CUVEX

CUVEX ACADEMY · 0.1

Aprende. Comprende. Toma el control.

Bitcoin y autocustodia, explicados paso a paso. Curso, manual, glosario y prácticas gratuitos, sin registro. Tú eliges por dónde empezar.

Gratis · sin registro

Todas las secciones

1. Preparar tu espacio de aprendizaje
2. Dinero digital y el problema de la confianza
3. Historia y límites de Bitcoin
4. Satoshis y cálculos sin errores
5. Tu modelo de amenazas
6. Nodos minería y consenso
7. UTXOs y el cambio de una transacción
8. Mempool confirmaciones y reorganizaciones
9. Comisiones tamaño virtual y sustitución
10. Redes direcciones y facturas
11. Hash firmas y cifrado
12. Semilla passphrase y contraseña
13. Derivación xpub y descriptores
14. Elegir una wallet y un modelo de custodia
15. Backups que se pueden recuperar
16. Conocer Original y BIT
17. Crear una semilla con entropía física
18. Cifrar y descifrar un secreto con Cuvex
19. Umbrales de cifrado y biometría
20. Clonar conservar y verificar copias
21. Instalar y proteger Cuvex Desk
22. Vincular criptogramas y organizar WOW
23. Enlazar Mirror con Desk
24. NFC mediante Mirror, USB-C y lectura de QR
25. Proveedores públicos y nodo propio
26. Recibir bitcoin y comprobar la dirección
27. Etiquetar congelar y seleccionar UTXOs
28. Preparar y revisar un pago
29. Firmar con Original y con BIT
30. Finalizar publicar y resolver incidencias
31. Qué se puede observar en Bitcoin
32. Separar contextos y gestionar el cambio
33. Privacidad de red Tor y VPN
34. CoinJoin Payjoin y límites actuales
35. Lecciones de incidentes reales

36. Crear identidad y verificar contactos de chat
37. Solicitar y pagar satoshis desde chat
38. Compartir criptogramas de forma consciente
39. Recuperar chat y entender sus metadatos
40. Configuración cotidiana y revisión de permisos
41. Diseñar una cartera multifirma
42. Crear invitaciones y aportar claves
43. Verificar políticas con Mirror en orden libre
44. Coordinar firmas y publicar multifirma
45. Recuperar y cambiar una multifirma
46. Actualizar firmware sin improvisar
47. Pérdida avería y recuperación de emergencia
48. Phishing soporte y fraudes con voz
49. Privacidad legalidad y registros personales
50. Herencia continuidad y simulacro anual
51. Precio ahorro y análisis fundamental
52. Elegir dónde adquirir bitcoin
53. Cuentas órdenes y costes de ejecución
54. Velas indicadores y sesgos del análisis técnico
55. Margen futuros y automatización
56. Lightning y otras capas
57. Taproot MuSig2 y futuro poscuántico
58. Interoperabilidad y salida del fabricante
59. Laboratorio técnico con regtest
60. Proyecto final y plan de continuidad
61. Manual del alumno
62. Glosario de Bitcoin y autocustodia
63. Comprueba lo que has aprendido

M01

Preparar tu espacio de aprendizaje

Objetivo

Preparar el curso, distinguir los tres equipos y acordar qué información nunca se comunica al tutor.

Comprender

Vas a aprender a recibir, custodiar, gastar y recuperar bitcoin con criterio propio. La meta final es poder explicar una decisión antes de autorizarla. El curso se puede leer sin asistencia; la voz aporta explicaciones, preguntas y acompañamiento. No necesita ver tu patrimonio ni controlar tus dispositivos.

Cuvex es el equipo que protege secretos y autoriza operaciones en su pantalla. Desk organiza criptogramas, carteras de observación, pagos y coordinación en el ordenador. Mirror es un puente local para operaciones compatibles y un comparador de datos; no es el firmante ni una wallet autónoma. Tu versión y tu modelo determinan qué trayecto puedes utilizar.

Reserva una pantalla para este curso y otra para Desk; mantén el teléfono y Cuvex a mano. Si solo tienes una pantalla, alterna sin compartirla por videollamada durante la introducción de secretos. Una llamada puede terminar antes de completar una práctica. Pausar no es fallar. Guarda únicamente el identificador de la lección, el paso alcanzado y la dificultad encontrada.

Ni el instructor humano ni la IA deben recibir semillas, passphrases BIP39, contraseñas, Clave Chat, PIN, archivos privados o códigos de compra completos. Tampoco necesitan tu xpub, descriptor real o dirección. Aunque estos últimos no permitan gastar, revelan actividad. Describe mensajes de error y utiliza los datos ficticios del laboratorio.

Práctica

1. Identifica físicamente ordenador, teléfono y modelo Cuvex. Anota sus versiones en tu cuaderno privado.
2. Separa un entorno de aprendizaje sin fondos de tu custodia real. No importes una semilla de producción para practicar.
3. Abre esta lección y localiza la pausa, la ayuda y el glosario. Si alguien te pide un secreto, detén esa interacción.

Demuestra

Explica quién firma, quién consulta la red y quién transporta datos. El criterio de avance es distinguir esas funciones sin ayuda.

Duda frecuente

¿Tengo que hablar todos los días con el tutor? No. Puedes estudiar por tu cuenta, repetir una sesión y solicitar ayuda solo en un procedimiento concreto. El acceso al curso y el saldo del servicio de voz son derechos distintos.

Punto de pausa

L01 completada; equipos identificados; ningún secreto registrado en el curso.

El tutor pide tu frase semilla para comprobar que la escribiste bien. ¿Qué haces?

1. La dicto lentamente.
2. Detengo la petición y compruebo la semilla solo en mi entorno seguro.
3. Envío únicamente las primeras palabras.

> **Ver respuesta: Detengo la petición y compruebo la semilla solo en mi entorno seguro.**
> Cualquier fragmento de un secreto queda fuera del servicio formativo.

M01

Dinero digital y el problema de la confianza

Objetivo

Comprender qué problema intenta resolver Bitcoin antes de abrir una wallet.

Comprender

Un saldo bancario es una anotación administrada por una entidad. Esa entidad autentica al cliente, decide qué transferencias procesa y lleva su contabilidad. Un archivo digital corriente se copia con facilidad: enviar una fotografía no impide conservar otra. Para que una unidad digital funcione como dinero, hace falta evitar que se gaste dos veces.

Bitcoin combina reglas de validación, firmas y una historia compartida de transacciones. En lugar de confiar a una única entidad el registro completo, permite que participantes independientes comprueben si una transacción respeta las reglas. La escasez depende de que esas reglas sigan siendo verificadas y aceptadas; no nace de una imagen de una moneda ni del precio publicado por un exchange.

La autocustodia cambia responsabilidades. Puedes conservar la capacidad de gastar sin pedir permiso a un custodio, pero también puedes perderla si destruyes todos tus respaldos o firmas un pago equivocado. La libertad operativa no elimina la necesidad de seguridad, coordinación, conectividad para publicar ni cumplimiento de obligaciones aplicables.

No confundas Bitcoin, la red y protocolo, con BTC, su unidad monetaria. Otras redes pueden usar la palabra blockchain y ofrecer propiedades distintas. Una promesa de una empresa denominada «bitcoin» tampoco equivale a disponer de una salida de Bitcoin bajo tus propias claves.

Práctica

1. Compara tres situaciones: saldo en banco, saldo en exchange y UTXO controlado con tus claves.
2. Para cada una escribe quién puede impedirte mover el saldo y quién puede ayudarte si olvidas el acceso.
3. Describe qué ocurriría al copiar una foto y qué ocurriría al intentar gastar dos veces la misma salida.

Demuestra

Explica con tus palabras por qué un saldo y la capacidad de firmar son conceptos diferentes. No hace falta memorizar términos técnicos.

Duda frecuente

¿Autocustodia significa que desaparecen todos los intermediarios? Puedes elegir servicios para comprar, consultar o comunicarte. La diferencia relevante es qué poder conservan y qué datos reciben.

Punto de pausa

Guarda tu comparación de responsabilidades sin nombres de cuentas reales.

¿Qué problema monetario no resuelve por sí sola una firma digital?

1. Impedir que se intente gastar dos veces la misma salida.
2. Probar autorización con una clave.
3. Detectar que cambió el mensaje firmado.

> **Ver respuesta: Impedir que se intente gastar dos veces la misma salida.**
> Las firmas autorizan; las reglas y el consenso ordenan gastos incompatibles.

M01

Historia y límites de Bitcoin

Objetivo

Situar el origen de Bitcoin y separar hechos históricos de relatos comerciales.

Comprender

El documento de Satoshi Nakamoto se difundió en 2008 y la red comenzó en 2009. Propuso efectivo electrónico entre pares, aprovechando ideas anteriores de criptografía, prueba de trabajo y dinero digital. La identidad civil de Satoshi no es necesaria para verificar el software o una transacción.

La evolución no ha consistido en que una empresa sustituya unilateralmente las reglas. Desarrolladores proponen y revisan cambios; operadores eligen software; mineros construyen bloques; usuarios y servicios deciden qué aceptan. Esa distribución puede producir desacuerdos. Una bifurcación y una actualización de aplicación no son sinónimos.

Un nodo puede rechazar un bloque que incumple sus reglas aunque tenga mucho trabajo detrás. El consenso no es una votación simple por número de ordenadores. Ejecutar miles de copias de un nodo no concede automáticamente más poder de decisión. Del mismo modo, una mayoría minera no obtiene por ese hecho la clave privada de un usuario.

Bitcoin tiene límites deliberados y compromisos: capacidad de bloque, coste de verificación, tiempos de confirmación variables y registro público. No ofrece reversión administrativa de pagos ni confidencialidad integral por defecto. Las capas y aplicaciones intentan resolver usos concretos a cambio de nuevas dependencias.

Práctica

1. Coloca en una línea temporal documento inicial, inicio de red, adopción de SegWit y activación de Taproot. Comprueba fechas en fuentes antes de publicarlas.
2. Clasifica «una empresa garantiza el precio», «un nodo valida» y «un minero propone un bloque» como promesa comercial o función técnica.
3. Explica una ventaja y un coste de no disponer de un administrador que revierta pagos.

Demuestra

Distingue regla de consenso, política local y decisión de una empresa. La aplicación que utilizas no es toda la red.

Duda frecuente

¿El software más reciente siempre cambia las reglas monetarias? No. Las versiones también corrigen errores, mejoran rendimiento o modifican políticas locales. Lee las notas de la versión y su compatibilidad.

Punto de pausa

Anota una propiedad comprobable y una afirmación que exigiría evidencia adicional.

Un bloque contiene un gasto sin autorización válida. ¿Lo vuelve válido una mayoría de mineros?

1. Sí, si supera el 51 %.
2. Solo si el exchange lo anuncia.
3. No para un nodo que aplica las reglas que lo rechazan.

> **Ver respuesta: No para un nodo que aplica las reglas que lo rechazan.**
> El trabajo acumulado se compara entre historias válidas según las reglas del nodo.

M01

Satoshis y cálculos sin errores

Objetivo

Convertir BTC y satoshis, y comprobar cantidades sin depender de una cotización.

Comprender

Un BTC equivale a 100.000.000 satoshis. «sat» es una unidad, no otra moneda. En la cadena base los importes se contabilizan como enteros en satoshis. 0,001 BTC son 100.000 sat; 0,00001000 BTC son 1.000 sat. El separador decimal que muestra una interfaz depende del idioma; no añadas ceros a ojo.

Una cotización convierte temporalmente BTC a una moneda como EUR o USD. No cambia cuántos satoshis controlas. Si tienes 100.000 sat y cambia el precio, el número de satoshis sigue siendo el mismo. En Desk la cotización es una referencia con fuente y fecha; un dato antiguo puede inducir una decisión económica incorrecta aunque el saldo BTC sea correcto.

Para un pago hay que distinguir importe del destinatario, comisión de red y gasto total. Si se envían 50.000 sat y la comisión es 600 sat, la salida de valor de tu cartera es 50.600 sat, salvo otras salidas propias. «Enviar el total» normalmente calcula un destinatario neto menor que el saldo disponible porque debe pagar la comisión.

Los ejemplos del curso son ejercicios aritméticos, no precios de mercado ni tarifas recomendadas. Antes de firmar, comprueba unidad, red, destinatario y coste total en la pantalla correspondiente. La voz puede decir «cincuenta mil satoshis» y mostrar a la vez «50.000 sat»; nunca debe decidir un importe por una transcripción dudosa.

Práctica

1. Convierte 250.000 sat a BTC: 0,0025 BTC. Convierte 0,00025000 BTC: 25.000 sat.
2. Calcula un envío de 75.000 sat con 900 sat de comisión: gasto de 75.900 sat.
3. En el simulador usa 120.000 sat, envío de 70.000 y comisión de 1.000. Comprueba un cambio de 49.000 sat.

Demuestra

Lee una cantidad en BTC y en sat, y explica cuál incluye la comisión. Si dudas, la operación se pausa.

Duda frecuente

¿Necesito comprar un bitcoin entero? No. Puedes adquirir una fracción, sujeta a mínimos y costes del proveedor.

Punto de pausa

Conserva solo tus resultados del ejercicio.

Dispones de 80.000 sat y quieres enviar el total con 1.200 sat de comisión. ¿Cuánto recibe el destinatario?

1. 80.000 sat.
2. 78.800 sat.
3. 81.200 sat.

> **Ver respuesta: 78.800 sat.**
> El destinatario recibe el saldo gastable menos la comisión en este supuesto sin otras salidas.

M01

Tu modelo de amenazas

Objetivo

Elegir medidas proporcionadas frente a pérdida, robo, engaño y exposición de datos.

Comprender

Seguridad es conservar la capacidad de actuar según tu intención. Privacidad es controlar quién conoce tus datos y relaciones. Disponibilidad es poder acceder cuando lo necesitas. Una caja inaccesible a todos también puede ser inaccesible para ti; una copia muy cómoda puede exponer demasiada información.

Define activos, adversarios y accidentes. Los activos incluyen claves, respaldos, historial, ubicación de copias e identidad de contactos. Los riesgos incluyen malware, phishing, incendio, olvido, coacción, avería, fallecimiento y errores propios. No todos se reducen con la misma herramienta.

Usa una matriz sencilla: probabilidad aproximada, impacto y medida concreta. Una contraseña larga reduce intentos de adivinación; no corrige un destinatario fraudulento que tú mismo autorizas. Dos copias en la misma bolsa no resuelven la pérdida de esa bolsa. Una multifirma cuyos equipos y respaldos controla una sola persona puede conservar un punto de fallo común.

El curso y el tutor también forman parte del modelo: compras, llamadas, tiempos de conexión y progreso pueden crear metadatos. El minisite no debe pedir direcciones o saldos para personalizar una clase. Que Desk o Mirror no requieran un registro convencional no implica que la tienda, un proveedor de voz o una consulta a terceros desconozcan tu actividad.

Práctica

1. Escribe tus tres riesgos más importantes sin cantidades patrimoniales ni ubicaciones exactas.
2. Para cada uno elige prevención, detección y recuperación. Ejemplo: pérdida de tarjeta; dos copias separadas; inventario; prueba de restauración.
3. Distingue qué persona o sistema puede observar compra, llamada, consulta de saldo y transacción pública.

Demuestra

Justifica por qué tu siguiente medida resuelve un riesgo concreto. No acumules complejidad que no puedas mantener o explicar a tus herederos.

Duda frecuente

¿Más dispositivos siempre significan más seguridad? Solo si reducen dependencias comunes y puedes probar la recuperación. Añadir equipos también añade mantenimiento y posibilidades de confusión.

Punto de pausa

Guarda el plan en tu documentación privada; registra en el curso únicamente «modelo de amenazas revisado».

¿Qué medida reduce mejor el riesgo de perder todas las copias en un incendio local?

1. Cambiar el color de la tarjeta.
2. Poner dos copias en el mismo cajón.
3. Mantener copias comprobadas en ubicaciones con riesgos independientes.

> **Ver respuesta: Mantener copias comprobadas en ubicaciones con riesgos independientes.**
> La redundancia debe resistir el mismo incidente que amenaza al original.

M02

Nodos minería y consenso

Objetivo

Explicar qué validan los nodos y qué aporta la minería.

Comprender

Un nodo completo recibe bloques y transacciones, verifica reglas y mantiene una vista de la cadena. No necesita confiar en el saldo que le anuncia una página. Minería es el proceso de proponer bloques mediante prueba de trabajo. Los mineros seleccionan transacciones válidas y compiten por encontrar un bloque admisible.

La prueba de trabajo hace costoso rehacer la historia. Cuando aparecen alternativas válidas, la referencia relevante es el trabajo acumulado, no simplemente contar bloques sin considerar dificultad. Los intervalos entre bloques varían: diez minutos es una media objetivo, no una cita para el próximo pago.

La recompensa minera combina subsidio y comisiones. El subsidio sigue un calendario de reducción por alturas de bloque; la comisión depende de las transacciones incluidas. Que una transferencia pague más no hace válida una firma incorrecta. La seguridad económica y el coste de ataque no convierten un pago reciente en irreversible de forma matemática.

Un nodo propio reduce la necesidad de comunicar consultas a proveedores ajenos y permite verificar. Todavía debes proteger su sistema operativo, acceso y conexión. Tener un nodo encendido sin sincronizar, o conectado a una app que consulta otro servidor, no proporciona automáticamente esas ventajas.

Práctica

1. Asigna estas tareas: comprobar firma, elegir transacciones de un bloque, custodiar tu semilla y decidir si aceptas un pago.
2. Explica por qué «el minero guarda mis bitcoins» es una descripción incorrecta.
3. En una red de laboratorio, observa altura y sincronización; no publiques credenciales RPC.

Demuestra

Describe la diferencia entre verificar y proponer. Puedes usar una analogía, pero termina con la función técnica correcta.

Duda frecuente

¿Necesito minar para usar Bitcoin? No. Tampoco necesitas tener un nodo propio para comenzar, aunque conocer el nivel de confianza de tu proveedor sí es necesario.

Punto de pausa

Anota el proveedor de laboratorio por su tipo, sin URL privada.

¿Qué aporta un nodo completo bien configurado a su usuario?

1. Verificar las reglas de la cadena que acepta.
2. Recuperar cualquier clave perdida.
3. Garantizar una subida de precio.

> **Ver respuesta: Verificar las reglas de la cadena que acepta.**
> Validación y custodia son funciones distintas.

UTXOs y el cambio de una transacción

Objetivo

Leer una transacción como consumo y creación de salidas.

Comprender

Una UTXO es una salida de una transacción anterior que sigue sin gastar. Una cartera calcula su saldo identificando las salidas que puede controlar. No hay una cuenta universal que se reste como en una hoja bancaria: una entrada referencia una salida anterior mediante identificador de transacción y posición.

Al gastar una UTXO se consume entera. Si necesitas pagar menos que su valor, normalmente creas una salida al destinatario y otra de cambio bajo tu control. Con una entrada de 120.000 sat, destinatario de 70.000 y comisión de 1.000, el cambio es 49.000. La suma de entradas debe igualar la suma de salidas más la comisión.

Una dirección no es una UTXO. Puede recibir varias salidas. Tampoco es necesariamente una persona. El identificador de transacción puede ser público, pero vincularlo a tu identidad o explicar de quién es cada salida añade información que la cadena no expresa por sí sola.

Esta estructura importa para privacidad: combinar entradas puede sugerir control común; el cambio puede relacionar pagos futuros. Esa inferencia no es una prueba universal porque existen transacciones colaborativas. Coin control consiste en elegir qué salidas gastar, conociendo las consecuencias de combinarlas.

Práctica

1. Dibuja tres entradas ficticias: 40.000, 60.000 y 200.000 sat. Paga 70.000 con 1.000 de comisión usando solo las dos primeras.
2. Comprueba que el cambio es 29.000 sat y que la tercera entrada no participa.
3. Repite usando únicamente 200.000: el cambio sería 129.000. Compara coste potencial y vínculos, sin asumir tamaños iguales.

Demuestra

Localiza entrada, destinatario, cambio y comisión en el diagrama del curso. Si no puedes identificar una salida, no debes firmar una operación real.

Duda frecuente

¿Todo lo que vuelve a mi cartera es cambio? No. Puede ser una transferencia a otra dirección propia. La clasificación exige conocer la política y la derivación, no adivinar por el importe.

Punto de pausa

Conserva el esquema ficticio; nunca una captura de tu patrimonio.

Una entrada de 100.000 sat genera una salida de 30.000 y otra de 69.200. ¿Cuál es la comisión?

1. 69.200 sat.
2. 800 sat.
3. 30.000 sat.

> **Ver respuesta: 800 sat.**
> 100.000 menos 99.200 equivale a 800 sat.

M02

Mempool confirmaciones y reorganizaciones

Objetivo

Distinguir una transacción preparada, publicada y confirmada.

Comprender

La mempool es el conjunto local de transacciones no confirmadas que un nodo conserva según su política. No existe una única mempool idéntica en todo el planeta. Que un explorador muestre un pago significa que ese servicio lo conoce; no garantiza que todos los nodos lo acepten ni que vaya a confirmarse en un tiempo concreto.

Preparar una PSBT no publica nada. Firmar produce autorización. Finalizar construye la transacción que puede difundirse. Publicar intenta transmitirla. Confirmar significa que fue incluida en un bloque de la cadena aceptada por tu fuente de verificación. Una segunda confirmación añade otro bloque encima; no es una segunda firma del destinatario.

Pueden producirse reorganizaciones en las que cambia un tramo de la cadena y una operación pierde confirmaciones o vuelve a pendiente. Para pagos con mayor exposición, las partes suelen exigir más confirmaciones. No hay un número que elimine cualquier riesgo para todos los importes y situaciones.

Si Desk muestra un estado guardado, consulta la fecha de sincronización. «Confirmado» según una instantánea antigua no describe necesariamente el estado actual. Si un envío no aparece, conserva su identificador local y revisa publicación e historial antes de volver a prepararlo: repetir por impaciencia puede crear otro pago válido.

Práctica

1. Ordena estas tarjetas: borrador, PSBT, firma, transacción final, difusión, inclusión en bloque.
2. Simula una desconexión tras publicar. Decide qué comprobar antes de pagar de nuevo.
3. Explica a un comercio por qué un mensaje del chat diciendo «pagado» no sustituye la verificación de red.

Demuestra

Puedes expresar el estado de una operación y la fuente y fecha de esa información sin confundirlo con una garantía.

Duda frecuente

¿Cerrar Desk cancela una transacción publicada? No. Otros nodos y participantes pueden conservarla. La cancelación de un borrador local tiene otro alcance.

Punto de pausa

Apunta el estado de la simulación; no añadas identificadores reales al tutor.

El ordenador se desconecta justo después de pulsar publicar. ¿Qué haces primero?

1. Preparar el mismo pago desde cero.
2. Borrar la cartera.
3. Reconectar y comprobar la transacción y sus entradas.

> **Ver respuesta: Reconectar y comprobar la transacción y sus entradas.**
> Un fallo de respuesta no demuestra que la difusión haya fallado.

M02

Comisiones tamaño virtual y sustitución

Objetivo

Estimar costes, interpretar sat por vbyte y comprender RBF y CPFP.

Comprender

La comisión de red es la diferencia entre entradas y salidas. Su competitividad se expresa habitualmente en sat/vB: satoshis por byte virtual. No depende directamente del valor económico enviado. Muchas entradas pueden encarecer un pago pequeño; un pago grande con pocas entradas puede ocupar menos.

En un ejemplo de 200 vB a 5 sat/vB, la comisión es 1.000 sat. Antes de firmar solo puedes tener una estimación, pues el tamaño final puede depender de firmas y estructura. Desk ofrece velocidades orientativas y tarifa manual; una etiqueta «rápida» no promete una confirmación puntual.

RBF es una política de sustitución de transacciones no confirmadas bajo determinadas condiciones. El mecanismo permite proponer un gasto conflictivo con mayor comisión; las políticas de los nodos han evolucionado y no conviene tratar una señal de no reemplazo como garantía de cobro. Una sustitución requiere una nueva revisión y las firmas necesarias.

CPFP consiste en gastar una salida de la operación pendiente para que el conjunto padre e hijo resulte atractivo. Requiere controlar una salida gastable, cumplir políticas y pagar su coste. Es un concepto de Bitcoin: no se presupone un botón CPFP en la versión de Cuvex del alumno.

«Dust» es una salida demasiado pequeña según políticas aplicables y costes estimados de gasto; no es un umbral universal para todo tipo de script. Evita enseñar una cifra fija como ley de consenso. Si el cambio no es viable, revisa importe, entradas o barrido y la comisión efectiva.

Práctica

1. Calcula 180 vB a 8 sat/vB: 1.440 sat. Comprueba si supera tu presupuesto de laboratorio.
2. Compara una entrada con diez entradas; explica por qué el importe enviado no basta para estimar el coste.

3. Simula una transacción pendiente y decide entre esperar, RBF o estudiar CPFP, sin asumir compatibilidad automática.

Demuestra

Justifica tarifa, comisión absoluta y coste respecto al envío. Rechaza una comisión incomprensible.

Duda frecuente

¿RBF cancela con certeza el pago anterior? No. Las versiones compiten hasta confirmarse y la propagación importa. No entregues bienes basándote en una promesa de cancelación.

Punto de pausa

Guarda la decisión del ejercicio y su motivo.

¿Qué comisión resulta de 250 vB a 4 sat/vB?

1. 1.000 sat.
2. 254 sat.
3. El 4 % del importe enviado.

> **Ver respuesta: 1.000 sat.**
> Tamaño virtual por tarifa da la comisión estimada.

M02

Redes direcciones y facturas

Objetivo

Reconocer red, formato de dirección e instrucciones de pago antes de copiar o escanear.

Comprender

Mainnet mueve bitcoin con valor económico. Las redes de prueba sirven para desarrollar y aprender, pero no son intercambiables entre sí. Regtest es una red local controlada por quien monta el laboratorio; signet y testnet tienen reglas y ecosistemas propios. Una función de monofirma en signet no implica que el perfil multifirma de Cuvex admita esa red.

Las direcciones codifican condiciones de recepción. En mainnet encontrarás formatos que empiezan por 1, 3, bc1q o bc1p. El prefijo ayuda a reconocer una familia, pero no verifica al destinatario, no garantiza compatibilidad del firmante y no sustituye la validación completa del formato.

Un QR es un contenedor visual. Puede transportar una dirección, una factura, un descriptor o texto malicioso. Escanearlo no autentica a su autor. Un enlace bitcoin: puede añadir importe y mensaje. BIP321 es la referencia moderna que sustituye BIP21; Desk mantiene terminología y compatibilidad BIP21 en su implementación revisada. Una mejora del estándar no amplía por sí sola lo que entiende la app.

Una factura Lightning no es una dirección on-chain. Puede incluir caducidad y otros campos; no debes pegarla en un envío de cadena si la aplicación no ofrece un flujo compatible. Un token denominado BTC en otra red tampoco es automáticamente bitcoin nativo.

Práctica

1. Clasifica muestras rotuladas del curso sin usar direcciones gastables: dirección, URI bitcoin:, invoice Lightning y descriptor.
2. Identifica la red seleccionada en el laboratorio. En Cuvex multifirma revisado, la compatibilidad del perfil es mainnet/regtest.
3. Compara el texto completo solicitado por el receptor mediante un canal autenticado antes de una operación real.

Demuestra

Puedes rechazar una solicitud cuya red o modalidad no conoces y explicar qué necesitas verificar.

Duda frecuente

¿Puedo enviar BTC por cualquier red que muestre un exchange? No. La red de retirada debe coincidir con la recepción real. Evita elegir solo por la comisión más baja.

Punto de pausa

Registra únicamente el tipo de red de aprendizaje.

Una dirección de recepción bc1 no autoriza por sí sola a retirar BTC mediante una red de tokens distinta. ¿Qué falta?

1. Cambiar el alias del destinatario.
2. Confirmar que la retirada utiliza Bitcoin on-chain y que todos los datos coinciden.
3. Introducir la semilla en el exchange.

> **Ver respuesta: Confirmar que la retirada utiliza Bitcoin on-chain y que todos los datos coinciden.**
> Activo, red y método de recepción deben ser compatibles.

M03

Hash firmas y cifrado

Objetivo

Distinguir integridad, autorización y confidencialidad.

Comprender

Un hash transforma datos en una huella de longitud fija. Comparar una huella conocida ayuda a detectar cambios; no cifra el archivo ni identifica por sí solo a quien lo publicó. Si descargas archivo y hash desde la misma página comprometida, el atacante puede haber sustituido ambos.

Una clave privada permite crear firmas; la clave pública correspondiente permite comprobarlas. La firma vincula una autorización a un mensaje concreto según el algoritmo y sus reglas. No oculta el contenido firmado. En Bitcoin, una firma válida es una parte de las condiciones necesarias para gastar una salida.

El cifrado busca que un contenido solo pueda leerse con la capacidad adecuada. El cifrado autenticado añade detección de alteraciones. En el ecosistema Cuvex hay criptogramas que protegen secretos, transacciones firmadas que autorizan gastos y canales cifrados que transportan mensajes. No son objetos equivalentes aunque todos usen criptografía.

Una contraseña humana suele pasar por una función de derivación antes de usarse como clave criptográfica. «AES-256» describe el algoritmo y tamaño de clave, pero no convierte una contraseña predecible en una elección fuerte. La generación, implementación, almacenamiento, pantalla y recuperación forman parte de la seguridad total.

Tampoco se deduce que un QR sea seguro porque parezca complejo. Hay que conocer qué contiene, quién lo produjo y qué va a hacer la aplicación con él. Antes de aceptar una acción, pide al tutor que explique su finalidad sin solicitar el dato privado.

Práctica

1. Asocia «detectar cambio de archivo», «ocultar una semilla» y «autorizar un pago» con hash, cifrado y firma.
2. Cambia una letra de un texto ficticio y observa que su hash cambia; no uses secretos para esta demostración.
3. Explica por qué una transacción puede ser pública y estar firmada a la vez.

Demuestra

Puedes describir qué garantía buscas y qué mecanismo la aporta, sin usar «encriptado» como sinónimo de todo lo seguro.

Duda frecuente

¿Un hash de firmware certifica que no tiene fallos? No. Identifica bytes si la referencia es fiable. Una auditoría, una firma de fabricante y una prueba física responden a preguntas diferentes.

Punto de pausa

Guarda las tres correspondencias del ejercicio.

¿Cuál de estos mecanismos oculta el contenido de un secreto?

1. Publicar su nombre de archivo.
2. Firmarlo sin cifrarlo.
3. Cifrarlo correctamente con una clave protegida.

> **Ver respuesta: Cifrarlo correctamente con una clave protegida.**
> La confidencialidad no la proporcionan por sí solas una firma o una huella.

M03

Semilla passphrase y contraseña

Objetivo

Evitar la confusión entre las distintas credenciales del sistema.

Comprender

Una mnemónica BIP39 representa entropía y una suma de comprobación mediante palabras de un diccionario. Las longitudes estándar son 12, 15, 18, 21 o 24 palabras. Elegir una frase memorable, una letra de canción o palabras al azar humano no reproduce una generación segura. La suma de comprobación detecta algunos errores; no demuestra quién creó la semilla ni que nadie más la conozca.

La passphrase BIP39 participa en la derivación de la semilla binaria. Una passphrase diferente puede abrir una cartera completamente diferente y aparentemente vacía. No existe necesariamente un mensaje «passphrase equivocada». No es obligatorio que sea una palabra del diccionario ni es literalmente una vigesimoquinta palabra.

La contraseña del criptograma Cuvex protege el secreto almacenado. La contraseña de Desk protege el almacén local del ordenador. El PIN de enlace autoriza una sesión de comunicación. La Clave Chat recupera una identidad de mensajería. Ninguno de ellos debe confundirse con la semilla, y conocer uno no implica poder reconstruir todos los demás.

Guardar semilla y passphrase juntas dentro de un criptograma puede facilitar recuperación, pero elimina su separación frente a quien consiga descifrarlo. Separarlas aumenta exigencias para ti y tus herederos. La decisión debe documentarse y probarse; no se toma porque el tutor considere una opción «más avanzada».

Práctica

1. Crea cinco tarjetas de papel sin valores secretos: semilla, passphrase, contraseña Cuvex, contraseña Desk y Clave Chat.
2. Escribe qué recupera cada una y qué perderías al olvidarla.
3. Diseña una prueba en una cartera vacía. La introducción de palabras y passphrase se hace en privado; al tutor solo se le informa del resultado.

Demuestra

Explica por qué el curso nunca debe pedir una contraseña para «validar» tu aprendizaje. Identifica qué secreto exige tu procedimiento de recuperación.

Duda frecuente

¿Puedo restablecer la passphrase mediante mi email? No existe ese mecanismo en BIP39. Un proveedor custodial puede tener recuperación de cuenta, pero es otro modelo.

Punto de pausa

Registra «credenciales diferenciadas», sin escribir sus valores.

Cambias una letra de una passphrase BIP39 y ves saldo cero. ¿Qué interpretación es correcta?

1. Puede ser otra cartera válida derivada de otra passphrase.
2. La red ha borrado tus fondos.
3. Desk debe adivinar la passphrase original.

> **Ver respuesta: Puede ser otra cartera válida derivada de otra passphrase.**
> Una passphrase distinta puede producir otra cartera sin señalar un error.

M03

Derivación xpub y descriptores

Objetivo

Comprender cómo se describe una cartera sin entregar capacidad de gasto.

Comprender

Una cartera jerárquica deriva muchas claves desde una raíz. Una ruta indica qué rama se utiliza. En mainnet, BIP84 suele emplear m/84'/0'/0' para la primera cuenta SegWit monofirma; BIP48 P2WSH usa m/48'/0'/0'/2' en la primera cuenta multifirma. La comilla indica derivación endurecida. Cambiar cuenta, red o tipo de script puede dar otras direcciones desde la misma mnemónica.

Una xpub es una clave pública extendida que permite derivar determinadas claves públicas descendientes. No es una contraseña de gasto, pero puede permitir observar una familia de direcciones. La huella maestra es un identificador corto útil para relacionar registros; no garantiza identidad por sí sola ni evita colisiones.

Un descriptor expresa cómo construir scripts y direcciones: tipo de script, claves, orígenes y derivaciones. Un descriptor watch-only con claves públicas permite observar, no firmar. La palabra «descriptor» no garantiza que solo contenga información pública: algunos formatos pueden incluir claves privadas. Nunca subas un descriptor real al curso.

Para recuperar una multifirma suele hacer falta la política completa, no solo las palabras de uno de los firmantes. Conserva umbral, participantes, xpubs, rutas, red, tipo de script y datos de descubrimiento. La suma de comprobación del descriptor ayuda a detectar errores de transcripción; no autentica a sus participantes.

Práctica

1. Lee una ruta ficticia y explica propósito, moneda, cuenta y rama. No introduzcas claves reales.
2. Distingue dirección de recepción, xpub de participante y descriptor completo.
3. Prepara una ficha privada de recuperación con nombres de campos vacíos y ubicación documental separada.

Demuestra

Puedes explicar por qué una wallet vacía tras restaurar no prueba pérdida: hay que comprobar red, passphrase, script, cuenta, ruta y descubrimiento.

Duda frecuente

¿Una xpub se puede publicar sin consecuencias? No concede por sí sola capacidad normal de gastar, pero expone privacidad y puede aumentar otros riesgos en combinaciones criptográficas particulares.

Punto de pausa

Guarda la ficha sin valores sensibles en el curso.

¿Qué información puede faltar al intentar recuperar una multifirma únicamente con una semilla?

1. El color del dispositivo.
2. La política y las claves públicas de los demás participantes.
3. La contraseña de una red social.

> **Ver respuesta: La política y las claves públicas de los demás participantes.**
> La reconstrucción de scripts exige la política completa, además del umbral de claves privadas.

M03

Elegir una wallet y un modelo de custodia

Objetivo

Comparar herramientas por funciones, confianza y recuperación.

Comprender

Una wallet es un conjunto de herramientas para describir, observar y, cuando corresponde, autorizar gastos. Una wallet caliente mantiene capacidad de firma en un entorno conectado. Un firmante aislado intenta separar los secretos del equipo que consulta la red. Una wallet watch-only conserva información pública suficiente para observar y preparar, pero necesita otro sistema para firmar.

En custodia de terceros, una cuenta puede representar un derecho frente a una empresa. En autocustodia tú mantienes la capacidad técnica de gasto, de forma individual o compartida. La recuperación mediante email y el poder de bloquear una retirada suelen reflejar el primer modelo. No debes evaluar ambas opciones con el mismo supuesto de responsabilidad.

Compara soporte de red y script, verificación en pantalla, copias, actualización, interoperabilidad, mantenimiento, consultas a proveedores y claridad de errores. Una lista de monedas o un acabado físico no bastan. Un dispositivo de firma tampoco evita que aceptes una dirección errónea si no la revisas.

Cuvex separa secretos protegidos en criptogramas de la organización y consulta en Desk. Este modelo requiere conservar el criptograma y sus medios de desbloqueo. La protección contra pérdida del dispositivo no implica recuperación si desaparecen también todas las copias o contraseñas. Aprende el proceso completo antes de trasladar patrimonio.

Práctica

1. Compara Cuvex con una wallet caliente y un exchange en una matriz: quién firma, quién ve consultas, quién puede recuperar acceso y qué sucede al cerrar la empresa.
2. Escoge dos criterios que debas verificar con evidencia y no con publicidad.
3. Comprueba que el entorno de prácticas no comparte claves con tu ahorro real.

Demuestra

Justifica una elección para un caso concreto sin declarar una herramienta invulnerable.

Duda frecuente

¿Una hardware wallet hace privadas todas las transacciones? No. Protege principalmente la capacidad de firma y parte de la revisión; la cadena, las consultas y las contrapartes siguen generando información.

Punto de pausa

Guarda tu matriz de criterios sin nombres de cuentas.

¿Qué puede hacer una wallet watch-only correctamente configurada con claves públicas?

1. Observar y preparar operaciones sin poder firmarlas por sí sola.
2. Cambiar una semilla perdida.
3. Garantizar anonimato.

> **Ver respuesta: Observar y preparar operaciones sin poder firmarlas por sí sola.**
> Observar y autorizar son capacidades separables.

M03

Backups que se pueden recuperar

Objetivo

Diseñar una copia completa y demostrar recuperación antes de depender de ella.

Comprender

Un backup útil recupera una capacidad, no simplemente un archivo. Para una monofirma puede requerir mnemónica, passphrase y datos de derivación. Para una multifirma exige además política y suficientes firmantes. Para Desk puede hacer falta una copia cifrada y su contraseña. Para el chat, recuperar identidad no equivale a recuperar mensajes históricos.

La redundancia protege frente a pérdida accidental; la separación protege frente a compromiso conjunto. Dos copias en distintos soportes y lugares pueden reducir fallos correlacionados. Cada copia adicional también necesita control de acceso, inventario y revisión. Los nombres de archivo y etiquetas no deben revelar patrimonio ni facilitar localizar todos los componentes.

Una prueba debe confirmar una dirección previamente verificada y, en un entorno de aprendizaje, la capacidad de firmar una operación controlada. Ver que el archivo abre no demuestra que pertenezca a la cartera correcta. Tampoco compruebes una copia introduciendo tu semilla de producción en un ordenador cualquiera.

Documenta qué cubre y qué excluye cada copia. Cambiar la contraseña actual no modifica automáticamente las copias antiguas. Si una contraseña anterior se expuso, esos respaldos siguen afectados. Borrar un archivo en almacenamiento moderno tampoco garantiza eliminar todas sus copias o versiones.

Práctica

1. Completa una tabla privada: objeto, contenido, contraseña asociada, ubicación independiente, fecha de prueba y responsable.
2. Restaura una copia de aprendizaje en un entorno separado. Verifica red, primera dirección y derivación.
3. Simula la pérdida del ordenador y después la del dispositivo. Identifica qué procedimiento cambia.

Demuestra

Puedes recuperar tu escenario de pruebas sin ayuda improvisada y explicar qué información seguiría faltando para otro escenario.

Duda frecuente

¿La copia global de Desk es una copia de todo? No debe asumirse. En la base revisada, historial y sesiones de chat no están incluidos. La política multifirma y las claves privadas tienen funciones distintas.

Punto de pausa

Registra fecha y resultado de la prueba; nunca el contenido de la copia.

Cambias la contraseña de Desk. ¿Qué ocurre con una copia anterior?

1. Se actualiza sola.
2. Pierde automáticamente su cifrado.
3. Conserva la protección y contraseña con las que fue creada.

> **Ver respuesta: Conserva la protección y contraseña con las que fue creada.**
> Las copias anteriores son objetos independientes.

M04

Conocer Original y BIT

Objetivo

Elegir el recorrido correcto según el dispositivo y su versión.

Comprender

Original utiliza tarjetas NFC para transportar criptogramas y operaciones compatibles; Bluetooth interviene en su actualización. Su USB-C se utiliza como alimentación en el modelo documentado. BIT utiliza USB-C con intercambio de archivos y añade biometría para los criptogramas que la requieren. No traslades instrucciones NFC o Bluetooth de Original a BIT.

En el dispositivo encontrarás funciones para cifrar, descifrar, crear carteras y firmar, además de ajustes. Original incorpora clonado de tarjetas; BIT trabaja con archivos del soporte USB. Los rótulos, idiomas y accesos pueden variar por versión. El nuevo acceso «Verificar políticas» en BIT conduce al flujo compatible y no cambia quién autoriza.

La referencia editorial revisada es Original 1.2.2 Final, BIT 1.2.3 Final, Desk beta.9.21 y Mirror beta.12.12. Son referencias de fuentes: la firma, distribución y aceptación física de cada combinación deben verificarse con el equipo. No sustituyas tu firmware por un binario sin firma incluido en un paquete de ingeniería.

Antes de usar un equipo revisa procedencia, precintos, aspecto y versión. La trazabilidad y una firma de actualización ayudan con amenazas concretas, pero no sustituyen todas las comprobaciones. Si observas manipulación o una versión inesperada, pausa la inicialización y consulta soporte por un canal que hayas verificado.

Práctica

1. Identifica tu modelo y registra versión visible sin fotografiar secretos.
2. Localiza cifrar, descifrar, crear wallet, PSBT y ajustes. No inicies un borrado ni una actualización para explorar menús.
3. Elige la rama Original o BIT en el curso. Mantén esa selección durante la práctica.

Demuestra

Explica cómo entra y sale una operación de tu modelo y qué soporte debes proteger de sobrescrituras.

Duda frecuente

¿BIT es automáticamente más seguro para cualquier persona? Los modelos ofrecen decisiones operativas distintas. La respuesta depende de amenazas, recuperación y uso correcto.

Punto de pausa

Guarda modelo y versión en tu cuaderno local; el curso solo necesita el modelo elegido.

Tienes un BIT y una guía te exige escribir una tarjeta NFC con el propio dispositivo. ¿Qué haces?

1. Compruebo que la guía corresponde a mi modelo y uso el flujo USB compatible.
2. Fuerzo la actualización de Original.
3. Envío la semilla al teléfono.

> **Ver respuesta: Compruebo que la guía corresponde a mi modelo y uso el flujo USB compatible.**
> Las instrucciones deben corresponder al transporte real del modelo.

Crear una semilla con entropía física

Objetivo

Entender la generación y ensayar el flujo sin convertir datos del curso en claves propias.

Comprender

La entropía es imprevisibilidad. Unos dados pueden aportar entropía si son adecuados, el orden se fija antes de lanzar y el algoritmo de conversión es correcto. Los resultados que rechaza un procedimiento deben repetirse exactamente como indique; sustituirlos por el número máximo o escoger otra palabra introduce sesgos.

El flujo Cuvex revisado combina una moneda y cuatro dados. Su función de conversión calcula moneda × 1.296 más el número formado en base seis por cada dado menos uno; admite índices de 0 a 2.047. Si el resultado cae fuera del diccionario, hay que repetir la moneda y los cuatro dados. Mantener la moneda y repetir solo los dados introduce sesgo. Esto describe el fuente revisado; la pantalla y el recorrido completo se validan en cada firmware distribuido.

No es equivalente a escoger palabras favoritas. No conviertas una demostración pública en material para custodiar dinero. Cualquier semilla que aparezca en material didáctico se considera conocida. La palabra final y su comprobación deben producirse mediante el algoritmo completo del dispositivo, sin completar una mnemónica a mano.

Prepara un espacio sin cámaras, asistentes de voz activos cerca, grabación de pantalla ni personas observando. El tutor debe detenerse durante la entrada y revisión del secreto. Puede explicar antes y evaluar después mediante preguntas sobre el proceso, sin escuchar los resultados de los lanzamientos ni las palabras.

Tras generar, hay que comprobar el respaldo, cifrarlo según el modelo y probar la recuperación de una cartera vacía. Una dirección de verificación ayuda a confirmar consistencia sin exponer la semilla al ordenador. Si el flujo acepta valores que contradicen las instrucciones o muestra palabras inesperadas, detén el uso y registra solo versión, pantalla y error.

Práctica

1. En el ensayo, sigue los pasos del dispositivo con material sin fondos. Fija el orden de los dados y no cambies resultados.

2. Repite las entradas rechazadas según la pantalla, sin corregirlas para que encajen.
3. Revisa en privado el contenido, crea copia y confirma que puedes reconstruir la misma cartera de aprendizaje.

Demuestra

Explica por qué entropía física, conversión correcta y secreto del resultado son tres requisitos distintos.

Duda frecuente

¿Puedo contar mis tiradas a la IA para que compruebe el algoritmo? No para una semilla que vayas a utilizar. La asistencia trabaja con ejemplos sintéticos diferentes.

Punto de pausa

Finaliza en un estado seguro del dispositivo; no dejes una semilla visible durante el descanso.

El firmware rechaza una entrada de dados. ¿Qué acción respeta el procedimiento?

1. Elegir manualmente una palabra.
2. Repetir según la indicación del dispositivo sin sesgar el resultado.
3. Reducir el número hasta que se acepte.

> **Ver respuesta: Repetir según la indicación del dispositivo sin sesgar el resultado.**
> Los rechazos son parte de la conversión de entropía y no deben sustituirse arbitrariamente.

M04

Cifrar y descifrar un secreto con Cuvex

Objetivo

Crear un criptograma de aprendizaje y verificar su recuperación.

Comprender

Elige el tipo de contenido correcto: BIP39, SLIP39, Monero o texto cuando esté disponible en tu flujo. Son formatos diferentes. Cifrar un texto SLIP39 no convierte Cuvex en un firmante de todas las redes que puedan usar ese texto. Almacenar secretos y ejecutar protocolos de firma tienen alcances distintos.

Introduce el contenido directamente en el dispositivo cuando busques mantenerlo fuera de equipos conectados. Un método de importación desde teléfono o PC puede haber expuesto ya el secreto en origen, aunque después quede cifrado. La pantalla de revisión previa es el lugar para detectar palabras, orden, mayúsculas y campos equivocados.

La contraseña del criptograma debe ser larga, única y recuperable de acuerdo con tu plan. El teclado de creación revisado tiene capacidad para 40 caracteres y el validador exige al menos 12, mayúscula y minúscula ASCII, número y símbolo reconocido. No apliques automáticamente los 12 a 1.024 caracteres de Desk al teclado de Cuvex: Desk aplica una política distinta. Otros campos de recuperación pueden tener límites diferentes; comprueba el flujo y la versión.

En Original escribe en una tarjeta adecuada y vacía; mantén la posición hasta recibir la confirmación. En BIT conserva los archivos que produzca el flujo USB, incluidos componentes biométricos necesarios cuando proceda. No renombres ni combines archivos por intuición. Después realiza una lectura y descifrado de prueba en el dispositivo, sin comunicar el secreto al tutor.

Práctica

1. Cifra un texto didáctico creado para esta práctica, sin credenciales ni valor económico.
2. Identifica el soporte y el objeto resultante; anota en privado el alias y su función.
3. Reinicia el proceso de descifrado, verifica el texto en la pantalla de confianza y cierra la visualización al terminar.

Demuestra

Puedes distinguir contenido correcto, escritura correcta y recuperación correcta. El mensaje «archivo copiado» no prueba los tres.

Duda frecuente

¿El alias de la tarjeta es una contraseña? No. Es información organizativa. Evita incluir saldos o descripciones que faciliten identificar tu patrimonio.

Punto de pausa

No dejes contenido descifrado visible. Registra solo el éxito o fallo del ensayo.

¿Qué demuestra mejor que un criptograma de prueba sirve para recuperar su contenido?

1. Que tenga un nombre bonito.
2. Que el archivo exista en dos carpetas.
3. Leerlo y descifrarlo por el flujo correcto y comprobar el contenido en privado.

> **Ver respuesta: Leerlo y descifrarlo por el flujo correcto y comprobar el contenido en privado.**
> La existencia de una copia no prueba su utilidad ni su correspondencia.

M04

Umbrales de cifrado y biometría

Objetivo

Separar la protección compartida del secreto de la multifirma de Bitcoin.

Comprender

Un criptograma protegido por varias contraseñas regula quién puede descifrar el contenido. Una cartera Bitcoin multifirma regula qué claves deben autorizar un gasto en la red. Puedes tener un secreto cifrado de forma compartida que corresponda a una cartera monofirma, o cada firmante de una multifirma con su propio criptograma individual.

Si varias personas desbloquean conjuntamente una sola semilla y esa semilla permite gastar sola, el umbral de la cadena sigue siendo de una clave. Una vez revelada, alguien podría conservarla. No describas ese esquema como si obligara a coordinar varias firmas para cada pago.

La biometría de BIT añade una condición de acceso en los formatos que la utilizan. Un dedo no es una semilla ni un reemplazo universal de la contraseña. Planifica lesiones, cambios de huella, avería, disponibilidad del equipo y herencia. Conserva y prueba la vía de recuperación documentada de ese criptograma antes de depender de ella.

Una exportación de recuperación puede revelar el secreto en un ordenador, precisamente para resolver una emergencia. La existencia de esa función no convierte el PC en un entorno equivalente al dispositivo. La práctica normal debe mantener el aislamiento; la recuperación local se estudia de forma consciente y con un plan posterior de migración si hubo exposición.

Práctica

1. Dibuja dos políticas: «dos contraseñas para abrir una semilla» y «dos claves de tres para gastar».
2. En una prueba sin fondos, identifica qué archivos requiere una copia biométrica y dónde se comprueba su recuperación.
3. Simula que una persona no está disponible. Determina si el umbral de tu esquema permite continuar.

Demuestra

Puedes explicar quién puede conocer el secreto y quién puede autorizar un gasto después de descifrarlo.

Duda frecuente

¿Puedo retirar a un participante cambiando una etiqueta? No. Debes distinguir cambios de organización de una nueva protección del secreto y de una nueva política de gasto.

Punto de pausa

Guarda el esquema sin nombres reales ni datos biométricos.

Tres personas abren con dos contraseñas un criptograma que contiene una única semilla monofirma. ¿Cuántas claves exige Bitcoin para gastar?

1. Una, si esa es la política de la cartera.
2. Dos porque el archivo tenía dos contraseñas obligatorias.
3. Tres por el número de personas.

> **Ver respuesta: Una, si esa es la política de la cartera.**
> El umbral del cifrado no altera el script que controla las monedas.

M04

Clonar conservar y verificar copias

Objetivo

Construir redundancia sin destruir la única copia válida.

Comprender

Clonar un criptograma copia datos cifrados; no crea un saldo nuevo, otra semilla o independencia frente a una contraseña expuesta. Las copias idénticas resuelven pérdida de soporte, no compromiso del secreto original. Por eso una restauración y una migración a nuevas claves responden a situaciones diferentes.

En Original distingue tarjeta de criptograma y tarjeta de transporte PSBT. Un soporte de operaciones se puede reutilizar conforme al flujo; una tarjeta con tu respaldo no debe convertirse en ese soporte. Si una operación rechaza una tarjeta que contiene un criptograma, no intentes saltarte la protección ni borrar a mano su cabecera.

En BIT una copia debe conservar el conjunto necesario y la relación entre archivos. Un gestor de archivos puede mostrar una transferencia completa sin garantizar que el dispositivo haya validado contenido o terminado su operación. Espera los estados indicados y comprueba una copia mediante recuperación controlada.

Mantén un inventario privado con identificadores discretos, versión de formato, fecha y resultado de última prueba. Separa al menos dos copias frente a los incidentes que has definido. Evita subir respaldos a canales de soporte para diagnosticar problemas; facilita metadatos depurados y códigos de error.

Práctica

1. Crea una copia de tu criptograma didáctico en otro soporte mediante el flujo correcto.
2. Desconecta el soporte original y recupera el texto de prueba desde la copia.
3. Documenta qué harías ante pérdida, daño de archivo y exposición de contraseña. No son el mismo procedimiento.

Demuestra

Puedes identificar la copia que has probado y explicar por qué no se ha sobrescrito la original.

Duda frecuente

¿Puedo borrar el original después de ver un segundo archivo? Primero verifica recuperación y cobertura. La eliminación debe responder a un plan, no al simple número de copias.

Punto de pausa

Guarda los soportes antes de cerrar la sesión; no dejes tarjetas mezcladas con las de pruebas de pago.

Si alguien conoce la contraseña y obtiene una copia del criptograma, ¿qué resuelve hacer tres clones más?

1. Revoca la copia del atacante.
2. Aporta redundancia, pero no revoca ese acceso.
3. Cambia automáticamente la semilla de Bitcoin.

> **Ver respuesta: Aporta redundancia, pero no revoca ese acceso.**
> La duplicación no elimina un compromiso existente.

M05

Instalar y proteger Cuvex Desk

Objetivo

Abrir una instalación de procedencia verificada y proteger su almacén local.

Comprender

Selecciona el paquete de tu sistema y arquitectura: macOS Intel o Apple Silicon, Windows x64 o ARM64 y Linux x64 o ARM64 según la distribución disponible. Un ZIP de fuentes, un paquete para el Manager y un instalador para el cliente son entregas diferentes. El curso no debe dirigir a un alumno a un paquete privado de firma.

Comprueba procedencia y las verificaciones del sistema. Una firma de ingeniería de Windows no aporta por sí sola confianza pública del editor. En Mac, firma de aplicación, notarización y evaluación al abrir son controles distintos. No desactives protecciones generales siguiendo una llamada de supuesto soporte. Si una versión da un aviso inesperado, conserva el texto y utiliza el canal oficial.

Desk crea un almacén local cifrado con contraseña. En la base revisada, las nuevas contraseñas admiten de 12 a 1.024 caracteres; la coincidencia de campos se exige donde hay confirmación. Esos límites no son una medida de calidad suficiente: usa una frase única y evita reutilización. La biometría del ordenador, cuando está disponible, es una comodidad de acceso que requiere su propia configuración.

Configura bloqueo por inactividad y, si procede, al pasar a segundo plano. El retraso tras fallos y el borrado opcional se estudian en el manual: no actives un borrado automático durante una demostración. La app puede funcionar sin una cuenta convencional de usuario, pero sus servicios de consulta, chat o descargas tienen requisitos y comunicaciones específicos.

Práctica

1. Verifica plataforma, versión visible y procedencia del paquete sin aportar al tutor identificadores privados.
2. Crea un almacén de aprendizaje y comprueba bloqueo y reapertura. Introduce la contraseña en privado.
3. Programa una copia cifrada y conserva su contraseña según tu plan. No pruebes bloqueos repetidos en el entorno real.

Demuestra

Puedes diferenciar contraseña local, cuenta comercial y credenciales de los servicios que añadas.

Duda frecuente

¿Cambiar la contraseña de Desk cambia la de mis tarjetas? No. Son protecciones independientes. Las copias antiguas tampoco cambian solas.

Punto de pausa

Bloquea Desk y guarda el identificador de lección, sin credenciales.

El instalador no corresponde a tu arquitectura. ¿Cuál es el primer paso?

1. Forzar su ejecución desactivando protecciones.
2. Conseguir el paquete oficial adecuado y comprobar sus requisitos.
3. Importar la semilla en una web para continuar.

> **Ver respuesta: Conseguir el paquete oficial adecuado y comprobar sus requisitos.**
> La compatibilidad y procedencia se resuelven antes de usar material de custodia.

M05

Vincular criptogramas y organizar WOW

Objetivo

Vincular una copia cifrada y distinguirla de una cuenta de observación.

Comprender

Desk organiza criptogramas vinculados por NFC, USB o archivo de copia compatible. Un diseño visual y un alias ayudan a reconocerlos, pero no son prueba criptográfica de identidad. En la ficha puedes consultar origen y propiedades interpretadas por la app, como formato, tamaño y características de acceso.

Vincular importa u organiza el objeto compatible; no significa descifrarlo en el PC ni comprobar su secreto. WOW es una cartera de observación asociada mediante información pública compatible. Un mismo conjunto de secretos puede tener distintas cuentas o derivaciones: la asociación debe corresponder a la cartera que pretendes gestionar.

Activa o importa la cuenta con el descriptor o información pública exportada por el flujo del dispositivo. Revisa red, tipo de script, huella, ruta y dirección de control. El nombre de la cuenta es organizativo; el identificador derivado de un nombre no debe tratarse como anonimización fuerte, porque un nombre predecible se puede adivinar.

En la base de Desk se conservan cuentas pendientes de asociación y funciones para exportar copias, clonar y eliminar registros locales. Borrar una tarjeta de la interfaz no destruye las copias externas ni mueve los fondos. «No hay backup» significa que la aplicación no acredita una copia bajo su criterio, no que ningún respaldo exista en el mundo.

Práctica

1. Vincula el criptograma didáctico por el transporte elegido y revisa su ficha.
2. Importa una cuenta de aprendizaje compatible y comprueba su red y dirección de verificación sin mostrar claves al tutor.
3. Distingue el registro del criptograma, la cuenta WOW y el soporte físico. Identifica qué desaparecería con una eliminación local.

Demuestra

Puedes explicar qué datos necesita Desk para observar y cuáles deben seguir fuera del ordenador durante el uso habitual.

Duda frecuente

¿Vincular un archivo .bin garantiza que sea mi semilla? No. Debes verificar su procedencia y recuperación. Una extensión de archivo no certifica contenido.

Punto de pausa

Conserva únicamente el estado «vinculación de prueba verificada».

Eliminar una cuenta WOW localmente, ¿mueve sus bitcoins?

1. No; elimina información local según el flujo, no gasta las UTXOs.
2. Sí; los envía al fabricante.
3. Cancela cualquier firma que otra persona conserve.

> **Ver respuesta: No; elimina información local según el flujo, no gasta las UTXOs.**
> Estado local y estado de la cadena son distintos.

M05

Enlazar Mirror con Desk

Objetivo

Establecer y terminar un enlace local autorizado sin confundir sus códigos.

Comprender

Mirror permite operaciones locales con Desk mediante el flujo de enlace, PIN y QR que presentan las aplicaciones. El PIN de seis cifras pertenece a esa sesión. No es la contraseña de Desk, la del criptograma ni una palabra de recuperación. Comprueba qué pantalla lo genera y dónde debe introducirse; no uses un código enviado por una persona desconocida.

Inicia la acción desde el contexto correcto de Desk: vincular, leer QR, transportar PSBT o firmware son finalidades distintas. La ventana informa de búsqueda, conexión, descubrimiento, PIN, QR y acción sobre tarjeta o archivo. Que un dispositivo aparezca en la búsqueda no demuestra que la operación completa haya terminado.

Concede permisos relevantes según el sistema: cámara para lectura óptica y Bluetooth o NFC cuando el flujo los requiere. Un teléfono sin una capacidad física necesaria no la obtiene instalando software. En iOS hay diferencias de adaptador y validación; no se debe presentar un proyecto compilable como si ya estuviera distribuido y probado en todos los iPhone.

Si falla, identifica la fase exacta: no aparece, aparece pero no conecta, PIN rechazado, QR ilegible, tarjeta no leída o respuesta no recibida. Cierra sesiones antiguas, verifica versiones compatibles y permisos, y reintenta de forma controlada. Un PIN incorrecto no justifica cambiar firmware o introducir semillas en otro lugar.

Práctica

1. Inicia una lectura de prueba desde Desk y conecta Mirror mediante sus pantallas locales.
2. Comprueba la finalidad antes de presentar un QR o una tarjeta didáctica.
3. Cancela la sesión y confirma que no se aplica después una lectura de un contexto anterior. Reabre una sesión nueva.

Demuestra

Puedes describir la fase fallida y los equipos implicados sin comunicar códigos activos ni contenido sensible.

Duda frecuente

¿Mirror tiene que permanecer conectado siempre? Depende de la operación. No lo trates como un servicio permanente ni supongas que una sesión sigue autorizada tras cerrar o pasar a segundo plano.

Punto de pausa

Cierra la sesión de enlace y bloquea las aplicaciones que no estés usando.

¿Qué debe hacer el tutor si el enlace falla antes de mostrar el PIN?

1. Pedir la semilla.
2. Revisar descubrimiento, permisos, sesión y versiones antes de avanzar.
3. Dar por completada la conexión.

> **Ver respuesta: Revisar descubrimiento, permisos, sesión y versiones antes de avanzar.**
> El diagnóstico debe seguir la fase observada y no inventar una conexión correcta.

NFC mediante Mirror, USB-C y lectura de QR

Objetivo

Utilizar cada transporte conservando su propósito y sus comprobaciones.

Comprender

Los flujos NFC de Cuvex Desktop requieren Cuvex Mirror en un smartphone compatible enlazado por Bluetooth al ordenador. Cuvex Desktop no admite lectores NFC USB externos. También deben ser compatibles la tarjeta, su formato y su capacidad. Una tarjeta pequeña que sirve para un criptograma puede no alojar una PSBT con transacciones anteriores. El límite efectivo depende del contenido completo, no solo de contar destinatarios. No conviertas una tarjeta de respaldo en tarjeta de transporte.

En Original, Mirror puede escribir una solicitud en una tarjeta de operaciones; el dispositivo la procesa y escribe una respuesta que Mirror devuelve a Desk. La confirmación de escritura no significa recepción de Desk. Mantén la tarjeta estable hasta que el equipo indique el resultado. Si el sistema protege un criptograma reconocido, respeta ese rechazo.

BIT utiliza un volumen o carpeta USB de intercambio. El proceso puede desmontar o volver a presentar el volumen. Desk debe seleccionar el soporte correcto, validar la respuesta y realizar el acuse previsto. Copiar un archivo a una carpeta del PC con el mismo nombre no equivale a entregarlo al dispositivo.

Una cámara que no lee un QR puede fallar por enfoque, reflejo, tamaño, movimiento o densidad. Amplía el dato y mejora luz y distancia. No sustituyas un identificador largo por sus primeras letras ni aceptes una transcripción parcial. La lectura exitosa es solo el comienzo de su validación semántica.

Práctica

1. Con material didáctico identifica solicitud, soporte y respuesta para Original y BIT en el diagrama.
2. Prueba cancelar una lectura QR sin guardar valores tardíos. Repite con otra finalidad.
3. Simula un archivo demasiado grande y explica por qué se debe reducir complejidad de la operación o elegir un medio compatible, sin quitar validaciones.

Demuestra

Puedes indicar qué equipo ha confirmado qué etapa: lectura, escritura, validación, recepción o acuse.

Duda frecuente

¿Un hash o un OK de copia demuestra que el destinatario Bitcoin es correcto? No. Debes revisar la operación y sus salidas en el firmante.

Punto de pausa

Retira y guarda tarjetas de respaldo; deja identificado el soporte de transporte.

Original dice que escribió la respuesta en la tarjeta. ¿Qué falta antes de afirmar que Desk la recibió?

1. Pintar la tarjeta de otro color.
2. Crear una semilla nueva.
3. Leer la respuesta y validarla en Desk por el flujo correspondiente.

> **Ver respuesta: Leer la respuesta y validarla en Desk por el flujo correspondiente.**
> El éxito de escritura y el éxito de recepción son eventos diferentes.

Proveedores públicos y nodo propio

Objetivo

Elegir una fuente de consulta y comprender sus fugas y límites.

Comprender

Desk puede consultar proveedores públicos compatibles o un Bitcoin Core configurado por el usuario. Un proveedor puede conocer las consultas que recibe, su secuencia y datos de conexión. No enviar una xpub completa reduce una exposición concreta, pero los scripts o sus hashes también pueden vincularse entre sí.

En Desk 9.21 aparece la elección explícita de Blockstream Electrum por TLS además de alternativas REST y nodo propio. TLS protege el canal frente a ciertos observadores de red; el propio proveedor sigue recibiendo las consultas. No hay una rotación silenciosa que garantice anonimato. La elección exige comprender ese intercambio de privacidad por comodidad.

Para Core configura endpoint, autenticación y wallet de observación según la guía correspondiente. No publiques el puerto RPC ni lo dejes expuesto a Internet para que la app «lo vea». Limita acceso a entornos de confianza y utiliza un transporte protegido apropiado. Una contraseña RPC no se dicta al tutor.

La sincronización inicial y un rescan pueden tardar. El progreso debe interpretarse como estado de trabajo, no como éxito anticipado. Desk conserva trabajo en segundo plano; cerrar la vista no equivale a detener el nodo. La ventana mínima histórica documentada no garantiza descubrir actividad anterior: si tu cartera es más antigua, comprueba la fecha de importación y el alcance real del escaneo.

Descubrimiento se basa en historial, no en saldo positivo. Una dirección gastada hasta cero sigue siendo usada. En multifirma revisada, se aplica un hueco de 20 direcciones consecutivas sin historial por rama y participante, con límites de emisión. No extrapoles un límite global a todas las carteras.

Práctica

1. Selecciona una fuente de aprendizaje y explica qué información puede ver.
2. Revisa fecha de última sincronización, red y progreso. Si hay HTTP 429, respeta la pausa y no cambies de proveedor sin decidirlo.
3. Simula una wallet con saldo cero e historial antiguo. Comprueba por qué «cero» y «sin usar» son diferentes.

Demuestra

Puedes decidir si tu fuente cubre tu necesidad de verificación y privacidad, y reconocer un estado incompleto.

Duda frecuente

¿Un nodo propio me hace anónimo? No. Reduce dependencias de consulta, pero debes considerar conexión, contrapartes, publicación y demás metadatos.

Punto de pausa

Registra solo tipo de proveedor y necesidad de completar el escaneo.

Una dirección tiene saldo cero pero recibió y gastó fondos. Para descubrir la cartera, ¿cómo debe tratarse?

1. Como dirección con historial.
2. Como dirección nunca utilizada.
3. Como dirección inválida.

> **Ver respuesta: Como dirección con historial.**
> El historial, no el saldo actual, determina si fue usada.

Recibir bitcoin y comprobar la dirección

Objetivo

Crear una solicitud de recepción y verificarla antes de entregarla.

Comprender

Abre la cuenta WOW correcta y confirma red y política. Genera o recupera una solicitud de recepción. Puedes añadir motivo, observador e importe esperado para tu organización. Esos campos describen tu información local; el importe esperado no impide que alguien envíe otra cantidad.

Verifica la dirección mediante el flujo disponible en el dispositivo y el contexto de cartera. Si ese recorrido todavía no está físicamente validado en tu combinación, la práctica se queda en simulación y se escala antes de recibir fondos importantes. Comparar dos pantallas alimentadas por la misma fuente no aporta una independencia que no exista.

Utiliza una dirección nueva para una nueva relación de cobro cuando el flujo lo permita. En la multifirma revisada, las direcciones ya mostradas no se reasignan ni caducan porque un pagador puede utilizarlas más tarde. Al llegar al límite de nuevas direcciones consecutivas sin historial, recupera la solicitud previa adecuada y comprende el motivo del límite; no rebobines índices.

Tras compartir, observa la entrada en tu fuente de verificación. Un correo, un justificante del exchange o una captura del pagador no demuestran liquidación. Comprueba red, txid, salida, importe y confirmaciones según la exposición. No abras un explorador público con tu dirección por comodidad si tu plan exige mantener esas consultas privadas.

Práctica

1. Genera una solicitud en el laboratorio, revisa cuenta y red y explica cómo verificarías la dirección.
2. Registra una etiqueta ficticia y recupera la misma solicitud después de cerrar la vista.
3. Simula un cobro por importe diferente y decide cómo conciliarlo sin cambiar el historial.

Demuestra

Puedes distinguir dirección generada, dirección verificada, solicitud compartida y cobro confirmado.

Duda frecuente

¿Una dirección vieja deja de funcionar al crear otra? Normalmente no. Conservar el descubrimiento y el registro de solicitudes evita perder visibilidad de pagos tardíos.

Punto de pausa

Guarda el estado de la solicitud de laboratorio, no su contenido en el tutor.

El pagador envía una captura que dice «retirada completada». ¿Qué compruebas para aceptar el cobro?

1. Solo la calidad de la captura.
2. La salida correspondiente en una fuente de red fiable y las confirmaciones necesarias.
3. La contraseña del pagador.

> **Ver respuesta: La salida correspondiente en una fuente de red fiable y las confirmaciones necesarias.**
> Una prueba comercial o una captura no sustituye la verificación del pago.

Etiquetar congelar y seleccionar UTXOs

Objetivo

Preparar entradas sin mezclar orígenes por accidente.

Comprender

Las etiquetas permiten conservar contexto que no figura en la cadena: origen, contraparte, finalidad y restricciones de uso. En Desk una etiqueta de UTXO y una nota de dirección pueden tener longitudes y funciones distintas. Anotar «cliente A» es útil; usar su documento o nombre completo puede crear un registro innecesariamente sensible.

Congelar una UTXO en Desk la excluye de ciertas selecciones locales. No bloquea su gasto en Bitcoin, no cambia el script y no impide que otra app con las claves la utilice. También puede hacer que el saldo total y el saldo gastable sean diferentes. Revisa si una moneda está congelada, reservada por un borrador o realmente gastada.

La selección automática optimiza conforme al algoritmo y su contexto; no conoce necesariamente tus relaciones privadas. Para un pago concreto revisa si conviene usar una salida de ese mismo contexto en vez de unir ahorro, nómina y actividad comercial. La separación útil requiere consistencia futura, no solo etiquetas bonitas.

Exportar etiquetas con formato BIP329 facilita conservarlas o migrarlas. El formato no cifra por sí solo. Desk ofrece envoltorio cifrado para su exportación; distingue el archivo protegido de un texto plano compatible. En la importación, comprueba coincidencia con la cartera y el tratamiento de congelaciones antes de sobrescribir información.

Práctica

1. Etiqueta tres UTXOs sintéticas como ahorro, actividad y donación.
2. Congela una y comprueba la diferencia entre saldo observado y disponible para seleccionar.
3. Exporta etiquetas del laboratorio con contraseña, importa en una copia y revisa resultados sin datos privados reales.

Demuestra

Justifica una selección de entradas por coste y exposición. Reconoce que congelar es una preferencia local.

Duda frecuente

¿Una etiqueta viaja al destinatario al pagar? No por el mero hecho de ser una etiqueta local. Puede filtrarse al exportar, compartir archivos, usar otro servicio o añadirla a un mensaje.

Punto de pausa

Guarda las etiquetas de práctica y el estado de congelación.

¿Qué efecto tiene congelar una UTXO en Desk?

1. Crea un bloqueo de consenso en la red.
2. La transfiere a una cuenta especial.
3. Aplica una restricción local de selección según la app.

> **Ver respuesta: Aplica una restricción local de selección según la app.**
> No revoca la capacidad de otras copias de las claves.

M06

Preparar y revisar un pago

Objetivo

Construir una PSBT comprensible y reconocer todos sus costes y salidas.

Comprender

Selecciona cuenta, entradas gastables, destinatarios e importes. Verifica el origen de la solicitud. Al pegar o escanear, revisa dirección completa y red; el portapapeles y una imagen pueden ser sustituidos. No confíes solo en primeros y últimos caracteres si el procedimiento permite una comprobación completa.

Elige tarifa y revisa comisión absoluta, tamaño estimado, total y cambio. Con «Enviar el total», Desk descuenta la comisión del importe disponible. Si la acción nace del chat y el neto no cubre lo solicitado, un pago parcial debe ser consciente; la solicitud original no se transforma para ocultar la diferencia.

Revisa si hay cambio pequeño o ninguna salida de cambio. Una salida marcada como propia requiere comprobación con la política, no con el nombre que le dé el coordinador. Si el cambio no es viable, revisa el barrido o añade una entrada compatible; no aceptes que se convierta silenciosamente en una comisión desproporcionada.

PSBT es un formato para transportar información y firmas. No contiene necesariamente privacidad ni autenticidad de origen. Puede incluir transacciones anteriores, claves públicas, rutas y metadatos. En los firmwares Final revisados el perfil multifirma usa PSBT v0/BIP174; «transacción versión 2» no significa «PSBT versión 2».

Práctica

1. Construye en el simulador un pago con entrada de 120.000, destinatario de 70.000 y comisión de 1.000 sat.
2. Enumera todas las salidas y explica el cambio de 49.000 sat. Repite con barrido.
3. Cancela el borrador y explica qué has cancelado localmente. No uses este simulador para firmar o publicar nada.

Demuestra

Antes de exportar puedes explicar qué entra, qué sale, quién recibe, cuánto cuesta y qué autorización falta.

Duda frecuente

¿Puedo enviar toda la cantidad que muestra el saldo? Solo si la app calcula un envío neto viable y se cubren comisiones. El saldo puede incluir monedas no disponibles.

Punto de pausa

Guarda un borrador de aprendizaje o cancélalo; nunca una PSBT real en el portal del curso.

Una pantalla indica «transaction version 2». ¿Prueba que el archivo es PSBT v2?

1. No; son campos de versiones diferentes.
2. Sí, siempre.
3. Prueba que usa Taproot.

> **Ver respuesta: No; son campos de versiones diferentes.**
> BIP370 distingue la versión del contenedor de la versión de la transacción.

Firmar con Original y con BIT

Objetivo

Completar cada rama de firma y recibir una respuesta vinculada a la operación correcta.

Comprender

Original: entrega la PSBT mediante la tarjeta de transporte del flujo compatible, con Cuvex Mirror. En el dispositivo lee la solicitud, aporta el criptograma y desbloquéalo en privado. Revisa todas las salidas, importes, cambio y comisión. La respuesta se escribe en la tarjeta; después se lee y valida en Desk. Un éxito en la tarjeta no sustituye este retorno.

BIT: selecciona el volumen correcto y entrega la solicitud por USB-C. El servicio local de Desk atiende el intercambio previsto mientras tú operas el dispositivo. Aporta el criptograma según la pantalla y revisa en BIT. «Recibir del BIT» importa la respuesta; Desk valida y guarda antes de confirmar el acuse. Una desconexión exige recuperar la misma operación, no otra elegida por parecido.

En la firma multifirma de los firmwares Final se revisan resumen y salidas obligatorias, avisos aplicables y las tres confirmaciones finales de «Firmar PSBT». La revisión ampliada opcional permite explorar más parámetros; elegir «No» no elimina las revisiones obligatorias. La verificación independiente de una política es otro recorrido y conserva su alcance de esa revisión.

La firma requiere un criptograma compatible cuya autenticidad pueda verificarse. Una copia histórica que todavía permite recuperar el secreto no queda por ello habilitada para firmar. Si el dispositivo avisa de copia antigua sin autenticidad verificada, sigue el recorrido de recuperar y comprobar el secreto y crear una copia nueva antes de firmar. No alteres cabeceras ni omitas el rechazo.

Si una dirección no coincide, hay una comisión inesperada, faltan datos, aparece otra red o el dispositivo rechaza política, cancela. No conviertas la presión por terminar la llamada en una aprobación. La IA no pulsa botones, no realiza la confirmación final y no declara firmado lo que tú no has verificado.

Práctica

1. Recorre la rama de tu modelo con una cartera sin fondos o un laboratorio físicamente aceptado.
2. Simula detenerte antes de las confirmaciones finales y explica por qué no equivale a autorizar.

3. Comprueba el retorno, la correlación con el borrador y, en BIT, el estado de recepción y acuse.

Demuestra

Puedes narrar el recorrido sin revelar credenciales y distinguir aprobación en el dispositivo, respuesta importada y operación publicada.

Duda frecuente

¿El dispositivo offline sabe que mis entradas siguen sin gastar? No puede comprobar el estado actual de la cadena por sí solo. La app debe verificar la transacción final contra su fuente de red.

Punto de pausa

Si interrumpes la firma, cancela o deja una operación pendiente identificada según el flujo, sin secretos visibles.

BIT firma pero Desk no confirma recepción. ¿Qué estado debes asumir?

1. Pago definitivamente publicado.
2. Respuesta pendiente de recibir o validar; recupera la misma operación.
3. Cartera perdida.

> **Ver respuesta: Respuesta pendiente de recibir o validar; recupera la misma operación.** Firmar, recibir y publicar son etapas distintas.

Finalizar publicar y resolver incidencias

Objetivo

Cerrar el ciclo de pago sin duplicarlo y diagnosticar fallos por etapa.

Comprender

Tras importar una firma, Desk debe verificar que corresponde al borrador y conserva la intención. En multifirma puede faltar el umbral; en monofirma una firma importada tampoco exime de revisión. Finalizar produce la transacción lista para difundir cuando sus condiciones están completas.

Publica solo después de la revisión final. Una respuesta de servidor o un txid indica un resultado de esa solicitud, pero el seguimiento debe confirmar aceptación y cadena. Si la app no recibió respuesta, consulta antes de repetir. No inventes un nuevo pago para resolver un problema de visualización.

Para un pago pendiente, revisa tarifa, validez, conflictos y posibilidad real de RBF. Si hay cambio de política o destinatario, la nueva propuesta requiere nuevas firmas apropiadas. Cancelar localmente no destruye una firma o transacción que ya conserve otra persona; tampoco revoca lo confirmado.

Diagnostica por fases: preparación, transporte, desbloqueo, revisión, firma, retorno, validación, finalización, difusión y confirmación. Registra sistema, versión, modelo, fase, hora aproximada y código de error. Los diagnósticos de la app están diseñados para excluir datos sensibles, pero revísalos antes de compartir y evita adjuntar copias, QR, Clave Chat o credenciales.

Práctica

1. Ordena los estados de un pago ficticio e identifica dónde harías una pausa segura.
2. Resuelve tres incidencias: saldo insuficiente, respuesta USB no recibida y publicación con conexión interrumpida.
3. Redacta un ticket usando datos sintéticos y un resultado esperado comprobable.

Demuestra

Puedes decidir si falta acción del alumno, del dispositivo, del coordinador o de la red, y evitar un segundo pago innecesario.

Duda frecuente

¿Un error FIRMWARE_CAPABILITY_REQUIRED se arregla cambiando el firmware a ciegas? No. En la incidencia documentada de Desk, el reconocimiento del build Final requería corregir el catálogo de Desk. Comprueba versión y perfil antes de modificar equipos.

Punto de pausa

Guarda el estado y siguiente acción. Si publicaste una operación real fuera del laboratorio, conserva su registro en tu documentación privada.

¿Qué acción puede revocar por sí sola una transacción ya confirmada?

1. Borrar el borrador local.
2. Cerrar Mirror.
3. Ninguna de esas acciones.

> **Ver respuesta: Ninguna de esas acciones.**
> La eliminación local no reescribe la cadena ni retira autorizaciones que ya circulan.

M07

Qué se puede observar en Bitcoin

Objetivo

Identificar datos públicos, inferencias y datos que añades fuera de la cadena.

Comprender

Bitcoin on-chain es público: scripts y direcciones representables, valores, relaciones entre entradas y salidas y posición en bloques pueden analizarse. Tu nombre no aparece obligatoriamente, pero una compra identificada, una factura publicada o una dirección compartida pueden vincularte a esa historia.

Pseudonimato significa operar con identificadores que no son por sí mismos tu identidad civil. Anonimato exigiría un conjunto y unas condiciones de indistinguibilidad que no se obtienen simplemente instalando una app. Privacidad es contextual: un comercio conoce tu pago; un exchange puede conocer tu retirada; un servidor conoce consultas; una persona puede observar tus dispositivos.

Distingue hechos e inferencias. «Esta salida se gastó en esa transacción» es verificable en la cadena. «Todas esas entradas pertenecen a la misma persona» es una heurística que puede fallar. La identificación fuera de la cadena puede aumentar la confianza de una hipótesis sin convertir todas las interpretaciones en certezas.

Reutilizar una dirección facilita agregar actividad. Unir UTXOs de contextos distintos puede relacionarlos. Revelar una xpub permite una observación más amplia que enseñar una sola dirección. Compartir un txid puede mostrar también otras salidas y relaciones que el receptor no necesitaba conocer.

Práctica

1. Marca en una transacción ficticia qué datos son públicos y qué etiquetas son tuyas.
2. Añade una factura con nombre y describe qué vínculo nuevo aparece.
3. Redacta una solicitud de soporte que resuelva un error sin incluir dirección, descriptor o saldo.

Demuestra

Puedes decir «esto se observa» o «esto se infiere» y explicar qué evidencia falta.

Duda frecuente

¿Si nunca reutilizo direcciones ya soy anónimo? No. La selección de entradas, el cambio, las consultas, las contrapartes y otros metadatos siguen importando.

Punto de pausa

Guarda un mapa de observadores sin identidades ni transacciones reales.

¿Qué dato suele permitir observar una familia de direcciones de una cuenta?

1. El color del icono.
2. Su xpub y contexto de derivación suficiente.
3. La marca del cable.

> **Ver respuesta: Su xpub y contexto de derivación suficiente.**
> La información pública extendida es sensible para privacidad aunque no autorice gasto por sí sola.

M07

Separar contextos y gestionar el cambio

Objetivo

Tomar decisiones de gasto coherentes con el origen de tus UTXOs.

Comprender

La separación de contextos empieza antes del pago. Decide si una recepción corresponde a ahorro, actividad profesional, gasto cotidiano o una relación concreta. Conserva esa información en etiquetas privadas para que la selección futura no la borre por desconocimiento.

Una etiqueta no separa criptográficamente salidas. Si gastas juntas dos UTXOs de contextos distintos, la transacción publica su relación. Consolidar reduce el número de entradas de futuros pagos, pero aumenta el vínculo entre las salidas consolidadas. Hacerlo con comisiones bajas puede ser eficiente y a la vez contrario a tu objetivo de privacidad.

El cambio es una nueva salida controlada por la misma política, no «dinero invisible». Su posterior uso puede extender relaciones previas. No marques una dirección como cambio porque tenga un importe extraño; en una revisión real el dispositivo debe verificar su pertenencia a la cartera.

Evita convertir la privacidad en patrones mecánicos de importes, tiempos o transferencias repetidas. Esos patrones también pueden ser reconocibles y generar más comisiones. Evalúa qué datos conoce cada parte y qué nueva información publicaría la operación propuesta. Ninguna secuencia borra la historia ya publicada.

Práctica

1. Crea cinco UTXOs ficticias de tres contextos y prepara un pago que use el menor número de contextos necesario.
2. Identifica el cambio resultante y decide cómo etiquetarlo.
3. Compara el coste y la exposición de consolidar todas las salidas frente a mantenerlas separadas.

Demuestra

Puedes justificar una consolidación o rechazarla con un motivo concreto, sin aplicar una regla absoluta para todos los casos.

Duda frecuente

¿Transferir todo a otra dirección mía rompe el historial? No. La transferencia publica una relación adicional y puede añadir coste sin resolver tu amenaza.

Punto de pausa

Conserva el razonamiento del laboratorio y la política de selección elegida.

¿Qué consecuencia puede tener consolidar nómina y donaciones en una sola transacción?

1. Hacer visible una relación entre esas entradas.
2. Borrar su origen público.
3. Convertirlas en efectivo anónimo garantizado.

> **Ver respuesta: Hacer visible una relación entre esas entradas.**
> La reducción de UTXOs puede aumentar vínculos observables.

Privacidad de red Tor y VPN

Objetivo

Separar la privacidad de conexión de la privacidad de la cadena.

Comprender

Un servidor de consulta puede relacionar peticiones con una conexión. Tu proveedor de Internet puede observar destinos o patrones según el transporte. Una VPN desplaza parte de esa confianza al operador de VPN; no elimina la información pública de Bitcoin ni impide que una cuenta identificada te reconozca.

Tor enruta tráfico a través de una red para reducir ciertos vínculos entre origen y destino. No convierte una dirección Bitcoin en privada y no protege una aplicación cuyo tráfico no pasa por Tor. Abrir Tor Browser no configura automáticamente Desk, Bitcoin Core ni todos los servicios del ordenador.

Antes de afirmar que una conexión está protegida hay que comprobar su ruta y configuración. En esta base no se presupone un interruptor Tor integrado en Desk. Un despliegue con nodo o proxy requiere guía de ingeniería y validación del tráfico real. No se inventa un campo de interfaz porque otra wallet lo tenga.

También hay fugas por DNS, sincronización de cuentas, enlaces de explorador y servicios de precio. Un esquema puede proteger las consultas de saldo y seguir revelando actividad al abrir un explorador público. Define el alcance de cada medida y el comportamiento al fallar la conexión; evita cambios silenciosos a un proveedor menos privado.

Práctica

1. Dibuja el recorrido ordenador, proveedor de conexión, proxy si existe, nodo o servicio y red Bitcoin.
2. Señala quién recibe consultas y quién ve tu identidad comercial.
3. Simula que el nodo privado no responde. Decide entre pausar o cambiar explícitamente de fuente con conocimiento de la exposición.

Demuestra

Puedes explicar qué amenaza reduce tu configuración y qué amenaza sigue existiendo.

Duda frecuente

¿Tor garantiza que nadie puede asociar un pago conmigo? No. Contrapartes, identificación comercial, patrones y errores operativos pueden seguir vinculándolo.

Punto de pausa

Registra el alcance del diseño, no endpoints privados ni contraseñas.

Abrir Tor Browser, ¿obliga a Desk a consultar por Tor?

1. Sí, por compartir ordenador.
2. Sí, si el icono está visible.
3. No; debe configurarse y verificarse la ruta de cada aplicación.

> **Ver respuesta: No; debe configurarse y verificarse la ruta de cada aplicación.**
> La protección de una aplicación no se hereda automáticamente a las demás.

CoinJoin Payjoin y límites actuales

Objetivo

Entender herramientas colaborativas sin atribuirles anonimato ni compatibilidad inexistentes.

Comprender

CoinJoin reúne aportaciones de varias personas en una transacción para dificultar ciertas inferencias sobre entradas y salidas. No es sinónimo de entregar monedas a un servicio custodial que promete devolver otras. Diseños distintos exigen revisar coordinación, custodia, comisiones, resistencia a participantes maliciosos y tratamiento posterior.

Payjoin incorpora entradas de pagador y receptor a un pago colaborativo, debilitando algunas heurísticas de propiedad común. Requiere soporte compatible en ambos extremos y un protocolo concreto. Es material de comprensión técnica: no se ha acreditado en los fuentes revisados un flujo Payjoin o CoinJoin integrado y operativo en Cuvex Desk.

La disponibilidad y el contexto jurídico cambian. La documentación de Wasabi registra el cierre del coordinador de zkSNACKs el 1 de junio de 2024; no debe enseñarse un botón histórico como si garantizara hoy un servicio. El Departamento de Justicia estadounidense comunicó en 2025 la declaración de culpabilidad y posteriores condenas de los fundadores de Samourai. Ese caso no permite concluir que toda técnica de privacidad sea ilegal en cualquier jurisdicción.

Una herramienta puede reducir una inferencia y dejar otras intactas. El origen identificado no desaparece de los registros de una contraparte. Las recombinaciones posteriores, metadatos y fallos del conjunto de participantes pueden degradar la privacidad. Además, ciertos servicios pueden aplicar políticas comerciales distintas a monedas con determinadas historias.

Práctica

1. Compara una transacción corriente, una colaborativa y un servicio que recibe custodia, sin ejecutar operaciones reales.
2. Para una herramienta concreta, busca versión, mantenedor, estado del servicio y documentación actual antes de proponer su uso.
3. Identifica riesgos técnicos, de custodia y jurídicos por separado. El tutor no debe diseñar evasión de controles ni prometer «fondos imposibles de rastrear».

Demuestra

Puedes explicar una ventaja limitada y al menos dos riesgos o requisitos de una técnica de privacidad.

Duda frecuente

¿Cuvex necesita un mezclador para servir de custodia privada? No. Control de consultas, datos, claves y selección de UTXOs ya resuelven riesgos concretos, sin prometer ocultación total.

Punto de pausa

Registra una herramienta como «estudiada», no como «compatible» sin evidencia.

¿Qué afirmación es defendible?

1. CoinJoin garantiza anonimato permanente.
2. Una técnica colaborativa puede dificultar ciertas inferencias, con requisitos y límites.
3. Cualquier servicio llamado mixer conserva autocustodia.

> **Ver respuesta: Una técnica colaborativa puede dificultar ciertas inferencias, con requisitos y límites.**
> Las propiedades dependen del protocolo, implementación, participantes y uso posterior.

Lecciones de incidentes reales

Objetivo

Transformar incidentes documentados en decisiones comprobables, sin atacar a competidores ni exagerar protección.

Comprender

Mt. Gox: una acusación del Departamento de Justicia de 2023 describe acceso no autorizado a servidores y claves, y la posterior desaparición de fondos de clientes. Una acusación expresa alegaciones, no una sentencia. La lección de custodia es preguntar quién controla realmente las claves y qué ocurre si falla la empresa.

Ledger Connect Kit, diciembre de 2023: Ledger documentó una publicación maliciosa de una biblioteca utilizada por aplicaciones descentralizadas, tras comprometer acceso de un antiguo empleado. El incidente afectó la cadena de distribución de software y engañó a usuarios de DApps EVM para firmar. No demuestra una ruptura del hardware de Ledger ni del consenso de Bitcoin.

Bybit, febrero de 2025: el FBI atribuyó a Corea del Norte un robo aproximado de 1.500 millones de dólares en activos virtuales. Fue un incidente de un exchange y activos de otras redes; no se presenta como una rotura de la criptografía de Bitcoin. Para el alumno importa verificar la intención de una firma y evitar que varias personas confíen ciegamente en la misma pantalla.

Coinbase, mayo de 2025: la empresa comunicó robo de datos por agentes de soporte sobornados para facilitar ingeniería social. Indicó que no se expusieron contraseñas ni claves privadas. El riesgo educativo es que un estafador conozca datos verdaderos y aun así sea un estafador.

Bitcoin Core también publica fallos de software: el aviso CVE-2024-35202 describió un cierre remoto posible en versiones anteriores a 25.0. Verificar reglas no elimina la necesidad de mantener software. No se deduce de ese aviso un robo de claves.

En enero de 2026, The Register informó de una exposición de datos de pedidos y contacto de compradores de Ledger a través de Global-e, con confirmaciones atribuidas a ambas compañías y sin afectación de claves de recuperación según esas declaraciones. El caso recuerda que una compra puede revelar que posees un dispositivo aunque el hardware no se haya vulnerado.

En abril de 2026, The Record informó del ataque a Drift y la suspensión de depósitos y retiradas anunciada por la plataforma. Se trata de un protocolo de finanzas descentralizadas sobre Solana, no de una ruptura de Bitcoin. Las pérdidas inicialmente estimadas y los procesos posteriores de recuperación no deben presentarse como una cifra definitiva ni como reembolso garantizado.

Práctica

1. Clasifica cada incidente por custodia, interfaz o distribución, datos personales, protocolos de otras redes y disponibilidad.
2. Para cada uno propón una prevención y una limitación de esa prevención.
3. Ensaya una llamada fraudulenta: «conozco tu compra; mueve tus fondos a esta dirección segura». Cuelga y verifica por un canal iniciado por ti.

Demuestra

Puedes explicar por qué ningún incidente prueba que una marca alternativa sea invulnerable. La evidencia respalda un alcance concreto.

Duda frecuente

¿Son los últimos hackeos que existen? No. Es una selección verificada para la edición del 17 de noviembre de 2026, no un inventario exhaustivo ni una monitorización en directo.

Punto de pausa

Anota el hábito que vas a cambiar y cómo comprobarás que lo mantienes.

Un interlocutor conoce tu compra y te pide transferir a una «wallet de rescate». ¿Qué demuestra conocer tu compra?

1. Que puede ser información filtrada; no autentica su identidad ni la dirección.
2. Que es necesariamente soporte legítimo.
3. Que debes compartir la semilla.

> **Ver respuesta: Que puede ser información filtrada; no autentica su identidad ni la dirección.**
> Datos ciertos pueden utilizarse para construir un engaño convincente.

M08

Crear identidad y verificar contactos de chat

Objetivo

Activar una identidad de chat sin exponer su clave y verificar a la contraparte.

Comprender

En Desk, el chat se vincula al criptograma mediante una Clave Chat generada en Cuvex. Aunque su representación pueda parecer una xpub, es secreta y no debe tratarse como una clave pública de una cuenta WOW. El tutor nunca necesita leerla ni verla por QR.

El flujo distingue alias nuevo y traslado o recuperación de uno existente. En la implementación revisada se elige el perfil móvil iOS o Android correspondiente, porque las identidades derivadas históricas no son intercambiables por intuición. DEV y Producción son entornos separados: cambiar de entorno no migra conversaciones o alias automáticamente.

Añadir un alias no verifica identidad. Comprueba la huella mediante un canal independiente y autenticado. Si la app ofrece preguntas de reconocimiento, utiliza información que no sea pública y evita respuestas que revelen contraseñas. Una voz conocida puede ser imitada; para situaciones de riesgo combina métodos acordados previamente.

Si cambia la identidad de un contacto, pausa pagos y coordinación hasta resolverlo. Puede ser una recuperación legítima o una sustitución maliciosa. El cifrado de extremo a extremo protege un canal según su protocolo e implementación, pero no demuestra quién está usando el dispositivo del otro lado.

Práctica

1. En un entorno de pruebas, explica el flujo de crear o recuperar sin facilitar la Clave Chat.
2. Añade un contacto de laboratorio y acuerda por otro canal una verificación de huella.
3. Simula un cambio de identidad. Define cómo confirmarías el cambio antes de pagar.

Demuestra

Puedes distinguir alias, huella pública, Clave Chat secreta y confianza humana en una persona.

Duda frecuente

¿Un alias antiguo garantiza que es la misma persona? No. La continuidad y los cambios de claves deben verificarse según el flujo.

Punto de pausa

Registra solo «contacto de prueba verificado» y el método, sin claves ni preguntas privadas.

Una cadena se llama Clave Chat y tiene aspecto de xpub. ¿Cómo se trata en Desk?

1. Como un dato publicable en foros.
2. Como un secreto de recuperación de identidad.
3. Como dirección de recepción Bitcoin.

> **Ver respuesta: Como un secreto de recuperación de identidad.**
> El formato visual no determina la confidencialidad ni el propósito del dato.

Solicitar y pagar satoshis desde chat

Objetivo

Pasar de una conversación a un pago sin perder revisión ni contexto.

Comprender

El chat permite solicitar dirección, responder con una dirección de recepción, solicitar pago y abrir la preparación desde una cuenta WOW. Mantener el contexto en el canal reduce errores de copiar información entre aplicaciones, pero no convierte cada mensaje en una orden autenticada de gasto.

Antes de responder o pagar, revisa contacto verificado, red, importe y solicitud original. El formulario compartido conserva selección de UTXOs y comisión. Si el mensaje solicita una cantidad y eliges «Enviar el total», el neto después de comisiones puede ser inferior; debe identificarse como pago parcial cuando corresponda.

La autorización permanece en Cuvex. El chat transporta intención y coordinación; no tiene permiso para firmar automáticamente. La confirmación de pago enviada al contacto debe distinguir que se ha recibido un mensaje de que existe una transacción confirmada. El receptor verifica con su propia cuenta o fuente.

Enlaces externos, QR adjuntos y direcciones siguen siendo datos no confiables hasta validarlos. «Ver en Mempool» puede abrir un servicio de terceros y revelar consultas. Si tu política utiliza nodo propio, prefiere la verificación compatible en WOW y evalúa cualquier salida a servicios públicos.

Práctica

1. Representa dos roles: receptor solicita 50.000 sat; pagador prepara sin publicar.
2. Simula un saldo disponible neto de 48.000 sat. Explica qué consentimiento y conciliación faltan para un pago parcial.
3. Cambia deliberadamente la red en un mensaje de prueba y detén el flujo.

Demuestra

Puedes seguir la relación entre solicitud, dirección, borrador, firma y confirmación sin reducirla a «el chat dice OK».

Duda frecuente

¿Enviar sats desde chat implica usar Lightning? No. El flujo WOW documentado prepara pagos Bitcoin en cadena. La palabra sats expresa una unidad, no una red de transporte.

Punto de pausa

Cancela el borrador de laboratorio o registra el estado; no publiques para demostrar una interfaz.

Recibes una confirmación en el chat. ¿Cuál es la comprobación decisiva del cobro?

1. Que el icono del mensaje sea verde.
2. Que el interlocutor diga «confirmado».
3. Verificar la operación y sus salidas en la red con la fuente apropiada.

> **Ver respuesta: Verificar la operación y sus salidas en la red con la fuente apropiada.**
> El estado del mensaje y el estado de la transacción no son equivalentes.

Compartir criptogramas de forma consciente

Objetivo

Entender qué implica entregar una copia cifrada a otra persona.

Comprender

Compartir un criptograma transmite una copia del objeto cifrado. No envía necesariamente bitcoins ni incorpora por sí solo a un nuevo firmante. Si el receptor obtiene también medios de desbloqueo suficientes, puede acceder al contenido conforme al esquema; por ello hay que decidir de antemano qué capacidad estás transfiriendo.

El cifrado de extremo a extremo del chat y el cifrado del archivo protegen capas distintas. Una vez descargado, el receptor puede conservar el objeto fuera del chat. Eliminar tu mensaje o registro local no garantiza retirar todas las copias. Una contraseña compartida por el mismo canal puede concentrar los componentes en una sola vía.

Antes de enviar, verifica identidad, formato y finalidad. Si la app permite vincular un criptograma recibido, eso organiza una copia, no acredita que sea seguro descifrar cualquier archivo. No utilices adjuntos que exijan introducir semilla o contraseña en una página externa.

La recuperación requiere un acuerdo operativo: quién conserva cada componente, quién puede abrirlo, cómo se detecta una exposición y cómo se cambia la custodia si termina la relación. Para un pago corriente normalmente basta una dirección validada; no es necesario compartir tu criptograma.

Práctica

1. Diseña una transferencia de un texto didáctico cifrado a un contacto de laboratorio.
2. Enumera qué sabe y qué podría hacer el receptor antes y después de conocer la contraseña.
3. Simula que la relación termina. Explica por qué borrar el mensaje no revoca la copia ni las claves.

Demuestra

Puedes distinguir «compartí datos», «compartí acceso a un secreto» y «firmé un gasto».

Duda frecuente

¿Un archivo cifrado puede circular sin ninguna consecuencia? Puede revelar metadatos, facilitar intentos de contraseña y conservarse indefinidamente. Evalúa la necesidad de compartirlo.

Punto de pausa

No dejes adjuntos de custodia en el curso. Registra solo la conclusión del ejercicio.

Compartir un criptograma por chat, ¿equivale a enviar bitcoins?

1. No; transmite un objeto cuyo contenido y acceso tienen otro alcance.
2. Sí, siempre que termine en .bin.
3. Activa automáticamente una multifirma nueva.

> **Ver respuesta: No; transmite un objeto cuyo contenido y acceso tienen otro alcance.**
> Transporte de secretos y movimiento de UTXOs son operaciones distintas.

M08

Recuperar chat y entender sus metadatos

Objetivo

Planificar cambio de equipo y separar recuperación de identidad y de mensajes.

Comprender

Desk indica que historial y sesiones se cifran localmente y no forman parte de su copia global. La Clave Chat permite recuperar la identidad; no garantiza recuperar todas las conversaciones antiguas. La app incluye estados y acciones para activación pendiente, mantenimiento de claves y recuperación local cuando existe material compatible.

Cada alias debe usarse en un solo dispositivo a la vez según la guía de la base revisada. No lo actives simultáneamente en dos equipos para «probar sincronización» si ese uso no está soportado. Un traslado debe seguir el procedimiento y verificar continuidad con los contactos.

«Pendiente», «aceptado por servidor», «recibido» y «no se pudo descifrar» describen etapas distintas. Un envío sin confirmar no se reenvía automáticamente a ciegas: primero hay que resolver si llegó. Si falta una clave de sesión o cambia identidad, conservar el mensaje pendiente no equivale a haberlo leído.

El contenido cifrado no oculta necesariamente horarios, tamaño, relaciones de entrega, alias o datos de conexión frente a todos los sistemas implicados. En la voz sucede algo parecido: el cifrado del transporte no convierte una llamada convencional en un canal apropiado para secretos. Usa el mínimo dato necesario para aprender y resolver incidencias.

Práctica

1. Simula perder el PC y explica qué recupera cada material disponible.
2. Clasifica estados de mensajes y decide cuándo no se debe reenviar una solicitud de pago.
3. Prepara un aviso de cambio de equipo que los contactos puedan verificar por un canal independiente.

Demuestra

Puedes explicar qué conversación se perdería y qué identidad podría restaurarse sin prometer restauraciones que el backup no cubre.

Duda frecuente

¿Borrar el chat local borra también los mensajes en el otro extremo? No debes asumirlo. El receptor puede conservar mensajes y archivos independientemente.

Punto de pausa

Guarda un plan de traslado con nombres de campos vacíos, sin Clave Chat.

¿Qué garantiza por sí sola la Clave Chat según la guía revisada?

1. Todas las conversaciones históricas en cualquier PC.
2. Capacidad de recuperación de identidad por el flujo compatible, no de todos los mensajes antiguos.
3. Acceso automático a las claves de Bitcoin de los contactos.

> **Ver respuesta: Capacidad de recuperación de identidad por el flujo compatible, no de todos los mensajes antiguos.**
> Identidad y archivo histórico son capacidades diferentes.

Configuración cotidiana y revisión de permisos

Objetivo

Controlar parámetros de Desk sin confundir comodidad con protección.

Comprender

Desk ofrece tema Noche, Día o Sistema; sincronización automática y periodos de 3 o 5 minutos; sonidos de transacción; fondo del chat; idioma y moneda de referencia. Esas preferencias cambian presentación o frecuencia de consulta. No modifican una firma de Bitcoin ni añaden anonimato.

La configuración de seguridad revisada permite bloqueo por inactividad, bloqueo al pasar a segundo plano, demora máxima tras fallos y borrado opcional. El intervalo admitido por el esquema de inactividad es 30 a 86.400 segundos; la interfaz puede presentar opciones más acotadas. Los valores por defecto deben leerse de la versión que ejecutas, no suponerse por una clase grabada.

La integración de enlaces bitcoin: abre una solicitud para desbloquear, elegir cuenta y revisar. No autoriza un pago automático. En Linux, la guía diferencia instalación integrada y AppImage para registrar enlaces. Una factura Lightning requiere un flujo compatible distinto; no se resuelve declarando Desk aplicación predeterminada.

La cotización, el gráfico de precio y los enlaces informativos pueden consultar servicios externos. Su función es informativa y no una señal de compra. Revisa fecha y fuente antes de utilizar el dato para traducir importes. Un modo oscuro o una ventana pequeña no deben ocultar botones finales, dirección o comisión; si ocurre, pausa y reporta el problema de geometría.

Práctica

1. Ajusta apariencia y bloqueo en el almacén de aprendizaje. Comprueba que puedes volver a entrar.
2. Revisa qué automatismos activas: sincronización, sonidos y comprobación de firmware no son lo mismo.
3. Abre una solicitud ficticia de enlace bitcoin: y cancela antes de preparar cualquier operación real.

Demuestra

Puedes explicar el efecto de cada ajuste y localizar los que implican consultas o acciones sensibles.

Duda frecuente

¿La biometría del PC sustituye mi copia de recuperación? No. Puede depender del equipo y del almacén seguro del sistema. Conserva la recuperación independiente.

Punto de pausa

Bloquea Desk y registra solo qué preferencias cambiaste.

¿Qué cambia al elegir sincronización cada tres minutos?

1. La frecuencia prevista de consulta cuando la función se ejecuta.
2. La política de firmas en la cadena.
3. La semilla del dispositivo.

> **Ver respuesta: La frecuencia prevista de consulta cuando la función se ejecuta.**
> Es una preferencia operativa, no una modificación de custodia.

M09

Diseñar una cartera multifirma

Objetivo

Elegir un umbral que resista pérdidas y compromisos razonables.

Comprender

En una política M de N, N es el número de participantes con claves distintas y M el número de firmas necesarias. Una 2 de 3 resiste la indisponibilidad de una clave, pero dos claves comprometidas pueden autorizar gasto. Si las tres semillas están en el mismo sitio o nacen de una misma exposición, la independencia se reduce.

El perfil multifirma revisado de Cuvex es P2WSH nativo con sortedmulti y derivación BIP48. Original admite estructuralmente hasta seis claves de política y BIT hasta quince. Si intervienen ambos, el flujo debe respetar el participante más limitado y el tamaño real del transporte. Máximos de estructura no garantizan que una política con muchas claves y entradas quepa.

La app admite umbrales que deben cumplir las relaciones de la política, pero una 1 de N no exige colaboración para gastar. El firmware conserva avisos específicos sobre ese riesgo. Elegir un número más grande no mejora todo: aumenta coordinación, costes, material de recuperación y posibilidad de bloqueo.

MuSig2 es un esquema distinto de agregación de firmas Schnorr y, por sí mismo, es N de N, no una 3 de 5 arbitraria. En los firmwares Final estudiados no está implementada firma de entradas Taproot, MuSig2 ni Miniscript. Recibir un destinatario P2TR no demuestra capacidad de firmar desde una cartera Taproot.

Práctica

1. Diseña una 2 de 3 ficticia con riesgos independientes para cada participante.
2. Simula pérdida de una clave y compromiso de una. Explica qué se puede y qué no se puede hacer.
3. Comprueba límites por modelo antes de escoger una política de mayor tamaño.

Demuestra

Puedes expresar tolerancia a pérdida, umbral de ataque y dependencias compartidas de tu diseño.

Duda frecuente

¿La multifirma exige que las personas conozcan las semillas de las demás? No. El propósito es que cada una conserve su capacidad privada y se comparta la información pública necesaria para construir y recuperar la política.

Punto de pausa

Guarda el diseño con participantes ficticios y sus responsabilidades.

En una 2 de 3 con claves independientes, ¿cuántas claves privadas bastan para autorizar un gasto válido según esa política?

1. Una.
2. Dos.
3. Siempre las tres.

> **Ver respuesta: Dos.**
> El umbral exige dos; las demás condiciones y validaciones también deben cumplirse.

Crear invitaciones y aportar claves

Objetivo

Construir una política con participantes verificados sin compartir semillas.

Comprender

El creador elige nombre, red, M, N, contactos, información pública propia y condiciones operativas de la invitación. En el esquema revisado se aceptan redes mainnet y regtest para este flujo, de 2 a 15 participantes antes de aplicar límites del dispositivo, y expiración operativa de 1 a 720 horas. No uses estos límites como autorización para saltar una comprobación de capacidad.

Cada participante revisa la invitación, decide aceptar o rechazar y aporta la clave pública extendida del participante con huella y ruta BIP48 mediante el flujo compatible. No aporta semilla, clave privada, dirección suelta ni descriptor entero de otra cartera. Una clave mal contextualizada puede producir una política distinta aunque tenga aspecto de xpub válida.

El creador coordina; no sustituye la validación de cada firmante. Antes de recibir fondos, todos deben poder reconstruir y verificar los mismos parámetros y una dirección de control. Un contacto aceptado en chat no implica aprobación automática de cualquier política que envíe.

La caducidad de una invitación es una regla de coordinación de la app. No cambia por sí sola un script ya financiado, no borra firmas guardadas por otras personas y no funciona como timelock de consenso. Cancelar una propuesta y retirar fondos de una política existente son acciones distintas.

Práctica

1. En laboratorio regtest preparado, crea una propuesta 2 de 3 con contactos de prueba.
2. Representa una aceptación, un rechazo y una aportación con red incorrecta. Comprueba que la última se detiene.
3. Enumera los datos que todos deben conservar antes de financiar: red, umbral, claves públicas, orígenes, script y dirección comprobada.

Demuestra

Puedes reconocer una invitación incompleta y explicar qué aprobación falta sin asumirla por la existencia del chat.

Duda frecuente

¿Una fecha de vencimiento hace imposible gastar después? No por ser un campo de invitación. Una restricción temporal de Bitcoin requiere condiciones de script o transacción específicas y soporte real.

Punto de pausa

Guarda el identificador didáctico de la propuesta y la aprobación pendiente.

Para aportar tu participación multifirma, ¿qué solicita el flujo documentado?

1. La semilla de todos los participantes.
2. Una dirección de cobro cualquiera.
3. Tu clave pública extendida con huella y origen BIP48 compatibles.

> **Ver respuesta: Tu clave pública extendida con huella y origen BIP48 compatibles.**
> El material público correcto permite construir la política sin divulgar claves privadas.

Verificar políticas con Mirror en orden libre

Objetivo

Comparar campos completos y entender exactamente qué acredita el resultado.

Comprender

La verificación independiente presenta umbral, red, perfil, SIGHASH, ID de política, primera dirección, posición del usuario y datos de cada participante. Es un control de intención y consistencia. No presupone que el dispositivo haya registrado permanentemente una política; el alcance documentado de la revisión es «esta revisión».

En Mirror 12.12 puedes leer primero el QR de Cuvex o el de Desk y escoger cualquier dato. No hay obligación de empezar por el paso 1, escanear todos ni mantener un orden. Si revisas un texto manualmente, omitir su escaneo no lo marca como comprobado por Mirror.

El comparador muestra texto literal completo. Espacios, saltos de línea, mayúsculas y diferencias Unicode cuentan. «Coincide» significa que los dos valores de ese par son iguales; no autentica origen, no prueba que corresponden a la misma política y no activa la cartera. La aprobación final y su respuesta correlacionada siguen el circuito Cuvex y Desk.

Los QR actuales de Desk contienen solo el valor, sin ordinal ni sesión. Mirror no puede deducir siempre el paso. «Indicar paso de Desk» añade contexto manual y debe mostrarse como tal. Con N participantes hay 7 + 4N campos del mapa documentado: 8+4k huella, 9+4k ruta, 10+4k xpub y 11+4k ID de clave, para k empezando en cero. Con N=2, el paso 15 es el ID de la segunda clave y puede compararse primero.

Práctica

1. Usa datos sintéticos y compara primero un ID rotulado como paso 15; después red y umbral.
2. Introduce una discrepancia de un carácter. Comprueba «No coincide» y comienza otro par sin arrastrar el resultado.
3. Compara «2 / 3» y explica por qué el texto no permite saber siempre si es umbral o posición del usuario.

Demuestra

Puedes describir qué campo verificaste, cómo lo contextualizaste y qué queda por aprobar. No conviertas coincidencias parciales en aprobación global.

Duda frecuente

¿Tengo que escanear todos los QR para continuar aprendiendo? No. La comparación es libre. Las revisiones y autorizaciones obligatorias del firmante conservan su propio flujo.

Punto de pausa

Cierra el comparador; los valores deben borrarse al salir o pasar a segundo plano según el diseño revisado.

Mirror compara dos QR del paso 15 y muestra «Coincide». ¿Qué acredita?

1. Igualdad literal de ese par, con el contexto que se haya identificado o indicado.
2. Aprobación de toda la política.
3. Autenticación del origen de ambos QR.

> **Ver respuesta: Igualdad literal de ese par, con el contexto que se haya identificado o indicado.**
> La comparación no sustituye autenticación, revisión global ni respuesta del hardware.

Coordinar firmas y publicar multifirma

Objetivo

Llevar una propuesta a umbral de firmas sin perder intención ni control.

Comprender

Una operación multifirma especifica entradas, destinatarios, importes, tarifa, reemplazo y notas operativas. El creador puede solicitar firmas a participantes compatibles. Cada firmante revisa por su cuenta red, política, entradas, todas las salidas y comisión antes de autorizar en su dispositivo.

Una firma parcial no mueve fondos por sí sola si falta el umbral. Cuando se alcanza, el coordinador puede combinar y finalizar según el flujo. Los informes de otros participantes o del coordinador son información de coordinación, no una verificación local que tú hayas hecho. La app debe distinguir esas procedencias.

La base ofrece reintento, recepción de firma, acuse, rechazo y traspaso de coordinación. Un traspaso no cambia las claves ni el umbral de la cadena. Una respuesta guardada debe correlacionarse con la solicitud y el perfil efectivo que se utilizó; no se elige otra política por ser parecida o por ser la primera del catálogo.

Si alguien modifica destinatarios o condiciones relevantes, hay que revisar una nueva propuesta y obtener las firmas que correspondan. No «arregles» a mano una PSBT eliminando datos de seguridad para que quepa en NFC. Los firmwares exigen el perfil y validaciones compatibles, con límites de entradas, salidas y tamaño.

Antes de publicar, verifica que la operación es la acordada y que no existe una versión ya difundida. Después sigue confirmaciones por la fuente elegida. Rechazar en tu app no revoca automáticamente firmas que otros ya conservaron ni impide cualquier acción compatible con el umbral restante.

Práctica

1. Representa una 2 de 3 con tres roles ficticios. Uno firma, otro rechaza y el tercero solicita aclaración.
2. Cambia la dirección del pago de prueba y explica por qué no se reutiliza una aprobación verbal anterior.

3. Simula un acuse fallido tras guardar la firma. Recupera el mismo trabajo, sin duplicar pago ni cambiar perfil.

Demuestra

Puedes señalar quién coordina, quién firma, quién finaliza y qué prueba existe de cada etapa.

Duda frecuente

¿Dos OK del chat equivalen a dos firmas? No. El umbral se satisface con autorizaciones criptográficas válidas bajo la política, no con mensajes.

Punto de pausa

Registra estado, firmas pendientes y siguiente responsable sin contenido privado.

Una operación 2 de 3 tiene una firma válida y dos mensajes que dicen «de acuerdo». ¿Está completo el umbral?

1. Sí, por tres participantes.
2. No; falta otra firma criptográfica válida.
3. Sí, si lo anuncia el coordinador.

> **Ver respuesta: No; falta otra firma criptográfica válida.**
> Consentimiento conversacional y firma válida son evidencias distintas.

Recuperar y cambiar una multifirma

Objetivo

Recuperar la política y planificar pérdida o sustitución de participantes.

Comprender

La recuperación necesita dos categorías: datos que reconstruyen la política y suficientes capacidades privadas para gastar. Una copia de política con xpubs puede revelar historial sin incluir semillas. Una copia cifrada añade protección al archivo, pero exige conservar su contraseña. La extensión .cuvexms no demuestra por sí sola que esté cifrada: el formato y su exportación concreta deben comprobarse.

En Desk 9.21 la recuperación solicita la clave pública extendida del participante con huella y ruta BIP48 exportada desde su dispositivo. Admite la lectura por webcam o Mirror del flujo compatible. No sustituyas esa aportación por una dirección de recepción ni envíes la semilla al soporte.

Si se pierde una clave en una 2 de 3, las otras dos pueden mantener capacidad de gasto. La política anterior sigue siendo la misma; para retirar de forma efectiva a un participante y establecer otras claves, normalmente se crea una política nueva y se trasladan fondos con las autorizaciones necesarias. Cambiar un alias o eliminar una wallet de Desk no modifica UTXOs existentes.

Las copias deben permitir reconstruir ambas ramas y descubrir el historial. Conserva índices, solicitudes emitidas y el contexto necesario para no reutilizar direcciones o interpretar una cartera vacía por un escaneo incompleto. Restaurar y reanudar una operación pendiente debe respetar el perfil que se guardó al crearla.

Práctica

1. Exporta y restaura una política de laboratorio mediante la función documentada. Verifica red y dirección conocida.
2. Simula pérdida de un participante y prepara un plan de rotación, sin mover fondos reales.
3. Simula pérdida por debajo del umbral. Reconoce que soporte o IA no pueden fabricar las firmas faltantes.

Demuestra

Puedes recuperar el escenario de pruebas y distinguir restaurar información de cambiar control sobre las monedas.

Duda frecuente

¿Eliminar la multifirma en Desk desactiva la cartera para todos? No. Elimina el estado local según el flujo. Otras personas y copias pueden seguir conservando capacidad compatible con la política.

Punto de pausa

Conserva copia probada y plan privado; registra en el curso solo el resultado.

Quieres retirar a una persona de una política ya financiada. ¿Basta con borrar su nombre en Desk?

1. Sí.
2. Sí, si el chat también se elimina.
3. No; hay que planificar una nueva política y el movimiento autorizado de fondos cuando corresponda.

> **Ver respuesta: No; hay que planificar una nueva política y el movimiento autorizado de fondos cuando corresponda.**
> Los scripts de las UTXOs existentes no cambian por editar registros locales.

M10

Actualizar firmware sin improvisar

Objetivo

Preparar una actualización compatible y verificar su resultado en el dispositivo.

Comprender

Una actualización cambia software de confianza. Verifica modelo, revisión de hardware, versión, procedencia y mecanismo de autenticación del fabricante. Una descarga completa o un hash igual al de una página no sustituyen la verificación de firma y compatibilidad. Nunca instales una aplicación de firmware sin firma destinada al ingeniero como si fuera una publicación para clientes.

Original actualiza por Bluetooth en el flujo documentado. BIT utiliza USB-C. Mirror incorpora recorridos de preparación y transporte compatibles. No se promete que una combinación concreta de PC, teléfono y dispositivo funcione hasta completar la aceptación física de esa combinación. La incidencia histórica de actualización de Original en Windows exige diagnóstico específico; no se resuelve fingiendo un éxito al 99 %.

Antes de empezar, verifica respaldos recuperables, alimentación estable y ausencia de otras operaciones. Prepara el archivo oficial o copia previamente verificada según la app. Durante el envío, diferencia transferencia, validación, instalación, reinicio y comprobación de versión. La barra no es prueba final.

Al terminar, comprueba versión visible en el equipo y registra fecha y resultado. El catálogo de compatibilidad de Desk no mide remotamente el firmware: firmwareAttestation permanece false. Seleccionar un perfil Final no acredita qué bytes están realmente instalados. Si la actualización falla, sigue recuperación documentada y conserva fase y error sin desconectar a ciegas en una etapa crítica.

Práctica

1. Revisa una lista de preparación sin iniciar una actualización real durante el ensayo.
2. Ordena estados y explica por qué «transferido» y «instalado» son distintos.
3. Redacta un informe ficticio de fallo al 99 % con modelo, versión, sistema, fase y mensaje final.

Demuestra

Puedes identificar el artefacto adecuado, el transporte y el criterio final de éxito.

Duda frecuente

¿Debo actualizar solo para que desaparezca un error de Desk? Primero identifica el origen. Una incompatibilidad del catálogo puede requerir corregir Desk y conservar el firmware validado.

Punto de pausa

Una actualización real solo se pausa en un estado expresamente seguro del procedimiento, no por alcanzar el fin de la llamada.

¿Qué verifica el catálogo explícito de Desk por sí solo?

1. Referencias de compatibilidad admitidas, sin medir remotamente el firmware instalado.
2. Una atestación física de todos los dispositivos conectados.
3. Ausencia de vulnerabilidades.

> **Ver respuesta: Referencias de compatibilidad admitidas, sin medir remotamente el firmware instalado.**
> Compatibilidad, firma, medición y aceptación física son evidencias diferentes.

Pérdida avería y recuperación de emergencia

Objetivo

Elegir una recuperación proporcional al incidente y preservar evidencias útiles.

Comprender

Ante un incidente, primero clasifica qué se ha perdido o expuesto: ordenador, dispositivo, tarjeta, archivo, contraseña, semilla, passphrase o política. «No puedo entrar» no significa necesariamente «me han robado». Si hay sospecha de compromiso, no sigas introduciendo secretos en el equipo sospechoso.

La pérdida del dispositivo puede resolverse con soportes y credenciales de recuperación compatibles. La pérdida del ordenador puede requerir restaurar el almacén de Desk y reconstruir observación. Perder todos los medios de desbloqueo o todas las claves necesarias por debajo del umbral puede no tener solución técnica. Ninguna IA puede garantizar rescate de claves inexistentes.

Desk incluye una recuperación local para formatos admitidos y exportación del material de recuperación correspondiente. Descifrar en el PC puede exponer el secreto al sistema operativo o malware. Es una decisión excepcional: utiliza un entorno preparado, material compatible y plan de traslado a claves nuevas si el secreto pudo quedar comprometido. No lo describas como una operación equivalente al aislamiento habitual de Cuvex.

Si una semilla se filtró, cambiar la contraseña de Desk no revoca esa semilla. Debes evaluar el traslado autorizado a una cartera nueva y protegerla desde un equipo fiable. Evita publicar detalles del incidente que ayuden al atacante o pagar servicios que prometen recuperación a cambio de otra semilla o anticipos fraudulentos.

Práctica

1. Resuelve cuatro tarjetas ficticias: PC perdido, tarjeta rota con copia válida, contraseña olvidada y semilla expuesta.
2. Para cada una, identifica material necesario, riesgo de actuar y criterio de recuperación.
3. Ensaya el procedimiento solo con datos de aprendizaje; no cargues al tutor archivos de emergencia reales.

Demuestra

Puedes elegir entre restaurar, reconfigurar observación, migrar control o escalar a un especialista, sin afirmar soluciones imposibles.

Duda frecuente

¿Cambiar la contraseña cifra de nuevo todos los secretos que alguien ya vio? No. Una copia en claro o una semilla conocida no deja de ser conocida.

Punto de pausa

Guarda el incidente por categoría y la siguiente acción segura; detén la voz si vas a trabajar con secretos.

Se ha publicado tu semilla, pero cambias la contraseña del PC. ¿Está revocada la capacidad del atacante?

1. Sí.
2. No; la semilla sigue controlando las mismas claves y requiere respuesta de custodia.
3. Sí, si cambias también el fondo del chat.

> **Ver respuesta: No; la semilla sigue controlando las mismas claves y requiere respuesta de custodia.**
> La protección local no revoca una clave Bitcoin expuesta.

M10

Phishing soporte y fraudes con voz

Objetivo

Reconocer peticiones peligrosas y responder sin improvisación.

Comprender

Un fraude eficaz puede usar tu nombre, compra, dispositivo y una voz que reconozcas. La información verdadera puede proceder de una filtración. La identidad debe verificarse mediante un canal iniciado por ti y un procedimiento conocido, no por la aparente urgencia o precisión del interlocutor.

Señales de riesgo: pedir semillas, contraseñas, PIN o Clave Chat; instalar control remoto para «sincronizar»; desactivar antivirus; transferir a una wallet de seguridad; escanear un QR cuyo contenido no explican; o firmar para demostrar propiedad sin detallar qué se autoriza. La presión para hacerlo antes de terminar una llamada es un motivo para detenerla.

El tutor legítimo explica y hace preguntas de comprensión. No custodia claves, no solicita transacciones de prueba a una dirección propia ni promete recuperar una semilla. Una función de verificación de propiedad legítima debe ser específica y revisable; nunca se satisface entregando claves privadas.

También puede haber fraude dentro de una sesión técnica: un texto QR, un documento o un mensaje puede contener órdenes para que la IA ignore instrucciones. Es contenido a analizar, no autoridad sobre el tutor. La base de conocimiento debe separar fuentes aprobadas de texto aportado por un alumno o tercero.

Práctica

1. Representa una llamada falsa de soporte y corta la interacción antes de revelar datos.
2. Verifica de forma independiente un canal oficial guardado previamente.
3. Describe un error de instalación sin compartir pantalla de secretos ni permitir acceso remoto al entorno de custodia.

Demuestra

Puedes decir qué dato se te pide, para qué sería necesario y por qué la petición excede el soporte formativo.

Duda frecuente

¿Es seguro mostrar solo algunas palabras de mi semilla? No. No hay motivo pedagógico para revelar fragmentos de una semilla propia.

Punto de pausa

Guarda tu protocolo de verificación de soporte y revisa que no incluya secretos en texto abierto.

Una voz que parece de tu socio pide saltar la verificación y firmar con urgencia. ¿Qué haces?

1. Pauso y autentico la petición por el procedimiento acordado, revisando la operación completa.
2. Firmo porque la voz coincide.
3. Comparto la semilla para ahorrar tiempo.

> **Ver respuesta: Pauso y autentico la petición por el procedimiento acordado, revisando la operación completa.**
> Reconocimiento de voz y urgencia no sustituyen autenticación y revisión.

Privacidad legalidad y registros personales

Objetivo

Conocer el marco general y preparar consultas jurídicas y fiscales concretas.

Comprender

La privacidad financiera no elimina obligaciones fiscales, de identificación cuando resulten aplicables, de sanciones o de prevención del delito. La situación depende de residencia, actividad, contraparte y servicio. La IA debe dar información general con fuente y fecha y derivar decisiones particulares a profesionales competentes.

En la UE, MiCA regula determinados criptoactivos y servicios. Su aplicación general comenzó el 30 de diciembre de 2024 y el régimen transitorio máximo indicado en el reglamento llegaba al 1 de julio de 2026, sujeto a decisiones nacionales. Comprueba autorización y alcance en registros oficiales vigentes; no basta una mención antigua de registro. La autorización no garantiza precio, solvencia ni compensación total.

El Reglamento 2023/1113 establece información que acompaña transferencias cuando intervienen proveedores obligados. Para transferencias superiores a 1.000 euros con direcciones autocustodiadas contempla medidas para evaluar propiedad o control. Ese umbral no crea una exención general de identificación por debajo. Las transferencias entre personas sin proveedor tienen una exclusión de alcance en ese reglamento; siguen existiendo otras obligaciones.

Conserva documentación suficiente de compras, ventas, comisiones y origen según tu caso, protegida de accesos innecesarios. No necesitas publicar el historial completo para llevar registros privados. Tampoco se enseña fragmentar operaciones para eludir controles, falsear información o ocultar rentas.

Si hay grabación o transcripción de voz y progreso identificable, el servicio debe definir finalidad, base jurídica, conservación, acceso, encargados y derechos aplicables. La configuración de privacidad comercial se valida antes de vender, no se improvisa durante una llamada.

Práctica

1. Redacta para un asesor un caso ficticio indicando residencia, actividad y operaciones, sin claves.

2. Comprueba dónde verificar autorización del proveedor y la fecha de la información.
3. Diseña un registro privado de movimientos y una política mínima de datos del alumno.

Demuestra

Puedes distinguir una regla jurídica, una política de exchange y una capacidad técnica de Bitcoin.

Duda frecuente

¿Toda autocustodia está prohibida en la UE? No se deduce eso de las normas citadas. Evita titulares absolutos y comprueba la disposición concreta y su alcance.

Punto de pausa

Guarda cuestiones pendientes para tu asesor sin introducir documentos personales en el tutor.

El umbral de 1.000 euros citado para ciertas medidas de control de dirección, ¿elimina todas las obligaciones por debajo?

1. Sí.
2. Solo si divides la operación.
3. No; no es una exención general de identificación u otras obligaciones.

> **Ver respuesta: No; no es una exención general de identificación u otras obligaciones.** La norma debe interpretarse por su medida y alcance, sin convertir un umbral en una exención universal.

Herencia continuidad y simulacro anual

Objetivo

Crear un plan que permita actuar a personas autorizadas sin exponerlo todo anticipadamente.

Comprender

La herencia combina legitimidad jurídica, localización de materiales y capacidad técnica. Una persona puede tener derecho a heredar y no saber reconstruir una wallet; otra puede tener una clave y carecer de autorización para usarla. El plan debe resolver ambas dimensiones con asesoramiento adecuado.

Separa instrucciones públicas de acceso a secretos. El inventario describe qué existe, a quién contactar y qué verificaciones hacer, sin colocar todas las claves y contraseñas juntas en un documento ampliamente accesible. Evita publicar semillas en testamentos o expedientes que puedan circular fuera de tu control.

En multifirma diseña quién conserva política y copias, qué umbral está disponible tras una pérdida y qué sucede si fallece una persona clave. Un mismo custodio guardando suficientes componentes puede convertirse en punto único de abuso. Una distribución demasiado compleja puede volver irrecuperable el patrimonio.

Incluye recuperación de contraseñas del criptograma y passphrase si existe, datos de derivación, compatibilidad de dispositivos y procedimiento si el fabricante deja de operar. No presupongas que un archivo propietario o una huella biométrica serán utilizables sin preparación. La interoperabilidad debe ensayarse con datos de prueba y formatos documentados.

Revisa tras cambios familiares, de domicilio, de política, de software o de participantes, y realiza un simulacro periódico. El ejercicio debe probar que una persona de confianza entiende las instrucciones sin revelar el patrimonio ni mover dinero innecesariamente.

Práctica

1. Completa una plantilla privada con responsables, componentes, acceso autorizado y sustitutos.
2. Da instrucciones de laboratorio a otra persona sin explicarlas oralmente y observa dónde se bloquea.

3. Corrige ambigüedades y registra una fecha de revisión. El curso no crea recordatorios automáticamente.

Demuestra

Puedes explicar qué ocurre si tú no estás disponible y qué información necesita cada rol en cada etapa.

Duda frecuente

¿Una 2 de 3 sustituye un plan de herencia? No. Es una herramienta técnica. Los herederos siguen necesitando contexto, materiales, coordinación y legitimidad.

Punto de pausa

Guarda el plan fuera del curso y marca solo «simulacro revisado».

¿Cuál es un criterio útil para evaluar un plan de herencia?

1. Que una persona autorizada pueda ejecutar un simulacro documentado sin improvisar ni recibir secretos prematuramente.
2. Que tenga muchas páginas.
3. Que dependa únicamente de recordar una contraseña.

> **Ver respuesta: Que una persona autorizada pueda ejecutar un simulacro documentado sin improvisar ni recibir secretos prematuramente.**
> Recuperabilidad y control de acceso deben comprobarse de forma práctica.

Precio ahorro y análisis fundamental

Objetivo

Analizar argumentos de inversión sin confundirlos con propiedades técnicas verificables.

Comprender

Precio es el resultado de intercambios en mercados concretos y puede diferir entre plataformas. Liquidez, moneda de cotización, profundidad, horario de proveedores bancarios y demanda influyen en el resultado que puedes ejecutar. Una cotización en pantalla no es una oferta garantizada para tu volumen.

El análisis fundamental estudia factores como adopción, demanda, competencia, seguridad económica, regulación y oferta. Un calendario de emisión conocido no determina por sí solo el precio futuro. Las valoraciones sobre utilidad monetaria o «valor intrínseco» dependen de supuestos; no existe una cifra objetiva que la IA pueda presentar como certeza universal.

Una estrategia de compras periódicas distribuye el momento de entrada, pero no garantiza beneficio ni evita pérdidas prolongadas. El ahorro a largo plazo también necesita liquidez para obligaciones, tolerancia a volatilidad y un plan de custodia. El curso no prescribe una proporción de tu patrimonio ni toma decisiones por ti.

Separa tres preguntas: ¿entiendo el activo?, ¿puedo custodiarlo y recuperarlo?, ¿puedo asumir su riesgo económico? Dominar claves no responde automáticamente a la tercera. La formación no convierte una proyección de precio o una gráfica histórica en una recomendación personalizada.

Práctica

1. Escribe una tesis ficticia, sus supuestos y hechos que la invalidarían.
2. Simula una caída del 50 % y necesidades de liquidez simultáneas, sin introducir tu patrimonio real.
3. Identifica qué datos del argumento son verificables y cuáles son expectativas.

Demuestra

Puedes discutir inversión sin prometer rentabilidad ni confundir convicción con evidencia.

Duda frecuente

¿La escasez asegura que el precio suba? No. La demanda y otras condiciones siguen siendo decisivas para el precio de mercado.

Punto de pausa

Guarda supuestos de laboratorio, no una instrucción automática de compra.

¿Qué garantiza una compra periódica?

1. Beneficio a largo plazo.
2. Ningún rendimiento; distribuye momentos de compra según una regla elegida.
3. Protección frente a pérdida de claves.

> **Ver respuesta: Ningún rendimiento; distribuye momentos de compra según una regla elegida.**
> Distribuir entradas no elimina riesgo económico u operativo.

M11

Elegir dónde adquirir bitcoin

Objetivo

Evaluar un proveedor por autorización, coste, retirada, privacidad y riesgo de custodia.

Comprender

Compara proveedores mediante criterios verificables: entidad jurídica y jurisdicción, servicios autorizados, red de retirada, comisiones, diferencial de precio, límites, soporte, autenticación y tratamiento de datos. El nombre comercial o un patrocinio no demuestran autorización para el servicio concreto.

El coste total puede incluir depósito, conversión, spread, comisión de negociación, retirada y coste bancario. Una negociación «sin comisión» puede tener un diferencial mayor. Comprueba cantidades netas y moneda de referencia. El presupuesto debe incluir retirar a autocustodia cuando ese sea tu objetivo.

Mientras mantienes un saldo custodial dependes del proveedor. Una prueba de reservas no demuestra por sí sola todos los pasivos, propiedad de fondos o solvencia futura. Verifica restricciones y realiza una retirada pequeña que puedas permitirte antes de depender de un flujo nuevo.

La identificación comercial puede asociar tu identidad a una retirada. Proteger esa información posteriormente no equivale a borrar lo que el proveedor conoce. No falsees datos ni uses el curso para eludir obligaciones. La compra de un código de formación también genera un registro comercial separado de tu wallet.

Práctica

1. Rellena una matriz ficticia con dos proveedores: coste total, red, retirada mínima, autorización y datos exigidos.
2. Calcula el neto para una operación de aprendizaje con todos los cargos especificados.
3. Diseña una retirada de prueba a una dirección previamente verificada, sin ejecutarla desde este minisite.

Demuestra

Puedes justificar una elección para tu caso y reconocer qué información está caducada o no comprobada.

Duda frecuente

¿El curso recomienda un exchange como el mejor para todos? No. Los permisos, tarifas, países atendidos y condiciones cambian. La comparación exige fecha y caso de uso.

Punto de pausa

Guarda la matriz sin credenciales ni documentos de identificación.

¿Qué comparación resulta más útil que mirar solo la comisión de negociación?

1. El coste total hasta recibir BTC en la red y dirección deseadas.
2. El número de seguidores del proveedor.
3. El color de su aplicación.

> **Ver respuesta: El coste total hasta recibir BTC en la red y dirección deseadas.**
> El precio final incluye conceptos que pueden quedar fuera de la comisión anunciada.

M11

Cuentas órdenes y costes de ejecución

Objetivo

Entender órdenes básicas y proteger la cuenta sin convertir el curso en una terminal de trading.

Comprender

Una orden de mercado prioriza ejecución disponible, con riesgo de deslizamiento. Una orden limitada fija un precio máximo de compra o mínimo de venta, pero puede no ejecutarse o hacerlo parcialmente. Una orden stop activa otra acción según las reglas del proveedor; no garantiza por sí sola el precio final.

El libro de órdenes muestra ofertas disponibles, no compromisos de que todos los volúmenes permanecerán. En una caída o baja liquidez, el resultado puede diferir de la última cotización. Las órdenes stop-market y stop-limit tienen riesgos distintos: ejecución a peor precio frente a posible no ejecución.

Protege acceso con contraseña única, autenticación resistente a phishing cuando esté soportada, revisión de sesiones y controles de retirada adecuados. Guarda recuperación de segundo factor de manera independiente. Una clave API para automatizar puede tener permisos más peligrosos que los que necesita una lectura de datos; no la introduzcas en el tutor ni en el minisite.

Antes de retirar, verifica activo y red Bitcoin, dirección de tu cartera y cantidades netas. Una plataforma puede usar los mismos símbolos para productos distintos. Al terminar, conserva documentación de compra, ejecución, comisiones y retirada conforme a tu caso; no confundas retirada a tu propia cartera con una nueva compra.

Práctica

1. Simula un libro ficticio con 1 unidad a 100 y otra a 102. Explica por qué comprar dos a mercado no asegura precio medio 100.
2. Diseña una orden limitada y describe el escenario en que no se completa.
3. Audita permisos de una API ficticia y elimina retirada si solo necesita consultar.

Demuestra

Puedes describir prioridad, precio y riesgo de no ejecución para cada orden.

Duda frecuente

¿Un stop-loss limita siempre la pérdida exactamente? No. Gaps, liquidez, deslizamiento y reglas del proveedor pueden impedirlo.

Punto de pausa

Guarda el resultado del ejercicio sin órdenes reales ni claves API.

Una orden limitada de compra a 100, ¿qué riesgo conserva?

1. Que nunca se ejecute o solo se ejecute parcialmente.
2. Que deba ejecutarse a cualquier precio.
3. Que cree automáticamente una copia de seguridad.

> **Ver respuesta: Que nunca se ejecute o solo se ejecute parcialmente.**
> El control de precio tiene como contrapartida posible falta de ejecución.

M11

Velas indicadores y sesgos del análisis técnico

Objetivo

Leer gráficos como datos históricos y evaluar una estrategia sin confundir patrones con predicción.

Comprender

Una vela resume apertura, máximo, mínimo y cierre de un periodo. El volumen depende de la fuente. Cambiar plataforma, moneda, huso horario o periodo puede cambiar lo que ves. Una vela no muestra todo el orden temporal de movimientos dentro de su intervalo.

Una media móvil suaviza precios pasados. Un indicador de momento transforma datos observados bajo una fórmula. Ninguno conoce el futuro. Dos indicadores derivados de la misma serie pueden aportar información muy correlacionada aunque sus colores y nombres sean distintos.

Para evaluar una regla define entrada, salida, invalidez, costes, tamaño y datos antes de mirar el resultado. Evita seleccionar solo ejemplos ganadores, ajustar parámetros hasta que encajen o utilizar datos futuros en una decisión pasada. Distingue datos de entrenamiento y validación temporal.

Un backtest debe considerar spread, comisiones, deslizamiento, disponibilidad de datos y ejecución posible. Rentabilidad bruta, tasa de acierto, pérdida máxima y distribución de pérdidas responden a preguntas diferentes. Un sistema con muchos aciertos puede perder dinero si sus fallos son grandes. No se enseña una señal de compra o venta como certeza.

Práctica

1. Lee una vela ficticia y explica qué información temporal no contiene.
2. Escribe una regla antes de evaluar diez resultados sintéticos, con costes y criterio de fallo.
3. Compara 9 ganancias de 1 con una pérdida de 15: el resultado bruto es -6 pese al 90 % de acierto.

Demuestra

Puedes criticar un resultado atractivo por selección, costes o riesgo sin necesitar ejecutar operaciones.

Duda frecuente

¿Combinar muchos indicadores garantiza una mejor señal? No. Puede aumentar sobreajuste y complejidad sin aportar información independiente.

Punto de pausa

Guarda la regla y los resultados de laboratorio, no una orden de mercado.

Nueve operaciones ganan 1 y una pierde 15. Antes de costes, ¿qué resultado hay?

1. +90 %.
2. +6.
3. -6.

> **Ver respuesta: -6.**
> Nueve unidades ganadas menos quince perdidas equivale a seis de pérdida.

M11

Margen futuros y automatización

Objetivo

Reconocer exposición, liquidación y fallos de automatización antes de considerar productos complejos.

Comprender

El apalancamiento aumenta exposición respecto al capital aportado. En un ejemplo simplificado, 100 de margen para una exposición de 1.000 implica que un movimiento adverso del 5 % del subyacente equivale a 50 antes de costes: la mitad del margen inicial. Las reglas reales de mantenimiento, liquidación, colateral y comisiones pueden empeorar el resultado y activarse antes de lo esperado.

Futuros y perpetuos pueden incorporar vencimiento, liquidación por diferencias, tasas de financiación y precios de referencia distintos del último intercambio. No son equivalentes a retirar bitcoin nativo a Cuvex. Custodiar una semilla no protege una posición frente a liquidación o fallo de contraparte.

Un bot automatiza reglas, incluidos sus errores. Necesita límites de posición, permisos mínimos, idempotencia de órdenes, reconciliación, control de pérdidas, interrupción de emergencia y supervisión. Duplicar una solicitud tras un timeout puede duplicar una exposición si no se conoce el resultado anterior.

La IA puede explicar conceptos y detectar incoherencias en un caso ficticio. No debe recibir claves API, activar trading ni prometer una estrategia rentable. Para el objetivo principal de este curso, comprender estos riesgos permite decidir no usar productos que no se entienden.

Práctica

1. Resuelve el ejemplo de exposición y margen sin asumir que el nivel de liquidación sea exactamente un 10 %.
2. Simula una API que ejecuta una orden pero pierde la respuesta. Explica por qué antes de repetir debes reconciliar.
3. Diseña un botón de parada que impida nuevas órdenes y compruebe las ya abiertas, sin conectar a un broker.

Demuestra

Puedes describir un riesgo que sobrevive al stop, otro que sobrevive al bot y otro que sobrevive a la autocustodia de fondos externos.

Duda frecuente

¿Automatizar elimina emociones y por ello garantiza resultados? No. Puede reducir una intervención impulsiva y multiplicar errores de diseño o ejecución.

Punto de pausa

Marca esta ampliación como comprendida sin habilitar productos complejos.

Con exposición 1.000 y margen 100, una pérdida del 5 % sobre exposición equivale, antes de costes, a:

1. 5 de pérdida.
2. 50 de pérdida, el 50 % del margen.
3. Ninguna pérdida si se usa un bot.

> **Ver respuesta: 50 de pérdida, el 50 % del margen.**
> Apalancamiento y costes hacen que el resultado sobre margen difiera del movimiento del activo.

M12

Lightning y otras capas

Objetivo

Entender pagos por canales y reconocer qué funciones no ofrece el flujo Cuvex revisado.

Comprender

Lightning utiliza canales y mecanismos de actualización para realizar pagos sin registrar cada intercambio individual en la cadena base. Abrir o cerrar canales y ciertos escenarios de recuperación sí pueden implicar transacciones on-chain. La disponibilidad, liquidez de entrada y salida y vigilancia dependen del diseño de la wallet y los servicios utilizados.

Una invoice puede incluir importe, descripción y caducidad. La unidad puede expresarse en satoshis o milisatoshis según el contexto, sin que estos últimos impliquen salidas sub-satoshi en la cadena base. Pagar una factura requiere compatibilidad y ruta disponibles; un QR no garantiza que se pueda pagar con cualquier app.

Hay servicios custodiales y no custodiales con modelos muy diferentes. La rapidez habitual no demuestra ausencia de riesgos. Tampoco se debe presentar Lightning como anonimato completo: existen observadores, rutas, contrapartes y metadatos relevantes.

El chat de Cuvex puede coordinar solicitudes de sats que se pagan por la cuenta WOW en cadena. En esta edición no se atribuye a Desk un nodo Lightning, gestión de canales ni firma de invoices Lightning. Si una solicitud incluye varias modalidades, comprueba cuál entiendes y cuál ejecutará tu aplicación.

Práctica

1. Clasifica una dirección on-chain, una URI bitcoin: y una invoice Lightning didácticas.
2. Compara pagar por cadena y por canal en términos de confirmación, liquidez, custodia y recuperación.
3. Explica por qué una invoice caducada debe revisarse con el receptor y no reinterpretarse como dirección.

Demuestra

Puedes rechazar una modalidad incompatible sin exponer claves ni atribuir un fallo a Cuvex.

Duda frecuente

¿Todos los pagos en sats son Lightning? No. Los satoshis expresan valor; la modalidad depende del protocolo utilizado.

Punto de pausa

Guarda la modalidad del ejercicio, sin facturas reales.

¿Qué dato basta para saber que una solicitud se paga por Lightning?

1. Que use la palabra sats.
2. Que llegue por chat.
3. Su formato y modalidad compatibles, no solo la unidad o el canal del mensaje.

> **Ver respuesta: Su formato y modalidad compatibles, no solo la unidad o el canal del mensaje.**
> Unidad de cuenta y red de pago son dimensiones distintas.

Taproot MuSig2 y futuro poscuántico

Objetivo

Distinguir estándares, propuestas y capacidades implementadas.

Comprender

Taproot permite condiciones de gasto con caminos de clave y de script. Las firmas Schnorr y la agregación pueden mejorar ciertas construcciones, pero el resultado de privacidad depende de cómo se configure y gaste. Que una dirección sea bc1p no demuestra que no haya otros participantes ni revela todas sus condiciones ocultas.

MuSig2 permite que un conjunto de firmantes agregue claves y produzca una firma Schnorr compatible mediante interacción. El estándar base es N de N. Un umbral arbitrario M de N requiere otra construcción o protocolo adicional. La gestión de nonces y sesiones es crítica y no se implementa mediante intercambio informal de mensajes.

PSBT v2 reorganiza información respecto a v0; no es una actualización automática de cualquier archivo que contenga una transacción de versión 2. Los firmwares Final de esta edición conservan PSBT v0, P2WSH/sortedmulti y SIGHASH_ALL para el perfil multifirma. Las futuras capacidades requieren contrato y validación propios.

NIST publicó en 2024 sus primeros estándares poscuánticos finalizados. Eso no cambia por sí mismo las firmas de Bitcoin. Usar un algoritmo poscuántico para autenticar firmware protegería esa capa; no convertiría automáticamente ECDSA o Schnorr de una UTXO en firmas poscuánticas. Tampoco existe una fecha de ataque futuro que el tutor pueda prometer con certeza.

Práctica

1. Clasifica cinco afirmaciones como estándar, implementación verificada, propuesta o publicidad.
2. Explica por qué «acepta un destinatario Taproot» no prueba «firma una entrada Taproot».
3. Dibuja capas separadas: firma de firmware, cifrado de secreto, chat y firma de gasto Bitcoin.

Demuestra

Puedes pedir evidencia específica de una capa y evitar trasladar garantías entre protocolos.

Duda frecuente

¿Debo migrar mis fondos por un titular sobre computación cuántica? Una decisión real exige evidencia técnica actual, soporte verificable, evaluación de riesgos y un plan de migración seguro; el curso no ordena movimientos por titulares.

Punto de pausa

Registra preguntas técnicas sin crear un plan de gasto automático.

Una firma poscuántica en el bootloader, si estuviera implementada y validada, ¿cambia las condiciones de firma de una UTXO existente?

1. No; son capas distintas.
2. Sí, convierte toda la red a otro algoritmo.
3. Elimina la necesidad de backups.

> **Ver respuesta: No; son capas distintas.**
> Autenticar una actualización no reescribe las condiciones de gasto de Bitcoin.

Interoperabilidad y salida del fabricante

Objetivo

Planificar continuidad si cambian el software, el dispositivo o el proveedor.

Comprender

La interoperabilidad no se comprueba con una lista de siglas. Debe conservar red, script, derivación, claves, política, formato de transacción y semántica de firmas. Dos aplicaciones pueden entender BIP174 y, aun así, no admitir los mismos campos, tamaños o tipos de entrada.

Para salir de una dependencia de interfaz, conserva información de recuperación documentada y ensaya con carteras de aprendizaje. Una mnemónica estándar puede permitir derivar claves, pero recuperar una multifirma requiere su política completa. Las etiquetas BIP329 añaden contexto de privacidad; el historial de chat tiene un alcance diferente.

No conviertas una prueba de compatibilidad en exposición de una semilla real. Primero comprueba exportación pública de descriptores y recuperación watch-only. Si una emergencia exige reconstruir claves, utiliza un entorno diseñado para ello y considera migrar después. Una wallet incompatible que muestra cero no demuestra por sí sola que los fondos se hayan perdido.

Mantén una copia verificable de documentación, versión del curso y herramientas necesarias. La firma de aplicaciones, certificados caducados y cambios de sistemas pueden afectar instalación. Un código abierto disponible no garantiza que cualquier persona pueda compilarlo años después sin conservar dependencias y conocimiento.

Práctica

1. Diseña una prueba de salida con una cuenta vacía: misma red, política y dirección de control en dos implementaciones compatibles.
2. Enumera qué piezas son estándares y cuáles requieren convertidor o documentación del formato Cuvex.
3. Define qué resultado permite afirmar compatibilidad y qué queda pendiente de hardware o firma real.

Demuestra

Puedes describir una ruta de recuperación sin depender de que una empresa siga ofreciendo el mismo servicio.

Duda frecuente

¿Código abierto significa que el fabricante ya no importa? No. Distribución, mantenimiento, componentes físicos y experiencia operativa siguen importando. Permite inspección y continuidad potencial, no una garantía automática.

Punto de pausa

Guarda resultados de laboratorio con versiones y límites observados.

¿Qué evidencia es más fuerte de interoperabilidad?

1. Que ambas apps digan «Bitcoin».
2. Reconstruir y comprobar en un laboratorio la misma política y dirección con versiones identificadas.
3. Que tengan iconos parecidos.

> **Ver respuesta: Reconstruir y comprobar en un laboratorio la misma política y dirección con versiones identificadas.**
> La prueba debe conservar las condiciones relevantes y un resultado verificable.

Laboratorio técnico con regtest

Objetivo

Entender un laboratorio reproducible sin confundir pruebas sintéticas y uso físico.

Comprender

Regtest permite crear una cadena local controlada para generar bloques y ensayar transacciones sin valor económico. Debe utilizar directorios y credenciales separados, sin importar material real. Sus resultados no demuestran por sí solos compatibilidad USB, NFC, Bluetooth o cámara de un equipo físico.

Un laboratorio completo registra versiones, configuración de red, política, entradas de prueba, PSBT, firmas, transacción final y resultado de aceptación. Puede comprobar que la suma cuadra, que una firma alterada se rechaza y que un pago válido entra en un bloque local. El ensayo debe incluir fallos, no solo el camino correcto.

La validación de Desk 9.21 informa de pruebas con Bitcoin Core 31 regtest y de pruebas automatizadas de motor y UI simulada. Esta edición las usa como evidencia documental, no afirma haber repetido esas pruebas ni haber ejecutado operaciones con dispositivos. La comprobación de un paquete tampoco prueba su instalación en todos los sistemas.

Antes de una clase técnica, el ingeniero debe entregar el laboratorio montado y el procedimiento compatible con la versión del alumno. No abras RPC a Internet para que el tutor lo controle. La IA puede guiar la interpretación de resultados sintéticos, pero no debe obtener credenciales ni permisos de administración.

Práctica

1. Con el laboratorio preparado, observa una transacción válida y otra con una firma alterada. Registra aceptación o rechazo.
2. Comprueba un caso de cambio incorrecto y otro de red incompatible.
3. Separa en tu informe «prueba de motor», «interfaz simulada» y «hardware físico».

Demuestra

Puedes describir exactamente qué se ha probado y qué queda pendiente, sin presentar una simulación como certificación.

Duda frecuente

¿Si regtest funciona ya puedo vender el curso como validado para todos los dispositivos? No. Faltan pruebas de recorridos físicos, instalación, accesibilidad, recuperación y servicio comercial.

Punto de pausa

Detén y guarda el laboratorio según sus instrucciones, conservando solo datos sintéticos.

Una prueba regtest del motor, ¿demuestra lectura NFC real en un teléfono concreto?

1. Sí, porque ambas usan Bitcoin.
2. Sí, si la PSBT es pequeña.
3. No; exige una prueba física separada.

> **Ver respuesta: No; exige una prueba física separada.**
> Los entornos de validación tienen alcances diferentes.

Proyecto final y plan de continuidad

Objetivo

Demostrar autonomía desde la preparación hasta recuperación y privacidad.

Comprender

El resultado del curso no es memorizar un menú: es poder explicar la intención, verificar el resultado y detener una operación que no entiendes. La evaluación combina conceptos, práctica guiada y un caso independiente. Nunca depende de revelar semillas, patrimonio o direcciones personales al evaluador.

Caso A: configura un entorno de aprendizaje, identifica modelos y versiones, protege Desk, vincula un criptograma didáctico y reconstruye una cuenta watch-only. Explica qué respaldos son necesarios y qué datos puede observar tu proveedor.

Caso B: diseña un pago con UTXOs ficticias de contextos distintos, justifica selección, verifica destinatario, cambio y comisión y narra la rama de firma correspondiente a tu dispositivo. Resuelve una interrupción de retorno y otra de publicación sin duplicar el pago. Si no hay hardware físicamente aceptado, la parte se registra como simulada y queda pendiente.

Caso C: diseña una 2 de 3, representa invitación y verificación, compara en Mirror un campo elegido en orden libre y explica el alcance del OK. Recupera la política de aprendizaje, simula pérdida de un participante y prepara continuidad y herencia.

La superación propuesta exige al menos 80 % en conocimientos y todos los controles críticos correctos: no revelar secretos, comprobar red y salidas, no confundir etapas y conservar recuperación. Un error crítico requiere revisión y nueva práctica; no se compensa con acertar preguntas de mercado. Un certificado comercial, si se emite, debe indicar qué se evaluó y si hubo observación física o solo simulación.

Práctica

1. Completa los tres casos con datos sintéticos y una explicación propia.
2. Resuelve la evaluación final del anexo y revisa cada respuesta fallida.
3. Entrega solo una hoja de resultados sin secretos, con evidencias de alcance y pendientes.

Demuestra

Puedes detenerte por iniciativa propia cuando una operación carece de evidencia suficiente y sabes qué necesitas para continuar.

Duda frecuente

¿Terminar las páginas equivale a estar preparado para custodiar cualquier importe? No. La capacidad debe probarse y el riesgo evaluarse según tu situación. La lectura y los ensayos no garantizan resultados futuros.

Punto de pausa

Conserva tu plan de revisión y las prácticas pendientes. Puedes volver al capítulo necesario sin repetir todo el curso.

¿Cuál es un requisito crítico para cerrar la formación práctica?

1. Haber abierto todas las páginas.
2. Demostrar recuperación y revisión de operaciones dentro de un alcance documentado, sin revelar secretos.
3. Predecir el precio del próximo mes.

> **Ver respuesta: Demostrar recuperación y revisión de operaciones dentro de un alcance documentado, sin revelar secretos.**
> El aprendizaje se acredita por capacidades y límites comprobados, no por navegación o predicción.

Manual del alumno

Manual operativo Cuvex

Este manual acompaña las lecciones. Cada procedimiento describe el flujo encontrado en los fuentes revisados, sus comprobaciones y su punto de parada. Es una edición candidata para piloto: no acredita ensayos físicos propios con Original, BIT, teléfonos o cada plataforma de escritorio. Antes de enseñar con fondos reales, el equipo debe completar la matriz de aceptación y ajustar cualquier rótulo o pantalla que difiera.

Referencias: Original 1.2.2 Final, BIT 1.2.3 Final, Desk 1.0.0-beta.9.21 y Mirror 1.0.0-beta.12.12. La selección de un perfil en Desk es compatibilidad declarada, no medición remota de firmware. Las capturas reales incluidas de Mirror proceden del emulador Android del paquete 12.12. Las fotografías de producto son material corporativo y no prueban la versión mostrada en un dispositivo actual.

P01 | Comprobar procedencia y versión | Cuvex | L16,L21 | C01,C02

Preparación: dispone de la compra y del canal oficial que puedas verificar de forma independiente. No introduzcas todavía secretos.

1. Inspecciona embalaje y precintos. Si hay signos de manipulación, detén la puesta en marcha y conserva evidencia no sensible.
2. Usa el flujo de integridad y sellos de la app compatible con tu entrega; introduce los códigos solo allí, nunca al tutor.
3. Identifica Original o BIT y la revisión disponible. Revisa versión visible del dispositivo y de las apps.
4. Compara con la matriz publicada por el equipo. Un catálogo o un hash no reemplazan autenticación de firmware ni aceptación física.

Resultado: modelo y versiones identificados, y procedencia revisada sin exposición de secretos. Si los códigos no son válidos o la interfaz difiere, no sigas una guía histórica para forzar el uso.

Pausa: antes de cargar material de custodia. La trazabilidad comercial no garantiza por sí sola ausencia de manipulación avanzada.

P02 | Actualizar Original por Bluetooth | Original | L46 | C01,C02,C03

Preparación: copias recuperables, alimentación estable, paquete oficial compatible y recorrido aceptado para tu sistema. La disponibilidad física completa en cada plataforma no está acreditada por este curso.

1. En dispositivos o firmware de la app, selecciona Original y la descarga oficial o el archivo local auténtico correspondiente.
2. Pon el dispositivo en actualización según su menú y conecta por el flujo de la aplicación. Mantén proximidad y evita sesiones competidoras.
3. Introduce el código de la pantalla de Original en el campo indicado. No lo confundas con contraseña de criptograma.
4. Sigue transferencia, validación, instalación y reinicio. No tomes el porcentaje como prueba de instalación.
5. Comprueba en Original la versión final y regístrala en la app si existe ese campo.

Resultado: versión comprobada en la pantalla tras reinicio y flujo final confirmado. Si falla antes de PIN, durante paquetes o al final, registra esa fase y el código. No desconectes ni cambies software de forma improvisada para «pasar el 99 %».

P03 | Actualizar BIT por USB | BIT | L46 | C01,C02,C03

Preparación: identifica el soporte real de BIT, alimentación y paquete oficial compatible. Conserva copias antes de cambiar software.

1. Selecciona BIT en el recorrido de firmware de Desk o Mirror compatible.
2. Conecta el dispositivo por el cable y adaptador de datos adecuados. Autoriza el acceso al volumen o carpeta cuando la app lo solicite.
3. Selecciona el firmware auténtico del modelo. Revisa versión y datos de compatibilidad antes de enviarlo.
4. Espera las etapas de transferencia y validación del dispositivo. Un volumen puede desaparecer o volver a montarse conforme al protocolo.
5. Tras reinicio, comprueba versión en BIT y el resultado final de la app.

Resultado: instalación comprobada en el propio equipo. Si el volumen no aparece, comprueba modo del dispositivo, cable de datos, permisos, montaje y otra sesión activa. No crees una carpeta con el mismo nombre en el PC como sustituto. La recuperación de una actualización fallida requiere el procedimiento oficial de ese hardware.

P04 | Generar cartera con moneda y dados | Cuvex | L17 | C01

Preparación: espacio privado, dados adecuados y moneda; sin micrófono del tutor activo ni cámaras. Utiliza una cartera de aprendizaje.

1. Abre crear wallet y el flujo de entropía del firmware. Fija previamente el orden de los cuatro dados.
2. Introduce moneda y cada dado como indique la pantalla, sin cambiar resultados por preferencia.
3. El fuente revisado calcula índice = moneda × 1.296 + (d1−1) × 216 + (d2−1) × 36 + (d3−1) × 6 + (d4−1). Solo acepta índices 0..2.047.
4. Ante rechazo vuelve a lanzar moneda y todos los dados. El aviso mantiene las palabras anteriores y pide repetir el conjunto.
5. Completa el algoritmo del dispositivo, incluida la validación final, protege la mnemónica y comprueba recuperación en privado.

Resultado: cartera generada por el recorrido completo, no palabras escogidas manualmente. Si pantalla y fuente no concuerdan, detén el uso. No uses un ejemplo público de dados, semilla o clave como material propio.

P05 | Cifrar un secreto | Cuvex | L18,L19 | C01

Preparación: elige modelo, formato de contenido y protección. La entrada en un PC o teléfono expone el origen aunque el destino quede cifrado.

1. Selecciona cifrar y el tipo BIP39, SLIP39, Monero o texto compatible. No intercambies diccionarios. El teclado de texto plano revisado admite hasta 500 caracteres; almacenar otro formato no implica poder firmar su red.
2. Introduce el contenido directamente en el dispositivo para conservar ese aislamiento. Revisa orden, caracteres y campos auxiliares en su pantalla.
3. Elige protección individual o compartida según el flujo, y biometría en BIT si procede. Diferencia este umbral del umbral Bitcoin.
4. Introduce y confirma las contraseñas en privado conforme al validador del firmware. No reutilices automáticamente reglas de Desk.
5. En Original graba en tarjeta vacía compatible; en BIT conserva los objetos de exportación del flujo USB. Espera confirmación.
6. Abre una recuperación de prueba para verificar el contenido y cierra el secreto al terminar.

Resultado: criptograma con recuperación comprobada. Si escritura o lectura falla, protege el original y sigue el reintento de la pantalla; no elimines cabeceras ni fuerces sobrescrituras.

P06 | Descifrar en el dispositivo | Cuvex | L18 | C01,C02

Preparación: privacidad física y componentes de desbloqueo suficientes; micrófono y captura de pantalla desactivados cerca del secreto.

1. Inicia descifrar en el modelo correcto y entrega el criptograma por NFC en Original o el flujo USB de BIT.
2. Comprueba alias e identificación del objeto antes de introducir credenciales.
3. Aporta las contraseñas necesarias y la biometría cuando el formato lo exija. No insistas automáticamente ante fallos: existe control de acceso y bloqueo.
4. Verifica el contenido únicamente en la pantalla prevista. Un QR de secreto tiene la misma sensibilidad que el texto.
5. Cierra o termina el proceso conforme al dispositivo y guarda soporte y credenciales por separado según tu plan.

Resultado: contenido recuperado en privado y sesión terminada. Si no se reconoce el formato, falla autenticación o aparece contenido inesperado, no lo «corrijas» con una app desconocida. Describe al soporte versión, formato y error, sin adjuntar el secreto.

P07 | Preparar recuperación de un criptograma biométrico | BIT | L19,L47 | C01,C02

Preparación: criptograma de aprendizaje y documentación de su formato. No deduzcas una recuperación por el simple hecho de tener una copia .bin.

1. En la ficha de Desk identifica si hay componentes biométricos y qué exportación de recuperación está disponible.
2. Conserva el conjunto de archivos que el flujo asocia y una copia independiente, con identificadores discretos.
3. Prueba el desbloqueo normal en BIT y documenta qué contraseñas y condiciones requiere.
4. Estudia la vía excepcional de recuperación local y sus formatos admitidos. Verifica que el material necesario existe antes de necesitarlo.
5. Ensaya con datos sin fondos el escenario de dispositivo averiado o huella no disponible.

Resultado: un plan probado, con sus límites, para ese formato concreto. No se afirma que cualquier biometría se pueda omitir ni que una huella sustituya las copias. Si se recupera un secreto en un PC, evalúa su exposición y la necesidad de migrar control después.

P08 | Crear y comprobar una copia de criptograma | Cuvex y Desk | L20 | C01,C02

Preparación: una copia original identificada y un destino compatible sin datos a preservar.

1. Para Original, utiliza clonar del dispositivo o la función compatible de Desk y presenta origen y destino en el orden indicado.
2. Mantén las tarjetas estables y respeta el rechazo de soportes que ya contienen criptogramas.
3. Para BIT o archivo, exporta el conjunto de componentes del flujo y conserva nombres o asociación necesarios.
4. Aísla la copia original y realiza lectura y recuperación de prueba desde la nueva.
5. Registra privadamente fecha, formato y resultado; guarda las copias con riesgos físicos independientes.

Resultado: una segunda copia probada. No implica una wallet distinta, revocación de contraseñas ni protección frente a una semilla que ya se filtró. Si falla el destino, conserva el original sin intentar «repararlo» para que ambos coincidan.

P09 | Crear desbloquear y cambiar contraseña de Desk | Desk | L21,L40 | C02

Preparación: instalador verificado, arquitectura adecuada y un plan de respaldo del almacén.

1. Crea el almacén con contraseña única de 12 a 1.024 caracteres y confirmación coincidente.
2. Bloquea y vuelve a abrir para comprobar que conservas acceso. La contraseña se introduce solo en Desk.
3. En Seguridad y Acceso y bloqueo revisa inactividad y paso a segundo plano. No actives borrado opcional durante una demostración.
4. Para cambiar contraseña aporta la actual y confirma la nueva por su flujo.
5. Si usabas biometría del PC, vuelve a configurarla según la indicación. Crea copia actual y conserva la relación con copias anteriores.

Resultado: acceso comprobado. Las copias previas conservan su contraseña y cifrado originales. Biometría de PC y biometría de BIT son mecanismos distintos. Si falla acceso, detén intentos repetidos y revisa recuperación sin pedir al tutor que guarde credenciales.

P10 | Vincular y revisar un criptograma en Desk | Desk | L22 | C02

Preparación: criptograma de prueba de procedencia conocida y transporte disponible.

1. Abre criptogramas o tarjetas y selecciona vincular mediante NFC, USB o copia compatible.
2. Selecciona diseño y fuente; usa Cuvex Mirror enlazado por Bluetooth al ordenador para NFC, o el volumen de Cuvex BIT conectado por USB-C. Los lectores NFC USB externos no están admitidos en Cuvex Desktop.
3. Revisa la ficha: alias, origen, tamaño, formato y condiciones interpretadas. Es metadato, no contenido descifrado.
4. Comprueba si hay cuentas conservadas pendientes de asociación y relaciona solo la cuenta verificada.
5. Exporta una copia si falta cobertura y prueba recuperación por separado.

Resultado: objeto organizado localmente. «Vinculado» no demuestra autenticación de la semilla ni saldo. Un objeto no reconocido exige comprobar formato y versión, sin cambiar extensión o borrar datos hasta que la app lo acepte.

P11 | Activar una cuenta WOW watch-only | Desk y Cuvex | L13,L22 | C01,C02

Preparación: información pública obtenida del flujo del dispositivo y control privado de su procedencia.

1. Abre activar WOW o añadir cuenta desde el criptograma correcto.
2. Importa el descriptor o material público admitido por archivo, webcam o Mirror según la función.
3. Revisa red, script, origen, huella, ruta y checksum cuando corresponda. No introduzcas semillas o xprv.
4. Nombra la cuenta y escoge fuente de consulta con consentimiento.
5. Comprueba una dirección de control y el alcance del descubrimiento antes de interpretar saldo.

Resultado: cartera de observación asociada. Si ves cero, comprueba red, passphrase original, derivación, cuenta, proveedor y escaneo sin concluir que las monedas desaparecieron. Una interfaz admite redes generales que no necesariamente admite el perfil multifirma: respeta cada contexto.

P12 | Configurar nodo y sincronización | Desk | L25,L33 | C02

Preparación: decisión de privacidad y, si utilizas Core, acceso a un nodo protegido y sincronizado.

1. En Seguridad y Privacidad y nodos elige la cuenta WOW y revisa su proveedor.
2. Escoge expresamente proveedor público compatible o Core. Para Core introduce endpoint, wallet y credenciales solo en la app.
3. Autoriza la consulta comprendiendo qué datos recibe cada servicio. TLS no oculta la consulta al proveedor.
4. Sincroniza y revisa fecha, punta, progreso y estado completo. Para rescan comprueba antigüedad cubierta y continuidad del trabajo.
5. Ante 429 respeta la pausa. Ante fallo no supongas que otro nodo se activó: la configuración no rota silenciosamente.

Resultado: fuente y estado conocidos. No abras RPC a Internet, compartas contraseña ni reduzcas descubrimiento a direcciones con saldo. Un historial vacío puede ser un resultado parcial.

P13 | Generar y recuperar solicitud de recepción | Desk y Cuvex | L26 | C01,C02

Preparación: cuenta, red y política comprobadas.

1. Abre recibir y genera o recupera la solicitud adecuada.
2. Añade observador, motivo e importe esperado solo si necesitas esos metadatos locales.
3. Verifica dirección por el recorrido compatible del dispositivo antes de un cobro relevante. Si falta aceptación física, detén la práctica en simulación.
4. Comparte exclusivamente los datos necesarios mediante el canal autenticado del receptor.
5. Comprueba ingreso, importe y confirmaciones en tu fuente de red.

Resultado: cobro conciliado, no solo solicitud emitida. En multifirma las direcciones mostradas se conservan para pagos tardíos y no se reasignan. Si el límite de nuevas direcciones sin historial se alcanza, recupera solicitudes previas; no fuerces índices manualmente.

P14 | Etiquetas congelación y BIP329 | Desk | L27 | C02,B13

Preparación: cuenta de laboratorio con UTXOs y una contraseña para la exportación protegida.

1. Etiqueta una entrada con su contexto sin datos personales innecesarios.
2. Congela o descongela conscientemente y revisa el saldo gastable. La restricción es local.
3. Exporta etiquetas mediante la función protegida. Distingue BIP329 como formato del cifrado del archivo.
4. Importa en una copia compatible; revisa coincidencia de referencias, etiquetas y congelaciones.
5. Conserva un respaldo de metadatos actualizado junto con su contraseña, de acuerdo con tu plan.

Resultado: contexto conservado y selección entendida. Una importación no debe usarse para desbloquear automáticamente monedas congeladas sin revisión. No envíes el archivo de etiquetas al tutor: puede revelar contrapartes y relaciones aunque no incluya claves de gasto.

P15 | Preparar un pago y enviar el total | Desk | L28 | C02

Preparación: solicitud verificada y cuenta con entradas gastables suficientes.

1. Abre pagar desde WOW, UTXOs o chat y confirma cuenta y red.
2. Selecciona entradas, destinatarios e importes, y revisa los contextos que se relacionan.
3. Elige tarifa y revisa comisión absoluta, cambio y advertencias. Si hay dust, revisa alternativas sin aceptar una comisión oculta.
4. Para enviar total comprueba el neto tras comisión. En chat confirma de forma explícita un pago parcial si no cubre la solicitud.
5. Prepara el borrador y revisa todos los datos antes de exportar para firma.

Resultado: intención comprensible y PSBT de esa operación. Un formulario general puede admitir más entradas o destinatarios que el hardware: aplica los límites efectivos del firmante y transporte. Si cambian salidas o condiciones, se inicia una nueva revisión.

P16 | Firmar y devolver una PSBT con Original | Original y Mirror | L29 | C01,C02,C03

Preparación: borrador correcto, tarjeta de transporte compatible, criptograma autenticado compatible y medios de desbloqueo en privado. Una copia histórica sin autenticidad verificada puede requerir recuperación comprobada y creación de copia nueva antes de firmar; no se corrige editando su cabecera.

1. Exporta la solicitud por el flujo NFC compatible desde Desk/Mirror.
2. Llévala a Original; aporta el criptograma cuando se solicite y desbloquea sin dictar credenciales.
3. Revisa red, resumen, salidas completas, comisión, cambio y avisos obligatorios.
4. En multifirma Final, decide si examinar parámetros ampliados; completa las tres confirmaciones finales solo si todo coincide.
5. Espera escritura y relectura de la respuesta en la tarjeta.
6. Lee la respuesta con Cuvex Mirror y valídala en la operación de Desk.

Resultado: firma recibida y vinculada al borrador, todavía distinta de publicación. Si falla escritura, conserva el estado y sigue el reintento. Nunca uses la tarjeta de respaldo como soporte prescindible de pago.

P17 | Firmar recibir y acusar con BIT | BIT y Desk | L29 | C01,C02

Preparación: borrador correcto, criptograma autenticado compatible y volumen real de BIT seleccionado. Si una copia histórica se rechaza para firma, sigue la recuperación y renovación indicada, sin forzar el formato.

1. Entrega la solicitud por USB-C mediante el servicio de Desk y sigue la pantalla del dispositivo para el criptograma.
2. Desbloquea en privado y revisa resumen, todas las salidas, comisión y avisos.
3. En multifirma Final, revisa opcionalmente detalles ampliados y autoriza con las confirmaciones finales obligatorias.
4. En Desk utiliza recibir del BIT para importar y validar la respuesta de ese trabajo.
5. Comprueba guardado y acuse. Si el acuse falla después de recibir, reintenta la misma operación, no una nueva elegida por el modelo.

Resultado: firma verificada y estado de intercambio coherente. Si se desconecta antes de recibir o después de guardar, conserva el perfil de la solicitud. No cambies a otro firmware de catálogo para hacer encajar una respuesta pendiente.

P18 | Finalizar publicar y seguir una operación | Desk | L30,L44 | C02

Preparación: firmas verificadas y umbral suficiente cuando corresponda.

1. Revisa de nuevo intención, entradas, salidas, comisión y red.
2. Finaliza mediante la acción correspondiente y comprueba que no faltan firmas ni condiciones.
3. Autoriza difusión y conserva el resultado local. Si se pierde la respuesta de red, consulta antes de repetir.
4. Sigue mempool y confirmaciones en el proveedor elegido con fecha de sincronización.
5. Si se plantea RBF, revisa la nueva operación y consigue las firmas requeridas. No supongas una función CPFP integrada.

Resultado: estado de cadena comprobado con su fuente. Cancelar un borrador no revoca firmas ya exportadas y no reescribe pagos confirmados. Un mensaje del chat o una captura no sustituyen el seguimiento.

P19 | Comparar dos QR de política libremente | Mirror | L43 | C03,C02

Preparación: campo visible en Desk y Cuvex; en la práctica utiliza solo las muestras sintéticas del curso.

1. Abre Comparar políticas y lee primero cualquiera de los dos lados.
2. Escoge el dato que quieras comprobar; puedes empezar por el paso 15 y omitir otros revisados manualmente.
3. Lee su contraparte y revisa ambos textos completos. Si el paso es ambiguo, usa Indicar paso de Desk y entiende que el contexto es manual.
4. Interpreta Coincide o No coincide solo para ese par literal. Espacios, mayúsculas y codificación cuentan.
5. Inicia otro par en cualquier orden. Sal o pasa a segundo plano para terminar según el comportamiento de borrado revisado.

Resultado: comparación local puntual. No acredita origen, sesión, aprobación global o activación. Una diferencia debe aclararse con sus fuentes, sin normalizar el texto para forzar un OK.

P20 | Activar recuperar y trasladar chat | Desk y Cuvex | L36,L39 | C02

Preparación: entorno DEV o Producción elegido, un alias y Clave Chat en el dispositivo, nunca en el curso.

1. Abre activar o recuperar chat desde el contexto del criptograma.
2. Elige alias nuevo o traslado existente y el perfil móvil compatible indicado por la app.
3. Introduce o lee la Clave Chat exclusivamente en el flujo privado. No uses semilla, PIN ni clave de WOW.
4. Comprueba activación con el servicio; si queda pendiente utiliza la acción de completar o comprobar, sin darla por correcta.
5. Verifica continuidad con contactos tras un traslado y evita uso simultáneo del mismo alias en varios equipos.

Resultado: identidad activada o recuperada en el entorno correcto. Historial y sesiones anteriores no se recuperan automáticamente con la Clave Chat ni con la copia global de Desk. Conserva los límites del material disponible.

P21 | Verificar identidad de un contacto | Desk | L36,L48 | C02

Preparación: canal independiente acordado previamente con la persona.

1. Añade el alias y consulta su identidad pública mediante la app.
2. Compara huella por el canal autenticado, no únicamente dentro de la conversación recién creada.
3. Si usas reconocimiento, evita información pública o secretos reutilizados en otros servicios.
4. Confirma solo tras resolver diferencias. Ante cambio de identidad suspende pagos y coordinación hasta verificar.
5. Documenta el método de verificación sin almacenar respuestas sensibles en el curso.

Resultado: confianza contextual en el contacto, no una garantía de todas sus solicitudes futuras. La voz puede ser imitada y un equipo legítimo comprometido. Cada operación mantiene su revisión.

P22 | Pedir dirección solicitar y pagar por chat | Desk y Cuvex | L37 | C02,C01

Preparación: contacto verificado y cuenta WOW compatible.

1. Selecciona solicitar dirección, responder con dirección o solicitar pago según la intención.
2. Revisa solicitud original, red, importe y nota antes de enviarla.
3. Para pagar, abre la preparación desde la cuenta adecuada, selecciona UTXOs y tarifa y revisa el importe neto.
4. Autoriza en Cuvex por el procedimiento del modelo. El chat no firma automáticamente.
5. Sigue publicación y confirmación por tu fuente; concilia pagos parciales explícitos con la solicitud original.

Resultado: coordinación conservando la revisión de custodia. Estado de mensaje y estado de transacción no son equivalentes. Un enlace a explorador puede enviar información a un tercero: evalúa su uso antes de abrirlo.

P23 | Compartir y vincular un criptograma recibido | Desk | L38 | C02

Preparación: necesidad concreta de compartir, contacto verificado y definición de medios de acceso que recibirá.

1. Selecciona compartir criptograma desde la acción de chat y revisa el objeto.
2. No adjuntes contraseñas, semilla o Clave Chat como comentario.
3. El receptor comprueba procedencia y vincula el objeto compatible mediante su acción de recepción.
4. Evalúa qué capacidad obtiene ahora y qué obtendría si consigue suficientes credenciales de desbloqueo.
5. Conserva un plan de revocación realista: borrar mensajes no retira copias externas ni claves conocidas.

Resultado: transferencia consciente de un objeto cifrado. No es un pago ni incorpora por sí sola una clave a una multifirma. Si el adjunto pide acudir a una página desconocida para descifrar, detén el flujo.

P24 | Copia global y restauración de Desk | Desk | L15,L21 | C02

Preparación: almacén de aprendizaje y destino de copia controlado.

1. Abre la función de copia del almacén y define la contraseña indicada; conserva su relación con esta copia concreta.
2. Guarda fuera del único equipo de uso y comprueba procedencia e integridad por el flujo.
3. Restaura en un entorno de pruebas separado y verifica cuentas, configuración y datos cubiertos.
4. Revisa exclusiones: chat, sus sesiones e historial no se deben asumir incluidos; política multifirma y claves privadas no son intercambiables.
5. Repite tras cambios importantes y conserva las instrucciones de recuperación.

Resultado: respaldo cuyo alcance y contraseña se conocen. Las copias antiguas conservan contraseñas anteriores. Si se cambia acceso o hay exposición, evalúa también esas copias; no basta con modificar el almacén actual.

P25 | Crear y aceptar una multifirma | Desk y Cuvex | L41,L42 | C01,C02

Preparación: participantes independientes, contactos verificados, red y límites efectivos acordados.

1. El creador elige nombre, M/N, red, participantes y vigencia operativa.
2. Aporta la clave pública extendida correcta con huella y ruta BIP48 por el flujo compatible.
3. Cada participante revisa, acepta o rechaza y aporta su material público. Nunca comparte semilla.
4. Construye la política completa y prepara su verificación en cada dispositivo.
5. Conserva copias de política antes de financiar. Comprueba la dirección de control y la capacidad de recuperación.

Resultado: propuesta completa y verificable. La aceptación de invitación no sustituye revisión de hardware. Si interviene Original, aplica su máximo de seis claves y el tamaño NFC; BIT no amplía las capacidades de los demás participantes.

P26 | Verificar política y recibir confirmación | Desk y Cuvex | L43 | C01,C02,C03

Preparación: misma política completa para todos, perfil de firmware correcto y dispositivo sin operaciones competidoras.

1. Inicia verificar políticas en el contexto compatible. Original requiere selección explícita del perfil instalado; BIT negocia capacidades según su contrato.
2. Entrega la solicitud por NFC/Mirror o USB-C según modelo.
3. Revisa los campos de política en el dispositivo. Usa Mirror como comparador opcional de pares elegidos sin orden obligatorio.
4. Completa la confirmación del equipo y devuelve su respuesta por el transporte correspondiente.
5. En Desk valida la respuesta vinculada a la solicitud. No sustituyas este paso por un OK visual del comparador.

Resultado: revisión correlacionada con alcance de esa revisión. El catálogo no atesta remotamente firmware y el dispositivo no se presenta como almacén persistente de políticas. Ante FIRMWARE_CAPABILITY_REQUIRED, revisa primero versión de Desk y combinación modelo/build.

P27 | Pedir firmas recibir y traspasar coordinación | Desk y Cuvex | L44 | C01,C02

Preparación: política verificada, operación identificada y destinatarios acordados.

1. Prepara entradas, salidas, comisión y notas y solicita firmas a participantes compatibles.
2. Cada participante revisa y firma en su equipo por su rama de transporte.
3. Recibe, valida y guarda cada firma; resuelve acuses pendientes sin cambiar el perfil conservado.
4. Si se traspasa coordinación, el receptor acepta el flujo y verifica estado. No cambia por ello M/N ni propiedad de claves.
5. Al alcanzar umbral, revisa y finaliza antes de publicar. Sigue la transacción por la red.

Resultado: coordinación con evidencias diferenciadas. Un informe de progreso del coordinador no es una verificación local tuya. Cancelar o rechazar en una app no destruye necesariamente firmas ya conservadas por terceros.

P28 | Exportar restaurar y eliminar multifirma local | Desk | L45 | C02

Preparación: política conocida y copia cifrada con contraseña única.

1. Exporta recuperación mediante la acción de Desk. El flujo actual usa un contenedor autenticado CVXMSBK1 para esa exportación.
2. Conserva copia y contraseña con riesgos independientes. No deduzcas cifrado por extensión de archivos históricos.
3. Para restaurar aporta copia, contraseña y clave pública de participante con origen correcto por webcam o Mirror si procede.
4. Comprueba política, red, dirección y descubrimiento antes de operar.
5. Para eliminar localmente, lee alcance y confirmación y guarda copia si quieres conservar recuperación. Restaurar después es explícito.

Resultado: política recuperable o eliminación local consciente. Eliminar no mueve fondos, no borra claves de otros firmantes ni cancela por sí sola operaciones que conservan otras personas.

P29 | Recuperación excepcional en un PC | Desk | L47 | C02

Preparación: material de formato admitido, entorno limpio preparado y copia de seguridad. Esta operación puede revelar un secreto al PC; utiliza datos de aprendizaje en el curso.

1. Inicia recuperación local desde el contexto correcto y lee las limitaciones del formato y los avisos.
2. Acepta el riesgo conscientemente y desconecta la red como exige el flujo; la ventana comprueba estado antes de permitir continuar.
3. Introduce únicamente las credenciales necesarias en la ventana privada. No se dictan, pegan en el curso ni comparten con soporte.
4. Activa visualización solo en un espacio sin cámaras o asistentes escuchando; respeta temporizador y cierre.
5. Termina, revisa qué exposición pudo existir y planifica migración a claves nuevas si procede.

Resultado: recuperación excepcional, no garantía de borrado forense o equivalencia con hardware aislado. Si falta autenticación, formato o material de acceso, no pruebes herramientas de Internet con tu copia real.

P30 | Revisar preferencias biometría y bloqueo | Desk | L40 | C02

Preparación: contraseña conocida y respaldo probado antes de modificar seguridad.

1. En Acceso y bloqueo revisa contraseña, biometría disponible, inactividad y bloqueo al pasar a segundo plano.
2. Comprende la demora tras fallos y el máximo configurado antes de cambiarlo.
3. Mantén el borrado opcional desactivado hasta comprender condiciones, umbral y recuperación. No lo pruebes en producción.
4. En Preferencias ajusta idioma, tema, moneda, sincronización de 3 o 5 minutos y sonidos.
5. Si registras enlaces bitcoin:, comprueba que abrir una solicitud mantiene desbloqueo, selección y revisión; no paga por sí solo.

Resultado: configuración entendida. La biometría del sistema operativo depende del equipo y no sustituye contraseña ni respaldo. Las preferencias visuales no modifican la política de Bitcoin.

P31 | Eliminar registros sin confundir su alcance | Desk | L22,L45 | C02

Preparación: identifica si vas a eliminar criptograma local, cuenta, WOW, chat o multifirma y qué copia conservarás.

1. Lee el objeto seleccionado y su aviso. Confirma alias exacto o condición explícita cuando la app lo pida.
2. Exporta y prueba copia si necesitas recuperar ese estado más tarde.
3. Elimina únicamente el objeto previsto y comprueba las asociaciones que conserva o retira el flujo.
4. Revisa si quedan operaciones o participantes externos. No asumas que desaparecen mensajes, firmas o archivos de otros equipos.
5. Documenta el cambio en tu inventario privado sin datos sensibles en el curso.

Resultado: estado local gestionado conscientemente. Ninguna de estas acciones cambia por sí sola scripts de UTXOs financiadas, destruye una semilla conocida por terceros o revierte transacciones confirmadas.

P32 | Diagnosticar sin exponer secretos | Desk y Mirror | L23,L30,L48 | C02,C03

Preparación: anota hora aproximada, sistema, arquitectura, versión y fase. Evita seguir repitiendo una operación sensible sin conocer su estado.

1. Identifica si el fallo es búsqueda, enlace, lectura, escritura, validación, firma, retorno, red o visualización.
2. Copia el código y texto del error sin incluir QR o datos privados. Usa diagnósticos de la app cuando proceda.
3. Revisa el archivo antes de compartirlo; no adjuntes copia del almacén, criptograma, semilla, Clave Chat, descriptor o credencial RPC.
4. En una incidencia de interfaz, registra tamaño de ventana, zoom y controles ocultos con una escena sintética.
5. Envía por el canal oficial un resultado esperado y pasos reproducibles. El curso no envía mensajes a soporte automáticamente.

Resultado: informe que permite investigar con mínimo dato. Si no hay evidencia de una etapa, se registra «pendiente», no «completada». La asistencia de voz no necesita acceso remoto a tu equipo de custodia.

Glosario de Bitcoin y autocustodia

Bitcoin

Red y conjunto de reglas para transferir valor y verificar su historia sin un administrador único del registro.

BTC

Unidad monetaria de Bitcoin; un BTC equivale a cien millones de satoshis.

Satoshi

Unidad de la cadena base equivalente a una cienmillonésima de BTC.

Blockchain

Historia de bloques enlazados y verificados bajo unas reglas; no describe por sí sola todas las propiedades de una red.

Bloque

Conjunto de datos que incluye transacciones y una cabecera validable.

Nodo completo

Software que verifica las reglas de los bloques y transacciones que acepta.

Minería

Construcción de bloques mediante prueba de trabajo bajo las reglas de la red.

Prueba de trabajo

Mecanismo que exige un trabajo computacional verificable para proponer un bloque.

Consenso

Compatibilidad de los participantes sobre las reglas y la historia válida que aceptan.

Política de mempool

Reglas locales de aceptación y retransmisión que no equivalen necesariamente a reglas de consenso.

Mempool

Conjunto local de transacciones no confirmadas conservadas por un nodo.

Confirmación

Inclusión en un bloque de la cadena aceptada y profundidad posterior de ese bloque.

Reorganización

Cambio de un tramo de la cadena aceptada que puede alterar confirmaciones.

UTXO

Salida de transacción no gastada que puede consumirse bajo sus condiciones.

Entrada

Referencia a una salida previa y datos necesarios para autorizar su gasto.

Salida

Valor y condición de gasto creados por una transacción.

Cambio

Salida que devuelve al control propio parte de las entradas tras el pago y la comisión.

Comisión

Diferencia entre valor de entradas y salidas de una transacción.

vbyte

Unidad de tamaño virtual utilizada para expresar el coste relativo de una transacción.

sat por vbyte

Tarifa de comisión expresada en satoshis por tamaño virtual.

Dust

Salida pequeña según políticas y coste de gasto; su umbral depende del contexto y script.

RBF

Sustitución de una transacción no confirmada bajo políticas compatibles; no es una cancelación garantizada.

CPFP

Uso de una transacción hija para mejorar el incentivo de incluir el conjunto con su padre.

Hash

Huella de datos útil para integridad; no cifra ni identifica por sí sola a su autor.

Clave privada

Capacidad criptográfica de producir autorizaciones bajo el esquema correspondiente.

Clave pública

Dato que permite verificar firmas y construir determinadas condiciones sin exponer la clave privada.

Firma digital

Prueba criptográfica de autorización de un mensaje concreto; no oculta su contenido.

Cifrado

Protección de confidencialidad mediante una clave y un algoritmo.

Cifrado autenticado

Cifrado con comprobación de alteraciones según su diseño.

AES GCM

Familia de cifrado autenticado utilizada en formatos del ecosistema; sus propiedades dependen de implementación y manejo de claves.

Mnemónica

Representación en palabras de material de generación y comprobación según un formato determinado.

Semilla

Material desde el que se derivan claves; el término se usa coloquialmente también para las palabras y exige aclarar contexto.

Entropía

Imprevisibilidad del material de generación; no se obtiene escogiendo palabras memorables.

Checksum

Suma de comprobación que detecta determinados errores; no autentica al autor.

BIP39

Especificación de mnemónicas y derivación de semilla con passphrase opcional.

Passphrase BIP39

Entrada adicional de derivación; una diferente puede producir otra cartera válida y vacía.

BIP32

Especificación de derivación jerárquica de claves.

Ruta de derivación

Secuencia de ramas utilizada para obtener claves de una raíz.

Derivación endurecida

Paso de derivación indicado habitualmente con comilla o h y con propiedades diferentes a la derivación pública ordinaria.

xpub

Clave pública extendida con contexto para derivación; sensible para privacidad.

xprv

Clave privada extendida; no debe compartirse ni importarse a un curso.

Huella maestra

Identificador corto de una raíz; útil para asociación, no una prueba de identidad suficiente.

Descriptor

Expresión de construcción de scripts con claves y derivaciones; puede ser público o contener material privado.

Watch only

Cartera de observación que carece de capacidad privada suficiente para firmar por sí sola.

WOW

Denominación de las cuentas de observación y gestión de cartera en el ecosistema Cuvex.

Wallet caliente

Herramienta con capacidad de firma en un entorno conectado.

Autocustodia

Modelo en el que el usuario conserva capacidad técnica de gasto individual o compartida bajo su política.

Custodio

Entidad que controla capacidad de gasto por cuenta del cliente y aplica sus condiciones de acceso.

Criptograma Cuvex

Objeto cifrado que protege un secreto; no es por sí mismo una transacción ni saldo.

Contraseña de Desk

Protección de acceso al almacén local; no equivale a semilla ni contraseña del criptograma.

Clave Chat

Secreto de recuperación de identidad de chat; su aspecto puede parecer público sin serlo.

PIN de enlace

Código temporal de una sesión de conexión; no es una contraseña de custodia.

Air gap

Separación operativa de entornos; los datos transportados aún requieren validación.

NFC

Tecnología de comunicación cercana utilizada con tarjetas y lectores compatibles.

USB Mass Storage

Interfaz de intercambio por archivos del modelo BIT; requiere protocolo, validación y acuses propios.

PSBT

Contenedor de información y firmas para coordinar construcción y autorización de transacciones.

PSBT v0

Versión de formato definida en BIP174 y utilizada por el perfil multifirma Final revisado.

PSBT v2

Versión definida en BIP370; no se deduce de que la transacción tenga versión 2.

SIGHASH ALL

Modo de compromiso de firma utilizado en el perfil revisado; su alcance técnico es parte de la validación de la operación.

P2WPKH

Tipo de condición SegWit de una clave asociado habitualmente a cuentas BIP84.

P2WSH

Condición SegWit que compromete un script; usada por la multifirma Final revisada.

P2TR

Tipo de salida Taproot; admitirla como destinatario no implica firmar desde ella.

sortedmulti

Construcción multifirma con orden determinista de claves para generar scripts.

Umbral M de N

Número M de autorizaciones necesarias entre N participantes según la política concreta.

MuSig2

Protocolo de agregación Schnorr cuyo esquema base es N de N; distinto de un umbral arbitrario.

Taproot

Conjunto de mecanismos de gasto y compromiso de Bitcoin con caminos de clave y de script.

Miniscript

Lenguaje para describir y analizar determinadas políticas de script; no implementado en el perfil Final revisado.

Regtest

Red local de laboratorio controlada por quien monta el entorno, sin valor económico.

Signet

Red de pruebas con características propias; no intercambiable por defecto con regtest.

Mainnet

Red Bitcoin de uso económico real.

Gap limit

Criterio de hueco de direcciones sin historial utilizado para descubrimiento, con ámbito que depende de la cartera.

Coin control

Selección consciente de las UTXOs que se van a gastar.

Consolidación

Combinación de salidas para reducir fragmentación, con implicaciones de coste y privacidad.

Pseudonimato

Uso de identificadores que no son directamente un nombre civil, sin anonimato automático.

Anonimato

Propiedad contextual de indistinguibilidad frente a observadores definidos; no una etiqueta garantizada por una app.

Metadatos

Información sobre comunicaciones o actividad como tiempos, tamaños y relaciones, diferente del contenido.

CoinJoin

Construcción colaborativa que dificulta ciertas inferencias sin garantizar anonimato permanente.

Payjoin

Pago colaborativo con entradas de pagador y receptor bajo un protocolo compatible.

Tor

Red y herramientas de protección de conexión; su uso debe configurarse por aplicación y verificarse.

VPN

Canal que desplaza parte de la confianza de conexión a su operador; no oculta la cadena.

Lightning

Sistema de pagos por canales con requisitos y riesgos diferentes de un envío on-chain.

Invoice

Solicitud estructurada de pago cuyo formato y modalidad deben identificarse.

RPC

Interfaz de llamadas a un servicio como Bitcoin Core; debe autenticarse y protegerse.

TLS

Protección de transporte frente a determinadas amenazas; el servidor receptor sigue viendo las solicitudes.

SRTP

Protección de audio en ciertos tramos VoIP; no implica automáticamente secreto frente al operador.

Idempotencia

Propiedad que evita duplicar un efecto al repetir una solicitud identificada.

Webhook

Evento enviado entre servidores cuya autenticidad y repetición deben comprobarse.

RAG

Recuperación de fragmentos de conocimiento para fundamentar una respuesta con contexto y versión.

Teach back

Comprobación de aprendizaje pidiendo al alumno que explique lo entendido con sus palabras.

Phishing

Engaño para obtener acceso o inducir una acción mediante suplantación y contexto convincente.

Ingeniería social

Manipulación de decisiones humanas que puede usar datos verdaderos y urgencia.

Notarización

Control de distribución de Apple distinto de una auditoría del producto o prueba física de todos sus flujos.

Atestación

Evidencia de estado bajo un mecanismo concreto; el catálogo de compatibilidad de Desk no es una medición remota.

MiCA

Marco europeo para determinados criptoactivos y servicios; no garantiza rentabilidad o compensación total.

Travel Rule

Obligaciones de información en transferencias bajo su ámbito; no se eluden por usar autocustodia.

Checkpoint

Punto de reanudación de aprendizaje con datos mínimos, sin información de cartera.

Comprueba lo que has aprendido

Practica sin fondos reales. La evaluación es libre y no requiere una cuenta.

¿Quién autoriza el gasto en el uso habitual de Cuvex?

1. El dispositivo con revisión del usuario
2. El tutor por voz
3. El servidor del curso

> **Ver respuesta: El dispositivo con revisión del usuario**
> La autorización conserva su recorrido en Cuvex.

¿Cuántos satoshis son 0,001 BTC?

1. 1.000
2. 100.000
3. 1.000.000

> **Ver respuesta: 100.000**
> Un BTC son 100.000.000 sat.

Entradas 120.000 y salidas 119.000 sat. ¿Comisión?

1. 1.000 sat
2. 119.000 sat
3. 1 sat/vB sin más datos

> **Ver respuesta: 1.000 sat**
> La diferencia de valores es la comisión absoluta.

Una transacción firmada todavía no difundida está:

1. Confirmada
2. Irreversible por estar firmada
3. Autorizada pero no necesariamente publicada

> **Ver respuesta: Autorizada pero no necesariamente publicada**
> Firma y publicación son etapas distintas.

200 vB a 6 sat/vB equivale a:

1. 206 sat
2. 1.200 sat
3. 6 % del envío

> **Ver respuesta: 1.200 sat**
> Tamaño virtual por tarifa.

Antes de retirar de un exchange debes comprobar:

1. Solo la comisión más baja
2. Activo red dirección e importe neto compatibles
3. La semilla de la contraparte

> **Ver respuesta: Activo red dirección e importe neto compatibles**
> No todas las redes con un símbolo BTC son Bitcoin on-chain.

Una firma digital por sí sola:

1. Oculta todo el mensaje
2. Autoriza un mensaje verificable bajo su esquema
3. Borra datos publicados

> **Ver respuesta: Autoriza un mensaje verificable bajo su esquema**
> La confidencialidad requiere otro mecanismo.

Cambiar una passphrase BIP39 puede:

1. Crear otra cartera válida y aparentemente vacía
2. Restablecerse siempre por email
3. Cambiar el registro público de pagos anteriores

> **Ver respuesta: Crear otra cartera válida y aparentemente vacía**
> La passphrase participa en la derivación.

La xpub de una cuenta se debe tratar como:

1. Dato sin ninguna consecuencia
2. Semilla privada idéntica
3. Información sensible para privacidad

> **Ver respuesta: Información sensible para privacidad**
> Puede ampliar observación de actividad.

En una multifirma, una única semilla puede ser insuficiente porque:

1. Faltan política y autorizaciones del umbral
2. Bitcoin no permite recuperar nada
3. Se necesita el color original de la app

> **Ver respuesta: Faltan política y autorizaciones del umbral**
> Conservar política y capacidades privadas son requisitos distintos.

Ante rechazo de dados en el algoritmo Final revisado debes:

1. Cambiar solo la moneda hasta aceptar
2. Repetir moneda y los cuatro dados
3. Escoger una palabra conocida

> **Ver respuesta: Repetir moneda y los cuatro dados**
> Repetir solo parte del conjunto puede sesgar el mapeo.

Dos contraseñas para abrir una semilla monofirma implican:

1. Dos claves obligatorias en cadena
2. Una multifirma Taproot
3. Umbral de acceso al secreto separado del umbral Bitcoin

> **Ver respuesta: Umbral de acceso al secreto separado del umbral Bitcoin**
> El cifrado no cambia el script.

Una copia global de Desk debe evaluarse sabiendo que:

1. Incluye necesariamente todo el chat
2. Tiene alcance y exclusiones; el chat no se asume incluido
3. Actualiza todas las copias viejas

> **Ver respuesta: Tiene alcance y exclusiones; el chat no se asume incluido**
> Recuperar identidad y mensajes son cosas diferentes.

Un nodo propio bien configurado:

1. Elimina todas las fugas
2. Reduce dependencia de consultas a terceros y permite verificar
3. Recupera claves perdidas

> **Ver respuesta: Reduce dependencia de consultas a terceros y permite verificar**
> No garantiza anonimato ni recuperación de secretos.

Congelar una UTXO en Desk:

1. Es una restricción local según la app
2. Modifica la condición de consenso
3. Revoca otras copias de la semilla

> **Ver respuesta: Es una restricción local según la app**
> No es un bloqueo global de gasto.

Tras perder conexión justo al publicar:

1. Paga otra vez inmediatamente
2. Borra la wallet
3. Comprueba primero si el pago ya se difundió

> **Ver respuesta: Comprueba primero si el pago ya se difundió**
> Un timeout no prueba ausencia de efecto.

Reutilizar direcciones o unir UTXOs de distintos contextos puede:

1. Facilitar relaciones observables
2. Borrar la historia
3. Garantizar anonimato

> **Ver respuesta: Facilitar relaciones observables**
> La privacidad depende del contexto y uso posterior.

Abrir Tor Browser configura automáticamente Desk:

1. Sí
2. No
3. Solo si el tema es oscuro

> **Ver respuesta: No**
> La ruta de cada aplicación debe verificarse.

La Clave Chat con apariencia de xpub es:

1. Publicable
2. Una dirección de cobro
3. Un secreto de identidad

> **Ver respuesta: Un secreto de identidad**
> El propósito determina sensibilidad.

Un mensaje de chat que dice pagado:

1. Sustituye confirmaciones
2. Necesita comprobación independiente del pago en la red
3. Cambia la red de la solicitud

> **Ver respuesta: Necesita comprobación independiente del pago en la red**
> El estado del mensaje no es el del pago.

El perfil multifirma Final revisado usa:

1. MuSig2 y PSBT v2
2. P2WSH sortedmulti BIP48 PSBT v0
3. Cualquier script de Bitcoin

> **Ver respuesta: P2WSH sortedmulti BIP48 PSBT v0**
> No se amplía soporte por deseos o por nombres comerciales.

En Mirror 12.12 puedes comenzar la comparación por:

1. Solo el paso 1
2. Cualquier dato elegido, incluido el 15
3. Solo el último después de todos

> **Ver respuesta: Cualquier dato elegido, incluido el 15**
> La comparación es libre e independiente por pares.

Coincide en Mirror acredita:

1. Aprobación global
2. Origen auténtico de ambos QR
3. Igualdad literal del par

> **Ver respuesta: Igualdad literal del par**
> El resto de revisión y respuesta sigue pendiente.

Si una semilla se expuso, cambiar contraseña de Desk:

1. Revoca al atacante
2. No revoca las claves que deriva esa semilla
3. Borra todas las copias

> **Ver respuesta: No revoca las claves que deriva esa semilla**
> Hay que evaluar migración segura del control.

El cierre de formación práctica debe indicar:

1. Qué fue lectura simulación y prueba física y qué falta
2. Solo horas vendidas
3. Una promesa de custodia invulnerable

> **Ver respuesta: Qué fue lectura simulación y prueba física y qué falta**
> Las evidencias tienen alcances distintos.