



JV CRYPTO · CRIPTO SIN HUMO

El curso completo de criptomonedas: desde cero hasta nivel profesional, con datos reales

MÓDULO 08

Wallets y custodia

De tu primera wallet al monedero de hardware: semillas, passphrase, multifirma y herencia

08

NIVEL 1 · BLOQUE 2 · USAR CRIPTO CON SEGURIDAD

Dificultad básica

Javier Ruiz · JV CRYPTO

Edición 2026 · datos a septiembre de 2026 · jvcrypto.es

Contenido formativo. No es asesoramiento financiero. Los criptoactivos pueden hacerte perder todo lo invertido.

En este módulo

Nivel 1 · Bloque 2 · Usar cripto con seguridad | Dificultad básica | Lectura: unos 35 minutos | 6.851 palabras

EN ESTE MÓDULO VAS A APRENDER

- Qué es de verdad una wallet, qué guarda y qué no, y la diferencia entre tener cripto en un exchange y tenerla tú.
- Los tipos de monederos (de móvil, de navegador, de hardware, multifirma, sin frase semilla) y cuál elegir según cuánto tienes.
- Qué es la frase semilla, por qué nadie puede adivinarla, cómo apuntarla, dónde guardarla y cuándo usar una passphrase.
- Cómo montar un monedero de hardware paso a paso y cómo firmar transacciones sin que te vacíen la cuenta.
- Cómo dejar tus criptomonedas preparadas para que tu familia pueda recuperarlas si te pasa algo.

Índice

1. Ocho mil bitcoins en un vertedero	3
2. Qué es de verdad una wallet	3
3. Custodia: en un exchange o en tu propia wallet	4
4. Tipos de monederos	5
5. Elegir y comprar un monedero de hardware	6
6. La frase semilla	7
7. Apuntar y guardar la semilla	8
8. La passphrase: la palabra 25	9
9. Montar un monedero de hardware paso a paso	10
10. Enviar y recibir sin sustos	10
11. Cuánta seguridad según cuánto tienes	11
12. La multifirma, para cantidades grandes	12
13. Firmar sin que te vacíen	12
14. Discreción: la seguridad que no se compra	13
15. Que tu familia pueda recuperar tus criptos	14
16. Ejercicios	15
17. Autoevaluación	16
18. El curso completo	17

01 Ocho mil bitcoins en un vertedero

En el verano de 2013, James Howells, un informático de Newport, en Gales, tiró a la basura un disco duro viejo. Dentro estaba la clave de una wallet con 8.000 bitcoins que había minado en 2009, cuando casi nadie sabía lo que era bitcoin y minar costaba cuatro euros de electricidad. En 2013 esos bitcoins valían unos pocos millones. Cuando Howells se dio cuenta, el disco estaba enterrado bajo miles de toneladas de basura en el vertedero municipal.

Desde entonces ha pedido al ayuntamiento, año tras año, que le deje excavar. Ha ofrecido repartir el dinero con la ciudad, ha presentado planes con excavadoras, robots y expertos en discos duros, y ha acabado en los tribunales. El 9 de enero de 2025, un juez del Tribunal Superior de Inglaterra y Gales desestimó su demanda: según la ley británica, lo que se tira a un vertedero pasa a ser propiedad del ayuntamiento. Ese día, sus 8.000 bitcoins valían más de 600 millones de libras.

La historia de Howells es la cara más conocida de un problema enorme. Las estimaciones más citadas calculan que entre tres y cuatro millones de bitcoins, casi uno de cada cinco, están perdidos para siempre por claves extraviadas, discos formateados, contraseñas olvidadas y dueños que murieron sin decírselo a nadie. En San Francisco, un programador llamado Stefan Thomas tiene 7.002 bitcoins en un pequeño disco cifrado que se borra solo después de diez intentos fallidos de contraseña. Le quedan dos.

Hay otra cara, igual de cara. En diciembre de 2018 murió en la India Gerald Cotten, fundador de QuadrigaCX, entonces el mayor exchange de Canadá. Era, según la empresa, la única persona que tenía las claves de sus wallets. Cuando los investigadores entraron, descubrieron que las wallets estaban casi vacías y que Cotten llevaba años usando el dinero de los clientes. Unos 76.000 clientes perdieron al menos 169 millones de dólares canadienses.

Entre esos dos extremos, perderlo todo por un descuido tuyo o perderlo todo por confiar en otro, está lo que vas a aprender en este módulo.

02 Qué es de verdad una wallet

Lo primero que hay que desmontar es el nombre. Una wallet no guarda criptomonedas. Las criptomonedas no están en tu móvil ni en ningún aparato: son apuntes en la blockchain, visibles para todo el mundo, asociados a unas direcciones. Lo que guarda una wallet son las claves privadas que permiten mover lo que hay en esas direcciones, como viste en el Módulo 02.

Por eso, en cripto, la frase que más se repite es literal: quien tiene las claves tiene el dinero (en inglés, *not your keys, not your coins*). Si alguien consigue tus claves, puede mover tus monedas desde cualquier lugar del mundo sin tocar tu móvil ni tu ordenador. Y si tú pierdes tus claves y no tienes copia, nadie puede devolvértelas, ni un juez, ni un técnico, ni la empresa que fabricó tu monedero.

En tu banco, si alguien entra en tu cuenta y te vacía, hay un sistema detrás: el banco puede anular la transferencia, reclamar al banco de destino o, en último caso, responder él. En cripto no. Las transacciones son definitivas. Casi todas las pérdidas se evitan con unos pocos hábitos, y el problema es que mucha gente los aprende después de perder dinero. Este módulo existe para que tú los aprendas antes.

PALABRAS NUEVAS

- **Wallet o monedero:** la aplicación o el aparato que guarda tus claves privadas y firma las transacciones.
- **Custodia:** quién tiene las claves. Si las tiene un exchange, es custodia de terceros; si las tienes tú, autocustodia.
- **Frase semilla:** las 12 o 24 palabras de las que salen todas tus claves. Es, a todos los efectos, tu dinero.

03 Custodia: en un exchange o en tu propia wallet

Tienes dos formas de tener criptomonedas, y conviene entender bien las dos antes de elegir.

En un exchange

Cuando compras en un exchange, las monedas no están en tu cuenta como están en tu wallet. Lo que ves en la pantalla es un apunte: el exchange te debe esa cantidad y tiene las monedas en sus propias wallets, mezcladas con las del resto de clientes.

Tiene ventajas reales. Si olvidas la contraseña, la recuperas. Si te equivocas, a veces hay un servicio de atención al cliente que te ayuda. Y para comprar, vender u operar no hay otra forma. Pero te expone a riesgos que no dependen de ti. Puede quebrar, como Mt. Gox en 2014 o FTX en 2022, que usaban o perdían el dinero de sus clientes (los verás en el Módulo 11). Puede sufrir un hackeo, como el de Bybit en febrero de 2025, al que le robaron unos 1.500 millones de dólares en un solo ataque. Y puede bloquearte la cuenta por una revisión, una orden judicial o un error, y mientras dure el bloqueo tu dinero no es tuyo.

Además, el dinero en un exchange no está cubierto por el Fondo de Garantía de Depósitos. Si el exchange cae, no hay 100.000 euros protegidos como en un banco. En la Unión Europea, el reglamento MiCA obliga desde 2024 a los exchanges autorizados a guardar los criptoactivos de sus clientes separados de los suyos, de forma que los acreedores del exchange no puedan quedarse con ellos si quiebra. Es una mejora grande respecto a lo que había, pero no te protege de un hackeo ni de un fraude interno, y separar las cuentas no sirve de nada si el dinero ya no está.

En tu propia wallet

Cuando usas tu propia wallet, las monedas están registradas en la blockchain a direcciones que solo tú controlas. Nadie puede congelarlas, nadie puede quebrar con ellas dentro y nadie tiene que devolvértelas, porque nunca las ha tenido. El precio de esa libertad es la responsabilidad: si pierdes la frase semilla, lo pierdes todo, y si firmas algo malicioso, te vacían y no hay a quién reclamar.

Cada vez más gente elige esta opción, sobre todo después de cada quiebra. Mira lo que pasó con los bitcoins guardados en exchanges:

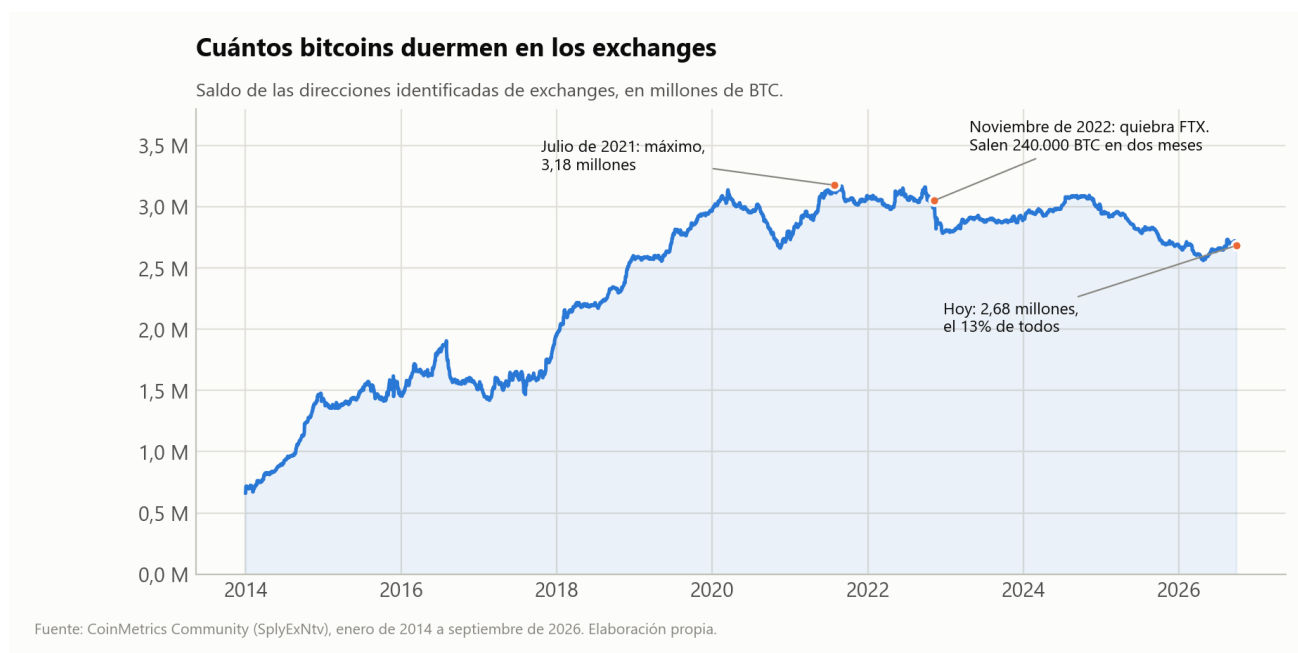


Figura 1. Bitcoins en exchanges desde 2014

Hasta 2021, el saldo de los exchanges no paró de crecer. Desde entonces baja. Solo en los dos meses que siguieron a la quiebra de FTX salieron unos 240.000 bitcoins, y hoy queda en ellos alrededor del 13% de todos los que existen. Una parte ha ido a wallets propias y otra a los fondos cotizados, que tienen sus propios custodios.

Entonces, ¿dónde las guardo?

No es una elección de todo o nada. Lo sensato para casi todo el mundo es combinar. En el exchange, lo que vas a usar pronto para operar o para vender, y cantidades pequeñas, siempre en una plataforma autorizada y con la cuenta bien protegida (lo verás en el Módulo 10). En tu propia wallet, lo que vas a tener durante meses o años. Piensa en el exchange como en la caja registradora de una tienda y en tu wallet como en la caja fuerte: por la caja pasa el dinero, pero nadie deja en ella la recaudación de todo el año.

04 Tipos de monederos

Calientes y fríos

Los monederos se dividen en dos grandes familias según dónde vive la clave privada. En los calientes (*hot wallets*), la clave privada vive en un aparato conectado a internet, como tu móvil o tu ordenador. Son gratis y cómodos, y el riesgo es que ese aparato se infecte con un programa malicioso. En los fríos (*cold wallets*), la clave vive en un aparato que nunca la expone a internet. El más habitual es el monedero de hardware, un aparato del tamaño de un USB que firma las transacciones por dentro. Tu ordenador le pasa la operación, tú la compruebas en la pantalla del propio aparato y pulsas su botón. La clave nunca sale de él.

Tipo	Ejemplos	Para qué	Riesgo principal
Móvil	Trust Wallet, BlueWallet (bitcoin), Rabby	Cantidades pequeñas y uso diario	Móvil infectado, robado o sin copia de la semilla
Extensión del navegador	Rabby, MetaMask	Usar aplicaciones DeFi desde el ordenador	Webs falsas y firmas maliciosas
Hardware	Ledger, Trezor, Coldcard, BitBox02, Keystone	Guardar cantidades relevantes a largo plazo	Comprarlo a quien no debes o perder la semilla
Multifirma	Safe (Ethereum), Sparrow y Nunchuk (bitcoin)	Cantidades grandes, empresas, herencias	La complejidad: un error de configuración
Cuenta de exchange	La del propio exchange	Comprar, vender y operar	Quiebra, hackeo o bloqueo

Los nombres son ejemplos para que te orientes, no recomendaciones, y el mercado cambia deprisa. Lo que importa es el tipo.

Monederos sin frase semilla

Desde 2024 se han popularizado monederos que no te enseñan ninguna frase semilla. Se protegen con tu huella o tu cara, con una *passkey* como las que usas para entrar en algunas webs sin contraseña, o repartiendo la clave entre tu móvil y los servidores de una empresa (una tecnología llamada MPC). En Ethereum, además, la actualización Pectra de 2025 permitió que las cuentas normales funcionen como cuentas inteligentes, con límites de gasto, recuperación por contactos de confianza y otras funciones que antes solo tenían los contratos.

Son cómodos y reducen el riesgo de apuntar mal las palabras, pero cambian el tipo de dependencia. Ahora dependes de tu móvil, de tu cuenta en la nube o de la empresa que da el servicio. Si los usas, entiende exactamente cómo recuperas la cuenta si pierdes el móvil, y hazlo antes de meter dinero en serio. Pregunta qué pasa si la empresa desaparece. Si la respuesta no te convence, ese monedero es para cantidades pequeñas.

05 Elegir y comprar un monedero de hardware

Un monedero de hardware cuesta entre 60 y 250 euros, y para cualquier cantidad que te dolería perder es la mejor inversión que vas a hacer en crypto. Pero hay que comprarlo bien.

En diciembre de 2020 se publicaron en un foro de piratas los datos de 272.853 clientes de Ledger, uno de los mayores fabricantes, con nombres, direcciones postales y teléfonos. Unos meses después, algunos de esos clientes empezaron a recibir en casa un paquete con un Ledger nuevo, precintado, y una carta que decía venir del director de la empresa: por culpa de la filtración, les enviaban un aparato de sustitución y debían pasar su frase semilla al nuevo. El aparato estaba manipulado. Quien siguió las instrucciones perdió todo.

De ahí salen las reglas de compra. Compra en la web oficial del fabricante o en su tienda oficial dentro de un gran comercio electrónico, nunca de segunda mano ni a un particular. Desconfía de cualquier aparato que venga ya configurado o con una tarjeta con 24 palabras impresas: un monedero legítimo genera la semilla delante de ti la primera vez que lo enciendes, y si viene con palabras, quien las imprimió tiene tu dinero. Descarga la aplicación que lo acompaña solo desde la web oficial, escribiendo tú la dirección,

porque hay aplicaciones falsas en tiendas y en anuncios. Y ningún fabricante te pedirá nunca que le envíes, le escribas o le dictes tu frase semilla, ni por carta, ni por correo, ni por teléfono.

CASO REAL

COLDCARD, verano de 2026. El 30 de julio de 2026, en 41 minutos, alguien vació unas 1.200 direcciones de bitcoin que tenían algo en común: sus semillas se habían creado con monederos COLDCARD, uno de los más apreciados por los usuarios de bitcoin más exigentes. En varias oleadas, se llevó en total unos 1.816 BTC, unos 116 millones de dólares, de más de 5.200 direcciones. La causa era un error en la versión del programa del aparato que se publicó en marzo de 2021: por un fallo de configuración, las semillas no usaban el generador de números aleatorios del chip, sino uno de software mucho más predecible, y en algunos modelos se podían adivinar por fuerza bruta. El fabricante detuvo las ventas y publicó una guía para migrar los fondos.

Si creaste una semilla en un COLDCARD entre marzo de 2021 y la corrección de 2026, trátala como comprometida: crea una semilla nueva en un aparato actualizado y mueve allí tus fondos. Y quédate con la lección general, que vale para cualquier marca. Ningún fabricante es infalible, así que mantén actualizado el programa del monedero, sigue los avisos oficiales de tu marca y, si guardas una cantidad importante, valora las capas extra que verás más abajo, como la passphrase o la multifirma, que no dependen de un solo aparato.

Al elegir modelo, mira qué vas a guardar. Para bitcoin solamente hay monederos que solo hacen eso y lo hacen muy bien, con menos código y menos superficie de ataque. Si vas a guardar muchas redes, busca uno que las soporte y que muestre en su pantalla, de forma legible, qué estás firmando. Hay debates largos entre marcas (código abierto frente a cerrado, chips de seguridad, funciones de copia en la nube como la que Ledger anunció en 2023 y que provocó muchas críticas), y te animo a leerlos, pero cualquier monedero de un fabricante conocido, comprado en su web y bien usado, es muchísimo más seguro que dejarlo todo en un exchange o en el móvil.

06 La frase semilla

Qué es exactamente

Cuando creas un monedero, te muestra 12 o 24 palabras en inglés en un orden concreto. Esa es tu frase semilla. De ella salen, siempre en el mismo orden, todas tus claves privadas y todas tus direcciones, en todas las redes que soporte el monedero.

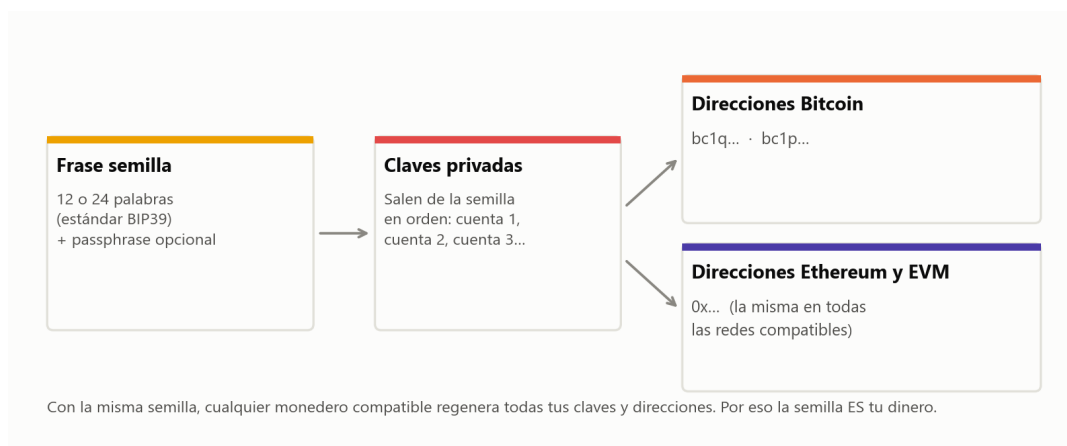


Figura 2. De la semilla salen todas las claves y direcciones

Las palabras salen de una lista estándar de 2.048 (el estándar BIP39), así que puedes restaurar tu semilla en casi cualquier monedero del mundo. Eso es una ventaja enorme, porque no dependes de ninguna marca: si tu Ledger se rompe, puedes recuperar tu dinero en un Trezor o en una aplicación de móvil. Y es también la razón por la que la semilla es tan peligrosa. Quien tenga esas palabras puede llevarse todo desde cualquier lugar, en minutos, sin tocar tu aparato.

Por qué nadie puede adivinarla

Mucha gente pregunta si alguien podría probar combinaciones de palabras hasta dar con la suya. La respuesta es que no, y merece la pena entender por qué. Una frase de 12 palabras representa un número elegido al azar entre unos 340 sextillones de sextillones de posibilidades (2 elevado a 128 , un 34 seguido de 37 ceros). Si todos los ordenadores del mundo probaran miles de millones de combinaciones por segundo desde el origen del universo, no habrían recorrido ni una fracción ridícula. Una de 24 palabras es todavía más grande.

Eso significa que tu semilla solo puede salir de tres sitios: de ti, de donde la guardes o de un aparato o una web que la haya visto. Casi todos los robos de semillas son de esos dos últimos tipos. Por eso importa tanto lo que viene a continuación.

AVISO

Nadie legítimo te pedirá nunca tu frase semilla. Ni el soporte de un exchange, ni el fabricante de tu monedero, ni una web de «verificación», ni un airdrop, ni yo. Si algo o alguien te la pide, es una estafa. Sin excepciones.

07 Apuntar y guardar la semilla

Cómo apuntarla

A mano, en papel, con letra clara y numerando las palabras del 1 al 12 o al 24. Comprueba cada una contra la pantalla del monedero. Nunca en una foto, una captura de pantalla, un documento del ordenador, un correo, una nota del móvil, un chat contigo mismo ni la nube. Todo lo que se sincroniza con internet puede acabar en manos de otros, y hay programas maliciosos que buscan precisamente imágenes con listas de palabras.

Casi todos los monederos te piden que confirmes algunas palabras al terminar. Hazlo con calma. Y después haz una prueba de recuperación con una cantidad pequeña: borra el monedero (o usa otro aparato), restáuralo con la semilla y comprueba que aparecen las mismas direcciones. Mucha gente descubre que había apuntado mal una palabra el día que la necesita, y ese día ya no tiene arreglo.

Dónde guardarla

El papel se moja, se quema y se pierde en una mudanza. Para cantidades que importan, pasa la semilla a una placa de metal (las hay específicas, en las que se graban o se montan letras de acero) que aguante fuego y agua.

Guárdala en un sitio que cumpla tres condiciones: que solo tú, o quien tú decidas, sepa dónde está; que no esté a la vista de visitas ni de quien haga una reforma en casa; y que no se pierda con el aparato. Si guardas el monedero y la semilla en el mismo cajón, un solo robo se lleva las dos cosas. Para cantidades grandes, lo

habitual es tener dos copias en dos lugares distintos, por ejemplo, tu casa y la de una persona de total confianza, para que un incendio o un robo no acaben con todo.

Repartir la semilla en trozos

Hay una tentación frecuente, que es cortar la semilla en dos mitades y guardar cada una en un sitio. No lo hagas así: si alguien encuentra una mitad, le quedan muchas menos combinaciones que probar, y si pierdes una mitad, pierdes todo.

Si quieres repartir, usa un sistema pensado para eso. Algunos monederos permiten crear copias con el método de Shamir, en el que la semilla se divide en varias partes, por ejemplo, tres, y hacen falta dos cualesquiera para recuperarla. Una sola parte no revela nada. Es una buena solución intermedia entre una semilla simple y una multifirma, siempre que entiendas cómo funciona antes de usarla.

ERROR A EVITAR

- Guardar la semilla en una foto o en la nube «porque es más cómodo».
- Escribirla en un documento del ordenador llamado «bitcoin.txt».
- Escribir la semilla en una web o una aplicación que promete «verificar», «sincronizar» o «validar» tu wallet.
- Pegar la clave privada en un bot de Telegram para operar más rápido.
- No hacer nunca una prueba de recuperación y descubrir años después que falta una palabra.
- Tener una sola copia, en el mismo sitio que el monedero.
- Que nadie de tu familia sepa que existe.

MI EXPERIENCIA

El cuarto error de esa lista lo he cometido yo. Hay bots de Telegram para comprar y vender memecoins que te piden importar la clave privada de una wallet para operar más rápido. Funcionan, pero en el momento en que pegas la clave, el operador del bot tiene control total sobre esa wallet para siempre, aunque borres el mensaje. Lo hice con una wallet de pruebas, y esa wallet quedó marcada: nunca más guardará nada de valor. Si algún día usas uno de esos bots, que sea con una wallet creada solo para eso y con el mínimo dinero imprescindible.

08 La passphrase: la palabra 25

Muchos monederos permiten añadir una passphrase, una contraseña extra que eliges tú y que se combina con la semilla. Con la misma semilla y otra passphrase se genera una wallet completamente distinta, y con cada passphrase posible, otra. Nada en el aparato indica si usas una o no.

Sirve sobre todo para dos cosas. Si alguien encuentra tus 24 palabras, sin la passphrase solo verá una wallet vacía, o una con poco dinero que dejaste a propósito como señuelo. Y te protege frente a una amenaza física: si alguien te obliga a abrir tu monedero, puedes enseñarle la wallet señuelo. También te protege si alguien consigue acceso físico a tu aparato y logra extraer la semilla de su memoria, algo que en 2020 unos investigadores de seguridad demostraron que podía hacerse en algunos modelos en unos quince minutos con el equipo adecuado. Con passphrase, la semilla extraída no basta.

Tiene un coste serio. Si olvidas la passphrase, lo pierdes todo, igual que si pierdes la semilla, y no puede guardarse junto a ella, porque entonces no protege nada. Si no te ves capaz de gestionarla sin errores, es mejor no usarla. Y si la usas, apúntala también, con el mismo cuidado que la semilla, en otro lugar.

09 Montar un monedero de hardware paso a paso

1. Desempaqueta y revisa que el precinto esté intacto, que no haya palabras impresas en la caja y que el aparato no venga configurado.
2. Instala la aplicación oficial desde la web del fabricante, escribiendo tú la dirección.
3. Actualiza el firmware (el programa interno del aparato) desde esa aplicación.
4. Crea una wallet nueva. El aparato generará la semilla y te la mostrará en su propia pantalla, nunca en la del ordenador.
5. Apunta las palabras en papel, en orden y numeradas, y confírmalas en el aparato.
6. Elige un PIN. Si alguien roba el aparato, sin el PIN no puede usarlo, y tras varios intentos fallidos se borra.
7. Prueba con poco. Envía una cantidad pequeña a una de sus direcciones, comprobando la dirección en la pantalla del aparato y no solo en la del ordenador, y confirma que llega.
8. Prueba la recuperación: restaura la semilla en el mismo aparato o en otro y confirma que salen las mismas direcciones.
9. Pasa la semilla a metal si la cantidad lo merece y guárdala en su sitio.
10. Ahora sí, mueve el resto, empezando por un envío mediano antes del grande.

TRUCO

Cuando recibas en tu monedero de hardware, verifica siempre la dirección en la pantalla del aparato. Hay programas maliciosos que cambian la dirección que ves en el ordenador por la del ladrón. La pantalla del aparato es lo único que no pueden tocar.

10 Enviar y recibir sin sustos

La mayoría de los errores caros de quien empieza no tienen nada que ver con piratas. Son envíos a la dirección equivocada, por la red equivocada o sin un dato que hacía falta. Unos pocos hábitos los evitan casi todos.

Copia y pega las direcciones, nunca las escribas a mano, y después compruébalas. No basta con mirar los primeros caracteres: hay estafadores que generan direcciones que empiezan y terminan igual que la tuya para colarse en tu historial (lo verás en el Módulo 09). Mira el principio, el final y un trozo del medio. Si el envío es grande, haz antes uno de prueba con una cantidad pequeña y espera a que llegue. Pagar dos comisiones es mucho más barato que perderlo todo.

Asegúrate de que la red es la misma en los dos lados. Una dirección de Ethereum sirve también en Base, Arbitrum o BNB Chain, porque todas usan el mismo formato, pero eso no significa que el exchange de destino acepte esa moneda en esa red. Si envías por una red que el destino no admite, en el mejor de los casos te tocará pedir una recuperación manual, que a veces cobran y a veces no hacen.

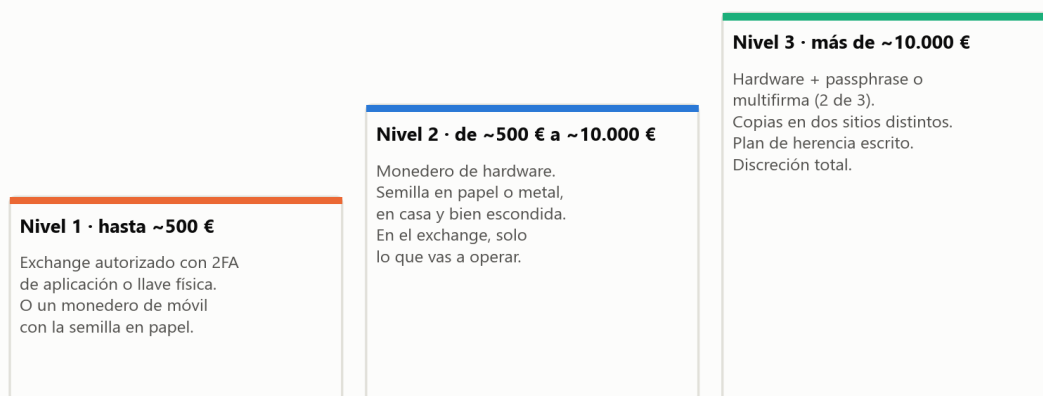
Algunas monedas, como XRP o Stellar, usan una etiqueta o memo cuando envías a un exchange, porque el exchange usa una sola dirección para muchos clientes y distingue a cada uno por ese número. Si lo olvidas, el dinero llega al exchange, pero no a tu cuenta, y tendrás que reclamarlo al servicio de atención al cliente.

Por último, activa en tus exchanges la lista blanca de direcciones de retirada si la ofrecen. Solo podrás retirar a direcciones que hayas guardado antes, y añadir una nueva suele llevar un día o dos de espera. Es una molestia pequeña que hace inútil que alguien entre en tu cuenta e intente mandar tu dinero a otra parte.

11 Cuánta seguridad según cuánto tienes

La seguridad perfecta no existe y la excesiva también cuesta. Si tu sistema es tan complicado que te da miedo tocarlo, acabarás cometiendo un error. Ajusta el esfuerzo a lo que te juegas:

Cuánta seguridad según cuánto dinero



Los importes son orientativos: el umbral real es la cantidad cuya pérdida te haría daño de verdad.

Figura 3. Tres niveles de seguridad según la cantidad

Los importes son orientativos. El umbral real es la cantidad cuya pérdida te haría daño de verdad, y eso depende de tu situación. Para un estudiante, 500 euros pueden ser el nivel 3; para otra persona, 5.000 euros pueden ser el nivel 1. Y la protección de la cuenta del exchange cuenta en todos los niveles: una contraseña única, larga y guardada en un gestor de contraseñas, y una verificación en dos pasos con una aplicación o una llave física, nunca por SMS (en el Módulo 09 verás por qué).

12 La multifirma, para cantidades grandes

Una wallet multifirma 2 de 3 tiene tres llaves (por ejemplo, tres monederos de hardware de marcas distintas guardados en tres sitios) y necesita dos cualesquiera para mover fondos. Si pierdes una llave, no pasa nada: con las otras dos recuperas. Si te roban una, el ladrón no puede hacer nada con ella sola. Es el estándar para empresas y para patrimonios importantes.

Puedes montarla tú mismo con programas como Sparrow o Nunchuk en bitcoin, o Safe en Ethereum, o apoyarte en servicios de custodia colaborativa, en los que tú tienes dos de las tres llaves y una empresa especializada guarda la tercera. Esa empresa no puede mover tu dinero sola, pero puede ayudarte a recuperarlo si pierdes una llave, y puede ser una pieza útil para la herencia.

La multifirma no te hace invulnerable. En febrero de 2025, el exchange Bybit guardaba sus fondos en una multifirma de Safe que necesitaba varias firmas de su equipo. Los atacantes, que el FBI atribuyó al grupo norcoreano Lazarus, habían comprometido el ordenador de un desarrollador del servicio y cambiaron lo que mostraba la web. Los firmantes vieron una operación normal y firmaron. Lo que firmaron de verdad cambiaba el contrato de la wallet y les daba el control a los atacantes, que se llevaron unos 1.500 millones de dólares. La pantalla del ordenador puede mentir; lo que importa es lo que muestra el aparato y lo que dice la simulación de la transacción.

13 Firmar sin que te vacíen

Este es el apartado que más dinero ahorra en la práctica, porque muchas de las pérdidas de 2024 a 2026 no fueron por semillas robadas, sino por firmas aprobadas sin entender lo que hacían.

Qué firmas cuando conectas tu wallet

Cuando entras en una aplicación DeFi y pulsas «Conectar wallet», solo compartes tu dirección, y eso en sí no es peligroso. El peligro llega después, con lo que firmas, y conviene distinguir cuatro tipos de firma.

Una transacción normal, como enviar o intercambiar, mueve fondos y paga gas, y tu monedero te enseña lo que va a pasar. Una aprobación (*approve*) da permiso a un contrato para mover tus tokens en tu nombre; es necesaria para usar un exchange descentralizado, pero muchas aplicaciones piden permiso ilimitado, y ese permiso sigue vivo hasta que lo revokes, así que si el contrato es malicioso o lo hackean después, puede vaciar ese token de tu wallet cuando quiera. Una firma de mensaje o de permiso no paga gas y parece inofensiva («firma para iniciar sesión»), pero algunos tipos de firma, llamados *permit*, autorizan movimientos de tus tokens; es la herramienta favorita de los kits de robo que usan las webs falsas. Y una autorización de delegación, posible en Ethereum desde la actualización Pectra de 2025, puede hacer que tu cuenta delegue su funcionamiento en un contrato: tiene usos legítimos y ya se ha usado para robar. Si una web te pide «actualizar tu cuenta» o «activar funciones inteligentes» y no sabes exactamente por qué, no firmes.

Cómo firmar con cabeza

Usa un monedero que simule las transacciones. Algunos, como Rabby, te enseñan antes de firmar qué tokens van a salir y entrar de tu wallet; si una «reclamación de airdrop» dice que vas a enviar todos tus USDC, ya sabes lo que es. Lee lo que pide la firma: si ves palabras como *approve*, *permit*, *setApprovalForAll*, *increaseAllowance* o una delegación, para y pregúntate por qué esa web necesita ese permiso. Da permisos limitados, porque muchos monederos permiten editar la aprobación para autorizar solo la cantidad que vas a usar. Firma lo que importe con el monedero de hardware y comprueba en su pantalla lo que firmas; si el aparato muestra datos ilegibles (la llamada firma a ciegas), desconfía.

Revisa y revoca permisos cada cierto tiempo con revoke.cash o con la función de tu monedero. Revocar cuesta un poco de gas y cierra puertas que dejaste abiertas meses atrás. Y separa wallets: una caliente, con poco dinero, para probar aplicaciones, y otra que nunca conectas a nada, para guardar.

CHECKLIST

- Sé exactamente en qué web estoy: la he abierto desde mis marcadores, no desde un anuncio ni un enlace.
- Sé qué hace esta firma: enviar, intercambiar, aprobar o firmar un mensaje.
- La simulación del monedero muestra lo que espero que pase.
- Si es una aprobación, es por la cantidad justa, no ilimitada.
- Si nadie me ha explicado por qué necesito firmar esto, no lo firmo.

14 Discreción: la seguridad que no se compra

Hay una parte de la seguridad que no depende de ningún aparato. En 2025, Francia vivió una oleada de secuestros y ataques a personas relacionadas con las criptomonedas, incluido el de uno de los cofundadores de Ledger, al que retuvieron en enero para pedir un rescate en cripto. Los expertos lo llaman el ataque de la llave inglesa, porque ninguna criptografía resiste a alguien que te amenaza en tu propia casa.

La mejor defensa es que no se sepa. No publiques cuánto tienes, ni capturas de tus ganancias, ni fotos en las que se vea tu monedero o tu casa. Usa en los exchanges un correo que no uses para nada más. Si compras un monedero de hardware, piensa si quieres que lo entreguen en tu domicilio o en un punto de recogida. Y ten preparada la passphrase con la wallet señuelo si tu nivel de riesgo lo justifica. En el Módulo 09 lo verás con más detalle.

15 Que tu familia pueda recuperar tus criptos

Esta es la parte que casi todo el mundo deja para más adelante, y es la que convierte una buena seguridad en un problema. Si eres la única persona que sabe que tienes criptomonedas, dónde están y cómo se recuperan, el día que te pase algo tu familia no podrá recuperarlas, o, peor, alguien se aprovechará de su desconocimiento para quedárselas.

El objetivo es un equilibrio difícil: que tu familia pueda recuperarlas cuando haga falta y que nadie pueda hacerlo antes. Hay varias formas de conseguirlo, y lo más habitual es combinar un documento de instrucciones con un buen sistema de copias.

El documento de instrucciones no debe contener la semilla. Debe explicar qué tienes (qué monedas, aproximadamente cuánto, en qué exchanges y en qué monederos), dónde están los aparatos y las copias de la semilla, cómo se usan paso a paso y a quién pueden pedir ayuda que sepa de esto y sea de confianza. Escríbelo pensando en alguien que no sabe nada de cripto, porque probablemente será así. Guárdalo donde tu familia lo vaya a encontrar, por ejemplo, con el resto de tus papeles importantes, y dile a una o dos personas que existe.

Las copias de la semilla deben estar donde tu familia pueda llegar y un ladrón no. Hay quien deja una copia en casa de un familiar de confianza, en un sobre cerrado, o reparte la semilla con el método de Shamir entre varias personas de forma que ninguna pueda recuperarla sola. Una multifirma en la que una de las llaves la tiene una persona de confianza o una empresa de custodia colaborativa es otra solución muy buena para cantidades grandes. No pongas la semilla en el testamento: pasa por demasiadas manos.

Recuerda, además, que las criptomonedas forman parte de la herencia a efectos fiscales. Tus herederos tendrán que declararlas en el impuesto de sucesiones, y si tienes cantidades relevantes en exchanges extranjeros, hay obligaciones informativas que conviene tener al día (lo verás en el Módulo 48).

CHECKLIST

- Hay al menos una persona de confianza que sabe que tengo criptomonedas.
- Existe un documento de instrucciones, sin la semilla, que explica qué tengo, dónde y cómo recuperarlo.
- Las copias de la semilla están en lugares a los que mi familia puede llegar y un ladrón no.
- He revisado el plan en el último año, con mis cantidades y mis monederos actuales.
- Si tengo una passphrase o una multifirma, las instrucciones explican también eso.

LO QUE TE LLEVAS

- Una wallet no guarda criptomonedas; guarda las claves que permiten moverlas. Quien tiene las claves tiene el dinero, y no hay forma de deshacer una transacción.
- Un exchange es cómodo y necesario para comprar y operar, pero puede quebrar, sufrir un hackeo o bloquearte la cuenta. MiCA obliga a separar el dinero de los clientes, pero no te cubre ningún fondo de garantía.
- Para lo que vas a tener meses o años, lo más sensato es tu propia wallet, y a partir de cantidades que te dolería perder, un monedero de hardware comprado en la web oficial.
- La semilla no se puede adivinar, así que solo se roba de donde la guardas o de donde la escribes. En papel o metal, nunca en foto ni en la nube, con una prueba de recuperación hecha y copias en sitios distintos.
- La passphrase y la multifirma añaden protección para cantidades grandes, a cambio de más complejidad.
- Muchas pérdidas recientes son firmas aprobadas sin entenderlas. Usa simulación, permisos limitados y revoca lo que no uses.
- La discreción y un plan de herencia escrito son parte de la seguridad.

16 Ejercicios

EJERCICIO

1. Tu mapa de custodia. Haz una lista de todo lo que tienes en cripto: dónde está (exchange, móvil, hardware), cuánto es aproximadamente y quién tiene las claves de cada cosa. ¿Hay algo en un exchange que no vayas a usar en los próximos meses?

2. Monta un monedero de móvil. Instala un monedero de móvil de un fabricante conocido, crea una wallet nueva, apunta la semilla en papel y haz la prueba de recuperación: bórrala, restáurala y comprueba que la dirección es la misma. Hazlo sin dinero.

3. Revisa tus permisos. Si ya usas una wallet de Ethereum o de otra red compatible, entra en revoke.cash con tu dirección (solo lectura, sin firmar nada) y mira qué permisos tienes activos. ¿Reconoces todas las aplicaciones?

4. La prueba del ladrón. Imagina que alguien entra hoy en tu casa y se lleva todo lo que encuentre. ¿Podría llevarse también tus criptomonedas? ¿Y si se produce un incendio, podrías recuperarlas?

5. El documento para tu familia. Escribe un borrador del documento de instrucciones, sin ninguna semilla ni contraseña. Dáselo a leer a alguien que no sepa de cripto y pregúntale si entiende qué tendría que hacer.

17 Autoevaluación

PARA PENSAR

1. ¿Qué guarda de verdad una wallet?
a) Las criptomonedas · b) Una copia de la blockchain con todos tus saldos · c) Las claves privadas que permiten moverlas
2. ¿Qué significa «not your keys, not your coins»?
a) Que las monedas son del exchange · b) Que hay que cambiar las claves cada año para que no caduquen · c) Que quien tiene las claves controla el dinero
3. ¿Qué protección tiene en España el dinero que dejas en un exchange si quiebra?
a) El Fondo de Garantía de Depósitos cubre hasta 100.000 euros, como en un banco · b) Ningún fondo de garantía; MiCA obliga a separarlo, pero no lo asegura · c) El Banco de España lo devuelve
4. Te llega un monedero de hardware con una tarjeta que trae 24 palabras impresas. ¿Qué haces?
a) No lo uso: quien imprimió las palabras controla el monedero · b) Lo uso con esas palabras, que para eso vienen de fábrica y están selladas · c) Cambio solo el PIN
5. ¿Por qué nadie puede adivinar tu frase semilla probando combinaciones?
a) Porque está cifrada por el fabricante y solo él puede leerla · b) Porque el número de combinaciones posibles es astronómico · c) Porque cambia cada día
6. ¿Dónde es más seguro guardar la frase semilla?
a) En una foto en el móvil · b) En papel o metal, en un lugar seguro y con una segunda copia en otro sitio · c) En un documento en la nube, protegido con una contraseña larga y la verificación en dos pasos
7. ¿Qué hace una passphrase?
a) Genera una wallet distinta con la misma semilla · b) Sustituye a la semilla · c) Recupera la semilla si pierdes la copia en papel
8. Una wallet multifirma 2 de 3 necesita...
a) Las tres llaves siempre, cada vez que firmas · b) Dos llaves cualesquiera de las tres · c) Una sola llave
9. Una web te pide firmar un «permit» para reclamar un airdrop. ¿Qué haces?
a) Firmo, porque una firma que no cuesta gas no puede mover fondos · b) Firmo dos veces · c) Desconfío: ese tipo de firma puede autorizar que se lleven mis tokens
10. Verdadero o falso: lo más seguro es que nadie de tu familia sepa que tienes criptomonedas.

Soluciones

1: c. · 2: c. · 3: b. · 4: a. · 5: b. · 6: b. · 7: a. · 8: b. · 9: c. · 10: Falso. Si nadie lo sabe, tu familia no podrá recuperarlas. Lo seguro es que lo sepan las personas adecuadas, con un documento de instrucciones sin la semilla y las copias en un lugar al que puedan llegar.

18 El curso completo

Este módulo es uno de los 100 de Cripto sin humo, el curso completo de criptomonedas, altcoins, DeFi, blockchain y trading, desde cero y con datos reales. Cada módulo tiene su PDF y su vídeo. Son cuatro niveles, de menos a más: fundamentos (bloques 1 a 4), dinero, inversión y trading (5 a 8), a fondo (9 a 12) y profesional (13 a 16). Si te ha servido, esto es lo que encontrarás en el resto.

Bloque	Módulos
1. Entender las criptomonedas	Empieza aquí · El dinero y el nacimiento de Bitcoin · Bitcoin por dentro · Bitcoin como inversión · Ethereum · El mapa de las altcoins · Stablecoins · Tokenomics y análisis de proyectos
2. Usar cripto con seguridad	Wallets y custodia · Estafas y hackeos · Exchanges y plataformas · Las grandes crisis de cripto
3. DeFi y los usos de la blockchain	Intercambios, AMM y puentes · Préstamos, staking y rendimientos · NFT, DAO y tokenización · Análisis on-chain · Memecoins y airdrops
4. El universo cripto a fondo	Consenso · Capas 2 · El mapa de las blockchains · Bitcoin más allá del precio · DeFi avanzado · Mercados de predicción · IA, DePIN, juegos y privacidad · Criptografía sin fórmulas · Contratos inteligentes en la práctica · La infraestructura invisible
5. Poder, dinero y mundo	Quién manda en cripto · Quién mueve el precio · Informarte sin que te manipulen · El gran debate económico · CBDC y euro digital · Geopolítica · Cripto en el mundo hispano · Pagar, cobrar y trabajar con cripto
6. Invertir en criptomonedas	Ciclos, macro y sentimiento · Tu cartera a largo plazo · Casos prácticos de cinco criptomonedas y cinco protocolos DeFi
7. Trading de criptomonedas	Fundamentos · Análisis técnico con evidencia · Futuros perpetuos · Gestión del riesgo · El método de ruptura de canal · Backtesting · Psicología · Bots y copy trading · Prop firms
8. Impuestos, ley y plan	Fiscalidad y regulación · Tu plan de 90 días
9. Mercados y derivados a fondo	Ejecutar bien · La curva de futuros · Funding y arbitraje · Opciones · Volatilidad · Correlación y diversificación
10. DeFi y on-chain a fondo	MEV · Proveer liquidez a fondo · Bóvedas y gestores · Staking líquido y restaking · Stablecoins por dentro · Comprobar antes de crear · Gobernanza y tesorías
11. Seguridad y custodia avanzada	Multifirma paso a paso · Seguridad operativa · Herencia y sucesión · Si te roban · Riesgo de plataforma
12. Impuestos, ley y profesión	Fiscalidad avanzada con casos · Tu contabilidad cripto · Pérdidas, robos y quiebras · Residencia fiscal · Regulación a fondo · Trabajar en cripto
13. Investigar con rigor	Estadística para decidir · Un experimento honesto · Los sesgos de los datos · Los costes · Remuestreo y Montecarlo · Tu laboratorio · Leer un backtest ajeno · Lo que probé y no funcionó
14. Estrategias sistemáticas	Seguimiento de tendencia · El método, versión 2 · Elegir el universo · Carry y primas de riesgo · Corto a nuevos listados · Rentas que explotan · Carteras de estrategias
15. Sistemas en producción	Del backtest al bot · Infraestructura y vigilancia · Claves y seguridad · Papel, demo y real · Cuándo apagar un sistema

Bloque	Módulos
16. Capital, expectativas y carrera	Tamaño óptimo y riesgo de ruina · Caídas y rentabilidades realistas · Operar capital ajeno · Tu patrimonio completo · Tu plan profesional

Y el material extra: un glosario de más de 440 términos, plantillas y listas para imprimir, un Excel con ocho herramientas, como la calculadora de posición y liquidación, el diario en R, las rachas, el DCA, el rebalanceo, los impuestos y las prop firms, el indicador del método para TradingView con su manual, una cronología de 2008 a 2026, un mapa de herramientas y un laboratorio con cinco programas para investigar por tu cuenta.

Todo con la misma idea que este módulo: explicado desde cero, con datos y sin promesas. Lo encontrarás en jvcrypto.es/curso.

Aviso legal y de riesgos

Este documento forma parte del curso «JV CRYPTO · Cripto sin humo» y tiene una finalidad exclusivamente formativa e informativa. No es asesoramiento financiero, fiscal ni legal, ni una recomendación personalizada de inversión, ni una oferta o invitación para comprar o vender ningún activo.

Los criptoactivos son muy volátiles y puedes perder todo el dinero que inviertas. Los productos con apalancamiento (futuros, perpetuos, CFD) amplifican las pérdidas y la mayoría de los particulares que los operan pierden dinero. Los criptoactivos no están cubiertos por el Fondo de Garantía de Depósitos ni por el Fondo de Garantía de Inversiones.

Los resultados de backtests y de operativa pasada no garantizan resultados futuros. Las cifras de este curso están fechadas (datos a septiembre de 2026) y pueden haber cambiado cuando lo leas: compruébalas antes de decidir.

La fiscalidad y la normativa dependen de tu país de residencia y cambian a menudo. Consulta con un profesional antes de declarar u operar. Desde el 1 de julio de 2026, en España solo pueden prestar servicios de criptoactivos las entidades autorizadas conforme a MiCA: comprueba el registro de la CNMV o de ESMA antes de abrir cuenta en una plataforma.

Conflictos de interés: el autor opera con criptoactivos, puede tener posiciones en activos mencionados y participa en programas de referidos de algunas plataformas. Cuando se menciona una de ellas, se indica.

© 2026 JV CRYPTO (Javier Ruiz). Uso personal del comprador. Prohibida su copia o redistribución.

jvcrypto.es · [YouTube @jvcrypto](#) · [Telegram @JVCRYPTOYT](#) · [X @JV_Crypto10](#)