Market Talks

CENTRO DE EDUCACIÓN

CRIPTO · PRINCIPIANTE · LECCIÓN 15 DE 15

Cómo empezar de verdad: exchanges, KYC y carteras

Cómo son los primeros pasos prácticos: elegir un exchange, pasar el KYC, proteger la cuenta, hacer una primera compra, configurar una cartera de autocustodia y mover fondos a ella

12 min de lectura 8 preguntas con sus respuestas

CRIPTO · PRINCIPIANTE · LECCIÓN 15 DE 15

Cómo empezar de verdad: exchanges, KYC y carteras

EN UNA FRASE

La mayoría de la gente empieza en cripto con un exchange centralizado y más adelante añade una cartera que controla por sí misma. Esta lección recorre cada paso, qué implica y dónde se producen los errores habituales.

Dos formas de tener criptomonedas

Antes de abrir ninguna cuenta, conviene conocer las dos formas básicas de tener criptomonedas:

- **En un exchange (custodial):** abres una cuenta en una empresa como Binance o Coinbase. El exchange tiene las claves privadas, y tu saldo es un número en su base de datos, como el dinero en una cuenta bancaria. Es sencillo, y si olvidas la contraseña, el exchange puede ayudarte a recuperar el acceso.
- **En tu propia cartera (autocustodia):** instalas una cartera como MetaMask o un dispositivo de hardware como Ledger. Tú tienes las claves a través de una frase semilla. Nadie puede congelar ni perder tus monedas por ti, pero tampoco nadie puede recuperarlas por ti.

Un dicho popular resume la diferencia: **«si no son tus claves, no son tus monedas»** (not your keys, not your coins). Mucha gente usa las dos cosas: un exchange para comprar y vender, y una cartera para guardar cripto y usarla en las blockchains (Lecciones 9 y 12, y Lección 9 de Blockchain).



Figura 1. En un exchange, la empresa tiene las claves; en una cartera de autocustodia, las tienes tú.

EJEMPLO: CUANDO LOS EXCHANGES FALLAN

En noviembre de 2022 el exchange FTX quebró, y sus clientes no pudieron retirar sus fondos durante mucho tiempo. En febrero de 2025, unos hackers a los que el FBI vinculó con Corea del Norte robaron a Bybit unos **1.500 millones de dólares** en ether. Bybit mantuvo abiertas las retiradas y dijo que cubriría las pérdidas de los clientes, pero los dos casos muestran lo mismo: las monedas guardadas en un exchange dependen de la seguridad y la honradez de esa empresa.

Elegir un exchange

Un exchange centralizado (Lección 9) es la puerta de entrada habitual, el lugar donde el dinero corriente se convierte en cripto. Aspectos que la gente suele comparar:

- **Disponibilidad y licencias:** si el exchange puede dar servicio a usuarios de tu país y qué regulador lo supervisa.
- **Métodos de depósito:** transferencia bancaria, tarjeta u opciones de pago locales, y qué divisas admite.
- **Monedas y redes:** qué monedas cotiza y qué redes admite para depósitos y retiradas (Lección 5).
- **Comisiones:** comisiones de trading, recargos por tarjeta, spreads en la «compra instantánea» y comisiones de retirada.
- **Historial:** hackeos o retiradas congeladas en el pasado, y si publica una prueba de reservas.

Exchange	Conocido por
Binance	El mayor exchange del mundo por volumen de negociación, con una lista de monedas muy amplia
Coinbase	Empresa cotizada de EE. UU., app sencilla, fuerte en EE. UU. y Europa
OKX	Exchange global con una cartera de autocustodia integrada
Bybit	Exchange global popular para operar con derivados
Kraken	Uno de los exchanges más antiguos, fuerte en EE. UU. y Europa
Upbit	El mayor exchange de Corea del Sur, opera en wones surcoreanos

Estos nombres son ejemplos de servicios muy usados, **no recomendaciones**. Los servicios y las normas cambian, y no todos los exchanges están disponibles en todos los países. En algunos

países, como Corea del Sur, los exchanges locales exigen además una cuenta bancaria a nombre real del titular en un banco asociado.

Registro y KYC

Los exchanges regulados deben comprobar quiénes son sus clientes. Esto se llama **KYC**, siglas de «conoce a tu cliente» (know your customer), y forma parte de las leyes contra el lavado de dinero (AML, anti-money laundering) de la mayoría de los países. Un registro típico es así:

1. **Cuenta:** correo electrónico o número de teléfono y una contraseña.
2. **Datos personales:** nombre completo, fecha de nacimiento, domicilio y nacionalidad.
3. **Documento de identidad:** una foto del pasaporte, del documento nacional de identidad o del permiso de conducir.
4. **Selfie o verificación por vídeo:** la app comprueba que la cara coincide con el documento y que hay una persona real delante.
5. **Aprobación:** a menudo en minutos, a veces en unos días. Algunos exchanges piden más adelante un justificante de domicilio o del origen de los fondos para tener límites más altos.

Según una norma relacionada llamada **Regla de viaje** (Travel Rule), los exchanges de muchos países también intercambian datos del remitente y del destinatario en las transferencias más grandes entre ellos, y pueden preguntar de quién es la cartera a la que se retira.

El KYC implica que el exchange guarda datos personales sensibles. Es una de las razones por las que importa que el sitio sea el auténtico: los sitios de exchanges falsos también recopilan fotos de documentos (Lección 14).

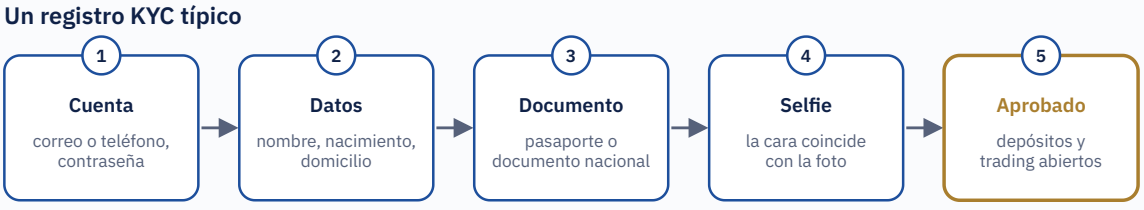


Figura 2. Los pasos habituales del KYC al abrir una cuenta en un exchange.

Proteger la cuenta

Una cuenta en un exchange es un objetivo, así que los exchanges ofrecen varias capas de protección. Estas son las que más a menudo se activan primero:

- **Autenticación de dos factores (2FA):** un segundo código necesario para iniciar sesión y para retirar. Las apps de autenticación como Google Authenticator, y las llaves de acceso (passkeys) o

las llaves de seguridad, son más difíciles de robar que los códigos por SMS, que pueden caer en otras manos mediante un duplicado de SIM (SIM swap).

- **Código antiphishing:** una palabra que eliges tú y que el exchange incluye en cada correo auténtico que envía. Un correo sin ella no procede del exchange.
- **Lista blanca de direcciones:** solo se permiten retiradas a direcciones guardadas de antemano, a menudo con un periodo de espera para las nuevas.
- **Alertas de dispositivo e inicio de sesión:** avisos cuando alguien inicia sesión desde un dispositivo o un lugar nuevos.
- **Una contraseña única y robusta** que no se usa en ningún otro sitio.



Figura 3. Los exchanges ofrecen varias capas de protección para la cuenta.

Hacer una primera compra

Una vez verificada la cuenta, se deposita dinero y se cambia por cripto:

- **Depósito:** la transferencia bancaria suele ser la vía más barata. Las tarjetas son más rápidas, pero a menudo cuestan un pequeño porcentaje del importe. Algunos exchanges ofrecen también mercados P2P (de persona a persona), donde los usuarios negocian directamente entre sí a través del exchange.
- **Botón «Comprar» o «Convertir»:** la vía más sencilla. Introduces un importe y recibes una cotización. La comisión suele ir incluida en un precio menos favorable (el spread).
- **Mercado spot:** la pantalla de trading con un libro de órdenes (Lección 9). Una orden de mercado compra al mejor precio disponible; una orden limitada espera a tu precio. Aquí las comisiones suelen ser más bajas.

Tras la compra, las monedas quedan en tu cuenta del exchange. Desde ahí pueden quedarse, venderse o retirarse a una cartera.

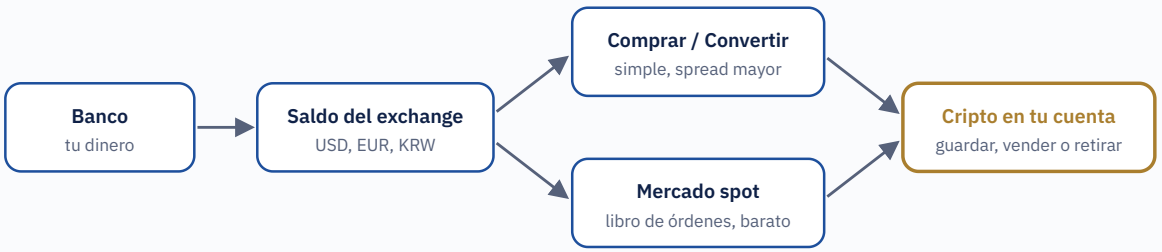


Figura 4. Dos formas de comprar en un exchange después de depositar dinero.

EJEMPLO: DOS FORMAS DE COMPRAR

Sophie deposita 500 $ por transferencia bancaria. Usa el sencillo botón «Comprar» para adquirir 250 $ de bitcoin y recibe algo menos de lo que esperaba, porque la cotización incluía un spread de alrededor del 1%. Para los otros 250 $ usa el mercado spot con una orden de mercado y paga una comisión de trading del 0,1%, unos 25 centavos. Las dos son formas normales de comprar; la diferencia está sobre todo en el coste y en cuánto quiere lidiar con la pantalla de trading.

Carteras: calientes, frías y los nombres más comunes

Una cartera de autocustodia es una app o un dispositivo que guarda tus claves y firma transacciones (Lección 9 de Blockchain). Los tipos principales:

- **Carteras calientes** (hot wallets): están conectadas a internet; son apps de móvil y extensiones del navegador. Son gratuitas y cómodas para el día a día y para conectarse a aplicaciones DeFi.
- **Carteras frías** (cold wallets): guardan las claves sin conexión, normalmente en un pequeño dispositivo de hardware. Las transacciones se aprueban pulsando botones en el propio dispositivo, así que un malware del ordenador no puede firmar por sí solo.

Cartera	Tipo	Redes principales
MetaMask	Extensión del navegador y app de móvil	Ethereum y otras redes EVM como BNB Chain, Base y Arbitrum, y ahora también Solana y Bitcoin
Trust Wallet	App de móvil y extensión	Muchas redes, entre ellas BNB Chain, Ethereum y Bitcoin
Phantom	App de móvil y extensión	Solana en primer lugar, y también Ethereum, Base y Bitcoin
Ledger	Cartera de hardware	Muchas redes; se usa con su app Ledger Live o con otras carteras
Trezor	Cartera de hardware	Muchas redes; se usa con su app Trezor Suite o con otras carteras

De nuevo, son ejemplos habituales, no recomendaciones. Las apps de cartera son uno de los blancos favoritos de las falsificaciones, así que la gente suele descargarlas solo desde la web oficial o desde un enlace de esa web. Las carteras de hardware se suelen comprar directamente al fabricante, ya que un dispositivo de segunda mano o manipulado puede no ser seguro.



Figura 5. Las carteras calientes están en línea y son cómodas; las frías guardan las claves sin conexión. Los nombres son ejemplos, no recomendaciones.

Configurar una cartera y la frase semilla

Al crear una cartera nueva, esta muestra una **frase semilla** (también llamada frase de recuperación) de 12 o 24 palabras. Esas palabras pueden recrear todas las claves de la cartera en cualquier app o dispositivo compatible. Eso significa que:

- Cualquiera que vea la frase semilla puede llevarse todo lo que hay en la cartera.
- Si se pierde el móvil y también la frase semilla, los fondos se pierden para siempre. La empresa de la cartera no tiene ninguna copia y no puede restablecerla.

Una práctica habitual es escribir las palabras en papel o grabarlas en metal, comprobarlas con cuidado y guardarlas sin conexión en un lugar seguro, a veces en dos sitios distintos. Las capturas de pantalla, las fotos, las notas en la nube, el correo y los gestores de contraseñas sincronizados en línea son las vías habituales por las que se roban frases semilla. Ningún agente de soporte, app o sitio web auténtico la necesita nunca (Lección 14).

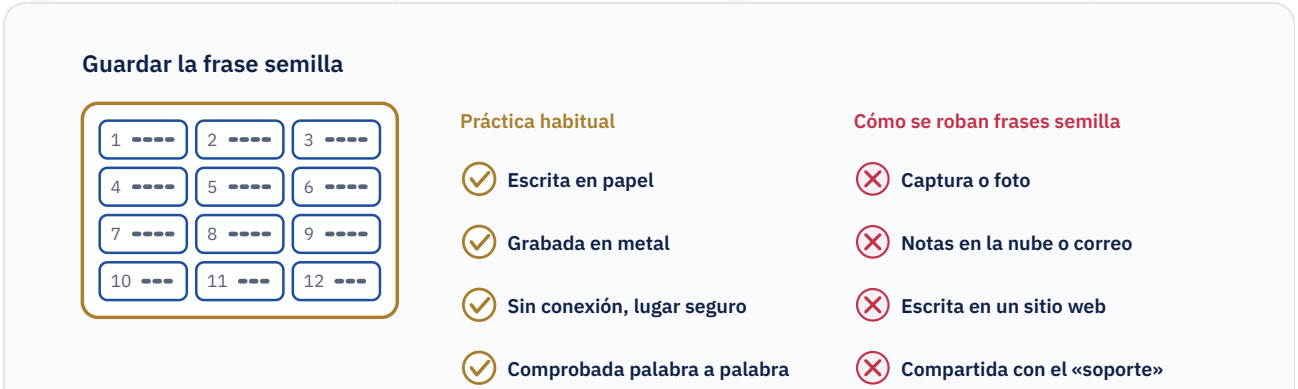


Figura 6. La frase semilla controla la cartera. La forma de guardarla decide quién puede llevarse los fondos.

Mover fondos a una cartera y un primer swap

Retirar de un exchange a tu propia cartera pone en práctica todo lo visto en la Lección 10:

1. Se copia la **dirección de recepción** de la cartera, para la red correcta.
2. En el exchange se elige **Retirar**, se pega la dirección y se selecciona la **misma red**. La etiqueta memo se añade solo si el lado receptor la necesita.
3. Se comprueban los primeros y los últimos caracteres de la dirección.
4. Mucha gente envía primero una **pequeña cantidad de prueba** y después el resto, cuando la prueba ha llegado.

Para usarse en esa red, la cartera también necesita un poco de la **moneda nativa de la red para el gas**, como ETH en Ethereum, BNB en BNB Chain o SOL en Solana (Lección 5).

Un primer swap en un exchange descentralizado (Lección 9) funciona entonces así: se abre el sitio oficial del DEX, se **conecta** la cartera, se eligen los dos tokens, se comprueban el impacto en el precio y el deslizamiento, se **aprueba** el token si se pide (la Lección 14 explica por qué importan las aprobaciones) y, por último, se **confirma** el swap en la cartera y se paga la comisión de gas.

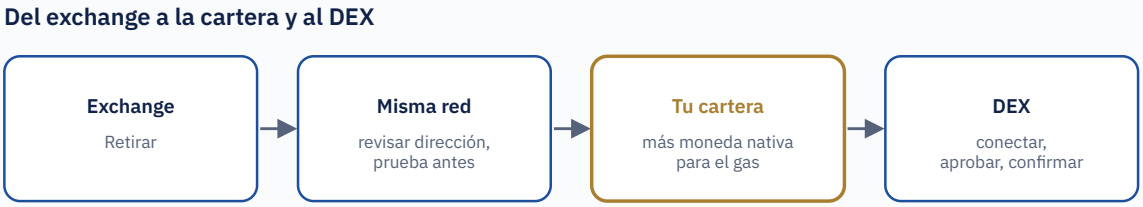


Figura 7. Mover fondos de un exchange a una cartera de autocustodia y hacer después un primer swap en un DEX.

Todo el recorrido de un vistazo

Juntando toda la lección, una primera configuración típica tiene ocho etapas. No todo el mundo pasa por todas: mucha gente solo usa un exchange, y otras personas pasan a la autocustodia al cabo de un tiempo.

Esta lección cierra el nivel Principiante de Cripto. Ya sabes qué son las criptomonedas, en qué se diferencian las monedas, los tokens y las redes, dónde se negocian, cómo se mueven los precios, cuáles son los riesgos principales y cómo son los primeros pasos prácticos. Los niveles Intermedio y Avanzado de Cripto, para miembros, profundizan en el trading, los datos on-chain y DeFi.



Figura 8. Una primera configuración típica, desde la cuenta en el exchange hasta el primer swap en un DEX.

Por qué esto importa a los traders

- **La elección del exchange influye en los costes.** Las comisiones de trading, los spreads, las tasas de financiación y las comisiones de retirada se acumulan a lo largo de muchas operaciones. Los tramos de comisiones suelen depender del volumen.
- **El riesgo de contraparte es real.** Los fondos que se tienen en un exchange para operar dependen de ese exchange. Muchos traders solo mantienen allí lo que necesitan para operar y guardan el resto en otro lugar.
- **Los ajustes de seguridad protegen la cuenta de trading.** La 2FA, un código antiphishing y una lista blanca de direcciones hacen que una contraseña robada le sirva de mucho menos a un atacante.
- **Moverse entre exchanges y carteras es rutina.** Elegir la red correcta y comprobar las direcciones se convierten en hábitos diarios para los traders activos.

Términos clave

Custodial	Un modelo en el que una empresa, como un exchange, tiene las claves privadas en tu nombre.
Autocustodia	Tener tus propias claves en una cartera que controlas, sin que ninguna empresa pueda congelar ni recuperar los fondos.
KYC	Conoce a tu cliente (know your customer): los controles de identidad que los exchanges regulados deben hacer antes de dar servicio a un cliente o mientras se lo dan.
Regla de viaje (Travel Rule)	Una norma que obliga a los exchanges a intercambiar datos del remitente y del destinatario en determinadas transferencias.
2FA	Autenticación de dos factores: una segunda prueba de identidad, como un código de una app de autenticación, además de la contraseña.
Código antiphishing	Una palabra personal que un exchange incluye en sus correos auténticos para que los usuarios puedan detectar los falsos.
Lista blanca de direcciones	Una lista de direcciones guardadas, las únicas autorizadas a recibir retiradas de una cuenta.
Cartera caliente (hot wallet)	Una cartera cuyas claves están en un dispositivo conectado a internet, como una app de móvil o una extensión del navegador.

Cartera fría (cold wallet)	Una cartera que guarda las claves sin conexión, normalmente en un dispositivo de hardware.
Frase semilla	Una lista de 12 o 24 palabras que puede recrear todas las claves de una cartera.
Red EVM	Una blockchain que ejecuta la máquina virtual de Ethereum (EVM), así que funciona con las mismas carteras, direcciones y aplicaciones que Ethereum. BNB Chain, Base, Arbitrum y Polygon son ejemplos.

Ideas clave

1. Las criptomonedas pueden guardarse en un exchange (custodial) o en tu propia cartera (autocustodia). Mucha gente usa las dos cosas.
2. Los exchanges se diferencian en disponibilidad, métodos de depósito, monedas, redes, comisiones e historial. Los nombres de esta lección son ejemplos, no recomendaciones.
3. El KYC son los controles de documento de identidad y selfie que exigen las leyes contra el lavado de dinero.
4. La 2FA con una app de autenticación o una llave de acceso, un código antiphishing y una lista blanca de direcciones son las principales protecciones de la cuenta.
5. Las carteras calientes son cómodas; las frías guardan las claves sin conexión. La frase semilla lo controla todo y no se puede restablecer.
6. Retirar a una cartera requiere la dirección correcta, la misma red y algo de moneda nativa para el gas. Un swap en un DEX consiste en conectar, aprobar y confirmar.

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 significa «si no son tus claves, no son tus monedas»?

- A Las monedas en un exchange siempre se pierden
- B Si otra persona tiene las claves, tus monedas dependen de ella
- C Las claves privadas solo hacen falta en Bitcoin
- D Hace falta una cartera de hardware para comprar cripto

2. ¿Por qué los exchanges regulados piden un documento de identidad y un selfie?

- A Para fijar tus comisiones de trading
- B Por el KYC y las leyes contra el lavado de dinero
- C Para elegir tu red
- D Para crear tu frase semilla

3. ¿Qué es un código antiphishing?

- A Una contraseña para las retiradas
- B Una palabra que el exchange incluye en sus correos auténticos
- C Un código que bloquea todos los inicios de sesión
- D Un tipo de cartera de hardware

4. ¿Qué forma de 2FA es más fácil de robar?

- A Una app de autenticación
- B Una llave de seguridad física
- C Los códigos por SMS
- D Una llave de acceso (passkey)

5. ¿Cuál es la principal diferencia entre una cartera caliente y una fría?

- A Las calientes solo guardan bitcoin
- B Las frías guardan las claves sin conexión
- C Las calientes no tienen frase semilla
- D Las frías no pueden enviar transacciones

6. Anna pierde el móvil y nunca anotó su frase semilla. ¿Qué pasa con su cartera de autocustodia?

- A La empresa de la cartera la restablece
- B Su exchange puede restaurarla
- C Ya no se puede acceder a los fondos
- D La blockchain le devuelve las monedas

7. Lucas retira USDT de un exchange a su cartera en BNB Chain. ¿Qué red tiene que elegir en el exchange?

A Cualquiera, todas son iguales

B Ethereum, porque es la mayor

C BNB Chain, la misma red que la dirección de su cartera

D Bitcoin

8. El USDT de Lucas llega, pero el swap falla porque no puede pagar la comisión. ¿Qué le falta?

A Una frase semilla

B Un poco de BNB para el gas

C La aprobación del KYC

D Un código antiphishing

Respuestas

1 B

Si otra persona tiene las claves, tus monedas dependen de ella

En un exchange, la empresa tiene las claves, así que tu saldo depende de su seguridad y su honradez.

2 B

Por el KYC y las leyes contra el lavado de dinero

Los controles KYC son un requisito legal para los exchanges regulados en la mayoría de los países.

3 B

Una palabra que el exchange incluye en sus correos auténticos

Si un correo que dice venir del exchange no muestra tu código, no es auténtico.

4 C

Los códigos por SMS

Los códigos por SMS se pueden interceptar mediante un duplicado de SIM, en el que un atacante traslada tu número de teléfono a su propia tarjeta SIM.

5 B

Las frías guardan las claves sin conexión

Las carteras calientes guardan las claves en dispositivos conectados a internet; las frías las guardan sin conexión y aprueban las transacciones en el propio dispositivo.

6 C

Ya no se puede acceder a los fondos

Solo la frase semilla puede recrear las claves. Sin ella, nadie puede recuperar los fondos.

7 C

BNB Chain, la misma red que la dirección de su cartera

Las redes de envío y de recepción deben coincidir; si no, los fondos pueden perderse o ser difíciles de recuperar (Lección 10).

8 B

Un poco de BNB para el gas

Cada transacción en una red se paga en la moneda nativa de esa red, aquí BNB en BNB Chain.

FUENTES

- TRM Labs, el hackeo de Bybit: siguiendo el mayor ataque de Corea del Norte: https://www.trmlabs.com/post/the-bybit-hack-following-north-koreas-largest-exploit
- TechTarget, FBI: el Grupo Lazarus, detrás del robo de 1.500 millones de dólares a Bybit: https://www.techtarget.com/cybersecurity/news/366619872/FBI-Lazarus-Group-behind-15-billion-Bybit-heist
- The Block, MetaMask se vuelve multicadena: una sola cuenta admite EVM, Solana y pronto Bitcoin: https://theblock.co/post/376450/metamask-multichain-account
- Cointelegraph, MetaMask añade compatibilidad con Bitcoin: https://cointelegraph.com/news/metamask-adds-bitcoin-support-after-teasing-february

- Tiger Research, el mercado de criptomonedas de Corea en 2026: https://reports.tiger-research.com/p/2026-korea-cryptocurrency-market-eng

Market Talks

SIGUE APRENDIENDO

Esta lección forma parte del curso de Cripto del Centro de Educación de MARKET TALKS. Las lecciones de nivel principiante son gratuitas, cada una con un cuestionario y un PDF descargable. Las lecciones de nivel intermedio y avanzado son para miembros.

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.