Introducción

Blockchain es una tecnología que ha dado mucho que hablar desde que empezó su andadura en 2009. Desde entonces ha crecido mucho y se utiliza como un término donde se refugian plantamientos técnicos que ya no tienen mucha relación con el método original. El propósito de este capítulo es definir qué es blockchain y recordar sus orígenes junto con las promesas intrínsecas que conlleva.

# ¿Qué es blockchain?

Vamos a empezar con una introducción a blockchain donde hablaremos de su definición, origen y las primeras aplicaciones. Este preámbulo le permitirá tener una visión de la génesis de esta tecnología.

Blockchain («cadena de bloques», en español) es una tecnología de gran envergadura, innovadora, que permite almacenar datos digitales de manera descentralizada y segura. Se trata de una especie de gran registro contable que contiene la lista de todos los intercambios efectuados entre usuarios. Este registro está descentralizado, es decir, almacenado en los servidores de los usuarios y no en un único lugar. Las transacciones se actualizan continuamente y son infalsificables, porque se basan en un sistema de validación criptográfico controlado por los usuarios.

Estas transacciones, materializadas a través de las líneas del registro, se inscriben en el mismo después de su validación, mediante bloques de datos, y así forman una cadena de bloques inalterable: blockchain.

Por lo tanto, blockchain es un registro descentralizado en el que todo el mundo tiene derecho a escribir, pero nadie puede eliminar lo que se ha escrito. Para simplificar las cosas, tomemos el ejemplo de un registro físico (un inmenso cuaderno de papel) en el que todos pueden escribir: una transacción, un trueque con otro usuario, un documento notarial, un reconocimiento de deuda, todo con fecha y hora para evitar dudas y malversaciones por parte de los hackers u otros maleantes. Este registro estaría disponible para todos.

Todos podrían consultarlo cuando quisieran, pero no podrían modificar su contenido una vez escrito. En esta descripción, tener una sola versión del registro físico sería un problema. Eso no sería práctico si todos quisieran tener la posibilidad de escribir en él, pero también sería muy peligroso si lo robaran o se destruyera. Para garantizar la continuidad de este registro, habría que hacer numerosas copias. Al contrario que con un buen registro antiguo en papel, los ordenadores actuales permiten compartir la información de manera rápida y masiva. Ahora podemos imaginar que este registro ya no es físico, sino informático, y que está copiado en muchos lugares. Así tendríamos un almacenamiento descentralizado. La tecnología Blockchain se basa en una red descentralizada denominada entre pares. Esto significa que, al contrario que la red de Internet actual, que funciona mediante nudos propiedad de multinacionales, los usuarios de la red se convierten en nudos de la misma. Algunos de estos usuarios guardan copias de blockchain en todo el mundo. Estos miles de copias se actualizan de manera simultánea y constante, lo que hace que blockchain sea completamente indestructible.

Algunas variantes de blockchain, como Ethereum o Hyperledger, incluso permiten ejecutar fragmentos de programas en la blockchain. Además del almacenamiento descentralizado, blockchain también permite la ejecución descentralizada. Ahora vamos a estudiar el origen de la tecnología.

# El origen de la tecnología

Los años 2007 y 2008 fueron horribles para el sector financiero. De repente, en los Estados Unidos, el precio de los bienes inmuebles dejó de aumentar entre un 8 % y un 15 % anual. Los prestatarios no pudieron pagar sus créditos y entraron en impagos. Las instituciones financieras que habían transformado los créditos en productos financieros asociados a un gran apalancamiento no pudieron cumplir con sus obligaciones. Los productos se habían estado vendiendo durante casi una década y la crisis fue mundial.

La leyenda dice que la primera blockchain nació en parte para responder a la actitud de algunos bancos hacia los ahorradores. La idea principal era desposeer a los Estados de su derecho a imprimir divisa y evitar así que devaluaran los depósitos acumulados por los ahorradores con el fruto de su trabajo. De la misma manera, la innovación técnica tenía la misión de liberarse del sistema bancario en su estado actual. Un hombre mítico, Satoshi Nakamoto, se convirtió entonces en un Lutero o un Voltaire moderno al proponer una alternativa. El objetivo no era la iglesia y sus prácticas no estaban relacionadas con la religión, sino con el sistema bancario que parecía haberse desviado mucho de su misión original. La historia le habrá enseñado a este hombre, que realmente es más probable que sea un equipo, a no hablar demasiado y poner en peligro su libertad o algo más.

Blockchain nació durante la creación del *bitcoin* en 2009. El *bitcoin* tiene la certificación "no duplicable", rastreable e infalsificable, todo ello garantizado por una tecnología llamada blockchain. Todos pueden ver los intercambios y las transferencias de *bitcoins*, por eso es imposible crear *bitcoins* falsos sin que se vea en el registro descentralizado. Esta tecnología también permite realizar pagos y evitar la duplicidad de los mismos (es decir, que una persona no puede utilizar un mismo *bitcoin* en dos transacciones distintas).

Blockchain también permite establecer un sistema de pago inmediato y sin necesidad de pasar por un tercero. Al final de la cadena, el proceso global está simplificado y más adaptado a las limitaciones del siglo XXI. A menudo se confunden los conceptos *bitcoins* y blockchain. El *bitcoin* es una aplicación particular de blockchain, que se basa en un valor monetario: es una criptomoneda.

Algunos creen que las criptomonedas pueden conducir a una desnacionalización de las divisas y al final de las divisas estatales. Las criptomonedas permitirían el nacimiento de una nueva era monetaria. Pero, aunque el ámbito de acción de las criptomonedas es ambicioso, los usos de la tecnología Blockchain son todavía más amplios.

En el caso del *bitcoin*, la tecnología se utiliza para garantizar la trazabilidad de las transacciones, ya que cada *bitcoin* tiene un código de encriptado propio. Así, un usuario solo puede utilizar sus *bitcoins* con un solo destinatario, correspondiente a una sola transacción determinada. Acabamos de ver que blockchain nos permite administrar las criptomonedas. El *bitcoin* resuelve el primer problema, la cuestión de la permanencia y la singularidad de los activos digitales. Pero el funcionamiento mismo de blockchain nos permite considerar otros usos añadiendo otra capa de sofisticación: el concepto de contrato inteligente (smart-contract). Blockchain puede tener un impacto social, económico, monetario, legislativo e incluso político. Eso es lo que vamos a demostrar.

Actualmente, siempre es necesario tener un tercero de confianza cuando realizamos una transacción (notario, banco, compañía de seguros, secretario judicial, estado, etc.). Este último se asegura de que se reúnen todas las condiciones para realizar la transacción, y luego la ejecuta de conformidad con los contratos firmados y la legislación en vigor. En la parte más alta de la cadena de confianza, el estado es el garante de la coherencia y estabilidad del conjunto del sistema. Puede conceder o retirar los acuerdos a los actores que no respeten las normas. Este sistema, probado desde hace décadas, está en proceso de transformación gracias a la tecnología blockchain. En efecto, mañana, esta función podría ser inútil porque blockchain se ha hecho cargo de ella. Mediante el mecanismo blockchain, las transacciones se realizarán directamente sin pasar por un tercero. Como hemos visto, la aplicación más conocida de blockchain es la de las criptomonedas, como el *bitcoin*. Pero blockchain también se puede utilizar en numerosos campos en los que no pensamos inmediatamente: los títulos de propiedad especialmente. Honduras gestiona su catastro con blockchain. De esta manera, el gobierno aprovecha este registro descentralizado y protegido para administrar los títulos de propiedad. Gracias a este sistema económico, este país en vías de desarrollo puede garantizarles a sus habitantes la propiedad de los terrenos. No olvide este ejemplo.

Blockchain permite implantar aplicaciones basadas en la infraestructura blockchain para intercambiar datos.

Este es un punto importante: el beneficio aportado por el uso de una estructura existente para el almacenamiento de datos.

Si consideramos esta característica desde un punto de vista empresarial, es más sencillo imaginar que blockchain permitirá aportar una generación nueva de procesos de negocios. Las instituciones financieras lo han comprendido. Después de largos períodos de inversiones en los procesos internos, es el momento de mirar las cosas con otros ojos y abrir los intercambios hacia el exterior con una visión más global. La faceta colaborativa y transparente de blockchain nos permite abrir estos intercambios, mientras se respeta el nivel de seguridad necesario en el entorno profesional. Pero las empresas no podrán conseguirlo solas. Habrá que formar alianzas complementarias con los proveedores, los clientes, los socios e incluso algunos competidores para ir realmente hasta el fondo de este nuevo método.

Para los proveedores de infraestructuras centralizadas, la confianza es el capital más importante. Para ello, además de la fiabilidad y la estabilidad del sistema, el principio básico es el control del acceso. Es necesario garantizar que, a priori, no se aparta a ningún participante del mercado financiero. Ese es exactamente el enfoque del esquema Blockchain, es decir, permitir a los usuarios un intercambio de transacciones sin intermediarios.

# Las promesas de la tecnología

La tecnología hace muchas promesas. En esta sección se recuerdan algunas de las ventajas principales, tanto técnicas como para los usuarios. Hemos hecho una lista de los siguientes puntos, es decir, de las ventajas tecnológicas relacionadas con un enfoque de sistema distribuido y con la creación de una red extendida. El beneficio de la transparencia también es importante y proporciona maneras nuevas de trabajar. La desaparición de los intermediarios y la creación de confianza algorítmica también son ventajas considerables, al mismo nivel que la búsqueda de la automatización iniciada hace varias décadas. Las expectativas de la reducción de costes y la creación de una continuidad digital tienen un valor real en una economía que alcanza la madurez bajo la atenta mirada de una gran cantidad de países.

Por fin es posible crear activos digitales únicos y vincularlos con el mundo físico, algo especialmente delicado en nuestros días.

La última ventaja, pero no la menos importante, es que mediante blockchain se puede acceder a nuevos modelos de negocio. En este apartado vamos a hablar de todas estas promesas para que el lector pueda comprender completamente la transcendencia que conlleva el término blockchain.

## **1. Sistema distribuido y red extendida**

En cierta manera, un sistema extendido es como el Santo Grial de las redes informáticas: resistente, incorruptible, eficaz, etc. Blockchain utiliza esa tipología de red y permite, al menos en teoría, utilizar mejor los recursos y además ofrecer un servicio más fiable y robusto.

El término «sistema distribuido» designa la interconexión de un conjunto de ordenadores autónomos, de procesos o de procesadores. Los ordenadores, los procesos o los procesadores se denominan nudos. Para poder ser considerado autónomo, como mínimo, el nudo debe estar equipado con su propio sistema de control. Para poder llamarse interconectados, los nudos deben ser capaces de intercambiar información.

La definición también incluye un sistema de software construido como un conjunto de procesos comunicantes, incluso si funcionan en una instalación única. En la mayoría de los casos, un sistema distribuido está formado, como mínimo, por varios procesadores interconectados mediante una herramienta de comunicación.

En algunos textos sobre el tema aparecen otras definiciones más restrictivas. Por ejemplo, un sistema es distribuido si y solo si la existencia de nudos autónomos es transparente para los usuarios del sistema. Un sistema distribuido de esta manera se comporta como un sistema de ordenadores virtuales e independiente. Sin embargo, la implementación de esta transparencia necesita el desarrollo de algoritmos distribuidos de control complejo.

Los sistemas distribuidos tienen muchas ventajas. Pueden ser preferibles a los sistemas secuenciales, o simplemente inevitables por diversas razones. Ahora vamos a hablar de ellas. En la lista que aparece a continuación se enumeran los principales argumentos a favor de los sistemas distribuidos. Las características de un sistema distribuido también pueden evolucionar en función del motivo de su existencia.

Estas ventajas son: compartir recursos, la simplificación del diseño de la aplicación y un aumento de la fiabilidad de la red y de su rendimiento.

Compartir recursos es posible mediante la democratización de los ordenadores debido a su precio y tamaño; de esta manera es posible crear una red local (*local area network*) en una organización para compartir los recursos y evitar replicarlos en todos los equipos. Este sistema distribuido también permite reducir los costes instalando ordenadores pequeños en lugar de granjas de servidores.

Además, el diseño de un sistema de ordenadores puede resultar muy complicado, especialmente cuando hay que tener muchas funcionalidades en cuenta. Esto se puede simplificar subdividiendo las funcionalidades en procesadores diferentes que se comunican entre ellos. Eso es exactamente lo que hace blockchain. Los procesos en la nube tienden a aproximarse a este modelo.

La red es más fiable gracias a la duplicación: los sistemas distribuidos tienen el potencial de ser más fiables que los sistemas «*stand-alone*» (independientes), porque tienen una posibilidad de fallo más pequeña. Esto significa que, si fallan algunos nudos, los otros nudos que operan correctamente pueden tomar el relevo y finalizar las tareas en curso. Sin embargo, esta propiedad que permite enfrentarse a los fallos necesita utilizar algoritmos complejos.

En conclusión, el rendimiento y la paralelización aumentan: la presencia de múltiples procesadores en un sistema distribuido ofrece la posibilidad de aumentar la rapidez de un cálculo repartiéndolo entre los distintos procesadores.

Estas ventajas técnicas no pueden ocultar las ventajas para los usuarios de la tecnología, la primera es probablemente el proceso de retirada de los intermediarios y la generación de una relación de confianza mediante algoritmos.

## **2. Desintermediación y creación de confianza**

Blockchain es una tecnología de desintermediación. En la década de 2010 se ha producido una revolución que afecta a la uberización de la sociedad, con la creación de mercados públicos y la reducción de la cantidad de actores entre el cliente y el proveedor de un servicio o de un bien. El enfoque no es nuevo y Leclerc generó rechazo en su momento por llevar a cabo una operación similar.

La ventaja con estos nuevos gigantes es que ofrecen la posibilidad de explotar recursos infrautilizados a escala internacional y a precios a menudo ventajosos. No olvidemos que la empresa de alojamiento más rentable del mundo no es un hotel, sino Airbnb, aunque no posee ningún alojamiento.

Blockchain permite hacer lo mismo, pero sin Uber o Airbnb. Actualmente es posible poner en contacto a un cliente con un proveedor, sin que se conozcan, y hacer una transacción con total confianza. La transacción puede ser financiera, al igual que una operación de verificación.

Esta desintermediación es un gran reto que suscita un enorme interés en los bancos, quienes deben pagar sumas considerables a empresas externas que se ocupan del control, la verificación y la reducción de algunos riesgos. Muchas empresas, especialmente en la industria, se enfrentan todos los días a los mismos problemas, pero no pueden permitirse un tercero de confianza si no es con precios muy elevados.

## **3. Aumento de la transparencia**

La transparencia es el elemento preponderante en la lógica de blockchain. Es posible que algunas empresas no quieran adherirse para conservar los datos de clientes concretos. Sin embargo, hay dos argumentos que hablan en favor de la transparencia.

El intercambio de datos está encriptado de manera predeterminada. Sin embargo, en función de la implementación de blockchain, es posible ocultar todo y revelar solo lo imprescindible, o, todavía más interesante, ocultar una información sin dejar de garantizar la conformidad. Las medidas sobre la propiedad intelectual pueden estar encriptadas. Sin embargo, la respuesta certificada a una exigencia normativa se puede mostrar solo a las personas autorizadas.

Esto abre horizontes inesperados y mejora los intercambios entre actores con intereses divergentes.

La cantidad de usos también consiste en garantizar que una operación se puede realizar sin riesgo de que una autoridad particular haya modificado la información en el pasado. Esta propiedad es especialmente útil para reducir los desacuerdos entre dos empresas, por ejemplo: durante el envío de documentos importantes.

Para terminar, otra ventaja de blockchain reside en el hecho de que se trata de una tecnología *push* y no *pull*. Esto significa que, para que un contrato pueda acceder a una información, la información tiene que estar explícitamente disponible. En cambio, si tomamos la tecnología Visa o MasterCard como ejemplo, esta utiliza un proceso *pull*, es decir, que desde el momento en que se da el número de tarjeta, cualquier aplicación o sistema puede acceder a todos los datos asociados a la tarjeta. En el caso de una tarjeta de pago, habitualmente los datos son el número de cuenta de la persona y la cantidad disponible en la cuenta. Este proceso sería demasiado peligroso con la tecnología Blockchain, porque los datos asociados al contrato son mucho más numerosos. Sin entrar en detalles, se podría identificar a una persona mediante la concordancia de datos y costumbres de uso de los contratos en cuestión.

## **4. Automatización avanzada y continuidad digital**

Blockchain es una tecnología informática. Como todas las tecnologías informáticas, reproduce operaciones conocidas desde hace tiempo, pero más rápido y a veces con mayor eficacia.

Pero estas ventajas están limitadas a un sistema informático concreto. Los gigantes como SAP han creado avances de productividad innegables con la implantación de referencias comunes a nivel de empresa. Sin embargo, este enfoque tiene límites en cuanto salimos de la empresa. Entonces las hojas de cálculo aparecen rápidamente para sustituir a un sistema informático eficaz, pero por el que hay que pagar un precio.

Blockchain es una solución que permite llegar todavía más lejos, con la creación de un sistema informático que no cree en las soluciones existentes. En algunos casos, blockchain puede sustituir a los sistemas informáticos ausentes, en caso contrario se coloca en la cima de los sistemas existentes.

Esta adaptabilidad permite hacer correspondencias de igual a igual entre las empresas, y de esta manera evita la posibilidad de imponer una solución costosa con los cambios de versión cada dos años.

La continuidad digital creada de esta manera reduce las fricciones asociadas a la recopilación de información. Esta recogida no se limita a la asociación inmediata, sino que por supuesto abarca toda la dimensión de la cadena de valor. También permite una automatización de los tratamientos a lo largo de toda la cadena de valor. Sin embargo, es importante observar que es fundamental una etapa de estandarización mediante iteraciones, con una gestión estricta.

## **5. Reducción de los costes y mejora del rendimiento**

Una blockchain, como veremos en el apartado donde se detalla la elección de la tecnología, toma todo su sentido en un contexto descentralizado y con numerosos actores. Eso implica que, probablemente, no hay que diseñar un proyecto blockchain como un proyecto informático interno en una empresa.

Un proyecto blockchain está claramente orientado a resolver problemas de interfaz, de recogida de información con referencias que no son necesariamente coherentes entre sociedades. La reducción de costes reside en la reducción de la energía necesaria para la recopilación de información. El segundo efecto es probablemente compartir el coste de creación de la solución informática. Por último, los procedimientos de recuperación y coherencia, bien conocidos por los perfiles administrativos, son evidentemente una fuente de ventajas. Lo que es menos evidente a primera vista, pero está constatado empíricamente, es que la recogida de información, con mucha antelación, reduce en gran medida el impacto negativo sobre los problemas de producción industrial. En un sitio industrial, por ejemplo, es muy difícil, con las soluciones actuales, mostrar en la cadena de suministro que un tsunami ha golpeado a un proveedor crítico en la cadena de valor, sobre todo si es de nivel bajo.

Estas reducciones ocultan forzosamente mejoras del rendimiento, que muy a menudo superan el 10 %. Sin embargo, esta no es la única ventaja que propone blockchain. Ahora es posible crear objetos digitales únicos.

## **6. Unicidad de los activos digitales**

El drama de la industria del arte digitalizado (por ejemplo: música, películas, etc.) está en las copias. Las pérdidas anuales a nivel mundial son abismales. Sin embargo, actualmente hay una solución con la creación de objetos únicos, transferibles y no duplicables entre dos partes. Eso implica tanto la transferencia como el disfrute del mencionado objeto.

La industria del lujo lo ha entendido enseguida y desde hace varios años lanza productos diversos para vincular sus artículos excepcionales con un código único unido a blockchain. Esto permite que los clientes se aseguren que el producto adquirido está correctamente unido al taller o al creador esperado.

En el ámbito financiero, una propiedad de este tipo permite hacer un seguimiento de los propietarios de un título financiero y transferirles, o recaudar, los fondos esperados a precios suficientemente competitivos para cuestionar los enfoques tradicionales y abrir modelos económicos nuevos.

## **7. Apertura hacia nuevos modelos de negocio**

Algunas blockchain utilizan un objeto denominado criptomoneda. Con mucha frecuencia se trata de una unidad monetaria similar a un euro o un dólar, pero casi nunca tiene un contravalor en el mundo físico. Esta herramienta ha permitido que los creadores de tecnología puedan financiar sus desarrollos, pensando poder liberarse de las legislaciones sobre recaudación de fondos privados. Posteriormente, este objeto se ha utilizado como divisa para comprar un servicio o un producto. Este esquema suscitó mucho interés durante los años 2017-2018, y actualmente sigue utilizándose. La idea de criptomoneda evolucionó enseguida en las empresas para convertirse en algo así como una divisa o incluso fichas utilizables similares a las fichas de las máquinas de café. Este segmento es uno de los más visibles actualmente, y parece permitir liberarse de las monedas estatales.

De manera complementaria, durante la última década se ha podido observar un segundo modelo de negocio dirigido por la criptomoneda, que financia los desarrollos de sus productos y plataformas. Así hemos podido ver emerger plataformas de comercio entre las monedas clásicas.

En la actualidad, el proceso de especulación todavía parece ser el medio principal de captación de fondos.

También se puede retirar el componente criptomoneda y crear oportunidades nuevas. Como se trata de conectarse para recoger información entre las empresas, una empresa financiada de manera conjunta puede ocuparse del desarrollo y el mantenimiento de un sistema de comunicación común. Posteriormente, se pueden posicionar los componentes de análisis de datos o de inteligencia artificial para predecir las rupturas de carga o los fallos en una cadena de valor. El análisis será más apropiado cuanto mayor sea la profundidad de los datos.

Blockchain es un paradigma nuevo. Cuestiona los métodos de trabajo, se encarga de la cadena de valor, retira las operaciones manuales, permite las estandarizaciones de común acuerdo e introduce la idea de criptomoneda. Todos estos elementos unidos ofrecen muchas oportunidades, y solo la creatividad humana será el límite.