Market Talks

CENTRO DE EDUCACIÓN

BLOCKCHAIN · PRINCIPIANTE · LECCIÓN 8 DE 13

Claves, direcciones y carteras

Qué demuestra realmente que un bitcoin es tuyo, qué compartes para que te paguen y qué guarda de verdad una cartera

6 min de lectura 6 preguntas con sus respuestas

BLOCKCHAIN · PRINCIPIANTE · LECCIÓN 8 DE 13

Claves, direcciones y carteras

EN UNA FRASE

Tener bitcoin significa tener una clave privada, un número secreto que te permite firmar pagos. De ella salen una clave pública y una dirección que puedes compartir. Una cartera no guarda monedas en absoluto: guarda claves y las usa para firmar.

Un secreto y dos cosas que puedes compartir

En la lección 5 vimos que la blockchain no guarda nombres, solo direcciones. Entonces, ¿cómo sabe la red que una moneda es tuya? La respuesta es un conjunto de tres piezas enlazadas:

- **Clave privada.** Un número secreto elegido al azar entre un rango tan enorme que tiene 78 cifras, la misma escala que los hashes de la lección 6. Quien lo conoce puede gastar las monedas vinculadas a él.
- **Clave pública.** Un número calculado a partir de la clave privada con un tipo especial de matemáticas. Se puede mostrar a cualquiera.
- **Dirección.** Un código más corto obtenido al aplicar un hash a la clave pública, con una comprobación incorporada que detecta errores de escritura. Es lo que das a la gente para que pueda pagarte.

Cada paso funciona en un solo sentido. Convertir una clave privada en una pública, y una pública en una dirección, le lleva a un ordenador una fracción de segundo. Ir hacia atrás es prácticamente imposible. Por eso puedes publicar tu dirección en cualquier parte sin poner en riesgo tus monedas.



Figura 1. La clave privada crea la clave pública, y esta crea la dirección. Cada paso funciona en un solo sentido, así que compartir tu dirección nunca revela tu clave privada.

Gastar es firmar

Para gastar bitcoin, tu cartera construye una transacción y le añade una **firma digital** hecha con tu clave privada. Cualquier nodo puede comprobar esa firma con tu clave pública y confirmar que la hizo la clave privada correspondiente, sin ver nunca la clave privada.

La firma también está ligada a los detalles exactos de esa única transacción. Si alguien cambia el importe o el destino aunque sea en un carácter, la firma deja de coincidir y todos los nodos la rechazan. Por eso nadie puede interceptar tu pago a su paso por la red y desviarlo.

Este es el gran cambio respecto a la banca. Un banco decide si puedes gastar comprobando quién eres. Bitcoin solo comprueba si la firma es válida. Sin nombre, sin restablecer contraseñas, sin atención al cliente: solo matemáticas.

ANALOGÍA: EL BUZÓN CON RANURA

Piensa en una dirección como un buzón con una ranura delante. Cualquiera que sepa dónde está puede echar una carta, y toda la calle ve cuántas cartas llegan. Pero solo quien tiene la llave puede abrir el buzón y sacar las cartas. Si pierdes la llave, las cartas quedan encerradas para siempre. Si alguien copia la llave, puede vaciar el buzón.

Cómo son las direcciones de Bitcoin

Bitcoin ha cambiado de formato de dirección varias veces. Todos siguen funcionando y se distinguen por sus primeros caracteres:

Empieza por	Tipo	Desde
1	Legacy, el formato original	2009
3	Dirección de script, usada a menudo para carteras compartidas o multifirma	2012
bc1q	Native SegWit, transacciones más pequeñas y comisiones más bajas	2017
bc1p	Taproot, el formato más nuevo, con más privacidad y flexibilidad	2021

Otras blockchains usan sus propios estilos. Las direcciones de Ethereum, por ejemplo, empiezan por *0x* seguido de 40 caracteres. No puedes sustituir una dirección de Bitcoin por una de Ethereum, aunque la misma aplicación muestre ambas.

Una buena cartera crea una dirección nueva cada vez que pides recibir. Todas pertenecen a la misma cartera, y las antiguas siguen funcionando. Usar direcciones nuevas dificulta que los extraños relacionen todos tus pagos.

Qué guarda de verdad una cartera

A pesar del nombre, una cartera nunca guarda monedas. Las monedas solo existen como anotaciones en la blockchain. Una **cartera** es una herramienta que guarda tus claves, lee la blockchain para mostrar tu saldo, crea transacciones y las firma.

Las carteras se dividen en dos grandes grupos:

- **Carteras calientes**: guardan las claves en un dispositivo conectado a internet, como una aplicación de móvil o un programa de ordenador. Son cómodas para el día a día, pero las claves quedan expuestas a cualquier cosa que pueda atacar ese dispositivo.
- **Carteras frías**: guardan las claves sin conexión. Una **cartera de hardware** es un pequeño dispositivo que guarda las claves dentro y firma transacciones sin revelarlas nunca a tu ordenador. Es más lenta de usar, pero mucho más difícil de hackear.

Si tus monedas están en un exchange, las claves las tiene el exchange, no tú. La lección 10 compara las dos opciones, y la lección 9 trata la copia de seguridad que protege todas tus claves a la vez.

UN EJEMPLO REAL: EL DISCO DURO DEL VERTEDERO

En 2013, James Howells, un ingeniero informático de Gales, tiró por error un disco duro viejo que contenía la clave privada de 8.000 bitcoins que había minado años antes. El disco acabó en un vertedero municipal. Pasó más de una década pidiendo permiso para excavarlo. En enero de 2025, un tribunal del Reino Unido desestimó su demanda, y su recurso fue rechazado ese mes de marzo. Las monedas siguen en la blockchain, visibles para todos y sin que nadie pueda gastarlas.

Por qué importa a los traders

- **Comprueba la dirección completa, siempre.** En la estafa de envenenamiento de direcciones, los atacantes envían una transacción diminuta desde una dirección casi idéntica a una que usas, con la esperanza de que la próxima vez la copies de tu historial. En mayo de 2024, un trader envió a una dirección así 1.155 bitcoins envueltos, unos 68 millones de dólares. El atacante devolvió después la mayor parte tras unas negociaciones, algo muy poco habitual.
- **Comprueba la red, no solo la dirección.** Los exchanges suelen admitir la misma moneda en varias redes. Enviar por una red que el receptor no admite puede hacer que recuperar los fondos sea muy difícil o imposible. Revisa la red y cualquier memo o etiqueta obligatoria antes de confirmar.
- **Envía primero una prueba pequeña.** En transferencias grandes o primeras, un pequeño pago de prueba cuesta algo de comisión y puede salvar el importe entero. Muchos traders también usan listas blancas de direcciones de retiro en sus cuentas de exchange.

Términos clave

Clave privada	Un número secreto y aleatorio que permite a quien lo tiene firmar transacciones y gastar las monedas vinculadas a él.
Clave pública	Un número calculado a partir de la clave privada que se puede compartir y sirve para comprobar firmas.
Dirección	Un código más corto obtenido de la clave pública, que compartes para que otros te envíen monedas.
Firma digital	Una prueba hecha con una clave privada que aprueba una transacción exacta y que cualquiera puede comprobar con la clave pública.
Cartera	Una herramienta que guarda tus claves, muestra tu saldo a partir de la blockchain y crea y firma transacciones.
Cartera de hardware	Un pequeño dispositivo que mantiene las claves privadas sin conexión y firma transacciones sin exponerlas a un ordenador.

Ideas clave

1. Tener bitcoin significa controlar una clave privada. Quien tiene la clave puede gastar las monedas.
2. La clave pública y la dirección se calculan a partir de la clave privada, y ninguna de las dos puede convertirse de nuevo en ella.
3. Para gastar hace falta una firma digital ligada a la transacción exacta, que cualquier nodo puede comprobar sin ver la clave privada.
4. Las direcciones de Bitcoin empiezan por 1, 3, bc1q o bc1p según su tipo, y una cartera puede crear una dirección nueva para cada pago.
5. Las carteras guardan claves, no monedas. Las calientes son cómodas, mientras que las frías mantienen las claves sin conexión y son mucho más seguras.

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 da a alguien el poder de gastar bitcoin?

- A Conocer la dirección
- B Tener la clave privada
- C Tener una cuenta en un exchange
- D Conocer el ID de la transacción

2. ¿Por qué es seguro compartir tu dirección públicamente?

- A Porque las direcciones caducan tras un solo uso
- B Porque la red oculta la dirección a los demás
- C Porque nadie puede llegar desde la dirección hasta la clave privada
- D Porque las direcciones están cifradas

3. ¿Qué pasa si alguien cambia el importe de una transacción firmada?

A La firma deja de coincidir y los nodos la rechazan
B La transacción se realiza con el nuevo importe
C La firma se actualiza automáticamente
D El minero decide qué importe usar

4. ¿Qué guarda realmente una cartera de criptomonedas?

A Tus monedas
B Una copia de toda la blockchain
C Tus datos bancarios
D Tus claves

5. Una dirección de Bitcoin empieza por bc1q. ¿De qué tipo es?

A Legacy
B Native SegWit
C Ethereum
D Taproot

6. ¿Cuál es la principal ventaja de una cartera de hardware?

A Hace las transacciones más rápidas
B Elimina todas las comisiones
C Mantiene las claves privadas sin conexión y firma sin exponerlas
D Permite recuperar monedas enviadas a una dirección equivocada

Respuestas

1 B

Tener la clave privada

La clave privada es la que firma los pagos. Cualquiera que la tenga puede gastar las monedas, por eso debe mantenerse en secreto.

2 C

Porque nadie puede llegar desde la dirección hasta la clave privada

Cada paso de clave privada a clave pública y a dirección va en un solo sentido. Otros pueden enviar a tu dirección, pero no pueden usarla para encontrar tu clave privada.

3 A

La firma deja de coincidir y los nodos la rechazan

Una firma está ligada a los detalles exactos de una transacción. Cualquier cambio, aunque sea de un carácter, la invalida.

4 D

Tus claves

Las monedas solo existen en la blockchain. La cartera guarda tus claves, lee tu saldo en la cadena y firma tus transacciones.

5 B

Native SegWit

Las direcciones que empiezan por bc1q son Native SegWit, introducidas en 2017. Las de Taproot empiezan por bc1p, y las Legacy por 1.

6 C

Mantiene las claves privadas sin conexión y firma sin exponerlas

Una cartera de hardware guarda las claves dentro del dispositivo y solo saca transacciones firmadas, así que el malware de tu ordenador no puede leer las claves.

FUENTES

- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008): https://bitcoin.org/bitcoin.pdf
- Wikipedia, los bitcoins enterrados en el vertedero de Newport: https://en.wikipedia.org/wiki/Bitcoin_buried_in_Newport_landfill
- Cointelegraph, un trader pierde 68 millones de dólares por envenenamiento de direcciones (mayo de 2024): https://cointelegraph.com/news/trader-loses-68-million-address-poisoning-scam
- Cointelegraph, el atacante devuelve los fondos tras negociar: https://cointelegraph.com/news/wbtc-address-poisoner-all-funds-negotiations

Market Talks

SIGUE APRENDIENDO

A continuación: Lección 9 Frases semilla y copias de seguridad

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.