Market Talks
CENTRO DE EDUCACIÓN

BLOCKCHAIN · PRINCIPIANTE · LECCIÓN 9 DE 13

Frases semilla y copias de seguridad

Las 12 o 24 palabras capaces de reconstruir toda tu cartera, cómo guardarlas y quién intentará conseguirlas

6 min de lectura · 6 preguntas con sus respuestas

BLOCKCHAIN · PRINCIPIANTE · LECCIÓN 9 DE 13

Frases semilla y copias de seguridad

EN UNA FRASE

Una frase semilla es una lista de 12 o 24 palabras corrientes que puede recrear todas las claves privadas de tu cartera. Si la conservas, puedes recuperarte de un dispositivo perdido o roto. Si se filtra, cualquiera puede llevárselo todo, sin forma de deshacerlo.

Una copia de seguridad para todas las claves

En la lección 8 vimos que una cartera crea una dirección nueva para cada pago, y que cada dirección sale de su propia clave privada. Hacer copia de decenas de claves sueltas sería una pesadilla. Las carteras modernas lo resuelven generando todas sus claves a partir de un único número inicial, llamado **semilla** (seed).

La semilla se te muestra una sola vez, cuando configuras la cartera, como una lista de 12 o 24 palabras. Es tu **frase semilla**, también llamada frase de recuperación. Introduce esas mismas palabras en casi cualquier aplicación de cartera moderna y recreará exactamente las mismas claves, en el mismo orden, y encontrará las mismas monedas. El móvil o el dispositivo de hardware se pueden perder, te los pueden robar o se pueden romper. Mientras tengas las palabras, tus bitcoins no han desaparecido.



Figura 1. Una frase semilla genera todas las claves privadas de la cartera, y cada clave da una dirección. Restaura la frase en cualquier cartera compatible y vuelven las mismas claves y monedas.

ANALOGÍA: EL NEGATIVO DE LA FOTO

En la época de las cámaras de carrete, el negativo valía más que cualquier copia. Si perdías una foto, podías revelar otra a partir del negativo, tantas veces como quisieras y en cualquier laboratorio. La frase semilla es el negativo de tu cartera. La aplicación de tu móvil es solo una copia. Pero cualquier otra persona que tenga el negativo también puede revelar sus propias copias.

Por qué palabras, y por qué estas palabras

En el fondo, una semilla es solo un número aleatorio muy grande. Anotarlo como 64 caracteres de dígitos y letras invitaría a errores, así que un estándar muy extendido lo convierte en palabras tomadas de una lista fija de 2.048 palabras sencillas en inglés. Cada palabra representa un trozo del número.

La lista se diseñó con cuidado. En la versión inglesa, no hay dos palabras que compartan las cuatro primeras letras, así que un final borroso sigue siendo legible. La última palabra funciona además como comprobación incorporada: si copias mal una palabra, la cartera normalmente te avisará de que la frase no es válida en lugar de abrir en silencio una cartera vacía.

Las palabras las elige la cartera al azar, no tú. Esa es la clave. Una frase de 12 palabras puede ser una de unos 340 sextillones de combinaciones, un número de 39 cifras. Una frase inventada por ti, o la letra de una canción, la adivinarían rápido programas diseñados para probar millones de frases comunes.

Algunas carteras también permiten añadir una contraseña extra opcional, a menudo llamada passphrase. Con ella, las 12 o 24 palabras por sí solas no bastan para abrir la cartera. Añade protección, pero si olvidas esa contraseña, las palabras tampoco te servirán.

Guardarla: sin conexión, duradera y localizable

Una buena copia de seguridad tiene que sobrevivir a tres amenazas: los ladrones, los accidentes como un incendio o el agua, y tu propia memoria dentro de muchos años. Así se comparan las opciones habituales:

Dónde	Protege contra	Vulnerable a
Escrita en papel, en casa	Hackers, porque nunca toca internet	Fuego, agua y cualquiera que la encuentre
Grabada en una placa de metal	Hackers, fuego y agua	Cualquiera que la encuentre, si no está bien escondida
Segunda copia en otro lugar, como una caja de seguridad	Perder la única copia en un solo desastre	Más copias significan más sitios por donde puede filtrarse
Foto, captura, notas, correo o nube	Nada que el papel no resuelva mejor	Cuentas hackeadas, copias sincronizadas y malware que escanea imágenes

Elijas lo que elijas, escribe las palabras en orden, numéralas y compara cada una con la pantalla. Después haz un simulacro de recuperación: con solo una cantidad pequeña en la cartera, bórrala o usa un segundo dispositivo, vuelve a escribir las palabras y confirma que aparecen las mismas direcciones. Encontrar un error ahora sale barato. Encontrarlo en una emergencia, no.

Nadie legítimo te la pedirá jamás

Como la frase semilla lo abre todo, es el objetivo principal de las estafas cripto. Los trucos varían, pero la petición siempre es la misma: escribe tus palabras en algún sitio. Puede llegar como un agente de soporte en tus mensajes, una ventana emergente que dice que tu cartera necesita "sincronizarse" o "validarse", una aplicación de cartera falsa en una tienda de aplicaciones o una web que promete un airdrop gratis.

La regla es sencilla y no tiene excepciones. Tu frase semilla solo se escribe en tu propia cartera, cuando la restauras tú mismo. Ninguna empresa de carteras, exchange, desarrollador ni administrador de canal la necesita nunca.

UN EJEMPLO REAL: LAS CARTERAS DE "REPUESTO" FALSAS

En 2020 se vulneró una base de datos del fabricante de carteras de hardware Ledger, y en diciembre se publicaron en internet los nombres, direcciones postales y teléfonos de unos 272.000 clientes. Meses después, algunos clientes recibieron un paquete con un embalaje que parecía el auténtico de Ledger y una carta que decía que su dispositivo no era seguro y que incluían uno de "repuesto". Las instrucciones les pedían introducir su frase de recuperación. El dispositivo estaba manipulado, y las palabras iban directamente a los ladrones.

Por qué importa a los traders

- **Los chats de trading son terreno de caza.** Los estafadores entran en grupos cripto con mucha actividad, copian los nombres y fotos de los administradores y escriben por privado ofreciendo ayuda o una "revisión de la cartera". MARKET TALKS nunca te pedirá tu frase semilla, tus claves privadas ni tus contraseñas, y tampoco lo hará ningún equipo real.
- **Tu cuenta de exchange tiene sus propios secretos parecidos a una semilla.** Las cuentas de exchange no usan frases semilla, pero los códigos de respaldo de tu autenticación en dos pasos cumplen un papel parecido. Si alguien los consigue junto con tu contraseña, puede hacerse con la cuenta. Guárdalos sin conexión, igual que una frase semilla.
- **Piensa en quienes vendrán después.** Los investigadores calculan que millones de bitcoins ya se han perdido para siempre, muchos porque la única persona que conocía las claves murió o las olvidó. Si tienes cantidades importantes, piensa en cómo una persona de confianza podría recuperarlas algún día, sin dar acceso a nadie hoy.

Términos clave

Semilla	El único número aleatorio grande a partir del cual una cartera genera todas sus claves privadas.
Frase semilla	La semilla escrita como 12 o 24 palabras. Puede recrear todas las claves de la cartera. También se llama frase de recuperación.
Lista de palabras	La lista fija de 2.048 palabras de la que salen las frases semilla, para que cualquier cartera compatible pueda leerlas.
Suma de verificación	Una comprobación incorporada, contenida en la última palabra, que ayuda a la cartera a detectar una frase mal copiada.
Passphrase	Una contraseña extra opcional que se añade a la frase semilla. Sin ella, las palabras solas no abren la cartera.
Simulacro de recuperación	Practicar una restauración con tu frase semilla escrita antes de guardar dinero importante en la cartera.

Ideas clave

1. Las carteras modernas generan todas las claves a partir de una semilla, que se te muestra como una frase de 12 o 24 palabras.
2. Con la frase semilla puedes reconstruir tu cartera en un dispositivo nuevo aunque el antiguo se pierda o se rompa.
3. Las palabras salen de una lista fija de 2.048, la cartera las elige al azar y la última sirve de comprobación de errores.
4. Guarda la frase sin conexión y en un soporte duradero, nunca en fotos, notas, correo o la nube, y prueba una recuperación con un saldo pequeño.
5. Quien te pide tu frase semilla intenta robarte. Solo se escribe en tu 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 puede hacer una frase semilla?

- A Restablecer la contraseña de tu exchange
- B Recrear todas las claves privadas de tu cartera
- C Acelerar tus transacciones
- D Cancelar un pago ya enviado

2. Te roban el móvil con tu aplicación de cartera. Tienes la frase semilla escrita. ¿Qué debes hacer?

- A Restaurar la cartera con la frase semilla en otro dispositivo
- B Contactar con el soporte de Bitcoin
- C Dar las monedas por perdidas
- D Pedir al exchange que revierta el robo

3. ¿Por qué no deberías inventarte tu frase semilla a partir de tu cita favorita?

A Las carteras no pueden leer frases
B Haría las transacciones más lentas
C Los programas adivinan fácilmente las frases que inventa la gente
D Las citas tienen derechos de autor

4. ¿Cuál es la forma más segura de guardar una frase semilla?

A Una captura en tu galería de fotos
B Una nota en los borradores del correo
C Un archivo en tu nube
D Escrita o grabada sin conexión, en un lugar protegido del fuego y del robo

5. ¿Para qué sirve la última palabra de una frase semilla?

A Fija la contraseña de la cartera
B Funciona como comprobación que detecta la mayoría de errores al copiar
C Decide qué moneda guarda la cartera
D Muestra el saldo de la cartera

6. Alguien de un grupo de trading te escribe ofreciéndose a arreglar tu cartera si le das tu frase semilla. ¿Qué está pasando?

A Es una práctica normal de soporte
B La necesita para comprobar tu saldo
C Es una estafa, porque ningún ayudante legítimo necesita tu frase semilla
D Está verificando tu identidad

Respuestas

1 B

Recrear todas las claves privadas de tu cartera

La frase semilla es la forma escrita de la semilla de la que salen todas tus claves. Cualquier cartera compatible puede usarla para reconstruir las mismas claves y encontrar las mismas monedas.

2 A

Restaurar la cartera con la frase semilla en otro dispositivo

Las monedas están en la blockchain, no en el móvil. Restaurar con la frase semilla te devuelve el control, y mover los fondos enseguida a una cartera nueva los protege.

3 C

Los programas adivinan fácilmente las frases que inventa la gente

La seguridad viene de que las palabras se eligen al azar entre un número enorme de combinaciones. Las frases elegidas por personas son mucho más previsibles.

4 D

Escrita o grabada sin conexión, en un lugar protegido del fuego y del robo

Todo lo que se guarda en una cuenta o dispositivo conectado a internet puede alcanzarlo un hacker o un malware. Una copia sin conexión y duradera evita ese riesgo.

5 B

Funciona como comprobación que detecta la mayoría de errores al copiar

Parte de la última palabra se calcula a partir de las demás, así que si una palabra se copia mal, la cartera normalmente dirá que la frase no es válida.

6 C

Es una estafa, porque ningún ayudante legítimo necesita tu frase semilla

Con tu frase semilla se puede vaciar toda la cartera. Los equipos de soporte reales nunca la piden, así que la propia petición demuestra que es una estafa.

FUENTES

- Bitcoin Improvement Proposal 39, código mnemotécnico para generar claves (GitHub): https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki
- BleepingComputer, delincuentes envían dispositivos Ledger manipulados para robar criptomonedas: https://www.bleepingcomputer.com/news/cryptocurrency/criminals-are-mailing-altered-ledger-devices-to-steal-cryptocurrency
- 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 10 Custodia: cuenta en un exchange o tu propia billetera

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.