ntroducción

Cuando empezamos a interesarnos por blockchain, nos impresionó el entusiasmo que suscita esta tecnología nueva, fruto de una combinación brillante de tecnologías ya probadas. De hecho, creemos que su fuerza reside en este aspecto de su creación. Para ilustrar nuestra afirmación, en una entrevista realizada a la portavoz del Mercado Único Digital de la Comisión Europea, Nathalie Vandystadt, en 2018, la portavoz declaró «los servicios basados en blockchain tienen el potencial de establecer servicios digitales descentralizados, confiables y orientados hacia el usuario. Esto estimula nuevos modelos de negocio que benefician a nuestra sociedad y a la economía» (Rafael Gómez Torres, 7 de julio, 2018). Todo esto solo ha servido para aumentar nuestro interés por blockchain e incrementar nuestra curiosidad por su funcionamiento.

En este capítulo, vamos a exponer nuestro punto de vista sobre blockchain, siempre intentando desvelar el secreto que rodea a esta tecnología tan prometedora como misteriosa.

Antes de hablar de blockchain, vamos a empezar por describir el contexto tecnológico que agita, y a veces incluso revoluciona, el sector financiero. Recordemos que la primera blockchain es la que subyace en el funcionamiento del bitcoin, esta criptomoneda que tenía la pretensión de destronar a los bancos centrales. Todo empezó en el sector financiero.

Durante estos últimos años, un germen revolucionario ha hecho su aparición en el sector financiero. La desaparición de los intermediarios bancarios iniciada por las tecnologías financieras, o “fintechs”, marca una etapa nueva, porque, hasta ahora, esta revolución, que permitió liberarse de las instituciones financieras, solo había afectado a las tarjetas de crédito y a algunos valores financieros como las obligaciones. Sin embargo, el objetivo de estas fintechs es revolucionar algunas funciones del banquero, hasta el punto de que estos empleos bancarios están amenazados. Permiten proteger los sistemas de pago, administrar los ahorros, prestar dinero, servir de intermediario a los inversores, y todo esto de una manera distinta, sin pasar por un banco o una institución financiera. La única diferencia notable con el sistema tradicional es la interacción con el cliente, que evoluciona y se perfecciona, especialmente gracias a las nuevas tecnologías, como Big Data y los algoritmos de Machine Learning, y también gracias a los nuevos medios de comunicación cada vez más eficientes.

En las décadas anteriores, los bancos españoles tardaron en adoptar nuevos medios de comunicación, funcionamiento y análisis, con el pretexto de la seguridad y la importancia de reunirse con el cliente de manera directa (el contacto con el cliente). Creyeron que la satisfacción del cliente pasaría principalmente por el contacto físico, que concordaba con sus procesos y costumbres en sus organizaciones sucesivas. Esta confusión los ha colocado en competencia directa con las fintechs, que deberán integrar y con las que tendrán que contemporizar. Las consecuencias de las fintechs de segunda generación para el sector bancario, financiero y económico en términos generales serán más importantes y tendrán un impacto mayor. Esta generación está representada por blockchain mediante todo un conjunto de procesos y protocolos de verificación y de validación distribuidos en una red, y no depende de una entidad central reguladora que garantice la confianza entre los miembros de la red. Las aplicaciones de blockchain son muy numerosas y no se reducen a los sectores bancario y financiero. Podría estar presente en los campos de la validación de transacciones, la protección de datos privados e incluso de las interacciones entre personas y objetos.

La eliminación de intermediarios y de terceros de confianza permite la reducción de los costes de las transferencias creando un sistema que administra él mismo las interacciones entre los participantes y la validación de las transacciones. Esta tecnología distribuida puede alcanzar este objetivo. Varios sectores o entidades se verán afectados (bancos, redes sociales, comunicación, intercambios, industria farmacéutica, etc.). Incluso los estados verán amenazada una de las bases de su soberanía: garantizar la confianza de sus ciudadanos.

Desembocamos en una arquitectura descentralizada en lugar de una arquitectura centralizada.

La siguiente figura representa las dos arquitecturas: centralizada y distribuida.

Diagrama

Descripción generada automáticamente

*Diferencia entre registro distribuido y registro centralizado (Fuente: Wikipedia)*

Es probable que se produzcan muchas transformaciones en el futuro y por eso es fundamental comprender los impactos y los retos, tanto para un responsable como para un actor de la transformación. Esta sección es esencial para los neófitos en blockchain y ofrece una introducción antes de entrar en el meollo del tema. El enfoque consiste en describir los distintos tipos de blockchain, sus componentes y su funcionamiento.

# Blockchain privada, de consorcio y pública

No existe una tecnología blockchain, pero, en el sentido estricto del término, hay cientos, con variaciones a veces muy técnicas, a menudo comerciales. En la selva de las tecnologías, es posible clasificarlas como blockchains denominadas privadas, de consorcio y públicas. Esta tipología se explica brevemente porque hablaremos de ella con más detalle en el capítulo siguiente.

## **1. Blockchain privada (con permisos)**

Una blockchain privada es una aplicación de la tecnología donde una persona debe dar la autorización para acceder. La gestión de la infraestructura, sus normas de gestión y su funcionamiento están completamente centralizados. Permite hacer intercambios de información entre distintos socios. La información inscrita se fecha y se firma. Esto permite garantizar que la información se ha intercambiado correctamente en una fecha y hora determinadas, y se puede identificar a su autor.

El nivel de seguridad nativo es elevado, los intercambios están encriptados y se conoce a los actores por el nombre. De manera predeterminada, hay una tabla de correspondencia a disposición del administrador para hacer una correspondencia entre un alias y una persona física, en blockchain solo se inscribe el alias, respetando las recomendaciones legales europeas y españolas.

En la práctica, no se habla forzosamente de una blockchain, sino más bien de un registro distribuido. Cuando todos los emisores de información son conocidos fiables, no es necesario tener un componente técnico que controle la veracidad de la información, solo que se ha realizado una operación.

El uso de una blockchain exclusivamente privada es una curiosidad en el plano técnico, porque desde el inicio se libera de la propiedad distribuida y no tiene autoridad de control. Sin embargo, ofrece muchas ventajas atractivas para las instituciones durante su implementación, como una gobernanza simplificada, actores conocidos, costes reducidos, la rapidez y la confidencialidad. Los casos prácticos se explicarán más adelante.

## **2. Blockchain de consorcio (permisionada)**

En esencia, una blockchain permisionada es comparable a una blockchain privada. Se agrega una cantidad de actores mayor procedentes de razones sociales distintas y en los que no es obligatorio confiar completamente.

El acceso a esta blockchain es menos centralizado, porque la autorización del acceso se hace habitualmente mediante el intermediario de una autoridad para cada empresa participante. La función de esta autoridad es administrar los accesos de manera delegada. Por lo tanto, los actores son conocidos y es muy recomendable utilizar una lógica de alias para identificarlos.

Con el fin de asegurar la fiabilidad de una información y la convergencia de una solución a un problema, un mecanismo debe garantizar la confianza en la red y los datos que circulan por ella. Se trata de un algoritmo de consenso. El más conocido, que alcanzó la fama gracias al bitcoin, es la "prueba de trabajo" o *proof-of-work* en inglés.

## **3. Blockchain pública (no permisionada)**

Una blockchain pública es un registro distribuido donde todos pueden leer y escribir sin pasar por una autoridad reguladora central. Por eso se habla también de solución sin permisos. Hay varias blockchains públicas y todo el mundo tiene derecho a crear la suya. Como sustitutas de las redes centralizadas, estas blockchains tienen un funcionamiento basado en principios criptoeconómicos definidos por Vitalik Buterin:

"*La combinación de incitaciones económicas y los mecanismos de verificación que utilizan la criptografía como una prueba de trabajo o prueba de la participación.*"

Dicho de otra manera, se anima a todos a participar en la verificación de las transacciones mediante ventajas económicas. La parte que puede tomar cada uno en el proceso de consenso se define en función de los recursos que puede poner a disposición. Pero el riesgo con este modo de funcionamiento es que el tratamiento se realice finalmente en grandes equipos de mineros extremadamente poderosos. Entonces, el funcionamiento puede parecerse a una blockchain pública con un funcionamiento de blockchain de consorcio.

Sin embargo, las blockchain públicas están completamente descentralizadas y pueden presentar riesgos considerables en los planes técnicos y de gobierno.

## **4. La gobernanza de la blockchain**

El grado de gobernanza depende del tipo de blockchain. Cuanto más abierta es, menos puede influir un actor concreto en la gobernanza.

En una blockchain pública, los nudos de red se encargan de validar las opciones analizadas e iniciadas por los desarrolladores decidiendo aprobar o no las modificaciones propuestas. La única norma de funcionamiento la define la tecnología (según la expresión «El código es la ley» del jurista americano Lawrence Lessig). Este planteamiento implica numerosos fallos y la experiencia de estos diez últimos años ha aportado muchas enseñanzas.

En un contexto de blockchain privada o de consenso, las normas de gobernanza son extrañamente diversas. En un grupo de empresas, el ejercicio puede volverse sensible con rapidez y se necesitan métodos de trabajo especializados con un personal cualificado. No se trata solo de ponerse de acuerdo sobre los actores susceptibles de leer o escribir en la blockchain. Las normas de negocio, las responsabilidades y la visibilidad de algunos datos exigen un gran rigor en la negociación e implementación.

# Componentes tecnológicos

Blockchain es una sabia combinación de componentes tecnológicos. La teoría de juegos se mezcla con protocolos informáticos y conceptos de programación raramente observados en los contextos digitales más convencionales.

En esta sección presentamos los componentes técnicos que dan soporte a lo que se agrupa bajo el término blockchain.

## **1. Los bloques: entidades que forman Blockchain**

El componente fundamental de una blockchain es un bloque. En otros autores, también se puede encontrar el término subregistro. Un bloque es un objeto informático independiente que agrupa a un conjunto de informaciones (por ej.: transacciones entre actores) organizadas para que un sistema informático pueda agregarlas en una cadena de bloques: una blockchain.

Las explicaciones que aparecen a continuación tratan fundamentalmente sobre la estructura de un bloque en el interior de la blockchain Bitcoin. Se pueden observar modificaciones de implementación en las tecnologías que concurren, pero los principios fundacionales son los mismos.

Los subregistros que forman la blockchain están protegidos contra todo tipo de manipulaciones o modificaciones. Cada subregistro está vinculado a su predecesor mediante un identificador, lo que permite tener un historial en cuanto a la incorporación de los subregistros. El primer subregistro que sirve para la construcción de la blockchain es el subregistro *Génesis*, o *bloque Génesis* (*Genesis block*). El vínculo entre los subregistros permite recorrer toda la blockchain en sentido inverso hasta el Génesis. Esta arquitectura se basa en el árbol de Merkle (Merkle, 1987).

Cada subregistro contiene una cantidad de verificaciones que garantizan su integridad y lo protegen contra cualquier modificación garantizándole una identificación. La verificación de esta información constituye la primera etapa de verificación, que eliminará los subregistros mal formados (sintaxis incorrecta) y los que ya se han tratado.

Los bloques se emiten a una gran cantidad de actores que los validan. La implementación de un método matemático denominado algoritmo de consenso elimina las duplicidades con la finalidad de conservar una sola copia para todos los actores de la red. Así, un bloque, incluso emitido a escala planetaria, se encuentra en última posición escrito en el registro una sola y única vez.

La cuestión que se plantea ahora es el envío de bloques.

## **2. El intercambio entre pares**

Las tecnológicas blockchains utilizan un protocolo de intercambio entre pares para enviar y recibir información entre dos nudos que van a validar transacciones. Sin embargo, además de este protocolo de intercambio, la seguridad está a cargo de una lógica de firmas electrónicas y un cifrado de datos transmitidos a través de una red.

### a. Metodología de envío de los datos: la red entre pares (P2P)

La definición comúnmente admitida de un sistema entre pares, o *peer-to-peer* en inglés (P2P), es la siguiente: permite que varios ordenadores o nudos se comuniquen mediante una red, donde comparten informaciones de manera sencilla y directa. Estas informaciones son de distintas naturalezas: objetos, archivos, pero también flujos continuos, un servicio o potencia de cálculo (cálculo distribuido).

La singularidad de los sistemas entre pares reside en el hecho de que los datos se pueden transferir directamente entre dos nudos conectados a la red, sin pasar por un servidor central. Así permiten que todos los nudos desempeñen directamente el papel de cliente y de servidor (Moore, 2001).

La figura que aparece más abajo representa una red entre pares con intercambios directos entre los nudos

Diagrama, Icono

Descripción generada automáticamente

*Red entre pares*

Para ello se requiere que cada nudo utilice un software especial. Este software se llama *servant*, una contracción de las palabras «servidor» y «cliente», que representan las dos funciones que cumple un *servant*. El término «entre pares» tiene su origen en la palabra «par»: las comunicaciones y los intercambios se hacen entre nudos que tienen la misma responsabilidad en el sistema.

Los sistemas para compartir archivos entre pares permiten distribuir la información en toda la red poniéndola a disposición de todos los participantes. La información se duplicará una cantidad de veces muy elevada, lo que también le garantiza una forma de eternidad. Cuanto más presente está la información en una gran cantidad de nudos, más disminuye la carga en relación con las peticiones en la red. Así se consigue aumentar la cantidad de informaciones o archivos en esta red, es un cambio de nivel.

Las funciones de este modelo van más allá de la simple puesta en común de archivos, porque es la base de un servicio descentralizado, haciendo que estén disponibles en la red diversos recursos, de distintas naturalezas, denominados objetos. Todos los nudos son independientes e interactúan entre ellos, ofreciendo o recibiendo objetos.

De esta manera, el sistema entre pares facilita la operación de compartir información y permite distribuirla entre todos los participantes, haciendo que los ataques maliciosos y los fraudes sean cada vez más difíciles. Debido a estas propiedades, los sistemas entre pares son los preferidos para la descentralización del servicio porque garantizan una cierta disponibilidad de los objetos con un coste de mantenimiento bajo (como en el caso del código abierto). Sin embargo, parecen ser sistemas más complejos de diseñar.

Una cuestión recurrente cuando se trata el tema de estos sistemas entre pares es la de la seguridad e integridad de los objetos. Los usuarios, en general, buscan el anonimato. Para garantizar el anonimato de estos usuarios, en las aplicaciones se ponen en práctica uno o varios conceptos como la interferencia del protocolo y el cifrado de los datos.

También se pueden utilizar otros protocolos. Cada uno tiene sus ventajas e inconvenientes. Sin embargo, en el ámbito del Bitcoin se utiliza principalmente el protocolo P2P y sigue siendo la norma en multitud de tecnologías blockchain.

## **3. La firma digital**

La firma digital representa una de las aplicaciones de criptografía por clave pública que ofrece ventajas esenciales en la verificación, la autentificación y la validación del origen de la información recibida por un destinatario. Las tecnologías blockchain utilizan estos mecanismos de manera casi sistemática para estos fines.

La firma digital también permite garantizar que esta información está intacta y no ha sido modificada por un tercero con una finalidad fraudulenta. Igualmente, la firma electrónica por clave pública ofrece una prueba de no repudio, para que el expedidor asuma todas sus responsabilidades respecto al envío de esta información. Por eso desempeña un papel principal en la criptografía y la confidencialidad de la información transmitida y de su expedidor.

Conceptualmente, la firma electrónica es parecida a la firma manual y tiene las mismas funciones, pero es sensiblemente más robusta.

### a. La criptografía o el cifrado de los datos

Una implementación de blockchain cifra de manera predeterminada los envíos de datos a través de una red. El mecanismo de cifrado se explica detalladamente en el capítulo La criptografía y blockchain.

En el vocabulario de la criptografía, un texto sin cifrar (texto plano) está formado por datos comprensibles, legibles y vírgenes de toda intervención específica. La ocultación de estos datos se realiza mediante procedimientos de encriptado. La criptografía, o el encriptado, consiste en utilizar funciones matemáticas o procesos analíticos para transformar una información normal y sin cifrar en una jerga ininteligible, que representa el texto cifrado.

El encriptado permite transferir la información de manera precisa y garantizar que solo podrán aprovechar la información los destinatarios de la misma. El desencriptado, que representa el proceso inverso, permite transformar texto incomprensible en información inteligible.

La palabra «criptografía» procede del griego antiguo *kruptos* (que significa «ocultar») y *graphein* (que significa «escribir»). El uso de la criptografía se remonta a la antigüedad. Ya en esa época era necesario guardar información en secreto. Durante el siglo XX, y especialmente durante y después de la Segunda Guerra Mundial, aumentó su popularidad y se encumbró al nivel de ciencia o disciplina de pleno derecho. Más tarde, la aparición de los ordenadores ha permitido su desarrollo.

Una función hash permite transformar una información o mensaje de tamaño y naturaleza diversos en una serie de caracteres de longitud constante y que parece haberse generado aleatoriamente. Lo que permite no tener ninguna indicación del mensaje de origen. La primera función hash que apareció fue la MD2. Después, le siguieron muchas como la MD4, MD5, SHA-1, SHA-256, RIPEMD160 y Whirlpool. Actualmente, las más utilizadas son SHA-1 y MD5. Sin embargo, se han vaticinado ataques a estas dos funciones hash. El NIST (*National Institute of Standards and Technology*, Instituto Nacional de Estándares y Tecnología) convoca concursos con regularidad para encontrar nuevas funciones hash más seguras e incluso procedimientos de encriptado nuevos.

Mientras que la finalidad de la criptografía es proteger los datos, el objetivo del criptoanálisis es estudiar la información encriptada para poder descubrir su secreto y utilizarla. Numerosos estudios tratan el criptoanálisis en distintos ámbitos como el razonamiento analítico, las matemáticas, la modelización, las probabilidades y las herramientas estocásticas o aleatorias. Esta combinación de varias disciplinas representa la combinación necesaria que debe reunir todo criptoanalista o pirata, según las circunstancias. Para generar texto cifrado, es primordial estar en posesión de una clave pública y de una clave privada, que representan los vínculos entre el emisor de un mensaje y el mensaje encriptado. Desde el punto de vista de la informática, es imposible adivinar la clave privada a partir de la clave pública. Solo pueden desencriptar los datos las personas que poseen la clave privada correspondiente a la clave pública utilizada para encriptarlos. Este vínculo entre la clave privada y la pública es primordial en el proceso de encriptado-desencriptado.

El intercambio de mensajes y de información de manera protegida representa la primera ventaja de la criptografía de clave pública. Ya no es necesario el intercambio de claves privadas o secretas entre las distintas partes. La clave pública es suficiente para evaluar la integridad del mensaje y la identidad de su emisor. Lo que representa una ventaja considerable en lo que respecta a la seguridad. Este sistema se ilustra en la figura siguiente.

Texto

Descripción generada automáticamente

*Esquema de cifrado con clave pública. La clave pública permite encriptar y la clave privada permite desencriptar.*

Elgamal (que toma el nombre de su inventor, Taher Elgamal), RSA (que toma el nombre de sus inventores, Ron Rivest, Adi Shamir y Leonard Adleman), Diffie-Hellman (que también toma el nombre de sus inventores) y DSA (el algoritmo de firma digital creado por David Kravitz) son ejemplos de sistemas criptográficos con clave pública.

### b. Las funciones de hash y las claves

El cifrado es eficaz para los datos sencillos como el texto y los números. Sin embargo, en el caso del intercambio de documentos, el cifrado y la firma electrónica son especialmente obligatorios. El proceso es muy lento, utiliza mucha potencia de cálculo y el volumen de datos al final del cifrado puede ser más voluminoso que el documento original. Un gran número de usos de blockchain exigen poder certificar que un documento se ha sustituido correctamente. Por eso necesitamos un mecanismo nuevo.

El uso de una función de hash irreversible (en un solo sentido) permite tener un esquema criptográfico más eficiente. Las funciones de hash toman como entrada una longitud variable e indefinida de unidades de información, y generan como salida una unidad de longitud fija de 256 o 512 bits. Las funciones de hash son muy sensibles al mensaje de entrada, una modificación ínfima implica una salida completamente distinta. La sensibilidad a las condiciones iniciales garantiza la no modificación del mensaje de inicio, lo que hace completamente imposible recuperar información, ni siquiera la firma electrónica para firmar otros documentos, y cualquier modificación implicará que el proceso de validación se detenga.

Por ejemplo, el hash de todo el texto anterior es:

*2f3706ec1594a7cc5362a3046b1f7f00f6807ccf3a63fd521601ee37bcd87bf0*

La siguiente figura es para ilustrar el proceso de hash y de firma electrónica.

Diagrama

Descripción generada automáticamente

*Función hash y firma electrónica*

Una clave es una serie de caracteres que permiten a un algoritmo de encriptado generar un mensaje encriptado y sellado. La clave desempeña un papel muy importante en el proceso de encriptado y en la generación de firmas electrónicas. El tamaño de la clave, que se mide en bits, refleja el nivel de encriptado: cuanto mayor es el tamaño, más alto es el nivel de seguridad.

Las claves privada y pública con completamente independientes. Sus tamaños también son independientes de los algoritmos de encriptado utilizados y, una vez más, cuanto mayor es su tamaño más eficientes son. Por ejemplo, una clave pública de 1024 bits, que es gigantesca, refleja un nivel de seguridad extremadamente alto.

Una vez efectuado el intercambio de información, las operaciones realizadas con la información pueden respaldarse con la presentación de Smart contracts.

## **4. Los programas: Smart contracts**

Los Smart contracts son una pieza fundamental de una blockchain, porque permiten llevar a cabo la lógica de una actividad de manera programática. A continuación, definimos un Smart contract y la importancia de que el lenguaje que lo sustenta sea Turing completo.

### a. Definición

Un Smart contract es un programa informático, también denominado *chaincode*, que permite realizar una tarea de manera programática cuando se reúnen determinadas condiciones. Los Smart contracts aúnan simultáneamente la tecnología y el derecho. Sin embargo, a día de hoy no hay una definición jurídica reconocida, ni en España ni en Europa.

Ethereum definió un Smart contract como: «*Un protocolo de transacción que ejecuta las cláusulas del contrato o grupo de contratos en una Blockchain criptográfica*.»

En un libro blanco, una comunidad de desarrolladores propone una definición más restrictiva de un Smart contract (Johnston, 2015). Equipara los términos aplicación y Smart contract. Se le suponen cuatro propiedades.

* La aplicación debe ser íntegramente de código abierto, funcionar de manera autónoma, sin ninguna contrapartida y controlar lo fundamental de sus tokens, es decir, sus reservas de criptomoneda. La aplicación puede adaptar su protocolo en función de las mejoras propuestas y de las respuestas del mercado. Sin embargo, todas las modificaciones deben hacerse mediante consenso de los usuarios.
* Los datos y las grabaciones de las operaciones efectuadas por la aplicación se deben encriptar y almacenar en una blockchain pública y descentralizada. El objetivo es evitar que la aplicación las modifique como consecuencia de un fallo en el único punto donde opera.
* La aplicación debe utilizar un token encriptado (bitcoin o cualquier otra criptomoneda nativa del sistema), necesaria para acceder a ella. Toda contribución de valor hecha por los mineros (a veces también llamados granjeros) se debe remunerar con tokens de la aplicación.

La aplicación debe generar tokens en función de un algoritmo de criptografía estándar. Estos tokens son la prueba de que en la aplicación y en un nudo determinado se ha realizado un trabajo que tiene un valor (Bitcoin utiliza el algoritmo denominado proof of work o prueba de trabajo).

No obstante, esta definición está restringida al universo de algunas blockchains públicas.

Nosotros proponemos la siguiente definición:

Un Smart contract es una aplicación que se ejecuta en una red distribuida. Los participantes comparten información protegida con total seguridad (y potencialmente con la ayuda de un pseudónimo). Las operaciones se ejecutan de manera descentralizada a través de los distintos nudos de la red.

### b. Turing completo

Para poder proporcionar una solución informática permanente que responda a las exigencias del futuro, toda blockchain debería necesitar un lenguaje de programación subyacente que sea Turing completo. Primero vamos a definir el concepto y luego presentaremos su implicación práctica.

En 1936, Alan Turing intentó definir precisamente el concepto de algoritmo. Así creó un modelo abstracto llamado máquina de Turing. El modelo se aplica a las máquinas mecánicas de cálculo y se divide en cuatro partes.

El primer elemento es una cinta infinita, dividida en celdas sucesivas. En cada celda hay un símbolo de un alfabeto finito. Las celdas que todavía no se han escrito contienen un símbolo blanco, es decir, que la celda todavía no contiene un símbolo alfabético.

El segundo elemento es el cabezal de lectura o de escritura, que, como su nombre indica, puede leer o escribir el contenido de la celda. Este cabezal se puede mover en los dos sentidos de la cinta.

El tercer elemento es el registro de estado. Este objeto memoriza el estado actual de la máquina de Turing. La cantidad de estados posibles siempre es finita. Hay un estado especial que corresponde al estado inicial de la máquina antes del inicio de su ejecución.

El último elemento es la tabla de acciones. Le indica a la máquina el símbolo que debe escribir y cómo moverse (hacia la izquierda o hacia la derecha). También informa a la máquina del estado nuevo, en función del símbolo alfabético leído sobre la cinta y del estado actual de la máquina. Si la combinación de símbolo leído y estado actual de la máquina no existe, la máquina se para.

Este modelo teórico está asociado con instrucciones. Por ejemplo, «si el valor de la celda es C, entonces moverse cinco celdas a la derecha y copiar el valor de la celda situada dos celdas a la izquierda en la celda actual».

El concepto de Turing completo es un sistema formal en el que se puede programar cualquier máquina de Turing, pero también cualquier cosa, mientas el código responde a las normas de una máquina de Turing. Como recordatorio, un sistema formal es una modelización matemática de un lenguaje que representa los elementos, términos, fórmulas, derivaciones, etc. con ayuda de objetos finitos. Gracias a él, podemos verificar de manera algorítmica si sus elementos son correctos (en el sentido gramatical), es decir, que forman un conjunto recursivo.

El aspecto recursivo es una propiedad fundamental de un lenguaje Turing completo. Una función puede llamarse a sí misma para resolver un problema.

Para explicarlo de manera sencilla, un lenguaje de programación Turing completo permite representar todas las funciones calculables, su realización es finita en el tiempo y en el espacio de memoria necesario para la realización de este cálculo. Entonces, esta propiedad hace que sea posible simular de manera informática cualquier objeto presente en el universo.

Hoy en día, a los lenguajes de programación como Solidity o Serpent se les denomina Turing completos. Estos lenguajes se utilizan en el contexto de la blockchain Ethereum. Todos los años aparecen muchos lenguajes. Recientemente apareció el lenguaje Go, desarrollado por Google y que se utiliza principalmente para producir código en la tecnología blockchain HyperLedger. La propriedad Turing completo es fundamental en el desarrollo de aplicaciones modernas, porque permite modelizar y automatizar los procesos de empresa. Por el contrario, hasta hace poco las implementaciones de Bitcoin no eran Turing completas y eso impedía ir más allá de las transferencias de dinero sencillas.

En el apartado siguiente vamos a presentar una pieza nueva: las carteras electrónicas y los tokens asociados.

## **5. Los tokens y las carteras electrónicas**

El primer caso de uso de la tecnología blockchain se resumen en la transferencia de activos. Para poder realizar la transferencia hay dos elementos esenciales: una cartera y un token. Aquí debajo presentamos estos elementos y su implicación económica. Sin embargo, hay que decir que no es necesario que todas las blockchains tengan una cartera o una divisa para poder funcionar.

### a. Definición de un token y de una cartera electrónica

Un token es un objeto digital que no tiene realidad física de manera nativa. Se supone que este objeto tiene un valor fiduciario, es decir, basado en la confianza. El token puede representar un objeto, un valor económico o incluso una referencia en un proceso logístico. Por eso hay que tomar el término en un sentido literal.

Una cartera electrónica es una dirección en una base de datos y para acceder a esta dirección se requiere una clave. La cartera sirve para almacenar tokens, también llamados en algunos casos criptomonedas.

Así, una persona que hace transacciones en una blockchain no tiene tokens en propiedad, sino un derecho de acceso a estos tokens.

### b. El modelo clásico y la economía de Hayek

El aspecto Turing completo abre la puerta a un universo hasta ahora infrautilizado: la economía de Hayek (Hayek, 2012). Friedrich Hayek fue un filósofo y economista británico originario de Austria. Fue miembro de la Escuela Austríaca, premio Nobel de economía en 1974 y defensor del liberalismo.

En 1931 retomó los trabajos de Ludwig Von Mises y desarrolló la teoría que considera que el intervencionismo de los bancos centrales en la política monetaria expansionista distorsiona los sistemas de fijación de precios en la estructura de producción. De lo que se deriva un exceso de crédito en la economía. Este dinero provechado por las empresas desemboca en una capacidad excesiva de producción o una sobreproducción, que inevitablemente termina en una crisis económica (Le portail de l’économie et des finances, 2016).

En 1976, el mismo autor consideró la necesidad de desnacionalizar las divisas para quitarles esta influencia a los estados y ralentizar la convergencia hacia gobiernos totalitarios. En su comprensión de los sistemas políticos y económicos, él considera que las cámaras bajas de los estados tienen el objetivo de proponer un modelo de sociedad y la misión de ponerlo en práctica. Hayek rechaza esta idea porque, si el proyecto de sociedad es contrario a la realidad económica, todo el estado está destinado al fracaso (como en el ejemplo de la URSS).

En su primer modelo, estimó que las unidades de producción (por ejemplo empresas) deberían tener derecho a producir su propia divisa y, si fuera posible, que estuviera basada en la producción generada. Así, el objetivo sería vincular los agentes de producción con los agentes de creación de valores, e implícitamente relacionar los agentes de creación de valores y los agentes de captación de valores económicos.

El uso de blockchain permite técnicamente la creación de este tipo de divisas, pero al mismo tiempo deforma y desestabiliza el sistema actual establecido. Asociada con un lenguaje Turing completo, la tecnología permite un intercambio de divisas criptográficas con cualquier otra divisa de intercambio, siempre que tenga una tabla de correspondencia perfectamente comparable durante el intercambio entre divisas clásicas. Por eso, a mediados de 2019 ya había más de 2000 criptomonedas cotizadas frente a 166 divisas nacionales.

Tras esta reflexión, Hayek llega con treinta años de adelanto a la misma conclusión que sus pares. Corrige su opinión en su nuevo libro de entonces (Hayek, 1990) y declara en él que, al final, todas estas divisas deberían converger en una sola. Recordemos que una de las resoluciones contempladas en los acuerdos de Bretton Woods en 1944 consistía en adoptar una divisa única mundial. Algo así es factible desde el punto de vista técnico y teórico.

Comprendemos que, en este modelo, la divisa única de transferencia es virtual, desde luego, pero basada en activos económicos. Si la divisa no se apoya en valores tangibles (materiales o intelectuales), se desplomará con rapidez. Sin ninguna duda, este enfoque les quita a los gobiernos una influencia de poder, pero reduce de manera simétrica el riesgo de burbujas económicas y de caídas bursátiles relacionadas exclusivamente con las políticas monetarias. También evita las oleadas de devaluaciones, como las que se pudieron observar a principios de la década de 1990 en Europa o a finales de la misma década en el sudeste asiático, y que tuvieron unas consecuencias económicas y humanas desastrosas.

Cabe señalar que esta noción de pérdida de poder económico sigue a priori la trayectoria tomada, al menos por los estados europeos, ya que la política monetaria está en manos del Banco central europeo y no en las de un estado a través de un banco central nacional. Entonces, el principal problema reside en la definición de los contratos y su marco legal, así como en la legislación sobre estas criptomonedas.

### c. Los tokens utilitarios

Un token utilitario, o *utility token* en inglés, es una categoría nueva de tokens. Se trata de objetos digitales que permiten responder a una necesidad funcional. Disponer de estos tokens permite tener acceso a un servicio. La mayor parte del tiempo, los tokens tienen un valor que se les asigna, de manera similar a los tokens utilizados en algunas máquinas de café. El intercambio debe realizarse según las condiciones, y la especulación es un concepto menos interesante. En la práctica, parece que los inversores se concentran poco en esta propiedad y los auténticos tokens utilitarios todavía están en fase de maduración.

La sutileza del token utilitario por oposición al estatus de criptomoneda tiene un impacto importante, especialmente frente a las autoridades.

En efecto, una criptomoneda es básicamente una divisa y, por lo tanto, está sujeta a una determinada cantidad de imposiciones en función del punto de vista adoptado. Para un economista, una divisa debe estar apoyada por un contravalor en el mundo real, como los euros respaldados por barras de oro en los bancos de los estados miembros. Para un especialista tributario, se trata, en función del país, de una obligación de inclusión en la declaración fiscal y, por lo tanto, de una imposición adecuada.

Los últimos cambios jurídicos en el mundo también han obligado a los empresarios a convertir los tokens en partes de la empresa. Así, comprar tokens equivale a comprar acciones de la empresa. El marco legal de la titulización empezó a desarrollarse jurídicamente en España en 1992.

Muy a menudo, declarar que el token emitido es en realidad un token utilitario es una manera de reducir la carga administrativa. En la práctica, los fundadores de este tipo de soluciones siguen estando muy presionados por los organismos financieros (p. ej. bancos), que desean efectuar los controles necesarios y evitar situaciones como fraudes o blanqueo de dinero. Al final, una declaración administrativa puede ser menor costosa que la resolución de los problemas ocasionados.

# La lógica de consenso

Además de los bloques, el protocolo de red, los programas y las carteras (opcionales), ahora es el momento de hablar del elemento fundamental para todas las tecnologías basadas en blockchain: un mecanismo de consenso. Proponemos un primer enfoque de desmitificación, que volveremos a ver con más lujo de detalles en el capítulo siguiente.

## **1. Algoritmos para establecer la confianza entre dos partes**

La coherencia del sistema descentralizado supone que la información esté presente y consolidada en todos los nudos (participantes) sin pasar por un punto o una autoridad central reguladora. La validación de las transacciones no pasa por un gran registro central donde está presente toda la información validada.

Esta necesidad causa dos problemas:

* Cómo garantizar la coherencia de los datos entre varios actores para que todos tengan la misma información;
* Cómo garantizar la unicidad de una información común al conjunto de los actores.

Estos dos problemas se complican por el riesgo de los agentes malintencionados y las averías que corrompen los datos.

Para dar respuesta a estas problemáticas, el tratamiento de la información se hace a través de la aplicación de teoremas procedentes de la teoría de juegos. Estos algoritmos llevan el nombre singular de prueba de trabajo o prueba de participación.

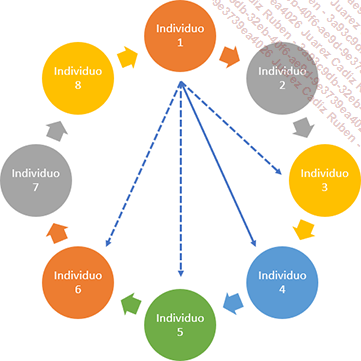
El principio básico de estos algoritmos es poner frente a frente los intereses de los usuarios de la red y los de los actores encargados de su mantenimiento para lograr un precio equilibrado que satisfaga a las dos partes. En el marco del Bitcoin, se anima a los actores que validan las transacciones a realizar un cálculo matemático costoso. Si encuentran la solución al cálculo, se les gratifica con una cantidad en criptomoneda.

Este cálculo es comprometedor y permite aportar una propiedad de fiabilidad a una información enviada a la red. A continuación, esta información validada se envía al conjunto de los actores para su integración. Una segunda parte del protocolo se asegura de que una transacción no se escribe por duplicado.

El proceso de consenso sobre un registro unificado varía en gran medida en función de la tecnología utilizada. Se necesita un compromiso entre comprobación de la fiabilidad de una información y eficacia en el tratamiento de esta información.

La multiplicación de los participantes, o nudos, en la red y la multitud de validaciones realizadas por cada participante permiten la instauración de la confianza en este sistema distribuido. En efecto, la creciente necesidad hace que la actividad de validación sea económicamente rentable, mientras que la multiplicación de la cantidad de actores a cargo de la validación reduce el riesgo de fraude o de manipulación de la red. Al final, este mecanismo permite liberarse de una autoridad central reguladora. El ejemplo siguiente ilustra esta arquitectura distribuida donde las transacciones entre dos individuos se hacen de manera directa y todos los individuos habilitados realizan la validación. Las transacciones validadas se incorporan en el registro principal accesible para todos.

La figura siguiente es un ejemplo de una arquitectura distribuida:



*Arquitectura distribuida que muestra las transacciones directas entre los individuos*

La criptografía está en el centro de este dispositivo y garantiza la confianza y la seguridad de los intercambios entre los participantes. Si un participante malicioso toma el control del procedimiento de cifrado, conducirá a una caída de la confianza que llevará a la destrucción de la red.

## **2. El caso de las transacciones maliciosas**

En interés del sistema, todos los participantes trabajan para garantizar el buen funcionamiento y la sostenibilidad del sistema. Sin embargo, la red es de libre acceso y todos pueden emitir transacciones, ofrecer su potencia de cálculo para convertirse en recolectores o simplemente nudos del sistema. Los participantes pueden tener una intención maliciosa, con un propósito de fraude, utilizando una versión corrupta del software compartido. En estos casos, el principio de sospecha entre los nudos es primordial, porque cada nudo y cada etapa deben verificar las transacciones que reciben considerándolas como potencialmente peligrosas. Únicamente imponiendo un protocolo estricto en todos los nudos , y de manera recursiva, las transacciones fraudulentas se encuentran aisladas muy rápido y nunca llegan a la blockchain.

Para introducir una transacción fraudulenta en los distintos registros de blockchain y en los múltiples nudos, hay que incorporarla en un subregistro y enviarla a la red por la vía normal para que todos los nudos la verifiquen. Si el protocolo de control no está defectuoso, estas transacciones fraudulentas no tienen ninguna posibilidad de ser validadas ni aceptadas por los otros nudos para ser incorporadas en la blockchain.

Integrar una transacción fraudulenta en un subregistro e introducirlo en lugar de un subregistro existente en la blockchain es una manera de modificar una parte de la cadena de bloques. Para que se convirtiera en una parte de la rama principal, habría que introducirle registros nuevos más rápido que la rama principal auténtica, para que esta rama nueva terminara superándola. Pero el resto de la red también sigue trabajando en paralelo, para incorporar subregistros nuevos y alargar la blockchain. Entonces, los defraudadores tendrían que movilizar una potencia de cálculo y de validación superior a la de toda la red. Considerando la cantidad de controles en todas las etapas y las técnicas de criptografía utilizadas, es difícil imaginarse que las modificaciones fraudulentas puedan superarlas. Las modificaciones maliciosas se quedarían aisladas en un grupo de nudos, que solo podrían realizar intercambios entre ellos, una opción que no resulta interesante. El resto de la red no se vería afectada ni infectada.

## **3. Esquema de validación de un bloque**

Una blockchain es en esencia una cadena de bloques. El mecanismo sufre ligeras modificaciones en función de la tecnología estudiada, sin embargo los principios rectores son los mismos.

En el caso clásico de un pago, se trata de transferir una información entre dos bases de datos con un débito en un lado y un crédito en el otro respectivamente, por ejemplo. El proceso se realiza como se describe a continuación:

* Bob emite una transacción informando en el sistema a quién debe entregarse la suma definida.
* En un segundo paso, la transacción se enriquece con distintas informaciones que permitirán a los actores de una red recepcionar la transacción y validarla. Por ejemplo, el envío de información está firmado. Este enriquecimiento permite que la información navegue libremente en una red y forme lo que se denomina un bloque.
* A continuación, el bloque se emite y se envía a varios actores de la red. Los actores se aseguran de que las informaciones recibidas son legítimas y no están corrompidas. Varios actores reciben la información para evitar que un actor corrompido o malicioso pueda distorsionar las informaciones recibidas y emitidas en su beneficio.
* El algoritmo de consenso recoge las respuestas de los distintos actores y valida o no la transacción. Por ejemplo: si el emisor no corresponde a la firma, la transacción se rechaza.
* Cuando la transacción se ha validado, se añade a la cadena ya existente y al mismo tiempo alarga la cadena de bloques o blockchain.
* Alice, el contacto de Bob, recibe la confirmación de la transacción y el recorrido se detiene.

La figura que aparece debajo repite de manera esquemática el recorrido que acabamos de describir.

Diagrama, Escala de tiempo

Descripción generada automáticamente

*Esquema de una transacción en una blockchain pública*

Esta figura es general y permite acceder a los conceptos detrás de la tecnología. Hay muchas variantes. En el caso de las blockchains permisionadas, se envía un mensaje antes de crear un bloque. El bloque solo se crea al final del proceso y luego se añade a la cadena. Estos casos se explicarán en profundidad más adelante en este libro.