Market Talks
CENTRO DE EDUCACIÓN

BLOCKCHAIN · PRINCIPIANTE · LECCIÓN 11 DE 13

El recorrido de una transacción

Qué ocurre entre pulsar Enviar y que lleguen las monedas, y por qué a veces tarda más de lo que esperas

6 min de lectura 6 preguntas con sus respuestas

BLOCKCHAIN · PRINCIPIANTE · LECCIÓN 11 DE 13

El recorrido de una transacción

EN UNA FRASE

Una transacción cripto se prepara y se firma en tu cartera, pasa de nodo en nodo, espera en una zona de espera, la recoge un minero o un validador y después queda enterrada bajo nuevos bloques. La comisión que pagas decide cuándo sale de la cola.

Paso 1: tu cartera la prepara y la firma

Cuando pulsas Enviar, todavía no llega nada a la blockchain. Primero tu cartera arma un pequeño mensaje que dice tres cosas: qué monedas se gastan, adónde van y cuánto ofreces como comisión.

En Bitcoin, tu saldo no es un único número. Es un conjunto de trozos de moneda separados que recibiste antes, llamados **salidas no gastadas**. Para enviar 0,3 BTC desde un trozo que vale 0,5 BTC, la cartera gasta el trozo entero: 0,3 va al destinatario, una pequeña cantidad va a la comisión y el resto vuelve a una dirección tuya como **cambio**. Ethereum funciona más como el saldo de un banco, pero la idea de la firma es la misma.

Por último, la cartera firma el mensaje con tu clave privada, como vimos en la lección 8. La firma demuestra que el dueño aprobó exactamente este pago. Si después cambias un solo dígito, la firma deja de encajar.

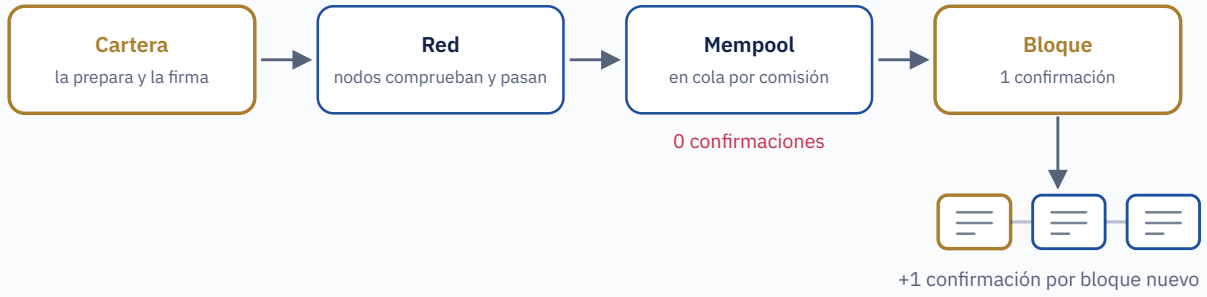


Figura 1. Una transacción se firma en la cartera, los nodos la comprueban y la reenvían, espera en la mempool y obtiene su primera confirmación cuando un minero la incluye en un bloque. Cada bloque posterior suma una más.

EJEMPLO: ADÓNDE VAN 0,5 BTC

Tienes un trozo que vale 0,5 BTC y quieres enviar 0,3 BTC a un amigo. Tu cartera escribe una transacción con dos salidas: 0,3 BTC para tu amigo y 0,1999 BTC de vuelta a tu propia dirección de cambio. Los 0,0001 BTC que faltan no figuran en ningún sitio como salida. Lo que sobra es la comisión, y la cobra el minero que incluye la transacción.

Paso 2: difusión y sala de espera

La transacción firmada se entrega a un nodo, que la comprueba: ¿son válidas las firmas?, ¿existen las monedas?, ¿se han gastado ya? Si todo está en orden, el nodo la pasa a sus pares y en pocos segundos se ha extendido por la red, como mostró la lección 7.

Cada nodo guarda las transacciones válidas que ha recibido en una zona de espera llamada **mempool**, abreviatura de memory pool. No existe una única mempool. Cada nodo tiene la suya, así que su contenido varía ligeramente. Mientras tu transacción está ahí tiene **cero confirmaciones**: la red la conoce, pero todavía no está en la blockchain y, en casos poco frecuentes, aún podría sustituirse.

Paso 3: la comisión decide quién va primero

Un bloque de Bitcoin llega más o menos cada diez minutos y tiene un espacio limitado. Cuando hay más transacciones esperando de las que caben en un bloque, los mineros lo llenan con las que más pagan por el espacio que ocupan. Por eso las comisiones de Bitcoin se expresan como una tarifa, en **satoshis por byte virtual** (sat/vB), y no como un porcentaje del importe. Enviar 10 dólares o 10 millones de dólares cuesta lo mismo si las transacciones tienen el mismo tamaño.

Estado de la red	Lo que suele ocurrir
Mempool tranquila	Incluso una comisión baja entra en el siguiente bloque o en el de después
Mempool congestionada	Las transacciones con comisión baja esperan, a veces horas o días
Avalancha repentina	Las comisiones pueden multiplicarse en menos de una hora

La avalancha puede ser extrema. El 20 de abril de 2024, el bloque que redujo a la mitad la recompensa de minería de Bitcoin, el bloque 840.000, recaudó más de 37 BTC en comisiones, unos 2,4 millones de dólares de entonces, porque muchísimos usuarios compitieron por entrar en ese bloque histórico.

ANALOGÍA: EL ÚLTIMO FERRI DE LA NOCHE

Un pequeño ferri sale cada diez minutos con un número fijo de asientos. En una noche tranquila sube todo el mundo. En un fin de semana festivo la cola es larga y la tripulación deja subir a quien ofrece el precio más alto por asiento. Si ofreciste el mínimo, sigues en la cola cuando llega el siguiente barco, y el que viene después.

Paso 4: confirmaciones y liquidación

Cuando un minero incluye tu transacción en un bloque que la red acepta, tiene **una confirmación**. Cada bloque que se añade encima suma una más. Cada bloque adicional hace más difícil revertir el pago, porque un atacante tendría que rehacer todos esos bloques, como explicó la lección 6.

Confirmaciones (Bitcoin)	Significado habitual
0	La red la ha visto, pero aún no está en un bloque
1	Está en un bloque, suficiente para importes pequeños del día a día
Varias	Lo que suelen esperar los exchanges antes de abonar un depósito, según la plataforma
6	Una regla práctica de toda la vida para importes grandes, alrededor de una hora

Otras redes tienen su propio ritmo. Ethereum añade un bloque cada 12 segundos y considera un bloque definitivo al cabo de unos 13 minutos, cuando ya no se puede revertir sin destruir una enorme cantidad de ETH en staking.

Cuando una transacción se atasca

Si pones una comisión demasiado baja en un momento de mucho tráfico, tu transacción puede pasar mucho tiempo esperando en las mempools. No se pierde nada: las monedas no se han movido. Las transacciones muy antiguas acaban eliminándose de la mayoría de las mempools y las monedas se quedan donde estaban. Hay dos soluciones habituales:

- **Replace-by-fee (RBF, sustitución por comisión).** Tu cartera envía una nueva versión del mismo pago con una comisión más alta, que sustituye a la anterior.
- **Child pays for parent (CPFP, el hijo paga por el padre).** El destinatario, o tú a través del cambio, gasta las monedas atascadas en una nueva transacción con una comisión alta, de modo que el minero tenga motivos para incluir las dos juntas.

Sea cual sea la solución, puedes seguir todo el recorrido por tu cuenta. Cada transacción tiene un identificador, el **txid**, que puedes pegar en un explorador de bloques para ver si está esperando, si está confirmada y a qué profundidad está enterrada.

Por qué importa a los traders

- **Los depósitos no son instantáneos.** Un exchange abona tus bitcoins solo después del número de confirmaciones que exige. Si piensas operar un movimiento rápido, las monedas tienen que estar en el exchange antes del movimiento, no de camino.
- **Las comisiones suben cuando el mercado se mueve.** Las oscilaciones bruscas de precio llevan a mucha gente a la blockchain a la vez, y las comisiones se disparan con ellas. Comprueba la tarifa actual antes de enviar y evita la opción más baja cuando el tiempo importa.
- **Guarda el txid.** Si un depósito o una retirada parece retrasarse, el txid te dice exactamente dónde está. También es lo primero que te pedirá el soporte del exchange.

Términos clave

Mempool	La zona de espera donde cada nodo guarda las transacciones válidas que esperan a ser incluidas en un bloque.
Comisión de transacción	Lo que paga el remitente para que se incluya su transacción. En Bitcoin es lo que queda al restar las salidas de las entradas.
sat/vB	Satoshis por byte virtual, la tarifa que se usa para comparar comisiones de Bitcoin. Un satoshi es una cienmillonésima de bitcoin.
Confirmación	Un bloque de la cadena que contiene tu transacción o que llega después de ella. Más confirmaciones significan un pago más difícil de revertir.
Salida de cambio	La parte de una moneda gastada que la cartera devuelve a la propia dirección del remitente.
ID de transacción (txid)	El código único que identifica una transacción y permite buscarla en un explorador de bloques.

Ideas clave

1. Una transacción se prepara y se firma en tu cartera antes de que se envíe nada a la red.

2. Los nodos la comprueban, la reenvían y la guardan en sus mempools, donde tiene cero confirmaciones.
3. El espacio en el bloque es limitado, así que los mineros eligen las transacciones con la tarifa más alta, no las de mayor importe.
4. Cada bloque añadido después del tuyo es una confirmación más, y los exchanges esperan un número fijo antes de abonarte.
5. Una transacción atascada se puede acelerar con replace-by-fee o child pays for parent, y seguir con su txid.

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. ¿Dónde se firma una transacción?

- A En el primer nodo que la recibe
- B En la cartera del remitente, antes de enviarla
- C La firma el minero que la incluye en un bloque
- D En la cartera del destinatario cuando llega

2. Gastas una moneda de 0,5 BTC para enviar 0,3 BTC. ¿Qué pasa con el resto?

- A Se pierde para siempre
- B Queda bloqueado hasta el próximo halving
- C La mayor parte vuelve a ti como cambio y el pequeño resto es la comisión
- D El destinatario se lo queda como propina

3. ¿Qué es la mempool?

- A La zona de espera de cada nodo para las transacciones válidas que esperan un bloque
- B Un único servidor mundial gestionado por los desarrolladores de Bitcoin
- C Una cartera que guarda monedas para los exchanges
- D La parte de un bloque donde se anotan las comisiones

4. Dos transacciones de Bitcoin tienen el mismo tamaño. Una envía 10 dólares y la otra 10 millones. ¿Cuál necesita una comisión más alta para entrar rápido?

A. La de 10 millones, porque las comisiones son un porcentaje
B. Ninguna, necesitan la misma tarifa
C. La de 10 dólares, porque los pagos pequeños se retrasan
D. Las comisiones las fija el exchange, no la red

5. Tu transacción está en un bloque y después se han añadido dos bloques más. ¿Cuántas confirmaciones tiene?

A. Una
B. Dos
C. Tres
D. Seis

6. Tu transacción con comisión baja lleva horas esperando en un momento de mucho tráfico. ¿Cuál es una solución habitual?

A. Enviar las mismas monedas otra vez a una dirección nueva
B. Contactar con los mineros y pedirles que la incluyan
C. Restaurar la cartera desde la frase semilla
D. Usar replace-by-fee para enviar una nueva versión con una comisión más alta

Respuestas

1 B

En la cartera del remitente, antes de enviarla

La cartera firma con la clave privada antes de difundirla. Los nodos y los mineros solo comprueban la firma, no pueden crearla.

2 C

La mayor parte vuelve a ti como cambio y el pequeño resto es la comisión

Bitcoin gasta monedas enteras. La cartera envía la diferencia a tu propia dirección de cambio y deja un poco sin asignar como comisión.

3 A

La zona de espera de cada nodo para las transacciones válidas que esperan un bloque

Cada nodo tiene su propia mempool, así que no hay una sola. Guarda transacciones válidas que todavía no están en un bloque.

4 B

Ninguna, necesitan la misma tarifa

Los mineros comparan las comisiones por byte virtual de espacio. El importe enviado no importa, solo el tamaño de la transacción.

5 C

Tres

El bloque que la contiene cuenta como la primera confirmación y cada bloque posterior suma una más, así que uno más dos son tres.

6 D

Usar replace-by-fee para enviar una nueva versión con una comisión más alta

Replace-by-fee cambia la transacción en espera por una versión con una comisión más alta. La otra opción habitual es child pays for parent.

FUENTES

- Bitcoin Developer Guide, transacciones: https://developer.bitcoin.org/devguide/transactions.html
- Cointelegraph, los usuarios de Bitcoin gastan un récord de 2,4 millones de dólares en comisiones en el bloque del halving: https://cointelegraph.com/news/bitcoin-halving-users-spend-record-millions-block-space-runes-rare-satoshis
- ethereum.org, prueba de participación y finalidad: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/
- Bitcoin Optech, Replace-by-fee: https://bitcoinops.org/en/topics/replace-by-fee/

Market Talks

SIGUE APRENDIENDO

A continuación: Lección 12 Blockchains públicas, privadas y de consorcio

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.