CUVEX

CUVEX ACADEMY · 0.1

Impara. Comprendi. Prendi il controllo.

Bitcoin e autocustodia, spiegati passo dopo passo. Corso, manuale, glossario ed esercitazioni gratuiti e senza registrazione. Scegli tu da dove iniziare.

Gratis · senza registrazione

Tutte le sezioni

1. Preparare il tuo spazio di apprendimento
2. Il denaro digitale e il problema della fiducia
3. Storia e limiti di Bitcoin
4. Satoshi e calcoli senza errori
5. Il tuo modello di minaccia
6. Nodi, mining e consenso
7. UTXO e resto di una transazione
8. Mempool, conferme e riorganizzazioni
9. Commissioni, dimensione virtuale e sostituzione
10. Reti, indirizzi e fatture
11. Hash, firme e cifratura
12. Frase seed, passphrase e password
13. Derivazione, xpub e descrittori
14. Scegliere un wallet e un modello di custodia
15. Backup che consentono il recupero
16. Conoscere Original e BIT
17. Creare un seed con entropia fisica
18. Cifrare e decifrare un segreto con Cuvex
19. Soglie di cifratura e biometria
20. Clonare, conservare e verificare le copie
21. Installare e proteggere Cuvex Desk
22. Associare crittogrammi e organizzare le WOW
23. Collegare Mirror a Desk
24. NFC tramite Mirror, USB-C e lettura dei codici QR
25. Fornitori pubblici e nodo proprio
26. Ricevere bitcoin e verificare l'indirizzo
27. Etichettare, congelare e selezionare gli UTXO
28. Preparare e verificare un pagamento
29. Firmare con Original e con BIT
30. Finalizzare, pubblicare e risolvere i problemi
31. Cosa si può osservare in Bitcoin
32. Separare i contesti e gestire il resto
33. Privacy di rete, Tor e VPN
34. CoinJoin, Payjoin e limiti attuali
35. Cosa ci insegnano gli incidenti reali

36. Creare un'identità e verificare i contatti della chat
37. Richiedere e pagare satoshi dalla chat
38. Condividere crittogrammi in modo consapevole
39. Recuperare la chat e comprenderne i metadati
40. Configurazione quotidiana e verifica delle autorizzazioni
41. Progettare un wallet multifirma
42. Creare inviti e fornire le chiavi
43. Verificare le politiche con Mirror nell'ordine che preferisci
44. Coordinare le firme e pubblicare una transazione multifirma
45. Recuperare e modificare un wallet multifirma
46. Aggiornare il firmware senza improvvisare
47. Perdita, guasto e recupero di emergenza
48. Phishing, assistenza e truffe vocali
49. Privacy, legalità e registri personali
50. Eredità, continuità e simulazione annuale
51. Prezzo, risparmio e analisi fondamentale
52. Scegliere dove acquistare bitcoin
53. Conti, ordini e costi di esecuzione
54. Candele, indicatori e distorsioni dell'analisi tecnica
55. Margine, futures e automazione
56. Lightning e altri livelli
57. Taproot, MuSig2 e il futuro post-quantistico
58. Interoperabilità e indipendenza dal produttore
59. Laboratorio tecnico con regtest
60. Progetto finale e piano di continuità
61. Manuale dello studente
62. Glossario di Bitcoin e autocustodia
63. Verifica ciò che hai imparato

M01

Preparare il tuo spazio di apprendimento

Obiettivo

Preparare il corso, distinguere i tre dispositivi e stabilire quali informazioni non vanno mai comunicate al tutor.

Comprendere

Imparerai a ricevere, custodire, spendere e recuperare bitcoin in autonomia. L'obiettivo finale è saper spiegare una decisione prima di autorizzarla. Puoi leggere il corso senza assistenza. La voce offre spiegazioni, domande e accompagnamento, senza bisogno di vedere il tuo patrimonio o controllare i tuoi dispositivi.

Cuvex protegge i segreti e ti permette di autorizzare operazioni sul suo schermo. Desk organizza sul computer crittogrammi, wallet di sola osservazione, pagamenti e coordinamento. Mirror funge da ponte locale per le operazioni compatibili e permette di confrontare i dati. Non firma e non è un wallet autonomo. Il percorso disponibile dipende dal modello e dalla versione.

Riserva uno schermo a questo corso e uno a Desk. Tieni a portata di mano il telefono e Cuvex. Se hai un solo schermo, passa da un'applicazione all'altra senza condividerlo in videochiamata mentre inserisci segreti. Una chiamata può terminare prima che tu abbia finito un'esercitazione. Fare una pausa non è un fallimento. Conserva soltanto l'identificativo della lezione, il passo raggiunto e la difficoltà incontrata.

Né il docente né l'IA devono ricevere frasi seed, passphrase BIP39, password, Chiave Chat, PIN, file privati o codici di acquisto completi. Non hanno nemmeno bisogno della tua xpub, del descrittore reale o dell'indirizzo. Questi ultimi non permettono di spendere, ma rivelano attività. Descrivi i messaggi d'errore e usa i dati fittizi del laboratorio.

Esercitazione

1. Individua fisicamente il computer, il telefono e il modello di Cuvex. Annota le versioni sul tuo quaderno privato.
2. Tieni separato l'ambiente di apprendimento senza fondi dalla custodia reale. Non importare una frase seed in uso per esercitarti.
3. Apri questa lezione e individua la pausa, la guida e il glossario. Se qualcuno ti chiede un segreto, interrompi l'interazione.

Dimostra cosa hai imparato

Spiega chi firma, chi consulta la rete e chi trasporta i dati. Puoi proseguire quando distingui queste funzioni senza aiuto.

Domanda frequente

Devo parlare tutti i giorni con il tutor? No. Puoi studiare in autonomia, ripetere una sessione e chiedere aiuto soltanto per una determinata procedura. L'accesso al corso e il saldo del servizio vocale sono diritti distinti.

Punto di pausa

L01 completata, dispositivi identificati e nessun segreto registrato nel corso.

Il tutor ti chiede la frase seed per verificare che tu l'abbia scritta correttamente. Cosa fai?

1. La detto lentamente.
2. Interrompo la richiesta e verifico la frase seed soltanto nel mio ambiente sicuro.
3. Invio solo le prime parole.

> **Mostra risposta: Interrompo la richiesta e verifico la frase seed soltanto nel mio ambiente sicuro.**
> Nessun frammento di un segreto deve essere comunicato al servizio di formazione.

M01

Il denaro digitale e il problema della fiducia

Obiettivo

Capire quale problema cerca di risolvere Bitcoin prima di aprire un wallet.

Comprendere

Il saldo bancario è una registrazione amministrata da un istituto che autentica il cliente, decide quali trasferimenti elaborare e tiene la contabilità. Un normale file digitale si copia facilmente. Inviare una fotografia non impedisce di conservarne un'altra copia. Perché un'unità digitale funzioni come denaro occorre evitare che sia spesa due volte.

Bitcoin combina regole di convalida, firme e una cronologia condivisa delle transazioni. Invece di affidare l'intero registro a un'unica entità, permette a partecipanti indipendenti di controllare se una transazione rispetta le regole. La scarsità dipende dal fatto che queste regole continuino a essere verificate e accettate. Non deriva dall'immagine di una moneta né dal prezzo pubblicato da un exchange.

L'autocustodia cambia le responsabilità. Puoi conservare la capacità di spendere senza chiedere il permesso a un custode, ma puoi perderla se distruggi tutti i backup o firmi il pagamento sbagliato. La libertà operativa non elimina la necessità di sicurezza, coordinamento, connettività per la pubblicazione e rispetto degli obblighi applicabili.

Distingui Bitcoin, la rete e il protocollo, da BTC, la sua unità monetaria. Altre reti possono usare la parola blockchain e avere proprietà diverse. Anche la promessa di un'azienda denominata in «bitcoin» è cosa diversa dal disporre di un output Bitcoin controllato dalle tue chiavi.

Esercitazione

1. Confronta tre situazioni: saldo in banca, saldo su un exchange e UTXO controllato con le tue chiavi.
2. Per ciascuna scrivi chi può impedirti di spostare il saldo e chi può aiutarti se dimentichi come accedere.
3. Descrivi cosa succederebbe copiando una foto e tentando di spendere due volte lo stesso output.

Dimostra cosa hai imparato

Spiega a parole tue perché il saldo e la capacità di firmare sono concetti diversi. Non serve imparare a memoria termini tecnici.

Domanda frequente

Con l'autocustodia scompaiono tutti gli intermediari? Puoi scegliere servizi per acquistare, consultare dati o comunicare. Conta quali poteri conservano e quali dati ricevono.

Punto di pausa

Conserva il confronto delle responsabilità senza i nomi di conti reali.

Quale problema monetario non risolve da sola una firma digitale?

1. Impedire che si tenti di spendere due volte lo stesso output.
2. Provare un'autorizzazione mediante una chiave.
3. Rilevare che il messaggio firmato è cambiato.

> **Mostra risposta: Impedire che si tenti di spendere due volte lo stesso output.**
> Le firme autorizzano. Le regole e il consenso stabiliscono l'ordine delle spese incompatibili.

M01

Storia e limiti di Bitcoin

Obiettivo

Collocare nel tempo le origini di Bitcoin e distinguere i fatti storici dai racconti commerciali.

Comprendere

Il documento di Satoshi Nakamoto fu diffuso nel 2008 e la rete fu avviata nel 2009. Proponeva denaro elettronico tra pari, riprendendo idee precedenti di crittografia, prova di lavoro e denaro digitale. Per verificare il software o una transazione non serve conoscere l'identità anagrafica di Satoshi.

Bitcoin non si è evoluto per effetto di un'azienda che sostituisce unilateralmente le regole. Gli sviluppatori propongono e rivedono modifiche, gli operatori scelgono il software, i miner costruiscono blocchi e gli utenti e i servizi decidono cosa accettare. La distribuzione delle decisioni può generare disaccordi. Una biforcazione e un aggiornamento dell'applicazione non sono sinonimi.

Un nodo può rifiutare un blocco che viola le sue regole anche se è stato necessario molto lavoro per produrlo. Il consenso non è una semplice votazione per numero di computer. Eseguire migliaia di copie di un nodo non dà automaticamente più potere decisionale. Allo stesso modo, una maggioranza di miner non ottiene per questo la chiave privata di un utente.

Bitcoin ha limiti intenzionali e comporta compromessi in termini di capacità dei blocchi, costi di verifica, tempi di conferma variabili e registro pubblico. Non offre l'annullamento amministrativo dei pagamenti o la riservatezza integrale per impostazione predefinita. I livelli e le applicazioni cercano di rispondere a esigenze specifiche introducendo nuove dipendenze.

Esercitazione

1. Disponi su una linea del tempo il documento iniziale, l'avvio della rete, l'adozione di SegWit e l'attivazione di Taproot. Verifica le date nelle fonti prima di pubblicarle.
2. Classifica «un'azienda garantisce il prezzo», «un nodo convalida» e «un miner propone un blocco» come promessa commerciale o funzione tecnica.
3. Spiega un vantaggio e un costo dell'assenza di un amministratore che possa annullare i pagamenti.

Dimostra cosa hai imparato

Distingui una regola di consenso, una politica locale e la decisione di un'azienda. L'applicazione che usi non è tutta la rete.

Domanda frequente

Il software più recente cambia sempre le regole monetarie? No. Le versioni correggono anche errori, migliorano le prestazioni o modificano le politiche locali. Leggi le note di rilascio e verifica la compatibilità.

Punto di pausa

Annota una proprietà verificabile e un'affermazione che richiederebbe altre prove.

Un blocco contiene una spesa priva di autorizzazione valida. Una maggioranza di miner lo rende valido?

1. Sì, se supera il 51 %.
2. Solo se l'exchange lo annuncia.
3. Non per un nodo che applica le regole che lo respingono.

> **Mostra risposta: Non per un nodo che applica le regole che lo respingono.**
> Il lavoro accumulato viene confrontato tra cronologie valide secondo le regole del nodo.

M01

Satoshi e calcoli senza errori

Obiettivo

Convertire BTC e satoshi e controllare gli importi senza dipendere da una quotazione.

Comprendere

Un BTC equivale a 100.000.000 di satoshi. «sat» è un'unità, non un'altra valuta. Sulla catena di base gli importi sono conteggiati come numeri interi di satoshi. 0,001 BTC sono 100.000 sat e 0,00001000 BTC sono 1.000 sat. Il separatore decimale mostrato dall'interfaccia dipende dalla lingua. Non aggiungere zeri a occhio.

Una quotazione converte BTC in una valuta come EUR o USD in un determinato momento. Non cambia quanti satoshi controlli. Se hai 100.000 sat e il prezzo cambia, il numero di satoshi resta uguale. In Desk la quotazione è un riferimento con fonte e data. Un dato obsoleto può portare a una decisione economica errata anche se il saldo in BTC è corretto.

In un pagamento occorre distinguere l'importo per il destinatario, la commissione di rete e la spesa totale. Se invii 50.000 sat con una commissione di 600 sat, dal wallet escono 50.600 sat, salvo altri output di tua proprietà. «Invia tutto» calcola normalmente un importo netto per il destinatario inferiore al saldo disponibile, poiché deve coprire la commissione.

Gli esempi del corso sono esercizi di aritmetica, non prezzi di mercato né tariffe consigliate. Prima di firmare, controlla unità, rete, destinatario e costo totale sullo schermo pertinente. La voce può dire «cinquantamila satoshi» mentre sullo schermo compare «50.000 sat». Una trascrizione incerta non deve mai determinare l'importo.

Esercitazione

1. Converti 250.000 sat in BTC: 0,0025 BTC. Converti 0,00025000 BTC in sat: 25.000 sat.
2. Calcola una spesa di 75.000 sat più 900 sat di commissione: in tutto 75.900 sat.
3. Nel simulatore usa 120.000 sat, un invio di 70.000 e una commissione di 1.000. Verifica un resto di 49.000 sat.

Dimostra cosa hai imparato

Leggi un importo in BTC e in sat e spiega quale comprende la commissione. Se hai dubbi, sospendi l'operazione.

Domanda frequente

Devo comprare un bitcoin intero? No. Puoi acquistarne una frazione, tenendo conto dei minimi e dei costi del fornitore.

Punto di pausa

Conserva solo i risultati dell'esercizio.

Hai 80.000 sat e vuoi inviare tutto con una commissione di 1.200 sat. Quanto riceve il destinatario?

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

> **Mostra risposta: 78.800 sat.**
> In questo esempio senza altri output, il destinatario riceve il saldo spendibile al netto della commissione.

Il tuo modello di minaccia

Obiettivo

Scegliere misure proporzionate contro perdita, furto, inganno ed esposizione dei dati.

Comprendere

Sicurezza significa conservare la possibilità di agire secondo le proprie intenzioni. Privacy significa controllare chi conosce i propri dati e le proprie relazioni. Disponibilità significa poter accedere quando serve. Una cassaforte inaccessibile a tutti può esserlo anche per te. Una copia molto comoda può esporre troppe informazioni.

Individua beni da proteggere, avversari e incidenti. I beni comprendono chiavi, backup, cronologia, posizione delle copie e identità dei contatti. Fra i rischi figurano malware, phishing, incendi, dimenticanze, coercizione, guasti, decesso ed errori personali. Non si riducono tutti con lo stesso strumento.

Usa una matrice semplice con probabilità approssimativa, impatto e misura concreta. Una password lunga ostacola i tentativi di indovinarla, ma non corregge un destinatario fraudolento che hai autorizzato tu. Due copie nella stessa borsa non risolvono la perdita della borsa. Un wallet multifirma con dispositivi e backup controllati da una sola persona può conservare un punto di guasto comune.

Anche il corso e il tutor fanno parte del modello. Acquisti, chiamate, tempi di connessione e progressi possono generare metadati. Il minisito non deve chiedere indirizzi o saldi per personalizzare una lezione. Il fatto che Desk o Mirror non richiedano una registrazione convenzionale non implica che il negozio, il fornitore vocale o un terzo consultato ignorino la tua attività.

Esercitazione

1. Scrivi i tre rischi principali senza indicare valori patrimoniali né luoghi precisi.
2. Per ogni rischio scegli misure di prevenzione, rilevamento e recupero. Per esempio, in caso di perdita di una carta: due copie separate, un inventario e una prova di ripristino.
3. Distingui quale persona o sistema può osservare un acquisto, una chiamata, una consultazione del saldo e una transazione pubblica.

Dimostra cosa hai imparato

Spiega come la tua prossima misura affronta un rischio specifico. Non aggiungere complessità che non sapresti gestire o spiegare ai tuoi eredi.

Domanda frequente

Più dispositivi significano sempre più sicurezza? Soltanto se riducono dipendenze comuni e puoi provare il recupero. Aggiungere dispositivi richiede anche più manutenzione e aumenta le occasioni di confusione.

Punto di pausa

Conserva il piano nella tua documentazione privata. Nel corso registra soltanto «modello di minaccia rivisto».

Quale misura riduce meglio il rischio di perdere tutte le copie in un incendio locale?

1. Cambiare il colore della carta.
2. Mettere due copie nello stesso cassetto.
3. Conservare copie verificate in luoghi esposti a rischi indipendenti.

> **Mostra risposta: Conservare copie verificate in luoghi esposti a rischi indipendenti.**
> La ridondanza deve resistere allo stesso incidente che minaccia l'originale.

M02

Nodi, mining e consenso

Obiettivo

Spiegare cosa convalidano i nodi e a cosa serve il mining.

Comprendere

Un nodo completo riceve blocchi e transazioni, verifica le regole e mantiene una propria vista della catena. Non deve fidarsi del saldo indicato da una pagina web. Il mining è il processo con cui si propongono blocchi mediante prova di lavoro. I miner selezionano transazioni valide e competono per trovare un blocco ammissibile.

La prova di lavoro rende costoso riscrivere la storia. Quando emergono alternative valide, conta il lavoro accumulato. Contare i blocchi senza considerarne la difficoltà non basta. Gli intervalli tra blocchi variano. Dieci minuti è una media obiettivo, non un appuntamento per il prossimo pagamento.

La ricompensa del miner comprende il sussidio e le commissioni. Il sussidio diminuisce secondo un calendario basato sull'altezza dei blocchi, mentre le commissioni dipendono dalle transazioni incluse. Pagare di più non rende valida una firma errata. La sicurezza economica e il costo di un attacco non rendono un pagamento recente matematicamente irreversibile.

Un nodo proprio permette di verificare e riduce la necessità di inviare richieste a fornitori esterni. Occorre comunque proteggere sistema operativo, accesso e connessione. Un nodo acceso ma non sincronizzato, o collegato a un'app che interroga un altro server, non offre automaticamente questi vantaggi.

Esercitazione

1. Assegna questi compiti: verificare una firma, scegliere le transazioni di un blocco, custodire la tua frase seed e decidere se accettare un pagamento.
2. Spiega perché «il miner conserva i miei bitcoin» è una descrizione errata.
3. In una rete di laboratorio osserva l'altezza e la sincronizzazione. Non pubblicare credenziali RPC.

Dimostra cosa hai imparato

Descrivi la differenza tra verificare e proporre. Puoi usare un'analogia, ma concludi indicando la funzione tecnica corretta.

Domanda frequente

Devo fare mining per usare Bitcoin? No. Per iniziare non devi neppure avere un nodo tuo, ma devi sapere quanta fiducia richiede il tuo fornitore.

Punto di pausa

Annota il tipo di fornitore del laboratorio, senza URL privati.

Cosa permette di fare all'utente un nodo completo correttamente configurato?

1. Verificare le regole della catena che accetta.
2. Recuperare qualsiasi chiave persa.
3. Garantire un aumento del prezzo.

> **Mostra risposta: Verificare le regole della catena che accetta.**
> Convalida e custodia sono funzioni diverse.

UTXO e resto di una transazione

Obiettivo

Leggere una transazione come consumo e creazione di output.

Comprendere

Un UTXO è un output di una precedente transazione che non è ancora stato speso. Un wallet calcola il saldo individuando gli output che può controllare. Non esiste un conto universale da addebitare come in un registro bancario. Ogni input fa riferimento a un output precedente attraverso l'identificativo della transazione e la posizione.

Quando spendi un UTXO lo consumi per intero. Se devi pagare meno del suo valore, normalmente crei un output per il destinatario e un output di resto che controlli tu. Con un input di 120.000 sat, 70.000 al destinatario e 1.000 di commissione, il resto è 49.000. La somma degli input deve essere uguale alla somma degli output più la commissione.

Un indirizzo non è un UTXO. Può ricevere vari output e non corrisponde necessariamente a una persona. L'identificativo di una transazione può essere pubblico, ma collegarlo alla tua identità o spiegare a chi appartiene ogni output aggiunge informazioni che la catena da sola non esprime.

Questa struttura incide sulla privacy. Unire input può suggerire un controllo comune e il resto può collegare pagamenti futuri. L'inferenza non è una prova universale, perché esistono transazioni collaborative. Il coin control consiste nello scegliere quali output spendere conoscendo le conseguenze della loro combinazione.

Esercitazione

1. Disegna tre input fittizi da 40.000, 60.000 e 200.000 sat. Paga 70.000 con una commissione di 1.000 usando solo i primi due.
2. Verifica che il resto sia 29.000 sat e che il terzo input non partecipi.
3. Ripeti usando soltanto 200.000. Il resto sarebbe 129.000. Confronta il costo potenziale e i collegamenti senza presumere dimensioni uguali.

Dimostra cosa hai imparato

Individua input, destinatario, resto e commissione nel diagramma del corso. Se non riconosci un output, non firmare un'operazione reale.

Domanda frequente

Tutto ciò che torna nel mio wallet è resto? No. Potrebbe essere un trasferimento a un altro indirizzo tuo. Per classificarlo occorre conoscere la politica e la derivazione, senza tirare a indovinare in base all'importo.

Punto di pausa

Conserva lo schema fittizio, mai una schermata del tuo patrimonio.

Un input da 100.000 sat genera un output da 30.000 e uno da 69.200. Qual è la commissione?

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

> **Mostra risposta: 800 sat.**
> 100.000 meno 99.200 equivale a 800 sat.

M02

Mempool, conferme e riorganizzazioni

Obiettivo

Distinguere una transazione preparata, pubblicata e confermata.

Comprendere

La mempool è l'insieme locale delle transazioni non confermate che un nodo conserva secondo la propria politica. Non esiste un'unica mempool identica in tutto il mondo. Se un esploratore mostra un pagamento, significa che quel servizio lo conosce. Non garantisce che tutti i nodi lo accettino né che sarà confermato entro un tempo preciso.

Preparare una PSBT non pubblica nulla. Firmare produce l'autorizzazione. Finalizzare costruisce la transazione che può essere diffusa. Pubblicare significa tentare di trasmetterla. La conferma indica l'inclusione in un blocco della catena accettata dalla fonte di verifica. Una seconda conferma aggiunge un altro blocco sopra al primo. Non è una seconda firma del destinatario.

Possono verificarsi riorganizzazioni che modificano un tratto della catena. Un'operazione può perdere conferme o tornare in attesa. Per i pagamenti con un'esposizione maggiore, le parti spesso richiedono più conferme. Nessun numero elimina ogni rischio per tutti gli importi e le situazioni.

Se Desk mostra uno stato salvato, controlla la data della sincronizzazione. «Confermato» in una vecchia istantanea non descrive necessariamente lo stato attuale. Se un invio non compare, conservane l'identificativo locale e verifica la pubblicazione e la cronologia prima di prepararlo di nuovo. Ripeterlo per impazienza può creare un altro pagamento valido.

Esercitazione

1. Metti in ordine queste schede: bozza, PSBT, firma, transazione finale, diffusione, inclusione in un blocco.
2. Simula una disconnessione dopo la pubblicazione. Decidi cosa verificare prima di ripagare.
3. Spiega a un esercente perché un messaggio in chat con la scritta «pagato» non sostituisce la verifica sulla rete.

Dimostra cosa hai imparato

Sai indicare lo stato di un'operazione, la fonte e la data di tale informazione senza confonderla con una garanzia.

Domanda frequente

Chiudere Desk annulla una transazione pubblicata? No. Altri nodi e partecipanti possono conservarla. Annullare una bozza locale ha una portata diversa.

Punto di pausa

Annota lo stato della simulazione. Non fornire identificativi reali al tutor.

Il computer si disconnette subito dopo aver premuto il pulsante di pubblicazione. Cosa fai per prima cosa?

1. Preparo lo stesso pagamento da capo.
2. Cancello il wallet.
3. Mi ricollego e verifico la transazione e i suoi input.

> **Mostra risposta: Mi ricollego e verifico la transazione e i suoi input.**
> La mancata risposta non dimostra che la diffusione sia fallita.

M02

Commissioni, dimensione virtuale e sostituzione

Obiettivo

Stimare i costi, interpretare i sat per vbyte e comprendere RBF e CPFP.

Comprendere

La commissione di rete è la differenza tra input e output. La sua competitività si esprime generalmente in sat/vB, satoshi per byte virtuale. Non dipende direttamente dal valore economico inviato. Molti input possono rendere costoso un piccolo pagamento, mentre un pagamento elevato con pochi input può occupare meno spazio.

Per esempio, per 200 vB a 5 sat/vB, la commissione è 1.000 sat. Prima di firmare puoi avere solo una stima, perché la dimensione finale può dipendere dalle firme e dalla struttura. Desk offre velocità indicative e una tariffa manuale. L'etichetta «veloce» non promette una conferma puntuale.

RBF è una politica di sostituzione delle transazioni non confermate a determinate condizioni. Permette di proporre una spesa in conflitto con una commissione maggiore. Le politiche dei nodi si sono evolute e una segnalazione di non sostituibilità non va considerata una garanzia di incasso. Una sostituzione richiede una nuova verifica e le firme necessarie.

CPFP consiste nello spendere un output della transazione in attesa per rendere interessante l'insieme delle transazioni genitore e figlia. Richiede il controllo di un output spendibile, il rispetto delle politiche e il pagamento del costo. È un concetto di Bitcoin. Non si presume la presenza di un pulsante CPFP nella versione di Cuvex dello studente.

«Dust» è un output troppo piccolo secondo le politiche applicabili e i costi di spesa stimati. Non esiste una soglia universale per tutti i tipi di script. Evita di insegnare un valore fisso come se fosse una regola di consenso. Se il resto non è praticabile, rivedi importo, input o trasferimento dell'intero saldo e commissione effettiva.

Esercitazione

1. Calcola 180 vB a 8 sat/vB: 1.440 sat. Verifica se superi il budget del laboratorio.
2. Confronta un input con dieci input. Spiega perché l'importo inviato non basta per stimare il costo.
3. Simula una transazione in attesa e scegli se aspettare, usare RBF o studiare CPFP, senza presumere la compatibilità automatica.

Dimostra cosa hai imparato

Motiva la tariffa, la commissione assoluta e il costo rispetto all'importo inviato. Rifiuta una commissione che non capisci.

Domanda frequente

RBF annulla con certezza il pagamento precedente? No. Le versioni competono fino alla conferma e la propagazione conta. Non consegnare beni basandoti su una promessa di annullamento.

Punto di pausa

Conserva la decisione presa nell'esercizio e il motivo.

Qual è la commissione per 250 vB a 4 sat/vB?

1. 1.000 sat.
2. 254 sat.
3. Il 4 % dell'importo inviato.

> **Mostra risposta: 1.000 sat.**
> La dimensione virtuale moltiplicata per la tariffa dà la commissione stimata.

M02

Reti, indirizzi e fatture

Obiettivo

Riconoscere la rete, il formato dell'indirizzo e le istruzioni di pagamento prima di copiare o scansionare.

Comprendere

La mainnet trasferisce bitcoin con valore economico. Le reti di prova servono per sviluppare e imparare, ma non sono intercambiabili. Regtest è una rete locale controllata da chi allestisce il laboratorio. Signet e testnet hanno regole ed ecosistemi propri. Una funzione a firma singola in signet non implica che il profilo multifirma di Cuvex supporti quella rete.

Gli indirizzi codificano le condizioni di ricezione. In mainnet troverai formati che iniziano con 1, 3, bc1q o bc1p. Il prefisso aiuta a riconoscere una famiglia, ma non verifica il destinatario, non garantisce la compatibilità del firmatario e non sostituisce la convalida completa del formato.

Un QR è un contenitore visivo. Può trasportare un indirizzo, una fattura, un descrittore o un testo malevolo. Scansionarlo non ne autentica l'autore. Un collegamento bitcoin: può aggiungere importo e messaggio. BIP321 è il riferimento moderno che sostituisce BIP21. Nell'implementazione esaminata, Desk mantiene la terminologia e la compatibilità BIP21. Una modifica dello standard da sola non amplia ciò che l'app sa interpretare.

Una fattura Lightning non è un indirizzo on-chain. Può includere scadenza e altri campi. Non incollarla in un invio sulla catena se l'applicazione non offre una procedura compatibile. Nemmeno un token denominato BTC su un'altra rete è automaticamente bitcoin nativo.

Esercitazione

1. Classifica esempi etichettati del corso senza usare indirizzi con fondi spendibili: indirizzo, URI bitcoin:, fattura Lightning e descrittore.
2. Individua la rete selezionata nel laboratorio. Nel profilo multifirma di Cuvex esaminato, le reti compatibili sono mainnet/regtest.
3. Confronta il testo completo richiesto dal destinatario attraverso un canale autenticato prima di un'operazione reale.

Dimostra cosa hai imparato

Sai rifiutare una richiesta di cui non conosci la rete o la modalità e spiegare cosa devi verificare.

Domanda frequente

Posso inviare BTC tramite qualsiasi rete indicata dall'exchange? No. La rete di prelievo deve corrispondere a quella effettiva di ricezione. Evita di scegliere soltanto in base alla commissione più bassa.

Punto di pausa

Registra solo il tipo di rete di apprendimento.

Un indirizzo di ricezione bc1 non autorizza da solo un prelievo di BTC tramite una rete di token diversa. Cosa manca?

1. Modificare l'alias del destinatario.
2. Confermare che il prelievo utilizzi Bitcoin on-chain e che tutti i dati corrispondano.
3. Inserire la frase seed nell'exchange.

> **Mostra risposta: Confermare che il prelievo utilizzi Bitcoin on-chain e che tutti i dati corrispondano.**
> Asset, rete e modalità di ricezione devono essere compatibili.

M03

Hash, firme e cifratura

Obiettivo

Distinguere integrità, autorizzazione e riservatezza.

Comprendere

Un hash trasforma dati in un'impronta di lunghezza fissa. Confrontare un'impronta nota aiuta a rilevare le modifiche. Non cifra il file né identifica da solo chi lo ha pubblicato. Se scarichi il file e l'hash dalla stessa pagina compromessa, l'aggressore potrebbe aver sostituito entrambi.

Una chiave privata permette di creare firme; la chiave pubblica corrispondente permette di verificarle. La firma collega un'autorizzazione ad un messaggio specifico secondo l'algoritmo e le sue regole. Non nasconde il contenuto firmato. In Bitcoin, una firma valida è una parte delle condizioni necessarie per spendere un'uscita.

La crittografia cerca che un contenuto possa essere letto solo con la capacità appropriata. La crittografia autenticata aggiunge il rilevamento delle alterazioni. Nell'ecosistema Cuvex ci sono crittogrammi che proteggono segreti, transazioni firmate che autorizzano spese e canali cifrati che trasportano messaggi. Non sono oggetti equivalenti, anche se tutti usano la crittografia.

Una password umana di solito passa attraverso una funzione di bypass prima di essere utilizzata come chiave di crittografia. ·AES-256" descrive l'algoritmo e la dimensione della chiave, ma non trasforma una password prevedibile in una scelta forte. La generazione, l'implementazione, lo storage, lo schermo e il recupero fanno parte della sicurezza totale.

Non si deduce neppure che un QR sia sicuro perché sembra complesso. Bisogna sapere cosa contiene, chi l'ha prodotto e cosa ne farà l'applicazione. Prima di accettare un'azione, chiede al tutor di spiegarne lo scopo senza richiedere il dato privato.

Esercitazione

1. Associa «rilevare una modifica a un file», «nascondere una frase seed» e «autorizzare un pagamento» a hash, cifratura e firma.
2. Cambia una lettera di un testo fittizio e osserva che il tuo hash cambia; non usare segreti per questa dimostrazione.
3. Spiega perché una transazione può essere pubblica ed essere firmata allo stesso tempo.

Dimostra cosa hai imparato

Sai indicare quale garanzia cerchi e quale meccanismo la offre, senza usare «cifrato» come sinonimo di tutto ciò che è sicuro.

Domanda frequente

Un hash firmware certifica che non ci sono bug? No. Identifica byte se il riferimento è affidabile. Un controllo, una ditta di produttori e un test fisico rispondono a domande diverse.

Punto di pausa

Salva tutte e tre le lettere dell'esercizio.

Quale di questi meccanismi nasconde il contenuto di un segreto?

1. Pubblicarne il nome del file.
2. Firmarlo senza cifrarlo.
3. Cifrarlo correttamente con una chiave protetta.

> **Mostra risposta: Cifrarlo correttamente con una chiave protetta.**
> La sola firma o impronta non garantisce la riservatezza.

M03

Frase seed, passphrase e password

Obiettivo

Evitare la confusione tra le varie credenziali del sistema.

Comprendere

Una mnemonica BIP39 rappresenta l'entropia e una somma di controllo mediante parole di un dizionario. Le lunghezze standard sono 12, 15, 18, 21 o 24 parole. Scegliere una frase memorabile, il testo di una canzone o parole casuali secondo il proprio intuito non equivale a una generazione sicura. La somma di controllo rileva alcuni errori. Non dimostra chi abbia creato il seed né che nessun altro lo conosca.

La passphrase BIP39 partecipa alla derivazione del seed binario. Una passphrase diversa può aprire un wallet completamente diverso e apparentemente vuoto. Non compare necessariamente un messaggio che indichi «passphrase errata». Non deve necessariamente essere una parola del dizionario e non è letteralmente una venticinquesima parola.

La password del crittogramma Cuvex protegge il segreto memorizzato. La password di Desk protegge l'archivio locale del computer. Il PIN di collegamento autorizza una sessione di comunicazione. La Chiave Chat permette di recuperare l'identità usata per i messaggi. Nessuna di queste credenziali va confusa con la frase seed. Conoscerne una non implica poter ricostruire tutte le altre.

Conservare insieme frase seed e passphrase in un crittogramma può agevolare il recupero, ma elimina la separazione tra le due per chi riesca a decifrarlo. Tenerle separate aumenta gli adempimenti per te e per i tuoi eredi. La decisione deve essere documentata e provata. Non prenderla solo perché il tutor considera un'opzione «più avanzata».

Esercitazione

1. Prepara cinque cartoncini senza valori segreti: frase seed, passphrase, password di Cuvex, password di Desk e Chiave Chat.
2. Scrivi cosa permette di recuperare ogni credenziale e cosa perderesti se la dimenticassi.
3. Progetta un test in un portafoglio vuoto. Inserisci le parole e la passphrase in privato e comunica al tutor solo il risultato.

Dimostra cosa hai imparato

Spiega perché il corso non dovrebbe mai richiedere una password per più di più di un anno. Identifica quale segreto richiede la tua procedura di recupero.

Domanda frequente

Posso reimpostare la passphrase via email? Questo meccanismo non esiste nel BIP39. Un fornitore di custodia può avere il recupero del conto, ma è un altro modello.

Punto di pausa

Registra i poteri diversi, senza scriverne i valori.

Cambi una lettera della passphrase BIP39 e vedi saldo zero. Qual è l'interpretazione corretta?

1. Potrebbe essere un altro wallet valido derivato da un'altra passphrase.
2. La rete ha cancellato i tuoi fondi.
3. Desk deve indovinare la passphrase originale.

> **Mostra risposta: Potrebbe essere un altro wallet valido derivato da un'altra passphrase.**
> Una passphrase diversa può produrre un altro wallet senza segnalare un errore.

M03

Derivazione, xpub e descrittori

Obiettivo

Comprendere come viene descritto un portafoglio senza fornire capacità di spesa.

Comprendere

Un portafoglio gerarchico deriva molte chiavi da una radice. Un percorso indica quale ramo viene utilizzato. In mainnet, BIP84 utilizza di solito m/84'/0'/0' per il primo account SegWit a firma singola; BIP48 P2WSH utilizza m/48'/0'/0'/2' sul primo conto multifirma. L'apostrofo indica una derivazione hardened. Cambiare account, rete o tipo di script può dare altri indirizzi dalla stessa mnemonica.

Una xpub è una chiave pubblica diffusa che permette di derivare determinate chiavi pubbliche discendenti. Non è una password di spesa, ma può permettere di osservare una famiglia di indirizzi. L'impronta master è un identificatore breve utile per collegare i registri; non garantisce l'identità da sola né evita collisioni.

Un descrittore esprime come costruire script e indirizzi: tipo di script, chiavi, origini e derivazioni. Un descrittore watch-only con chiavi pubbliche permette di osservare, non firmare. La parola «descrittore» non garantisce che contenga soltanto informazioni pubbliche. Alcuni formati possono includere chiavi private. Non salire mai su un vero descrittore al corso.

Per recuperare una multifirma è spesso necessaria la politica completa, non solo le parole di uno dei firmatari. Conserva soglia, partecipanti, xpubs, percorsi, rete, tipo di script e dati di scoperta. La somma di controllo del descrittore aiuta a individuare errori di trascrizione; non autentica i suoi partecipanti.

Esercitazione

1. Leggi un percorso fittizio e spiega scopo, moneta, conto e ramo. Non inserire chiavi vere.
2. Distingui indirizzo di ricezione, xpub partecipante e descrittore completo.
3. Prepara una scheda privata di recupero con nomi di campi vuoti e posizione documentaria separata.

Dimostra cosa hai imparato

Sai spiegare perché un wallet vuoto dopo il ripristino non dimostra la perdita dei fondi. Occorre verificare la rete, la passphrase, lo script, il conto, il percorso di derivazione e la ricerca degli indirizzi.

Domanda frequente

Una xpub può essere pubblicata senza conseguenze? Non concede di per sé normale capacità di spendere, ma espone la privacy e può aumentare altri rischi in particolari combinazioni criptografiche.

Punto di pausa

Salva la scheda senza valori sensibili nel corso.

Quale informazione può mancare se tenti di recuperare un wallet multifirma con una sola frase seed?

1. Il colore del dispositivo.
2. La politica e le chiavi pubbliche degli altri partecipanti.
3. La password di un social network.

> **Mostra risposta: La politica e le chiavi pubbliche degli altri partecipanti.**
> Per ricostruire gli script occorrono la politica completa e il numero di chiavi private previsto dalla soglia.

M03

Scegliere un wallet e un modello di custodia

Obiettivo

Confronta strumenti per funzioni, fiducia e recupero.

Comprendere

Un wallet è un insieme di strumenti per descrivere, osservare e, se del caso, autorizzare le spese. Un wallet caldo mantiene la capacità di firma in un ambiente collegato. Un dispositivo di firma isolato cerca di tenere i segreti separati dal computer che interroga la rete. Una Wallet watch-only conserva informazioni pubbliche sufficienti per osservare e preparare, ma ha bisogno di un altro sistema per firmare.

In custodia di terzi, un conto può rappresentare un diritto nei confronti di un'impresa. In autocustodia tu mantieni la capacità tecnica di spesa, individualmente o in comune. Il recupero via email e il potere di bloccare un ritiro riflettono spesso il primo modello. Non devi valutare entrambe le opzioni con lo stesso presupposto di responsabilità.

Confronta il supporto di rete e script, la verifica dello schermo, le copie, l'aggiornamento, l'interoperabilità, la manutenzione, la consultazione dei fornitori e la chiarezza degli errori. Una lista di monete o una finitura fisica non bastano. Un dispositivo di firma non ti impedisce nemmeno di accettare un indirizzo sbagliato se non lo controlli.

Cuvex separa la protezione dei segreti nei crittogrammi dalle funzioni di organizzazione e consultazione in Desk. Questo modello richiede di conservare il crittogramma e i suoi mezzi di sblocco. La protezione contro la perdita del dispositivo non implica il recupero se tutte le copie o le password scompaiono. Impara l'intero processo prima di trasferire il patrimonio.

Esercitazione

1. Confronta Cuvex con un wallet caldo e un exchange in una matrice: chi firma, chi vede le domande, chi può recuperare l'accesso e cosa succede alla chiusura dell'azienda.
2. Scegli due criteri da verificare con le prove e non con la pubblicità.
3. Controlla che l'ambiente pratico non condivida le chiavi con il tuo vero risparmio.

Dimostra cosa hai imparato

Giustifica una scelta per un caso specifico senza dichiarare uno strumento invulnerabile.

Domanda frequente

Un hardware Wallet rende private tutte le transazioni? No. Protegge principalmente la capacità di firma e parte della revisione; la catena, le consultazioni e le controparti continuano a generare informazioni.

Punto di pausa

Salva la tua matrice di criteri senza nomi di account.

Cosa può fare un wallet watch-only configurato correttamente con chiavi pubbliche?

1. Osservare e preparare operazioni senza poterle firmare da solo.
2. Modificare una frase seed persa.
3. Garantire l'anonimato.

> **Mostra risposta: Osservare e preparare operazioni senza poterle firmare da solo.**
> Osservazione e autorizzazione sono capacità separabili.

M03

Backup che consentono il recupero

Obiettivo

Progettare una copia completa e dimostrare il recupero prima di dipendere da esso.

Comprendere

Un backup utile recupera una capacità, non semplicemente un file. Per una a firma singola può richiedere mnemonica, passphrase e dati di derivazione. Per una multifirma, inoltre, occorre una politica e un numero sufficiente di firmatari. Per Desk può essere necessaria una copia crittografata e la password. Per la chat, recuperare identità non equivale a recuperare messaggi storici.

La ridondanza protegge dalla perdita accidentale. La separazione protegge dalla compromissione simultanea degli elementi. Due copie su diversi supporti e luoghi possono ridurre i bug correlati. Ogni copia aggiuntiva richiede anche il controllo dell'accesso, dell'inventario e della revisione. I nomi dei file e dei tag non devono rivelare il patrimonio o facilitare la localizzazione di tutti i componenti.

Un test deve confermare un indirizzo precedentemente verificato e, in un ambiente di apprendimento, la capacità di firmare un'operazione controllata. Vedere che il file apre non dimostra che appartiene al portafoglio corretto. Non controllare un backup inserendo la frase seed che usi realmente su un computer qualsiasi.

Documenta cosa copre e cosa esclude ogni copia. Cambiare la password corrente non modifica automaticamente le vecchie copie. Se una password precedente è stata esposta, questi backup sono ancora interessati. Eliminare un file in archivio moderno non garantisce nemmeno l'eliminazione di tutte le copie o versioni.

Esercitazione

1. Completa una tabella privata: oggetto, contenuto, password associata, posizione indipendente, data di prova e responsabile.
2. Ripristina una copia di apprendimento in un ambiente separato. Controlla rete, prima direzione e derivazione.
3. Simula la perdita del computer e poi quella del dispositivo. Identifica la procedura che cambia.

Dimostra cosa hai imparato

Puoi recuperare il tuo scenario di prova senza l'aiuto di improvvisazione e spiegare quali informazioni mancherebbero per un altro scenario.

Domanda frequente

La copia globale di Desk e' una copia di tutto? Non si deve prendere in considerazione. Nella base riveduta, cronologia e sessioni di chat non sono incluse. La politica multifirma e le chiavi private hanno ruoli diversi.

Punto di pausa

Registra data e risultato della prova; mai il contenuto della copia.

Cambi la password di Desk. Cosa succede a un backup precedente?

1. Si aggiorna da solo.
2. Perde automaticamente la cifratura.
3. Conserva la protezione e la password con cui è stato creato.

> **Mostra risposta: Conserva la protezione e la password con cui è stato creato.**
> I backup precedenti sono oggetti indipendenti.

M04

Conoscere Original e BIT

Obiettivo

Scegliere il percorso corretto secondo il dispositivo e la sua versione.

Comprendere

Original utilizza carte NFC per trasportare crittogrammi e operazioni compatibili. Il Bluetooth interviene nell'aggiornamento del dispositivo. Il tuo USB-C è utilizzato come alimentazione nel modello documentato. BIT scambia file tramite USB-C e aggiunge la biometria per i crittogrammi che la richiedono. Non spostare le istruzioni NFC o Bluetooth da Original a BIT.

Sul dispositivo troverai funzioni per crittografare, decifrare, creare portafogli e firmare, oltre alle impostazioni. Original incorpora clone di schede; BIT lavora con i file di supporto USB. Le insegne, le lingue e gli accessi possono variare per versione. Su BIT la nuova voce «Verifica politiche» apre la procedura compatibile e non cambia chi autorizza l'operazione.

Il riferimento editoriale rivisto è Original 1.2.2 Final, BIT 1.2.3 Final, Desk beta.9.21 e Mirror beta.12.12. Si tratta di riferimenti di fonti: la firma, la distribuzione e l'accettazione fisica di ciascuna combinazione devono essere verificate con l'apparecchiatura. Non sostituire il tuo firmware con un binario senza firma incluso in un pacchetto di ingegneria.

Prima di usare il dispositivo, verificane provenienza, sigilli, aspetto e versione. La tracciabilità e la firma di aggiornamento aiutano con minacce specifiche, ma non sostituiscono tutte le verifiche. Se si osserva una manipolazione o una versione inaspettata, interrompere l'inizializzazione e consultare il supporto tramite un canale verificato.

Esercitazione

1. Identifica il tuo modello e registra la versione visibile senza fotografare segreti.
2. Trova crittografia, decifrazione, creazione di Wallet, PSBT e impostazioni. Non avviare né una cancellazione né un aggiornamento per esplorare i menu.
3. Scegli nel corso il percorso corrispondente a Original o a BIT. Mantieni quella selezione durante la pratica.

Dimostra cosa hai imparato

Spiega come entra ed esce un'operazione dal tuo modello e quale supporto devi proteggere da sovrascritture.

Domanda frequente

BIT è automaticamente più sicuro per chiunque? I modelli offrono scelte operative diverse. La risposta dipende da minacce, recupero e uso corretto.

Punto di pausa

Salva modello e versione nel tuo quaderno locale; il corso richiede solo il modello scelto.

Hai un BIT e una guida richiede di scrivere una carta NFC con il dispositivo stesso. Cosa fai?

1. Verifico che la guida corrisponda al mio modello e uso la procedura USB compatibile.
2. Forzo l'aggiornamento di Original.
3. Invio la frase seed al telefono.

> **Mostra risposta: Verifico che la guida corrisponda al mio modello e uso la procedura USB compatibile.**
> Le istruzioni devono corrispondere all'effettivo mezzo di trasporto dei dati utilizzato dal modello.

M04

Creare un seed con entropia fisica

Obiettivo

Capire la generazione e provare il flusso senza convertire i dati del corso in chiavi proprie.

Comprendere

L'entropia è imprevedibile. Alcuni dadi possono apportare entropia se sono adatti, l'ordine è impostato prima di lanciare e l'algoritmo di conversione è corretto. Quando la procedura scarta un risultato, occorre ripetere il lancio esattamente come indicato. Sostituirlo con il numero massimo o scegliere un'altra parola introduce una distorsione.

Il flusso Cuvex rivisto combina una moneta e quattro dadi. La funzione di conversione moltiplica il valore della moneta per 1.296 e somma il numero in base sei formato dai valori dei quattro dadi dopo aver sottratto uno a ciascuno. Sono ammessi indici da 0 a 2.047. Se il risultato cade fuori dal dizionario, bisogna ripetere la moneta e i quattro dadi. Mantenere il risultato della moneta e rilanciare solo i dadi introduce una distorsione. È quanto descrive il codice sorgente esaminato. Lo schermo e l'intera procedura vengono convalidati in ogni versione del firmware distribuita.

Non è come scegliere le parole preferite. Non trasformare una dimostrazione pubblica in materiale per la custodia dei soldi. Qualsiasi seed che compaia in materiale didattico è considerato noto. La parola finale e il controllo devono essere effettuati mediante l'algoritmo completo del dispositivo, senza completare una mnemonica a mano.

Prepara uno spazio senza telecamere, assistenti vocali attivi nelle vicinanze, registrazione dello schermo o persone che osservano. Il tutor deve fermarsi durante l'ingresso e la revisione del segreto. È possibile spiegare prima e poi valutare con domande sul processo, senza ascoltare i risultati dei lanci e le parole.

Dopo aver generato, è necessario controllare il backup, crittografarlo secondo il modello e provare il recupero di un portafoglio vuoto. Un indirizzo di verifica aiuta a confermare la coerenza senza esporre il seed al computer. Se il flusso accetta valori che contraddicono le istruzioni o visualizza parole inaspettate, ferma l'uso e registra solo versione, schermo ed errore.

Esercitazione

1. Nella prova, segui le orme del dispositivo con materiale privo di fondi. Imposta l'ordine dei dadi e non cambiare i risultati.
2. Ripeti le voci rifiutate secondo lo schermo, senza correggerle per adattarsi.

3. Controlla in privato il contenuto, crea copia e conferma che puoi ricostruire lo stesso portafoglio di apprendimento.

Dimostra cosa hai imparato

Spiega perché entropia fisica, corretta conversione e segreto del risultato sono tre requisiti diversi.

Domanda frequente

Posso contare i miei giri in IA per controllare l'algoritmo? Non per un seed che userai. L'assistenza lavora con esempi sintetici diversi.

Punto di pausa

Termina in uno stato sicuro del dispositivo; non lasciare un seed visibile durante il riposo.

Il firmware rifiuta il risultato dei dadi. Quale azione rispetta la procedura?

1. Scegliere manualmente una parola.
2. Ripetere come indicato dal dispositivo senza introdurre distorsioni.
3. Ridurre il numero finché viene accettato.

> **Mostra risposta: Ripetere come indicato dal dispositivo senza introdurre distorsioni.**
> Gli scarti fanno parte della conversione dell'entropia e i risultati non vanno sostituiti arbitrariamente.

M04

Cifrare e decifrare un segreto con Cuvex

Obiettivo

Creare un crittogramma di apprendimento e verificare il recupero.

Comprendere

Scegli il tipo di contenuto corretto: BIP39, SLIP39, Monero o testo, se disponibile nella tua procedura. Sono formati diversi. Cifra un testo SLIP39 non trasforma Cuvex in un firmatario di tutte le reti che possono utilizzare quel testo. Memorizzare i segreti ed eseguire i protocolli di firma hanno diverse dimensioni.

Inserisci il contenuto direttamente sul dispositivo quando cerchi di tenerlo fuori dai computer collegati. Un metodo di importazione da telefono o PC può già aver esposto il segreto alla fonte, anche se in seguito viene crittografato. La schermata di revisione precedente è il luogo per rilevare parole, ordine, maiuscole e campi sbagliati.

La password del crittogramma deve essere lunga, unica e recuperabile secondo il tuo piano. La tastiera di creazione riveduta ha capacità per 40 caratteri e il validatore richiede almeno 12, maiuscola e minuscola ASCII, numero e simbolo riconosciuto. Non applicare automaticamente i 12 a 1.024 caratteri Desk alla tastiera Cuvex: Desk applica una politica diversa. Altri campi di recupero possono avere limiti diversi; controlla il flusso e la versione.

In Original scrivi su una scheda vuota e adeguata; mantieni la posizione fino a quando non riceverai la conferma. In BIT conserva i file che producono il flusso USB, compresi i componenti biometrici necessari, se del caso. Non rinominare o combinare file per intuizione. Poi esegue una lettura e decrittografia di prova sul dispositivo, senza comunicare il segreto al tutor.

Esercitazione

1. Cita un testo didattico creato per questa pratica, senza credenziali né valore economico.
2. Identifica il supporto e l'oggetto risultante; annota in privato l'alias e la sua funzione.
3. Riavviare il processo di decrittografia, controllare il testo sullo schermo affidabile e chiudere la visualizzazione alla fine.

Dimostra cosa hai imparato

Puoi distinguere il contenuto corretto, la scrittura corretta e il recupero corretto. Il messaggio copiato non prova tutti e tre.

Domanda frequente

L'alias della carta di credito e' una password? No. Sono informazioni organizzative. Evita di includere saldi o descrizioni che facilitano l'identificazione del tuo patrimonio.

Punto di pausa

Non lasciare contenuti decrittati visibili. Registra solo il successo o il fallimento della prova.

Cosa dimostra meglio che un crittogramma di prova è idoneo a recuperarne il contenuto?

1. Che abbia un bel nome.
2. Che il file esista in due cartelle.
3. Leggerlo e decifrarlo con la procedura corretta, verificandone il contenuto in privato.

> **Mostra risposta: Leggerlo e decifrarlo con la procedura corretta, verificandone il contenuto in privato.**
> L'esistenza di una copia non ne prova l'utilizzabilità né la corrispondenza al contenuto atteso.

M04

Soglie di cifratura e biometria

Obiettivo

Separare la protezione condivisa del segreto dalla multifirma di Bitcoin.

Comprendere

Un crittogramma protetto da varie password regola chi può decifrare il contenuto. Un portafoglio Bitcoin multifirma regola quali chiavi devono autorizzare una spesa nella rete. Puoi avere un segreto criptato in modo condiviso che corrisponda a un portafoglio a firma singola, o ogni firmatario di una multifirma con il suo singolo crittogramma.

Se più persone sbloccano insieme un solo seed e questo seed permette di spendere da soli, la soglia della catena rimane di una chiave. Una volta rivelata, qualcuno potrebbe tenerla. Non descrivere quello schema come se costringesse a coordinare più firme per ogni pagamento.

La biometria BIT aggiunge una condizione di accesso ai formati che la utilizzano. Un dito non è un seed o una sostituzione universale della password. Pianifica lesioni, cambiamenti di impronta, guasto, disponibilità dell'attrezzatura e eredità. Conserva e testa la via di recupero documentata di quel crittogramma prima di affidarsi a esso.

Un'esportazione di recupero può rivelare il segreto su un computer, proprio per risolvere un'emergenza. L'esistenza di tale funzione non rende il PC un ambiente equivalente al dispositivo. La pratica normale deve mantenere l'isolamento; il recupero locale è studiato con consapevolezza e con un piano di migrazione successivo se vi è stata esposizione.

Esercitazione

1. Disegna due politiche: «due password per aprire una frase seed» e «due chiavi su tre per spendere».
2. In un test senza fondi, identifica quali file richiedono una copia biometrica e dove viene verificato il recupero.
3. Fai finta che una persona non sia disponibile. Determina se la soglia del tuo schema permette di continuare.

Dimostra cosa hai imparato

Puoi spiegare chi può conoscere il segreto e chi può autorizzare una spesa dopo averlo decifrato.

Domanda frequente

Posso ritirare un partecipante cambiando un'etichetta? No. Devi distinguere i cambiamenti organizzativi da una nuova protezione del segreto e da una nuova politica di spesa.

Punto di pausa

Salva lo schema senza nomi reali o dati biometrici.

Tre persone usano due password per aprire un crittogramma che contiene una sola frase seed a firma singola. Quante chiavi richiede Bitcoin per spendere?

1. Una, se questa è la politica del wallet.
2. Due, perché il file aveva due password obbligatorie.
3. Tre, per il numero delle persone.

> **Mostra risposta: Una, se questa è la politica del wallet.**
> La soglia di cifratura non modifica lo script che controlla le monete.

Clonare, conservare e verificare le copie

Obiettivo

Costruire ridondanza senza distruggere l'unica copia valida.

Comprendere

Clonare un crittogramma copia dati cifrati; non crea un nuovo saldo, un altro seed o indipendenza rispetto a una password esposta. Copie identiche permettono di affrontare la perdita del supporto, ma non risolvono la compromissione del segreto originale. Per questo motivo una restaurazione e una migrazione a nuove chiavi rispondono a situazioni diverse.

Su Original distingui la carta del crittogramma dalla carta di trasporto della PSBT. Un supporto operativo può essere riutilizzato in base al flusso; una scheda con il tuo backup non deve diventare tale supporto. Se un'operazione rifiuta una carta contenente un crittogramma, non provare a saltare la protezione o a cancellare a mano la sua intestazione.

In BIT una copia deve conservare l'insieme necessario e il rapporto tra file. Un gestore dei file può visualizzare un trasferimento completo senza garantire che il dispositivo abbia convalidato il contenuto o abbia terminato l'operazione. Attendere gli stati indicati e controllare una copia tramite recupero controllato.

Tieni un inventario privato con identificatori discreti, versione di formato, data e risultato dell'ultimo test. Divide almeno due copie rispetto agli incidenti che hai definito. Evita di caricare backup su canali di supporto per diagnosticare problemi; facilita i metadati debuttati e i codici di errore.

Esercitazione

1. Crea una copia del tuo crittogramma didattico su un altro supporto tramite il flusso corretto.
2. Scollega il supporto originale e recupera dalla copia il testo di prova.
3. Documenta cosa faresti in caso di perdita, danneggiamento di file e password. Non sono la stessa procedura.

Dimostra cosa hai imparato

Sai identificare la copia che hai verificato e spiegare perché l'originale non è stato sovrascritto.

Domanda frequente

Posso cancellare l'originale dopo aver visto un secondo file? Prima controlla il recupero e la copertura. L'eliminazione deve rispondere a un piano, non al semplice numero di copie.

Punto di pausa

Salva i supporti prima di chiudere la sessione; non lasciare carte mescolate con quelle dei test di pagamento.

Se qualcuno conosce la password e ottiene una copia del crittogramma, a cosa serve creare altri tre cloni?

1. Revoca la copia dell'aggressore.
2. Aumenta la ridondanza ma non revoca quell'accesso.
3. Cambia automaticamente il seed Bitcoin.

> **Mostra risposta: Aumenta la ridondanza ma non revoca quell'accesso.**
> La duplicazione non elimina una compromissione già avvenuta.

M05

Installare e proteggere Cuvex Desk

Obiettivo

Aprire un impianto di provenienza verificato e proteggere il tuo archivio locale.

Comprendere

Seleziona il pacchetto dal tuo sistema e architettura: macOS Intel o Apple Silicon, Windows x64 o ARM64 e Linux x64 o ARM64 in base alla distribuzione disponibile. Uno ZIP di font, un pacchetto per il Manager e un installatore per il cliente sono consegne diverse. Il corso non deve indirizzare uno studente ad un pacchetto privato di firma.

Controlla la provenienza e le verifiche del sistema. Una ditta di ingegneria di Windows non fornisce di per sé la fiducia pubblica dell'editor. Su Mac, firma applicazione, notarizzazione e valutazione all'apertura sono controlli diversi. Non disattivare protezioni generali seguendo una chiamata di supposto supporto. Se una versione dà un avviso inaspettato, conserva il testo e utilizza il canale ufficiale.

Desk crea un vault locale cifrato con password. Nella base riveduta, le nuove password supportano da 12 a 1.024 caratteri; la corrispondenza dei campi è richiesta dove c'è conferma. Questi limiti non sono una misura di qualità sufficiente: usa una frase unica ed evita il riutilizzo. La biometria del computer, quando disponibile, è una comodità di accesso che richiede la propria configurazione.

Configura il blocco per inattività e, se del caso, quando passa in background. Il ritardo dopo i bug e la cancellazione opzionale sono studiati nel manuale: non attivare una cancellazione automatica durante una dimostrazione. L'app può funzionare senza un account utente convenzionale, ma i suoi servizi di consultazione, chat o download hanno requisiti e comunicazioni specifici.

Esercitazione

1. Verifica piattaforma, versione visibile e provenienza del pacchetto senza fornire al tutor identificatori privati.
2. Crea un magazzino di apprendimento e controlla il blocco e la riapertura. Inserisci la password in privato.
3. Programma una copia crittografata e salva la tua password secondo il tuo piano. Non provare a bloccare ripetutamente l'ambiente reale.

Dimostra cosa hai imparato

Puoi distinguere password locale, account commerciale e credenziali dai servizi che aggiungi.

Domanda frequente

Cambiare la password di Desk cambia quella delle mie carte? No. Sono protezioni indipendenti. Le vecchie copie non cambiano nemmeno da sole.

Punto di pausa

Blocca Desk e conserva l'identificativo della lezione, senza credenziali.

Il programma di installazione non corrisponde alla tua architettura. Qual è il primo passo?

1. Forzarne l'esecuzione disattivando le protezioni.
2. Procurarsi il pacchetto ufficiale adatto e verificarne i requisiti.
3. Importare la frase seed su un sito per continuare.

> **Mostra risposta: Procurarsi il pacchetto ufficiale adatto e verificarne i requisiti.**
> Compatibilità e provenienza vanno verificate prima di utilizzare materiale di custodia.

M05

Associare crittogrammi e organizzare le WOW

Obiettivo

Collegare una copia crittografata e distinguerla da un conto di osservazione.

Comprendere

Desk organizza i crittogrammi associati tramite NFC, USB o un file di copia compatibile. Un disegno visivo e uno pseudonimo aiutano a riconoscerli, ma non sono una prova di identità. Nella scheda puoi vedere origine e proprietà interpretate dall'app, come formato, dimensione e funzionalità di accesso.

Collegare importa o organizza l'oggetto compatibile; non significa decifrarlo sul PC o controllarne il segreto. WOW è un portafoglio di osservazione associato da informazioni pubbliche compatibili. Una stessa serie di segreti può avere diversi conti o derivazioni: l'associazione deve corrispondere al portafoglio che si intende gestire.

Attiva o importa l'account con il descrittore o informazioni pubbliche esportate dal flusso del dispositivo. Controlla rete, tipo di script, impronte, percorso e direzione di controllo. Il nome del conto è organizzativo; l'identificatore derivato da un nome non deve essere trattato come anonimizzazione forte, perché un nome prevedibile può essere indovinato.

Nella base di Desk vengono conservati conti in sospeso di associazione e funzioni per esportare copie, clonare ed eliminare registri locali. Eliminare una scheda dall'interfaccia non distrugge le copie esterne né sposta i fondi. Non c'è backup di un'applicazione significa che l'applicazione non acconsenta a una copia a sua discrezione, non che nessun backup esista nel mondo.

Esercitazione

1. Collega il crittogramma didattico per il trasporto scelto e controlla la scheda.
2. Importa un account di apprendimento compatibile e controlla la tua rete e l'indirizzo di controllo senza mostrare le chiavi al tutor.
3. Distingui il record del crittogramma, il conto WOW e il supporto fisico. Identifica cosa sarebbe scomparso con una rimozione locale.

Dimostra cosa hai imparato

Puoi spiegare quali dati Desk ha bisogno di osservare e quali devono rimanere al di fuori del computer durante l'uso abituale.

Domanda frequente

Collegare un file.bin garantisce che sia il mio seed? No. Devi verificare la sua provenienza e il suo recupero. Un'estensione file non certifica il contenuto.

Punto di pausa

Conserva solo lo stato di prova in corso.

Eliminare localmente un conto WOW ne sposta i bitcoin?

1. No. Elimina informazioni locali secondo la procedura, senza spendere gli UTXO.
2. Sì. Li invia al produttore.
3. Annulla ogni firma di cui un'altra persona conservi una copia.

> **Mostra risposta: No. Elimina informazioni locali secondo la procedura, senza spendere gli UTXO.**
> Lo stato locale e quello della catena sono distinti.

M05

Collegare Mirror a Desk

Obiettivo

Impostare e terminare un link locale autorizzato senza confondere i codici.

Comprendere

Mirror consente operazioni locali con Desk attraverso il flusso di link, PIN e QR che presentano le applicazioni. Il PIN a sei cifre appartiene a questa sessione. Non è la password di Desk, quella del crittogramma o una parola di recupero. Controlla quale schermo è generato e dove deve essere inserito; non usare un codice inviato da una persona sconosciuta.

Avvia l'azione dal contesto corretto di Desk: collegare, leggere QR, trasportare PSBT o firmware sono obiettivi diversi. La finestra segnala ricerca, connessione, scoperta, PIN, QR e azione su scheda o file. Il fatto che un dispositivo sia presente nella ricerca non dimostra che l'intera operazione sia terminata.

Concede autorizzazioni rilevanti secondo il sistema: fotocamera per lettura ottica e Bluetooth o NFC quando il flusso le richiede. Un telefono senza una capacità fisica necessaria non lo ottiene installando software. In iOS ci sono differenze di adattatore e convalida; un progetto compilato non deve essere presentato come se fosse già distribuito e testato su tutti gli iPhone.

Se fallisce, identifica la fase esatta: non appare, appare ma non collega, PIN respinto, QR illeggibile, carta non letta o risposta non ricevuta. Chiudi le vecchie sessioni, verifica la compatibilità delle versioni e le autorizzazioni, poi riprova in modo controllato. Un PIN errato non giustifica la modifica del firmware o l'inserimento di frasi seed altrove.

Esercitazione

1. Inizia una lettura di prova da Desk e collega Mirror tramite i suoi schermi locali.
2. Controlla l'obiettivo prima di presentare un QR o una scheda di insegnamento.
3. Annulla la sessione e conferma che dopo non si applica una lettura di un contesto precedente. Riapri una nuova sessione.

Dimostra cosa hai imparato

Sai descrivere la fase non riuscita e i dispositivi coinvolti senza comunicare codici attivi o contenuti sensibili.

Domanda frequente

Mirror deve rimanere sempre connesso? Dipende dall'operazione. Non trattarlo come un servizio permanente o supponiamo che una sessione sia ancora autorizzata dopo la chiusura o il passaggio in background.

Punto di pausa

Chiudi la sessione di collegamento e blocca le applicazioni che non stai usando.

Cosa deve fare il tutor se il collegamento fallisce prima di mostrare il PIN?

1. Chiedere la frase seed.
2. Verificare rilevamento, autorizzazioni, sessione e versioni prima di procedere.
3. Dare per completata la connessione.

> **Mostra risposta: Verificare rilevamento, autorizzazioni, sessione e versioni prima di procedere.**
> La diagnosi deve seguire la fase osservata senza presumere che la connessione sia riuscita.

NFC tramite Mirror, USB-C e lettura dei codici QR

Obiettivo

Utilizzare ogni trasporto mantenendo il suo scopo e i suoi controlli.

Comprendere

Le operazioni NFC di Cuvex Desktop richiedono Cuvex Mirror su uno smartphone compatibile collegato al computer tramite Bluetooth. Cuvex Desktop non supporta lettori NFC USB esterni. Anche la carta, il formato e la capacità devono essere compatibili. Una carta piccola sufficiente per un crittogramma potrebbe non contenere una PSBT con transazioni precedenti. Il limite effettivo dipende dall’intero contenuto, non solo dal numero dei destinatari. Non usare una carta di backup come carta di trasporto.

In Original, Mirror può scrivere una richiesta su una scheda operativa; il dispositivo la elabora e scrive una risposta che Mirror restituisce a Desk. La conferma di scrittura non significa ricezione di Desk. Tieni ferma la carta finché il dispositivo non indica l'esito. Se il sistema protegge un crittogramma riconosciuto, rispetta questo rifiuto.

BIT utilizza un volume o una cartella USB di scambio. La procedura può smontare il volume o renderlo di nuovo disponibile. Desk deve selezionare il supporto corretto, convalidare la risposta e inviare la conferma di ricezione prevista. Copiare un file in una cartella del PC con lo stesso nome non equivale a consegnarlo al dispositivo.

Una fotocamera che non legge un QR può non essere messa a fuoco, riflesso, dimensione, movimento o densità. Amplia i dati e migliora luce e distanza. Non sostituire un identificatore lungo con le prime lettere o accettare una trascrizione parziale. La lettura di successo è solo l'inizio della sua convalida semantica.

Esercitazione

1. Con materiale didattico identifica richiesta, supporto e risposta per Original e BIT nel diagramma.
2. Prova a cancellare una lettura QR senza salvare valori tardivi. Ripeti con un altro scopo.
3. Simula un file troppo grande e spiega perché si dovrebbe ridurre la complessità dell'operazione o scegliere un supporto compatibile, senza rimuovere le validazioni.

Dimostra cosa hai imparato

Sai indicare quale dispositivo ha confermato ciascuna fase: lettura, scrittura, convalida, ricezione o conferma di ricezione.

Domanda frequente

Un hash o un OK di copia prova che il destinatario Bitcoin è corretto? No. Dovresti controllare l'operazione e le sue uscite dal firmatario.

Punto di pausa

Rimuovere e salvare le schede di backup; lasciare identificato il supporto di trasporto.

Original segnala di aver scritto la risposta sulla carta. Cosa manca prima di affermare che Desk l'ha ricevuta?

1. Dipingere la carta di un altro colore.
2. Creare una nuova frase seed.
3. Leggere la risposta e convalidarla in Desk con l'apposita procedura.

> **Mostra risposta: Leggere la risposta e convalidarla in Desk con l'apposita procedura.**
> Il successo della scrittura e quello della ricezione sono eventi distinti.

Fornitori pubblici e nodo proprio

Obiettivo

Scegliere una fonte di consultazione e comprendere le vostre perdite e limiti.

Comprendere

Desk può consultare fornitori pubblici compatibili o un Bitcoin Core configurato dall'utente. Un fornitore può conoscere le richieste ricevute, la sequenza e i dati di connessione. Non inviare una xpub completa riduce una specifica esposizione, ma gli script o i suoi hash possono anche collegarsi tra loro.

In Desk 9.21 viene visualizzata l'esplicita scelta di Blockstream Electrum da parte di TLS, oltre a alternative REST e nodo proprio. TLS protegge il canale da alcuni osservatori di rete; il fornitore stesso continua a ricevere le consultazioni. Non c'è una rotazione silenziosa che garantisca l'anonimato. La scelta richiede di comprendere questo scambio di privacy per comodità.

Per Core configura endpoint, autenticazione e wallet di osservazione secondo la guida corrispondente. Non pubblicare il porto della RPC o lasciarlo esposto a Internet per far vedere all'app !" Limita l'accesso ad ambienti affidabili e utilizza un trasporto protetto appropriato. Una password RPC non è dettata al tutor.

La sincronizzazione iniziale e una scansione possono richiedere. Il progresso deve essere interpretato come uno stato di lavoro, non come un successo anticipato. Desk mantiene un lavoro in background; chiudere la vista non significa fermare il nodo. La finestra minima storica documentata non garantisce la scoperta di attività precedenti: se il portafoglio è più vecchio, controlla la data di importazione e la portata effettiva della scansione.

Scoperta si basa su storia, non su saldo positivo. Un indirizzo speso fino a zero e' ancora usato. In multifirma riveduta, viene applicato un spazio di 20 indirizzi consecutivi senza cronologia per ramo e partecipante, con limiti di emissione. Non estrapolare un limite globale a tutti i portafogli.

Esercitazione

1. Seleziona una fonte di apprendimento e spiega quali informazioni puoi visualizzare.
2. Controlla la data di ultima sincronizzazione, rete e avanzamento. Se c'è HTTP 429, rispetta la pausa e non cambiare fornitore senza decidere.
3. Fai finta di avere un wallet con un saldo zero e una vecchia storia. Controlla perché il tuo nome è diverso.

Dimostra cosa hai imparato

Puoi decidere se la tua fonte copre la tua necessità di verifica e privacy e riconoscere uno stato incompleto.

Domanda frequente

Un nodo mi rende anonimo? No. Riduce le dipendenze di consultazione, ma devi considerare connessione, controparti, pubblicazione e altri metadati.

Punto di pausa

Registra solo tipo di fornitore e necessità di completare la scansione.

Un indirizzo ha saldo zero, ma in passato ha ricevuto e speso fondi. Come va trattato nella ricerca degli indirizzi del wallet?

1. Come un indirizzo con cronologia.
2. Come un indirizzo mai usato.
3. Come un indirizzo non valido.

> **Mostra risposta: Come un indirizzo con cronologia.**
> È la cronologia, non il saldo attuale, a determinare se l'indirizzo è stato usato.

Ricevere bitcoin e verificare l'indirizzo

Obiettivo

Creare una richiesta di ricezione e verificarla prima di consegnarla.

Comprendere

Apre il corretto account WOW e conferma rete e politica. Genera o recupera una richiesta di ricezione. Puoi aggiungere motivo, osservatore e importo atteso per la tua organizzazione. Questi campi descrivono le tue informazioni locali; l'importo atteso non impedisce a qualcuno di inviare un altro importo.

Verifica la direzione tramite il flusso disponibile sul dispositivo e il contesto del portafoglio. Se questo percorso non è ancora fisicamente convalidato nella tua combinazione, la pratica rimane in simulazione e si scala prima di ricevere fondi importanti. Confrontare due schermi alimentati dalla stessa fonte non offre alcuna indipendenza che non esista.

Utilizza un nuovo indirizzo per un nuovo rapporto di riscossione quando il flusso lo consente. Nella multifirma riveduta, gli indirizzi già mostrati non vengono riassegnati né scaduti perché un pagatore può utilizzarli più tardi. Quando si arriva al limite di nuovi indirizzi consecutivi senza cronologia, recupera la richiesta precedente appropriata e comprende il motivo del limite; non riavvolgere indici.

Dopo la condivisione, controlla l'ingresso nella tua fonte di verifica. Una posta, un giustificativo dell'exchange o una cattura del pagatore non mostrano liquidazione. Controlla rete, txid, uscita, importo e conferma in base all'esposizione. Non aprire un esploratore pubblico con il tuo indirizzo per comodità se il tuo piano richiede di mantenere quelle richieste private.

Esercitazione

1. Genera una richiesta in laboratorio, controlla account e rete e spiega come controlleresti l'indirizzo.
2. Registra un'etichetta fittizia e recupera la stessa richiesta dopo la chiusura della vista.
3. Simula un addebito di importo diverso e decide come conciliarlo senza modificare la cronologia.

Dimostra cosa hai imparato

Puoi distinguere indirizzo generato, indirizzo verificato, richiesta condivisa e recupero confermato.

Domanda frequente

Un vecchio indirizzo smette di funzionare creandone un altro? Di solito no. Mantenere la scoperta e la registrazione delle richieste evita di perdere visibilità dei pagamenti tardivi.

Punto di pausa

Salva lo stato della richiesta di laboratorio, non il suo contenuto nel tutor.

Il pagatore ti invia una schermata che dice «prelievo completato». Cosa verifichi per accettare il pagamento?

1. Solo la qualità della schermata.
2. L'output corrispondente su una fonte di rete affidabile e le conferme necessarie.
3. La password del pagatore.

> **Mostra risposta: L'output corrispondente su una fonte di rete affidabile e le conferme necessarie.**
> Un documento commerciale o una schermata non sostituisce la verifica del pagamento.

Etichettare, congelare e selezionare gli UTXO

Obiettivo

Preparare ingressi senza mescolare le origini per caso.

Comprendere

Le etichette consentono di conservare un contesto che non figura nella catena: origine, controparte, finalità e restrizioni d'uso. In Desk un'etichetta UTXO e una nota di direzione possono avere lunghezze e funzioni diverse. Annotare · client "A" è utile; utilizzare il documento o il nome completo può creare un record inutilmente sensibile.

Congelare un UTXO in Desk la esclude da alcune selezioni locali. Non blocca la spesa in Bitcoin, non cambia lo script e non impedisce ad un'altra app di utilizzarla con le chiavi. È inoltre possibile rendere il saldo totale e il saldo speso diverso. Controlla se una moneta è congelata, prenotata da una bozza o effettivamente spesa.

La selezione automatica ottimizza in base all'algoritmo e al contesto; non conosce necessariamente le tue relazioni private. Per un pagamento specifico, controlla se sia opportuno utilizzare un'uscita dallo stesso contesto invece di unire il risparmio, il libro paga e l'attività commerciale. La separazione utile richiede coerenza futura, non solo belle etichette.

Esporta etichette formattate BIP329 facilita la conservazione o la migrazione. Il formato da solo non cifra i dati. Desk offre una confezione crittografata per l'esportazione; distingue il file protetto da un testo piatto compatibile. All'importazione, controlla la corrispondenza con il portafoglio e il trattamento di congelamento prima di sovrascrivere le informazioni.

Esercitazione

1. Etichetta tre UTXOs sintetiche come risparmio, attività e donazione.
2. Congela una e verifica la differenza tra il saldo osservato e quello disponibile per la selezione.
3. Esporta etichette dal laboratorio con password, importa in una copia e controlla i risultati senza dati privati reali.

Dimostra cosa hai imparato

Giustifica la selezione degli input in termini di costo ed esposizione. Riconosce che il congelamento è una preferenza locale.

Domanda frequente

Un'etichetta viaggia al destinatario quando paga? Non per il semplice fatto di essere un'etichetta locale. È possibile filtrare quando si esporta, condividere file, utilizzare un altro servizio o aggiungerlo a un messaggio.

Punto di pausa

Salva le etichette di pratica e lo stato di congelamento.

Che effetto ha congelare un UTXO in Desk?

1. Crea un blocco di consenso nella rete.
2. Lo trasferisce a un conto speciale.
3. Applica una restrizione locale alla selezione nell'app.

> **Mostra risposta: Applica una restrizione locale alla selezione nell'app.**
> Non revoca la capacità di spesa di altre copie delle chiavi.

Preparare e verificare un pagamento

Obiettivo

Costruire una PSBT comprensibile e riconoscere tutti i costi e le uscite.

Comprendere

Seleziona account, voci spendibili, destinatari e importi. Verifica l'origine della domanda. Quando incolla o scansiona, controlla l'indirizzo completo e la rete; gli appunti e un'immagine possono essere sostituiti. Non fidarti solo dei primi e degli ultimi caratteri se la procedura permette un controllo completo.

Scegli la tariffa e verifica la commissione assoluta, la dimensione stimata, il totale e il resto. Con l'invio del totale di lettere, Desk sottrae la commissione dall'importo disponibile. Se l'azione nasce dalla chat e il netto non copre quanto richiesto, un pagamento parziale deve essere consapevole; la richiesta originale non si trasforma per nascondere la differenza.

Verifica se il resto è ridotto o se manca del tutto un output di resto. Un'uscita segnata come propria richiede una verifica politica, non con il nome che gli dà il coordinatore. Se il resto non è praticabile, rivedi il trasferimento dell'intero saldo o aggiungi un input compatibile. Non accettare che si trasformi senza preavviso in una commissione sproporzionata.

PSBT è un formato per il trasporto di informazioni e firme. Non contiene necessariamente la privacy o l'autenticità di origine. È possibile includere transazioni precedenti, chiavi pubbliche, percorsi e metadati. Nei firmware Finale esaminati il profilo multifirma utilizza PSBT v0/BIP174; termini di transazione versione 2 più non significa bambino PSBT 2 più.

Esercitazione

1. Prepara nel simulatore un pagamento con un input di 120.000 sat, 70.000 al destinatario e una commissione di 1.000.
2. Elenca tutti gli output e spiega il resto di 49.000 sat. Ripeti l'operazione trasferendo l'intero saldo.
3. Annulla la bozza e spiega cosa hai cancellato localmente. Non usare questo simulatore per firmare o pubblicare niente.

Dimostra cosa hai imparato

Prima dell'esportazione puoi spiegare cosa entra, cosa esce, chi riceve, quanto costa e quale autorizzazione manca.

Domanda frequente

Posso inviare l'intero importo che mostra il saldo? Solo se l'app calcola una spedizione netta valida e le commissioni sono coperte. Il saldo può includere monete non disponibili.

Punto di pausa

Salva una bozza di apprendimento o annullalo; mai una vera PSBT sul portale del corso.

Uno schermo indica «transaction version 2». Dimostra che il file è una PSBT v2?

1. No. Sono campi di versione distinti.
2. Sì, sempre.
3. Dimostra che utilizza Taproot.

> **Mostra risposta: No. Sono campi di versione distinti.**
> BIP370 distingue la versione del contenitore dalla versione della transazione.

Firmare con Original e con BIT

Obiettivo

Completa ogni ramo di firma e riceve una risposta legata all'operazione corretta.

Comprendere

Con Original, consegna la PSBT usando la carta di trasporto della procedura compatibile, tramite Cuvex Mirror. Sul dispositivo leggi la richiesta, presenta il crittogramma e sbloccalo in privato. Verifica tutti gli output, gli importi, il resto e la commissione. La risposta viene scritta sulla carta e poi letta e convalidata in Desk. L’esito positivo della scrittura sulla carta non sostituisce questo ritorno.

BIT: seleziona il volume corretto e consegna la richiesta via USB-C. Il servizio locale di Desk risponde allo scambio previsto mentre tu operi il dispositivo. Presenta il crittogramma come indicato sullo schermo e verifica i dati su BIT. «Ricevi da BIT» importa la risposta. Desk la convalida e la salva prima di confermare la ricezione. Una disconnessione richiede di recuperare la stessa operazione, non un'altra scelta per somiglianza.

Durante la firma di una transazione multifirma con i firmware Final si verificano il riepilogo, gli output obbligatori, gli avvisi applicabili e le tre conferme finali di «Firma PSBT». La revisione estesa opzionale consente di esplorare più parametri; scegliendo No più non si eliminano le revisioni obbligatorie. La verifica indipendente di una politica è un altro percorso e mantiene la sua portata di tale revisione.

La firma richiede un crittogramma compatibile la cui autenticità può essere verificata. Una copia storica che permette ancora di recuperare il segreto non è quindi autorizzata a firmare. Se il dispositivo segnala una vecchia copia non autenticamente verificata, segui il percorso di recuperare e controllare il segreto e crearne una nuova prima di firmare. Non alterare le intestazioni o omettere il rifiuto.

Se un indirizzo non corrisponde, c'è una commissione inaspettata, mancano i dati, c'è un'altra rete o il dispositivo rifiuta la politica, cancella. Non trasformare la pressione in un'approvazione per aver finito la chiamata. L'IA non preme pulsanti, non effettua la conferma finale e non dichiara firmato ciò che non hai verificato.

Esercitazione

1. Segui il percorso del tuo modello con un wallet senza fondi o in un laboratorio già accettato mediante prove fisiche.

2. Fai finta di fermarti prima delle conferme finali e spiega perche' non e' come autorizzare.
3. Verifica il ritorno, la corrispondenza con la bozza e, su BIT, lo stato della ricezione e della relativa conferma.

Dimostra cosa hai imparato

Puoi narrare il percorso senza rivelare credenziali e distinguere approvazione sul dispositivo, risposta importata e operazione pubblicata.

Domanda frequente

Il dispositivo offline sa se i miei input sono ancora non spesi? Da solo non può verificare lo stato attuale della catena. L'app deve verificare la transazione finale contro la sua fonte di rete.

Punto di pausa

Se interrompete la firma, annullate o lasciate un'operazione in sospeso identificata in base al flusso, senza segreti visibili.

BIT firma, ma Desk non conferma la ricezione. Quale stato devi presumere?

1. Pagamento definitivamente pubblicato.
2. Risposta in attesa di ricezione o convalida. Riprendi la stessa operazione.
3. Wallet perso.

> **Mostra risposta: Risposta in attesa di ricezione o convalida. Riprendi la stessa operazione.**
> Firma, ricezione e pubblicazione sono fasi diverse.

Finalizzare, pubblicare e risolvere i problemi

Obiettivo

Chiudere il ciclo di pagamento senza raddoppiarlo e diagnosticare i bug per fase.

Comprendere

Dopo l'importazione di una firma, Desk deve verificare che corrisponda alla bozza e mantenere l'intenzione. In più firme può mancare la soglia; in a firma singola una firma importata non dispensa nemmeno dalla revisione. Terminare produce la transazione pronta a diffondere quando le sue condizioni sono complete.

Pubblica solo dopo la revisione finale. Una risposta del server o un txid indica un esito della richiesta. Bisogna seguire l'operazione per verificarne l'accettazione e lo stato sulla catena. Se l'app non ha ricevuto risposta, consulta prima di ripetere. Non inventare un nuovo pagamento per risolvere un problema di visualizzazione.

Per un pagamento in sospeso, controlla la tariffa, la validità, i conflitti e la possibilità reale di RBF. In caso di cambiamento di politica o di destinatario, la nuova proposta richiede nuove firme adeguate. Annullare localmente non distrugge una firma o una transazione che già conservi un'altra persona; né revoca la conferma.

Diagnostica per fasi: preparazione, trasporto, sblocco, revisione, firma, ritorno, convalida, completamento, diffusione e conferma. Registra sistema, versione, modello, fase, ora approssimativa e codice di errore. I dati diagnostici dell'app sono progettati per escludere informazioni sensibili. Controllali prima di condividerli ed evita di allegare copie, codici QR, la Chiave Chat o credenziali.

Esercitazione

1. Ordina gli stati di un pagamento fittizio e identifica dove faresti una pausa sicura.
2. Risolvi tre casi: saldo insufficiente, risposta USB non ricevuta e pubblicazione con connessione interrotta.
3. Scrivi una richiesta di assistenza usando dati sintetici e indicando un risultato atteso verificabile.

Dimostra cosa hai imparato

Puoi decidere se manca l'azione dell'allievo, del dispositivo, del coordinatore o della rete ed evitare un secondo pagamento inutile.

Domanda frequente

Un errore FIRMWARE_CAPABILITY_REQUIRED viene risolto cambiando il firmware alla cieca? No. Nell'incidenza documentata di Desk, il riconoscimento del build Final richiedeva la correzione del catalogo di Desk. Controlla la versione e il profilo prima di modificare i computer.

Punto di pausa

Salva lo stato e la prossima azione. Se hai pubblicato un'operazione vera fuori dal laboratorio, tieni i suoi documenti personali.

Quale azione può da sola revocare una transazione già confermata?

1. Cancellare la bozza locale.
2. Chiudere Mirror.
3. Nessuna delle due.

> **Mostra risposta: Nessuna delle due.**
> La cancellazione locale non riscrive la catena e non ritira autorizzazioni già in circolazione.

Cosa si può osservare in Bitcoin

Obiettivo

Identificare dati pubblici, inferenze e dati che si aggiungono al di fuori della catena.

Comprendere

Bitcoin on-chain è pubblico: script e indirizzi rappresentativi, valori, rapporti tra ingressi e uscite e posizione in blocchi possono essere analizzati. Il tuo nome non compare necessariamente, ma un acquisto identificato, una fattura pubblicata o un indirizzo condiviso possono collegarti a quella cronologia.

Pseudonimato significa operare con identificatori che non sono di per sé la tua identità civile. Anonimato richiederebbe un insieme e condizioni di indistinguibilità che non si ottengono semplicemente installando un'app. La privacy dipende dal contesto: un esercente conosce il tuo pagamento, un exchange può conoscere il tuo prelievo, un server conosce le richieste e una persona può osservare i tuoi dispositivi.

Distingui fatti e inferenze. «Questo output è stato speso in quella transazione» è un'affermazione verificabile sulla catena. «Tutti questi input appartengono alla stessa persona» è un'inferenza euristica che può essere errata. L'identificazione al di fuori della catena può aumentare la fiducia di un'ipotesi senza convertire tutte le interpretazioni in certezze.

Riusare un indirizzo facilita l'aggiunta di attività. Unire UTXOs di contesti diversi può collegarli. Rivelare un xpub permette un'osservazione più ampia che insegnare un solo indirizzo. Condividere un txid può anche mostrare altre uscite e relazioni che il ricevitore non aveva bisogno di conoscere.

Esercitazione

1. Segna in una transazione fittizia quali dati sono pubblici e quali etichette sono tue.
2. Aggiunge una fattura con nome e descrive quale nuovo link appare.
3. Invia una richiesta di supporto che risolve un errore senza includere indirizzo, descrittore o saldo.

Dimostra cosa hai imparato

Puoi dire questo, o questo si osserva più o meno, e spiegare quali prove mancano.

Domanda frequente

Se non riutilizzassi mai indirizzi, sarei gia' anonimo? No. La selezione degli input, il resto, le richieste, le controparti e altri metadati continuano a essere importanti.

Punto di pausa

Tieni una mappa degli osservatori senza identita' o transazioni reali.

Quale dato permette generalmente di osservare una famiglia di indirizzi di un conto?

1. Il colore dell'icona.
2. La sua xpub con un contesto di derivazione sufficiente.
3. La marca del cavo.

> **Mostra risposta: La sua xpub con un contesto di derivazione sufficiente.**
> Le informazioni pubbliche estese sono sensibili per la privacy anche se non autorizzano da sole la spesa.

Separare i contesti e gestire il resto

Obiettivo

Prendere decisioni di spesa coerenti con l'origine dei tuoi UTXOs.

Comprendere

La separazione dei contesti inizia prima del pagamento. Decide se una ricezione corrisponde a risparmio, attività professionale, spesa quotidiana o relazione concreta. Conserva queste informazioni su etichette private così che la selezione futura non le cancelli per ignoranza.

Un'etichetta non separa criptograficamente le uscite. Se spendi insieme due UTXOs di contesti diversi, la transazione pubblica la sua relazione. Consolidare riduce il numero di entrate di pagamenti futuri, ma aumenta il legame tra le uscite consolidate. Fare questo con tariffe basse può essere efficiente e al tempo stesso contrario al tuo obiettivo di privacy.

Il resto è un nuovo output controllato dalla stessa politica, non «denaro invisibile». L'uso successivo può estendere le precedenti relazioni. Non classificare un indirizzo come resto perché ha un importo insolito. In una verifica reale, il dispositivo deve controllare se appartiene al wallet.

Evita di convertire la privacy in modelli meccanici di importi, tempi o trasferimenti ripetuti. Questi modelli possono anche essere riconoscibili e generare più commissioni. Valuta quali dati conosce ogni parte e quali nuove informazioni pubblicherebbe l'operazione proposta. Nessuna sequenza cancella la storia già pubblicata.

Esercitazione

1. Crea cinque UTXOs fittizie in tre contesti e prepara un pagamento che utilizzi il minor numero di contesti necessari.
2. Individua il resto risultante e decidi come etichettarlo.
3. Confronta il costo e l'esposizione di consolidare tutte le uscite rispetto a tenerle separate.

Dimostra cosa hai imparato

Puoi giustificare un consolidamento o respingerlo con un motivo specifico, senza applicare una regola assoluta per tutti i casi.

Domanda frequente

Trasferire tutto in un'altra mia direzione mi rompe la cronologia? No. Il trasferimento pubblica un rapporto aggiuntivo e può aggiungere costi senza risolvere la tua minaccia.

Punto di pausa

Conserva il ragionamento del laboratorio e la politica di selezione scelta.

Quale conseguenza può avere consolidare stipendio e donazioni in un'unica transazione?

1. Rendere visibile un collegamento fra quegli input.
2. Cancellarne l'origine pubblica.
3. Trasformarli in denaro di anonimato garantito.

> **Mostra risposta: Rendere visibile un collegamento fra quegli input.**
> Ridurre il numero di UTXO può aumentare i collegamenti osservabili.

M07

Privacy di rete, Tor e VPN

Obiettivo

Distinguere la privacy della connessione dalla privacy sulla catena.

Comprendere

Un server di consultazione può collegare richieste ad una connessione. Il tuo provider di Internet può osservare destinazioni o modelli in base al trasporto. Una VPN sposta parte di tale fiducia all'operatore VPN; non elimina le informazioni pubbliche di Bitcoin né impedisce a un account identificato di riconoscerti.

Tor instrada il traffico attraverso una rete per ridurre determinati collegamenti tra origine e destinazione. Non trasforma un indirizzo Bitcoin in privato e non protegge un'applicazione il cui traffico non passa attraverso Tor. Apri Tor Browser non configura automaticamente Desk, Bitcoin Core e tutti i servizi del computer.

Prima di affermare che una connessione è protetta è necessario controllare il percorso e le impostazioni. In questa base non si presuppone un interruttore Tor integrato a Desk. Una distribuzione con nodo o proxy richiede una guida di ingegneria e convalida del traffico reale. Non si inventa un campo d'interfaccia perche' ce l'ha un altro Wallet.

Ci sono anche perdite da DNS, sincronizzazione account, link browser e servizi di prezzo. Uno schema può proteggere le domande di saldo e continuare a rivelare attività quando si apre un browser pubblico. Definisce la portata di ogni misura e il comportamento quando la connessione non funziona; evita cambiamenti silenziosi a un fornitore meno privato.

Esercitazione

1. Disegna il percorso del computer, il provider di connessione, il proxy se esiste, il nodo o il servizio e la rete Bitcoin.
2. Indica chi riceve le domande e chi vede la tua identità commerciale.
3. Fai finta che il nodo privato non risponda. Decidete tra fermare o cambiare esplicitamente fonte con conoscenza dell'esposizione.

Dimostra cosa hai imparato

Puoi spiegare quale minaccia riduce la tua configurazione e quale minaccia esiste ancora.

Domanda frequente

Tor garantisce che nessuno può associare un pagamento con me? No. Controparti, identificazione commerciale, modelli ed errori operativi possono continuare a collegarlo.

Punto di pausa

Registra la portata del progetto, non endpoint privati né password.

Aprire Tor Browser obbliga Desk a effettuare le richieste tramite Tor?

1. Sì, perché condividono il computer.
2. Sì, se l'icona è visibile.
3. No. Si deve configurare e verificare il percorso di rete di ciascuna applicazione.

> **Mostra risposta: No. Si deve configurare e verificare il percorso di rete di ciascuna applicazione.**
> La protezione di un'applicazione non si estende automaticamente alle altre.

M07

CoinJoin, Payjoin e limiti attuali

Obiettivo

Capire strumenti collaborativi senza attribuire loro anonimato o compatibilità inesistenti.

Comprendere

CoinJoin raccoglie contributi da parte di più persone in una transazione per rendere più difficili alcune inferenze su ingressi e uscite. Non è sinonimo di consegna di monete a un servizio di custodia che promette di restituire altre. Disegni diversi richiedono una revisione di coordinamento, custodia, commissioni, resistenza a partecipanti dannosi e trattamento successivo.

Payjoin include input del pagatore e del destinatario in un pagamento collaborativo, indebolendo alcune euristiche sulla proprietà comune. Richiede supporto compatibile su entrambe le estremità e un protocollo specifico. È materiale di comprensione tecnica: non è stato accreditato nelle fonti riviste un flusso Payjoin o CoinJoin integrato e operativo in Cuvex Desk.

La disponibilità e il contesto giuridico cambiano. La documentazione di Wasabi registra la chiusura del coordinatore di zkSNACKs l'1 giugno 2024; non deve essere mostrato un pulsante storico come se oggi garantisse un servizio. Nel 2025 il Dipartimento di Giustizia americano comunicò la dichiarazione di colpevolezza e le successive condanne dei fondatori di Samourai. Questo caso non permette di concludere che qualsiasi tecnica di privacy sia illegale in qualsiasi giurisdizione.

Uno strumento può ridurre un'inferenza e lasciarne intatti altri. L'origine identificata non scompare dai registri di una controparte. Ricombinazioni successive, metadati e bug dell'insieme dei partecipanti possono degradare la privacy. Inoltre, alcuni servizi possono applicare politiche commerciali diverse da quelle delle monete con determinate storie.

Esercitazione

1. Confronta una transazione corrente, una collaborativa e un servizio che riceve la custodia, senza eseguire operazioni reali.
2. Per uno strumento specifico, cerca versione, manutentore, stato del servizio e documentazione attuale prima di proporne l'uso.
3. Identifica i rischi tecnici, di custodia e giuridici separatamente. Il tutor non deve progettare evasioni di controllo né promettere suddetto fondo impossibile da rintracciare.

Dimostra cosa hai imparato

Puoi spiegare un vantaggio limitato e almeno due rischi o requisiti di una tecnica di privacy.

Domanda frequente

Cuvex ha bisogno di un mixer per la custodia privata? No. Controllo di query, dati, chiavi e selezione di UTXOs già risolvere rischi specifici, senza promettere totale occultamento.

Punto di pausa

Registra un attrezzo come "studiato" non come "compatibile" senza prove.

Quale affermazione è sostenibile?

1. CoinJoin garantisce anonimato permanente.
2. Una tecnica collaborativa può rendere più difficili alcune inferenze, con requisiti e limiti.
3. Qualsiasi servizio chiamato mixer mantiene l'autocustodia.

> **Mostra risposta: Una tecnica collaborativa può rendere più difficili alcune inferenze, con requisiti e limiti.**
> Le proprietà dipendono da protocollo, implementazione, partecipanti e uso successivo.

Cosa ci insegnano gli incidenti reali

Obiettivo

Trasformare incidenti documentati in decisioni verificabili, senza attaccare concorrenti né esagerare la protezione.

Comprendere

Mt. Gox: un'accusa del Dipartimento di Giustizia del 2023 descrive l'accesso non autorizzato ai server e alle chiavi e la successiva scomparsa dei fondi dei clienti. Un'accusa manifesta accuse, non una sentenza. La lezione di custodia è chiedere chi controlla realmente le chiavi e cosa succede se l'azienda fallisce.

Ledger Connect Kit, dicembre 2023: Ledger ha documentato una pubblicazione malvagia di una libreria utilizzata da applicazioni decentrate, dopo aver compromesso l'accesso di un ex dipendente. L'incidente ha colpito la catena di distribuzione del software e ha ingannato gli utenti di DApps EVM per firmare. Non dimostra una rottura dell'hardware di Ledger o del consenso di Bitcoin.

Bybit, febbraio 2025: FBI ha attribuito alla Corea del Nord un furto di circa 1.500 milioni di dollari in attivi virtuali. E 'stato un incidente di un exchange e risorse di altre reti; non si presenta come una rottura della crittografia di Bitcoin. Per l'allievo è importante verificare l'intenzione di una firma ed evitare che più persone si fidino ciecamente sullo stesso schermo.

Coinbase, maggio 2025: la società ha comunicato il furto di dati da parte di agenti di supporto corrotti per facilitare l'ingegneria sociale. Ha indicato che non sono state presentate password o chiavi private. Il rischio educativo e' che un truffatore conosca i veri dati e sia comunque un truffatore.

Bitcoin Core pubblica anche bug software: l'avviso CVE-2024-35202 ha descritto una possibile chiusura remota nelle versioni precedenti 25.0. Verificare le regole non elimina la necessità di mantenere il software. Da questo avviso non risulta un furto di chiavi.

Nel gennaio 2026 The Register ha riferito di un'esposizione di dati di ordini e di contatti degli acquirenti di Ledger tramite Global-e, con conferma attribuita a entrambe le aziende e senza alcuna incidenza di chiavi di recupero secondo tali dichiarazioni. Il caso ricorda che un acquisto può rivelare che possiedi un dispositivo anche se l'hardware non è stato violato.

Nell'aprile 2026 The Record ha riferito dell'attacco a Drift e della sospensione dei depositi e dei ritiri annunciata dalla piattaforma. Si tratta di un protocollo finanziario decentralizzato su Solana, non di una rottura di Bitcoin. Le perdite inizialmente stimate e i processi di recupero successivi non devono essere presentati come importi definitivi né come rimborsi garantiti.

Esercitazione

1. Classifica ogni incidente per custodia, interfaccia o distribuzione, dati personali, protocolli di altre reti e disponibilità.
2. Per ciascuno propone una prevenzione e una limitazione di tale prevenzione.
3. Prova una telefonata fraudolenta: conosco il tuo acquisto; sposta i tuoi fondi in questa direzione sicura. Riaggancia e verifica la richiesta tramite un canale di comunicazione che hai aperto tu.

Dimostra cosa hai imparato

Puoi spiegare perche' nessun incidente prova che un marchio alternativo sia invulnerabile. Le prove supportano una certa portata.

Domanda frequente

Sono gli ultimi hacker che esistono? No. È una selezione verificata per l'edizione del 17 novembre 2026, non un inventario completo né un monitoraggio dal vivo.

Punto di pausa

Scrivi l'abitudine che cambierai e come vedrai che lo manterrai.

Una persona conosce il tuo acquisto e ti chiede di trasferire i fondi su un «wallet di salvataggio». Cosa dimostra il fatto che conosca l'acquisto?

1. Potrebbe trattarsi di informazioni trapelate. Non autentica né la sua identità né l'indirizzo.
2. Si tratta necessariamente dell'assistenza ufficiale.
3. Devi condividere la frase seed.

> **Mostra risposta: Potrebbe trattarsi di informazioni trapelate. Non autentica né la sua identità né l'indirizzo.**
> Dati veri possono essere usati per costruire un inganno convincente.

Creare un'identità e verificare i contatti della chat

Obiettivo

Attivare un' identità chat senza esporre la chiave e verificare la controparte.

Comprendere

In Desk, la chat è collegata al crittogramma tramite una Chiave Chat generata in Cuvex. Anche se la sua rappresentazione può sembrare una xpub, è segreta e non deve essere trattata come una chiave pubblica di un account WOW. Il tutor non ha mai bisogno di leggerla o vederla da QR.

Il flusso distingue alias nuovo e trasferimento o recupero di uno esistente. Nell'implementazione riveduta viene scelto il profilo mobile iOS o Android corrispondente, perché le identità derivate storiche non sono intercambiabili per intuizione. DEV e produzione sono ambienti separati: cambiare ambiente non migra automaticamente conversazioni o alias.

Aggiungere un alias non verifica l'identità. Controlla l'impronta tramite un canale indipendente e autenticato. Se l'app fornisce domande di riconoscimento, utilizza informazioni non pubbliche ed evita risposte che rivelino password. Una voce nota può essere imitata; per situazioni di rischio combina metodi concordati in precedenza.

Se cambia l'identità di un contatto, pausa pagamenti e coordinamento fino a risolverlo. Può essere un recupero legittimo o una sostituzione dannoso. La cifratura end-to-end protegge il canale secondo il protocollo e l'implementazione, ma non dimostra chi stia utilizzando il dispositivo all'altro capo.

Esercitazione

1. In un ambiente di prova, spiega il flusso di creare o recuperare senza facilitare la Chiave Chat.
2. Aggiungi un contatto di laboratorio e passa attraverso un altro canale un controllo delle impronte.
3. Fai finta di cambiare identita'. Definisci come verificheresti il resto prima di pagare.

Dimostra cosa hai imparato

Puoi distinguere pseudonimi, impronte pubbliche, Chiave Chat segreta e fiducia umana in una persona.

Domanda frequente

Un vecchio alias garantisce che sia la stessa persona? No. La continuità e le modifiche delle chiavi devono essere verificate in base al flusso.

Punto di pausa

Registra solo «contatto di prova verificato» e il metodo utilizzato, senza chiavi né domande private.

Una stringa si chiama Chiave Chat e assomiglia a una xpub. Come va trattata in Desk?

1. Come un dato pubblicabile nei forum.
2. Come un segreto per il recupero dell'identità.
3. Come un indirizzo di ricezione Bitcoin.

> **Mostra risposta: Come un segreto per il recupero dell'identità.**
> L'aspetto non determina la riservatezza o la finalità del dato.

Richiedere e pagare satoshi dalla chat

Obiettivo

Passare da una conversazione a un pagamento senza perdere revisione o contesto.

Comprendere

La chat permette di richiedere l'indirizzo, rispondere con un indirizzo di ricezione, richiedere il pagamento e aprire la preparazione da un conto WOW. Mantenere il contesto nel canale riduce gli errori di copia delle informazioni tra le applicazioni, ma non trasforma ogni messaggio in un ordine di spesa autenticato.

Prima di rispondere o pagare, controlla contatto verificato, rete, importo e richiesta originale. Il modulo condiviso conserva selezione di UTXOs e commissione. Se il messaggio richiede un importo e scegli !"Invia l'intero più basso, il netto dopo le commissioni può essere inferiore; deve essere identificato come pagamento parziale, se del caso.

L'autorizzazione rimane a Cuvex. La chat trasporta intenzione e coordinamento; non ha il permesso di firmare automaticamente. La conferma di pagamento inviata al contatto deve distinguere che è stato ricevuto un messaggio che esiste una transazione confermata. Il destinatario verifica con il proprio account o fonte.

Collegamenti esterni, allegati QR e indirizzi rimangono dati inaffidabili fino a convalidarli. Visualizza in Mempool è possibile aprire un servizio di terze parti e rivelare le domande. Se la tua politica utilizza un nodo proprio, preferisci la verifica supportata in WOW e valuta qualsiasi output per i servizi pubblici.

Esercitazione

1. Rappresenta due ruoli: ricevitore richiede 50.000 sat; pagatore prepara senza pubblicare.
2. Simula un saldo netto disponibile di 48.000 sat. Spiega quale consenso e conciliazione mancano per un pagamento parziale.
3. Cambia deliberatamente la rete in un messaggio di prova e ferma il flusso.

Dimostra cosa hai imparato

Sai seguire il rapporto tra richiesta, indirizzo, bozza, firma e conferma senza ridurlo a «la chat dice OK».

Domanda frequente

Inviare sats dalla chat significa usare Lightning? No. Il flusso WOW documentato prepara i pagamenti Bitcoin a catena. La parola sats esprime un'unità, non una rete di trasporto.

Punto di pausa

Cancella la bozza di laboratorio o registra lo stato; non pubblicare per mostrare un'interfaccia.

Ricevi una conferma in chat. Qual è la verifica decisiva dell'incasso?

1. Che l'icona del messaggio sia verde.
2. Che l'altra persona dica «confermato».
3. Verificare l'operazione e i relativi output sulla rete usando la fonte appropriata.

> **Mostra risposta: Verificare l'operazione e i relativi output sulla rete usando la fonte appropriata.**
> Lo stato del messaggio non equivale a quello della transazione.

Condividere crittogrammi in modo consapevole

Obiettivo

Capire cosa significa consegnare una copia crittografata a qualcun altro.

Comprendere

Condividere un crittogramma trasmette una copia dell'oggetto cifrato. Non invia necessariamente bitcoins né incorpora da solo un nuovo firmatario. Se il ricevitore ottiene anche mezzi di sblocco sufficienti, è possibile accedere al contenuto secondo lo schema; è quindi necessario decidere in anticipo quale capacità stai trasferendo.

La cifratura end-to-end della chat e la cifratura del file proteggono livelli diversi. Una volta scaricato, il ricevitore può conservare l'oggetto al di fuori della chat. Eliminare il messaggio o la registrazione locale non garantisce il ritiro di tutte le copie. Una password condivisa dallo stesso canale può concentrare i componenti su un unico binario.

Prima di inviare, verificare identità, formato e finalità. Se l'app permette di collegare un crittogramma ricevuto, questo organizza una copia, non attesta che sia sicuro decifrare qualsiasi file. Non usare allegati che richiedono l'inserimento di seed o password in una pagina esterna.

Il recupero richiede un accordo operativo: chi conserva ogni componente, chi può aprirlo, come viene rilevata un'esposizione e come viene cambiata la custodia se la relazione termina. Per un pagamento corrente è normalmente sufficiente un indirizzo convalidato; non è necessario condividere il tuo crittogramma.

Esercitazione

1. Progetta il trasferimento di un testo didattico cifrato a un contatto di laboratorio.
2. Elenca cosa sa e cosa potrebbe fare il ricevitore prima e dopo aver conosciuto la password.
3. Fai finta che la relazione sia finita. Spiega perché cancellare il messaggio non revoca né la copia né le chiavi.

Dimostra cosa hai imparato

Puoi distinguere i dati da me condivisi, ho condiviso l'accesso a un segreto e ho firmato una spesa.

Domanda frequente

Un file crittografato può circolare senza alcuna conseguenza? È possibile rivelare metadati, facilitare i tentativi di password e conservare indefinitamente. Valuta il bisogno di condividerlo.

Punto di pausa

Non lasciare gli assistenti di custodia durante il corso. Registra solo la conclusione dell'esercizio.

Condividere un crittogramma in chat equivale a inviare bitcoin?

1. No. Trasmette un oggetto il cui contenuto e accesso hanno una portata diversa.
2. Sì, purché il nome finisca con .bin.
3. Attiva automaticamente un nuovo wallet multifirma.

> **Mostra risposta: No. Trasmette un oggetto il cui contenuto e accesso hanno una portata diversa.**
> Trasportare segreti e spostare UTXO sono operazioni distinte.

Recuperare la chat e comprenderne i metadati

Obiettivo

Pianificare il cambio di dispositivo e distinguere il recupero dell'identità dal recupero dei messaggi.

Comprendere

Desk indica che cronologia e sessioni sono crittografate localmente e non fanno parte della loro copia globale. La Chiave Chat permette di recuperare l'identità; non garantisce il recupero di tutte le vecchie conversazioni. L'app include stati e azioni per l'attivazione in pendenza, la manutenzione delle chiavi e il recupero locale quando c'è materiale compatibile.

Ogni alias deve essere utilizzato in un unico dispositivo contemporaneamente secondo la guida alla base riveduta. Non attivarlo contemporaneamente su due dispositivi per «provare la sincronizzazione» se tale utilizzo non è supportato. Un trasferimento deve seguire la procedura e verificare la continuità con i contatti.

«In attesa», «accettato dal server», «ricevuto» e «impossibile decifrare» descrivono fasi diverse. Una spedizione non confermata non viene automaticamente inoltrata alla cieca: prima bisogna risolvere se è arrivata. Se manca una chiave di sessione o cambia identità, conservare il messaggio in attesa non equivale a averlo letto.

Il contenuto crittografato non nasconde necessariamente orari, dimensioni, rapporti di consegna, alias o dati di connessione rispetto a tutti i sistemi coinvolti. Nella voce accade qualcosa di simile: la cifratura del trasporto non trasforma una chiamata convenzionale in un canale adatto ai segreti. Usa il minimo dato necessario per imparare e risolvere i problemi.

Esercitazione

1. Simula perdere il PC e spiega cosa recupera ogni materiale disponibile.
2. Classifica gli stati dei messaggi e decidi quando non inviare una richiesta di pagamento.
3. Prepara un avviso di cambio di computer che i contatti possano verificare tramite un canale indipendente.

Dimostra cosa hai imparato

Puoi spiegare quale conversazione si perderebbe e quale identità potrebbe essere ristabilita senza promettere restauri che il backup non copre.

Domanda frequente

Cancellare la chat locale cancella anche i messaggi dall'altra parte? Non devi pensarci. Il ricevitore può conservare messaggi e file indipendentemente.

Punto di pausa

Salva un piano di trasferimento con nomi di campi vuoti, senza Chiave Chat.

Secondo la guida esaminata, cosa garantisce da sola la Chiave Chat?

1. La disponibilità di tutte le conversazioni precedenti su qualsiasi PC.
2. La possibilità di recuperare l'identità tramite la procedura compatibile, ma non tutti i vecchi messaggi.
3. L'accesso automatico alle chiavi Bitcoin dei contatti.

> **Mostra risposta: La possibilità di recuperare l'identità tramite la procedura compatibile, ma non tutti i vecchi messaggi.**
> L'identità e l'archivio storico sono capacità diverse.

Configurazione quotidiana e verifica delle autorizzazioni

Obiettivo

Controllare i parametri di Desk senza confondere comfort e protezione.

Comprendere

Desk offre tema Notte, Giorno o Sistema; sincronizzazione automatica e periodi di 3 o 5 minuti; suoni di transazione; sfondo della chat; lingua e valuta di riferimento. Queste preferenze cambiano presentazione o frequenza di consultazione. Non modificano una firma di Bitcoin, né aggiungono anonimato.

La configurazione di sicurezza riveduta consente blocco per inattività, blocco per il passaggio in background, ritardo massimo dopo bug e cancellazione opzionale. Lo schema di inattività ammette un intervallo da 30 a 86.400 secondi. L'interfaccia può offrire opzioni più ristrette. I valori di default devono essere letti dalla versione che esegui, non da una classe registrata.

L'integrazione di link bitcoin: apre una richiesta per sbloccare, scegliere account e rivedere. Non autorizza un pagamento automatico. In Linux, la guida differenza installazione integrata e AppImage per registrare i link. Una fattura Lightning richiede un flusso compatibile diverso; non è risolto dichiarando Desk applicazione predefinita.

La quotazione, il grafico dei prezzi e i link informativi possono consultare servizi esterni. La sua funzione è informativa e non un segnale di acquisto. Controlla data e fonte prima di utilizzare il dato per tradurre importi. Una modalità scura o una piccola finestra non devono nascondere pulsanti finali, direzione o commissione; se accade, pausa e segnala il problema della geometria.

Esercitazione

1. Regola l'aspetto e il blocco nel magazzino di apprendimento. Controlla se riesci a tornare dentro.
2. Controlla quali automatismi attivi: sincronizzazione, suoni e controllo firmware non sono la stessa cosa.
3. Apre una richiesta fittizia di link bitcoin: e cancella prima di preparare qualsiasi operazione reale.

Dimostra cosa hai imparato

Puoi spiegare l'effetto di ogni regolazione e individuare quelli che comportano domande o azioni sensibili.

Domanda frequente

La biometria del PC sostituisce la mia copia di recupero? No. Può dipendere dall'attrezzatura e dal deposito sicuro del sistema. Conserva il recupero indipendente.

Punto di pausa

Blocca Desk e annota solo le preferenze che hai cambiato.

Cosa cambia scegliendo la sincronizzazione ogni tre minuti?

1. La frequenza prevista delle richieste quando la funzione è in esecuzione.
2. La politica delle firme sulla catena.
3. La frase seed del dispositivo.

> **Mostra risposta: La frequenza prevista delle richieste quando la funzione è in esecuzione.**
> È una preferenza operativa e non una modifica della custodia.

M09

Progettare un wallet multifirma

Obiettivo

Scegliere una soglia che resiste a perdite e impegni ragionevoli.

Comprendere

In una politica N M, N è il numero di partecipanti con chiavi diverse e M il numero di firme necessarie. Una 2 su 3 resiste all'inammissibilità di una chiave, ma due chiavi compromesse possono autorizzare la spesa. Se i tre frasi seed sono nello stesso luogo o nascono da una stessa esposizione, l'indipendenza è ridotta.

Il profilo multifirma rivisto di Cuvex è P2WSH nativo con sortedmulti e derivazione BIP48. Original supporta strutturalmente fino a sei chiavi di politica e BIT fino a quindici. Se entrambi intervengono, il flusso deve rispettare il partecipante più limitato e la dimensione effettiva del trasporto. I limiti massimi strutturali non garantiscono che vi sia spazio per una politica con molte chiavi e molti input.

L'app ammette soglie che devono rispettare le relazioni politiche, ma una 1 di N non richiede la collaborazione per spendere. Il firmware conserva avvisi specifici su tale rischio. Scegliere un numero più grande non migliora tutto: aumenta il coordinamento, i costi, il materiale di recupero e la possibilità di blocco.

MuSig2 è un diverso schema di aggregazione delle firme Schnorr e, di per sé, è N di N, non una 3 di 5 arbitrariamente. Nei firmware Finale studiati non è stata implementata la firma di voci Taproot, MuSig2 o Miniscript. Ricevere un destinatario P2TR non dimostra la capacità di firmare da un portafoglio Taproot.

Esercitazione

1. Progetta una 2 su 3 fittizia con rischi indipendenti per ogni partecipante.
2. Simula la perdita di una chiave e, in un altro scenario, la compromissione di una chiave. Spiega cosa si può e cosa non si può fare.
3. Controlla i limiti per modello prima di scegliere una politica più grande.

Dimostra cosa hai imparato

Puoi esprimere tolleranza alla perdita, soglia di attacco e dipendenze condivise del tuo design.

Domanda frequente

La multifirma richiede che le persone conoscano le frasi seed degli altri? No. L'obiettivo è che ciascuna conservi la propria capacità privata e si condivida le informazioni pubbliche necessarie per costruire e recuperare la politica.

Punto di pausa

Salva il design con partecipanti fittizi e le loro responsabilità.

In una politica 2 su 3 con chiavi indipendenti, quante chiavi private bastano per autorizzare una spesa valida secondo quella politica?

1. Una.
2. Due.
3. Sempre tutte e tre.

> **Mostra risposta: Due.**
> La soglia richiede due chiavi. Anche le altre condizioni e convalide devono essere soddisfatte.

M09

Creare inviti e fornire le chiavi

Obiettivo

Costruire una politica con i partecipanti controllati senza condividere le frasi seed.

Comprendere

Il creatore sceglie nome, rete, M, N, contatti, informazioni pubbliche proprie e condizioni operative dell'invito. Nello schema rivisto sono accettate le reti mainnet e regtest per questo flusso, da 2 a 15 partecipanti prima di applicare i limiti del dispositivo, e la scadenza operativa da 1 a 720 ore. Non usare questi limiti come autorizzazione per saltare una verifica della capacità.

Ogni partecipante rivede l'invito, decide di accettare o rifiutare e fornisce la chiave pubblica estesa del partecipante con traccia e percorso BIP48 attraverso il flusso compatibile. Non fornisce seed, chiave privata, indirizzo libero o descrittore intero di un altro portafoglio. Una chiave non contestualizzata può produrre una politica diversa anche se ha un aspetto di xpub valido.

Il creatore coordina; non sostituisce la convalida di ciascun firmatario. Prima di ricevere fondi, tutti devono essere in grado di ricostruire e verificare gli stessi parametri e una direzione di controllo. Un contatto accettato in chat non implica l'approvazione automatica di qualsiasi politica che invii.

La scadenza di un invito è una regola di coordinamento dell'app. Non cambia da sola uno script già finanziato, non cancella le firme salvate da altre persone e non funziona come timelock consenso. Annullare una proposta e ritirare fondi da una politica esistente sono azioni diverse.

Esercitazione

1. In laboratorio regtest preparato, crea una proposta 2 di 3 con contatti di prova.
2. Rappresenta un'accettazione, un rifiuto e un contributo con rete errata. Controlla che l'ultima si fermi.
3. Elenca i dati che tutti devono conservare prima di finanziare: rete, soglia, chiavi pubbliche, origini, script e indirizzo verificato.

Dimostra cosa hai imparato

Puoi riconoscere un invito incompleto e spiegare quale approvazione manca senza assumerla per l'esistenza della chat.

Domanda frequente

Una data di scadenza rende impossibile spendere dopo? Non per essere un campo d'invito. Una limitazione temporanea di Bitcoin richiede condizioni di script o transazione specifiche e supporto reale.

Punto di pausa

Salva l'identificatore didattico della proposta e l'approvazione in sospeso.

Per contribuire a un wallet multifirma, cosa richiede la procedura documentata?

1. La frase seed di tutti i partecipanti.
2. Un indirizzo di ricezione qualsiasi.
3. La tua chiave pubblica estesa con impronta e origine BIP48 compatibili.

> **Mostra risposta: La tua chiave pubblica estesa con impronta e origine BIP48 compatibili.**
> Il materiale pubblico corretto permette di costruire la politica senza divulgare chiavi private.

Verificare le politiche con Mirror nell'ordine che preferisci

Obiettivo

Confrontare campi completi e capire esattamente che cosa attesta il risultato.

Comprendere

La verifica indipendente presenta soglia, rete, profilo, SIGHASH, ID policy, primo indirizzo, posizione utente e dati di ciascun partecipante. E' un controllo dell'intenzione e della coerenza. Non si presume che il dispositivo abbia registrato la politica in modo permanente. La portata documentata si limita a «questa verifica».

In Mirror 12.12 puoi leggere prima il QR di Cuvex o quello di Desk e scegliere qualsiasi dato. Non c'è obbligo di iniziare con il passaggio 1, di eseguire la scansione di tutti o di mantenere un ordine. Se controlli manualmente un testo, omettere la scansione non lo segna come verificato da Mirror.

Il comparatore mostra un testo letterale completo. Spazi, interruzioni di linea, maiuscole e differenze Unicode contano. Il valore dei due valori di tale coppia è uguale; non autentica origine, non prova che corrispondono alla stessa politica e non attiva il portafoglio. L'approvazione finale e la risposta correlata seguono il circuito Cuvex e Desk.

Gli attuali QR di Desk contengono solo il valore, senza ordine né sessione. Mirror non può sempre dedurre il passo. ·Indicare il passaggio di Desk è un'aggiunta manuale di contesto e deve essere visualizzata come tale. Con N partecipanti ci sono 7 + 4N campi mappa documentata: 8+4k traccia, 9+4k percorso, 10+4k xpub e 11+4k ID chiave, per k a partire da zero. Con N=2, il punto 15 è l'ID della seconda chiave e può essere confrontato per primo.

Esercitazione

1. Usa i dati sintetici e confronta prima un ID registrato come punto 15; poi rete e soglia.
2. Inserisci una discrepanza di un carattere. Controlla "Non corrisponde" e inizia un'altra coppia senza trascinare il risultato.
3. Confronta il testo con il testo ·2 / 3 · e spiega perché non è sempre possibile sapere se è una soglia o una posizione dell'utente.

Dimostra cosa hai imparato

Puoi descrivere quale campo hai controllato, come l'hai contestualizzato e cosa resta da approvare. Non trasformare le coincidenze parziali in approvazione globale.

Domanda frequente

Devo scansionare tutti i QR per continuare a imparare? No. Il confronto è libero. Le revisioni e le autorizzazioni obbligatorie del firmatario conservano il proprio flusso.

Punto di pausa

Chiude il confronto; i valori devono essere cancellati quando vengono fuori o passati in background secondo il disegno rivisto.

Mirror confronta due QR del passaggio 15 e indica una corrispondenza. Cosa attesta?

1. L'uguaglianza letterale degli elementi di quella coppia, nel contesto individuato o indicato.
2. L'approvazione di tutta la politica.
3. L'autenticazione dell'origine di entrambi i QR.

> **Mostra risposta: L'uguaglianza letterale degli elementi di quella coppia, nel contesto individuato o indicato.**
> Il confronto non sostituisce l'autenticazione, la verifica complessiva o la risposta dell'hardware.

Coordinare le firme e pubblicare una transazione multifirma

Obiettivo

Portare una proposta alla soglia delle firme senza perdere intenzione o controllo.

Comprendere

Un'operazione multifirma specifica voci, destinatari, importi, tariffe, sostituzioni e note operative. Il creatore può richiedere firme a partecipanti compatibili. Ogni firmatario controlla per conto proprio rete, politica, ingressi, tutte le uscite e commissioni prima di autorizzare sul proprio dispositivo.

Una firma parziale non muove fondi da sola se manca la soglia. Quando viene raggiunto, il coordinatore può combinare e terminare in base al flusso. Le relazioni di altri partecipanti o del coordinatore sono informazioni di coordinamento, non una verifica locale che tu hai fatto. L'app deve distinguere queste origini.

L'implementazione di riferimento consente un nuovo tentativo, la ricezione della firma, la conferma di ricezione, il rifiuto e il trasferimento del coordinamento. Un trasferimento non cambia le chiavi o la soglia della catena. Una risposta salvata deve essere correlata alla richiesta e al profilo effettivo utilizzato; non si sceglie un'altra politica perché simile o come prima nel catalogo.

Se qualcuno modifica destinatari o condizioni pertinenti, è necessario rivedere una nuova proposta e ottenere le firme corrispondenti. Non riparare a mano una PSBT eliminando i dati di sicurezza per farla entrare in NFC. I firmware richiedono il profilo e le validazioni compatibili, con limiti di ingressi, uscite e dimensioni.

Prima di pubblicare, verifica che l'operazione sia quella concordata e che non esista una versione già diffusa. Poi continua a confermare la fonte scelta. Rifiuta la tua app non revoca automaticamente le firme che altri hanno già conservato o impedito qualsiasi azione compatibile con la soglia restante.

Esercitazione

1. Rappresenta una politica 2 su 3 con tre ruoli fittizi. Uno firma, uno respinge e il terzo chiede chiarimenti.
2. Cambia l'indirizzo del pagamento di prova e spiega perché non viene riutilizzata una precedente approvazione verbale.

3. Simula un errore nella conferma di ricezione dopo il salvataggio della firma. Recupera lo stesso lavoro, senza raddoppiare il pagamento o modificare il profilo.

Dimostra cosa hai imparato

Puoi indicare chi coordina, chi firma, chi termina e quale prova esiste in ogni fase.

Domanda frequente

Due OK della chat corrispondono a due firme? No. La soglia è soddisfatta con autorizzazioni criptografiche valide sotto la politica, non con messaggi.

Punto di pausa

Registra stato, firme pendenti e successivo responsabile senza contenuti privati.

Un'operazione 2 su 3 ha una firma valida e due messaggi che dicono «d'accordo». È raggiunta la soglia?

1. Sì, perché ci sono tre partecipanti.
2. No. Manca un'altra firma crittografica valida.
3. Sì, se lo annuncia il coordinatore.

> **Mostra risposta: No. Manca un'altra firma crittografica valida.**
> Il consenso espresso in una conversazione e una firma valida sono prove diverse.

Recuperare e modificare un wallet multifirma

Obiettivo

Recuperare la politica e pianificare la perdita o la sostituzione dei partecipanti.

Comprendere

Il recupero ha bisogno di due categorie: dati che ricostruiscono la politica e capacità private sufficienti per spendere. Una copia politica con xpubs può rivelare la cronologia senza includere le frasi seed. Una copia crittografata aggiunge protezione al file, ma richiede di mantenere la password. L'estensione.cuvexms non dimostra da sola che è crittografata: il formato e la sua esportazione specifica devono essere controllati.

In Desk 9.21 il recupero richiede la chiave pubblica estesa del partecipante con traccia e rotta BIP48 esportata dal dispositivo. Supporta la lettura tramite webcam o Mirror del flusso compatibile. Non sostituire tale apporto con un indirizzo di ricezione o inviare il seed al supporto.

Se si perde una chiave in una 2 di 3, le altre due possono mantenere la capacità di spesa. La politica precedente rimane la stessa; per ritirare efficacemente un partecipante e stabilire altre chiavi, di solito viene creata una nuova politica e vengono trasferiti fondi con le necessarie autorizzazioni. Cambiare un alias o rimuovere un wallet da Desk non modifica UTXOs esistenti.

I backup devono permettere di ricostruire entrambi i rami e individuare la cronologia. Conserva indici, richieste emesse e il contesto necessario per non riutilizzare indirizzi o interpretare un portafoglio vuoto con una scansione incompleta. Ripristinare e riprendere un'operazione in sospeso deve rispettare il profilo salvato durante la creazione.

Esercitazione

1. Esporta e ripristina una politica di laboratorio attraverso la funzione documentata. Controlla rete e indirizzo noto.
2. Simula la perdita di un partecipante e prepara un piano di rotazione, senza spostare fondi reali.
3. Fa finta di perdere al di sotto della soglia. Riconosce che supporto o IA non possono fabbricare le firme mancanti.

Dimostra cosa hai imparato

È possibile recuperare lo scenario di prova e distinguere ripristinare le informazioni di cambiare controllo sulle monete.

Domanda frequente

Eliminare la multifirma in Desk disattiva il portafoglio per tutti? No. Elimina lo stato locale in base al flusso. Altre persone e copie possono continuare a mantenere la capacità compatibile con la politica.

Punto di pausa

Conserva copia provata e piano privato; registra nel corso solo il risultato.

Vuoi rimuovere una persona da una politica che ha già ricevuto fondi. Basta cancellarne il nome in Desk?

1. Sì.
2. Sì, se si elimina anche la chat.
3. No. Occorre pianificare una nuova politica e, quando necessario, lo spostamento autorizzato dei fondi.

> **Mostra risposta: No. Occorre pianificare una nuova politica e, quando necessario, lo spostamento autorizzato dei fondi.**
> Gli script degli UTXO esistenti non cambiano modificando registri locali.

M10

Aggiornare il firmware senza improvvisare

Obiettivo

Preparare un aggiornamento compatibile e verificarne il risultato sul dispositivo.

Comprendere

Un aggiornamento cambia software di fiducia. Verifica modello, revisione hardware, versione, provenienza e meccanismo di autenticazione del produttore. Un download completo o un hash uguale a quello di una pagina non sostituiscono la verifica della firma e della compatibilità. Non installare mai un'applicazione firmware senza firma destinata all'ingegnere come se fosse una pubblicazione per i clienti.

Original aggiorna per Bluetooth nel flusso documentato. BIT utilizza USB-C. Mirror include percorsi di preparazione e trasporto compatibili. Non si promette che una combinazione specifica di PC, telefono e dispositivo funzioni fino a completarne l'accettazione fisica. L'incidenza storica dell'aggiornamento di Original su Windows richiede una diagnosi specifica; non si risolve fingendo un successo a 99 %.

Prima di iniziare, controlla backup recuperabili, alimentazione stabile e assenza di altre operazioni. Prepara il file ufficiale o la copia precedentemente verificata in base all'app. Durante l'invio, differenza trasferimento, convalida, installazione, riavvio e controllo versione. Il bar non e' una prova finale.

Alla fine, controlla la versione visibile sul computer e registra la data e il risultato. Il catalogo di compatibilità di Desk non misura da remoto il firmware: firmwareAttestation rimane impostato su false. Selezionare un profilo Finale non accredita quale byte sono realmente installati. Se l'aggiornamento non riesce, segui la procedura di recupero documentata e annota la fase e l'errore. Non scollegare alla cieca il dispositivo in una fase critica.

Esercitazione

1. Controlla un elenco di preparazione senza avviare un aggiornamento reale durante la prova.
2. Ordina gli stati e spiega perché il trasferimento di termini e di installazioni è diverso.
3. Invia un report fittizio di bug al 99 % con modello, versione, sistema, fase e messaggio finale.

Dimostra cosa hai imparato

Puoi identificare l'artefatto giusto, il trasporto e il criterio finale di successo.

Domanda frequente

Devo aggiornare solo per far sparire un errore da Desk? Prima identifica l'origine. Un'incompatibilità del catalogo può richiedere la correzione di Desk e la conservazione del firmware convalidato.

Punto di pausa

Un aggiornamento reale si ferma solo in uno stato espressamente sicuro della procedura, non per raggiungere la fine della chiamata.

Cosa verifica da solo il catalogo esplicito di Desk?

1. I riferimenti di compatibilità supportati, senza misurare da remoto il firmware installato.
2. L'attestazione fisica di tutti i dispositivi connessi.
3. L'assenza di vulnerabilità.

> **Mostra risposta: I riferimenti di compatibilità supportati, senza misurare da remoto il firmware installato.**
> Compatibilità, firma, misurazione e accettazione fisica sono prove diverse.

Perdita, guasto e recupero di emergenza

Obiettivo

Scegliere un recupero proporzionale all'incidente e preservare prove utili.

Comprendere

In caso di incidente, classifica anzitutto ciò che è stato perso o esposto: computer, dispositivo, carta, file, password, frase seed, passphrase o politica. Non riesco ad entrare, non significa necessariamente che mi abbiano rubato. Se sospetti che un dispositivo sia compromesso, smetti di inserirvi segreti.

La perdita del dispositivo può essere risolta con supporti e credenziali di recupero compatibili. La perdita del computer può richiedere di ripristinare il deposito di Desk e ricostruire l'osservazione. Perdere tutti i mezzi di sblocco o tutte le chiavi necessarie al di sotto della soglia potrebbe non avere soluzione tecnica. Nessuna IA può garantire il salvataggio di chiavi inesistenti.

Desk include un recupero locale per i formati supportati ed esportazione del materiale di recupero corrispondente. Decifrare sul PC può esporre il segreto al sistema operativo o malware. È una decisione eccezionale: utilizza un ambiente preparato, materiale compatibile e un piano di trasferimento a nuove chiavi se il segreto potrebbe essere compromesso. Non descriverlo come un'operazione equivalente al solito isolamento di Cuvex.

Se un seed è stato diffuso, cambiare la password di Desk non revoca quel seed. È necessario valutare il trasferimento autorizzato in un nuovo portafoglio e proteggerlo da un team affidabile. Evita di pubblicare dettagli sull'incidente che aiutano l'aggressore o di pagare servizi che promettono il recupero in cambio di altri frasi seed o anticipi fraudolenti.

Esercitazione

1. Risolvi quattro scenari fittizi: PC perso, carta danneggiata con copia valida, password dimenticata e frase seed esposta.
2. Per ciascuna di esse, identifica materiale necessario, rischio di agire e criterio di recupero.
3. Prova la procedura solo con i dati di apprendimento; non caricare al tutor file di emergenza reali.

Dimostra cosa hai imparato

Puoi scegliere tra ripristinare, riconfigurare l'osservazione, migrare il controllo o scalare uno specialista senza affermare soluzioni impossibili.

Domanda frequente

Cambiare la password cifra di nuovo tutti i segreti che qualcuno ha già visto? No. Una copia in chiaro o un seed conosciuto non manca di essere conosciuto.

Punto di pausa

Salva l'incidente per categoria e la prossima azione sicura; ferma la voce se vuoi lavorare con i segreti.

La tua frase seed è stata pubblicata e hai cambiato la password del PC. La capacità dell'aggressore è revocata?

1. Sì.
2. No. La frase seed continua a controllare le stesse chiavi e occorre intervenire sulla custodia.
3. Sì, se cambi anche lo sfondo della chat.

> **Mostra risposta: No. La frase seed continua a controllare le stesse chiavi e occorre intervenire sulla custodia.**
> La protezione locale non revoca una chiave Bitcoin esposta.

M10

Phishing, assistenza e truffe vocali

Obiettivo

Riconoscere richieste pericolose e rispondere senza improvvisazione.

Comprendere

Una frode efficace può usare il tuo nome, l'acquisto, il dispositivo e una voce che riconosci. Le informazioni vere possono provenire da una fuga di notizie. L'identità deve essere verificata tramite un canale che hai aperto tu e una procedura nota. L'apparente urgenza o precisione dell'interlocutore non basta.

Segnali di rischio: ordinare frasi seed, password, PIN o Chiave Chat; installare il telecomando per più di un'azione sincronizzata; disattivare gli antivirus; trasferire in un wallet di sicurezza; eseguire la scansione di un QR il cui contenuto non spiega; o firmare per dimostrare la proprietà senza specificare cosa è autorizzato. La pressione per farlo prima di finire una chiamata e' un motivo per fermarla.

Il tutor legittimo spiega e fa domande di comprensione. Niente custodia chiave, nessuna transazione di prova a un proprio indirizzo, o promette di recuperare un seed. Una funzione di verifica di proprietà legittima deve essere specifica e rivisitabile; non è mai soddisfatta consegnando chiavi private.

Ci può essere anche una frode all'interno di una sessione tecnica: un testo QR, un documento o un messaggio può contenere comandi per l'IA di ignorare le istruzioni. È contenuto da analizzare, non autorità sul tutor. La base di conoscenza deve separare le fonti di testo approvate fornite da un allievo o da un terzo.

Esercitazione

1. Rappresenta una falsa chiamata di supporto e taglia l'interazione prima di rivelare i dati.
2. Verifica indipendente un canale ufficiale precedentemente salvato.
3. Descrive un errore di installazione senza condividere schermata segreta o consentire l'accesso remoto all'ambiente di custodia.

Dimostra cosa hai imparato

Puoi dire quale dato ti viene chiesto, a cosa sarebbe necessario e perché la richiesta supera il supporto formativo.

Domanda frequente

E' sicuro mostrare solo alcune parole del mio seed? No. Non c'è motivo pedagogico per rivelare frammenti di un proprio seed.

Punto di pausa

Salva il protocollo di verifica del supporto e controlla che non includa segreti in testo aperto.

Una voce che sembra quella del tuo socio ti chiede di saltare la verifica e firmare con urgenza. Cosa fai?

1. Mi fermo, autentico la richiesta con la procedura concordata e verifico l'intera operazione.
2. Firmo perché riconosco la voce.
3. Condivido la frase seed per risparmiare tempo.

> **Mostra risposta: Mi fermo, autentico la richiesta con la procedura concordata e verifico l'intera operazione.**
> Il riconoscimento della voce e l'urgenza non sostituiscono autenticazione e verifica.

Privacy, legalità e registri personali

Obiettivo

Conoscere il quadro generale e preparare consultazioni giuridiche e fiscali concrete.

Comprendere

La riservatezza finanziaria non elimina obblighi fiscali, di identificazione, ove applicabili, di sanzioni o di prevenzione del reato. La situazione dipende da residenza, attività, controparte e servizio. L'IA dovrebbe fornire informazioni generali con fonte e data e condurre decisioni particolari a professionisti competenti.

Nell'UE, la MiCA regola alcuni criptoattivi e servizi. La sua applicazione generale ha avuto inizio il 30 dicembre 2024 e il regime transitorio massimo indicato nel regolamento è arrivato al 1 luglio 2026, soggetto a decisioni nazionali. Controlla l'autorizzazione e la portata nei registri ufficiali esistenti; non basta una vecchia menzione di registrazione. L'autorizzazione non garantisce prezzo, solvibilità o compensazione totale.

Il regolamento 2023/1113 prevede informazioni che accompagnano i trasferimenti quando intervengono fornitori obbligati. Per trasferimenti superiori a 1.000 euro con indirizzi auto-custodiati, sono previste misure per valutare la proprietà o il controllo. Tale soglia non crea un'esenzione generale dall'identificazione al di sotto. I trasferimenti tra persone senza fornitore sono esclusi da tale regolamento; vi sono ancora altri obblighi.

Conserva una documentazione sufficiente di acquisti, vendite, commissioni e origine a seconda del tuo caso, protetta da accessi non necessari. Non c'e' bisogno di pubblicare la cronologia completa per tenere i registri privati. Non si insegna neppure la frammentazione delle operazioni per eludere controlli, falsare informazioni o nascondere redditi.

In caso di registrazione o trascrizione vocale e progresso identificabile, il servizio dovrebbe definire finalità, base giuridica, conservazione, accesso, responsabili e diritti applicabili. Le impostazioni della privacy commerciale vengono convalidate prima di vendere, non si improvvisa durante una chiamata.

Esercitazione

1. Prepara per un consulente un caso fittizio indicando residenza, attività e operazioni, senza includere chiavi.
2. Verifica dove verificare l'autorizzazione del fornitore e la data delle informazioni.
3. Progetta un registro privato dei movimenti e una politica minima dei dati dello studente.

Dimostra cosa hai imparato

Puoi distinguere una regola giuridica, una politica di exchange e una capacità tecnica di Bitcoin.

Domanda frequente

Tutte le autocustodie sono vietate nell'UE? Non si può dedurre questo dalle norme citate. Evita i titolari assoluti e verifica la specifica disposizione e la sua portata.

Punto di pausa

Salva questioni in sospeso per il tuo consulente senza inserire documenti personali nel tutor.

La soglia di 1.000 euro citata per determinate misure di verifica del controllo dell'indirizzo elimina tutti gli obblighi al di sotto di tale importo?

1. Sì.
2. Solo se suddividi l'operazione.
3. No. Non è un'esenzione generale dall'identificazione o da altri obblighi.

> **Mostra risposta: No. Non è un'esenzione generale dall'identificazione o da altri obblighi.**
> La norma va interpretata secondo la misura prevista e il suo ambito, senza trasformare una soglia in un'esenzione universale.

Eredità, continuità e simulazione annuale

Obiettivo

Creare un piano che consenta di agire a persone autorizzate senza esporre tutto in anticipo.

Comprendere

L'eredità combina legittimità giuridica, localizzazione dei materiali e capacità tecnica. Una persona può avere il diritto di ereditare e non saper ricostruire un wallet; un'altra può avere una chiave e non avere l'autorizzazione ad usarla. Il piano deve risolvere entrambe le dimensioni con una consulenza adeguata.

Separa le istruzioni pubbliche per l'accesso ai segreti. L'inventario descrive che cosa esiste, a chi contattare e quali controlli fare, senza mettere tutte le chiavi e le password insieme in un documento ampiamente accessibile. Evita di pubblicare frasi seed in testamenti o file che possano circolare al di fuori del tuo controllo.

In multifirma progetta chi conserva la politica e le copie, quale soglia è disponibile dopo una perdita e cosa succede se una persona chiave muore. Uno stesso custode che conserva abbastanza componenti può diventare un punto unico di abuso. Una distribuzione troppo complessa può rendere irrecuperabile il patrimonio.

Prevedi il recupero delle password del crittogramma e dell'eventuale passphrase, i dati di derivazione, la compatibilità dei dispositivi e la procedura da seguire se il produttore cessa l'attività. Non presumere che un file proprietario o un'impronta biometrica siano utilizzabili senza preparazione. L'interoperabilità deve essere provata con dati di prova e formati documentati.

Controlla dopo cambiamenti familiari, di domicilio, di politica, di software o di partecipanti e fa un'esercitazione periodica. L'esercizio deve dimostrare che una persona di fiducia capisce le istruzioni senza rivelare il patrimonio o spostare denaro inutilmente.

Esercitazione

1. Completa un modello privato con responsabili, componenti, accesso autorizzato e sostituti.
2. Da istruzioni di laboratorio a qualcun altro senza spiegarle oralmente e osserva dove si blocca.

3. Corregge le ambiguità e registra una data di revisione. Il corso non crea automaticamente promemoria.

Dimostra cosa hai imparato

Puoi spiegare cosa succede se non sei disponibile e quali informazioni hanno bisogno di ogni ruolo in ogni fase.

Domanda frequente

Una 2 su 3 sostituisce un piano ereditario? No. E' uno strumento tecnico. Gli eredi hanno ancora bisogno di contesto, materiali, coordinamento e legittimità.

Punto di pausa

Salva il piano fuori dal corso e segna solo il simbolo "simulacro" rivisto.

Qual è un criterio utile per valutare un piano successorio?

1. Che una persona autorizzata riesca a svolgere una simulazione documentata senza improvvisare né ricevere segreti prematuramente.
2. Che abbia molte pagine.
3. Che dipenda unicamente dal ricordare una password.

> **Mostra risposta: Che una persona autorizzata riesca a svolgere una simulazione documentata senza improvvisare né ricevere segreti prematuramente.**
> La possibilità di recupero e il controllo degli accessi devono essere provati nella pratica.

M11

Prezzo, risparmio e analisi fondamentale

Obiettivo

Analizzare gli argomenti d'investimento senza confonderli con proprietà tecniche verificabili.

Comprendere

Prezzo è il risultato di scambi su mercati specifici e può differire tra piattaforme. Liquidità, valuta di quotazione, profondità, orario dei fornitori bancari e domanda influenzano il risultato che puoi eseguire. Una citazione sullo schermo non è un'offerta garantita per il tuo volume.

L'analisi fondamentale esamina fattori quali adozione, domanda, concorrenza, sicurezza economica, regolamentazione e offerta. Un calendario di emissione noto non determina di per sé il prezzo futuro. Le valutazioni sull'utilità monetaria o sul valore intrinseco di un'impresa dipendono da ipotesi; non esiste una cifra oggettiva che l'IA possa presentare come certezza universale.

Una strategia di acquisto regolare distribuisce il momento dell'ingresso, ma non garantisce profitti né evita perdite prolungate. Il risparmio a lungo termine richiede anche liquidità per le obbligazioni, tolleranza alla volatilità e un piano di custodia. Il corso non prescrive una quota del tuo patrimonio e non prende decisioni al posto tuo.

Separa tre domande: capisco la risorsa?, posso custodirla e recuperarla?, posso correre il suo rischio economico? Il dominio delle chiavi non risponde automaticamente alla terza. La formazione non trasforma una proiezione di prezzo o un grafico storico in una raccomandazione personalizzata.

Esercitazione

1. Scrivi una tesi fittizia, i suoi presupposti e i fatti che la invaliderebbero.
2. Simula un calo del 50 % e bisogni di liquidità simultanei, senza introdurre il tuo patrimonio reale.
3. Identifica quali dati dell'argomento sono verificabili e quali sono le aspettative.

Dimostra cosa hai imparato

Puoi discutere di investimenti senza promettere redditività o confondere convinzione con le prove.

Domanda frequente

La scarsità assicura che il prezzo aumenti? No. La domanda e le altre condizioni restano determinanti per il prezzo di mercato.

Punto di pausa

Salva ipotesi di laboratorio, non un'istruzione automatica di acquisto.

Cosa garantisce un acquisto periodico?

1. Un guadagno a lungo termine.
2. Nessun rendimento. Distribuisce i momenti di acquisto secondo una regola scelta.
3. Protezione contro la perdita delle chiavi.

> **Mostra risposta: Nessun rendimento. Distribuisce i momenti di acquisto secondo una regola scelta.**
> Distribuire gli ingressi sul mercato non elimina il rischio economico od operativo.

M11

Scegliere dove acquistare bitcoin

Obiettivo

Valutare un fornitore per autorizzazione, costo, ritiro, privacy e rischio di custodia.

Comprendere

Confronta fornitori con criteri verificabili: soggetto giuridico e giurisdizione, servizi autorizzati, rete di ritiro, commissioni, differenziale di prezzo, limiti, supporto, autenticazione e trattamento dei dati. La denominazione commerciale o una sponsorizzazione non dimostrano l'autorizzazione per il servizio specifico.

Il costo totale può comprendere depositi, conversione, spread, commissione di negoziazione, ritiro e costo bancario. Un'operazione «senza commissioni» può avere un differenziale di prezzo più elevato. Controlla gli importi netti e la valuta di riferimento. Il budget dovrebbe includere il ritiro di auto-custodia quando questo è il tuo obiettivo.

Mentre tieni un saldo di custodia, dipende dal fornitore. Una prova di riserva non dimostra da sola tutte le passività, la proprietà di fondi o la solvibilità futura. Controlla le restrizioni e fai un piccolo prelievo che puoi permetterti prima di dipendere da un nuovo flusso.

L'identificazione commerciale può associare la tua identità ad un ritiro. Proteggere tali informazioni successivamente non equivale a cancellare ciò che il fornitore conosce. Non falsificare i dati e non usare il corso per aggirare gli obblighi. L'acquisto di un codice di formazione genera anche un registro commerciale separato dal tuo wallet.

Esercitazione

1. Compila una matrice fittizia per due fornitori, indicando costo totale, rete, prelievo minimo, autorizzazione e dati richiesti.
2. Calcola il netto per un'operazione di apprendimento con tutte le spese specificate.
3. Progetta un ritiro di prova ad un indirizzo precedentemente verificato, non eseguito da questo minisite.

Dimostra cosa hai imparato

Puoi giustificare una scelta per il tuo caso e riconoscere quali informazioni sono decadute o non verificate.

Domanda frequente

Il corso raccomanda un exchange come il migliore per tutti? No. I permessi, le tariffe, i paesi curati e le condizioni cambiano. Il confronto richiede data e caso di utilizzo.

Punto di pausa

Salva la matrice senza credenziali o documenti di identificazione.

Quale confronto è più utile che considerare solo la commissione di negoziazione?

1. Il costo totale fino alla ricezione di BTC sulla rete e all'indirizzo desiderati.
2. Il numero di follower del fornitore.
3. Il colore dell'applicazione.

> **Mostra risposta: Il costo totale fino alla ricezione di BTC sulla rete e all'indirizzo desiderati.**
> Il prezzo finale include voci che possono non comparire nella commissione pubblicizzata.

M11

Conti, ordini e costi di esecuzione

Obiettivo

Capire i comandi di base e proteggere l'account senza trasformare il corso in un terminale di trading.

Comprendere

Un ordine di mercato priorità esecuzione disponibile, con il rischio di scivolare. Un ordine limitato fissa un prezzo massimo di acquisto o minimo di vendita, ma può non essere eseguito o parzialmente eseguito. Un ordine stop attiva un'altra azione secondo le regole del fornitore; non garantisce da sola il prezzo finale.

Il libretto degli ordini mostra offerte disponibili, non impegni che tutti i volumi rimarranno. In una caduta o in una bassa liquidità, il risultato può differire dall'ultima quotazione. Gli ordini stop-market e stop-limit hanno rischi diversi: esecuzione a prezzo peggiore rispetto a possibile non esecuzione.

Protegge l'accesso con password unica, l'autenticazione resistente a phishing quando supportata, la revisione delle sessioni e i controlli di rimozione appropriati. Salva il recupero del secondo fattore in modo indipendente. Una chiave API per automatizzare può avere permessi più pericolosi di quelli che richiedono una lettura dei dati; non inserire la chiave nel tutor o nel minisite.

Prima di ritirare, verificare attivo e rete Bitcoin, indirizzo del portafoglio e importi netti. Una piattaforma può utilizzare gli stessi simboli per prodotti diversi. Alla fine, conserva la documentazione di acquisto, esecuzione, commissioni e ritiro secondo il tuo caso; non confondere il ritiro nel tuo portafoglio con un nuovo acquisto.

Esercitazione

1. Simula un libro fittizio con 1 unità a 100 e un altro a 102. Spiega perché comprare due sul mercato non garantisce un prezzo medio di 100.
2. Progetta un ordine limitato e descrive lo scenario in cui non è completato.
3. Verifica le autorizzazioni di un'API fittizia e rimuovi quella di prelievo se serve soltanto consultare dati.

Dimostra cosa hai imparato

Puoi descrivere priorità, prezzo e rischio di non esecuzione per ogni ordine.

Domanda frequente

Uno stop-loss limita sempre la perdita esattamente? No. Gaps, liquidità, scivolamento e regole del fornitore possono impedirlo.

Punto di pausa

Salva il risultato dell'esercizio senza comandi reali o chiavi API.

Quale rischio rimane con un ordine limite di acquisto a 100?

1. Che non venga mai eseguito o che venga eseguito solo in parte.
2. Che debba essere eseguito a qualsiasi prezzo.
3. Che crei automaticamente una copia di sicurezza.

> **Mostra risposta: Che non venga mai eseguito o che venga eseguito solo in parte.**
> Il controllo del prezzo comporta il rischio di mancata esecuzione.

M11

Candele, indicatori e distorsioni dell'analisi tecnica

Obiettivo

Leggere grafici come dati storici e valutare una strategia senza confondere schemi con previsioni.

Comprendere

Una candela riassume apertura, massima, minima e chiusura di un periodo. Il volume dipende dalla fonte. Cambiare piattaforma, moneta, fuso orario o periodo può cambiare quello che vedi. Una candela non mostra tutto l'ordine temporale dei movimenti entro il suo intervallo.

Una media mobile ammorbidisce i prezzi passati. Un indicatore di momento trasforma i dati osservati in una formula. Nessuno conosce il futuro. Due indicatori derivati dalla stessa serie possono fornire informazioni molto correlate, anche se i loro colori e nomi sono diversi.

Per valutare una regola definisce l'ingresso, l'uscita, l'invalidità, i costi, le dimensioni e i dati prima di guardare il risultato. Evita di selezionare solo gli esempi vincenti, di regolare i parametri fino a quando non si adattano o utilizzare i dati futuri in una decisione passata. Distingue dati di addestramento e convalida temporanea.

Un backtest dovrebbe considerare spread, commissioni, scorrimento, disponibilità di dati ed esecuzione possibile. Redditività lorda, tasso di successo, perdita massima e distribuzione delle perdite rispondono a domande diverse. Un sistema con molti successi può perdere denaro se i suoi fallimenti sono grandi. Non si mostra un segnale di acquisto o di vendita come certezza.

Esercitazione

1. Leggi una candela finta e spiega quali informazioni temporali non contengono.
2. Scrivi una regola prima di valutare dieci risultati sintetici, con costi e criteri di guasto.
3. Confronta 9 guadagni di 1 con una perdita di 15: il risultato lordo è -6 nonostante il 90 % di successo.

Dimostra cosa hai imparato

Puoi criticare un risultato interessante per selezione, costi o rischi senza dover eseguire operazioni.

Domanda frequente

La combinazione di molti indicatori garantisce un segnale migliore? No. Può aumentare l'adeguamento e la complessità senza fornire informazioni indipendenti.

Punto di pausa

Salva la regola e i risultati di laboratorio, non un ordine di mercato.

Nove operazioni guadagnano 1 ciascuna e una perde 15. Qual è il risultato al lordo dei costi?

1. +90 %.
2. +6.
3. −6.

> **Mostra risposta: −6.**
> Nove unità guadagnate meno quindici perse equivalgono a una perdita di sei.

M11

Margine, futures e automazione

Obiettivo

Riconoscere esposizione, regolamento e automazione prima di considerare prodotti complessi.

Comprendere

La leva aumenta l'esposizione rispetto al capitale investito. In un esempio semplificato, 100 margini per un'esposizione di 1.000 significa che un movimento negativo del 5 % del sottostante equivale a 50 prima dei costi: metà del margine iniziale. Le reali regole di manutenzione, liquidazione, garanzie e commissioni possono peggiorare il risultato e attivarsi prima del previsto.

I futuri e perpetui possono includere scadenza, regolamento per differenze, tassi di finanziamento e prezzi di riferimento diversi dall'ultimo scambio. Non sono equivalenti a rimuovere bitcoin nativo a Cuvex. Custodire un seed non protegge una posizione da liquidazione o fallimento della controparte.

Un bot automatizza le regole, compresi i suoi errori. Ha bisogno di limiti di posizione, permessi minimi, idempotenza degli ordini, riconciliazione, controllo delle perdite, interruzione di emergenza e supervisione. Duplicare una richiesta dopo un timeout può raddoppiare un'esposizione se il risultato precedente non è noto.

L'IA può spiegare concetti e rilevare incongruenze in un caso fittizio. Non devi ricevere chiavi API, attivare trading o promettere una strategia redditizia. Per l'obiettivo principale di questo corso, comprendere questi rischi permette di decidere di non utilizzare prodotti che non si capiscono.

Esercitazione

1. Risolvi l'esempio di esposizione e margine senza supporre che il livello di liquidazione sia esattamente del 10 %.
2. Simula un'API che esegue un comando ma perde la risposta. Spiega perche' prima di ripetere, devi riconciliarti.
3. Progetta un pulsante di arresto che impedisce nuovi comandi e controlla quelli già aperti, senza collegarsi a un broker.

Dimostra cosa hai imparato

Puoi descrivere un rischio che sopravvive allo stop, un altro che sopravvive al bot e un altro che sopravvive all'autocustodia di fondi esterni.

Domanda frequente

Automatizzare elimina emozioni e quindi garantisce risultati? No. È possibile ridurre un intervento impulsivo e moltiplicare errori di progettazione o esecuzione.

Punto di pausa

Segna questa estensione come compresa senza abilitare prodotti complessi.

Con un'esposizione di 1.000 e un margine di 100, a quanto equivale una perdita del 5 % sull'esposizione, prima dei costi?

1. Una perdita di 5.
2. Una perdita di 50, pari al 50 % del margine.
3. Nessuna perdita se si usa un bot.

> **Mostra risposta: Una perdita di 50, pari al 50 % del margine.**
> La leva e i costi fanno sì che il risultato sul margine differisca dalla variazione dell'asset.

M12

Lightning e altri livelli

Obiettivo

Capire i pagamenti per canali e riconoscere quali funzioni non offre il flusso Cuvex rivisto.

Comprendere

Lightning utilizza canali e meccanismi di aggiornamento per effettuare pagamenti senza registrare ogni singolo scambio nella catena base. Aprire o chiudere canali e alcuni scenari di recupero possono comportare transazioni on-chain. La disponibilità, la liquidità in entrata e in uscita e la sorveglianza dipendono dalla progettazione del wallet e dai servizi utilizzati.

Un'invoice può includere l'importo, la descrizione e la scadenza. L'unità può essere espressa in satoshis o millisatoshis secondo il contesto, senza che questi ultimi comportino uscite sub-satoshi nella catena base. Pagare una fattura richiede compatibilità e percorso disponibili; un QR non garantisce che possa essere pagato con qualsiasi app.

Ci sono servizi di custodia e non custodi con modelli molto diversi. La velocità usuale non dimostra l'assenza di rischi. Lightning non deve essere presentato come anonimo completo: ci sono osservatori, percorsi, controparti e metadati pertinenti.

La chat di Cuvex può coordinare le richieste di sats che vengono pagate per conto WOW a catena. Questa edizione non attribuisce a Desk un nodo Lightning, gestione dei canali o firma di invoices Lightning. Se una richiesta include diverse modalità, controlla quale intendi e quale eseguirà la tua applicazione.

Esercitazione

1. Classifica un indirizzo on-chain, un URI bitcoin: e una invoice Lightning didattiche.
2. Confronta pagare per catena e per canale in termini di conferma, liquidità, custodia e recupero.
3. Spiega perché un'invoice decaduta deve essere rivista con il ricevitore e non reinterpretata come direzione.

Dimostra cosa hai imparato

Puoi rifiutare una modalità incompatibile senza esporre le chiavi o attribuire un errore a Cuvex.

Domanda frequente

Tutti i pagamenti in sats sono Lightning? No. I satoshi esprimono valore; la modalità dipende dal protocollo utilizzato.

Punto di pausa

Salva la modalità dell'esercizio, senza bollette reali.

Quale informazione permette di capire che una richiesta va pagata tramite Lightning?

1. L'uso della parola sats.
2. Il fatto che arrivi via chat.
3. Il formato e la modalità compatibili, oltre alla semplice unità o al canale del messaggio.

> **Mostra risposta: Il formato e la modalità compatibili, oltre alla semplice unità o al canale del messaggio.**
> L'unità di conto e la rete di pagamento sono aspetti distinti.

Taproot, MuSig2 e il futuro post-quantistico

Obiettivo

Distinguere standard, proposte e capacità implementate.

Comprendere

Taproot consente condizioni di spesa con percorsi chiave e script. Le firme Schnorr e l'aggregazione possono migliorare alcune costruzioni, ma il risultato della privacy dipende da come viene configurato e speso. Che un indirizzo sia bc1p non dimostra che non ci siano altri partecipanti né rivela tutte le loro condizioni nascoste.

MuSig2 consente a un insieme di firmatari di aggiungere chiavi e produrre una firma Schnorr compatibile con l'interazione. Lo standard base è N di N. Una soglia arbitraria M di N richiede un'altra costruzione o protocollo aggiuntivo. La gestione dei nonces e delle sessioni è fondamentale e non si implementa con uno scambio informale di messaggi.

PSBT v2 riorganizza informazioni su v0; non è un aggiornamento automatico di qualsiasi file contenente una transazione di versione 2. I firmware Finali di questa edizione conservano PSBT v0, P2WSH/sortedmulti e SIGHASH_ALL per il profilo multifirma. Le future capacità richiedono un contratto e una convalida propri.

NIST ha pubblicato nel 2024 i suoi primi standard post-quantitativi completati. Questo non cambia di per sé le firme di Bitcoin. Usando un algoritmo post-quantico per autenticare il firmware proteggerebbe quel livello; non convertirebbe automaticamente ECDSA o Schnorr da un UTXO in firme post-quantitative. Né esiste una data di attacco futuro che il tutor possa promettere con certezza.

Esercitazione

1. Classifica cinque affermazioni come standard, implementazione verificata, proposta o pubblicità.
2. Spiega perche' Taproot non prova Taproot in arrivo.
3. Disegna strati separati: firma firmware, crittografia segreta, chat e firma di spesa Bitcoin.

Dimostra cosa hai imparato

Puoi richiedere prove specifiche di un livello ed evitare di trasferire garanzie tra protocolli.

Domanda frequente

Devo migrare i miei fondi per un titolo di calcolo quantistico? Una decisione reale richiede una prova tecnica attuale, un supporto verificabile, una valutazione dei rischi e un piano di migrazione sicuro; il corso non ordina movimenti per titolari.

Punto di pausa

Registra domande tecniche senza creare un piano di spesa automatico.

Una firma post-quantistica nel bootloader, se implementata e convalidata, cambia le condizioni di firma di un UTXO esistente?

1. No. Sono livelli distinti.
2. Sì. Fa passare tutta la rete a un altro algoritmo.
3. Elimina la necessità dei backup.

> **Mostra risposta: No. Sono livelli distinti.**
> Autenticare un aggiornamento non riscrive le condizioni di spesa di Bitcoin.

Interoperabilità e indipendenza dal produttore

Obiettivo

Pianificare la continuità se il software, il dispositivo o il fornitore cambiano.

Comprendere

L'interoperabilità non è verificata con un elenco di sigle. È necessario conservare rete, script, derivazione, chiavi, politica, formato di transazione e semantica delle firme. Due applicazioni possono comprendere BIP174 e, tuttavia, non supportare gli stessi campi, dimensioni o tipi di input.

Per uscire da una dipendenza di interfaccia, conserva informazioni di recupero documentate e prova con portafogli di apprendimento. Una mnemonica standard può consentire di derivarne le chiavi, ma recuperare una multifirma richiede la vostra politica completa. I tag BIP329 aggiungono un contesto di privacy; la cronologia della chat ha una portata diversa.

Non trasformare un test di compatibilità in esposizione di un seed reale. Prima controlla l'esportazione pubblica di descrittori e recupero watch-only. Se un'emergenza richiede la ricostruzione delle chiavi, utilizza un ambiente progettato per farlo e pensa di migrare dopo. Una wallet incompatibile che mostra zero non dimostra da sola che i fondi sono andati perduti.

Mantieni una copia verificabile di documentazione, versione del corso e strumenti necessari. La firma di applicazioni, certificati scaduti e modifiche di sistema possono influenzare l'installazione. Un open source non garantisce che chiunque possa compilarlo anni dopo senza conservare dipendenze e conoscenze.

Esercitazione

1. Progetta una prova di output con un account vuoto: stessa rete, politica e direzione di controllo in due implementazioni compatibili.
2. Indica quali componenti sono standard e quali richiedono un convertitore o la documentazione del formato Cuvex.
3. Definisce il risultato che permette di affermare la compatibilità e ciò che resta in attesa di hardware o firma reale.

Dimostra cosa hai imparato

Puoi descrivere un percorso di recupero senza dipendere dal fatto che un'azienda continui a offrire lo stesso servizio.

Domanda frequente

Codice aperto significa che il produttore non ha più importanza? No. Distribuzione, manutenzione, componenti fisici ed esperienza operativa continuano ad importare. Consente l'ispezione e la continuità potenziale, non una garanzia automatica.

Punto di pausa

Salva risultati di laboratorio con versioni e limiti osservati.

Qual è la prova più significativa di interoperabilità?

1. Che entrambe le app dicano «Bitcoin».
2. Ricostruire e verificare in laboratorio la stessa politica e lo stesso indirizzo con versioni identificate.
3. Che le icone si assomiglino.

> **Mostra risposta: Ricostruire e verificare in laboratorio la stessa politica e lo stesso indirizzo con versioni identificate.**
> La prova deve preservare le condizioni rilevanti e produrre un risultato verificabile.

M12

Laboratorio tecnico con regtest

Obiettivo

Capire un laboratorio riproduttore senza confondere prove sintetiche e uso fisico.

Comprendere

Regtest permette di creare una catena locale controllata per generare blocchi e provare transazioni prive di valore economico. È necessario utilizzare cartelle e credenziali separate, indipendentemente dal materiale reale. I suoi risultati non dimostrano da soli la compatibilità USB, NFC, Bluetooth o la fotocamera di un computer fisico.

Un laboratorio completo registra versioni, impostazioni di rete, politica, voci di prova, PSBT, firme, transazione finale e risultato di accettazione. Si può verificare che l'importo è isolato, che una firma modificata è respinta e che un pagamento valido entra in un blocco locale. La prova deve includere errori, non solo la strada giusta.

La convalida di Desk 9.21 riporta test con Bitcoin Core 31 regtest e test automatici del motore e UI simulato. Questa edizione le usa come prove documentarie, non sostiene di aver ripetuto quelle prove o di aver eseguito operazioni con dispositivi. Il controllo di un pacchetto non prova nemmeno la sua installazione su tutti i sistemi.

Prima di una classe tecnica, l'ingegnere deve fornire il laboratorio montato e la procedura compatibile con la versione dell'allievo. Non aprire la RPC a Internet per il tutor. L'IA può guidare l'interpretazione dei risultati sintetici, ma non deve ottenere credenziali o permessi di somministrazione.

Esercitazione

1. Con il laboratorio preparato, nota una transazione valida e una con una firma alterata. Registra accettazione o rifiuto.
2. Controlla un caso di cambiamento errato e un caso di rete incompatibile.
3. Separa nel tuo rapporto · prova del motore ·, · interfaccia simulata · e · hardware fisico ·.

Dimostra cosa hai imparato

Puoi descrivere esattamente ciò che è stato testato e ciò che resta da fare, senza presentare una simulazione come certificazione.

Domanda frequente

Se regtest funziona, posso vendere il corso come convalidato per tutti i dispositivi? No. Mancano prove di percorsi fisici, installazione, accessibilità, recupero e servizio commerciale.

Punto di pausa

Ferma e salva il laboratorio secondo le sue istruzioni, conservando solo dati sintetici.

Un test del motore su regtest dimostra l'effettiva lettura NFC su uno specifico telefono?

1. Sì, perché entrambi usano Bitcoin.
2. Sì, se la PSBT è piccola.
3. No. Occorre una prova fisica separata.

> **Mostra risposta: No. Occorre una prova fisica separata.**
> Gli ambienti di convalida hanno ambiti diversi.

Progetto finale e piano di continuità

Obiettivo

Dimostrare autonomia dalla preparazione al recupero e alla privacy.

Comprendere

Il risultato del corso non è memorizzare un menu: è potere spiegare l'intenzione, verificare il risultato e fermare un'operazione che non capisci. La valutazione combina concetti, pratica guidata e un caso indipendente. Non dipende mai dal rivelare le frasi seed, il patrimonio o gli indirizzi personali al valutatore.

Caso A: configura un ambiente di apprendimento, identifica modelli e versioni, protegge Desk, collega un crittogramma didattico e ricostruisce un account watch-only. Spiega quali backup sono necessari e quali dati possono essere osservati dal tuo fornitore.

Caso B: progetta un pagamento con UTXOs fittizi provenienti da contesti diversi. Giustifica la selezione, verifica destinatario, resto e commissione e descrivi il percorso di firma previsto per il tuo dispositivo. Risolvi un'interruzione di ritorno e un'altra di pubblicazione senza raddoppiare il pagamento. Se non c'è hardware fisicamente accettato, la parte viene registrata come simulata e in pendenza.

Caso C: progetta una 2 di 3, rappresenta invito e verifica, confronta in Mirror un campo scelto in ordine libero e spiega la portata dell'OK. Recupera la politica di apprendimento, simula la perdita di un partecipante e prepara continuità ed eredità.

Il superamento proposto richiede almeno 80 % di conoscenze e di tutti i controlli critici corretti: non rivelare segreti, controllare la rete e le uscite, non confondere le tappe e mantenere il recupero. Un errore critico richiede una revisione e una nuova pratica; non è compensato da domande di mercato. Un certificato commerciale, se rilasciato, deve indicare che cosa è stato valutato e se vi sono state osservazioni fisiche o solo simulazione.

Esercitazione

1. Completa tutti e tre i casi con dati sintetici e una spiegazione propria.
2. Risolvi la valutazione finale dell'allegato e controlla ogni risposta non riuscita.
3. Consegna solo un foglio di risultati senza segreti, con prove di portata e orecchini.

Dimostra cosa hai imparato

Puoi fermarti di tua iniziativa quando un'operazione non ha prove sufficienti e sai di cosa hai bisogno per continuare.

Domanda frequente

Finire le pagine equivale a essere pronti a custodire qualsiasi importo? No. La capacità deve essere dimostrata e il rischio deve essere valutato in base alla tua situazione. La lettura e le prove non garantiscono risultati futuri.

Punto di pausa

Conserva il tuo piano di revisione e le pratiche in sospeso. Puoi tornare al capitolo necessario senza ripetere tutto il corso.

Qual è un requisito fondamentale per concludere la formazione pratica?

1. Aver aperto tutte le pagine.
2. Dimostrare il recupero e la verifica delle operazioni entro un ambito documentato, senza rivelare segreti.
3. Prevedere il prezzo del prossimo mese.

> **Mostra risposta: Dimostrare il recupero e la verifica delle operazioni entro un ambito documentato, senza rivelare segreti.**
> L'apprendimento si comprova con capacità e limiti verificati, non con la navigazione o le previsioni.

Manuale dello studente

Manuale operativo Cuvex

Questo manuale accompagna le lezioni. Ogni procedura descrive il flusso trovato nelle fonti controllate, i controlli e il punto di interruzione. Questa edizione è candidata per un progetto pilota. Non attesta prove fisiche proprie con Original, BIT, telefoni o ciascuna piattaforma desktop. Prima di insegnare con i fondi reali, il team deve completare la matrice di accettazione e regolare qualsiasi cartellino o schermo diverso.

Riferimenti: Original 1.2.2 Fine, BIT 1.2.3 Fine, Desk 1.0.0-beta.9.21 e Mirror 1.0.0-beta.12.12. La selezione di un profilo in Desk è la compatibilità dichiarata, non la misurazione remota del firmware. Le catture reali incluse di Mirror provengono dall'emulatore Android del pacchetto 12.12. Le foto di prodotto sono materiale aziendale e non provano la versione visualizzata su un dispositivo corrente.

P01 | Verificare provenienza e versione | Cuvex | L16,L21 | C01,C02

Preparazione: dispone dell'acquisto e del canale ufficiale che puoi verificare in modo indipendente. Non inserisca ancora dei segreti.

1. Ispeziona l'imballaggio e i sigilli. Se ci sono segni di manipolazione, fermare l'avviamento e conservare prove non sensibili.
2. Usa il flusso di integrità e i sigilli dell'app compatibile con la tua consegna; inserisci i codici solo lì, mai al tutor.
3. Identifica Original o BIT e la revisione disponibile. Controlla la versione visibile del dispositivo e delle app.
4. Confronta con la matrice pubblicata dal computer. Un catalogo o un hash non sostituiscono l'autenticazione del firmware o l'accettazione fisica.

Risultato: modello e versioni identificati e provenienza riveduta senza esposizione di segreti. Se i codici non sono validi o l'interfaccia differisce, non seguire una guida storica per forzare l'uso.

Pausa: prima di caricare materiale di custodia. La tracciabilità commerciale non garantisce di per sé alcuna manipolazione avanzata.

P02 | Aggiornare Original tramite Bluetooth | Original | L46 | C01,C02,C03

Preparazione: copie recuperabili, alimentazione stabile, pacchetto ufficiale compatibile e percorso accettato per il tuo sistema. La disponibilità fisica completa su ogni piattaforma non è accreditata da questo corso.

1. Nei dispositivi o firmware dell'app, seleziona Original e il download ufficiale o il file locale autentico corrispondente.
2. Mettere il dispositivo in aggiornamento secondo il menu e collegarlo al flusso dell'applicazione. Tieni la bocca chiusa ed evita sessioni concorrenti.
3. Inserisci il codice dello schermo di Original nel campo indicato. Non confonderlo con la password del crittogramma.
4. Continua a trasferire, convalidare, installare e riavviare. Non prendere la percentuale come prova di installazione.
5. Controlla in Original la versione finale e registrala nell'app se questo campo esiste.

Risultato: versione verificata sullo schermo dopo reset e flusso finale confermato. Se non riesce prima di PIN, durante i pacchetti o alla fine, registra quella fase e il codice. Non disconnettere o modificare il software in modo improvvisato per passare il 99 % ·.

P03 | Aggiornare BIT tramite USB | BIT | L46 | C01,C02,C03

Preparazione: identifica il supporto reale di BIT, alimentazione e pacchetto ufficiale compatibile. Conserva le copie prima di cambiare software.

1. Seleziona BIT nel percorso firmware di Desk o Mirror compatibile.
2. Collegare il dispositivo tramite cavo e adattatore dati appropriati. Autorizza l'accesso al volume o alla cartella quando l'app lo richiede.
3. Seleziona il firmware autentico del modello. Controlla la versione e i dati di compatibilità prima di inviarlo.
4. Attendere le fasi di trasferimento e convalida del dispositivo. Un volume può scomparire o rimontare secondo il protocollo.
5. Dopo il riavvio, controlla la versione in BIT e il risultato finale dell'app.

Risultato: installazione verificata nell'apparecchiatura stessa. Se il volume non viene visualizzato, controlla la modalità del dispositivo, il cavo dati, le autorizzazioni, il montaggio e un'altra sessione attiva. Non crei una cartella con lo stesso nome sul PC come sostituto. Il recupero di un aggiornamento fallito richiede la procedura ufficiale di tale hardware.

P04 | Generare un wallet con una moneta e dei dadi | Cuvex | L17 | C01

Preparazione: spazio privato, dadi adatti e moneta; senza microfono del tutor attivo né telecamere. Usa un portafoglio di apprendimento.

1. Apre la creazione di Wallet e il flusso di entropia del firmware. Preferisci l'ordine dei quattro dadi.
2. Inserisci moneta e ciascun dato come indicato dallo schermo, senza cambiare i risultati di preferenza.
3. Il codice sorgente esaminato calcola l'indice = moneta × 1.296 + (d1−1) × 216 + (d2−1) × 36 + (d3−1) × 6 + (d4−1). Accetta solo indici 0..2.047.
4. Di fronte al rifiuto rilancia la moneta e tutti i dadi. L'avviso mantiene le parole precedenti e chiede di ripetere l'insieme.
5. Completa l'algoritmo del dispositivo, compresa la convalida finale, protegge la mnemonica e controlla il recupero in privato.

Risultato: portafoglio generato dall'intero percorso, non parole scelte manualmente. Se lo schermo e il font non corrispondono, ferma l'uso. Non usare un esempio pubblico di dadi, seed o chiave come materiale proprio.

P05 | Cifrare un segreto | Cuvex | L18,L19 | C01

Preparazione: scegliere modello, formato contenuto e protezione. L'ingresso su un PC o telefono espone l'origine anche se la destinazione è crittografata.

1. Seleziona la cifratura e il tipo compatibile: BIP39, SLIP39, Monero o testo. Non scambiare dizionari. La tastiera a testo piatto rivista supporta fino a 500 caratteri; memorizzare un altro formato non significa poter firmare la rete.
2. Inserisci il contenuto direttamente nel dispositivo per mantenere tale isolamento. Controlla comando, caratteri e campi ausiliari sullo schermo.
3. Scegli protezione individuale o condivisa in base al flusso e biometria in BIT, se applicabile. Differisca questa soglia della soglia Bitcoin.
4. Inserisci e conferma le password in privato in base al validatore del firmware. Non riutilizzate automaticamente le regole di Desk.
5. In Original registra su scheda vuota compatibile; in BIT conserva gli oggetti di esportazione del flusso USB. Aspetta la conferma.
6. Apre un recupero di prova per verificare il contenuto e chiude il segreto alla fine.

Risultato: crittogramma di cui è stato verificato il recupero. Se la scrittura o la lettura fallisce, proteggi l'originale e segui le indicazioni sullo schermo per riprovare. Non eliminare le intestazioni e non forzare la sovrascrittura.

P06 | Decifrare sul dispositivo | Cuvex | L18 | C01,C02

Preparazione: privacy fisica e componenti di sblocco sufficienti; microfono e screenshot disabilitati vicino al segreto.

1. Inizia a decifrare il modello corretto e consegna il crittogramma NFC in Original o il flusso USB di BIT.
2. Controlla gli alias e l'identificazione dell'oggetto prima di inserire credenziali.
3. Fornisci le password necessarie e i dati biometrici quando il formato li richiede. Non insistere automaticamente su errori: c'è il controllo dell'accesso e del blocco.
4. Verifica il contenuto solo sullo schermo previsto. Un QR segreto ha la stessa sensibilità del testo.
5. Chiudi o termina il processo secondo il dispositivo e salva il supporto e le credenziali separatamente secondo il tuo piano.

Risultato: contenuto recuperato in privato e sessione terminata. Se il formato non è riconosciuto, l'autenticazione non è valida o il contenuto inaspettato appare, non lo più corretto con un'app sconosciuta. Descrive al supporto versione, formato ed errore, senza allegare il segreto.

P07 | Preparare il recupero di un crittogramma biometrico | BIT | L19,L47 | C01,C02

Preparazione: crittogramma di apprendimento e documentazione del suo formato. Non deduci un recupero dal semplice fatto di avere una copia.bin.

1. Nella scheda Desk si identifica se ci sono componenti biometrici e quale esportazione di recupero è disponibile.
2. Conserva l'insieme di file che il flusso associa e una copia indipendente, con identificatori discreti.
3. Prova lo sblocco normale in BIT e documenta quali password e condizioni richiedono.
4. Studia la via eccezionale di recupero locale e i suoi formati supportati. Controlla che il materiale necessario esista prima di averne bisogno.
5. Scoprite con i dati senza fondi lo scenario del dispositivo guasto o l'impronta non disponibile.

Risultato: un piano collaudato, con i suoi limiti, per quel formato specifico. Non si afferma che qualsiasi biometria possa essere omessa o che un'impronta sostituisca le copie. Se si recupera un segreto su un PC, valuta la sua esposizione e la necessità di migrare controllo dopo.

P08 | Creare e verificare una copia di un crittogramma | Cuvex e Desk | L20 | C01,C02

Preparazione: una copia originale identificata e una destinazione compatibile senza dati da conservare.

1. Per Original, utilizza il clone del dispositivo o la funzione compatibile di Desk e presenta origine e destinazione nell'ordine indicato.
2. Mantieni le schede stabili e rispetta il rifiuto di supporti che contengono già crittogrammi.
3. Per BIT o file, esporta l'insieme dei componenti del flusso e conserva i nomi o le associazioni necessari.
4. Isola la copia originale ed esegui una prova di lettura e recupero dalla nuova copia.
5. Registra privatamente data, formato e risultato; salva le copie con rischi fisici indipendenti.

Risultato: una seconda copia provata. Non implica una Wallet diversa, revoca di password o protezione da un seed che è già stato diffuso. Se la destinazione fallisce, conserva l'originale senza cercare di ripararlo !"

P09 | Creare e sbloccare l'archivio di Desk e modificarne la password | Desk | L21,L40 | C02

Preparazione: installatore verificato, architettura adeguata e piano di backup del magazzino.

1. Crea il vault con password unica da 12 a 1.024 caratteri e conferma corrispondente.
2. Blocca e riapri per verificare che l'accesso sia ancora possibile. La password viene inserita solo in Desk.
3. In Sicurezza e Accesso e Blocco controlla inattività e passo in secondo piano. Non attivare la cancellazione opzionale durante una dimostrazione.
4. Per cambiare la password, fornisce la nuova corrente e conferma la nuova per il suo flusso.
5. Se si utilizza la biometria del PC, riimpostarla in base all'indicazione. Crea copia corrente e salva il rapporto con le copie precedenti.

Risultato: accesso controllato. Le copie precedenti conservano la password e la crittografia originali. Biometria PC e biometria BIT sono meccanismi diversi. Se l'accesso fallisce, ferma i tentativi ripetuti e controlla il recupero senza chiedere al tutor di conservare le credenziali.

P10 | Associare e verificare un crittogramma in Desk | Desk | L22 | C02

Preparazione: crittogramma di prova di provenienza nota e trasporto disponibile.

1. Apri l'area crittogrammi o carte e seleziona l'associazione tramite NFC, USB o copia compatibile.
2. Seleziona il design e l’origine. Per NFC usa Cuvex Mirror collegato al computer tramite Bluetooth. Per Cuvex BIT usa il volume del dispositivo collegato tramite USB-C. Cuvex Desktop non supporta lettori NFC USB esterni.
3. Controlla la scheda: alias, origine, dimensione, formato e condizioni interpretate. E' metadato, non contenuto decifrato.
4. Controlla se ci sono conti ancora in sospeso e collega solo il conto verificato.
5. Esporta una copia se manca la copertura e prova il recupero separatamente.

Risultato: l'oggetto è stato organizzato nell'archivio locale. Il collegamento di un campione non dimostra l'autenticazione del seed o il saldo. Un oggetto non riconosciuto richiede la verifica di formattazione e versione, senza modifica di estensione o cancellazione di dati fino a quando l'app non lo accetta.

P11 | Attivare un conto WOW watch-only | Desk e Cuvex | L13,L22 | C01,C02

Preparazione: informazioni pubbliche ottenute dal flusso del dispositivo e dal controllo privato della sua provenienza.

1. Apri l'attivazione WOW o aggiungi account dal crittogramma corretto.
2. Importa il descrittore o il materiale pubblico supportato da file, webcam o Mirror secondo la funzione.
3. Controlla rete, script, origine, impronta, percorso e checksum, se del caso. Non inserire frasi seed o xprv.
4. Dimmi l'account e scegli fonte di consultazione con il consenso.
5. Controlla un indirizzo di controllo e la portata della scoperta prima di interpretare il saldo.

Risultato: portafoglio di osservazione associato. Se vedi saldo zero, verifica la rete, la passphrase originale, la derivazione, il conto, il fornitore e la scansione degli indirizzi prima di concludere che le monete sono scomparse. Un'interfaccia supporta reti generali che non supporta necessariamente il profilo multifirma: rispetta ogni contesto.

P12 | Configurare il nodo e la sincronizzazione | Desk | L25,L33 | C02

Preparazione: decisione sulla privacy e, se si utilizza Core, accesso a un nodo protetto e sincronizzato.

1. In Sicurezza e Privacy e nodi sceglie l'account WOW e controlla il suo fornitore.
2. Scegli espressamente fornitore pubblico compatibile o Core. Per Core introduce endpoint, wallet e credenziali solo nell'app.
3. Autorizza la consultazione comprendendo quali dati riceve ogni servizio. TLS non nasconde la richiesta al fornitore.
4. Sincronizza e controlla data, punta, progresso e stato completo. Per recuperare controlla l'antichità coperta e la continuità del lavoro.
5. Ante 429 rispetta la pausa. Non supponiamo che un altro nodo sia stato attivato in caso di guasto: la configurazione non è rotta in silenzio.

Risultato: fonte e stato conosciuti. Non aprire la RPC a Internet, condividere la password o ridurre la scoperta a indirizzi con saldo. Una storia vuota può essere un risultato parziale.

P13 | Generare e recuperare una richiesta di ricezione | Desk e Cuvex | L26 | C01,C02

Preparazione: conto, rete e politica verificate.

1. Apre ricevere e generare o recuperare la richiesta appropriata.
2. Aggiungi osservatore, movente e importo atteso solo se hai bisogno di questi metadati locali.
3. Controlla l'indirizzo per il percorso compatibile del dispositivo prima di un recupero rilevante. Se manca l'accettazione fisica, ferma la pratica nella simulazione.
4. Condivide esclusivamente i dati necessari tramite il canale autenticato del ricevitore.
5. Controlla l'ingresso, l'importo e la conferma nella tua fonte di rete.

Risultato: recupero conciliato, non solo richiesta emessa. In più firme gli indirizzi visualizzati sono conservati per pagamenti tardivi e non sono riassegnati. Se il limite di nuovi indirizzi senza cronologia viene raggiunto, recupera le richieste precedenti; non forzare manualmente gli indici.

P14 | Etichette, congelamento e BIP329 | Desk | L27 | C02,B13

Preparazione: ha un laboratorio con UTXOs e una password per l'esportazione protetta.

1. Etichetta un'iscrizione con il contesto senza dati personali non necessari.

2. Congelate o scongelate consapevolmente e controllate il saldo speso. La restrizione e' locale.
3. Esporta etichette tramite la funzione protetta. Distingui BIP329 come formato dalla cifratura del file.
4. Importa in una copia compatibile; controlla la corrispondenza di referenze, etichette e congelazioni.
5. Conserva un backup dei metadati aggiornato insieme alla tua password, secondo il tuo piano.

Risultato: contesto conservato e selezione intesa. Un'importazione non deve essere utilizzata per sbloccare automaticamente le monete congelate senza revisione. Non inviare il file di tag al tutor: puoi rivelare controparti e relazioni anche se non include le chiavi di spesa.

P15 | Preparare un pagamento e inviare l'intero saldo | Desk | L28 | C02

Preparazione: richiesta verificata e dispone di sufficienti ingressi spendibili.

1. Apre il pagamento da WOW, UTXOs o chat e conferma account e rete.
2. Seleziona voci, destinatari e importi e controlla i contesti correlati.
3. Scegli la tariffa e verifica la commissione assoluta, il resto e gli avvisi. Se c'è un dust, controlla le alternative senza accettare una commissione nascosta.
4. Per inviare totale controlla il netto dopo commissione. In chat conferma esplicitamente un pagamento parziale se la richiesta non viene soddisfatta.
5. Prepara la bozza e controlla tutti i dati prima di esportare per la firma.

Risultato: intenzione comprensibile e PSBT di tale operazione. Un modulo generale può ammettere più voci o destinatari dell'hardware: applica i limiti effettivi del firmatario e del trasporto. In caso di cambiamento di uscite o condizioni, viene avviata una nuova revisione.

P16 | Firmare e restituire una PSBT con Original | Original y Mirror | L29 | C01,C02,C03

Preparazione: bozza corretta, carta di trasporto compatibile, crittogramma autenticato e compatibile, e mezzi di sblocco mantenuti in privato. Una copia storica non verificata può richiedere il recupero verificato e la creazione di una nuova copia prima di firmare; non viene corretta modificando l'intestazione.

1. Esporta la richiesta per il flusso NFC compatibile da Desk/Mirror.
2. Portala in Original; apporta il crittogramma quando richiesto e sblocca senza emettere credenziali.
3. Verifica rete, riepilogo, tutti gli output, commissione, resto e avvisi obbligatori.
4. In Multifirma Finale, decide se esaminare parametri estesi; completa tutte e tre le conferme finali solo se tutto coincide.

5. Aspetta la scrittura e la rilettura della risposta sulla carta.
6. Leggi la risposta con Cuvex Mirror e convalidala nell’operazione di Desk.

Risultato: firma ricevuta e collegata alla bozza, ancora diversa dalla pubblicazione. Se la scrittura fallisce, conserva lo stato e segui le indicazioni per riprovare. Non usare mai la carta di backup come supporto gratuito a pagamento.

P17 | Firmare, ricevere e confermare la ricezione con BIT | BIT y Desk | L29 | C01,C02

Preparazione: bozza corretta, crittogramma autenticato e compatibile e volume effettivo di BIT selezionato. Se una copia storica è respinta per la firma, segue il recupero e il rinnovo indicato, senza forzare il formato.

1. Trasmetti la richiesta tramite USB-C usando il servizio di Desk e segui le indicazioni del dispositivo per presentare il crittogramma.
2. Sblocca in privato e controlla il sommario, tutte le uscite, commissioni e avvisi.
3. In multifirma Final, controlla opzionalmente i dettagli estesi e autorizza con le conferme finali obbligatorie.
4. In Desk usa ricevere dal BIT per importare e convalidare la risposta di quel lavoro.
5. Verifica il salvataggio e la conferma di ricezione. Se la conferma fallisce dopo la ricezione, riprova la stessa operazione, senza sceglierne una nuova in base al modello.

Risultato: firma verificata e stato di scambio coerente. Se si disconnette prima di ricevere o dopo aver salvato, conserva il profilo della richiesta. Non passare ad un altro firmware di catalogo per inserire una risposta in sospeso.

P18 | Finalizzare, pubblicare e seguire un'operazione | Desk | L30,L44 | C02

Preparazione: firme verificate e soglia sufficiente, se del caso.

1. Ricontrolla le intenzioni, le entrate, le uscite, la commissione e la rete.
2. Si conclude con l'azione corrispondente e si accerta che non manchino firme e condizioni.
3. Autorizza la diffusione e conserva il risultato locale. Se la risposta di rete viene persa, consulta prima di ripetere.
4. Segui la mempool e le conferme presso il fornitore scelto, verificando la data di sincronizzazione.
5. Se si pone RBF, controllare la nuova operazione e ottenere le firme richieste. Non assumere una funzione CPFP integrata.

Risultato: stato della catena verificato tramite la fonte corrispondente. Annullare una bozza non revoca firme già esportate e non riscrive pagamenti confermati. Un messaggio di chat o una cattura non sostituiscono il tracciamento.

P19 | Confrontare liberamente due codici QR di una politica | Mirror | L43 | C03,C02

Preparazione: campo visibile in Desk e Cuvex; in pratica utilizza solo i campioni sintetici del corso.

1. Apri Confronta le politiche e leggi prima uno dei due lati.
2. Scegli il dato che vuoi controllare; puoi iniziare dal punto 15 e saltarne altri manualmente.
3. Leggete la vostra controparte e controllate entrambi i testi completi. Se il passaggio è ambiguo, usa Indica il passaggio di Desk e capisci che il contesto è manuale.
4. Interpreta Corrisponde o non corrisponde solo a quella coppia letterale. Spazi, maiuscole e codifica contano.
5. Inizia un'altra coppia in qualsiasi ordine. Esci o vai in background per finire in base al comportamento di cancellazione rivisto.

Risultato: confronto locale in un momento specifico. Non accreditare origine, sessione, approvazione globale o attivazione. Una differenza deve essere chiarita con le sue fonti, senza normalizzare il testo per forzare un OK.

P20 | Attivare, recuperare e trasferire la chat | Desk e Cuvex | L36,L39 | C02

Preparazione: ambiente DEV o produzione scelto, un alias e Chiave Chat sul dispositivo, mai nel corso.

1. Aprire l'attivazione o il ripristino della chat dal contesto del crittogramma.
2. Scegli nuovi alias o trasferimento esistente e il profilo mobile supportato indicato dall'app.
3. Inserisci o leggi la Chiave Chat esclusivamente nel flusso privato. Non usare seed, PIN o chiave WOW.
4. Controlla l'attivazione con il servizio; se rimane in sospeso, utilizza l'azione di completare o controllare, senza darla per corretta.
5. Verifica la continuità con i contatti dopo il trasferimento ed evita di usare lo stesso alias contemporaneamente su più dispositivi.

Risultato: identità attivata o recuperata nell'ambiente giusto. Cronologia e sessioni precedenti non vengono recuperati automaticamente con la Chiave Chat o con la copia globale di Desk. Conserva i limiti del materiale disponibile.

P21 | Verificare l'identità di un contatto | Desk | L36,L48 | C02

Preparazione: canale indipendente precedentemente concordato con la persona.

1. Aggiunge l'alias e consulta la sua identità pubblica tramite l'app.
2. Confronta l'impronta attraverso il canale autenticato, non solo all'interno della conversazione appena creata.
3. Se usi il riconoscimento, evita informazioni pubbliche o segreti riutilizzati in altri servizi.
4. Conferma solo dopo aver risolto le divergenze. Se l'identità cambia, sospendi i pagamenti e il coordinamento fino alla verifica.
5. Documenta il metodo di verifica senza memorizzare risposte sensibili nel corso.

Risultato: fiducia contestuale nel contatto, non una garanzia di tutte le vostre richieste future. Una voce può essere imitata e un dispositivo legittimo può essere compromesso. Ogni operazione mantiene la sua revisione.

P22 | Chiedere un indirizzo, richiedere ed effettuare un pagamento in chat | Desk e Cuvex | L37 | C02,C01

Preparazione: contatto verificato e conto WOW compatibile.

1. Seleziona per richiedere l'indirizzo, rispondere con l'indirizzo o richiedere il pagamento secondo l'intenzione.
2. Controlla la richiesta originale, la rete, l'importo e la nota prima di inviarla.
3. Per pagare, apre la preparazione dal conto giusto, seleziona UTXOs e tariffa e controlla l'importo netto.
4. Autorizza in Cuvex con la procedura del modello. La chat non firma automaticamente.
5. Continua a pubblicare e confermare dalla tua fonte; concilia pagamenti parziali espliciti con la richiesta originale.

Risultato: coordinamento mantenendo la revisione della custodia. Stato di messaggio e stato di transazione non sono equivalenti. Un link a browser può inviare informazioni a terzi: valuta il loro utilizzo prima di aprirlo.

P23 | Condividere e associare un crittogramma ricevuto | Desk | L38 | C02

Preparazione: specifica necessità di condivisione, contatto verificato e definizione dei mezzi di accesso che riceverà.

1. Seleziona l'azione di condivisione del crittogramma nella chat e verifica l'oggetto.
2. Non aggiungere password, seed o Chiave Chat come commento.
3. Il destinatario verifica la provenienza e collega l'oggetto compatibile con la sua azione di ricezione.
4. Valuta che capacità ottiene ora e che cosa otterrà se ottiene abbastanza credenziali di sblocco.
5. Conserva un piano di revoca realistico: eliminare i messaggi non rimuove copie esterne né chiavi conosciute.

Risultato: trasferimento consapevole di un oggetto cifrato. Non è un pagamento, né una chiave per una multifirma. Se l'allegato ti chiede di visitare una pagina sconosciuta per decifrarlo, interrompi la procedura.

P24 | Backup globale e ripristino di Desk | Desk | L15,L21 | C02

Preparazione: magazzino di apprendimento e destinazione di copia controllata.

1. Apre la funzione di copia del vault e definisce la password indicata; conserva il rapporto con questa copia specifica.
2. Tenere fuori dall'unico apparecchio di utilizzo e verificare la provenienza e l'integrità del flusso.
3. Ripristina in un ambiente di prova separato e verifica account, impostazioni e dati coperti.
4. Controlla le esclusioni: chat, le sessioni e la cronologia non devono essere prese in considerazione; politica multifirma e chiavi private non sono intercambiabili.
5. Ripeti dopo modifiche importanti e conserva le istruzioni di recupero.

Risultato: backup la cui portata e password sono note. Le vecchie copie conservano le password precedenti. Se l'accesso è cambiato o se c'è esposizione, valuta anche queste copie; non basta modificare l'attuale magazzino.

P25 | Creare e accettare un wallet multifirma | Desk e Cuvex | L41,L42 | C01,C02

Preparazione: partecipanti indipendenti, contatti verificati, rete e limiti effettivi concordati.

1. Il creatore sceglie nome, M/N, rete, partecipanti e durata operativa.
2. Fornisci la chiave pubblica estesa corretta con impronta e percorso BIP48 tramite la procedura compatibile.
3. Ogni partecipante controlla, accetta o rifiuta e fornisce il suo materiale pubblico. Non condivide mai il seed.
4. Costruisci la politica completa e prepara la verifica su ogni dispositivo.
5. Conserva delle copie di politica prima di finanziare. Controlla la direzione di controllo e la capacità di recupero.

Risultato: proposta completa e verificabile. L'accettazione dell'invito non sostituisce la revisione hardware. Se Original interviene, applica il suo massimo di sei chiavi e la dimensione NFC; BIT non amplia le capacità degli altri partecipanti.

P26 | Verificare la politica e ricevere la conferma | Desk e Cuvex | L43 | C01,C02,C03

Preparazione: stessa politica completa per tutti, profilo firmware corretto e dispositivo senza operazioni concorrenti.

1. Inizia a verificare le politiche nel contesto compatibile. Original richiede una selezione esplicita del profilo installato; BIT negozia le capacità secondo il contratto.
2. Consegna la richiesta per NFC/Mirror o USB-C secondo modello.
3. Controlla i campi di politica sul dispositivo. Usa Mirror come confronto opzionale delle coppie scelte senza ordine obbligatorio.
4. Completa la conferma dell'apparecchiatura e restituisce la risposta per il trasporto corrispondente.
5. In Desk è valida la risposta connessa alla richiesta. Non sostituire questo passaggio con un OK visivo del comparatore.

Risultato: revisione correlata alla portata di tale revisione. Il catalogo non riempie remotamente il firmware e il dispositivo non viene presentato come archivio politico persistente. Prima di FIRMWARE_CAPABILITY_REQUIRED, controlla la prima versione di Desk e la combinazione modello/build.

P27 | Richiedere e ricevere le firme e trasferire il coordinamento | Desk e Cuvex | L44 | C01,C02

Preparazione: politica verificata, operazione identificata e destinatari concordati.

1. Prepara input, output, commissione e note, quindi richiedi le firme ai partecipanti compatibili.
2. Ogni partecipante verifica e firma sul proprio dispositivo seguendo il rispettivo percorso di trasporto.
3. Ricevi, valida e salva ogni firma; risolvi le accuse pendenti senza modificare il profilo conservato.
4. Se viene superato il coordinamento, il ricevitore accetta il flusso e verifica lo stato. Non cambia per questo M/N o proprietà chiavi.
5. Quando si raggiunge la soglia, controlla e termina prima di pubblicare. Segui la transazione in rete.

Risultato: coordinamento con prove differenziate. Un rapporto sui progressi del coordinatore non equivale a una verifica locale da parte tua. Annullare o rifiutare in un'app non distrugge necessariamente le firme già conservate da terzi.

P28 | Esportare, ripristinare ed eliminare il wallet multifirma locale | Desk | L45 | C02

Preparazione: politica conosciuta e copia crittografata con password unica.

1. Esporta recupero tramite l'azione di Desk. Il flusso corrente utilizza un contenitore autenticato CVXMSBK1 per tale esportazione.
2. Conserva copia e password con rischi indipendenti. Non devi dedurne la crittografia per estensione di file storici.
3. Per ripristinare fornisce copia, password e chiave pubblica del partecipante con origine corretta tramite webcam o Mirror, se applicabile.
4. Controlla la politica, la rete, la direzione e la scoperta prima di operare.
5. Per rimuovere localmente, leggi l'estensione e la conferma e salva copia se vuoi conservare il recupero. Ripristinare dopo è esplicito.

Risultato: politica recuperabile o smaltimento locale cosciente. L'eliminazione non sposta fondi, non cancella le chiavi di altri firmatari e non annulla da sola le operazioni conservate da altre persone.

P29 | Recupero eccezionale su un PC | Desk | L47 | C02

Preparazione: materiale di formato supportato, ambiente pulito preparato e backup. Questa operazione può rivelare un segreto al PC; utilizza i dati di apprendimento nel corso.

1. Inizia il recupero locale dal contesto corretto e leggi le limitazioni del formato e gli avvisi.
2. Accetta il rischio consapevolmente e disconnette la rete come richiesto dal flusso; la finestra controlla lo stato prima di permettere di continuare.
3. Inserisci solo le credenziali necessarie nella finestra privata. Non si dettano, si picchiano nel corso, né si condividono con supporto.
4. Attiva la visualizzazione solo in uno spazio senza telecamere o assistenti in ascolto; rispetta il timer e la chiusura.
5. Infine, controlla l'esposizione e pianifica la migrazione a nuove chiavi, se del caso.

Risultato: recupero eccezionale, non garanzia di cancellazione forense o equivalenza con hardware isolato. Se manca l'autenticazione, il formato o il materiale di accesso, non provare gli strumenti Internet con la tua copia reale.

P30 | Verificare preferenze, biometria e blocco | Desk | L40 | C02

Preparazione: password conosciuta e backup testato prima di modificare la sicurezza.

1. In Accesso e blocco controlla password, biometria disponibile, inattività e blocco quando si passa in background.
2. Comprende il ritardo dopo i bug e il massimo impostato prima di cambiarlo.
3. Tieni la cancellazione opzionale disabilitata fino a comprendere le condizioni, la soglia e il recupero. Non provarlo in produzione.
4. In Impostazioni imposta lingua, tema, moneta, sincronizzazione di 3 o 5 minuti e suoni.
5. Se registri link bitcoin:, controlla che l'apertura di una richiesta mantenga sblocco, selezione e revisione; non paga da solo.

Risultato: configurazione intesa. La biometria del sistema operativo dipende dal computer e non sostituisce password o backup. Le preferenze visive non modificano la politica di Bitcoin.

P31 | Eliminare i registri senza confondere la portata dell'operazione | Desk | L22,L45 | C02

Preparazione: individua se stai per eliminare il crittogramma locale, il conto, la WOW, la chat o il wallet multifirma, e stabilisci quale copia conserverai.

1. Leggi l'oggetto selezionato e il tuo avviso. Conferma l'esatto alias o la condizione esplicita quando l'app lo richiede.
2. Esporta e prova copia se hai bisogno di recuperare quello stato più tardi.
3. Elimina solo l'oggetto previsto e verifica le associazioni che conservano o ritirano il flusso.
4. Controlla se ci sono altre operazioni o partecipanti esterni. Non presumere che vengano eliminati i messaggi, le firme o i file di altri dispositivi.
5. Documenta il cambiamento nel tuo inventario privato senza dati sensibili nel corso.

Risultato: stato locale gestito consapevolmente. Nessuna di queste azioni cambia da sola script di UTXOs finanziati, distrugge un seed conosciuto da terzi o inverte transazioni confermate.

P32 | Diagnosticare i problemi senza esporre segreti | Desk e Mirror | L23,L30,L48 | C02,C03

Preparazione: segna ora approssimativa, sistema, architettura, versione e fase. Evita di ripetere un'operazione sensibile senza conoscere le sue condizioni.

1. Identifica se il bug è ricerca, collegamento, lettura, scrittura, convalida, firma, ritorno, rete o visualizzazione.
2. Copia il codice e il testo dell'errore senza includere QR o dati privati. Usa la diagnostica dell'app quando applicabile.
3. Verifica il file prima di condividerlo. Non allegare una copia dell'archivio locale, crittogrammi, frasi seed, la Chiave Chat, descrittori o credenziali RPC.
4. In un'incidenza di interfaccia, registra dimensioni delle finestre, zoom e controlli nascosti con una scena sintetica.
5. Invia un risultato atteso e passi riproducibili sul canale ufficiale. Il corso non invia automaticamente messaggi a supporto.

Risultato: rapporto che permette di indagare con minimo dati. Se non c'è evidenza di una fase, si registra più di un livello, non si completa. L'assistenza vocale non ha bisogno di accesso remoto al tuo team di custodia.

Glossario di Bitcoin e autocustodia

Bitcoin

Rete e insieme di regole per trasferire valore e verificarne la cronologia senza un unico amministratore del registro.

BTC

Unità monetaria di Bitcoin. Un BTC equivale a cento milioni di satoshi.

Satoshi

Unità della catena di base pari a un centomilionesimo di BTC.

Blockchain

Cronologia di blocchi collegati e verificati secondo determinate regole. Il termine, da solo, non descrive tutte le proprietà di una rete.

Blocco

Insieme di dati che comprende transazioni e un'intestazione verificabile.

Nodo completo

Software che verifica il rispetto delle regole da parte dei blocchi e delle transazioni che accetta.

Mining

Costruzione di blocchi mediante prova di lavoro secondo le regole della rete.

Prova di lavoro

Meccanismo che richiede un lavoro computazionale verificabile per proporre un blocco.

Consenso

Concordanza dei partecipanti sulle regole e sulla cronologia valida che accettano.

Politica della mempool

Regole locali di accettazione e ritrasmissione che non corrispondono necessariamente alle regole di consenso.

Mempool

Insieme locale delle transazioni non confermate conservate da un nodo.

Conferma

Inclusione in un blocco della catena accettata e profondità che il blocco raggiunge in seguito.

Riorganizzazione

Modifica di un tratto della catena accettata che può alterare le conferme.

UTXO

Output di una transazione non ancora speso, utilizzabile soddisfacendo le relative condizioni.

Input

Riferimento a un output precedente e dati necessari per autorizzarne la spesa.

Output

Valore e condizione di spesa creati da una transazione.

Resto

Output che riporta sotto il proprio controllo parte del valore degli input dopo il pagamento e la commissione.

Commissione

Differenza fra il valore degli input e quello degli output di una transazione.

vbyte

Unità di dimensione virtuale usata per esprimere il costo relativo di una transazione.

sat per vbyte

Tariffa della commissione espressa in satoshi per unità di dimensione virtuale.

Dust

Output di valore ridotto rispetto alle politiche e al costo per spenderlo. La soglia dipende dal contesto e dallo script.

RBF

Sostituzione di una transazione non confermata secondo politiche compatibili. Non garantisce l'annullamento.

CPFP

Uso di una transazione figlia per aumentare l'incentivo a includere l'insieme formato con la transazione genitore.

Hash

Impronta dei dati utile per verificarne l'integrità. Non li cifra né identifica da sola il loro autore.

Chiave privata

Permette di produrre autorizzazioni crittografiche secondo lo schema corrispondente.

Chiave pubblica

Dato che permette di verificare firme e costruire determinate condizioni senza esporre la chiave privata.

Firma digitale

Prova crittografica dell'autorizzazione di un messaggio specifico. Non ne nasconde il contenuto.

Cifratura

Protezione della riservatezza mediante una chiave e un algoritmo.

Cifratura autenticata

Cifratura che permette di rilevare alterazioni secondo il suo schema.

AES GCM

Famiglia di cifratura autenticata utilizzata nei formati dell'ecosistema. Le sue proprietà dipendono dall'implementazione e dalla gestione delle chiavi.

Mnemonica

Rappresentazione mediante parole del materiale di generazione e verifica secondo un formato specifico.

Seed

Materiale da cui si derivano le chiavi. Nel linguaggio comune il termine indica anche la sequenza di parole, quindi occorre precisare il contesto.

Entropia

Imprevedibilità del materiale di generazione. Non si ottiene scegliendo parole memorabili.

Checksum

Somma di controllo che rileva determinati errori. Non autentica l'autore.

BIP39

Specifica delle mnemoniche e della derivazione del seed con una passphrase facoltativa.

Passphrase BIP39

Dato aggiuntivo per la derivazione. Una passphrase diversa può produrre un altro wallet valido e vuoto.

BIP32

Specifica della derivazione gerarchica delle chiavi.

Percorso di derivazione

Sequenza di rami utilizzata per ottenere chiavi da una radice.

Derivazione hardened

Passaggio di derivazione solitamente indicato da un apostrofo o da h, con proprietà diverse dalla normale derivazione pubblica.

xpub

Chiave pubblica estesa con il contesto per la derivazione. È sensibile sotto il profilo della privacy.

xprv

Chiave privata estesa. Non va condivisa né importata in un corso.

Impronta della chiave master

Identificativo breve di una radice. Aiuta ad associare i dati, ma non è una prova d'identità sufficiente.

Descrittore

Espressione che descrive come costruire script con chiavi e derivazioni. Può essere pubblica o contenere materiale privato.

Watch only

Wallet di sola osservazione che non dispone della capacità privata sufficiente per firmare autonomamente.

WOW

Denominazione dei conti di osservazione e gestione del wallet nell'ecosistema Cuvex.

Hot wallet

Strumento con capacità di firma in un ambiente connesso.

Autocustodia

Modello in cui l'utente conserva la capacità tecnica di spesa, individualmente o in forma condivisa, secondo la propria politica.

Custode

Entità che controlla per conto del cliente la capacità di spesa e applica le proprie condizioni di accesso.

Crittogramma Cuvex

Oggetto cifrato che protegge un segreto. Di per sé non è una transazione né un saldo.

Password di Desk

Protegge l'accesso all'archivio locale. È distinta dal seed e dalla password del crittogramma.

Chiave Chat

Segreto per recuperare l'identità della chat. Può sembrare un dato pubblico senza esserlo.

PIN di collegamento

Codice temporaneo di una sessione di connessione. Non è una password di custodia.

Air gap

Separazione operativa tra ambienti. I dati trasportati richiedono comunque una convalida.

NFC

Tecnologia di comunicazione a corto raggio utilizzata con carte e lettori compatibili.

USB Mass Storage

Interfaccia di scambio tramite file del modello BIT, con protocollo, convalida e conferme di ricezione propri.

PSBT

Contenitore di informazioni e firme per coordinare la costruzione e l'autorizzazione delle transazioni.

PSBT v0

Versione del formato definita in BIP174 e utilizzata dal profilo multifirma Final esaminato.

PSBT v2

Versione definita in BIP370. Il fatto che la transazione sia di versione 2 non implica che la PSBT sia v2.

SIGHASH ALL

Modalità che determina quali dati sono vincolati dalla firma nel profilo esaminato. La sua portata tecnica fa parte della verifica dell'operazione.

P2WPKH

Tipo di condizione SegWit a chiave singola solitamente associato a conti BIP84.

P2WSH

Condizione SegWit che vincola uno script. È utilizzata dalla multifirma Final esaminata.

P2TR

Tipo di output Taproot. Accettarlo come destinazione non implica la capacità di firmare per spenderlo.

sortedmulti

Costruzione multifirma che genera script ordinando le chiavi in modo deterministico.

Soglia M su N

Numero M di autorizzazioni necessarie tra N partecipanti secondo la politica applicabile.

MuSig2

Protocollo di aggregazione Schnorr il cui schema di base è N su N, diverso da una soglia arbitraria.

Taproot

Insieme di meccanismi di spesa e di vincolo di Bitcoin con percorsi basati su chiave o su script.

Miniscript

Linguaggio per descrivere e analizzare determinate politiche di script. Non è implementato nel profilo Final esaminato.

Regtest

Rete locale di laboratorio senza valore economico, controllata da chi allestisce l'ambiente.

Signet

Rete di prova con caratteristiche proprie. Non è intercambiabile per impostazione predefinita con regtest.

Mainnet

Rete Bitcoin di effettivo utilizzo economico.

Gap limit

Criterio per la ricerca degli indirizzi basato sul numero di indirizzi consecutivi senza cronologia. Il suo ambito dipende dal wallet.

Coin control

Scelta consapevole degli UTXO da spendere.

Consolidamento

Combinazione di output per ridurre la frammentazione, con conseguenze sui costi e sulla privacy.

Pseudonimato

Uso di identificativi che non corrispondono direttamente a un nome anagrafico. Non implica anonimato automatico.

Anonimato

Proprietà, dipendente dal contesto, di non essere distinguibili agli occhi di determinati osservatori. Un'app non la garantisce con un'etichetta.

Metadati

Informazioni sulle comunicazioni o sull'attività, come tempi, dimensioni e relazioni, distinte dal contenuto.

CoinJoin

Costruzione collaborativa che rende più difficili alcune inferenze senza garantire anonimato permanente.

Payjoin

Pagamento collaborativo con input del pagatore e del destinatario secondo un protocollo compatibile.

Tor

Rete e strumenti per proteggere la connessione. L'uso va configurato e verificato per ciascuna applicazione.

VPN

Canale che sposta parte della fiducia nella connessione sul suo operatore. Non nasconde la catena.

Lightning

Sistema di pagamenti tramite canali con requisiti e rischi diversi da quelli di un invio on-chain.

Invoice

Richiesta strutturata di pagamento di cui occorre identificare il formato e la modalità.

RPC

Interfaccia per effettuare chiamate a un servizio come Bitcoin Core. Deve prevedere autenticazione e protezione.

TLS

Protezione del trasporto da determinate minacce. Il server destinatario continua a vedere le richieste.

SRTP

Protezione dell'audio in determinati tratti VoIP. Non implica automaticamente la segretezza nei confronti dell'operatore.

Idempotenza

Proprietà che evita di duplicare un effetto quando si ripete una richiesta identificata.

Webhook

Evento inviato tra server. Occorre verificarne l'autenticità e rilevare le ripetizioni.

RAG

Recupero di frammenti di conoscenza per fondare una risposta su un contesto e una versione.

Teach back

Verifica dell'apprendimento in cui si chiede allo studente di spiegare a parole proprie ciò che ha capito.

Phishing

Inganno che usa l'impersonificazione e un contesto convincente per ottenere accesso o indurre un'azione.

Ingegneria sociale

Manipolazione delle decisioni umane che può servirsi di dati veri e di un senso di urgenza.

Notarizzazione

Controllo di distribuzione di Apple, distinto da un audit del prodotto o da una prova fisica di tutte le sue procedure.

Attestazione

Prova dello stato ottenuta tramite un meccanismo specifico. Il catalogo di compatibilità di Desk non è una misurazione remota.

MiCA

Quadro europeo per determinate criptoattività e servizi. Non garantisce rendimento né indennizzo integrale.

Travel Rule

Obblighi informativi per i trasferimenti che rientrano nel suo ambito. L'autocustodia non li elimina.

Checkpoint

Punto da cui riprendere l'apprendimento con dati minimi, senza informazioni sul wallet.

Verifica ciò che hai imparato

Esercitati senza fondi reali. La valutazione è ad accesso libero e non richiede un account.

Chi autorizza la spesa durante il normale utilizzo di Cuvex?

1. Il dispositivo, dopo la verifica dell'utente
2. Il tutor vocale
3. Il server del corso

> **Mostra risposta: Il dispositivo, dopo la verifica dell'utente**
> L'autorizzazione segue il suo percorso su Cuvex.

Quanti satoshi sono 0,001 BTC?

1. 1.000
2. 100.000
3. 1.000.000

> **Mostra risposta: 100.000**
> Un BTC equivale a 100.000.000 sat.

Gli input ammontano a 120.000 sat e gli output a 119.000 sat. Qual è la commissione?

1. 1.000 sat
2. 119.000 sat
3. 1 sat/vB, senza altri dati

> **Mostra risposta: 1.000 sat**
> La differenza fra gli importi è la commissione assoluta.

In che stato si trova una transazione firmata e non ancora diffusa?

1. Confermata
2. Irreversibile perché firmata
3. Autorizzata, ma non necessariamente pubblicata

> **Mostra risposta: Autorizzata, ma non necessariamente pubblicata**
> Firma e pubblicazione sono fasi distinte.

A quanto equivalgono 200 vB a 6 sat/vB?

1. 206 sat
2. 1.200 sat
3. Il 6 % dell'importo inviato

> **Mostra risposta: 1.200 sat**
> Si moltiplica la dimensione virtuale per la tariffa.

Cosa devi verificare prima di prelevare da un exchange?

1. Solo la commissione più bassa
2. La compatibilità di asset, rete, indirizzo e importo netto
3. La frase seed della controparte

> **Mostra risposta: La compatibilità di asset, rete, indirizzo e importo netto**
> Non tutte le reti con il simbolo BTC sono Bitcoin on-chain.

Cosa fa da sola una firma digitale?

1. Nasconde l'intero messaggio
2. Autorizza un messaggio verificabile secondo il suo schema di firma
3. Cancella i dati pubblicati

> **Mostra risposta: Autorizza un messaggio verificabile secondo il suo schema di firma**
> La riservatezza richiede un altro meccanismo.

Cosa può succedere cambiando una passphrase BIP39?

1. Si può ottenere un altro wallet valido e apparentemente vuoto
2. La passphrase si può sempre reimpostare via email
3. Si modifica il registro pubblico dei pagamenti precedenti

> **Mostra risposta: Si può ottenere un altro wallet valido e apparentemente vuoto**
> La passphrase partecipa alla derivazione.

Come si deve trattare la xpub di un account?

1. Come un dato privo di conseguenze
2. Come se fosse la stessa frase seed privata
3. Come informazione sensibile per la privacy

> **Mostra risposta: Come informazione sensibile per la privacy**
> La xpub può permettere di osservare più attività.

Perché in un wallet multifirma una sola frase seed può essere insufficiente?

1. Mancano la politica e le autorizzazioni necessarie per raggiungere la soglia
2. Bitcoin non permette di recuperare nulla
3. Serve il colore originale dell'app

> **Mostra risposta: Mancano la politica e le autorizzazioni necessarie per raggiungere la soglia**
> Conservare la politica e mantenere la capacità di usare le chiavi private sono requisiti diversi.

Cosa devi fare se l'algoritmo Final esaminato rifiuta il risultato dei dadi?

1. Rilanciare soltanto la moneta fino all'accettazione
2. Rilanciare la moneta e tutti e quattro i dadi
3. Scegliere una parola nota

> **Mostra risposta: Rilanciare la moneta e tutti e quattro i dadi**
> Ripetere solo parte dell'insieme può introdurre una distorsione nella corrispondenza tra risultati e parole.

Cosa significa usare due password per aprire la frase seed di un wallet a firma singola?

1. Occorrono due chiavi sulla catena
2. Si tratta di una multifirma Taproot
3. La soglia di accesso al segreto è distinta dalla soglia di Bitcoin

> **Mostra risposta: La soglia di accesso al segreto è distinta dalla soglia di Bitcoin**
> La cifratura non cambia lo script.

Cosa bisogna sapere per valutare un backup globale di Desk?

1. Include necessariamente l'intera chat
2. Ha un ambito e delle esclusioni. Non si deve presumere che includa la chat
3. Aggiorna tutte le vecchie copie

> **Mostra risposta: Ha un ambito e delle esclusioni. Non si deve presumere che includa la chat**
> Recuperare l'identità e recuperare i messaggi sono cose diverse.

Cosa consente un nodo proprio ben configurato?

1. Eliminare tutte le fughe di informazioni
2. Ridurre la dipendenza da richieste a terzi ed eseguire verifiche
3. Recuperare le chiavi perse

> **Mostra risposta: Ridurre la dipendenza da richieste a terzi ed eseguire verifiche**
> Non garantisce anonimato né recupero dei segreti.

Cosa succede congelando un UTXO in Desk?

1. Si applica una restrizione locale dell'app
2. Si modifica la condizione di consenso
3. Si revocano le altre copie della frase seed

> **Mostra risposta: Si applica una restrizione locale dell'app**
> Non è un blocco globale della spesa.

Cosa fai se perdi la connessione al momento della pubblicazione?

1. Pago di nuovo immediatamente
2. Cancello il wallet
3. Controllo prima se il pagamento è già stato diffuso

> **Mostra risposta: Controllo prima se il pagamento è già stato diffuso**
> Un timeout non prova che l'azione non abbia avuto effetto.

Cosa può comportare il riutilizzo di indirizzi o l'unione di UTXO di contesti diversi?

1. Rendere più facili da osservare i collegamenti
2. Cancellare la cronologia
3. Garantire l'anonimato

> **Mostra risposta: Rendere più facili da osservare i collegamenti**
> La privacy dipende dal contesto e dall'uso successivo.

Aprire Tor Browser configura automaticamente Desk?

1. Sì
2. No
3. Solo se il tema è scuro

> **Mostra risposta: No**
> Occorre verificare il percorso di rete di ogni applicazione.

Cos'è la Chiave Chat che assomiglia a una xpub?

1. Un dato che si può pubblicare
2. Un indirizzo per ricevere un pagamento
3. Un segreto di identità

> **Mostra risposta: Un segreto di identità**
> La finalità determina quanto è sensibile il dato.

Cosa significa un messaggio di chat con la scritta «pagato»?

1. Sostituisce le conferme
2. Il pagamento richiede una verifica indipendente sulla rete
3. Modifica la rete della richiesta

> **Mostra risposta: Il pagamento richiede una verifica indipendente sulla rete**
> Lo stato del messaggio è diverso da quello del pagamento.

Cosa utilizza il profilo multifirma Final esaminato?

1. MuSig2 e PSBT v2
2. P2WSH, sortedmulti, BIP48 e PSBT v0
3. Qualsiasi script Bitcoin

> **Mostra risposta: P2WSH, sortedmulti, BIP48 e PSBT v0**
> Le funzionalità supportate non si estendono per volontà dell'utente o per il nome commerciale.

Da quale elemento puoi iniziare il confronto in Mirror 12.12?

1. Solo dal passaggio 1
2. Da qualsiasi dato a scelta, incluso il 15
3. Solo dall'ultimo, dopo tutti gli altri

> **Mostra risposta: Da qualsiasi dato a scelta, incluso il 15**
> Il confronto è libero e ogni coppia viene confrontata in modo indipendente.

Cosa attesta l'indicazione di corrispondenza in Mirror?

1. L'approvazione globale
2. L'origine autentica di entrambi i QR
3. L'uguaglianza letterale dei due elementi della coppia

> **Mostra risposta: L'uguaglianza letterale dei due elementi della coppia**
> Il resto della verifica e la risposta sono ancora in sospeso.

Se una frase seed è stata esposta, cosa succede cambiando la password di Desk?

1. Si revoca l'accesso dell'aggressore
2. Non vengono revocate le chiavi derivate dalla frase seed
3. Si cancellano tutte le copie

> **Mostra risposta: Non vengono revocate le chiavi derivate dalla frase seed**
> Occorre valutare come trasferire il controllo in sicurezza.

Cosa occorre indicare al termine della formazione pratica?

1. Cosa è stato letto, simulato e provato fisicamente, e cosa manca
2. Solo le ore vendute
3. Una promessa di custodia invulnerabile

> **Mostra risposta: Cosa è stato letto, simulato e provato fisicamente, e cosa manca**
> Le prove hanno portate diverse.