Market Talks

CENTRO DE EDUCACIÓN

BLOCKCHAIN · PRINCIPIANTE · LECCIÓN 1 DE 13

# El problema de la confianza

Por qué cada pago digital necesita un intermediario y por qué se inventó blockchain para cambiarlo

7 min de lectura  6 preguntas con sus respuestas

BLOCKCHAIN · PRINCIPIANTE · LECCIÓN 1 DE 13

# El problema de la confianza

EN UNA FRASE

Hoy en día, cada pago digital depende de un intermediario de confianza que lleva las cuentas. Blockchain es un intento de llevar unas cuentas compartidas en las que nadie tenga que confiar.

## El dinero es un registro, no un objeto

La mayor parte del dinero que tienes no es efectivo guardado en un cajón. Es un número en la base de datos de un banco. Cuando le pagas a alguien desde tu cuenta, no viaja nada físico. Tu banco reduce una anotación en sus registros y el banco del destinatario aumenta otra.

Así que lo que realmente tienes es una *promesa*: la promesa del banco de que sus registros son correctos y de que los respetará cuando se lo pidas. Lo mismo ocurre con el saldo de una tarjeta, las aplicaciones de pago y los fondos depositados en un exchange. En esencia, el dinero digital es un registro que alguien lleva.

## Por qué dependemos de un intermediario

Imagina que le pagas a un vendedor al otro lado del mundo al que nunca has visto. Tú no puedes revisar sus registros y él no puede revisar los tuyos. Ninguno de los dos tiene motivos para confiar en el otro. Un intermediario resuelve esto haciendo tres trabajos a la vez:

- **Llevar el registro oficial** de quién es dueño de qué.
- **Verificar cada pago**, por ejemplo que realmente tienes los fondos que envías.
- **Resolver desacuerdos**, incluida la anulación de errores y fraudes.

Los bancos, las redes de tarjetas, las aplicaciones de pago y los exchanges cumplen este papel. La mayoría de las veces el sistema funciona bien, y precisamente por eso domina el mundo financiero.

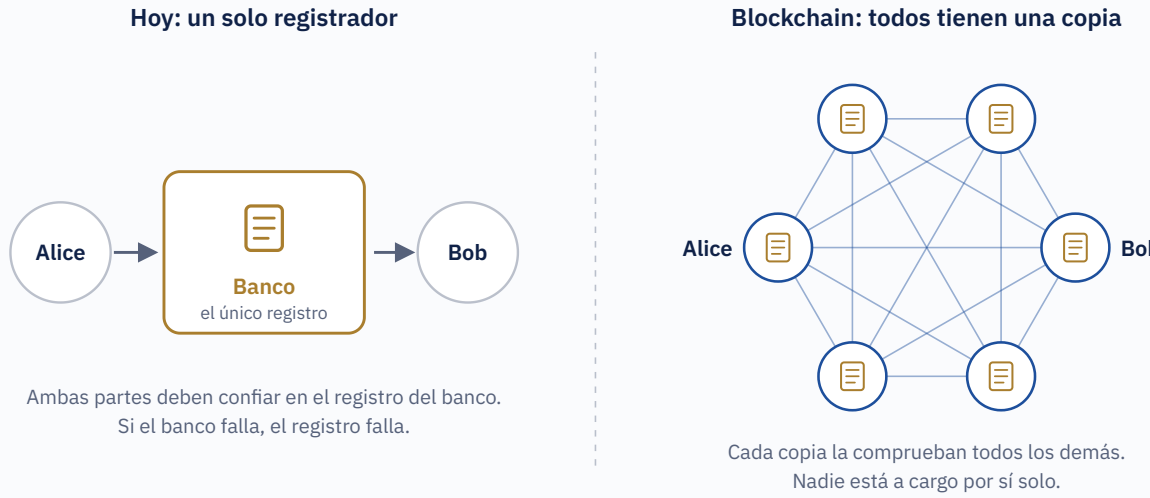



Figura 1. Con un intermediario, una sola parte tiene el único registro. Con una blockchain, cada participante guarda y verifica una copia idéntica.

## El coste oculto de confiar en alguien

Depender de un intermediario es cómodo, pero nunca es gratis. Los costes aparecen de cuatro formas:

- **Comisiones y demoras.** Una transferencia internacional puede pasar por una cadena de bancos, y cada uno añade tiempo y cargos. Según el Banco Mundial, enviar 200 dólares al extranjero costaba de media un 6,49% a principios de 2025, más del doble del objetivo mundial del 3%.
- **Control del acceso.** Un intermediario puede congelar, cerrar o negarte una cuenta. Según el Banco Mundial, más de mil millones de adultos en el mundo siguen sin tener ninguna cuenta bancaria.
- **Un único punto de fallo.** Si el intermediario sufre un hackeo, deja de funcionar o quiebra, todos los que dependían de él se ven afectados a la vez.
- **Registros que no puedes comprobar.** Ves el saldo que el intermediario decide mostrarte. No puedes auditar sus libros por tu cuenta.

Nada de esto significa que los bancos sean malos. Significa que la confianza tiene un precio, y lo pagas lo notes o no.

UN EJEMPLO REAL

En noviembre de 2022, el exchange de criptomonedas FTX colapsó y se declaró en quiebra. Los clientes que creían tener bitcoin y dólares en la plataforma descubrieron que en realidad solo tenían un derecho de cobro frente a una empresa en quiebra. Sus fondos quedaron congelados durante años mientras se resolvía el proceso.

# ¿Por qué no crear simplemente dinero digital? El problema del doble gasto

Lo digital se copia a la perfección. Cuando envías una foto a un amigo por correo electrónico, no pierdes la foto. Ahora la tienen los dos. Eso no es problema con una foto, pero es un desastre con el dinero. Si el dinero fuera solo un archivo, podrías enviar el mismo archivo a cien personas distintas y pagarles a todas con él.

Una moneda física no puede estar en dos bolsillos a la vez. El dinero digital sí puede, a menos que algo lo impida. Esto se llama **el problema del doble gasto**, y es el desafío central del dinero digital.

Hasta 2008, la única solución fiable era un registrador central que decidiera qué pago había llegado primero y rechazara la copia. Por eso, todo intento de crear efectivo digital seguía necesitando un intermediario, y cuando ese intermediario fallaba o era clausurado, el dinero desaparecía con él. Veremos esos primeros intentos en la Lección 3.

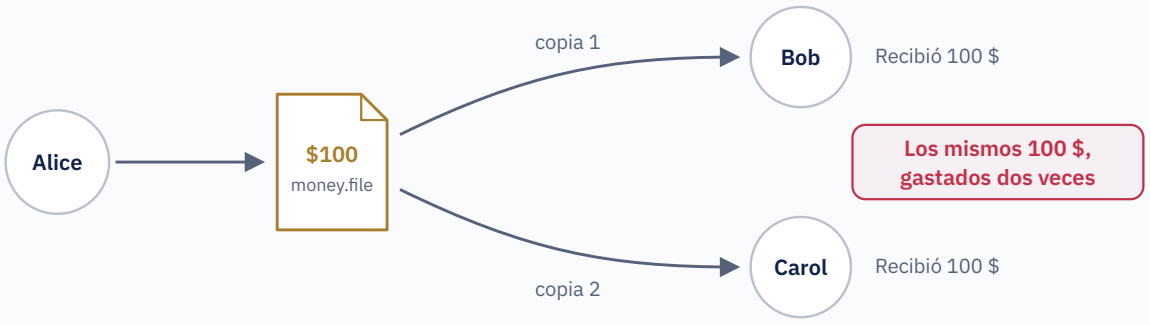



Figura 2. Un archivo digital se puede copiar, así que sin una protección el mismo dinero podría enviarse a dos personas a la vez.

# La pregunta que blockchain vino a responder

Si juntamos todo lo anterior, llegamos a una sola pregunta:

> ¿Puede un grupo de desconocidos que no confían entre sí mantener un único registro compartido que todos acepten, sin que nadie esté a cargo?

Ese es el problema que blockchain fue diseñado para resolver. En 2008 se publicó un artículo firmado con el nombre de Satoshi Nakamoto que proponía una solución, y unos meses después Bitcoin se puso en marcha. Contamos esa historia en la Lección 4.

La idea central, en pocas palabras:

- En lugar de un registro en manos de un único guardián, existen **muchas copias idénticas** en manos de cualquiera que quiera tener una.
- Cada nueva anotación es **verificada por todos** según las mismas reglas públicas.
- Cambiar anotaciones pasadas resulta **extremadamente caro**, así que se puede confiar en el historial.

La confianza pasa de una institución a las reglas, las matemáticas y la verificación abierta. La comunidad cripto lo resume en una frase: *no confíes, verifica*.

**ANALOGÍA: LA HOJA DE CÁLCULO COMPARTIDA**

Piensa en una hoja de cálculo en línea alojada por una sola empresa. La empresa puede bloquearte el acceso, editar filas o perder el archivo. Ahora imagina otra hoja de cálculo: todos tienen una copia completa, una fila nueva solo se añade cuando todo el grupo confirma que cumple las reglas, y las filas antiguas quedan selladas y ya no se pueden editar. Nadie es su dueño y cualquiera puede comprobarla. Esa segunda hoja de cálculo es la idea básica de una blockchain.

## Lo que blockchain no elimina

Es importante ser honestos con los límites desde el principio. Una blockchain elimina la necesidad de confiar en *un único registrador*, pero no elimina la confianza por completo. Sigues dependiendo de que el software funcione correctamente, de tu propio cuidado al proteger tus claves y, a menudo, de nuevos intermediarios como los exchanges y las aplicaciones de billetera.

También desaparecen las redes de seguridad. Normalmente no hay un servicio de atención al cliente que pueda revertir un pago enviado por error. En el resto de este curso verás en detalle las dos caras de estas compensaciones.

## Por qué esto importa a los traders

- **El riesgo de contraparte está en todas partes.** Cuando tus fondos están en un exchange o con un bróker, tienes la promesa de esa empresa, no el activo en sí. El colapso de FTX mostró lo que esa diferencia significa en la práctica.
- **La liquidación funciona de otra manera.** Las operaciones con acciones en Estados Unidos se liquidan un día hábil después de la operación (T+1, desde mayo de 2024) y solo en días hábiles. Una transferencia de bitcoin se liquida según las propias reglas de la red, a cualquier hora, incluidos los fines de semana.
- **La confianza da forma a las narrativas del mercado.** Bitcoin nació tras la crisis bancaria de 2008. Cuando varios bancos regionales de Estados Unidos quebraron en marzo de 2023, bitcoin subió con fuerza en las semanas siguientes, y muchos comentaristas del mercado relacionaron ese movimiento con las nuevas dudas sobre los bancos. Entender el problema de la confianza te ayuda a entender por qué historias como estas mueven los precios.

## Términos clave

| | |
|---|---|
| **Intermediario** | Un tercero, como un banco o un exchange, que lleva los registros y procesa los pagos entre dos partes. |
| **Libro mayor (ledger)** | Un registro de transacciones y saldos. Una blockchain es un tipo especial de libro mayor. |
| **Riesgo de contraparte** | El riesgo de que la otra parte de un acuerdo no cumpla con lo que le corresponde. |
| **Doble gasto** | Gastar el mismo dinero digital más de una vez. Evitarlo es el desafío central del efectivo digital. |
| **Liquidación** | El momento en que un pago u operación se completa y el cambio de propiedad es definitivo. |
| **Sin confianza (trustless)** | Un sistema en el que no necesitas confiar en ninguna parte concreta, porque cualquiera puede comprobar las reglas. No significa que no haga falta ninguna confianza. |

## Ideas clave

1. El dinero digital es un registro, y hoy un intermediario lleva ese registro por nosotros.

2. Los intermediarios aportan comodidad, pero también comisiones, demoras, control del acceso y un único punto de fallo.
3. Como los archivos digitales se copian a la perfección, el dinero digital se enfrenta al problema del doble gasto.
4. Antes de 2008, solo un registrador central podía evitar el doble gasto.
5. Blockchain permite que muchas partes independientes mantengan un único registro compartido que cualquiera puede verificar, sin que nadie esté a cargo.

## 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. Cuando le pagas a alguien desde tu cuenta bancaria, ¿qué ocurre en realidad?**

- A Se traslada efectivo entre las cámaras acorazadas de los bancos
- B El banco actualiza las anotaciones de sus registros
- C Se envía al destinatario un archivo de moneda digital
- D El banco central imprime dinero nuevo para el destinatario

**2. ¿Qué es el problema del doble gasto?**

- A Pagar dos comisiones por una sola transacción
- B Que te cobren dos veces por error
- C Gastar el mismo dinero digital más de una vez, porque los archivos digitales se pueden copiar
- D Enviar dinero a dos bancos al mismo tiempo

**3. Antes de 2008, ¿cómo solían evitar el doble gasto los sistemas de pago digitales?**

- A Dependiendo de una autoridad central que llevaba el registro oficial
- B Limitando los pagos a cantidades pequeñas
- C Usando monedas físicas junto con las digitales
- D No podían evitarlo en absoluto

**4. ¿Cuál de estos NO es un coste de depender de un intermediario?**

A Comisiones y demoras
B El riesgo de que te congelen la cuenta
C Un único punto de fallo
D Pagos que nunca se pueden revertir

**5. Si guardas fondos en un exchange, ¿qué tienes en realidad?**

A Los propios activos, registrados a tu nombre en la blockchain
B Un derecho de cobro frente al exchange, que depende de que siga siendo solvente
C Un seguro que garantiza la devolución total
D Una copia de las claves privadas del exchange

**6. En blockchain, ¿qué significa «sin confianza» (trustless)?**

A Nadie confía en nadie, así que nada funciona
B No hace falta ningún tipo de confianza
C No necesitas confiar en ninguna parte concreta, porque cualquiera puede comprobar las reglas y los registros
D Solo los miembros de confianza pueden unirse a la red

# Respuestas

1 B

**El banco actualiza las anotaciones de sus registros**

No se mueve nada físico. El banco reduce tu saldo y aumenta el del destinatario en sus registros. Tu dinero es en realidad el registro del banco y su promesa de respetarlo.

2 C

**Gastar el mismo dinero digital más de una vez, porque los archivos digitales se pueden copiar**

Los archivos digitales se copian a la perfección, así que sin una protección el mismo dinero digital podría enviarse a muchas personas. Evitarlo es el desafío central del efectivo digital.

3 A

**Dependiendo de una autoridad central que llevaba el registro oficial**

Un registrador central decidía qué pago había llegado primero y rechazaba las copias. Funcionaba, pero significaba que todos los sistemas dependían de un intermediario.

4 D

**Pagos que nunca se pueden revertir**

Los intermediarios normalmente pueden revertir errores y fraudes. Los pagos irreversibles son una característica, y también un riesgo, de las blockchains, no de los intermediarios tradicionales.

5 B

**Un derecho de cobro frente al exchange, que depende de que siga siendo solvente**

Tienes la promesa del exchange. Si el exchange quiebra, como FTX en 2022, esa promesa puede quedar congelada o perderse. Eso es el riesgo de contraparte.

6 C

**No necesitas confiar en ninguna parte concreta, porque cualquiera puede comprobar las reglas y los registros**

Significa que no tienes que fiarte de la palabra de una sola institución. Queda algo de confianza, por ejemplo en el software y en la forma en que tú mismo gestionas tus claves.

FUENTES


- Banco Mundial, Remittance Prices Worldwide, informe del primer trimestre de 2025: https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q125_1_0.pdf

Market Talks

SIGUE APRENDIENDO

# A continuación: Lección 2 Centralizado, distribuido, descentralizado

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.