Market Talks
CENTRO DE EDUCACIÓN

BLOCKCHAIN · PRINCIPIANTE · LECCIÓN 4 DE 13

2008 y el nacimiento de Bitcoin

Un documento de nueve páginas, un titular de periódico escondido en el primer bloque y un creador que se marchó

8 min de lectura 6 preguntas con sus respuestas

BLOCKCHAIN · PRINCIPIANTE · LECCIÓN 4 DE 13

2008 y el nacimiento de Bitcoin

EN UNA FRASE

En 2008, un autor desconocido llamado Satoshi Nakamoto combinó las piezas de los experimentos anteriores y resolvió el único problema que ninguno pudo: lograr que desconocidos se pongan de acuerdo en una sola historia sin nadie al mando.

Nueve páginas en plena crisis

En septiembre de 2008 quebró el banco de inversión Lehman Brothers, y los gobiernos de todo el mundo se apresuraron a rescatar a sus bancos con dinero público. La confianza en el sistema financiero estaba por los suelos.

Seis semanas después, el 31 de octubre de 2008, apareció un mensaje en una lista de correo que leían criptógrafos. Su autor, que firmaba como **Satoshi Nakamoto**, anunciaba un nuevo tipo de dinero electrónico que funcionaba directamente entre usuarios, sin un tercero de confianza. Incluía un enlace a un documento breve: *Bitcoin: A Peer-to-Peer Electronic Cash System*. Tenía solo nueve páginas.

El documento no ocultaba sus raíces. Citaba b-money, Hashcash y la investigación sobre marcas de tiempo que conociste en la lección 3. Lo que aportaba era una forma de hacer funcionar esas piezas juntas sin una empresa, un banco ni un servidor de confianza en el centro. Muchos lectores de la lista se mostraron escépticos. Algunos sostenían que nunca podría procesar suficientes pagos. Otros simplemente lo ignoraron.

La pieza que faltaba, resuelta

La lección 3 terminó con una pregunta abierta: si miles de ordenadores independientes guardan cada uno una copia del registro, ¿cómo se ponen de acuerdo sobre qué versión es la correcta cuando nadie manda? La respuesta de Bitcoin tiene tres partes.

Primero, los pagos se agrupan en lotes llamados **bloques**, y cada bloque está enlazado con el anterior, como en la cadena de marcas de tiempo de la lección 3. Segundo, el derecho a añadir el siguiente bloque se gana mediante **prueba de trabajo**, la idea que usó por primera vez Hashcash. Unos ordenadores llamados **mineros** compiten por resolver un acertijo, y todos los demás

comprueban el bloque del ganador antes de construir sobre él. Tercero, si alguna vez compiten dos versiones de la historia, cada ordenador sigue la cadena que tiene más trabajo detrás.

Juntas, estas reglas hacen que hacer trampa sea carísimo. Para reescribir un pago ya enterrado en la cadena, un atacante tendría que rehacer el trabajo de ese bloque y de todos los posteriores, y hacerlo más rápido que el resto de la red junta. Además, el minero ganador recibe bitcoins recién creados como recompensa, así que el mismo trabajo que protege el registro también emite el dinero. Ninguna de las dos tareas necesita una empresa.



Figura 1. A veces dos mineros encuentran un bloque casi al mismo tiempo. La red sigue construyendo sobre la cadena con más trabajo y el bloque rival se descarta.

ANALOGÍA: LA RIFA CARA

Imagina un cuaderno compartido en el que solo una persona puede escribir a la vez. Para decidir quién escribe la página siguiente, todos compran boletos de una rifa, y cada boleto cuesta electricidad real. Se sortea un ganador más o menos cada diez minutos. Quien quiera falsificar páginas antiguas tiene que ganar la rifa una y otra vez, lo que significa comprar más boletos que todos los demás juntos. Los participantes honestos siguen ganando porque son muchísimos más.

3 de enero de 2009: el primer bloque

El 3 de enero de 2009, Satoshi creó el primerísimo bloque de la cadena de Bitcoin, conocido como **bloque génesis**. Su recompensa fue de 50 bitcoins y, por una peculiaridad del código, esas monedas nunca se pueden gastar. Seis días después se publicó el programa para que cualquiera pudiera descargarlo y ejecutarlo.

El 12 de enero de 2009, Satoshi envió 10 bitcoins a Hal Finney, el criptógrafo detrás de RPOW de la lección 3. Fue el primer pago de una persona a otra en la red. Durante meses, los usuarios fueron un pequeño grupo de aficionados que ejecutaban el programa en sus ordenadores de casa.

UN MENSAJE EN EL PRIMER BLOQUE

Satoshi escribió una línea de texto en el bloque génesis: *The Times 03/Jan/2009 Chancellor on brink of second bailout for banks* («El ministro de Hacienda, al borde de un segundo rescate a los bancos»). Era el titular de portada del periódico británico ese día. Como las huellas publicadas en el periódico de la lección 3, demuestra que el bloque no pudo crearse antes de esa fecha. Muchos lectores también lo ven como un comentario sobre por qué se creó Bitcoin.

Reglas escritas desde el primer día

A diferencia de DigiCash o e-gold, Bitcoin no tiene un emisor que decida cuánto dinero crear. La oferta sigue reglas integradas en el programa desde el principio:

- **Un bloque nuevo cada 10 minutos aproximadamente.** Cada 2.016 bloques, más o menos cada dos semanas, el acertijo se vuelve automáticamente más difícil o más fácil para mantener ese ritmo, tanto si los mineros añaden máquinas como si las retiran.
- **Una recompensa que se reduce.** La recompensa por bloque empezó en 50 bitcoins y se reduce a la mitad cada 210.000 bloques, aproximadamente cada cuatro años. Este evento se llama **halving**. Tras el halving de abril de 2024, la recompensa es de 3,125 bitcoins.
- **Un límite fijo.** Como la recompensa sigue reduciéndose a la mitad, la oferta total nunca podrá superar los 21 millones de bitcoins. Se espera que las últimas fracciones se minen hacia el año 2140.

Cambiar estas reglas no es algo que pueda hacer una sola persona. Cada ordenador de la red comprueba cada bloque según las reglas que ejecuta, así que un bloque que las incumple simplemente se rechaza. La lección 7 analiza estos ordenadores con más detalle.

De afición a primer precio

Durante la mayor parte de 2009, los bitcoins no tenían ningún precio. En octubre de 2009, un usuario que se hacía llamar New Liberty Standard publicó el primer tipo de cambio frente al dólar: 1.309,03 bitcoins por un dólar estadounidense. Llegó a esa cifra calculando cuánta electricidad gastaba su ordenador para minar monedas.

El 22 de mayo de 2010, un programador de Florida, Laszlo Hanyecz, pagó 10.000 bitcoins por dos pizzas, una de las primeras compras de bienes reales con esta moneda. A lo largo de 2010 aparecieron los primeros exchanges, y Bitcoin empezó a tener un precio de mercado que cambiaba cada día. Había nacido un mercado de trading.

El creador que se marchó

Satoshi nunca reveló un nombre real, una cara ni una ubicación, y solo escribía mediante publicaciones en foros y correos electrónicos. Durante 2010, Satoshi fue cediendo poco a poco el control del código a otros desarrolladores voluntarios. El último mensaje confirmado, un correo fechado el 23 de abril de 2011, decía que Satoshi había «pasado a otras cosas». La identidad detrás del nombre sigue siendo desconocida.

Los investigadores que estudiaron los primeros bloques estiman que un solo minero, al que muchos identifican con Satoshi, reunió unos 1,1 millones de bitcoins durante el primer año. Las pruebas son circunstanciales, y esas monedas nunca se han movido.

La desaparición resultó importante. DigiCash y e-gold tenían cada uno un fundador y una empresa que podían quebrar, ser acusados o recibir presiones. Bitcoin no tiene ni lo uno ni lo otro. No hay una sede que cerrar ni un líder cuyas decisiones todos deban seguir.

Debilidad anterior	La respuesta de Bitcoin
El dinero digital se podía copiar	Cada pago se comprueba frente a una única historia compartida
Una empresa decidía cuánto dinero existía	Las monedas nuevas solo surgen de reglas fijas en el programa
Un servidor de confianza frenaba el doble gasto	Miles de ordenadores independientes comprueban cada bloque
No había forma de acordar sin un líder	La prueba de trabajo elige quién añade el siguiente bloque, y gana la cadena con más trabajo
Un fundador al que se podía acusar o presionar	Un creador anónimo que se apartó

Por qué importa a los traders

- **La crisis forma parte de la historia.** Bitcoin se lanzó en plena crisis bancaria, con un titular sobre rescates en su primer bloque. Esa historia vuelve cada vez que los bancos están bajo presión. En marzo de 2023, cuando quebraron varios bancos de EE. UU., bitcoin subió con fuerza mientras algunos inversores buscaban activos fuera del sistema bancario. Narrativas así pueden mover los precios, aunque no duren.
- **El calendario de emisión es público.** La fecha de cada halving se puede estimar con años de antelación, y muchos traders siguen un ciclo de unos cuatro años en torno a ellos. Recuerda que un evento conocido puede estar ya descontado en el precio, y que los ciclos pasados no garantizan el siguiente.
- **Las monedas antiguas se vigilan de cerca.** Las monedas de los primeros años son noticia cada vez que se mueven. En septiembre de 2026, 600 bitcoins minados en 2010 se movieron tras 16 años, y los analistas comprobaron enseguida que no había un vínculo claro con Satoshi. Revisar los datos on-chain antes de reaccionar a un titular puede evitarte operar con un rumor.

Términos clave

Whitepaper	Un documento breve que explica cómo debe funcionar un nuevo sistema o proyecto. El de Bitcoin tenía nueve páginas.
Bloque génesis	El primer bloque de una blockchain. El de Bitcoin se creó el 3 de enero de 2009.
Minero	Un ordenador, o quien lo opera, que compite por añadir el siguiente bloque mediante prueba de trabajo a cambio de una recompensa.
Recompensa por bloque	Los bitcoins nuevos que recibe el minero ganador por añadir un bloque. Es como se crean todos los bitcoins nuevos.
Halving	La reducción a la mitad de la recompensa por bloque cada 210.000 bloques, aproximadamente cada cuatro años.
Cadena con más trabajo	La regla según la cual, cuando compiten versiones de la historia, la red sigue la que tiene más prueba de trabajo detrás.

Ideas clave

1. Satoshi Nakamoto publicó el whitepaper de Bitcoin, de nueve páginas, el 31 de octubre de 2008, en plena crisis bancaria.
2. Bitcoin combinó bloques enlazados en cadena, la prueba de trabajo y la regla de la cadena con más trabajo, para que desconocidos puedan acordar una sola historia sin nadie al mando.
3. El bloque génesis del 3 de enero de 2009 lleva un titular de periódico sobre rescates bancarios que demuestra la fecha en que se creó.
4. Los bitcoins nuevos solo surgen de recompensas por bloque que se reducen a la mitad cada cuatro años aproximadamente, y el total nunca podrá superar los 21 millones.
5. Satoshi se marchó en 2011 sin revelar su identidad, y no quedó ningún fundador ni empresa que se pudiera cerrar.

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. ¿Cuándo se publicó el whitepaper de Bitcoin?

- A) En enero de 2009
- B) El 31 de octubre de 2008
- C) En mayo de 2010
- D) En abril de 2011

2. Si compiten dos versiones de la blockchain, ¿cuál sigue la red?

- A) La creada por el ordenador más antiguo
- B) La elegida por votación de los exchanges
- C) La que tiene más prueba de trabajo detrás
- D) La que contiene más pagos

3. ¿Qué demuestra el titular de periódico del bloque génesis?

A Que el bloque no pudo crearse antes del 3 de enero de 2009
B Que un banco aprobó Bitcoin
C Que Satoshi vivía en el Reino Unido
D Que los primeros bitcoins estaban respaldados en libras

4. ¿Cómo se crean los bitcoins nuevos?

A Un banco central los imprime cuando hace falta
B Satoshi los libera cada año
C Los exchanges los crean cuando sube la demanda
D Los mineros los reciben como recompensa por añadir bloques

5. ¿Qué ocurre en un halving?

A El precio de bitcoin se reduce a la mitad
B La recompensa por añadir un bloque se reduce a la mitad
C Se destruye la mitad de todos los bitcoins
D Los bloques se añaden el doble de rápido

6. ¿Por qué la desaparición de Satoshi ayudó a Bitcoin?

A Abarató la minería de bitcoin
B Eliminó todas las reglas del sistema
C No dejó ningún fundador ni empresa que se pudiera cerrar o presionar
D Permitió a Satoshi vender monedas en secreto

Respuestas

1 B

El 31 de octubre de 2008

Satoshi compartió el documento de nueve páginas en una lista de correo de criptografía el 31 de octubre de 2008, unas seis semanas después de la quiebra de Lehman Brothers.

2 C

La que tiene más prueba de trabajo detrás

Cada ordenador sigue la cadena con más trabajo detrás. Para reemplazarla, un atacante necesitaría más potencia de cálculo que el resto de la red junta.

3 A

Que el bloque no pudo crearse antes del 3 de enero de 2009

El titular se imprimió el 3 de enero de 2009, así que el bloque no puede ser anterior. Quién era Satoshi y dónde vivía sigue siendo un misterio.

4 D

Los mineros los reciben como recompensa por añadir bloques

La recompensa por bloque es la única forma en que nacen bitcoins nuevos. Sigue reglas fijas del programa, así que nadie puede decidir emitir más.

5 B

La recompensa por añadir un bloque se reduce a la mitad

Cada 210.000 bloques, aproximadamente cada cuatro años, la recompensa por bloque se reduce a la mitad. Por eso la oferta total nunca podrá superar los 21 millones.

6 C

No dejó ningún fundador ni empresa que se pudiera cerrar o presionar

DigiCash y e-gold cayeron junto con sus empresas. Sin un líder conocido, Bitcoin no tiene una sede que cerrar ni una sola persona cuyas decisiones todos deban seguir.

FUENTES

- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008): https://bitcoin.org/bitcoin.pdf
- Lista de correo de criptografía, Bitcoin P2P e-cash paper (31 de octubre de 2008): https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html
- Cointelegraph, Bitcoin cumple diez años en el aniversario del bloque génesis: https://cointelegraph.com/news/bitcoin-turns-ten-on-anniversary-of-genesis-block
- Bitcoin Magazine, Bitcoin ha subido un 6.500 millones por ciento desde su primer precio en dólares: https://bitcoinmagazine.com/culture/bitcoin-is-up-6-5-billion-percent-since-it-was-first-priced-in-usd
- The Defiant, el último correo de Satoshi Nakamoto a Mike Hearn (23 de abril de 2011): https://thedefiant.io/news/people/bitcoin-creator-satoshi-nakamoto-sent-final-email-to-mike-hearn-on-april-23-2011-6735013c
- Cointelegraph, ¿tiene Satoshi realmente 1 millón de bitcoins?: https://cointelegraph.com/news/big-questions-does-satoshi-actually-own-1-million-bitcoin

Market Talks

SIGUE APRENDIENDO

A continuación: Lección 5 Qué es realmente una blockchain

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.