Market Talks
CENTRO DE EDUCACIÓN

CRIPTO · PRINCIPIANTE · LECCIÓN 14 DE 15

Estafas, rug pulls e indicios de alarma

Cómo funcionan las estafas cripto más comunes, desde los rug pulls y los pump and dumps hasta las plataformas de inversión falsas, los suplantadores y los vaciadores de carteras, y los indicios de alarma que comparten

11 min de lectura 8 preguntas con sus respuestas

CRIPTO · PRINCIPIANTE · LECCIÓN 14 DE 15

Estafas, rug pulls e indicios de alarma

EN UNA FRASE

Las estafas cripto se llevan miles de millones de dólares cada año. La mayoría sigue un número reducido de patrones, y cuando se reconocen esos patrones, los indicios de alarma son mucho más fáciles de ver.

Por qué las estafas ocupan tanto espacio en cripto

Las transacciones cripto son rápidas, globales e irreversibles. No hay un banco al que llamar para pedir un reembolso, ni una oficina central que pueda congelar un pago que ya ha salido de tu cartera. Las mismas características que hacen útiles las criptomonedas las hacen también atractivas para los estafadores.

Las cifras son grandes. La empresa de análisis blockchain Chainalysis estimó que las estafas cripto se llevaron **más de 17.000 millones de dólares** en 2025, un récord. Solo en Estados Unidos, el Centro de Denuncias de Delitos en Internet del FBI (IC3) recibió en 2025 denuncias relacionadas con cripto con pérdidas declaradas de unos **11.400 millones de dólares**, un 22% más que el año anterior. Unos 7.200 millones de dólares de esa cifra procedían de esquemas de inversión falsos.

Las estafas también son cada vez más profesionales. Chainalysis observó que las estafas de suplantación crecieron más de un 1.400% en 2025, y que la cantidad media obtenida por pago pasó de unos 782 $ a unos 2.764 $. Muchas organizaciones usan ya IA para redactar mensajes, traducir conversaciones y crear vídeos falsos.



Figura 1. Las estafas cripto alcanzaron niveles récord en 2025. Las cifras son estimaciones de Chainalysis y denuncias presentadas al FBI.

Rug pulls y honeypots

Un **rug pull** ocurre cuando quienes están detrás de un token o un proyecto se llevan de repente el dinero y desaparecen: literalmente, «tiran de la alfombra» bajo los pies de los compradores. Es más común con tokens nuevos en exchanges descentralizados, donde cualquiera puede crear un token y un pool de negociación en minutos (Lecciones 7 y 9).

Entre las variantes habituales están:

- **Retirada de liquidez:** los creadores retiran los fondos del pool de negociación. Sin nada contra lo que operar, el precio del token se desploma casi a cero.
- **Venta masiva del equipo:** los creadores tienen una gran parte de la oferta y la venden toda de golpe en el mercado.
- **Honeypot (trampa de miel):** el contrato inteligente del token está escrito para que se pueda comprar pero no vender. El gráfico del precio solo sube, porque nadie salvo los creadores puede vender.

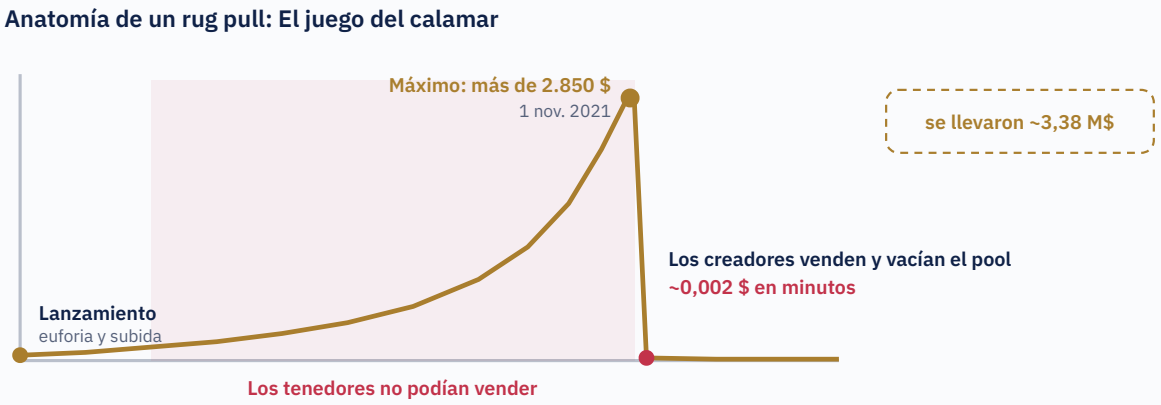


Figura 2. Una visión simplificada del rug pull del token de El juego del calamar. Los tenedores no podían vender mientras el precio subía; después, los creadores vaciaron el pool.

EJEMPLO: EL TOKEN DE EL JUEGO DEL CALAMAR, 2021

A finales de 2021 apareció en PancakeSwap, un exchange descentralizado, un token no oficial con el nombre de la popular serie de televisión El juego del calamar (Squid Game). Su precio se disparó decenas de miles por ciento en pocos días y superó los **2.850 $** el 1 de noviembre de 2021. Los compradores pronto descubrieron que no podían venderlo. Después, los creadores vendieron sus tenencias y vaciaron el pool, y en cuestión de minutos el precio cayó a unos **0,002 $**. Los creadores se llevaron aproximadamente 3,38 millones de dólares. Los responsables de la serie no tenían nada que ver.

Pump and dump

En un **pump and dump** (inflar y vender), un grupo compra discretamente una moneda pequeña y con poca negociación, y luego la promociona a bombo y platillo mediante publicaciones en redes sociales, influencers de pago o grupos de chat. A medida que entran nuevos compradores, el precio se dispara. Los organizadores venden entonces («dump») sus monedas a esos compradores tardíos, y el precio vuelve a caer, a menudo por debajo de donde empezó.

Los pump and dumps funcionan porque las monedas pequeñas tienen muy poca liquidez (Lección 8), así que una cantidad modesta de compras puede mover mucho el precio. Un aluvión repentino de publicaciones que dicen todas lo mismo sobre una moneda desconocida, a menudo con cuentas atrás y objetivos de precio, es un rasgo típico.

Plataformas de inversión falsas y la «matanza del cerdo»

La mayor categoría de pérdidas procede de los esquemas de inversión falsos. Una forma muy conocida se llama **matanza del cerdo** (pig butchering), traducción de una expresión china que usan los propios estafadores: «engordan» a la víctima con confianza antes de «sacrificarla».

Normalmente empieza con un mensaje de apariencia inofensiva: un SMS a un «número equivocado», una coincidencia en una aplicación de citas o un contacto nuevo en redes sociales. Durante semanas, el estafador construye una amistad o un romance. Al final menciona que gana buen dinero operando con cripto y se ofrece a enseñar cómo lo hace.

A la víctima se la guía hasta un sitio web o una aplicación de trading que parece profesional pero es falsa. El saldo en pantalla crece rápido, e incluso pueden funcionar pequeñas retiradas al principio, lo que genera confianza. Los depósitos aumentan. Cuando la víctima intenta sacar una cantidad grande, la plataforma exige de repente pagar antes un «impuesto», una «comisión» o un «depósito de desbloqueo». Una vez pagado, la plataforma y el amigo desaparecen.



Figura 3. Las etapas típicas de una estafa de matanza del cerdo. La confianza se construye despacio, y las pérdidas llegan al final.

EJEMPLO: CÓMO SE VE DESDE DENTRO

Laura recibe un mensaje de Michael: «Hola, David, ¿sigue en pie el golf del sábado?». Ella le responde que se ha equivocado de número. Michael se disculpa y empiezan a charlar. Seis semanas después, él le enseña capturas de sus ganancias en trading y la ayuda a abrir una cuenta en una plataforma que usa. Sus primeros 1.000 $ crecen hasta 1.600 $ en pantalla, y una retirada de 200 $ llega a su cartera. Deposita 25.000 $. Cuando pide retirar, el soporte le dice que primero debe pagar un «impuesto» del 20% sobre sus ganancias. Las cifras de la pantalla nunca fueron reales.

Suplantadores, falso soporte y estafas de recuperación

Muchas estafas funcionan haciéndose pasar por alguien de confianza:

- **Falso soporte:** después de publicar una pregunta en un foro público o un grupo de chat, alguien envía un mensaje privado diciendo ser del equipo de soporte del exchange o de la cartera. Los equipos de soporte reales no inician chats privados y nunca piden una frase semilla ni una contraseña.
- **Falso contacto del exchange o del gobierno:** una llamada, un correo o un SMS dice que tu cuenta está en peligro y que hay que mover los fondos de inmediato a una cartera «segura».
- **Famosos falsos y regalos:** un vídeo o una publicación muestra a una persona famosa que promete devolver el doble de cualquier cantidad de cripto que se le envíe. Los vídeos deepfake generados con IA hacen ahora que parezcan convincentes. Ningún regalo real funciona así.
- **Estafas de recuperación:** cuando alguien pierde dinero, un «experto en recuperación» o un falso bufete de abogados se ofrece a recuperarlo a cambio de una comisión por adelantado. Van dirigidas a personas que ya han sido estafadas una vez.

Vaciadores de carteras, aprobaciones y airdrops falsos

Algunas estafas no necesitan que envíes nada. En su lugar, te engañan para que des a un contrato inteligente malicioso permiso para mover tus tokens.

Cuando se usa una aplicación DeFi, la cartera a menudo pide **aprobar** que un contrato gaste un token concreto en tu nombre (Lección 12). Un sitio web falso, a menudo promocionado como un **airdrop** gratuito, un mint o el cobro de una recompensa, pide conectar la cartera y firmar. Lo que se firma en realidad es una aprobación, a veces por una cantidad ilimitada, que permite al contrato del estafador llevarse los tokens. Este tipo de herramienta se llama **vaciador de carteras** (wallet drainer).

Otros trucos habituales son las aplicaciones de cartera y extensiones de navegador falsas que roban la frase semilla mientras se escribe, las direcciones web que imitan a las reales y el

envenenamiento de direcciones (Lección 10). Quien tiene tu **frase semilla** tiene el control total de tu cartera, como se vio en la Lección 9 de Blockchain. Las aprobaciones antiguas siguen activas hasta que se eliminan, y herramientas como Revoke.cash y algunos exploradores de bloques muestran qué aprobaciones ha dado una cartera.



Figura 4. Un vaciador de carteras no pide que se le envíen fondos. Pide firmar un permiso que le deja llevárselos.

Los indicios de alarma que comparten casi todas las estafas

Las historias cambian, pero los indicios de alarma se repiten:

- **Rentabilidades garantizadas o muy altas**, como «un 2% al día» o «sin riesgo».
- **Urgencia y presión:** hay que actuar ya, la oferta termina esta noche, la cuenta se va a cerrar.
- **Peticiones de la frase semilla o la clave privada**, por cualquier motivo.
- **Contactos no solicitados** que poco a poco derivan hacia la inversión.
- **Una plataforma poco conocida**, recomendada por un nuevo amigo de internet, o una aplicación que no se ha obtenido por canales oficiales.
- **Retiradas que exigen pagar antes una comisión.**
- **«Envía cripto y recibe el doble».**
- **Tokens que no se pueden vender**, un equipo anónimo que tiene la mayor parte de la oferta o una liquidez sin bloquear.

Un solo indicio de alarma no demuestra que haya una estafa, pero varios juntos son una advertencia seria.



Figura 5. Indicios de alarma habituales que comparten casi todas las estafas cripto.

Qué ocurre después de una estafa

Como las transferencias en blockchain son definitivas, el dinero enviado a un estafador muy rara vez se recupera. A veces, si los fondos llegan rápido a un exchange regulado, ese exchange puede congelarlos, y emisores de stablecoins como Tether y Circle han congelado fondos robados en algunos casos.

Entre los pasos que describen autoridades como el FBI están denunciar la estafa a la policía y, en EE. UU., al IC3; informar al exchange o a la plataforma que se usó; conservar registros como los hashes de las transacciones, las direcciones de cartera, los mensajes y los enlaces a sitios web; y eliminar las aprobaciones de cartera que se hayan dado. Muchas personas también trasladan los fondos restantes a una cartera nueva con una frase semilla nueva si creen que la antigua ha quedado expuesta.

Las autoridades advierten además de que quienes denuncian una pérdida suelen recibir después el contacto de estafadores de recuperación, de modo que a la primera pérdida puede seguirle una segunda.

Por qué esto importa a los traders

- **Las ganancias rápidas atraen estafas.** Los tokens nuevos con enormes subidas diarias son justo donde se producen los rug pulls, los honeypots y los pump and dumps. Comprobar si un token se puede vender, quién tiene la oferta y si la liquidez está bloqueada forma parte de la investigación básica que hacen muchos traders.
- **Ofertas de «copia mis operaciones».** Los grupos que prometen consejos de trading privados o gestión de cuentas a cambio de depósitos son una vía de entrada habitual a las plataformas falsas.
- **Las aprobaciones se acumulan.** Los usuarios activos de DeFi pueden acumular con el tiempo muchas aprobaciones de tokens antiguas. Cada una es un riesgo posible si el contrato llega a verse comprometido.
- **Los mismos hábitos de seguridad protegen las cuentas de trading.** Las cuentas de los exchanges también son un objetivo: los correos de phishing, las páginas de inicio de sesión falsas y los duplicados de SIM (SIM swap) buscan tomar el control de las cuentas y retirar los fondos. La Lección 15 trata las protecciones básicas que ofrecen los exchanges.

Términos clave

Rug pull	Cuando los creadores de un proyecto se llevan de repente el dinero, por ejemplo retirando la liquidez o vendiendo de golpe sus tokens, y dejan el token casi sin valor.
Honeypot	Un token cuyo contrato inteligente permite comprar pero bloquea la venta a todos salvo a los creadores.
Pump and dump	Un esquema en el que los organizadores compran una moneda pequeña, la promocionan para hacer subir el precio y luego venden a los compradores tardíos.
Matanza del cerdo (pig butchering)	Una estafa larga en la que el estafador se gana la confianza de la víctima durante semanas y luego la lleva a depositar grandes sumas en una plataforma de inversión falsa.
Phishing	Mensajes, correos o sitios web falsos que imitan un servicio real para engañar a la gente y que entregue contraseñas, códigos o frases semilla.
Vaciador de carteras (wallet drainer)	Código malicioso en un sitio web falso que engaña a los usuarios para que firmen aprobaciones o transacciones que envían sus tokens al estafador.

Aprobación de token	Un permiso firmado que deja a un contrato inteligente gastar un token concreto de tu cartera, hasta una cantidad fijada o sin límite.
Deepfake	Un vídeo o audio falso, normalmente hecho con IA, que muestra a una persona real diciendo algo que nunca dijo.
Estafa de recuperación	Una estafa posterior dirigida a personas que ya han perdido dinero, con la promesa de recuperarlo a cambio de una comisión por adelantado.

Ideas clave

1. Los pagos cripto son rápidos y definitivos, lo que los hace atractivos para los estafadores. Chainalysis estimó más de 17.000 millones de dólares en pérdidas por estafas en 2025.
2. Los rug pulls, los honeypots y los pump and dumps son más comunes con tokens nuevos y pequeños. El token de El juego del calamar cayó de más de 2.850 $ a casi cero en minutos.
3. Las plataformas de inversión falsas, a las que a menudo se llega a través de una larga amistad en internet, causan las mayores pérdidas. Los saldos falsos y las pequeñas retiradas iniciales generan confianza.
4. Los suplantadores se hacen pasar por personal de soporte, exchanges, funcionarios y famosos. El soporte real nunca pide una frase semilla.
5. Los vaciadores de carteras usan aprobaciones firmadas en lugar de pedir que se envíen fondos. Las aprobaciones antiguas siguen activas hasta que se eliminan.
6. Las rentabilidades garantizadas, la urgencia, las peticiones de la frase semilla y las comisiones para retirar son los indicios de alarma más comunes.

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. ¿Por qué los pagos cripto atraen a los estafadores?

- A) Siempre son anónimos e invisibles
- B) Son rápidos, globales e irreversibles
- C) Los exchanges garantizan los beneficios de los estafadores
- D) Solo se pueden enviar de noche

2. ¿Qué es un token honeypot?

A Un token respaldado por miel real
B Un token que paga altas recompensas de staking
C Un token cuyo contrato permite comprar pero no vender
D Una stablecoin vinculada al oro

3. ¿Qué pasó con el token de El juego del calamar en noviembre de 2021?

A Se listó en todos los grandes exchanges
B Sus creadores vaciaron el pool y el precio cayó de más de 2.850 $ a unos 0,002 $
C Los responsables de la serie compraron toda la oferta
D Se convirtió en una stablecoin

4. En un pump and dump, ¿quién suele perder dinero?

A Los organizadores que compraron primero
B Los compradores tardíos que entraron por la euforia
C Los validadores de la blockchain
D Nadie, no tiene riesgo

5. En una estafa de matanza del cerdo, ¿por qué suelen funcionar las pequeñas retiradas iniciales?

A Porque la plataforma es real
B Para generar confianza antes de depósitos mayores
C Por las reglas de la blockchain
D Porque el banco lo impone

6. Alguien dice en un mensaje privado que es del equipo de soporte de tu cartera y pide tu frase semilla para arreglar un problema. ¿Qué es esto?

A Un procedimiento normal de soporte
B Un control de seguridad obligatorio
C Una estafa de suplantación típica
D Una actualización de software

7. ¿Cómo se lleva normalmente los tokens un vaciador de carteras?

A Adivinando tu contraseña
B Haciendo que firmes una aprobación o una transacción en un sitio falso
C Hackeando toda la blockchain
D Cambiando el precio del token

8. ¿Cuál de estos es un indicio de alarma habitual de una estafa?

A Una plataforma que pide una comisión antes de poder retirar
B Poder vender un token en cualquier momento
C Un exchange muy conocido con auditorías públicas
D Un precio que sube y baja

Respuestas

1 B

Son rápidos, globales e irreversibles

Una vez confirmada, una transferencia no la puede revertir un banco ni una empresa de pagos, y los fondos pueden cruzar fronteras en minutos.

2 C

Un token cuyo contrato permite comprar pero no vender

El contrato bloquea la venta a los tenedores normales, así que el precio solo parece subir hasta que los creadores cobran.

3 B

Sus creadores vaciaron el pool y el precio cayó de más de 2.850 $ a unos 0,002 $

Los compradores no podían vender; después los creadores vendieron y se llevaron la liquidez, y el precio se hundió en minutos.

4 B

Los compradores tardíos que entraron por la euforia

Los organizadores compran pronto y venden a quienes llegan después de la promoción, que se quedan con una moneda en caída.

5 B

Para generar confianza antes de depósitos mayores

Dejar salir una cantidad pequeña hace que la plataforma falsa parezca real, así que la víctima se siente segura para depositar mucho más.

6 C

Una estafa de suplantación típica

Quien tiene tu frase semilla controla tu cartera. Los equipos de soporte reales nunca la piden.

7 B

Haciendo que firmes una aprobación o una transacción en un sitio falso

El usuario firma un permiso, a menudo presentado como el cobro de un airdrop, que permite al contrato del estafador mover los tokens.

8 A

Una plataforma que pide una comisión antes de poder retirar

Exigir un impuesto, una comisión o un depósito antes de liberar una retirada es un rasgo clásico de una plataforma falsa.

FUENTES

- Decrypt, la IA y la suplantación llevaron las pérdidas por estafas cripto a un récord de 17.000 millones de dólares en 2025 (Chainalysis): https://decrypt.co/354624/ai-impersonation-drove-crypto-scam-losses-record-17-billion-2025-chainalysis
- Yahoo Finance, el FBI informa de un aumento del 22% en las pérdidas por fraude cripto en 2025: https://finance.yahoo.com/markets/crypto/articles/fbi-reports-22-rise-crypto-191510401.html
- Cointelegraph, se hunde la estafa cripto inspirada en El juego del calamar: el precio cae de 2.800 $ a cero: https://cointelegraph.com/news/game-over-squid-game-inspired-crypto-scam-collapses-as-price-crashes-from-2-8k-to-

zero

- Cointelegraph, los usuarios no pueden vender el token de El juego del calamar: https://cointelegraph.com/news/users-not-able-to-sell-squid-game-token-clocking-45-000-gains

Market Talks

SIGUE APRENDIENDO

A continuación: Lección 15 Cómo empezar de verdad: exchanges, KYC y carteras

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.