Market Talks
CENTRO DE EDUCACIÓN

BLOCKCHAIN · PRINCIPIANTE · LECCIÓN 5 DE 13

Qué es realmente una blockchain

Una definición clara, las tres partes que tiene toda blockchain y las afirmaciones populares que no son ciertas

7 min de lectura 6 preguntas con sus respuestas

BLOCKCHAIN · PRINCIPIANTE · LECCIÓN 5 DE 13

Qué es realmente una blockchain

EN UNA FRASE

Una blockchain es un registro de transacciones que muchos ordenadores independientes mantienen juntos. Las entradas nuevas se añaden en lotes enlazados, las antiguas no se pueden cambiar en silencio y son unas reglas compartidas, no una empresa, las que deciden qué entra.

Una definición que de verdad sirve

En las últimas cuatro lecciones seguimos un problema y la larga búsqueda de una solución. Ahora podemos ponerle nombre a esa solución. Si quitamos el ruido, una blockchain es esto:

Un registro de transacciones que muchos ordenadores independientes mantienen juntos, donde las entradas nuevas se añaden en lotes enlazados, las antiguas no se pueden cambiar en silencio y unas reglas compartidas deciden qué se añade.

Cada parte de esa frase importa. «Muchos ordenadores independientes» es lo que elimina al intermediario de la lección 1. «Lotes enlazados» es la cadena de bloques que nació del trabajo sobre marcas de tiempo de la lección 3. «Reglas compartidas» es el método de acuerdo de la lección 4. Quita cualquiera de ellas y ya no tendrás una blockchain en el sentido que introdujo Bitcoin.

A este tipo de registro se le llama **libro de cuentas** o ledger: una lista de quién envió qué a quién y cuándo. Una blockchain es una forma concreta de llevar un libro de cuentas, pensada para situaciones en las que los participantes no se fían del todo unos de otros.

Tres partes que trabajan juntas

Ayuda pensar en toda blockchain pública como tres capas apiladas:

- **El registro.** Las transacciones se agrupan en bloques, y cada bloque apunta al anterior, hasta llegar al primero. La lección 6 muestra exactamente cómo se crea ese enlace.
- **La red.** Miles de ordenadores, llamados **nodos**, guardan cada uno una copia completa del registro y se pasan entre sí las transacciones y los bloques nuevos. La lección 7 los analiza en detalle.

- **Las reglas.** Cada nodo comprueba cada bloque nuevo con las mismas reglas antes de aceptarlo. Un bloque que incumple una regla se rechaza, lo envíe quien lo envíe. El método para elegir quién añade el siguiente bloque se llama **consenso**, y la versión de Bitcoin es la prueba de trabajo que conociste en la lección 4.

Ninguna de estas partes es nueva por sí sola. Las bases de datos, las redes y las comprobaciones de reglas existían mucho antes de 2008. Lo que hace diferente a una blockchain es la combinación, y el hecho de que ninguna parte controla ninguna de las tres.

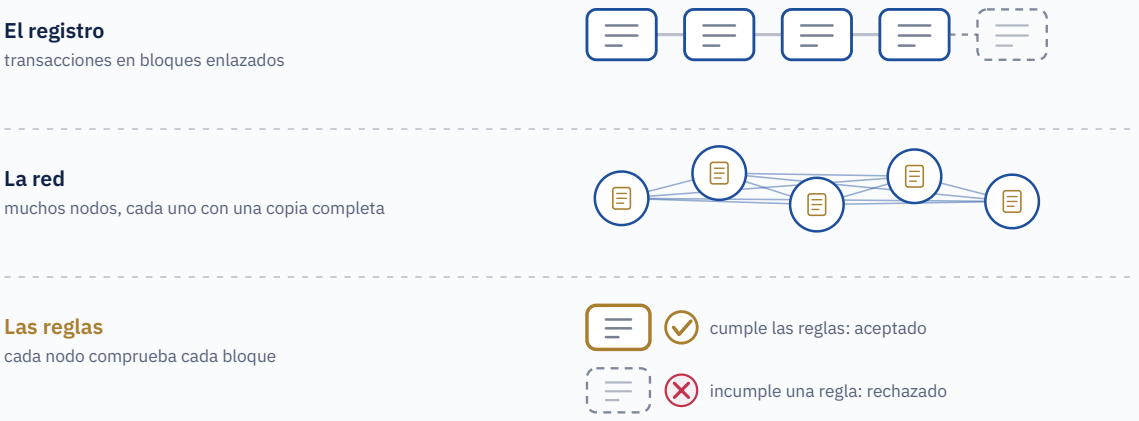


Figura 1. Una blockchain combina tres partes: un registro de bloques enlazados, una red de copias independientes y unas reglas compartidas con las que cada nodo acepta o rechaza los bloques nuevos.

Qué hay realmente dentro

Una imagen habitual es la de una cámara acorazada llena de monedas. La realidad se parece más a una lista muy larga de transferencias. Un bloque de Bitcoin contiene sobre todo transacciones, cada una de las cuales dice, en esencia, «estas monedas pasan de aquí a aquí», más una pequeña cabecera que lo enlaza con el bloque anterior.

No hay ninguna línea que diga «Alicia tiene 2 bitcoins». Tu cartera calcula tu saldo revisando todas las transacciones pasadas de tus direcciones. Tu saldo es un resultado del historial, no un número aparte que alguien guarda y podría editar.

Tampoco se guardan nombres. Las transacciones apuntan a **direcciones**, largas cadenas de letras y números. Esto hace que Bitcoin sea **seudónimo**, no anónimo: cualquiera puede ver lo que ha hecho cada dirección, pero no sabe automáticamente quién está detrás. La lección 8 explica de dónde salen las direcciones.

COMPRUÉBALO TÚ MISMO

El primer pago de una persona a otra, los 10 bitcoins de Satoshi a Hal Finney en enero de 2009, está en el bloque 170. Abre cualquier explorador de bloques gratuito, busca el bloque 170 y lo encontrarás intacto después de más de 17 años. Todos los nodos completos del mundo siguen guardando esa misma transacción.

Cuatro propiedades que importan

Las blockchains públicas como Bitcoin comparten cuatro propiedades que los sistemas habituales no suelen tener:

- **Solo de adición.** Se pueden añadir entradas nuevas al final. Las antiguas nunca se editan ni se borran. Un error se corrige con una transacción nueva, no borrando la anterior.
- **Replicada.** El mismo registro completo existe en miles de máquinas en muchos países. Perder algunas no cambia nada.
- **Transparente.** Cualquiera puede descargar el registro y leer todas las transacciones realizadas, sin pedir permiso.
- **Sin permisos.** Cualquiera puede enviar una transacción o ejecutar un nodo, sin registrarse ni ser aprobado. La lección 12 trata las blockchains privadas, donde esto no ocurre.

ANALOGÍA: EL CHAT DE GRUPO QUE NADIE PUEDE EDITAR

Imagina un chat de grupo en el que el teléfono de cada miembro guarda todo el historial, los mensajes nunca se pueden editar ni borrar, y un mensaje nuevo solo aparece cuando la mayoría de los teléfonos han comprobado que cumple las normas del grupo. Podrías borrar la aplicación de tu teléfono, pero la conversación seguiría en todos los demás. Para cambiar lo que se dijo el año pasado, tendrías que cambiarlo a la vez en miles de teléfonos.

Lo que una blockchain no es

Las blockchains atraen grandes promesas. Conviene corregir algunas desde el principio:

- **No es una base de datos más rápida ni más barata.** Mantener de acuerdo miles de copias es lento y costoso a propósito. Para la mayoría del software cotidiano, una base de datos normal es mejor opción.
- **No es inhackeable.** El registro de Bitcoin en sí ha demostrado ser muy difícil de atacar, pero los exchanges, las carteras y las aplicaciones construidas alrededor de las blockchains sufren hackeos con frecuencia. La mayoría de las pérdidas ocurren ahí, no en la cadena.

- **No es una máquina de la verdad.** Una blockchain demuestra que se hizo una entrada y que no ha cambiado. No puede demostrar que la entrada fuera cierta desde el principio. Si entra información falsa, la cadena guardará fielmente un registro falso.

	Base de datos normal	Blockchain pública
Quién puede añadir registros	El propietario y quien él apruebe	Cualquiera que siga las reglas
Editar registros antiguos	Posible, a menudo sin que se note	Imposible sin que todos lo vean
Quién guarda copias	El propietario	Miles de nodos independientes
Quién puede leerla	Quien el propietario permita	Cualquiera
Velocidad y coste	Rápida y barata	Más lenta y más cara
Si el operador desaparece	El sistema se detiene	La red sigue funcionando

Por qué importa a los traders

- **Los saldos del exchange no están en la blockchain.** Cuando compras bitcoin en un exchange, la operación se anota en la base de datos propia del exchange. La blockchain solo ve los depósitos y los retiros. Cuando FTX quebró en noviembre de 2022, las pantallas de los clientes mostraban saldos que la empresa no podía pagar. La lección 10 explica cómo pensar en este riesgo.
- **Los datos públicos son datos de trading.** Como el registro es transparente, cualquiera puede vigilar grandes transferencias, monedas que entran o salen de los exchanges y carteras que llevaban años inactivas. Muchos traders usan estos datos on-chain, y el nivel avanzado tiene una lección completa sobre ellos.
- **La propia palabra puede mover mercados.** En diciembre de 2017, Long Island Iced Tea Corp. cambió su nombre a Long Blockchain y el precio de sus acciones se multiplicó en cuestión de horas, sin ningún negocio real de blockchain detrás. Más tarde la SEC revocó el registro de las acciones y acusó a tres personas de uso de información privilegiada. Entender qué es una blockchain te ayuda a reconocer el bombo cuando lo ves.

Términos clave

Libro de cuentas (ledger)	Un registro de quién envió qué a quién y cuándo. Una blockchain es una forma de llevar un libro de cuentas.

Nodo	Un ordenador que guarda una copia de la blockchain, comprueba los bloques nuevos según las reglas y los comparte con otros.
Consenso	El método con el que una red blockchain acuerda qué bloque se añade a continuación. Bitcoin usa prueba de trabajo.
Solo de adición	Un registro en el que se pueden añadir entradas nuevas, pero las antiguas nunca se editan ni se borran.
Seudónimo	Vinculado a una dirección en lugar de a un nombre real. La actividad es pública, pero no se sabe automáticamente quién hay detrás.
Sin permisos	Abierto a cualquiera, sin registro ni aprobación para enviar transacciones o ejecutar un nodo.

Ideas clave

1. Una blockchain es un registro de transacciones que mantienen juntos muchos ordenadores independientes, añadido en lotes enlazados y regido por reglas compartidas.
2. Toda blockchain pública tiene tres partes: el registro, la red de nodos y las reglas que deciden qué se añade.
3. Los bloques contienen transacciones, no saldos ni nombres. Tu saldo se calcula a partir del historial completo de tus direcciones.
4. Las blockchains públicas son solo de adición, replicadas, transparentes y sin permisos.
5. Una blockchain no es una base de datos más rápida, no es inhackeable y no es una máquina de la verdad. Demuestra que una entrada no cambió, no que fuera cierta.

Ponte a prueba

Marca con un círculo una respuesta en cada pregunta. Las respuestas con su explicación están en la página siguiente. También puedes hacer este cuestionario en línea en markettalks.info y ver tu puntuación al instante.

1. ¿Qué descripción de una blockchain es la más precisa?

A. Una cámara acorazada segura que guarda monedas digitales
B. Un registro de transacciones que muchos ordenadores independientes mantienen juntos con reglas compartidas
C. Un tipo de base de datos más rápida gestionada por una empresa tecnológica
D. Una web donde la gente compra y vende criptomonedas

2. ¿Qué tres partes combina toda blockchain pública?

A. Monedas, carteras y exchanges
B. Mineros, bancos y reguladores
C. El registro, la red de nodos y las reglas
D. Contraseñas, servidores y copias de seguridad

3. ¿Cómo sabe tu cartera cuál es tu saldo de bitcoin?

A. Suma todas las transacciones pasadas de tus direcciones
B. Lee una línea de saldo guardada en cada bloque
C. Se lo pregunta a la empresa que gestiona Bitcoin
D. Busca tu nombre en la blockchain

4. ¿Qué significa «solo de adición»?

A. Solo los usuarios aprobados pueden añadir registros
B. Los registros se borran pasado un tiempo
C. Solo se puede leer el bloque más reciente
D. Se pueden añadir entradas nuevas, pero las antiguas nunca se editan ni se borran

5. ¿Por qué se dice que Bitcoin es seudónimo y no anónimo?

A. Porque las transacciones se ocultan al público
B. Porque la actividad es pública y está vinculada a direcciones, pero no automáticamente a nombres reales
C. Porque los usuarios deben registrarse con su nombre real
D. Porque solo los mineros pueden ver las transacciones

6. ¿Qué afirmación sobre las blockchains es cierta?

A. Una blockchain demuestra que la información que contiene es verdadera

B. Las blockchains son más rápidas y baratas que las bases de datos normales

C. Una blockchain demuestra que una entrada no ha cambiado, pero no que fuera cierta al introducirla

D. Nada construido alrededor de una blockchain puede ser hackeado

Respuestas

1 B

Un registro de transacciones que muchos ordenadores independientes mantienen juntos con reglas compartidas

Una blockchain es un libro de cuentas compartido. Muchos ordenadores independientes guardan copias, las entradas nuevas se añaden en bloques enlazados y unas reglas compartidas deciden qué entra.

2 C

El registro, la red de nodos y las reglas

El registro contiene los bloques enlazados, la red de nodos guarda y comparte copias, y las reglas deciden qué bloques se aceptan.

3 A

Suma todas las transacciones pasadas de tus direcciones

Los bloques guardan transferencias, no saldos. Tu saldo se calcula a partir del historial de todas las transacciones hacia y desde tus direcciones.

4 D

Se pueden añadir entradas nuevas, pero las antiguas nunca se editan ni se borran

En un registro solo de adición, el historial solo crece. Un error se corrige con una transacción nueva, no cambiando una antigua.

5 B

Porque la actividad es pública y está vinculada a direcciones, pero no automáticamente a nombres reales

Cualquiera puede ver todas las transacciones de una dirección. Lo que no sabe automáticamente es quién es la persona real detrás de esa dirección.

6 C

Una blockchain demuestra que una entrada no ha cambiado, pero no que fuera cierta al introducirla

Una blockchain protege un registro para que no cambie. Si se introduce información falsa, guardará ese registro falso con la misma fidelidad.

FUENTES

- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008): https://bitcoin.org/bitcoin.pdf
- Guinness World Records, primera transacción de Bitcoin: https://guinnessworldrecords.com/world-records/696243-first-bitcoin-transaction
- Fortune, la SEC presenta cargos por uso de información privilegiada tras el cambio de nombre a Long Blockchain (julio de 2021): https://fortune.com/2021/07/09/sec-insider-trading-long-blockchain
- CoinDesk, la SEC excluye las acciones de Long Blockchain Corporation: https://www.coindesk.com/long-blockchain-corporation-shares-delisted-sec

Market Talks

SIGUE APRENDIENDO

A continuación: Lección 6 Bloques y hash, explicados de forma sencilla

Esta lección forma parte del curso gratuito de Blockchain del Centro de Educación de MARKET TALKS: lecciones de nivel principiante, intermedio y avanzado, cada una con un cuestionario y un PDF descargable.

Centro de Educación
Lecciones desde los principios básicos hasta temas avanzados

Análisis de Mercados
Análisis técnico y fundamental de los principales mercados

Informes
Bitcoin, Oro, Plata, SPX y más

markettalks.info

Telegram @MARKET_TALKS

Solo con fines educativos. Nada en este documento constituye asesoramiento financiero. © 2026 MARKET TALKS. Puedes compartir este PDF libremente sin modificarlo.