Market Talks
CENTRO DE EDUCACIÓN

BLOCKCHAIN · PRINCIPIANTE · LECCIÓN 10 DE 13

Custodia: cuenta en un exchange o tu propia cartera

Quién tiene de verdad tus monedas, qué dice la historia de cada opción y cómo reparten la diferencia la mayoría de los traders

5 min de lectura · 6 preguntas con sus respuestas

BLOCKCHAIN · PRINCIPIANTE · LECCIÓN 10 DE 13

Custodia: cuenta en un exchange o tu propia cartera

EN UNA FRASE

Guardar cripto en un exchange significa que el exchange tiene las claves y tú tienes una promesa. Guardarla en tu propia cartera significa que tienes las claves y toda la responsabilidad. Cada opción te protege de riesgos distintos.

Dos formas de tener el mismo bitcoin

Custodia significa simplemente quién tiene las claves privadas. Hay dos modelos básicos:

- **Custodial.** Un exchange u otra empresa tiene las claves. Entras con una contraseña, y tu saldo es un número en la propia base de datos de la empresa, como vimos en la lección 5. Cuando retiras, la empresa firma la transacción por ti.
- **Autocustodia.** Tú tienes las claves, normalmente en una cartera respaldada con una frase semilla de la lección 9. Nadie puede mover tus monedas ni impedirte moverlas, pero tampoco nadie puede rescatarte si pierdes las claves.

En la blockchain no existe "tu cuenta" en un exchange. Las direcciones del exchange guardan juntas las monedas de todos, y su base de datos registra qué parte de ese montón pertenece a cada cliente.

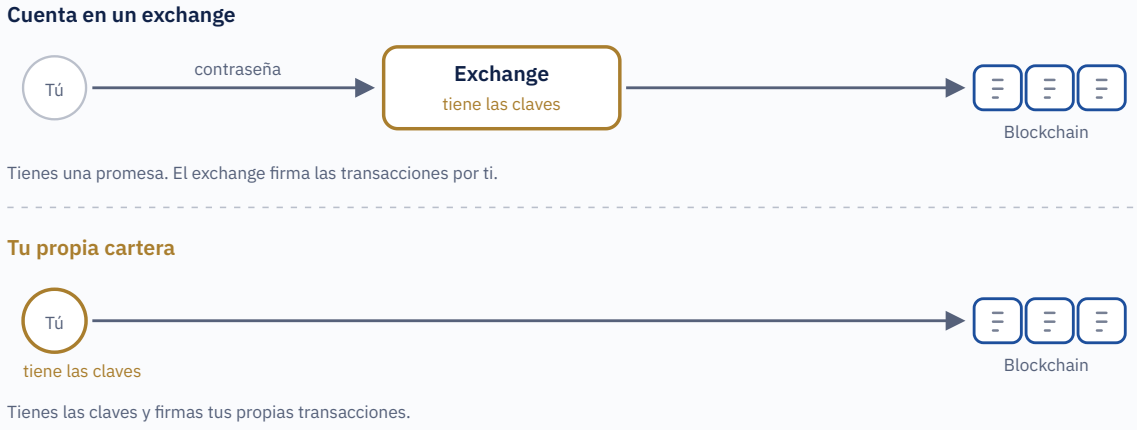


Figura 1. Con una cuenta en un exchange, la empresa tiene las claves y llegas a la blockchain a través de ella. Con tu propia cartera, tienes las claves y tratas con la blockchain directamente.

ANALOGÍA: EL GUARDARROPA

En un evento concurrido, dejas el abrigo en el guardarropa y te dan un tique numerado. Es cómodo, y normalmente recuperas el abrigo. Pero durante la noche tienes un tique, no un abrigo. Si roban el guardarropa, cierra antes de tiempo o ha prestado abrigos a otros a escondidas, tu tique vale lo que valgan las personas detrás del mostrador. Llevar el abrigo puesto es menos cómodo, pero nadie más puede perderlo.

Lo que dice la historia sobre los exchanges

La mayoría de los exchanges nunca quiebran. Pero cuando han caído los grandes, los clientes han esperado años y a menudo han perdido gran parte de su dinero:

Exchange	Qué pasó	Qué vivieron los clientes
Mt. Gox (2014)	El mayor exchange de bitcoin de su época perdió unos 850.000 BTC por robo y mala gestión	Los pagos de lo que quedaba no empezaron hasta julio de 2024, diez años después
QuadrigaCX (2019)	El fundador murió, y las carteras frías que solo él controlaba resultaron estar casi vacías	Se debían unos 215 millones de dólares canadienses a unos 76.000 usuarios
FTX (2022)	El dinero de los clientes lo había usado una empresa de trading hermana, y los retiros se detuvieron en pocos días	Faltaban miles de millones de fondos de clientes, y el fundador fue condenado después por fraude

En todos los casos, las pantallas mostraban saldos normales hasta el final. Un saldo en un exchange es un derecho frente a la empresa, no una prueba de que las monedas estén ahí.

Los riesgos de guardarlo tú mismo

La autocustodia saca a la empresa de la ecuación, pero te pasa todo el trabajo a ti. Las formas más comunes en que la gente pierde monedas por su cuenta son:

- **Perder la copia de seguridad.** Una frase semilla perdida y un dispositivo roto significan monedas bloqueadas para siempre. Investigadores de Chainalysis calcularon en 2017 que ya se habían perdido así entre unos 2,8 y 3,8 millones de bitcoins, cerca de una quinta parte de todas las monedas minadas hasta entonces.
- **Filtrar la copia de seguridad.** Una frase semilla escrita en una web o app falsa se lo entrega todo a un ladrón, como mostró la lección 9.
- **Errores al enviar.** Una dirección o red equivocada no se puede revertir, como mostró la lección 8.

No hay atención al cliente ni forma de restablecer la contraseña. Ese es el precio de no tener una empresa que pueda quebrar o congelar tus fondos.

Cómo lo reparte la mayoría

Para mucha gente la respuesta no es una cosa o la otra. Un enfoque habitual es tratar el exchange como la cartera que llevas en el bolsillo y la autocustodia como la caja fuerte de casa:

	Cuenta en un exchange	Tu propia cartera
Quién tiene las claves	El exchange	Tú
Si olvidas la contraseña	El soporte normalmente puede devolverte el acceso	Solo tu frase semilla puede
Si la empresa quiebra	Tus monedas pueden quedar congeladas o perderse	No cambia nada
Más adecuada para	Trading activo y cantidades que vas a usar pronto	Inversiones a largo plazo y ahorros
Riesgo principal	La empresa: hackeos, fraude, congelaciones, quiebra	Tú: copias perdidas, estafas, errores

Si mantienes fondos en un exchange, elige plataformas grandes y reguladas con una larga trayectoria, activa todas las funciones de seguridad que ofrezcan y comprueba si publican con regularidad una prueba de reservas (proof of reserves). Recuerda que la prueba de reservas muestra los activos que el exchange tiene en un momento dado, pero no siempre todo lo que debe.

Por qué importa a los traders

- **Futuros y margen necesitan custodia.** Para operar contratos perpetuos, tu garantía tiene que estar en el exchange. Deja allí lo que tus posiciones necesitan, no todo tu patrimonio, y pasa con regularidad a tu propia cartera los beneficios que no necesites para operar.
- **Vigila las señales de alarma.** Retiros lentos o pausados, cambios repentinos en los límites de retiro y grandes salidas de monedas de un exchange en la cadena han precedido a menudo a los problemas. A principios de noviembre de 2022, los retiros de FTX se ralentizaron y se detuvieron en pocos días. Actuar ante las primeras señales es más fácil que ante las últimas.
- **La autocustodia cuesta velocidad.** Mover monedas de tu cartera a un exchange lleva tiempo y comisiones de red, y en un mercado rápido los minutos cuentan. Decide cuánto tener en cada lado antes de que llegue la volatilidad, no durante ella.

Términos clave

Custodia	El control de las claves privadas y, por tanto, de las monedas que desbloquean.
Custodial	Un sistema en el que una empresa guarda las claves por ti, como una cuenta en un exchange.
Autocustodia	Tener tus propias claves en una cartera que controlas, normalmente respaldada con una frase semilla.
Riesgo de contraparte	El riesgo de que una empresa que guarda tus activos quiebre, los congele o no te los devuelva.
Prueba de reservas	Una comprobación publicada que muestra los activos de un exchange en un momento dado y que puede no mostrar todo lo que debe.
Not your keys, not your coins	Un dicho muy extendido: "si no son tus claves, no son tus monedas". Si otro tiene las claves, tú solo tienes su promesa de devolverte las monedas.

Ideas clave

1. Custodia significa quién tiene las claves. En un exchange las tiene la empresa, y en la autocustodia las tienes tú.
2. Un saldo en un exchange es un número en la base de datos de la empresa y un derecho frente a ella, no monedas bajo tu control.

3. Mt. Gox, QuadrigaCX y FTX muestran que la quiebra de un exchange puede congelar los fondos de los clientes durante años o perderlos por completo.
4. La autocustodia elimina el riesgo de la empresa pero añade riesgo personal: copias perdidas, frases semilla filtradas y errores al enviar.
5. Mucha gente guarda los fondos de trading en un exchange de confianza y las inversiones a largo plazo en su propia cartera.

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 custodia en cripto?

A. Quién tiene las claves privadas
B. Qué exchange cobra menos comisiones
C. Cuánto tiempo piensas mantener una moneda
D. Qué país regula una moneda

2. Tienes 1 BTC en tu cuenta de un exchange. ¿Qué tienes en realidad?

A. Una clave privada a tu nombre
B. Un derecho frente al exchange, anotado en su base de datos
C. Monedas en una dirección personal que solo controlas tú
D. Una cartera de hardware que guarda el exchange

3. ¿Cuál fue una razón clave por la que los clientes de QuadrigaCX no pudieron recuperar su dinero?

A. La red de Bitcoin dejó de funcionar
B. Los clientes perdieron sus frases semilla
C. Solo el fundador controlaba las carteras, y estaban casi vacías cuando murió
D. Un gobierno confiscó todos los exchanges de Canadá

4. ¿Qué riesgo elimina la autocustodia?

A. El riesgo de perder tu frase semilla
B. El riesgo de enviar a una dirección equivocada
C. El riesgo de phishing
D. El riesgo de que un exchange congele o pierda tus monedas

5. ¿Cuál es una forma habitual de repartir los fondos entre los dos modelos?

A. Todo en el exchange por comodidad
B. Fondos de trading en un exchange de confianza y ahorros a largo plazo en tu propia cartera
C. Todo en autocustodia, incluida la garantía de los futuros
D. Repartido a partes iguales en tantos exchanges como sea posible

6. ¿Qué puede no mostrar una prueba de reservas?

A. Qué monedas tiene el exchange
B. Las direcciones de las carteras del exchange
C. Todo lo que el exchange debe a clientes y prestamistas
D. La fecha de la comprobación

Respuestas

1 A

Quién tiene las claves privadas

Quien tiene las claves privadas controla las monedas. La custodia es simplemente la pregunta de quién es esa persona.

2 B

Un derecho frente al exchange, anotado en su base de datos

El exchange tiene las claves de direcciones compartidas. Tu saldo es su registro de cuánto te debe.

3 C

Solo el fundador controlaba las carteras, y estaban casi vacías cuando murió

Con una sola persona controlando las claves y los fondos mal utilizados, tras su muerte no hubo forma de recuperar la mayor parte del dinero.

4 D

El riesgo de que un exchange congele o pierda tus monedas

Con tus propias claves, ninguna empresa puede congelar, prestar o perder tus monedas. Los riesgos que quedan son tus propios errores y las estafas.

5 B

Fondos de trading en un exchange de confianza y ahorros a largo plazo en tu propia cartera

El trading necesita fondos en el exchange, mientras que los ahorros están más a salvo del riesgo de la empresa en tu propia cartera. Cada lado hace lo que mejor sabe hacer.

6 C

Todo lo que el exchange debe a clientes y prestamistas

La prueba de reservas muestra activos en un momento dado. Sin una visión completa de las deudas, no puede demostrar que el exchange pueda pagar a todos.

FUENTES

- The Block, Mt. Gox repartirá los pagos en bitcoin a partir de julio de 2024: https://www.theblock.co/post/301448/mt-gox-to-distribute-9-billion-of-bitcoin-bitcoin-cash-repayments-from-beginning-of-july
- Crowdfund Insider, informe del administrador de QuadrigaCX: 76.000 usuarios perdieron 215 millones: https://www.crowdfundinsider.com/2019/05/147401-quadrigacx-trustees-final-report-finds-not-much-left-for-76-000-exchange-users-who-lost-215-million/
- Wikipedia, quiebra de FTX: https://en.wikipedia.org/wiki/Bankruptcy_of_FTX
- Cointelegraph, hasta cuatro millones de bitcoins podrían haberse perdido para siempre (estimación de Chainalysis): https://cointelegraph.com/news/up-to-four-million-bitcoins-gone-forever

Market Talks

SIGUE APRENDIENDO

A continuación: Lección 11 El recorrido de una transacción

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.