Market Talks
CENTRO DE EDUCACIÓN

BLOCKCHAIN · PRINCIPIANTE · LECCIÓN 6 DE 13

Bloques y hashing, explicados de forma sencilla

Los códigos cortos que mantienen unida la cadena, lo que realmente contiene un bloque y por qué minar es un gigantesco juego de adivinanzas

7 min de lectura 6 preguntas con sus respuestas

BLOCKCHAIN · PRINCIPIANTE · LECCIÓN 6 DE 13

Bloques y hashing, explicados de forma sencilla

EN UNA FRASE

Un hash es un código corto calculado a partir de cualquier dato. Si cambias el dato, aunque sea un poco, el código cambia por completo. Cada bloque guarda el hash del bloque anterior, así que editar la historia antigua rompe todos los eslabones que vienen después.

Un código corto que representa cualquier dato

En la lección 3 dijimos que cada registro de una cadena lleva una huella digital del anterior. Esa huella tiene un nombre propio: un **hash**.

Una **función hash** es un cálculo que toma cualquier dato, ya sea una palabra, un contrato o un bloque entero de transacciones, y lo convierte en un código corto de longitud fija. La función hash de Bitcoin se llama **SHA-256**. Su resultado siempre tiene 64 caracteres, formados por los dígitos del 0 al 9 y las letras de la a a la f. Da igual que la entrada sea una palabra o una biblioteca entera. El resultado siempre tiene 64 caracteres.

Cualquier ordenador calcula un hash en una fracción de segundo, y todo el que aplica el hash a los mismos datos obtiene exactamente el mismo resultado. Por eso un hash es una forma rápida de comprobar si dos copias de algo son idénticas sin compararlas línea por línea.

PRUÉBALO CON NUESTRO NOMBRE

Este es el hash SHA-256 del texto *Market Talks*:

`16e127cc0d60a230a1f1f80040012fc10164f835b2a99ab8f42b2ea457d9964c`

Y este es el hash de *Market talks*, con una sola letra cambiada a minúscula:

`79eaca857fb12aa6db2d1ab5c896ae9a3241eb2c96f99dd0640f2c6517a5a972`

Un cambio mínimo, y nada en el resultado parece relacionado. Puedes comprobarlos tú mismo con cualquier herramienta SHA-256 gratuita en línea.

Cuatro garantías de una buena función hash

- **Misma entrada, mismo resultado.** Los mismos datos siempre producen el mismo hash, en cualquier ordenador y en cualquier lugar del mundo.
- **Un cambio mínimo, un resultado totalmente distinto.** Cambiar un solo carácter revuelve todo el resultado, como muestra el ejemplo anterior. Esto se llama **efecto avalancha**.
- **Solo en un sentido.** Pasar de los datos al hash es fácil. Pasar de un hash a los datos originales es prácticamente imposible. La única forma de encontrar una entrada que coincida con un hash es adivinar una y otra vez.
- **En la práctica, nunca se repite.** En teoría dos entradas distintas podrían compartir un hash, pero con SHA-256 nadie ha encontrado nunca un par así. El número de resultados posibles tiene 78 cifras, más o menos tantas como los átomos que se estima que hay en el universo observable.

Juntas, estas cuatro reglas permiten que un hash funcione como un sello sobre los datos. Si el hash sigue coincidiendo, los datos no han cambiado. Si no coincide, algo se alteró, aunque sea una sola coma.

ANALOGÍA: EL BATIDO

Pon en la batidora un plátano, un poco de leche y cinco fresas. Cualquiera con la misma receta obtiene el mismo batido. Añade una fresa más y el sabor cambia. Pero nadie puede convertir un batido otra vez en un plátano entero y cinco fresas separadas. Un hash funciona igual: fácil de hacer, sensible a cada ingrediente e imposible de revertir.

Qué contiene un bloque

Un bloque de Bitcoin tiene dos partes. La parte más grande es el **cuerpo**: una lista de transacciones, normalmente unos pocos miles. La parte más pequeña es la **cabecera**, un breve resumen que incluye:

- **El hash del bloque anterior.** Es el enlace que lo convierte en una cadena.
- **Un resumen de todas sus transacciones.** Las transacciones se combinan con hashes en un único código, así que cambiar cualquiera de ellas cambia el resumen. El nivel intermedio muestra exactamente cómo se construye.
- **Una marca de tiempo** que indica aproximadamente cuándo se creó el bloque.
- **El objetivo de dificultad**, que fija lo difícil que es el acertijo de minería en ese momento.
- **Un nonce**, un número que los mineros cambian una y otra vez mientras buscan un bloque válido. Más sobre esto a continuación.

El hash del propio bloque se calcula a partir de su cabecera. Como la cabecera contiene tanto el resumen de transacciones como el hash del bloque anterior, ese único código depende de todo lo que hay en el bloque y de todo lo anterior.

Cómo los hashes bloquean la cadena

Ahora todo encaja. El bloque 102 guarda el hash del bloque 101. El bloque 103 guarda el hash del bloque 102. Y así sucesivamente, hasta el bloque génesis.

Supongamos que alguien edita una sola transacción del bloque 101. Su resumen de transacciones cambia, así que su hash cambia. Pero el bloque 102 sigue guardando el hash antiguo, de modo que el enlace entre ambos ya no coincide, y cualquier nodo lo ve al instante.

Para ocultar la edición, el atacante tendría que recalcular el bloque 101, luego el 102 y luego todos los siguientes. Y, como muestra la próxima sección, producir cada uno de esos bloques exige una cantidad enorme de intentos. Mientras tanto, la red honesta sigue añadiendo bloques nuevos encima. Por eso un pago es más seguro con cada bloque que se añade después de él.



Figura 1. Cada bloque guarda el hash del bloque anterior. Editar el bloque 101 cambia su hash, el enlace con el bloque 102 deja de coincidir y todo el mundo puede ver que la cadena fue manipulada.

Minar: un gigantesco juego de adivinanzas

La lección 4 decía que los mineros compiten por resolver un acertijo. Esto es lo que ese acertijo es en realidad. Para que un bloque sea válido, su hash debe estar por debajo de un número objetivo fijado por la red, lo que, dicho de forma sencilla, significa que el hash debe empezar con cierta cantidad de ceros.

Como los hashes funcionan en un solo sentido, no hay ningún truco para producir un hash con muchos ceros. Los mineros cambian el nonce, calculan el hash de la cabecera, comprueban el

resultado y lo vuelven a intentar, miles de millones de veces por segundo. Cada cero adicional exigido hace la búsqueda unas 16 veces más difícil.

Hicimos este experimento nosotros mismos: calculamos el hash de *Market Talks* seguido de un número que iba aumentando hasta que el resultado empezaba con suficientes ceros:

Ceros exigidos	Intentos que nos llevó	Intentos esperados de media
1	15	16
2	262	256
3	5.931	4.096
4	120.539	65.536
5	129.996	1.048.576
6	13.591.130	16.777.216

Fíjate en la fila de cinco ceros: tuvimos suerte. Minar es una lotería, y cualquier intento puede ganar. Pero, de media, el trabajo crece muy rápido. El primerísimo bloque de Bitcoin necesitó un hash que empezara con 10 ceros. Los bloques de hoy necesitan unos 19 o 20, y por eso toda la red hace ahora alrededor de mil trillones de intentos por segundo.

Por qué importa a los traders

- **Cada transacción también tiene un hash.** Se llama **ID de transacción**, o TXID. Cuando un exchange o una contraparte te diga que un pago ya se envió, pide el TXID y búscalo en un explorador de bloques. Verás si la transacción existe, cuánto se envió y cuántos bloques nuevos hay ya encima de ella.
- **El hashrate es una señal de salud.** El hashrate es el número total de intentos que hace la red por segundo. El hashrate de Bitcoin superó por primera vez un zettahash por segundo, un 1 seguido de 21 ceros, en abril de 2025. Un hashrate creciente significa que los mineros están invirtiendo en la red. Una caída brusca, como cuando una tormenta invernal en EE. UU. obligó a los mineros a apagar gran parte de sus máquinas en enero de 2026, puede poner a los mineros bajo presión.
- **Los mineros bajo presión pueden convertirse en vendedores.** Los mineros pagan la electricidad y las máquinas, a menudo vendiendo los bitcoins que ganan. Cuando sus ingresos caen, algunos venden más o apagan sus equipos. Por eso algunos traders siguen indicadores basados en el hashrate junto a los gráficos de precio.

Términos clave

Hash	Un código corto de longitud fija calculado a partir de cualquier dato. Los mismos datos siempre dan el mismo hash.
SHA-256	La función hash que usa Bitcoin. Sus resultados siempre tienen 64 caracteres.
Efecto avalancha	La propiedad por la que un cambio mínimo en la entrada produce un hash completamente distinto.
Cabecera del bloque	El breve resumen al principio de un bloque. Contiene el hash del bloque anterior, un resumen de las transacciones, una marca de tiempo y el nonce.
Nonce	Un número que los mineros cambian repetidamente mientras buscan un hash de bloque que cumpla el objetivo.
Hashrate	El número total de intentos de hash que hace la red por segundo. Una medida habitual de la potencia de minería.

Ideas clave

1. Un hash es un código corto de longitud fija calculado a partir de cualquier dato. Bitcoin se basa en SHA-256, cuyos resultados tienen 64 caracteres.
2. Los buenos hashes son constantes, cambian por completo con cualquier edición, no se pueden revertir y en la práctica no se repiten.
3. Un bloque tiene un cuerpo de transacciones y una cabecera que incluye el hash del bloque anterior y un resumen de sus transacciones.
4. Como cada bloque guarda el hash del anterior, editar un bloque antiguo rompe todos los eslabones posteriores.
5. Minar consiste en probar nonces hasta que el hash del bloque empiece con suficientes ceros, y cada cero adicional hace la búsqueda unas 16 veces más difícil.

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 hace una función hash?

A. Cifra los datos para que solo el dueño pueda leerlos
B. Convierte cualquier dato en un código corto de longitud fija
C. Comprime archivos para que ocupen menos espacio
D. Guarda transacciones en una base de datos

2. Cambias una letra de un documento y vuelves a calcular el hash. ¿Qué le pasa al hash?

A. Cambia en un carácter
B. Sigue igual
C. Se vuelve completamente distinto
D. Se hace más largo

3. ¿Por qué nadie puede recuperar los datos originales a partir de un hash?

A. Las funciones hash van en un solo sentido, así que solo queda adivinar
B. La red mantiene el hash en secreto
C. Los datos originales se borran después del hash
D. Solo los mineros tienen la clave para revertirlo

4. ¿Qué une un bloque con el bloque anterior?

A. El mismo minero crea ambos bloques
B. Ambos bloques tienen la misma marca de tiempo
C. Ambos bloques contienen las mismas transacciones
D. La cabecera de cada bloque guarda el hash del bloque anterior

5. ¿Qué es el nonce?

A. La recompensa que recibe un minero
B. Un número que los mineros cambian una y otra vez buscando un hash de bloque válido
C. El identificador de una transacción
D. El número de transacciones de un bloque

6. ¿Qué le pasa a la búsqueda de minería cada vez que se exige un cero inicial más?

A Se vuelve el doble de difícil

B No cambia

C Se vuelve unas 16 veces más difícil

D Se vuelve más fácil

Respuestas

1 B

Convierte cualquier dato en un código corto de longitud fija

Una función hash calcula un código corto de longitud fija a partir de cualquier entrada. Con SHA-256, el resultado siempre tiene 64 caracteres, sea cual sea el tamaño de la entrada.

2 C

Se vuelve completamente distinto

Es el efecto avalancha. Cualquier cambio, por pequeño que sea, revuelve todo el resultado, lo que hace que incluso las ediciones mínimas sean fáciles de detectar.

3 A

Las funciones hash van en un solo sentido, así que solo queda adivinar

El hash es fácil en un sentido y prácticamente imposible al revés. Precisamente por eso la minería tiene que hacerse por ensayo y error.

4 D

La cabecera de cada bloque guarda el hash del bloque anterior

Cada cabecera incluye el hash del bloque anterior. Si se edita un bloque antiguo, su hash cambia y deja de coincidir con lo que guarda el bloque siguiente.

5 B

Un número que los mineros cambian una y otra vez buscando un hash de bloque válido

Los mineros cambian el nonce, calculan el hash de la cabecera y comprueban el resultado, una y otra vez, hasta que el hash empieza con suficientes ceros.

6 C

Se vuelve unas 16 veces más difícil

Cada carácter de un hash puede tomar uno de 16 valores, así que exigir un cero más hace que un resultado válido sea unas 16 veces menos frecuente.

FUENTES

- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008): https://bitcoin.org/bitcoin.pdf
- NIST, FIPS 180-4, estándar de hash seguro (SHA-256): https://csrc.nist.gov/files/pubs/fips/180-4/final/docs/fips180-4.pdf
- Forklog, el hashrate de Bitcoin supera por primera vez un zettahash (abril de 2025): https://forklog.com/en/bitcoin-hashrate-surpasses-one-zettahash-for-the-first-time/
- KuCoin, el hashrate de Bitcoin en 2026: tendencias, dificultad de minería y seguridad de la red: https://www.kucoin.com/blog/in-bitcoin-hashrate-in-2026-latest-trends-mining-difficulty-network-security-analysis

Market Talks

SIGUE APRENDIENDO

A continuación: Lección 7 Nodos y la red entre pares

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.