Blockchain

Cómo desarrollar confianza en entornos complejos para generar valor de impacto social.

ITE/IPS TechLab

Autor: Marcos Allende López

Ilustraciones: Vanessa Colina Unda

BID
Banco Interamericano de Desarrollo

CONTENIDO

Presentando blockchain 3
Introducción 3
Nacimiento y evolución de la tecnología blockchain 4

Entendiendo blockchain 5
Qué es blockchain 5
a. Base de datos distribuida 6
b. *Peer-to-Peer* (P2P) 7
c. No necesidad de confianza 7
Cómo funciona la tecnología blockchain 8
Protocolos de consenso 13
Seguridad de la cadena 18
a. Hash 18
b. Capacidad de rechazar transacciones y bloques maliciosos 21
c. Protocolos de consenso, descentralización y teoría de juegos 22

Utilizando blockchain 23
Tipos de blockchain 23
a. Públicos 23
b. Federados 23
c. Privados 25
d. *Blockchain as a Service* (BaaS) 25
Comparativa entre los tipos de blockchain 26
Características y aplicaciones de blockchain 27
Smart Contracts & IoT 30
Cómo identificar cuándo blockchain es útil 31
Cómo empezar a construir una solución con blockchain 36
Arquitectura de la solución 41
Anonimato 43

Conclusiones 44

Anexo: Criptomonedas 46

Este trabajo es resultado del esfuerzo que, desde ITE/IPS, hemos venido realizando en el equipo de Marcelo Da Silva para poder presentar la tecnología blockchain desde un punto de vista a la vez técnico y práctico, con la intención de que sea de utilidad para los especialistas del banco en los distintos campos en los que puede ser aplicado. De ninguna forma habría sido posible sin la participación en la investigación técnica de Raul Ignacio Cerrato, la visión estratégica de Mariana Gutierrez Aldabalde, y el diseño e ilustraciones de Vanessa Colina Unda.

El documento se divide en tres bloques de contenido, las conclusiones y un anexo. El primer bloque consiste en una breve presentación de la tecnología; el segundo bloque aborda los aspectos técnicos de la misma, de forma no excesivamente formal pero sí rigurosa y el tercer bloque trata las cuestiones más relacionadas con la conveniencia, aplicación y utilización de la tecnología blockchain para proyectos específicos, con un *checklist* y un caso de uso detallado. En el anexo se presenta el campo de las criptomonedas.

Introducción

Desde que en 2008 Bitcoin adoptase la tecnología blockchain, el interés en la misma ha ido creciendo de forma exponencial. Si bien su primer y más exitoso campo de aplicación hasta el momento han sido las criptomonedas, hay un gran interés global y multidisciplinar en su potencial para ofrecer soluciones a gran escala en diversos campos.

Este documento pretende ser una guía rápida para entender cómo funciona la tecnología blockchain, cuáles son las características que la hacen diferente y revolucionaria y cuáles son los casos en los que su implementación resulta beneficiosa.

Se presentan también las diferencias entre los distintos tipos de blockchain, abordando las cuestiones que se han de plantear para determinar si alguno de ellos es conveniente, y en caso positivo cuál, como herramienta para construir una solución que sea útil para un proyecto determinado.

Nacimiento y evolución de la tecnología blockchain

La primera publicación[1] sobre la tecnología blockchain se remonta a 1991. La idea de los autores consistía en tener un registro digital de archivos -de audio, imagen, video o texto- ordenado cronológicamente, permitiendo conocer con exactitud su fecha de creación y su autoría.

Casi dos décadas después, en 2008, nace Bitcoin[2]. La propuesta de esta criptomoneda consiste en utilizar la tecnología blockchain para proveer un método de pago electrónico que no necesita supervisión y elude el control de las instituciones financieras. El ingrediente fundamental y definitivo que incorpora Bitcoin, convirtiéndole en la más exitosa de todas las propuestas de dinero digital hasta la fecha, es la combinación de la inteligente idea de la tecnología blockchain junto con un protocolo de consenso conocido como ***Proof-of-Work***. Tal y como explicaremos más adelante, este es el mecanismo mediante el cual las transacciones de moneda virtual han de ser validadas -comprobando, por ejemplo, que el dinero a transferir existe y aun no se ha gastado- y los validadores son recompensados con una cierta cantidad de la moneda virtual. A raíz del éxito cosechado, otros han seguido sus pasos siendo ya superior a 1300 el número de criptomonedas funcionado con el mismo mecanismo, con diferentes variantes técnicas poco relevantes en general.

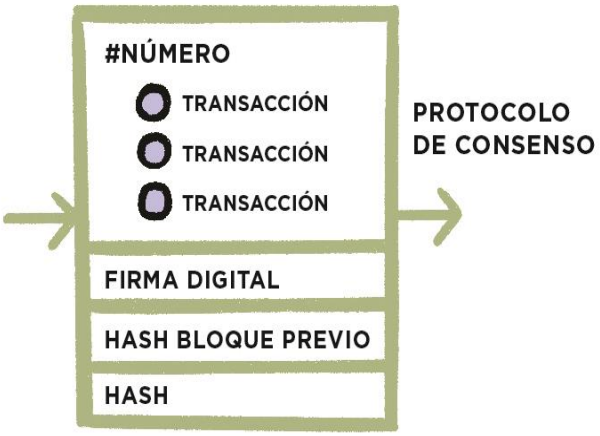
En cuanto a su aplicación fuera del mundo de las criptomonedas, en el que se centrará este documento, se ha venido estudiando y explorando desde 2008 el uso de la tecnología blockchain como una herramienta con múltiples aplicaciones en muy diversos campos. Algunos de los más atractivos son el registro de documentos de forma descentralizada, historiales médicos, registro de propiedad, organización y distribución de recursos energéticos, control de aduanas, sistemas de votación, identidad digital o monitorización de procesos de producción.

[1] **S. Habber, W.S. Stornetta –** ***How to time-stamp a digital document,*** **1991.**
[2] **Sathosi Nakamoto –** ***A Peer-to-Peer Electronic Cash System,*** **2008.**

Qué es blockchain

En términos generales, blockchain es registro de información **distribuido**[3] tipo **P2P (*Peer-to-Peer*)** en donde los diferentes participantes **no tienen por qué confiar los unos en los otros**, puesto que hay un **protocolo de consenso** que garantiza la seguridad y la veracidad de las transacciones. Otra de las características principales, y sin duda una de las más relevantes, es la **inmutabilidad de la cadena**; en blockchain no es posible editar o borrar información.

El término blockchain, o cadena de bloques en español, se debe a la estructura de esta base de datos, consistente en conjuntos de transacciones que son organizados y almacenados en bloques. Los bloques están **ordenados cronológicamente** y tienen un **número de bloque**, un código alfanumérico conocido como ***hash*** -sobre el que profundizaremos pronto- y están **firmados digitalmente** por la persona que encontró dicho código -la responsable de la validación del bloque-.



Desde la perspectiva inversa, pueden verse los bloques como conjuntos de transacciones a las que se les ha asignado un número de bloque y un código *hash*. En cuanto a la inmutabilidad de la cadena, en el caso de que se quiera cambiar una información que ha sido introducida en un bloque ya validado, la única forma de hacerlo será emitiendo una nueva transacción que actualice la información deseada. **En ningún caso será posible editar o borrar** nada que haya sido previamente validado y añadido a la cadena.

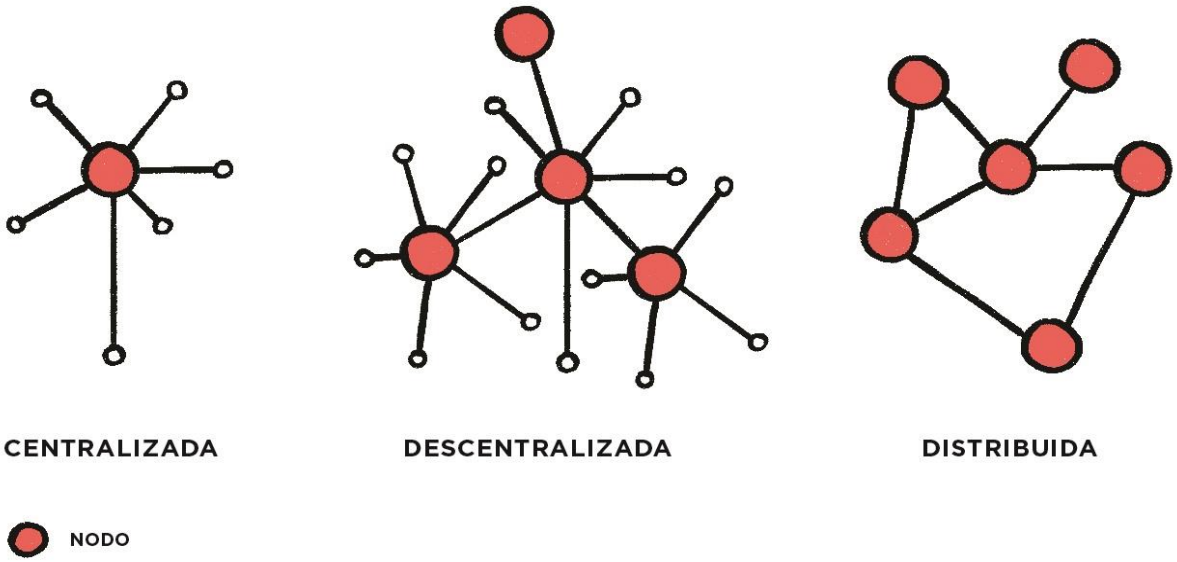
[3] **Aunque podría definirse como tal, técnicamente blockchain no es una base de datos ya que su propósito principal no es albergar datos si no registrar transacciones. De hecho, como comentaremos más adelante, muchas veces necesitamos una base de datos como complemento al blockchain para albergar documentos pesados que pueda haber, por razones de eficiencia. En caso contrario, las copias de la cadena de bloques en posesión de cada participante autorizado se volverían muy pesadas.**

a. Registro de información distribuido

Las bases de datos o registros de información centralizados pueden definirse como aquellos en las que los datos se almacenan en un único lugar físico -un único servidor- aunque sea accesible desde otros lugares y por diferentes entidades. Por contra, en las bases de datos descentralizadas y distribuidas la información se almacena en varios servidores.

Blockchain nace como una propuesta de registro de información distribuido, y opera de manera que cada una de las computadoras o servidores conectados a la base de datos tiene una **copia de todo el blockchain** o cadena de bloques.

No es solo una cuestión de donde se almacena la información, sino que también es una cuestión de quién está a cargo, y es que en blockchain todos los participantes no solo tienen una copia del blockchain sino que además se encuentran al **mismo nivel jerárquico** en cuanto a la toma de decisiones -proposición y validación de bloques- que los demás. Esto hace que se eluda completamente la necesidad de una entidad central. Ningún participante puede imponerse sobre los demás, hasta el punto de no poder añadir información nueva sin el consenso y la autorización de resto.



b. P2P (*Peer-to-Peer*)

P2P hace referencia al hecho de que la interacción entre los distintos participantes, que llamaremos de aquí en adelante **nodos**[4], se realiza por parejas. Los nodos no están conectados todos entre sí, sino **que cada uno está solamente conectado con un número determinado de ellos**. El valor de esto puede verse en términos de eficiencia y anonimato, como se explica en la página 33. Cuando un nodo quiere informar al resto de nodos de una transacción, le envía la información sobre la misma a aquellos con los que está conectado y estos la replican con aquellos con los que ellos, a su vez, están conectados. El proceso se itera hasta que la información es compartida por toda la red. Esto ocurre siempre así, a no ser que la transacción enviada sea inválida -por ejemplo, si se pretende enviar dinero que no existe-, en cuyo caso cuando los nodos la "escuchan" simplemente la ignoran.

c. No necesidad de confianza

En las bases de datos utilizadas tradicionalmente se asume que todos los participantes son de confianza, es decir, que ninguno de los nodos -en el lenguaje que estamos utilizando- va a introducir en la base de datos información no veraz. La idea revolucionaria de blockchain consiste en ofrecer un protocolo de consenso que permite que los distintos nodos no tengan por qué confiar unos en otros y aun así puedan compartir un registro de información confiable. El protocolo de consenso sirve para **evitar que bloques con información no veraz sean añadidos a la cadena** o que, si consiguiesen añadirse, sean rechazados por el resto de nodos.

---

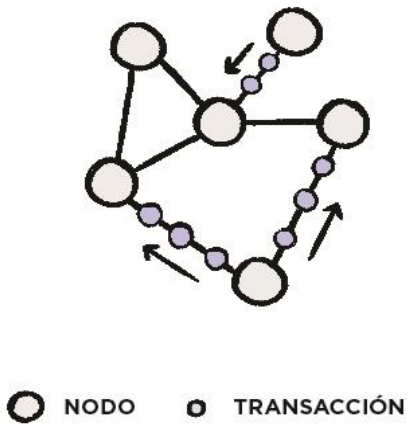
[4] El término nodo se utiliza en el lenguaje de las bases de datos para hacer referencia al servidor físico en el que se aloja la información. En el lenguaje de blockchain, este término es usado por extension para referirse a la persona o participante que está conectada al blockchain utilizando el servidor nodo, puesto que en las redes públicas, de las que hablaremos más adelante, todos los participantes van a interactuar como nodos con la red. En las redes privadas y federadas es necesario ser más preciso o explícito al definir los conceptos de nodo y participante.

Cómo funciona la tecnología blockchain

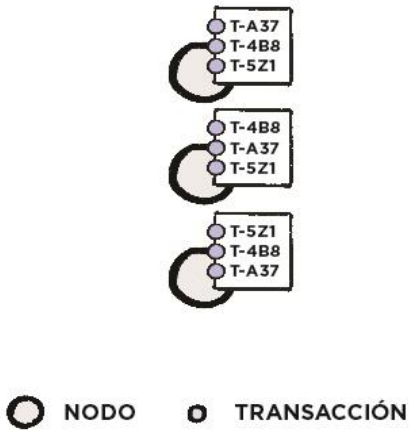
El proceso mediante el cual se genera información y se publican nuevos bloques válidos puede describirse en los siguientes 6 pasos. Es conveniente aclarar primero que el significado de la palabra **transacción**, en este contexto, engloba **cualquier tipo de intercambio de información susceptible de ser contenida en un bloque**. A saber, información sobre una transacción económica, sobre un contrato inteligente, sobre un cambio en los permisos de un usuario -en caso de que la red permita tal posibilidad- y un largo etcétera. En general, cualquier información que tenga que ver con la cadena de bloques, ya sea relativa a sus participantes o a la información que comparten entre ellos, queda registrada en un bloque del blockchain en forma de transacción.

Paso 0. Cualquier persona o colectivo de personas que quieran ser parte de la red tienen dos opciones en función del tipo de blockchain que se esté utilizando; **descargarse la aplicación correspondiente** que les convierte en un nodo con los mismos derechos que todos los demás **o acceder vía una interfaz web** que los nodos administradores hayan provisto para el resto de usuarios autorizados. La primera opción es generalmente la correspondiente a redes públicas, donde todo aquel que lo desee puede participar; solamente tiene que descargar el software correspondiente y este, de forma automática, se conectará con un número determinado de nodos y les preguntará por la copia más actualizada de la cadena. La opción alternativa corresponde a blockchains federados o privados, sobre los que profundizaremos más adelante. En estas cadenas de bloques habrá unos nodos privilegiados administrando la cadena y decidiendo cómo el “usuario promedio” accede a través de una interfaz web que ellos proveerán.

Paso 1. Una vez los participantes están conectados a la cadena, el primer paso consiste en enviar información en forma de transacciones que finalmente acabarán constituyendo los bloques de la misma. Es decir, cuando un nodo quiere realizar una transacción -ya sea una operación económica, un *Smart Contract*, etc-, le **envía la información sobre esa transacción a los nodos con los que está conectado**. Un primer protocolo actúa aquí de forma que automáticamente **cada nodo comprueba que las transacciones que "escucha" sean válidas**[5] -por ejemplo, que no se esté intentando transferir un dinero que ya haya sido gastado-. En caso de que la transacción sea correcta, **cada nodo la añade a su lista de transacciones** -que en lo sucesivo llamaremos por su nombre habitual en este contexto: ***pool***- y la reenvía a los nodos a los que cada uno de ellos está conectado. El proceso continúa pero no por siempre ya que, cuando a un nodo le llega información sobre una transacción que ya tiene en su lista, simplemente la ignora.

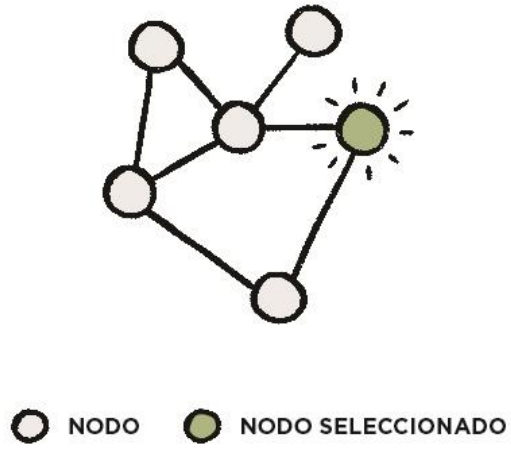


[5] **Dado que el concepto de transacción abarca cualquier tipo de información añadida a la red y que cada red tiene su propia arquitectura, la forma en la que se determina si una transacción es o no válida depende de cada caso particular.**



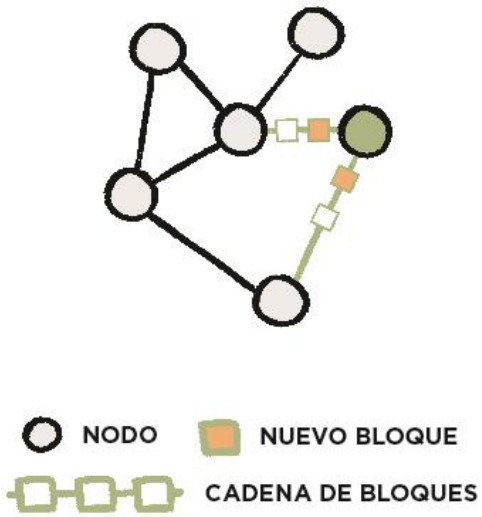
Paso 2. **Cada nodo va llenando su *pool*** con las transacciones que va escuchando. En general, los *pools* de dos nodos diferentes no tienen por qué coincidir puesto que lo normal es que escuchan las transacciones en distinto orden.

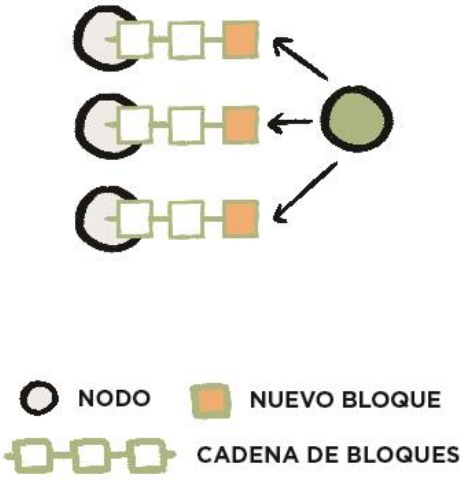
Paso 3. **En cada ronda** -que dependiendo del blockchain tiene lugar tras un tiempo que puede variar, en promedio, desde unos pocos segundos hasta varios minutos-, **un nodo es escogido aleatoriamente para proponer un bloque**. Este proceso es el más importante, siendo el que hace que blockchain sea una base de datos donde las distintas partes no tienen por qué confiar unas en otras. La forma en la que el nodo es escogido aleatoriamente se conoce como



protocolo de consenso y se explicará en la siguiente sección. La manera en la que el nodo elegido propone el bloque es tomando la versión actual de la cadena, añadiéndole al final un bloque que contenga las transacciones que había ido registrando en su *pool* y enviando esta nueva copia de la cadena a los nodos con los que está conectado, que a su vez la replicarán al resto de la red al igual que hacían con las transacciones individuales. Los bloques tienen un tamaño máximo que depende del blockchain, por lo que han de llenarse con un número limitado de transacciones.

Paso 4**. La persona elegida propone un bloque nuevo con las transacciones que ha ido "escuchando" y registrando en su *pool*.** Antes de ser enviado a los demás nodos, este bloque ha de ser validado con un ***hash*** -que es el código alfanumérico obtenido a partir de toda la información del bloque-. En la sección correspondiente hablaremos en profundidad de cómo se encuentra este código, quién lo hace y para qué sirve.





Paso 5. El sistema -los protocolos internos del blockchain- solo acepta el bloque si tiene un *hash* válido. En caso positivo, el resto de **nodos verifican** que todas las transacciones también sean correctas y **actualizan su copia de la cadena** con esta nueva versión que contiene el nuevo bloque.

Protocolos de consenso

El protocolo de consenso es el **procedimiento mediante el cual se elige a un nodo para proponer un nuevo bloque**. Se pretende que esta elección sea aleatoria, como comentábamos en la anterior sección, aunque no todos los participantes tienen la misma probabilidad de ganar el "sorteo".

El propósito de esta elección aleatoria es **evitar que haya un responsable único de la proposición de bloques**. Para ello, se pretende que todos los participantes puedan ser elegidos para proponer pero aquellos que tengan un mayor interés individual en el correcto desarrollo del blockchain tengan mayor probabilidad de ser elegidos -de ganar el sorteo- para proponer bloques.

Hay, fundamentalmente, dos formas de determinar este interés. La primera es **exigir a la personas o entidades que realicen un esfuerzo para competir por ser el elegido y darle una recompensa al ganador** -en forma de criptomoneda, en general-. La segunda es **distribuir las probabilidades de ganar el sorteo proporcionalmente al número de activos, propiedades o bienes en la red de cada participante.**

A continuación, se describen algunos de los procedimientos más utilizados como protocolos de consenso, basados en las dos metodologías anteriores.

Proof-of-Work (PoW)**.** PoW corresponde al grupo de protocolos de consenso donde **se exige un esfuerzo a los participantes en el sorteo para determinar quién propone el siguiente bloque, y se da una recompensa al ganador.** El esfuerzo aquí consiste **emplear capacidad computacional para encontrar el código *hash*** que valide el bloque anterior. En la siguiente sección hablaremos de cómo se obtiene, pero por el momento basta con decir que se necesita tener una computadora que realice intentos aleatorios para encontrarlo. Cuanto mayor es la potencia del ordenador, mayor es el consumo energético y mayor es la probabilidad de obtener el código válido.

Lo que ocurre entonces es que cuando alguien propone un nuevo bloque lo hace sin un código *hash*, de forma que **todos los nodos pueden competir por encontrarlo** -solo algunos lo hacen y son conocidos como mineros, ya que **al proceso de encontrar el *hash* se le conoce como minar**-.

Dado que emplear capacidad computacional para encontrar el *hash* implica gastar dinero, y que ningún nodo tiene la garantía de ser el primero en encontrarlo, parece poco razonable que un nodo maligno malgaste energía y dinero en ese propósito. Más aun teniendo en cuenta que, en caso de que ganase el sorteo y propusiese un bloque inválido, el resto de nodos lo rechazarían y se quedaría sin la recompensa.

Para motivar a los mineros no malignos a intentar encontrar los *hashes* válidos, los blockchain que implementan este método ofrecen una recompensa en forma de criptomoneda al primer nodo que lo encuentre -actualmente[6] la recompensa por cada bloque validado en Bitcoin es de 12.5 bitcoins, que equivalen a más de 185.000 dólares, y se valida un bloque cada 10 minutos en promedio-. Este método solo se puede usar, por tanto, en blockchains asociados a criptomonedas.

[6] **A día 9 de enero de 2018.**

Uno de los argumentos esgrimidos en contra de este protocolo es la **gran cantidad de energía empleada** -algunos dirían desperdiciada- en validar o minar los bloques. Por un lado es necesario decir que este proceso no sirve solamente para determinar quién propone el siguiente bloque sino que también redunda en la seguridad de la cadena. Como veremos en la siguiente sección, si alguien cambia algo en un bloque tanto ese bloque como todos los posteriores pasarán a tener un *hash* inválido que necesita ser minado de nuevo.

Por tanto, si alguien consiguiese modificar el blockchain tendría que volver a minar de nuevo no solo ese bloque sino todos los posteriores, y tendría que hacer eso en cada copia del blockchain que está en propiedad de cada nodo. Como es evidente, la dificultad que tendrá dicho hacker que superar será la misma que tuvieron los mineros iniciales. Cerrando el argumento, aquel que quiera corromper la red va a tener que gastar tanta energía en hacerlo como la que se gastó en validarla originalmente.

Por otro lado, también hay que decir que, a partir de un cierto nivel de dificultad en el *hash* -lo que implica un mayor gasto energético en encontrarlo-, la cadena puede considerarse suficientemente segura y la energía extra empleada para obtener *hashes* válidos de mayor dificultad puede considerarse desperdiciada. No solo eso, sino que hay otros métodos para aumentar la seguridad como pueden ser aumentar la descentralización -con más nodos manteniendo copias de la cadena-.

La razón por la cual, a pesar de ello, se gasta toda esta energía es que **la dificultad del *hash* no se configura en función de cuánta seguridad se pretende si no de cuál es el tiempo promedio que se pretende que los mineros tarden en minar**. Es decir, como los mineros compiten por encontrar el *hash* para cada bloque, si se fijase una dificultad de minado que aportase suficiente seguridad para la cadena, entonces cuando los mineros aumentasen en número o incrementasen sus recursos los bloques se minarían cada vez más rápido y por tanto más vacíos. Esto no interesa, de forma que lo que se fija es el tiempo promedio que se desea que tarden los bloques en ser minados -en Bitcoin son 10 minutos y cada 2 semanas aproximadamente se recalcula la dificultad de minado de forma que se satisfaga ese requisito-. Si, por ejemplo, se duplica el número de nodos o los nodos que ya hay duplican su capacidad computacional, entonces disminuirá el tiempo que tardan en minar y, tras el periodo establecido, se recalculará la dificultad de obtener el *hash* a la alza.

Para dar una idea en términos de energía consumida, según los datos ofrecidos por el sitio web digiconomist **el consumo anual de electricidad empleado en Bitcoin[7] es de 39.03 TWh,** que es del mismo orden que los 39 TWh que sirvieron para abastecer energéticamente a todo Perú el pasado año, según **worlddata.info**.

[7] **A día al 9 de enero de 2018.**

Proof-of-Stake (PoS). Tanto PoS como los protocolos que mencionaremos a continuación consisten en asignar mayor probabilidad de ganar el sorteo a aquellos que tienen más activos en la red. Aquí no hay personas compitiendo por validar el bloque y por tanto, en general, tampoco hay recompensa para quien lo consigue.

Leased-Proof-of-Stake (LPoS). LPoS una variación de PoS en la que usuarios con poco capital pueden ceder sus probabilidades de ganar el sorteo. En caso de que el nodo en el que hayan delegado resulte el ganador y haya algún tipo de recompensa por el minado, se reparte proporcionalmente entre él y las personas que lo apoyaron.

Delegated-Proof-of-Stake (DPoS). DPoS una variación de PoS en la que los nodos pueden proponer a cualquier otro nodo bien para validar bloques -a los que se conoce como testigos- o bien para decidir sobre las características, como tiempo entre bloques o tamaño del bloque, de la propia red -a los que se conoce como delegados-. Cuanto más poder tiene un nodo en la red, más cuenta su voto. Cada nodo propone un número de nodos suficiente como para que se considere suficientemente descentralizada la red, y la elección se repite tras un tiempo establecido.

Proof of Importance (PoI). PoI funciona como PoW pero asignando la probabilidad de ser elegido en función de la actividad -transacciones, balance o reputación- en la red del nodo en lugar de su dinero. La idea es la misma, premiar con el derecho de proposición de bloques a las personas que más interesadas están en el buen funcionamiento de la cadena, de forma que no les convenga proponer bloques maliciosos que puedan perjudicarla.

Es decir, en general los protocolos de consenso buscan que la persona que propone un bloque sea elegida de forma aleatoria, pero en esa elección o sorteo la probabilidad de que un nodo sea elegido se asigna de forma que se intente garantizar que la persona seleccionada no tenga interés en comportarse de forma malintencionada. Para ello, como indicábamos al principio, unos blockchains exigen aportar capacidad computacional que redunda en la seguridad de la cadena y dan una recompensa por ello. Otros blockchain, en cambio, asignan distintas probabilidades para ganar el sorteo de proponer el bloque en función de criterios como el dinero que tienen los participantes en la cadena, su actividad en ella, etc.

Seguridad de la cadena

Hay tres puntos a destacar en cuanto a la seguridad de la cadena.

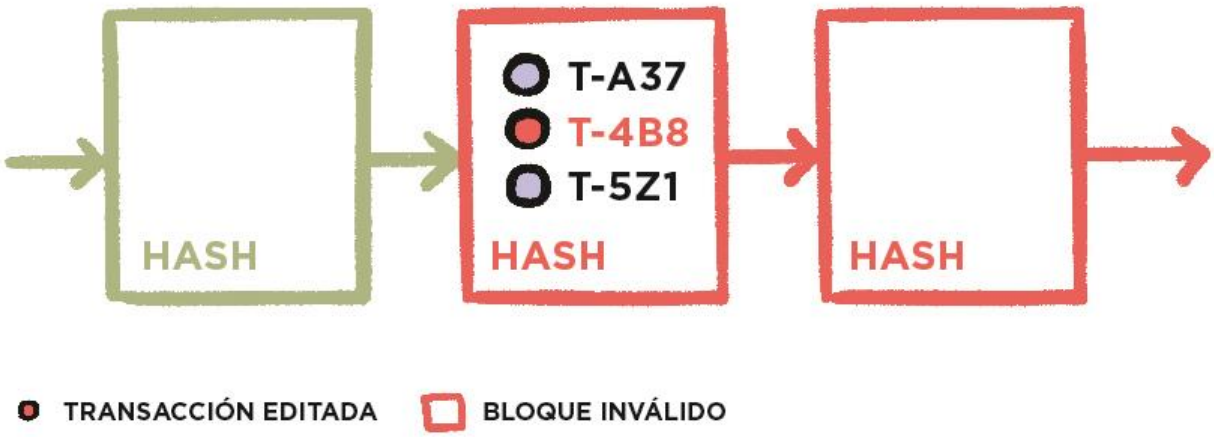
a. Hash

El *hash* es el código alfanumérico que se obtiene aplicando una función matemática, conocida como función *hash,* a un conjunto de datos concatenados. A cada conjunto de datos le corresponde un único *hash*. El objetivo de utilizar este *hash* en blockchain es tener toda la información de cada bloque condensada en un único código alfanumérico. Esto nos va a pemitir, como ahora veremos, **detectar cambios en los bloques mirando únicamente al *hash***.

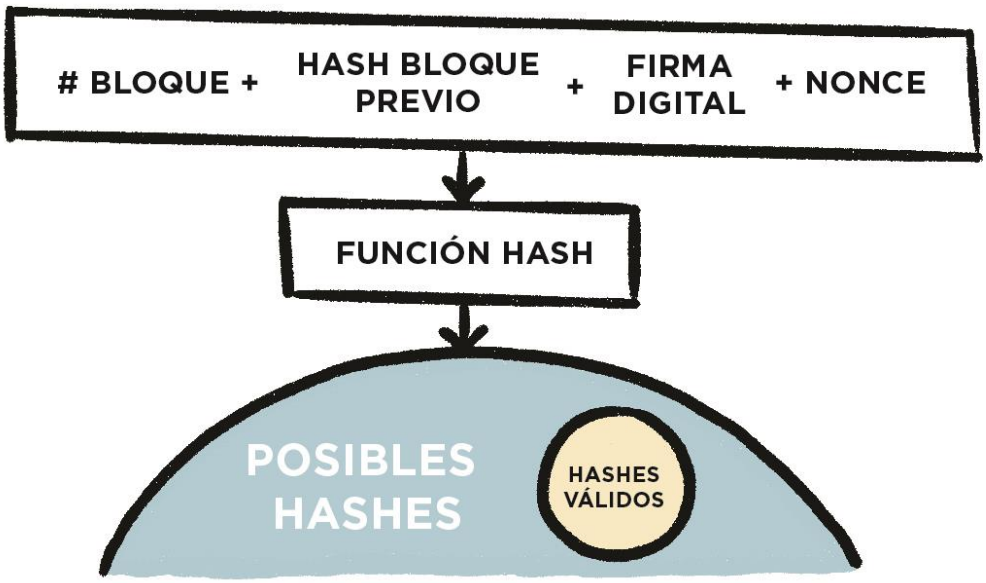
Si, llegados a este punto, nos preguntamos qué información se necesita concatenar para obtener el *hash*, la respuesta rápida es toda aquella información del bloque que queremos encriptar y sobre la que queremos poder detectar cambios. Esto es, el número del bloque, las transacciones que contiene y la firma digital de la persona que lo propone, que son las partes constituyentes del bloque tal y como se definió previamente.

Sin embargo, aunque es cierto que esto permite tener un *hash* único y diferente para cada bloque, en blockchain se introducen dos piezas más que son fundamentales para la seguridad de la cadena.

La primera pieza es el código *hash* del bloque previo. Hemos explicado que, **si se cambia algo en cualquier bloque, automáticamente el *hash* va a cambiar**, de forma que si el *hash* previo era el que identificábamos como válido, el nuevo lo detectaremos como fraudulento. Si en la concatenación para obtener el código *hash* de cada bloque introducimos, junto con los datos anteriores, el *hash* del bloque previo, entonces conseguimos que si alguien altera la información de un bloque, tanto el *hash* de ese bloque como los *hashes* de todos los posteriores pasarán a ser inválidos. Es decir, propagamos el error a todos los bloques posteriores de la cadena. **Esto nos permite poder detectar cualquier modificación de cualquier bloque de la cadena mirando solamente al último bloque.**



La segunda pieza a introducir es el *nonce*. **El *nonce* es un código alfanumérico totalmente aleatorio.** Pretendemos que el *hash* no solo nos sirva para identificar un bloque sino que además añada seguridad. Si simplemente concatenásemos el número de bloque, las transacciones, la firma y el *hash* del bloque previo para obtener el *hash* de cada bloque, al aplicar la función matemática siempre obtendríamos el mismo *hash* porque estamos aplicándosela a un conjunto fijo de elementos. Digamos que, por ejemplo, el código *hash* de una concatenación determinada es 9ka41k3h5j18403k298g. Lo que se hace es exigir que los *hashes* empiecen por un número determinado de ceros para que sean válidos, de forma que hay que introducir un elemento variable, que es el *nonce*, que concatenamos con el resto de elementos. **La forma de obtener un *hash* válido es, entonces, ir cambiando el *nonce* de forma aleatoria y aplicar la función *hash* hasta que el resultado -el código *hash*- empiece por el número de ceros exigido**. Si fuesen cinco ceros, un resultado válido sería por ejemplo 00000x92ka7r91ja9k3.



Lo que hacen entonces los mineros cuando el protocolo de consenso de la red es PoW, es probar *nonces* aleatoriamente hasta conseguir un *hash* válido. El primero que lo encuentra tiene derecho a proponer el bloque siguiente y, si este es aceptado, recibe la recompensa en forma de criptomoneda que la red haya establecido -en Bitcoin, tal y como comentábamos en la sección previa, la recompensa actual es de 12.5 Bitcoins y el tiempo promedio de minado es de un bloque cada 10 minutos-.

b. Capacidad de rechazar transacciones y bloques inválidos

Cuando a cada nodo le llega una transacción, automáticamente se verifica que las operaciones involucradas sean correctas -por ejemplo que quien realiza una venta sea poseedor del activo que vende- y que todo sea coherente y consistente. Igualmente, para que un bloque sea aceptado tiene que contener transacciones válidas y tener *hash* válido. En el caso de que un usuario consiguiese introducir un bloque malicioso en la cadena -supongamos que le tocó el turno aleatoriamente y propuso una versión maliciosa de la cadena con transacciones incorrectas-, no sería ninguna catástrofe. Si el siguiente usuario al que aleatoriamente le toca proponer un bloque no es malintencionado también, entonces propondrá su nueva versión de la cadena obviando el bloque malicioso anterior y añadiendo en su lugar el que él propone. Se conoce como *Byzantine Fault Tolerant* la capacidad de superar la adversidad de tener individuos maliciosos en una red que requiere de consenso.

c. Protocolos de consenso, descentralización y teoría de juegos

Los protocolos de consenso permiten tener una base de datos distribuida en la que las distintas partes, sin necesidad de confiar unas en otras, puedan estar seguras de que la información que comparten y aceptan es veraz, y puedan además rechazar una información que no lo sea, en el caso de que consiga colarse en la red. Además, dado que PoW requiere del empleo de capacidad computacional para validar bloques y en PoS se va a penalizar tu *stake* -que viene a ser tu valoración dentro de la red- en caso de que actúes de forma negativa para la red, y teniendo en cuenta que tu actuación maliciosa va a poder ser rechazada por el resto de la misma, estudios utilizando la teoría de juegos concluyen que la forma más beneficiosa para una persona en una cadena blockchain es siempre actuar en beneficio de la red, ya que este será el suyo propio.

Tipos de Blockchain

Pueden fácilmente distinguirse al menos tres tipos de redes blockchain: las públicas, las federadas y las privadas. Cabe mencionar asimismo la opción *Blockchain as a Service* para almacenamiento en la nube.

Públicas. Las redes blockchain públicas son aquellas a las que **cualquier persona tiene acceso**. En general, el procedimiento para participar es descargarse la aplicación correspondiente y conectarse, de forma automática, con un determinado número de nodos a los que se les pregunta por la versión más actualizada de la cadena. Una vez el nodo está actualizado, tiene los mismos derechos y deberes que el resto de participantes a la hora de proponer y validar transacciones, replicar las transacciones que escucha o minar -si desea hacerlo-. También en su mayoría, la seguridad de estas redes está basada en protocolos de consenso y funciones *hash*, y los usuarios interactúan con la red de forma anónima.

Federadas. Los blockchain federados son un concepto de red diferente a los públicos e incluso podrían considerarse una tecnología diferente, puesto que no satisfacen en muchas ocasiones la definición o descripción que hemos abordado en las secciones previas. **Estos blockchain han ido surgiendo con la idea de servir como bases de datos descentralizadas que pueden generar confianza en entornos complejos, con entidades con diferentes intereses y usuarios sin conocimientos.** En general no son públicos, sino que **un número determinado de organizaciones, entidades o compañías se encargan de administrar la red y mantener copias sincronizadas**. El acceso mayoritario es en este caso mediante una **interfaz web** que estos administradores ponen a disposición del usuario medio.

Es por eso de vital importancia, a la hora de diseñar e implementar soluciones de este tipo, **acompañar a la herramienta blockchain con un plan estratégico adecuado** consistente en definir desde **quiénes y cómo van a administrar la red** hasta **qué información se les va a mostrar a los usuarios vía interfaz web.**

En muchos casos el usuario que accede vía web puede no tener interés ni conocimiento sobre blockchain, pero sí necesitar un plataforma que involucre entidades diferentes, necesidad de confianza y transparencia. Un blockchain federado puede ser entonces una buena opción siempre que las reglas del juego establecidas en la administración y mantenimiento de la cadena sean las adecuadas y se ofrezca al usuario, a través de la interfaz web, el grado de transparencia requerido.

Queda claro entonces que, al ser su acceso vía web y no como nodos de pleno derecho, **los usuarios comunes tendrán acceso a tanta información como se les decida mostrar** a través de la misma. Se tendrán entonces opciones que varien desde un gran nivel de transparencia hasta una transparencia nula.

En minado de bloques actúa aquí también de forma diferente. En general ahora la red ni siquiera tendrá una criptomoneda asociada, de forma que **el minado de bloques con recompensa que tenía lugar en las redes públicas es inexistente**. Sin embargo, sigue siendo necesario que los bloques tengan un *hash.* ¿Quién es entonces el encargado de encontrarlo? Una opción razonable es que las propias organizaciones o entidades al mando de la red se encarguen de proporcionar y mantener servidores que cumplan con este propósito. Es decir, **la labor del minado que en las redes públicas es el corazón que las mantiene vivas y es responsabilidad de los usuarios, ahora pasa a jugar un papel secundario y son los administradores de la red quienes se encargan de proporcionar los recursos energéticos necesarios para encontrar *hashes*** -o minar-.

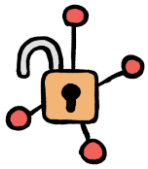
Actualmente hay varias opciones de código abierto para construir un blockchain federado como Hyperledger, Corda, EFW o Multichain donde puedes descargar la aplicación de blockchain y programar la cadena a tu gusto, decidiendo quién quieres que participe, bajo qué reglas se regulan las transacciones, etc. Las redes públicas como Ethereum o Litecoin también ofrecen la oportunidad de hacer un *fork*[8] para crear entornos federados o privados.

Privadas. Los blockchain privados son aquellos en los que el control está reducido a una única entidad que se encarga de mantener la cadena, dar permisos a los usuarios que se desea que participen, proponer transacciones y aceptar los bloques. Son iguales que las federadas pero con solo una entidad a cargo, de forma que además de todas las diferencias que las federadas y las públicas tienen, hay que añadir también que se pierde la descentralización.

Blockchain as a Service (BaaS): Algunas grandes compañías ofrecen servicios de almacenamiento de los datos de tu blockchain en la nube. Algunos ejemplos son IBM especializada en Hyperledger Fabric, Amazon colaborando con Digital Currency Group, o Microsoft ofreciendo servicios de R3, Hyperledger Fabric o Quorum, entre otras. Generalmente, las ventajas de este tipo de servicios son un aumento en la seguridad, la no necesidad de invertir en hardware y la posibilidad de un entorno más amigable con el que trabajar, pudiendo crear tu propio canal de blockchain sin necesidad de programar.

[8] Un *fork* a la situación en la cual se crea una nueva rama a partir de un punto en una cadena blockchain de forma temporal -*soft fork*- o permanente -*hard fork*- que implementa sus propias reglas con respecto a características como el tamaño del bloque, por ejemplo.

Comparativa entre los tipos de blockchain




	Públicos Bitcoin, Ethereum, Litecoin	**Privados** Hyperledger, Corda, Quorum	**Federados** Hyperledger, Corda, Quorum	***Blockchain as a Service*** IBM, Microsoft, Amazon
Cualquiera puede participar	✓	✗	✗	NA
Los participantes actúan, en general, como nodos	✓	✗	✗	NA
Transparencia	✓	≈	≈	NA
Hay un único administrador	✗	✓	✗	NA
Hay más de un administrador	✗	✗	✓	NA
No hay administradores	✓	✗	✗	NA
Ningún participante tiene más derechos que los demás	✓	✗	✗	NA
Se pueden implementar Smart *Contracts*	✓	✓	✓	NA
Existe recompensa por minado de bloques	≈	✗	✗	NA
Soluciona problema de falta de confianza	✓	✗	≈	NA
Seguridad basada en protocolos de consenso	✓	✗	≈	NA
Seguridad basada en funciones *hash*	✓	≈	≈	NA
Provee servicios en la nube	NA	NA	NA	✓

Características y aplicaciones de blockchain

Entre las características que convierten a blockchain en una herramienta útil pueden destacarse **transparencia, descentralización y no necesidad de intermediarios.**

En concepto de **transparencia**, o la forma en que se consigue, es diferente dependiendo del tipo de red que estemos utilizado. **En las redes públicas, en general, la transparencia es total** puesto que cualquier usuario que se registre en la cadena es provisto de una copia de todo el blockchain, pudiendo ver en ella el estado actual de los activos y el historial de transacciones. **En las redes privadas y federadas el acceso es restringido y mediante vía web para la mayoría de los usuarios, como comentábamos en la sección previa. Para estos usuarios el nivel de transparencia es el que los administradores de la red decidan ofrecerles mediante esta interfaz web.**

La **descentralización** es un requisito determinante a la hora de decidir si blockchain es o no una buena herramienta para un caso concreto. En la medida en que la descentralización es deseada, blockchain gana enteros. Si, en cambio, se pretende tener una base de datos centralizada, entonces blockchain en general no va a ser en absoluto la mejor opción. La descentralización consiste básicamente en determinar el número de nodos que van a mantener la cadena. Sin embargo, es interesante mencionar que esto no implica necesariamente transparencia, puesto que **los propios nodos pueden tener diferentes roles dentro del sistema que les den acceso a un tipo determinado de información, teniendo vetado el acceso a cierto contenido de la red.**

El tener distintos servidores con una copia sincronizada de la cadena añade un gran valor en cuanto a seguridad, dado que **si alguna consiguiese modificar o corromper una de las copias, sería tan sencillo como re-sincronizarla con las demás.**

En cuanto a la **no necesidad de intermediarios**, conviene hacer énfasis en las palabras “no necesidad”. Blockchain nace con Bitcoin para evitar necesidad de que instituciones financieras tengan que intervenir o verificar transacciones monetarias -o cryptomonetarias- entre individuos, de forma que aquí la eliminación de la intermediación de las mismas era un objetivo deseado y conseguido.

Sin embargo, a la hora de diseñar un blockchain privado o federado la situación es diferente. Podría ser que, en un sistema funcionando con blockchain consistente en el envío de un producto o un material determinado de un lugar a otro, **sea de interés para las dos partes realizar ciertos controles intermedios**. Digamos, por ejemplo, que se pretende llevar a cabo un envío de productos alimenticios que requiere unos ciertos controles de humedad y temperatura durante su transporte en avión y barco. **Las dos partes establecerían entonces el acuerdo -en forma de *Smart Contract*- de los parámetros a evaluar en los controles y el pago a realizar en caso de que todo siga su curso de la forma deseada.**

Estas instituciones podrían tener su propio nodo provisto solo con permisos para ver información sobre las condiciones de temperatura y humedad que tienen que verificar, y no podrían saber en ningún momento cuál es el precio que se ha acordado pagar por el cargamento, por ejemplo. Al finalizar satisfactoriamente el proceso establecido en el *Smart Contract*, el dinero se transferiría automáticamente al vendedor.

Entre los numerosos casos de uso de esta tecnología de esta forma son interesantes las posibilidades de aplicación para elecciones políticas transparentes y públicas, registro de procesos de fabricación de ropa o comida -al que luego se podría tener acceso mediante un código QR en el producto-, registro de propiedad -los gobiernos de Georgia, Honduras o Suecia han sido pioneros explorando esta vía-, todo tipo de operaciones como alquileres o ventas de propiedades sin necesidad de intermediarios, controles de aduanas, registros médicos, IPFS -almacenamiento de datos inter-planetario- y un largo etcétera.

Smart Contracts & IoT

Los *Smart Contracts* o Contratos Inteligentes son un elemento fundamental de la tecnología blockchain, ya que **establecen y definen cómo y quién puede llevar a cabo qué transacciones**. Son contratos en los que se definen y especifican una serie de cláusulas, como los controles a cumplir por la mercancía mencionados en la sección previa y el pago final acordado en caso de que estos sean superados. La diferencia con los contratos usuales es que estos **son incorporados a un blockchain o cadena de bloques en la red, que garantiza su seguridad y proporciona el entorno adecuado para su realización autónoma.**

Por **IoT** -Internet de las Cosas en castellano- se entiende la **red de objetos, instrumentos o dispositivos conectados a internet**, que van desde un automóvil hasta una lavadora. Distintas estimaciones calculan que en 2020 el número de dispositivos conectados a internet será de entre 25 y 30 millones. Estos dispositivos son de gran utilidad como complemento a la tecnología blockchain, puesto que permiten la comprobación automática de cláusulas establecidas en los *Smart Contracts*. Esto acelera, abarata y optimiza la realización de las transacciones. Los dispositivos inteligentes que envíen información al blockchain han de tener una identidad digital que les permita firmar digitalmente dicha información, dado que en caso contrario la información no sería de confianza.

Cómo identificar cuándo blockchain es una herramienta útil[9]

Como hemos venido discutiendo, blockchain tiene unas características determinadas y ofrece unas prestaciones concretas. A la hora de responder la pregunta de si blockchain es útil para un caso determinado conviene considerar en primer lugar es que **blockchain no es una solución en sí misma. Blockchain es una herramienta tecnológica que ha de ser rodeada de un plan estratégico que entienda las necesidades del proyecto, identifique el grado de transparencia y descentralización, determine los miembros que actuarán como nodos y establezca la estructura de blockchain adecuada**, definiendo cómo van a ser las transacciones y/o los *Smart Contracts* a ejecutar. Blockchain es un software que permite crear cosas muy diferentes entre sí, por lo que la implementación concreta que se lleve a cabo será determinante a la hora de decir si añade valor o no.

Esencialmente, blockchain será útil en la medida que el caso de uso tenga necesidad de descentralización, registro inmutable, transparencia, consenso y validación.

Una forma de ver si blockchain es necesario y útil es hacerse una serie de preguntas como las que ahora vamos a detallar, y ver si entre las respuestas aparecen los anteriores 5 componentes. Dado que en la actualidad hay un gran interés en blockchain, no son pocas las veces que se pretende hacer algo con blockchain sin saber qué. Nuestro punto de vista es que como entrenamiento para entender la tecnología es positivo, pero de cara a querer llevar un proyecto a una fase de producción es altamente desaconsejable. Es por eso que la primera pregunta que consideramos hay que plantearse es:

[9] **El enfoque estratégico que se presenta en esta sección corresponde a la labor realizada por Mariana Gutierrez, y será ampliado en futuras versiones de este documento.**

- ¿Cuál es el problema que se está tratando de resolver?

  Esto evita empezar con “quiero utilizar blockchain para algo”. Es imposible encontrar una buena solución si no se tiene bien definido un problema, y **es imposible saber si utilizar blockchain y cómo sin saber para qué.**

- ¿Quién va a tener acceso a la red blockchain? ¿Quién va a administrar los permisos?

  Es importante establecer bien quién y cómo va a participar en la red. **Si es una red privada o federada, habrá que diseñar cuidadosamente la estructura de nodos y las transacciones que cada uno puede efectuar y/o validar**. En cuanto al acceso web para los usuarios corrientes, en el caso de haberlo, también será importante estudiar qué se les va a mostrar y cómo se va a mostrar. No es necesario que el usuario sepa que detrás de la interfaz web que está utilizando hay una red blockchain al igual que ahora no tiene información de qué base de datos utilizan las páginas que frecuenta. Ahora bien, como comentábamos anteriormente, si se quiere utilizar blockchain por motivos de transparencia, entonces no solo se le informará de que está utilizando blockchain sino que se aprovechará para hacerle participe quizás del historial de transacciones o incluso de ciertas validaciones.

- ¿Son de diferentes categorías (gobiernos, empresas, trabajadores, …)?

  Cuanto más diferentes sean los participantes de la red, más complejos habrán de ser los consensos y más variadas serán las transacciones, y ahí es donde blockchain puede ayudar. Cada organización podrá desempeñar un papel distinto y a la vez importante para el sistema.

  Por ejemplo, para una red de registro de vehículos en un país determinado podría ser que el gobierno, la agencia tributaria, las aseguradoras y las grandes empresas de compra/venta de vehículos fuese nodos de la red. Cada usuario accedería a través de la interfaz web proporcionada para dicho propósito y tendría acceso a la ficha técnica de su vehículo.

A la hora de realizar una compra/venta, comprador y vendedor informarían al sistema vía página web y la transacción sería validada por la aseguradora -verificando que todo estaba en regla con respecto a pagos del seguro-, la agencia tributaria -tomando nota de los impuestos y verificando igualmente que no hay insolvencia o deudas por ninguna de las partes- y el ministerio correspondiente -que daría el visto bueno y tomaría nota para sus propios registros.

- ¿Confían los distintos participantes unos en otros? En caso contrario, ¿cuáles son las causas de disputa? ¿Tienen intereses diferentes?

  De nuevo **blockchain es de mayor utilidad cuanto más dispersos son los intereses**, puesto que **va a obligar a los participantes a llegar a acuerdos en cuanto a las reglas del juego** -acerca de cómo serán permisos, transacciones, *Smart Contracts*-. **Sin embargo, es necesario decir que blockchain no va a obligar a los participantes a dejar de ser corruptos**; si estos establecen unas reglas del juego deficientes que les permiten actuar de forma maligna o si se conceden permisos de validación a entidades que no van a realizar su trabajo de forma honesta, blockchain no va a poder evitarlo.

  De ahí que volvamos a hacer énfasis en **lo importante que es envolver la herramienta blockchain con una buena solución que emerja de un correcto estudio del problema**. Bien es cierto, eso sí, que blockchain va a ofrecer siempre un registro de las transacciones realizadas y que, si bien no puede evitar que haya comportamientos fraudulentos si un número determinado de nodos se ponen de acuerdo en acometerlos, al menos va a quedar registrado.

- ¿Hay intermediarios involucrados? ¿Quién o quiénes serán encargados de validar? ¿Cuáles son las reglas para validar?

  El involucramiento de intermediarios no es algo negativo pero sí ha de ser bien manejado puesto que, como venimos comentando, la puerta de entrada para la corrupción del sistema está en las validaciones. **Si se le da a un intermediario la posibilidad de validar habrá que estudiar la forma más eficiente y segura para la red de hacerlo.**

- ¿Cuál es el presupuesto?

  Dado que la tecnología no está pensada para soluciones a pequeñas escalas y las posibles implementaciones componen un abanico muy grande y diverso, es imposible estimar un presupuesto general sobre cuánto puede costar una solución utilizando blockchain. Es interesante, sin embargo, detallar los diferentes componentes de la solución.

  En lo relativo al blockchain, se necesitarán recursos para financiar la **programación de la cadena** en la etapa inicial y el **minado de transacciones** una vez esté en funcionamiento.

  En cuanto a la primera, actualmente hay varias opciones de software gratuito que cualquier desarrollador podría utilizar. La dificultad a la hora de programar reside en el número de nodos que vayan a participar, el número de activos que se vayan a intercambiar y la dificultad en las transacciones o *Smart Contracts* a llevar a cabo. Por ejemplo, una solución utilizando blockchain en la que dos compañías intercambien un único certificado será mucho más económica que otra en la que el gobierno de un país desee albergar el registro de automóviles de toda la población, con múltiples posibilidades de intercambio de información entre ellos.

En cuanto al minado de transacciones, es importante diferenciar si el blockchain estará sobre una red pública o en un ambiente privado o federado**. En las redes públicas la dificultad de minado y el tamaño de bloque están predefinidos**, por lo que **el costo de validación de cada transacción no podrá ser controlado** y dependerá de cada red. En la red Ethereum la tasa promedio por transacción a finales de 2017 es de entre uno y dos dólares, mientras que en Bitcoin alcanzó los 50. Si bien muchas otras redes tienen tasas mucho más bajas, un ambiente aislado podría ser más interesante para un proyecto ambicioso que requiriese un gran volumen de transacciones. En una red **aislada - como serían las federadas o privadas- se puede elegir el tamaño del bloque y la dificultad del minado**. Por tanto, el costo vendría dado por el número de computadoras necesarias -y en este caso provistas por los administradores- para minar las transacciones realizadas en la red, sin estar condicionado a agentes externos.

Si bien estos son los dos aspectos económicos a tener en cuenta en cuanto a la herramienta blockchain, esto no constituye toda la solución. En la solución completa será necesario conectar el blockchain con una **interfaz web** que también habrá de ser diseñada e implementada, y en la mayoría de los casos acompañarla con una **base de datos** que albergue los documentos -ya que en el blockchain solo se almacenan los *hashes* de los mismos-.

Actualmente la mayoría de los proyectos empleando blockchain se encuentran en fase de piloto, que parece lo más recomendable para comenzar dada la fase prematura de la tecnología y la muy probable gran envergadura de la solución. Varias compañías tienen equipos que ofrecen levantar un piloto en un plazo de 3 meses.

Cómo empezar a construir una solución con blockchain

Una vez se haya definido con claridad el problema que se quiere resolver; se haya analizado el grado de descentralización, transparencia, consenso y validación; se hayan identificado los participantes y se haya llegado a la conclusión de que blockchain es la herramienta adecuada para comenzar a resolver el problema, es el momento de comenzar a usar dicha herramienta.

Una forma de hacerlo es clasificar en tres grupos todos los elementos que van a estar involucrados en la solución. Vamos primero a definirlos y después veremos un ejemplo.

- **Participantes:** Los participantes son todos aquellos colectivos que van a jugar un papel, desde las compañías que administran la red -en el caso de que las haya- hasta los usuarios de a pie, pasando por entidades auditoras, instituciones financieras, etc. La pregunta que hay que hacerse es **quién es cada grupo**, **cuáles son los permisos que tiene sobre la red** -es decir, si va a interactuar con ella a través de un sitio web, si va a mantener una copia de toda la cadena, si va a poder ver solo las transacciones en las que participe o va a tener acceso a más información, etc.- y **cuáles van a ser las transacciones que va a poder realizar.**

- **Activos/haberes/valores:** Una vez tenemos claro quién va a participar, necesitamos saber **qué van a intercambiar**. Quizás ahora pueda parecer un poco abstracto, pero la forma de entender este grupo es pensar que **cuando los participantes hacen una transacción, ciertamente están transfiriendo algo**. Ese algo es el activo, y puede ser desde un certificado o documento -en realidad en el blockchain no se guardan los documentos en si sino solo su *hash*-, un *token* que dé por ejemplo derecho a voto en una votación, una certificación, etc.

- **Transacciones:** El tercer elemento son las transacciones. Si bien ya sabemos quién va a jugar y cuáles van a ser los juguetes, falta definir cuáles van a ser las reglas del juego. Sin las transacciones tenemos a todo el mundo estático sin poder moverse, y son estas las que permiten que la rueda empiece a girar. **Las transacciones son las operaciones mediante las cuales los participantes crean, intercambian, modifican o destruyen activos.** Además, al definir las transacciones podemos también **especificar qué participantes tienen permisos para realizar una determinada transacción** y **cuáles son las validaciones necesarias** para que esa transacción se procese y se añada al blockchain. Como hemos venido manteniendo en este documento, una transacción es en realidad cualquier cambio o actualización que se lleve a cabo en la red que es recogido en los bloques del blockchain.

Veamos un ejemplo. Supongamos que una empresa uruguaya quiere exportar un cargamento de carne a México. El gobierno mexicano exige que la carne esté certificada como libre de aftosa y que no sobrepase una temperatura determinada en todo el recorrido. Con este objetivo, se realizará un control periódico de la temperatura, digamos cada 15 minutos, en el contenedor en el que viaja la carne. Si la carne llega a México teniendo el certificado “libre de aftosa” y sin haber superado la temperatura exigida, se desea que el gobierno mexicano realice el pago acordado a la empresa uruguaya. ¿Cómo sería en este caso una solución utilizando blockchain?

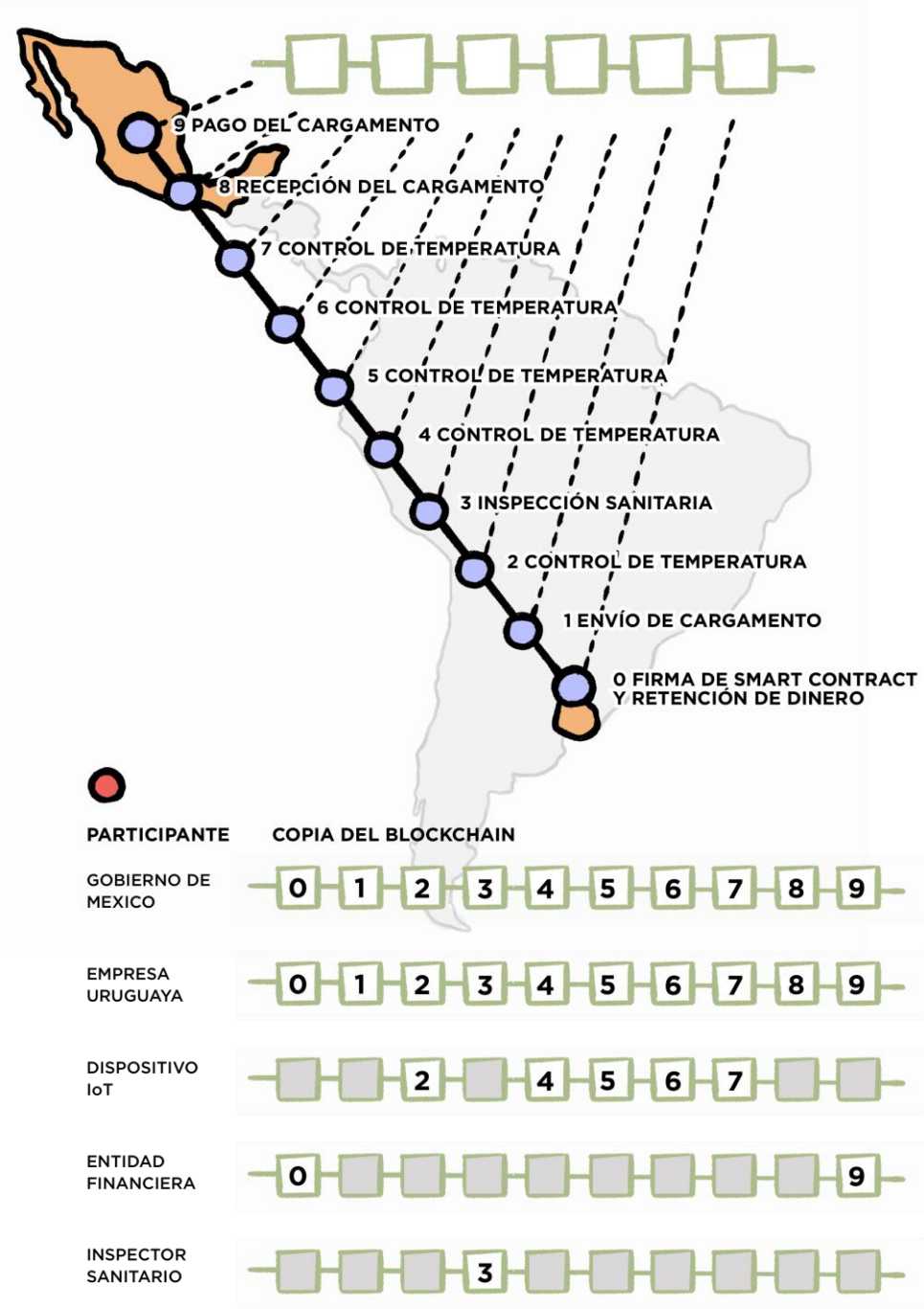
- **Participantes:** La empresa exportadora uruguaya, el gobierno de México, una entidad financiera que retendrá el dinero de México mientras el cargamento viaja, un dispositivo IoT que va a enviar información periódica sobre la temperatura del contenedor, una entidad certificadora que compruebe que el cargamento está libre de aftosa y emita el correspondiente certificado y una posible entidad auditora que supervise todo el proceso.

- **Activos/haberes/valores:** Los activos aquí podrían ser el certificado de que la mercancía está libre de aftosa y el historial de evolución de la temperatura medido por el dispositivo IoT.

- **Transacciones:** Las transacciones podrían ser la notificación del envío del cargamento de Uruguay, la notificación de depósito de pago, la emisión del certificado de ausencia de aftosa, la información sobre las medidas periódicas del dispositivo IoT, la notificación de llegada del cargamento y la notificación de la realización del pago.

La forma en la que el proceso tendría lugar sería entonces la siguiente:

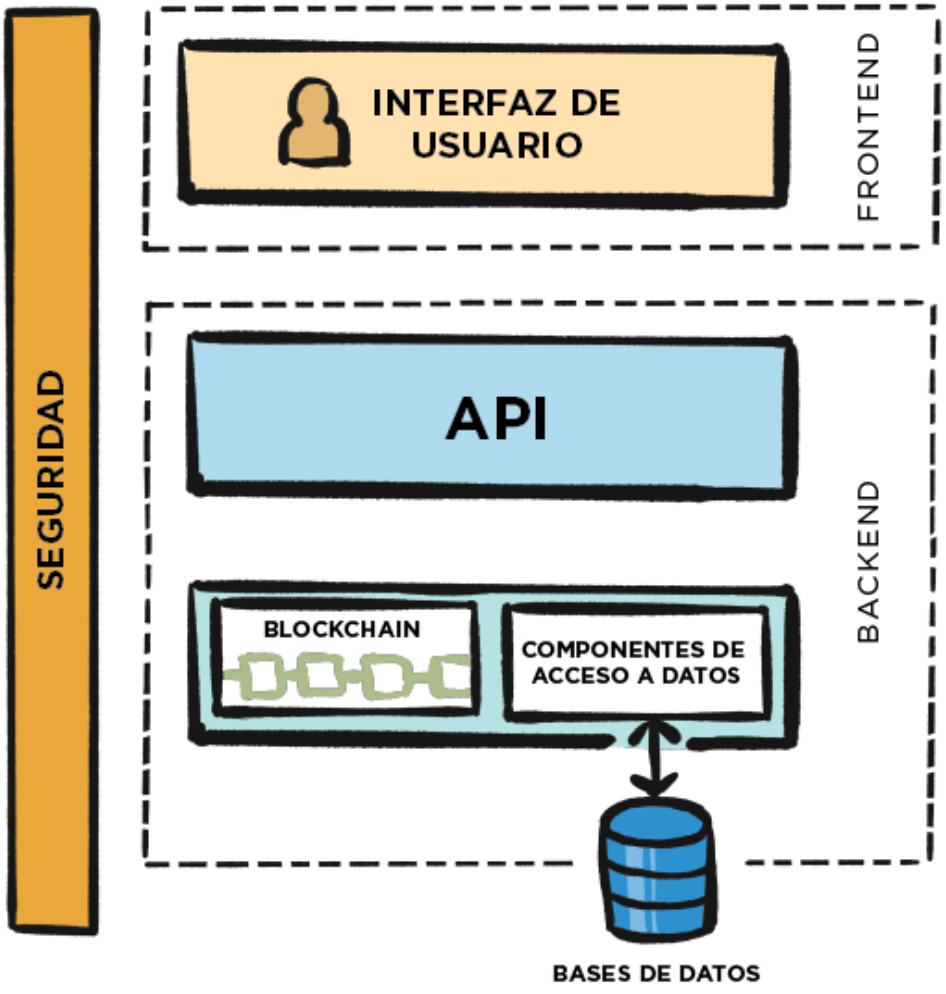
0. La empresa uruguaya y el gobierno de México firman un acuerdo -en forma de *Smart Contract*- mediante el cual todo lo anterior se implementa en un blockchain, y el gobierno de México reserva el dinero acordado en la entidad financiera correspondiente para ser enviado si todo procede de la forma establecida.
1. La empresa exportadora uruguaya envía el cargamento y notifica en el blockchain que ha sido así.
2. La entidad asignada verifica que el producto está en las condiciones requeridas y emite el certificado “libre de aftosa” que se registra en el blockchain.
3. El dispositivo inteligente colocado en el interior del contenedor envía cada 15 minutos el valor de la temperatura al blockchain.
4. El contenedor llega al punto de recepción del gobierno mexicano, emitiéndose la notificación correspondiente en el blockchain.
5. La entidad financiera que tenía retenido el dinero del gobierno mexicano lo libera en favor de la empresa uruguaya.


9 PAGO DEL CARGAMENTO
8 RECEPCIÓN DEL CARGAMENTO
7 CONTROL DE TEMPERATURA
6 CONTROL DE TEMPERATURA
5 CONTROL DE TEMPERATURA
4 CONTROL DE TEMPERATURA
3 INSPECCIÓN SANITARIA
2 CONTROL DE TEMPERATURA
1 ENVÍO DE CARGAMENTO
0 FIRMA DE SMART CONTRACT Y RETENCIÓN DE DINERO
PARTICIPANTE
COPIA DEL BLOCKCHAIN
GOBIERNO DE MEXICO
0 1 2 3 4 5 6 7 8 9
EMPRESA URUGUAYA
0 1 2 3 4 5 6 7 8 9
DISPOSITIVO IoT
2 4 5 6 7
ENTIDAD FINANCIERA
0 9
INSPECTOR SANITARIO
3

Arquitectura del blockchain

A lo largo del documento hemos insistido mucho en que blockchain no es una solución sino una herramienta. La solución está compuesta por el entero proceso consiste en, al menos, el entendimiento del problema, la identificación de los actores, la selección de la tecnología y la implementación de la misma.

Es conveniente indicar que, en una solución que utilice blockchain, será frecuente encontrarse con otros dos componentes además del blockchain, a saber, interfaz web y base de datos.



Hemos hablando con cierto detalle sobre cómo en las redes federadas y privadas lo habitual es tener una **interfaz web** a través de la cual los usuarios interactúan con el sistema. Asimismo, también es necesario indicar que los documentos pesados no se guardan en el blockchain sino que se almacenan en una **base de datos**, siendo el *hash* resultado de encriptar ese documento lo que sí se guarda en el blockchain.

Un diagrama sencillo que ilustra una posible arquitectura simple y genérica podría ser el que se muestra en la página anterior. En el diseño propuesto, a los usuarios se les proporciona un acceso web o móvil que consume una API. Por debajo, tenemos el blockchain y una capa de acceso a datos que se encarga, en caso necesario, de controlar el intercambio de información con las bases de datos. El usuario genérico tendría su usuario y contraseña de acceso para acceder a la información en la interfaz web y solo las entidades designadas tendrían una copia del blockchain y acceso a las bases de datos.

Anonimato

En las redes privadas y federadas con propósitos sociales, empresariales y/o comerciales los usuarios corresponden o bien a organizaciones bien identificadas o bien a usuarios que acceden mediante la web, igualmente acreditados. En general el anonimato es inexistente.

En las redes públicas asociadas a criptomonedas, en cambio, los usuarios interactúan con el blockchain de forma anónima. Se registran con una clave privada y muestran a los demás usuarios su clave pública. Dado que todo el historial es público, basta con asociar la identidad real de una persona con su clave pública una sola vez para poder seguir todo su rastro.

Hay procedimientos para evitar que esta identificación pueda tener lugar. Se conoce como *mixing* al proceso mediante el cual varios usuarios realizan el mismo ingreso en una "caja negra" que devuelve las mismas cantidades a unas nuevas carteras que los participantes iniciales han facilitado. Esta redistribución se realiza de forma que las entradas y las salidas se relacionan aleatoriamente, dificultando la posibilidad de rastreo. Algunas redes de criptomonedas tienen la capacidad de implementar procesos de este tipo en el propio código de la red y se facilita la posibilidad de llevarlo a cabo en cada transacción.

También es interesante comentar que, aunque pueda parecer que lo más eficiente es que cada nodo esté conectado con todos los demás, esto iría en perjuicio del anonimato. Si cada nodo estuviese conectado con todos los demás, cuando un nodo reciba información de una transacción sabrá que quien la está realizando es precisamente quien se le está enviando esa información. Esto le permitiría relacionar la IP del nodo que le está enviando la información de la transacción con la clave pública que en esa transacción está realizando la transferencia, y por tanto podría fácilmente desvelar la identidad de los usuarios.

Conclusiones

Durante los últimos años, blockchain se ha convertido en una de las tecnologías que más interés suscita a nivel global. Instituciones gubernamentales, organizaciones internacionales o grandes empresas están intentando construir soluciones haciendo uso de estas cadenas de bloques.

Pese a que la tecnología, aunque ingeniosa, no es excesivamente compleja, sí lo es el construir una solución a gran escala donde cada participante entienda, respete y cumpla su función. Es por eso que, a medida que un proyecto gana envergadura, los desafíos no son solo tecnológicos sino que la dificultad también reside en juntar a todos los actores bajo un mismo consenso y unas mismas reglas.

En este documento se ha tratado de explicar el funcionamiento de blockchain, resaltando las características que la convierten en una tecnología diferente. También hemos querido, sin embargo, dejar claro que blockchain no es una solución sino una herramienta y que, consecuentemente, al igual que un martillo es bueno para clavar clavos pero no para atornillar tornillos, blockchain no es siempre la mejor opción. Una forma de empezar a discernir si blockchain nos va a ser útil en un determinado caso es hacerse una serie de preguntas como las que hemos establecido en la sección *Cómo identificar cuándo blockchain es útil.*

Una vez se tiene el problema bien establecido y acotado, y la solución identificada, es momento de hacer el ejercicio de organizarla y estructurarla. En el caso de que esa solución tenga un componente de blockchain, una posible forma de hacerlo se ha proporcionado en la sección *Cómo empezar a construir una solución con blockchain.*

Cabe también mencionar que en proyectos a gran escala son importantes la validación y el aprendizaje en fases intermedias. Es por eso que, una vez realizados los dos pasos anteriores y antes de pasar a producción, hemos recomendado comenzar con un piloto que ponga en práctica el prototipo diseñado, valide que los participantes sepan cómo interactuar con la solución, que lo hagan de forma correcta y que les aporte lo buscado.

En cuanto a los desafíos a los que se enfrentará blockchain en el futuro, es necesario hablar de la llegada de las nuevas tecnologías cuánticas. Estas, como contaremos con detalle en la próxima publicación, cambiarán por completo las técnicas de encriptación y ciberseguridad en la próxima década. Si bien la tecnología blockchain podrá continuar siendo segura y útil, tendrá que someterse a ciertos cambios para adaptarse a esta nueva era.

Sin duda, en los próximos años veremos si blockchain ha venido para quedarse o simplemente ha sido una moda pasajera. En cualquier caso, es una idea inteligente digna de ser explicada, entendida y explorada.

Criptomonedas

Bitcoin nace en 2009. Tras su éxito, muchas otras criptomonedas han creado su propio blockchain. Actualmente hay más de 1300 criptomonedas en circulación. Hasta hace unos meses -septiembre de 2017- Bitcoin acaparaba prácticamente el 50% de la capitalización total de las criptomonedas y la mayoría del volumen de mercado diario. En los últimos dos meses -diciembre de 2017 y enero de 2018- ha habido una auténtica fiebre primero con Bitcoin y después con una gran cantidad de criptomonedas alternativas, conocidas como Altcoins.

Bitcoin comenzó con un precio de $0.06 por unidad[10]. Actualmente su valor es de $15,261.80. Como se puede ver en la imagen, los primeros años su precio aumentó de forma moderada hasta finales de 2013, donde tuvo lugar el primer crecimiento exponencial. A finales del pasado año 2017 ha tenido lugar el segundo crecimiento exponencial, disparando su precio desde $2.735,99 el 1 de agosto de 2017 a los más de $19.535,70 que llegó a alcanzar el 17 del mismo año. Esto supone un aumento del 714%, esto es, su valor aumentó en 7.14 veces en solo 4 meses y medio.

[10] **Todos los datos numéricos relativos a las criptomonedas, así como el gráfico, son cortesía de** https://coinmarketcap.com.

Para ponerlo en perspectiva, en el mismo periodo las acciones de Amazon aumentaron de $996.19 dólares a $1174,14-, lo que equivale a un aumento del 118%, es decir, prácticamente 7 veces menos rentable[11].

Evolución del precio de las acciones de Amazon desde enero de 2017 hasta enero de 2018.

La capitalización de mercado a día 9 de enero de 2018 es de casi $257.000 millones, con un volumen diario de unos $20 millones. En el último mes el número de criptomonedas con más de $1.000 millones de capitalización de mercado era 12, mientras que ahora ya son 43.

La mayoría de las criptomonedas utilizan *proof-of work* como protocolo de consenso, incluyendo Bitcoin y Ethereum que son las dos más relevantes.

[11] La fuente de los datos y el gráfico correspondientes a las acciones de Amazon es http://www.nasdaq.com.

¿Para qué sirven las criptomonedas?

Como cualquier moneda fiduiciaria, las criptomonedas sirven como un activo en el que invertir y como forma de pago.

Inversión: Dada su tendencia general a la alza, las criptomonedas más asentadas han venido siendo una buena inversión a medio plazo. A corto plazo su volatilidad en 24 horas ha venido siendo de en torno al 10% en promedio. Dado que las más longevas solo tienen de vida 9 años, no hay precedentes sobre lo que ocurrirá a largo plazo.

Método de pago: Actualmente algunas de las compañías más conocidas que aceptan Bitcoins son Expedia, eGifter, Save the Children, Microsoft, Overstock.com, Newegg, Shopify stores, Wikipedia, Peach Airlines o Tesla. Otras compañías como Amazon están valorando la posibilidad de incorporarlo también. Quizás en el futuro próximo algunos comercios locales o industrias pequeñas se sumen a la iniciativa.

Formas de obtener divisa de criptomoneda.

En general, hay cuatro formas de conseguir criptomoneda.

1. *Genesis Block*: Cuando se crea una criptomoneda, generalmente en el primer bloque se envía divisa a un número determinado de participantes con la intención de motivarlos a utilizarla. Esta es la única manera de obtener criptomoneda "gratis".

2. *Minning*: En las redes que funcionan con PoW, y en algunas que utilizan PoS, se recompensa con divisa a las personas que emplean capacidad computacional para obtener el *hash* de los bloques. Como se dijo en la explicación de los protocolos de consenso, solo obtiene recompensa el ganador de la competición. En los blockchains criptomonetarios más importantes la gente está organizada en *minning pools*, que son grupos de personas uniendo recursos computacionales bajo la supervisión de un gestor que divide en partes proporcionales las recompensas en caso del minado. Esto hace difícil que mineros aislados puedan tener éxito y abre el debate sobre la descentralización real de la red.

3. *Transaction Fees*: Los distintos nodos que realizan transacciones u otras operaciones que han de ser validadas por la comunidad pueden dejar una recompensa para la persona encargada de minar. En Ethereum se conocen como gas y dependen de la dificultad de cada transacción o *Smart Contract*. En Bitcoin, si bien no eran algo relevante hasta hace poco, con la gran congestión de transacciones actual, estos "intereses" para los mineros se han disparado. Cuando la recompensa por minado llegue a su fin -todas las emisiones de criptomoneda tienen una fecha límite para que la cantidad de moneda emitida sea fija- se espera que estas comisiones sigan motivando a los mineros para validar transacciones y bloques.

4. *Trading*: Como cualquier activo, siempre puede intercambiarse por otro, ya sea dinero fiduiciario, otra criptomoneda o cualquier otro bien, siempre que haya alguien dispuesto a ello. Hay multitud de casas de intercambio en la red que facilitan una interfaz amigable mediante la cual conseguir una cartera virtual con la que poder comprar y vender criptomonedas. La contrapartida es que exigen prueba de identidad, cobran comisiones y si son hackeadas y roban la dirección de tu cartera de su página pierdes todo tu dinero. Para comprar Bitcoin, Ethereum, BitcoinCash o Litecoin las más utilizadas son **Coinbase** y **Kraken**. En ellas puedes adquirir estas criptomonedas a cambio de divisas reales. Para invertir en Altcoins menos habituales hay que utilizar Bitcoins o Ethereums -en general- adquiridos en los sitios web recién mencionados y enviarlos a otros como **Binance** o **Kucoin** donde puedes intercambiarlos por estas otras monedas.