontrarnos con este bloque, el último en el que se pagan 25 bitcoins:

Altura de bloque	**419999**

Marca de tiempo	2016-07-09 16:41:53
Nonce	2544228497
Hash	0000 0000 0000 0000 0303 5bc3 1911 d3ee a46c 8a23 b36d 6d55 8141 d1d0 9cc9 60cf
Bloque previo	0000 0000 0000 0000 046b c4b7 b377 29ce 5a94 cf12 e02b 3aea f994 374b ff2e 509d
Total de transacciones	1
Premio de Bloque	25 BTC

y veamos el siguiente bloque:

Altura de bloque	**420000**
Marca de tiempo	2016-07-09 16:46:13
Nonce	2193437364
Hash	0000 0000 0000 0000 02cc e816 c0ab 2c5c 269c b081 896b 7dcb 34b8 422d 6b74 ffa1
Bloque previo	0000 0000 0000 0000 0303 5bc3 1911 d3ee a46c 8a23 b36d 6d55 8141 d1d0 9cc9 60cf
Total de	1257

transacciones	
Premio de Bloque	12.5 BTC

En el cual solamente se pagan 12.5 BTC, lo cual seguirá siendo pagado a los mineros hasta mediados del año 2020[25].

Evolución de la cadena

A través de la prueba de trabajo, los nodos de la red tienen una forma de que la cadena crezca cada cierto tiempo. Sin embargo aún no hemos visto como regular ese tiempo ¿podrían crearse

bloques tan rápidamente que se genere confusión entre cuál es el siguiente bloque? O por el contrario ¿podría ocurrir que nos tardáramos días o meses en encontrar el siguiente bloque válido?

Las reglas del juego establecen un mecanismo de **ajuste de dificultad** para que el **tiempo promedio de bloque** sea de unos 10 minutos. Ese ajuste de dificultad consiste en revisar cada 2016 bloques cuanto tiempo tardaron en producirse los bloques. Si los bloques se hubieran producido cada 10 minutos, se debió tardar dos semanas en generar el total de 2016.

Si esos últimos 2016 bloques tardaron

menos de dos semanas en producirse, se aumenta la dificultad de producir bloques. Por el contrario si tardaron más de dos semanas, se disminuye la dificultad para que puedan generarse más rápido. Esto afecta al número de ceros que debe tener un hash al principio para considerarse un bloque válido. Cuanto más cantidad de ceros, mayor dificultad y cuanto menor cantidad de ceros, menor dificultad de conseguir el bloque.

De esta forma, en promedio, los bloques deben generarse cada 10 minutos. Veamos por ejemplo el promedio de los bloques desde el 12000 al 12010:

Bloque	Marca de tiempo	Diferencia en minutos
120000	2011-04-24 23:20	
120001	2011-04-24 23:28	8.25
120002	2011-04-24 23:36	8.30
120003	2011-04-24 23:43	6.48
120004	2011-04-25 00:03	20.35
120005	2011-04-25 00:05	2.45
120006	2011-04-25 00:16	10.92

120007	2011-04-25 00:17	0.92
120008	2011-04-25 00:28	10.48
120009	2011-04-25 00:46	18.27
120010	2011-04-25 00:56	9.57
Total:		95.98

Vemos que uno de los bloques tardó más de 20 minutos en generarse, mientras que otro lo hizo en menos de un minuto. Sin embargo, en total para producir los 10 bloques del 120001 al 120010 la red tardó casi 96 minutos, lo que hace un

promedio de 9.6 minutos muy cercano a los 10 minutos que se buscan como promedio.

El Consenso Distribuido consiste en buscar el conjunto de reglas de juego para que la blockchain evolucione con el tiempo. ¿Con que frecuencia?. Eso depende, pero podríamos buscar que en promedio ocurra cada cierto tiempo, por ejemplo, en el Bitcoin cada bloque se genera, en promedio, cada 10 minutos[26].

Cumpliendo las reglas del juego cualquiera puede hacer cambios, evitando una situación en que cada nodo modifique su libro y al día siguiente

todos estén en un estado diferentes.

La codicia castigada

Quizás te has preguntado, que ocurre si en lugar de crear 50 bitcoins, decides en tu bloque agregar 900 bitcoins. Piensas que finalmente obtendrás más dinero. Sin embargo, el número de bitcoins que se pagan es también parte de las reglas de Bitcoin. Si comunicas al resto de los nodos un bloque en el cual te pagas 900 bitcoins, los nodos verán ese bloque que has creado como no válido y simplemente lo ignorarán.

Tus pagos en espera

Cuando realizas una transacción de pago en bitcoins esta no se procesa como una tarjeta de crédito a través de un servidor central. Tienes que esperar. No puedes obligar a que la transacción sea tomada en el siguiente segundo. Lo que esperas es que algún minero logre encontrar el hash de acuerdo a la dificultad definida, y entonces la red tiene un bloque válido que, si has tenido suerte, incluye esa transacción. O tendrás que esperar al siguiente bloque.

Si la red se encuentra muy saturada, hay demasiadas transacciones para ser procesadas, puede tardarse más el pago.

Y recordemos que el tiempo promedio de generación de cada bloque es de 10 minutos.

Seis confirmaciones

La espera es en realidad más larga. El estándar de número de confirmaciones en las cuales se considera que la transacción no puede revertirse es de seis. Esto equivale a aproximadamente una hora de espera para que el pago se realice completamente. Otras redes blockchain tienen tiempos de bloque promedio diferente, eso lo podrás ver más adelante en el libro.

Comisiones

Dentro de las reglas de consenso se incluyó la posibilidad de que cada usuario que quiere realizar una transacción pague una comisión por la misma para hacerla más atractiva a los mineros y que sea incluida en los siguientes bloques. Cabe comentar que durante las épocas de mayor volatilidad las comisiones de Bitcoin han sido relativamente altas: de hasta 50 dólares americanos. Podrías ofrecer valores más bajos, pero tu transacción quedaba horas esperando a ser tomada. Otros criptoactivos han aprovechado esto para ofrecerse como alternativas más económicas para hacer transacciones

que el Bitcoin.

El proceso completo

Ya conoces el cuarto pilar: el consenso distribuido que en Bitcoin se logra con la prueba de trabajo. Antes de visitar el quinto pilar, cerremos la sección con una cita:

***Citando a Satoshi**:*
"Los pasos para gestionar la red son como sigue:
1) Transacciones nuevas son emitidas a todos los nodos.
2) Cada nodo recolecta nuevas

transacciones en un bloque.
3) Cada nodo trabaja en encontrar una prueba de trabajo difícil para su bloque.
4) Cuando un nodo encuentra una prueba de trabajo, emite el bloque a todos los nodos.
5) Los nodos aceptan el bloque si todas las transacciones en el bloque son válidas y no se han gastado ya.
6) Los nodos expresan su aceptación del bloque al trabajar en crear el próximo bloque en la cadena, utilizando el hash del bloque aceptado como el hash previo."
Satoshi Nakamoto, 2008.

Notas:

[22] - Mencionamos el más conocido en la parte II como Ataque del 51%

[23] - Esta regla es arbitraria para el ejemplo, en Bitcoin son más ceros y la dificultad es variable.

[24] - Personalmente creo que es generar confusión cuando en muchos artículos de Internet y metáforas usadas para explicar blockchain, que los nodos de los mineros se dedican a resolver "una serie de complejos problemas matemáticos". Un problema matemático complejo suele implicar la aplicación de diferentes técnicas con un profundo conocimiento de la teoría, algo que por ahora, solamente los humanos hacen (la Inteligencia Artificial va hacia ese camino...). Sin embargo, lo que hace un

nodo minero es una cantidad masiva de cálculos matemáticos claramente predefinidos en busca de una coincidencia numérica. Si eres desarrollador de software, puedes escribir el código de un programa de ese tipo en minutos.

[25] - Esta disminución periódica del monto de pago a los mineros será explicada en la parte II de este libro.

[26] - Otras redes blockchain tienen tiempos promedio de bloque diferentes, en general más breves, esto será tratado en la parte II.

Quinto Pilar - Código común

Todas las reglas que aparecen previamente en los pilares anteriores deben encontrarse en algún lugar.
Si no hay una entidad central que las contenga ¿cómo puede asegurarse su cumplimiento?.

Se requiere que de alguna forma se asegure que cada nodo se comporte coherente con las reglas establecidas de consenso distribuido, que la comunicación sea establecida de la misma forma, que la cadena de bloques se almacene en forma consistente para

que no existan diferencias posteriores al comunicarse con otro nodo.

Cada registro de la cadena de bloques debe contener la información suficiente en cada nodo, aunque la almacenen en forma diferente. En definitiva, debe buscarse algo que asegure el funcionamiento correcto de la red. Y esa responsabilidad recae en el software que debe ejecutar cada nodo.

El software se escribe con código en algún lenguaje de programación previamente seleccionado. Ese código debe contener todas las reglas del juego de la red blockchain. El quinto pilar, el código común, es clave para que una red

blockchain funcione, siendo también lo que sustituye en cierta forma la necesidad de una entidad central.

Todos los participantes deben conocer ese código. Todos deben poder ver las reglas, y poder "compilar" el código en su computador. La mejor manera de hacer esto es utilizando código abierto. Así es como ocurre en el caso de la red Bitcoin. En la siguiente sección abordamos la filosofía de código abierto, y explicamos por qué es una de las claves para la existencia del Bitcoin y la mayoría de las criptomonedas.

Todas las reglas y técnicas de funcionamiento de una red

blockchain se encuentran en un código de programación común, que todos los participantes pueden leer. La confianza se traslada de un intermediario al código común.

El Código Abierto

Todo programa de cómputo debe escribirse en algún lenguaje de programación. A nivel más bajo, en el "idioma de las máquinas" se encuentra el Lenguaje Ensamblador. Básicamente es una serie de ordenes codificadas de forma que un valor específico corresponde a cierta orden. En la

década de los 80s tuve la suerte de programar en lenguaje ensamblador Z80, un microprocesador que poseían la gran mayoría de las computadoras domésticas de esa época. Luego aprendí a programar en lenguaje ensamblador del microprocesador Intel 8080 (el de las primeras PCs) y posteriormente durante mis estudios de ingeniería en computación en Assembler Sun SPARC, en cada caso con diferencias dadas por la variada arquitectura de esas computadoras. Porque finalmente, si estás hablando lenguaje de máquina, según como sea la máquina, es como debes hablarle.

La mayoría de los programadores

jóvenes en el presente no conocen de lenguaje ensamblador. El desarrollo de software ha evolucionado de tal forma, que se han agregado capas de software encima para que los programadores puedan hablar algo más parecido al lenguaje humano. Así es como surgió la programación estructurada, la programación orientada a objetos y la programación funcional. Nuevos lenguajes de programación con propiedades que permitían trasmitir más fácilmente la "idea" que surge de la mente humana, y que a través de otros programas denominados compiladores, se convertían en lenguaje de máquina.

*El movimiento del **Software Libre** no*

debe confundirse con el ***Código Abierto****. El primero consiste en una serie de principios que proporcionan libertad en torno al código, el segundo en la capacidad de colaborar mediante a la publicación abierta (no restringida) del código. Aún siendo diferentes, es muy común que el código abierto se libere en licencias compatibles con el software libre.*

Cuando comenzó la era de la computación, la mayor parte de los programas de cómputo que se crearon eran ocultos al público en general y en general a los clientes que recibían los programas. Solamente las empresas

conocían ese código fuente, ya sea en ensamblador o en algún lenguaje de programación de más alto nivel, como C, Fortran o Cobol. Surgieron alrededor del año 1970 diferentes movimientos para que el código pudiera leerse. Entre ellos, el más conocido es el movimiento del Software Libre, liderado por Richard Stallman donde se establecieron principios de libertad para el uso del código.

El software de referencia

Al tener un código abierto visible por todos los miembros de la comunidad de Bitcoin, cada uno puede hacer

sugerencias de cambio, correcciones, mejoras para que funcione con mejor calidad. Incluso revisando el funcionamiento de otras redes de blockchain, como Litecoin o Ethereum, se pueden incorporar mejoras tomando las ideas de esos sistemas, en principio manteniendo el funcionamiento general del registro en la cadena de bloques.

En el mundo del software se dice que "el código es ley". En blockchain es más evidente. Esto tiene el sentido de que el código define las reglas que regirán el funcionamiento de la red blockchain de la misma manera que las leyes rigen el funcionamiento de una sociedad. En particular, las reglas de consenso

distribuido son parte de esa ley en la blockchain, lo cual es fundamental que exista para evitar que cualquier persona haga trampa. Podrá intentarlo, pero será fácilmente descubierto.

Bitcoin Core

Bitcoin Core es el software de referencia de Bitcoin. Está programado en el lenguaje C++ y fue originalmente desarrollado por Satoshi Nakamoto, pero ha evolucionado desde sus primeros tiempos y actualmente es desarrollado y mantenido por un numeroso equipo de desarrolladores, entre ellos Wladimir van der Laan,

Gavin Andresen y Cory Fields. El proyecto tiene el apoyo de la Iniciativa de Monedas Digitales del Instituto de Tecnología de Massachusetts (MIT, por sus siglas en inglés).

En el código está escrito todo lo necesario para que la blockchain exista: también se definen las reglas de criptografía necesarias para validar los bloques encadenados, así como para verificar las transacciones firmadas, asegurándose que se encuentran correctas y pueden ser incluidas en un nuevo bloque.

En Bitcoin, al ser código abierto, todo esto se encuentra en el código que

cualquiera puede ver y puede auditar. Gracias a Internet, los desarrolladores pueden encontrarse en cualquier parte del mundo. La mayor parte de los proyectos usan GitHub como repositorio de código, el cual se basa en el software Git creado por Linus Torvalds.

Puedes ver el código directamente desde el repositorio de GitHub bajo el nombre bitcoin/bitcoin. Gracias a que el código se guarda en repositorios Git, todos tienen el historial de cambios y las piezas completas de código para volver a levantar el repositorio en cualquier momento.
Gracias a esos repositorios se pueden monitorear los cambios del código y las

modificaciones que como veremos pueden implicar bifurcaciones que significa que se hacen cambios sobre el código original.

Por ejemplo, en el código de referencia pueden verse las semillas DNS que conocimos al revisar el Primer Pilar, las siguientes líneas[27]:

```
vSeeds.emplace_back("seed.bitcoin.sip
vSeeds.emplace_back("dnsseed.bluema
vSeeds.emplace_back("dnsseed.bitcoin
vSeeds.emplace_back("seed.bitcoinsta
vSeeds.emplace_back("seed.bitcoin.jor
vSeeds.emplace_back("seed.btc.peterto
vSeeds.emplace_back("seed.bitcoin.spi
```

Cambios en el código

Afirmamos que el código es ley, ya que gobierna el comportamiento de toda la red blockchain. ¿qué ocurre si se quieren introducir mejoras o cambios? Cada comunidad de blockchain tiene algún procedimiento para hacerlo. En Bitcoin, existen las denominadas Propuestas de Mejora de Bitcoin (BIP, por su siglas en inglés). Estas propuestas son publicadas y revisadas por la comunidad. En ocasiones estos cambios son para todos muy razonables, y todos los nodos lo aplican.

De esta forma, el código no está estático evoluciona con el tiempo eso significa

que se pueden realizar justamente cambios que mejoran la funcionalidad. Siempre que surjan algunos problemas en la red como lentitud, defectos en el procesamiento de las transacciones, o incluso aspectos de estética o separación lógica del código, el equipo de desarrolladores disperso en todo el mundo puede hacer las correcciones necesarias.

Bifurcaciones

¿Qué ocurre si un grupo de desarrolladores realiza un cambio en el código común? Entonces, si una parte de los nodos no actualizan ese software, se

produce una bifurcación. Una bifurcación puede ser suave (en inglés: soft fork), lo cual significa que nada más se corrige alguna parte del código sin afectar para nada el funcionamiento de la cadena de bloques y los protocolos base.

*Una bifurcación suave (**soft fork**) consiste en el conjunto de cambios de código en cierto número de nodos de la red blockchain, sin afectar la forma en que se almacena la cadena de bloques ni el conjunto de reglas que hace que un bloque sea válido. Los nuevos nodos pueden funcionar conjuntamente con los viejos nodos siendo la misma cadena.*

Pero también puede tratarse de lo que se denomina un hard fork o bifurcación dura lo cual significa que va haber incompatibilidad entre la versión vieja y la versión nueva.

Cuando ocurre esa incompatibilidad si no se cambian todos los viejos nodos a la versión nueva pasan a existir de pronto dos cadenas de bloques válidas una para la versión vieja y otra para la versión nueva.

Por ejemplo, en el año 2017 se realizó una bifurcación de la cadena de Bitcoin que pasó a ser denominada Bitcoin Cash, creándose una nueva

criptomoneda.

*Una bifurcación dura (**hard fork**) consiste en el conjunto de cambios de código que de implementarse en cierto número de nodos de la red blockchain afectará la producción de la cadena de bloques generando en determinado momento un bloque que será válido para los nuevos bloques pero inválido para los viejos bloques (o viceversa). Los nuevos y viejos nodos pasan a funcionar respectivamente sobre cadenas de bloques diferentes, con una colección común de bloques históricos.*

Aunque tiene que existir una versión que se considera "de referencia", el software que va en cada nodo puede escribirse en diferentes lenguajes de programación. Por ejemplo, en el caso de Ethereum, adicional a la versión existente en lenguaje Go, existen versiones escritas en los lenguajes Java y en Rust. Aunque el lenguaje de programación sea diferente, el código tendrá las mismas reglas, traducidas, que la implementación de referencia. Claro que si se encuentran pequeñas diferencias de comportamiento entre las implementaciones, la que se considera válida es la de referencia, siempre y cuando no se trate de un defecto.

El software se hace hardware

Cuando se requiere alta performance en cálculos puede convenir convertir el software en hardware especializado, chips que contienen internamente el código equivalente al software original pero que se encuentran diseñados para trabajar intensivamente con resultados cientos de veces superiores.

A fines del año 2012 y desarrollándose durante los siguientes años, surgieron chips permitieron realizar minado de bloques con tasas de hash muy superiores a las que se podían lograr

con una computadora personal, incluso utilizando tarjetas gráficas[28]. Estos nuevos chips se denominan Circuitos Integrados para Aplicaciones Específicas (ASICs, por sus siglas en inglés).

Existen ya grandes centros de minado, en particular en china, donde se juntan miles de estos dispositivos para generar bitcoins. Es imposible en la práctica competir con ello con una computadora de uso general[29]. Claro que como es hardware, si cambiara el software de referencia entonces estos chips pasarían a ser obsoletos. En la red blockchain Monero se usa la estrategia de cambiar constantemente el software para evitar

que los fabricantes de ASICs puedan crear una para realizar minería de esa moneda con ventajas considerables.

Hemos llegado al final de la revisión de los cinco pilares, viene bien un repaso de la definición propuesta:

" U n **libro distribuido** de **registros inalterables** que incluyen transacciones **firmadas digitalmente**, cumpliendo un conjunto de reglas de **consenso distribuido** y asegurando su funcionamiento en un **código [abierto] común**."

y para concluir, una cita:

***Citando a Satoshi**:*

"Conclusión: Hemos propuesto un sistema para transacciones electrónicas sin depender en confianza. Comenzamos con el marco habitual de monedas hechas de firmas digitales, el cual provee un control fuerte de propiedad, pero es incompleto sino existe una forma de prevenir doble gasto. Para solucionar esto, hemos propuesto una red P2P que utiliza prueba de trabajo para registrar una historia pública de transacciones la cual rápidamente se convierte impráctica computacionalmente para que un atacante pueda cambiar si nodos honestos controlan la mayoría del

poder de CPU. La red es robusta en su simplicidad no estructurada. Los nodos pueden trabajar todos al mismo tiempo con poca coordinación. No necesitan ser identificados, dado que los mensajes no son enrutados a ningún lugar en particular y solo necesitan ser entregados bajo la base de un mejor esfuerzo. Los nodos pueden irse y volver a la red a voluntad, aceptando la cadena de prueba de trabajo como prueba de lo que sucedió mientras estuvieron ausentes. Votan con su poder de CPU, expresando su aceptación de los bloques válidos al trabajar extendiéndose y rechazando bloques inválidos al refutar trabajar

en ellos." Satoshi Nakamoto, 2008.

Notas:

[27] - Código tomado en Agosto de 2018, quitando comentarios.

[28] - Las tarjetas gráficas tienen propiedades que las hacen muy eficientes para el minado de criptoactivos. Durante algunos años se agotaron de la venta justamente debido a la adquisición intensiva por parte de los mineros.

[29] - Existe sin embargo una técnica con la cual se pueden obtener bitcoins indirectamente con computadoras de propósito general, utilizando tarjetas gráficas, mediante el minado de bloques de otras redes blockchain. Esto se verá

en la parte II del libro bajo la pregunta ¿qué otros criptoactivos existen?

Parte II - Preguntas Frecuentes

Seguramente aún te quedarán muchas interrogantes sobre blockchain y el mundo de los criptoactivos. Durante el recorrido por los conceptos centrales del Bitcoin hemos aprendido mucho y te hemos dado respuesta a algunas de ellas. Pero quedan otras por responder. Muchas de las respuestas que se presentan en esta segunda parte se derivan de combinar los conceptos que ya has visto con cierta profundidad en la primera parte.

De todas formas no agotaremos la gran

cantidad de preguntas posibles sobre esta tecnología novedosa, lo que sí podrás afirmar es que terminando este libro estarás preparado para revisar tú mismo en Internet la información existente para encontrar las respuestas que faltan. Ahora los términos usados, los razonamientos seguidos y las opiniones presentadas por los miembros de la comunidad, podrás entenderlas mucho mejor pues será para ti un idioma conocido.

Las preguntas que vamos a responder son:

1. ¿Por qué se afirma que solo existirán 21 millones de bitcoins

como máximo?
2. ¿Qué es la escasez digital?
3. ¿Qué significa en Bitcoin que los pagos son irreversibles?
4. ¿Qué es un ataque del 51%?
5. ¿Qué es una casa de cambio de Bitcoin?
6. ¿Por qué existe un mercado de valor del Bitcoin?
7. ¿Qué fraudes han existido relacionados con Bitcoin?
8. ¿Qué alternativas de Consenso Distribuido existen?
9. ¿Cuál es la definición de criptoactivo?
10. ¿Qué otros criptoactivos existen?
11. ¿Es Bitcoin la criptomoneda de referencia?

12. ¿Por qué Bitcoin ya no es aceptado en algunos sitios de Internet?
13. ¿Qué es Ethereum?
14. ¿Qué es un Contrato Inteligente?
15. ¿Qué es una oferta inicial de moneda (ICO, por sus siglas en inglés)?
16. ¿Qué retos tiene la tecnología blockchain hacia el futuro?

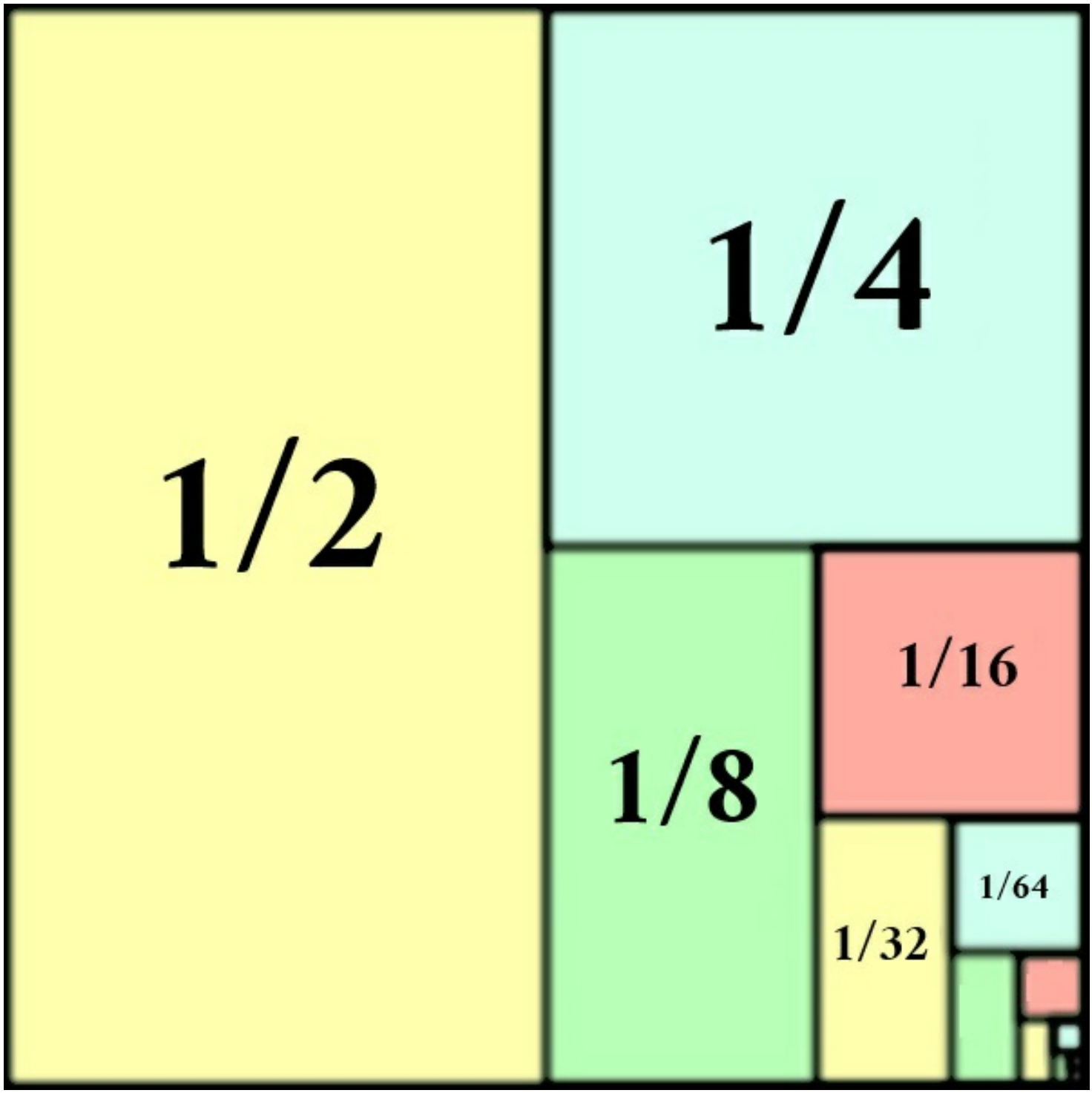
Las respuestas serán muy resumidas porque muchas de ellas abren capítulos completos y podríamos escribir otros libros. Pero te dejamos algunas referencias para que puedas profundizar en el tema.

1-¿Por qué se afirma que solo existirán 21 millones de bitcoins como máximo?

Es momento de que repasemos un poco de matemáticas. Se conoce como serie convergente a una sucesión de valores cuya suma final da como resultado un número fijo y finito.
Por ejemplo si sumamos la sucesión de los números enteros 1,2,3,4 y así sucesivamente, tendremos una suma de esta forma:
suma1 = 1 + 2 + 3 + 4 ...
la cual cómo puedes imaginar tendrá un resultado de valor infinito.

Sin embargo, ¿qué pasa si sumamos fracciones? Por ejemplo la sucesión de valores 1/2, 1/4, 1/8 ...
suma1 = 1/2 + 1/4 + 1/8 + 1/16 ...

La siguiente imagen permite mostrar gráficamente que el resultado final da un total de 1:



Las series como esta se denominan series convergentes, ya que el resultado

converge a un número finito. En Bitcoin, una de las reglas indica que cada 210,000 bloques se divide entre dos el pago a los nodos mineros. Por lo cual se tiene una serie de la siguiente forma:

MaximoDeBitcoins = 50*bloques + 50/2*bloques + 50/4*bloques + 50/8*bloques + 50/16*bloques ....

donde bloques=210,000, esto se puede resumir a lo siguiente sacando factores comunes:

MaximoDeBitcoins = 10,500,000 + 50*bloques * (1/2 + 1/4 + 1/8 + 1/16 ...)

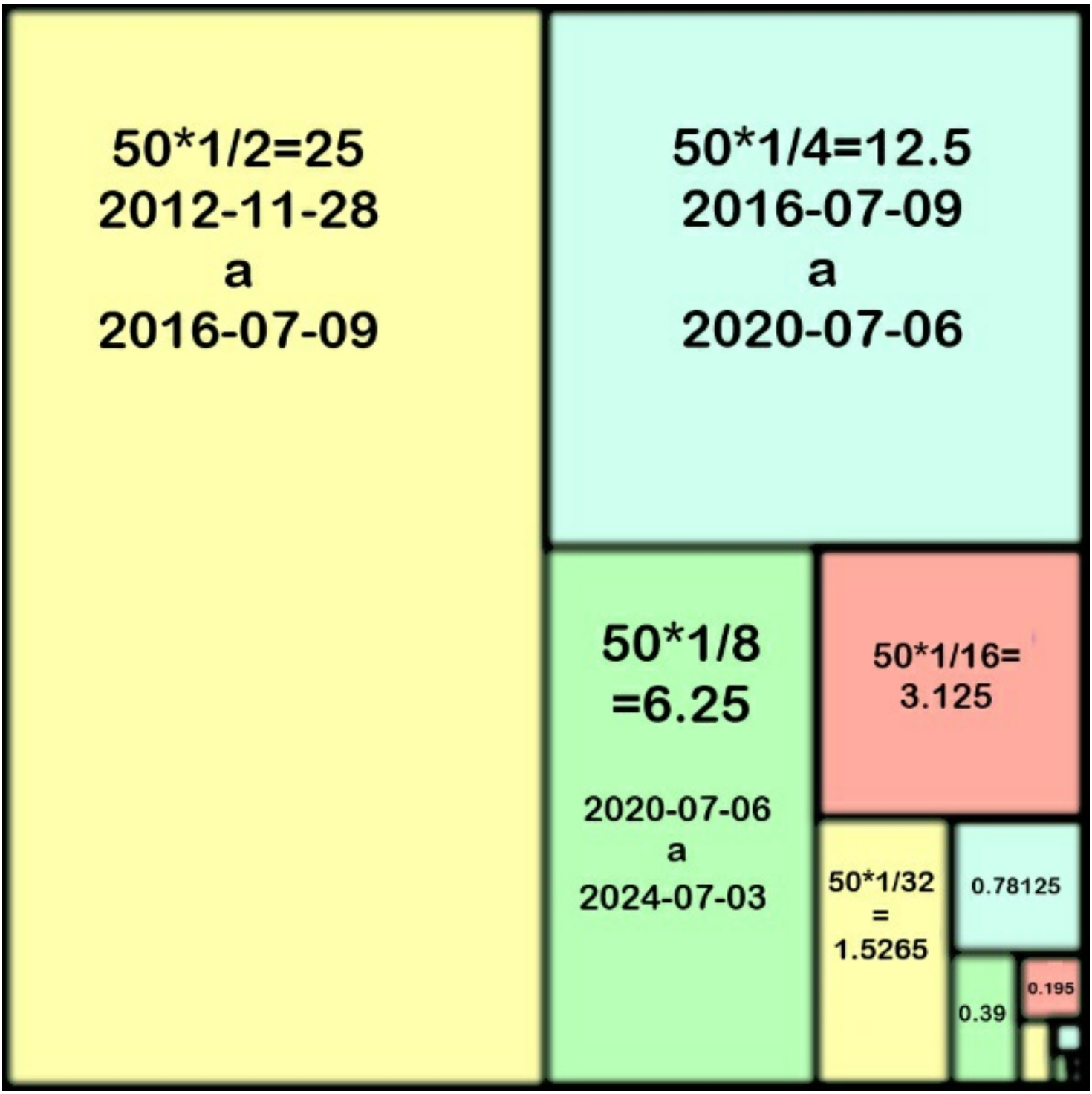
Si te diste cuenta que lo que está entre paréntesis vale 1 porque es la suma convergente que vimos antes, entonces el resultado es:

MaximoDeBitcoins = 10,500,000 + 10,500,000 = 21,000,000

En conclusión, la producción de Bitcoins está planeada para ser convergente, y generar un total de 21 millones de Bitcoins en toda su existencia.

La siguiente representación muestra la cantidad de bitcoins que se ganaron o ganarán por cada bloque minado incluyendo las fechas aproximadas en

las que se producirá el cambio, donde nuevamente puede verse la convergencia.



2-¿Qué es la escasez digital?

En el tercer pilar sobre registros inalterables tratamos el tema del doble gasto. Comentábamos que en la vida real cuando entregas un billete de 100 dólares, este pasa a manos de un nuevo propietario y tú ya no lo tienes. Pensábamos en lo conveniente que sería poder copiar el billete de la misma forma que se copia un archivo digital y poder gastarlo tantas veces como quisiéramos. En el mundo real es difícil evitar la escasez.

En forma opuesta, en el mundo digital lo que es difícil es producirla. Siempre puedo copiar los archivos digitalmente.

Si el concierto del fin de semana pasado estuvo genial y lo grabaste en video, puede copiarse a cualquier parte del mundo en minutos. Por eso en muchos conciertos los guardias de seguridad son tan insistentes en evitar que ingreses tu cámara de video profesional al evento.

La escasez digital es el mecanismo por el cual se logra llevar al mundo digital el mismo concepto de escasez del mundo real. En Bitcoin se logra esta escasez porque no tienes la opción de realizar doble gasto, si transfieres tus 3 Bitcoins a tu primo en Australia, ya no aparecerán en tu balance.

Pero Bitcoin va más allá con el

concepto de escasez. Dado que la cantidad total de bitcoins será de 21 millones, a medida que la producción de bitcoins por los mineros se va acercando a ese valor, más difícil es producirlos. Si quieres un bitcoin y no tienes la capacidad energética para producirlo, entonces se lo tendrás que comprar a alguien más. Dado que la tasa de emisión del bitcoins decrece, la unidad Bitcoin vista como moneda pasa a ser deflacionaria en el largo plazo. Si se compara con una moneda que tiene creación continua como ocurre con las monedas de los bancos centrales, podría esperarse un aumento de precio con el tiempo.

Existen otras criptomonedas con diseños inflacionarios, en ocasiones porque su objetivo es diferente, como es el caso de Steem que permite crear esquemas de pago dentro de una aplicación de red social.

El diseño limitado a 21 millones solamente aplica si consideramos como "Bitcoin" la cadena original jamás bifurcada. Algunos podrían afirmar que cuando se hizo la bifurcación de Bitcoin Cash ya se tuvo un tope de 42 millones, 21 por BTC y otros 21 millones por BTH. Pero como comentamos, al bifurcarse una cadena cada unidad pasa a ser un criptoactivo diferente, con valor de mercado diferente.

Actualmente la red original de Bitcoin tiene el respaldo de una comunidad mucho mayor que sus bifurcaciones, por lo tanto toda esa comunidad, que cree en el valor de Bitcoin como el equivalente digital del oro es la que hace pujar al mercado para que el precio se mantenga.

Esto debe tomarse con cierto cuidado, ya que al ser bifurcaciones las tecnologías son muy similares pero los objetivos de las comunidades son diferentes, lo cual en el futuro podría implicar también modificaciones en el precio. Por ejemplo, los promotores de Bitcoin Cash afirman que su tecnología tiene una mejor velocidad de desarrollo y por lo tanto tendrá más valor en el

futuro.

Como puedes ver, no hay una última palabra en estos debates y si te interesa conocer el estado de esta tecnología tendrás que mantenerte actualizado con noticias después de leer este libro.

Me gusta comparar esta competencia entre las comunidades de criptoactivos con las grandes empresas que cotizan en bolsa y discuten que son mejores que su competencia. El valor de sus acciones varía dependiendo de muchos factores, y no olvidemos que Bitcoin en el presente está compitiendo con más de 2000 criptoactivos diferentes, muchos de los cuales quizás no existan para la próxima

semana, pero con que solo uno implique una tecnología que evolucione la blockchain y atraiga una comunidad suficientemente grande, podría ser un competidor serio para la unidad de la primera blockchain.

3-¿Qué significa en Bitcoin que los pagos son irreversibles?

Una transacción de tarjeta de crédito parece durar solo unos segundos. Pero ¿creerías que según el concepto informático de transacción podríamos decir que dura varios meses?. Está bien, quizás sea una exageración: el hecho es que una transacción de tarjeta de crédito no está realmente finalizada (digamos, no es definitiva) una vez que la haces. Hay espacio para reclamos. Puede revertirse. El concepto de contracargo consiste en regresar el dinero a la tarjeta de crédito cuando el cliente, por algún

procedimiento que no siempre puede ser justo para el comerciante, reclama que nunca tuvo su producto a cambio. Y entonces el dinero se regresa en la forma de un abono a su tarjeta de crédito.

Eso no ocurre en el caso de la red Bitcoin, debido que justamente está diseñada para que las transacciones sean definitivas. Una vez que firmaste digitalmente la transacción de enviar 2 Bitcoins, llega a los nodos, y si tu firma es válida, ya no podrás cancelar ese pago. No hay ctrl-Z.

Efectivamente, cuando se realiza una transacción firmada y se envía a la red cada uno de los nodos comienza a

buscar incluirla dentro de los bloques potenciales. Pero además, una vez que ya se ha colocado en un bloque válido los demás mineros comenzarán a colocar bloques sobre ella.

El bloque de nuestra pasa a quedar sepultado bajo más y más bloques. También tratamos en el cuarto pilar que esa cantidad de bloques bajo se denomina número de confirmaciones.

Si la cantidad de bitcoins que tienes es el balance basado en todas las transacciones históricas puedes llegar a la conclusión de que ya no ha forma de revertir lo que ocurrió. Si enviaste 5 bitcoins a tu primo y ya han ocurrido

unas 100 confirmaciones, entonces todos los nodos de la red verán que el balance de tu primo tiene 5 bitcoins adicionales y tú tienes 5 bitcoins menos. No hay doble gasto. No hay contracargos. Así ocurre en Bitcoin.

El hecho de que se generen mecanismos reversibles para los pagos es algo criticado en la publicación original de Satoshi manifestando que es uno de los esquemas para que se tenga tanta complejidad, como vemos en la siguiente cita:

***Citando a Satoshi**:*
" Mientras que el sistema funciona lo suficientemente bien para la mayoría

de las transacciones, aún sufre de las debilidades inherentes del modelo basado en confianza. Transacciones completamente no reversibles no son realmente posibles, dado que las instituciones financieras no pueden evitar mediar disputas. El costo de la mediación incrementa costos de transacción, limitando el tamaño mínimo práctico por transacción y eliminando la posibilidad de pequeñas transacciones casuales, y hay un costo más amplio en la pérdida de la habilidad de hacer pagos no reversibles por servicios no reversibles." Satoshi Nakamoto, 2008.

Con lo anterior puedes comprender por qué son escasos los servicios de venta de Bitcoins a través de tarjeta de crédito. Podrías pedir comprar 10 Bitcoins a una casa de cambio, un mes después solicitar un contracargo porque tus Bitcoins nunca llegaron, y te quedarías con los Bitcoins y con el dinero. Los pocos servicios que existen hacen una evaluación de riesgo y ponen una tasa muy alta por el riesgo: pagarás cada Bitcoin hasta 20% más caro que el precio de mercado en ese momento.

4-¿Qué es un ataque del 51%?

Bitcoin también tiene sus puntos débiles. Si hubiera uno solo, sería este: el ataque del 51%. El mecanismo de consenso distribuido de la prueba de trabajo implica que si alguien tiene suficiente poder de procesamiento (alta tasa de hash) podría generar una larga cadena y pegarla en el momento adecuado para que se convierta en "la cadena más larga". Si pasaron demasiadas confirmaciones como para hacer ciertas combinaciones tramposas de transacciones, lograría el doble gasto. Y la técnica serviría no importando el

monto de la transacción. Podría equivaler a muchos millones de dólares.

Se estima que se requiere más de la mitad (usualmente se refiere como el 51%) de los nodos deshonestos para provocar un ataque de este tipo. Pero aún que eso ocurra, en la prueba de trabajo el premio a los mineros puede ayudarnos a que no suceda. Veamos la siguiente cita:

Citando a Satoshi:
"El incentivo puede ayudar a animar a los nodos a mantenerse honestos. Si un atacante egoísta es capaz de reunir más potencia de CPU que todos los nodos honestos, este

tendría que elegir entre utilizarla para defraudar a la gente robando sus pagos de vuelta, o en utilizarla para generar monedas nuevas. Debería encontrar más rentable jugar por las reglas, tales reglas lo favorecen a él con más monedas que a todos los demás combinados, que socavar el sistema y la validez de su propia riqueza." Satoshi Nakamoto, 2008.

En definitiva, técnicamente sería posible hacer un ataque de este tipo, pero no sería conveniente para los participantes. A menos claro que exista otro tipo de motivación (filosófica por ejemplo). En la historia de las cadenas de bloques se

conocen varios intentos de ataque del 51% pero nunca en Bitcoin, sino en redes más pequeñas donde la tasa de hash es muy baja. En esos casos, si el software es muy similar al que se usa para redes más grandes, un porcentaje de la potencia de la gran red puede dirigirse a atacar a la red pequeña para generar un ataque de este tipo.

5-¿Qué es una casa de cambio de Bitcoin?

Una casa de cambio es generalmente un portal web administrado por una empresa, el cual incluye una aplicación donde se puede hacer la compra o venta de un criptoactivo, ya sea frente a otro criptoactivo (ejemplo: intercambiar bitcoins por ether) o por una moneda de curso legal (ejemplo: intercambiar bitcoins por dólares americanos).

El funcionamiento de una casa de cambios ocurre de una manera muy similar (sino idéntica) a la forma en que funcionan las aplicaciones en línea para

intercambiar divisas (dólares versus yenes, euros vs libras, etc.).

El proceso para hacer estos intercambios implica generalmente que realices algún tipo de depósito en monedas tradicionales (dólares, euros o pesos) y este es acreditado dentro del portal. Supongamos que transfieres 100 dólares. Desde ese momento lo que existe es un registro en la base de la empresa de que tienes 100 dólares en su cuenta. Ese registro no es más es un reconocimiento de que la empresa te debe 100 dólares.

Posteriormente mediante paneles de compra-venta te permitirán hacer las

compras de bitcoins al precio del mercado en ese momento, puedes comprar en decimales, lo cual es lo más común, aunque cada casa de cambio tiene una cantidad mínima que puedes comprar. Para simplificar supongamos un precio del Bitcoin de 5,000 dólares. Podrás comprar 0.02 bitcoins, sin considerar que la casa de cambio te cobrará una comisión la cual depende de cada casa de cambio, vamos a usar en el ejemplo un valor del 1%. Al final al operación el panel de control te mostrará 0.0198 bitcoins en tu saldo.

¿Cuántos bitcoins tienes? Si respondiste 0.0198, estás en un error. Tienes cero bitcoins. Nuevamente la casa de cambio

te muestra en el panel un registro según el cual reconoce que te debe 0.0198. Pero no existe ningún registro en la blockchain de Bitcoin de que tienes ese balance[30].

Para que tengas tus bitcoins debes hacer un procedimiento en la casa de cambio que se llama **retiro**. En alguna pantalla que te presentará, te pedirá que le indiques tu dirección de Bitcoin a la cual quieres que se haga el depósito (recuerda que puedes haber generado muchas direcciones, como explicamos en el pilar sobre firmas digitales).
Algunas casas de cambio te pedirán también un pin de seguridad para garantizar la transacción. Entonces

pondrán tu solicitud en una lista de pendientes, y los tiempos en que se procese la solicitud varían según la casa de cambio.

Todavía no ha habido comunicación con la red de Bitcoin, este es un proceso interno de la casa de cambios y en ocasiones tiene costo (se les denomina **comisiones por retiro**).

Finalmente, el sistema interno de la casa de cambios decide procesar tu solicitud, la verifica y entonces, ahora sí, establece conexión con un nodo propio de la red Bitcoin y genera una transacción que puede agrupar varios retiros: el tuyo, el de tu primo en

Australia, y el de una señora que no conoces que vive en Luxemburgo. Las casas de cambio agrupan gran cantidad de retiros para ahorrar en comisiones cobradas por transacción.

Lo que sigue ya lo conoces: se comunica la transacción Bitcoin a la red, los nodos la validan, algún nodo mina un bloque incluyendo tu transacción y este bloque pasa a ser sepultado poco a poco bajo otros bloques válidos. Ya puedes verificar tu balance en un explorador blockchain y suponiendo que los retiros fueran gratuitos en esa casa de cambio, tendrás 0.0198 bitcoins. Ahora realmente tienes bitcoins.

Las casas de cambio de Bitcoin funcionan continuamente, se trata de mercados que operan las 24 horas del día los 365.25 días del año. Prácticamente en tiempo real se pueden hacer operaciones entre diferentes criptoactivos. Los especuladores y **traders**[31] muchas veces no se preocupan por retirar sus bitcoins debido a que operan continuamente, únicamente retiran las ganancias, con el riesgo que ello conlleva.

Uno de los grandes problemas con las casas de cambios es que centralizan las operaciones. Eso es miel que atrae como osos a los ciberdelincuentes para realizar robos de criptoactivos. Si una

casa de cambio es robada pueden pasar dos cosas:

- Que decida proteger a sus cuentahabientes regresándole sus monedas y sacándolos de sus fondos
- o bien qué no haga esto ya sea porque así lo decida o porque no tenga suficientes fondos para poder responder a los usuarios

En el segundo caso quien mantenga saldos en bitcoins lo perdería todo. Por ello existen muchos sitios insistiendo en que si quieres guardar criptoactivos debes hacer los retiros correspondientes a las direcciones Bitcoin de tus billeteras digitales.

Notas:

[30] - El hecho de que se encuentre como registro en una entidad centralizada tiene la gran desventaja que cualquier cosa que le ocurra a esa entidad (crisis, cierre, robo, etc.) podría afectar a su capacidad para regresarte tu dinero o tus criptoactivos. Por ejemplo, la casa de cambio Mt.Gox al cerrar sus puertas en Febrero de 2014 dejó a una gran cantidad de clientes sin su dinero y sin "sus" bitcoins.

[31] - Un trader en este contexto es una persona que opera en estas casas de cambio realizando análisis de precios e invirtiendo en diferentes criptoactivos para obtener un beneficio por

diferencias de precio en función del tiempo o del criptoactivo. No existe una traducción concreta al español aunque algo cercano podría ser "negociador de casa de cambio".

6-¿Por qué existe un mercado de valor del Bitcoin?

Para responder esta pregunta debemos entender primero que te llamamos "valor". Puede referirse a una propiedad intrínseca de un activo, o simplemente una medida relativa que el mercado le otorga en función de fuerzas particulares.

Si nos referimos algo intrínseco y consideramos que en realidad del Bitcoin es un intangible que no puede "tomarse con las manos", podríamos afirmar que su valor prácticamente es

cero. Sin embargo, también son intangibles las marcas, las patentes y los secretos industriales, pudiendo valer muchos miles de millones de dólares. Por ejemplo en el año 2000 la marca Coca Cola fue valorizada en más de 72 mil millones de dólares, liderando el ranking de valor de marca, mientras que en 2017 la marca más valorizada fue Apple con 184 mil millones de dólares.

Desde el momento que Bitcoin fue intercambiado por un activo real empezó a tener un valor en el mundo real. Muy poco valor, eso sí, pero aunque fueron 10,000 bitcoins intercambiados por dos pizzas, el intercambio por bienes tangibles comenzó. A medida que más

personas fueron involucrándose en la comunidad, su valor fue poco a poco aumentando. Quizás en algunos aspectos esta valorización funcionó en forma similar a lo que ocurre con quien tiene algún bien coleccionable como estampillas y deja pasar el tiempo (aunque en este caso los bitcoins no son diferentes entre sí, porque de hecho no existen, son una cantidad que resulta del balance entre todas las transacciones que tu cuenta ha realizado).

Adicionalmente, cuando el Bitcoin logró comenzar a intercambiarse en casas de cambio, comenzó a existir también espacio para la especulación. Y cuando un activo está diseñado para ser escaso,

puede sospecharse que está diseñado para aumentar su valor (al menos en ciertos contextos) y con ello atrae muchos especuladores.

Hoy Bitcoin soporta su valor en diferentes causas, que si se debilitan o fortalecen afectan su valor. Entre ellas se encuentra la propia tecnología, el tamaño y soporte de la comunidad, el talento y unidad de los desarrolladores del software Bitcoin Core, el haberse convertido en moneda de referencia dentro de las casas de cambio, o incluso la propia promoción e impulso que los primeros poseedores de bitcoins convertidos en multimillonarios, han hecho para que la tecnología siga

desarrollándose y extendiéndose en uso.

Aún con lo anterior, en un contexto de existencia de más de mil criptomonedas, puede encontrarse con una fuerte competencia en algún momento en el futuro, que pudiera no solo quitarle el primer puesto en capitalización teórica de mercado, sino hacerlo poco útil en varios sentidos. De hecho, durante Junio de 2017 la capitalización de ETH llegó a un 34% del total de los criptoactivos, frente a un 39% de Bitcoin en ese momento, por lo cual Ethereum estuvo a punto de convertirse en la red blockchain mejor capitalizada.

Mientras existan personas interesadas en

poseer un balance positivo de bitcoins, la unidad de la blockchain más antigua seguirá teniendo valor, ¿cuánto? dependerá de cuántas sean estas personas, su capacidad económica para mantener el precio, las características comentadas antes y por supuesto, que cantidad de redes alternativas aparezcan y la calidad de las mismas que les hagan buenas competidoras frente a la red Bitcoin.

7-¿Qué fraudes han existido relacionados con Bitcoin?

Bitcoin ha sido relacionado muchas veces con:

- Fraudes (en particular engaños para quitarte tu dinero)
- Uso para actividades ilícitas (como comercio de artículos prohibidos, lavado de dinero, etc.)
- Robos (de bitcoins, pero también de otros criptoactivos)

Los fraudes se han reportado en numerosos países utilizando el nombre

de Bitcoin, en la mayoría de casos solicitando inversiones que nunca fueron usadas para nada relacionado con blockchain, ni Bitcoin.

La receta es tristemente sencilla: un grupo de estafadores junta información relacionada con Bitcoin y su aumento de precio en momentos en que está al alza, lleva su campaña a personas que poco conocen del tema y los anima a "invertir" en su nueva criptomoneda que, según ellos mismos afirman, es "mucho mejor" que el Bitcoin. Algunos juntan el dinero y se marchan con él. Otros comienzan a ofrecer retornos, pero que en realidad es dinero que viene de otros nuevos integrantes (esquema piramidal)

haciendo crecer al grupo de seguidores hasta que alguien no puede dar retornos y entonces sí se marchan con el dinero supuestamente invertido.

En ocasiones la prensa mal informada usa titulares confusos en relación a este tema: como "otro fraude con bitcoins" o "nuevamente red piramidal de Bitcoin" cuando en realidad jamás existieron bitcoins en juego. Actualmente Bitcoin como unidad de valor está reconocido existiendo incluso mercados de futuros ya legalizados en Estados Unidos.

Por otra parte, la historia de el uso de bitcoins para actividades ilícitas es conocida desde hace tiempo desde la

existencia del mercado negro llamado Silk Road en el período 2011-2013, en el cual entre otros artículos prohibidos se comercializaban drogas ilegales. También se reporta que ha sido utilizado para transferencia de activos entre diferentes países facilitando así el lavado de dinero. En muchos de estos casos, la trazabilidad de Bitcoin (todos los registros son públicos) ha permitido llegar a los responsables, por lo cual muchas actividades han pasado a realizarse en plataformas realmente anónimas[32] o regresado al uso de efectivo.

Notas:

[32] - Existen otras redes de

criptoactivos como Monero, Z-Cash o Dash que tienen características que permiten el anonimato en las transacciones.

8-¿Qué alternativas de Consenso Distribuido existen?

La prueba de trabajo de la cual se deriva la minería, es la forma en que se establece el consenso distribuido en Bitcoin y muchas otras cadenas blockchain, como Ethereum, Litecoin o NameCoin.
Sin embargo, debido al crecimiento de las plataformas de hardware especializadas en minería, (ASICs, por sus siglas en inglés) muchos miembros de la comunidad de Bitcoin y de criptoactivos en general, han criticado que la producción de bitcoins se ha

concentrado en organizaciones que han aportado grandes sumas de capital de inversión para comprar este tipo de hardware. Para 2018 más del 70% de la minería de Bitcoin se concentra en China, lo cual indicaría que la moneda no se encuentra tan descentralizada como debería. Veamos otras alternativas de consenso que han nacido.

Prueba de Participación

Si en la prueba de trabajo tener más dinero permite comprar más equipo y con eso ganar más monedas, alguien se preguntó ¿por qué no hacer que quienes

compren más monedas se les permita generar más bloques? Y con eso ahorrar todo el hardware y el consumo eléctrico de la PoW. La prueba de participación, PoS (por sus siglas en inglés) consiste en una serie de propuestas similares de consenso distribuido por las cuales los propietarios de cierto volumen de criptoactivos pueden pasar a generar bloques.

Las técnicas para habilitar PoS son algo complejas, y muchas veces incluyen "congelar" cierta cantidad de tu balance para que ese permita generar nuevas monedas. Pasa a ser similar a colocar tu dinero en un depósito a plazo para que recuperes la inversión. El retorno suele

llegar después de un período denominado **maduración** de las monedas.

Prueba de Quemado

En lugar de comprar hardware, otro mecanismo es que el nodo productor de bloques tome monedas y literalmente las destruya. Al hacerlo gana derechos para poder producir el siguiente bloque. Generalmente esta destrucción ocurre haciendo transferencias a una dirección desde la cual no se pueden gastar[33].

Prueba de Capacidad

Algunos algoritmos de consenso buscan recursos dentro de la propia computadora, como espacio en disco. Si se tiene la suficiente capacidad entonces se podrán producir nuevos bloques. Existen algoritmos especiales para lograr este objetivo, sin embargo en la práctica pocas implementaciones han podido usar este método de consenso.

Prueba de Autoridad

Si nos olvidamos de la descentralización podemos decidir que uno o varios nodos sean determinantes para la creación de los bloques. Evidentemente esto no tiene sentido para

sustituir una cantidad de sistemas, bases de datos o software simplemente porque tenemos estructuras de bloques. Pero cuando se trata de hacer verificaciones de calidad de todo el software que funciona en una blockchain, la prueba de autoridad sirve como una opción para no gastar recursos energéticos. Cuando la red blockchain va a salir a producción, simplemente se sustituye la parte de código de consenso quitando la prueba de autoridad y colocando ahora prueba de trabajo. Muchas redes de donde los desarrolladores solamente quieren probar la plataforma funcionan de esta manera.

Más adelante en el libro presentamos

una tabla con diferentes redes que usan cada tipo de prueba de consenso.

Notas:

[33] - Aunque no es el mejor método, enviar monedas a una dirección Bitcoin donde todos los dígitos sean ceros o todos todos unos, por ejemplo, hace que esas monedas no puedan gastarse porque hasta ahora no se ha descubierto la llave privada de una dirección así, y probablemente nunca se descubra.

9-¿Cuál es la definición de criptoactivo?

Aún no existe consenso en la definición de un criptoactivo, criptomoneda o activo virtual. Desde el punto de vista técnico y si nos limitamos a redes similares a la de Bitcoin, está claro que es la unidad de medida que se utiliza en las transacciones de una red blockchain particular. Esto puede observarse con más claridad cuando una red se bifurca y se generan dos estructuras de cadena de bloques: cada una pasa a tener su propia unidad y el mercado les da valores diferentes. Así ocurrió con la bifurcación de Ethereum versus

Ethereum Classic[34] y también con la bifurcación de Bitcoin vs Bitcoin Cash

Hasta los nombres son problemáticos. Si se bifurca la cadena ¿cuál de las dos cadenas queda con el nombre original? Hasta ahora se ha usado la regla de la mayoría: la cadena que queda con la mayoría de tasa de hash conserva el nombre original y la otra pasa a tener un nuevo nombre.

El problema es el tratamiento legal que se le da a un criptoactivo: ¿es una moneda que permite hacer pagos? ¿es un valor similar a las acciones de las empresas? Estas respuestas aún están discutiéndose y los países han tenido

posiciones diferentes. Durante los próximos años van a ir apareciendo respuestas a estas preguntas del punto de vista jurídico.

Notas:

[34] - Esta bifuración ocurrió el 25 de Octubre de 2016.

10-¿Qué otros criptoactivos existen?

Si eres desarrollador puedes crear una blockchain con tu propia criptomoneda en una tarde. Serán suficientes unos servidores en la nube. Pero no será muy útil a menos que tengas una idea bastante original. Aún así, miles de desarrolladores han creado sus propias criptomonedas y esperan que tengan valor.

En la historia de los criptoactivos muchos han cumplido su ciclo de vida completo, otros ni siquiera han visto la luz (por ser fraudes donde lo único que

existió fue el nombre). Existe un curioso sitio en Internet que recolecta todas las "criptomonedas" que han muerto[35].

Pero hay muchos casos de redes con comunidades grandes y activas, algunas con propósitos específicos. Exploremos algunas.

Litecoin

Debido a que Bitcoin siempre se proclamó como oro digital, Litecoin vio la oportunidad de identificarse como plata digital. El código original es relativamente similar, pero los tiempos de bloque de Litecoin son de 2.5

minutos.

En lugar de usar un algoritmo basado en los hashes SHA-256, la red Litecoin usa un algoritmo denominado Scrypt que también es PoW. Este es más difícil de implementar con alta performance en dispositivos de hardware como ASICs, que si bien existen, no generan tanta ventaja frente a la generación con CPU o GPU. Por esta razón hoy todavía se pueden generar Litecoins usando tu computadora, aunque no es la criptomoneda más rentable.

La red tiene un equipo de desarrollo muy activo, involucrado en diferentes proyectos como la interoperabilidad con

otras cadenas blockchain.

Ripple

Creado por la empresa Ripple Labs se trata de un criptoactivo con tiempos de bloque muy rápidos (solamente tres segundos) y con un esquema de consenso distribuido propietario, denominado Algoritmo de Consenso del Protocolo Ripple (RPCA, por sus siglas en inglés) que implica la participación de varios nodos en la validación de bloques. Debido a que recuerda a la prueba de autoridad, se han presentado críticas sobre su mecanismo de consenso en relación a que se aleja mucho a la

descentralización propuesta en el Bitcoin.

Es actualmente considerada la tercer red por valor teórico de mercado y es muy usada para transferencias entre países, en particular suele ser implementada por casi todas las casas de cambio ya que permite retiros veloces por su tiempo de bloque.

Ripple Labs ofrece otros servicios además de mantener su criptomoneda, denominada XRP, en particular a entidades financieras y empresas de envío de dinero.

Ethereum

Dedicaremos una pregunta específica a esta red blockchain más adelante.

Bitcoin Cash

Nos referimos ya a esta red blockchain al explorar el quinto pilar, surgiendo de la Bifurcación de Bitcoin tras una propuesta por un equipo de desarrolladores denominado Bitcoin ABC, que dan nombre al software de referencia para implementar la red Bitcoin Cash. La principal diferencia es el tamaño de bloque, aumentado de 1Mb a 2Mb en el momento de la bifurcación.

Stellar

También con tiempos de bloque reducidos, esta red blockchain es mantenida por una organización sin fines de lucro denominada Stellar.org. La unidad de medida en las transacciones se denomina Lumen. El tiempo de bloque es de aproximadamente 5 segundos.

Monero

Monero consiste en una red blockchain donde las entradas y salidas de dinero

digital son empaquetadas buscando que los pagos sean totalmente anónimos. También utiliza prueba de trabajo, pero el algoritmo se denomina CryptoNight.

Por sus características de anonimato es un criptoactivo de interés para los ciberdelincuentes, por ejemplo es frecuentemente solicitada en rescates de ransomware[36].

Adicionalmente como mencionamos antes, el código ha sido diseñado para ser resistente a las ASICs, con lo cual puede ser minado utilizando una PC con cierto poder de cómputo. Esto último permite una técnica indirecta de obtención de Bitcoins con una PC: se

realiza minería de Monero (u otra criptomoneda fácilmente minable con equipos domésticos), cuando se obtienen unidades de Monero se cambian por bitcoins en una casa de cambio. En ese caso muchas veces se pierde el anonimato, porque la casa de cambio suele exigir identificación para realizar las operaciones.

Dogecoin

Esta red es muy conocida porque comenzó como una broma. Se trata de una red blockchain que usa código similar a Litecoin, pero tiene una comunidad muy fuerte cuyo símbolo es

un perro Shiba Inu, por lo cual es conocida como la "criptomoneda del perrito". Se ha orientado fuertemente a un ser un mecanismo para dar propinas o regalos a otras personas, ya que las comisiones por las transacciones son prácticamente cero.

Notas:

[35] - Puedes visitarlo en https://deadcoins.com/

[36] - Se trata de software similar a un virus que encripta el contenido del disco duro de tu computadora solicitando un rescate (usualmente en criptomonedas) para que puedas volver a acceder a tus propios datos.

11-¿Por qué es Bitcoin el criptoactivo de referencia?

Las casas de cambio no permiten el intercambio directo de cualquier criptoactivo por otro criptoactivo. Por ejemplo, si tú tienes 100,000 dogecoins y quieres comprar Monero, primero tendrás que comprar bitcoins con tus dogecoins en un mercado Dogecoin/Bitcoin. Con esos bitcoins podrás comprar monero en un mercado Monero/Bitcoin. Si lo has notado has tenido que pasar por Bitcoin. Las casas de cambio usan generalmente Bitcoin como referente para crear sus mercados, aunque algunas aceptan ether u otros

criptoactivos, es menos frecuente.

Bitcoin se ha convertido en referencia por su poder de hash y por ser una cadena de bloques que ha resistido prácticamente diez años sin que haya sido dañada por ataques a su seguridad o tecnología, lo cual sí ha ocurrido con otras redes. Esto también contribuye al mantenimiento de valor del Bitcoin. De hecho, en 2018, la **dominancia Bitcoin** que mide el porcentaje de tamaño teórico de mercado de Bitcoin sobre el total de los criptoactivos, volvió a superar el 50%.

12-¿Por qué Bitcoin ya no es aceptado en algunos sitios de Internet?

Para sorpresa de algunos, Bitcoin parece estar siendo menos aceptado en muchos sitios de compras, tanto físicos como de Internet como medio de pago. Justamente cuando está por cumplir diez años como tecnología, se esperaría que su uso continuara aumentando .

Existen varias razones para que esta situación esté ocurriendo. La primera de ellas tiene relación con un aspecto tecnológico que deriva en una funcionalidad (o ausencia de la misma).

Cuando conociste las reglas del consenso distribuido, se comentó sobre el ajuste de dificultad para que en promedio los bloques sean producidos cada 10 minutos. Ese tiempo de espera, de la mano de que deben esperarse seis confirmaciones, implican que el pago debe realizarse en aproximadamente una hora. Esto es muy tardado en un mundo donde se ha estudiado que un usuario promedio se impacienta cuando pasan más de tres segundos que no carga su sitio de Internet en su teléfono móvil.

La siguiente tabla muestra los tiempos promedio de bloque aproximados de varias redes blockchain de criptoactivos más conocidos:

Criptoactivo	Tiempo de Bloque
Bitcoin	10 minutos
Dash	2.625 minutos
Litecoin	2.5 minutos
Monero	2 minutos
Dogecoin	1 minuto
Ethereum	15 segundos
Stellar	5 segundos
Ripple	3.5 segundos

También sabes ya que cuando haces pagos con Bitcoin se debe pagar una comisión a los mineros, una especie de propina, para que la transacción sea

tomada e incluida en un bloque potencial de la cadena. En épocas de saturación, el valor necesario para no tener que esperar horas ha sido de más de 50 dólares, lo cual para compras pequeñas puede ser un valor elevado.

Ante lo anterior, otros criptoactivos como Litecoin, Dash, Ripple y el propio Ethereum han comenzado a ser vistos con muchos mejores ojos por aquellos que están dispuestos a aceptar pagos en línea.

13-¿Qué es Ethereum?

La segunda red blockchain[37] en la actualidad se denomina Ethereum y tiene su origen en otra publicación, "Una nueva generación de contratos inteligentes y plataforma de aplicaciones centralizadas" realizada por Vitalik Buterin, un joven nacido cerca de Moscú y formado en Canadá que en esos momentos tenía solamente 19 años.

Ethereum comparte ciertas características similares a Bitcoin pero con difetencias cuantitativas y cualitativas.

También se basa en una estructura de

cadena de bloques que se referencian unos con otros, también utiliza prueba de trabajo por lo cual existen mineros de **ether**, el nombre que lleva la unidad de medida dentro de la red.

Los bloques en Ethereum tienen un tiempo promedio de aproximadamente 15 segundos, por lo cual la red es mucho más rápida que la de Bitcoin. Una espera de 12 confirmaciones, un valor común usado para considerar el pago finalizado, tarda dos minutos y medio en esta red blockchain.

El ajuste de dificultad en Ethereum es más rápido, si un bloque tarda menos de 9 segundos el software de referencia de

Ethereum denominado **geth**[38] aumenta la dificultad, si un bloque tarda en aparecer más de 20 segundos, entonces disminuye la dificultad.

Las direcciones Ethereum son un poco diferentes que las de Bitcoin y se expresan en números hexadecimales comenzando con un 0x.

Pero la característica más conocida de Ethereum, y de lo que trata la publicación de Buterin, es la de funcionar como la "computadora mundial", permitir la ejecución de programas distribuidos que registran información sobre su cadena de bloques, los denominados contratos

inteligentes[39].

Notas:

[37] - En tamaño teórico de mercado, aunque es la mayor en número de nodos.

[38] - Abreviatura de go-ethereum, nombre derivado de que el software está programado en el lenguaje de programación Go.

[39] - Traducción más utilizada del inglés "Smart Contract".

14-¿Qué es un Contrato Inteligente?

Cuando se desarrolló Bitcoin, las operaciones necesarias la momento de una transacción eran sencillas: sumas y restas son suficientes para calcular un balance. Estas sumas y restas son implementadas con código en algún lenguaje de programación. ¿Podríamos realizar operaciones más complejas al momento de generar transacciones? La respuesta es sí, y esto tiene gran relación con el nacimiento de los denominados contratos inteligentes (SC, por sus siglas en inglés, de Smart Contracts).

Los SC son programas de cómputo especializados que están diseñados para que puedan crearse a través de transacciones, vivir en la cadena de bloques y poder ejecutarse en todos los nodos.

Cuando un programa de este tipo se ejecuta en todos los nodos en forma simultánea, no solamente tenemos garantía de que los datos se mantienen iguales en toda las copias del libro distribuido, sino que los procesos que modifican la información también se ejecutan de forma igual en todos ellos. Por ello podemos presumir que si muchas partes están de acuerdo en que el proceso se ejecute de cierta forma,

entonces al escribir este tipo de programas pasan a funcionar como un contrato, aunque en realidad son programas.

¿Porqué se dice que son inteligentes? En realidad no lo son, ni tienen nada que ver con inteligencia artificial. Lo que sí ocurre es que al ejecutarse las transacciones estas no dependen de una tercera parte, por lo cual se trata de programas "independientes de un tercero".

La red más común donde se programan es la de Ethereum, pero existen muchas otras redes donde pueden usarse, incluso se ha creado capas de software sobre

Bitcoin como Omni y Rootstock (también conocida como RSK).

Para generar contratos inteligentes dentro de la red Ethereum se creó un lenguaje de programación específico similar a JavaScript, denominado Solidity, el cual puede compilar al motor de contratos inteligentes de Ethereum: la Máquina Virtual Ethereum (EVM, por sus siglas en inglés).

Este tipo de programas ya tienen muchas aplicaciones:

1. Permiten crear condiciones acerca de las transacciones realizadas con ether

2. Habilitan mecanismos de votación independientes de un tercero, ya que el programa no corre en un servidor específico
3. Dan la posibilidad de crear otro tipo de criptomonedas, unidades que viven dentro de Ethereum adicionales al ether, y que se conocen como "tokens"[40].
4. Facilita la creación de organizaciones descentralizadas
5. Permiten la recaudación de dinero en forma de ether en campañas por períodos específicos (ver la siguiente pregunta en esta parte II)
6. En general, pueden desarrollarse sobre la plataformas aplicaciones

descentralizadas, conocidas como dApps[41]

Un desarrollo más amplio de la red Ethereum y otras redes derivadas escapan del alcance de este libro, sin embargo en la siguiente sección visitaremos uno de los temas por los cuales la red se ha hecho muy conocida: las ofertas iniciales de moneda.

Notas:

[40] - Un token es como una ficha de casino a la cual se le da un valor dentro de la propia red de Ethereum, generalmente expresado en ether. Como se encuentra dentro de la misma

blockchain, los contratos inteligentes pueden incluso saber la cotización entre el ether y el token.

[41] - En diciembre de 2017 se hizo muy famosa una dApp para coleccionar gatitos virtuales denominada Cryptokitties, llegando a saturar la red de Ethereum.

15-¿Qué es una oferta inicial de moneda (ICO, por sus siglas en inglés)?

Una oferta inicial de moneda puede verse como en un equivalente a una Oferta Pública Inicial[42] pero aplicada al mundo de los criptoactivos. Ocurre cuando se realiza una captación de valor en algún tipo de criptoactivo, por ejemplo ether, donde una serie de personas, generalmente desarrolladores y algunos asesores, ofrecen al mercado la venta de un conjunto de tokens que usualmente representan una participación (similar a acciones) a un producto o un proyecto de inversión.

Mientras las IPO se encuentran fuertemente reguladas, la regulación de una ICO es prácticamente inexistente en muchos países y en otros está comenzando normarse.

Muchas veces el proyecto presupone la generación de alguna nueva red blockchain donde estarán representados éstos tokens en el futuro, prometiéndose la conversión de esos tokens en criptomonedas cuando la red esté lista. En teoría, el equipo que propone el proyecto debería presentar un plan del mismo así como explicar su visión y a las metas a alcanzar.

Surgieron numerosas ICO durante el año

2017 de las cuales muchas terminaron siendo fraudes[43], otras tuvieron inconvenientes para hacer funcionar la visión de su proyecto y apenas un pequeño porcentaje realmente puso en funcionamiento su red blockchain planeada.

En algunos casos lo que es asombroso es la capacidad para captar el dinero. El programador Brendan Eich de Mozilla, también creador del lenguaje JavaScript, planteó un proyecto para anuncios dentro de su navegador Brave, recaudando nada menos que 35 millones de dólares en únicamente 30 segundos. ¿Cómo fue esto posible? Utilizando un contrato inteligente que permitía recibir

el dinero (en ether) a partir de determinada fecha y que una vez reunida la cantidad necesaria bloqueaba la recepción de más aportaciones. El proyecto fue anunciado con anticipación y los tokens se agotaron más rápido que los boletos de concierto de la estrella más famosa del momento.

Lo anterior es solo una muestra del potencial de los contratos inteligentes dentro de redes como Ethereum.

Notas:

[42] - Una Oferta Publica Inicial, IPO por sus siglas en inglés, es cuando una empresa ingresa a una bolsa de valores para ofrecer por primera vez sus

acciones al público en general, para lo cual debe cumplir con una serie de normativas y un proceso previamente definido.

[43] - La empresa Statis Group realizó un estudio según el cual el 80% de las ICO resultaron en fraudes donde en muchos casos los fundadores terminaron llevandose el dinero y no implementando ningún proyecto real.

16-¿Qué retos tiene la tecnología blockchain hacia el futuro?

Se ha generado gran expectativa por lo que las DLTs pueden significar como herramienta de cambio, con lo cual comienzan a existir muchos cuestionamientos si realmente se podrá lograr todo ese impacto anunciado.

Quizás el hecho de que se trate de la primera vez que la tecnología impacta directamente al concepto de valor y rompa fronteras al fundamentarse sobre Internet, sea uno de los factores clave que han llevado a generar toda clase de

promesas sobre el potencial de blockchain. Y lamentablemente, como ha ocurrido siempre con los cambios revolucionarios, aparecen muchos vendedores de humo que aprovechan ese momento en el cual la mayoría del público aún no sabe realmente de que trata.

La tecnología enfrenta varios problemas actualmente[44]:

1. Poca escalabilidad, la red se satura fácilmente tolerando solamente 3-10 transacciones por segundo[45]
2. Ausencia de interoperabilidad, algo que se ha estado trabajando

fuertemente y en este año 2018 se están viendo los primeros frutos

3. Herramientas poco amigables con el usuario
4. Buena parte de la tecnología está poco probada en entornos reales
5. Dificultades para el resguardo de las llaves criptográficas
6. Escasez de desarrolladores y alto costo de los mismos
7. Barreras legales
8. Gobernanza pobremente definida

La buena noticia es que aún con las muchas exageraciones que han habido, la tecnología sigue siendo muy prometedora: la capacidad de

descentralización, la eliminación de intermediarios, la reducción eficiente de la fricción en los procesos entre organizaciones y personas, el aporte de transparencia, el reforzamiento en ciertos aspectos de la seguridad, son entre otros, aspectos clave que parecen encajar muy bien como soluciones a problemas muy presentes en las últimas décadas en todo el mundo.

El "hype" no es casualidad, es causado por la búsqueda de respuestas a esos problemas de la mano de la esperanza de muchos participantes. Ocurrirán éxitos pero también decepciones, la maduración de blockchain seguramente llevará de cinco a quince años y

probablemente vaya a ser poco uniforme entre los diferentes países del mundo.

Las regulaciones demasiado tempranas en algunos países van a frenar la innovación, en otros el desarrollo será muy rápido y pronto se verán las consecuencias, sean beneficiosas o no, si son las primeras los cautelosos tendrán que ponerse al día. Pero justamente una gran cuestión es si realmente buena parte de lo que las DLTs proveen es regulable: las características hacen que se trate de un entorno donde el regulador tiene poco poder de acción real.

Lo que es claro es que se requiere

aumentar la difusión y el entendimiento de la tecnología: si los reguladores no entienden de que se trata, difícilmente formularán buenas regulaciones, si los usuarios no conocen de qué forma participar correctamente, seguirán cayendo en fraudes y trampas.

Bitcoin ha revolucionado el concepto de valor, blockchain está impactando con fuerza en los modelos vigentes basados en confianza. Quizás mucho sea exageración, quizás los vientos de cambio nunca hayan soplado tan fuertes.

Notas:

[44] - Listado basado en el informe de Gartner en 2017: Practical

Blockchain: A Gartner Trend Insight Report.

[45] - La dApp Cryptokitties en diciembre de 2017 fue un buen ejemplo de cómo una aplicacion inocente podía saturar la red de Ethereum. Era casi imposible hacer pagos en ether durante los días que ocurrió la saturación.

Bibliografía

Anjum, A. et al. Blockchain Standards for Compliance and Trust, IEEE Cloud Computing, 2017

Antonopoulos, Andreas. Mastering Bitcoin: Unlocking Digital Cryptocurrencies, O'Reilly Media, 2014

Antonopoulos, Andreas. El Internet del Dinero, Merkle Bloom LLC, 2017

Beck, Roman. Opportunities and Risks of Blockchain Technologies, IT University of Copenhagen, Dagstuhl Seminar 17132, 2017

Furlonger, David. Practical Blockchain: A Gartner Trend Insight Report, Gartner

Research, 2017
Gates, Mark. Cadena de Bloques, 2017
Gates, Mark. Bitcoin: Complete Guide To Bitcoin, 2017
Meguerditchian, Varant. Roadmap for Blockchain Standards, Standards Australia, 2017
Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008
Yaga et al. Blockchain Technology Overview, Draft NISTIR 8202, National Institute of Standards and Technology, 2018

Acerca del Autor

José G. Moisés se desempeña como Arquitecto de Software y Director de Proyectos.
Obtuvo el título de Ingeniero en Computación por la Universidad de la República de Uruguay en el año 2000 y el de Maestro en Ciencias en Administración de Negocios por parte de la Escuela Superior de Comercio y Administración, del Instituto Politécnico Nacional en el año 2012.
Es ScrumMaster Certificado tras ser alumno de Mike Beedle, y además miembro fundador del capítulo del Business Agility Institute en México,

BAMMX.
Ha trabajado en reconocidas firmas internacionales en Uruguay y México, como Bull, Pepsico, North American Software, Grupo Citibank, Grupo Estafeta y Grupo Santander, teniendo adicionalmente más de diez años de experiencia como docente a nivel público y privado.
Conociendo Bitcoin desde el año 2013, ha estado vinculado a la criptografía a través de su trabajo en facturación electrónica, lo que le ha servido para comprender más a fondo el funcionamiento de las redes blockchain.
Desde el año 2016 ha estado asesorando a particulares y empresas mexicanas, así como realizando presentaciones del

modelo de "los 5 pilares" con la confianza de que puede ayudar a explicar mejor el funcionamiento de la tecnología blockchain a todo tipo de público.
