CUVEX

CUVEX ACADEMY · 0.1

Aprende. Compreende. Assume o controlo.

Bitcoin e autocustódia, passo a passo. Curso, manual, glossário e exercícios gratuitos, sem registo. Escolhe por onde começar.

Grátis · sem registo

Todas as secções

1. Preparar o teu espaço de aprendizagem
2. Dinheiro digital e o problema da confiança
3. História e limites do Bitcoin
4. Satoshis e cálculos sem erros
5. O teu modelo de ameaças
6. Nós, mineração e consenso
7. UTXO e o troco de uma transação
8. Mempool, confirmações e reorganizações
9. Comissões, tamanho virtual e substituição
10. Redes, endereços e faturas
11. Funções de hash, assinaturas e cifragem
12. Frase-semente, passphrase e palavra-passe
13. Derivação, xpub e descritores
14. Escolher uma carteira e um modelo de custódia
15. Cópias de segurança que permitem a recuperação
16. Conhecer o Original e o BIT
17. Criar uma semente com entropia física
18. Cifrar e decifrar um segredo com o Cuvex
19. Limiares de cifragem e biometria
20. Clonar, conservar e verificar cópias
21. Instalar e proteger o Cuvex Desk
22. Associar criptogramas e organizar as contas WOW
23. Ligar o Mirror ao Desk
24. NFC através do Mirror, USB-C e leitura de códigos QR
25. Prestadores públicos e nó próprio
26. Receber bitcoin e verificar o endereço
27. Etiquetar, congelar e selecionar UTXO
28. Preparar e rever um pagamento
29. Assinar com o Original e com o BIT
30. Finalizar, publicar e resolver problemas
31. O que se pode observar no Bitcoin
32. Separar contextos e gerir o troco
33. Privacidade na rede, Tor e VPN
34. CoinJoin, Payjoin e limites atuais
35. O que nos ensinam incidentes reais

36. Criar uma identidade e verificar contactos de chat
37. Pedir e pagar satoshis pelo chat
38. Partilhar criptogramas de forma consciente
39. Recuperar o chat e compreender os seus metadados
40. Configuração do dia a dia e revisão das permissões
41. Conceber uma carteira multiassinatura
42. Criar convites e fornecer chaves
43. Verificar políticas com o Mirror pela ordem que escolheres
44. Coordenar assinaturas e publicar uma transação multiassinatura
45. Recuperar e alterar uma carteira multiassinatura
46. Atualizar o firmware sem improvisar
47. Perda, avaria e recuperação de emergência
48. Phishing, apoio técnico e fraudes por voz
49. Privacidade, legalidade e registos pessoais
50. Herança, continuidade e simulação anual
51. Preço, poupança e análise fundamental
52. Escolher onde adquirir bitcoin
53. Contas, ordens e custos de execução
54. Velas, indicadores e enviesamentos da análise técnica
55. Margem, futuros e automatização
56. Lightning e outras camadas
57. Taproot, MuSig2 e o futuro pós-quântico
58. Interoperabilidade e independência do fabricante
59. Laboratório técnico com regtest
60. Projeto final e plano de continuidade
61. Manual do aluno
62. Glossário de Bitcoin e autocustódia
63. Verifica o que aprendeste

M01

Preparar o teu espaço de aprendizagem

Objetivo

Preparar o curso, distinguir os três equipamentos e identificar a informação que nunca se comunica ao tutor.

Compreender

Vais aprender a receber, guardar, gastar e recuperar bitcoin segundo o teu próprio critério. O objetivo final é conseguires explicar uma decisão antes de a autorizar. Podes ler o curso sem assistência. A voz oferece explicações, perguntas e acompanhamento e não precisa de ver o teu património nem de controlar os teus dispositivos.

O Cuvex protege os segredos e permite autorizar operações no seu ecrã. O Desk organiza criptogramas, carteiras de observação, pagamentos e a respetiva coordenação no computador. O Mirror serve de ponte local nas operações compatíveis e permite comparar dados. Não assina nem funciona como carteira autónoma. O modelo e a versão determinam o percurso que podes utilizar.

Reserva um ecrã para este curso e outro para o Desk. Mantém o telemóvel e o Cuvex à mão. Se só tiveres um ecrã, alterna entre aplicações e não partilhes o ecrã numa videochamada enquanto introduzes segredos. Uma chamada pode acabar antes de concluíres um exercício. Fazer uma pausa não é um fracasso. Guarda apenas o identificador da lição, o passo que alcançaste e a dificuldade que encontraste.

Nem o formador nem a IA devem receber frases-semente, passphrases BIP39, palavras-passe, a Chave de Chat, PIN, ficheiros privados ou códigos de compra completos. Também não precisam da tua xpub, do teu descritor real ou do teu endereço. Embora estes últimos não permitam gastar, revelam atividade. Descreve as mensagens de erro e usa os dados fictícios do laboratório.

Prática

1. Identifica fisicamente o computador, o telemóvel e o modelo do Cuvex. Anota as versões no teu caderno privado.
2. Separa o ambiente de aprendizagem sem fundos da tua custódia real. Não importes uma frase-semente em uso para praticar.
3. Abre esta lição e localiza a pausa, a ajuda e o glossário. Se alguém te pedir um segredo, interrompe a interação.

Mostra o que aprendeste

Explica quem assina, quem consulta a rede e quem transporta os dados. Podes avançar quando conseguires distinguir estas funções sem ajuda.

Pergunta frequente

Tenho de falar com o tutor todos os dias? Não. Podes estudar por tua conta, repetir uma sessão e pedir ajuda apenas para um procedimento específico. O acesso ao curso e o saldo do serviço de voz são direitos distintos.

Ponto de pausa

L01 concluída, equipamentos identificados e nenhum segredo registado no curso.

O tutor pede-te a frase-semente para verificar se a escreveste corretamente. O que fazes?

1. Dito-a devagar.
2. Interrompo o pedido e verifico a frase-semente apenas no meu ambiente seguro.
3. Envio apenas as primeiras palavras.

> **Ver resposta: Interrompo o pedido e verifico a frase-semente apenas no meu ambiente seguro.**
> Nenhum fragmento de um segredo deve ser comunicado ao serviço de formação.

M01

Dinheiro digital e o problema da confiança

Objetivo

Perceber que problema o Bitcoin procura resolver antes de abrir uma carteira.

Compreender

Um saldo bancário é um registo administrado por uma instituição. A instituição autentica o cliente, decide quais as transferências que processa e mantém a sua contabilidade. Um ficheiro digital comum é fácil de copiar. Enviar uma fotografia não impede que se guarde outra cópia. Para que uma unidade digital funcione como dinheiro, é necessário evitar que seja gasta duas vezes.

O Bitcoin combina regras de validação, assinaturas e um histórico de transações partilhado. Em vez de confiar todo o registo a uma única entidade, permite que participantes independentes verifiquem se uma transação cumpre as regras. A escassez depende de essas regras continuarem a ser verificadas e aceites. Não deriva da imagem de uma moeda nem do preço publicado por uma plataforma de câmbio.

A autocustódia altera a distribuição de responsabilidades. Podes conservar a capacidade de gastar sem pedir autorização a um custodiante. Também podes perdê-la se destruíres todas as cópias de segurança ou assinares um pagamento errado. A liberdade de operar não dispensa segurança, coordenação, ligação à rede para publicar nem o cumprimento das obrigações aplicáveis.

Distingue Bitcoin, a rede e o protocolo, de BTC, a unidade monetária. Outras redes podem usar a palavra blockchain e ter propriedades diferentes. Uma promessa empresarial denominada em «bitcoin» também não equivale a controlar uma saída de Bitcoin com as tuas próprias chaves.

Prática

1. Compara três situações: saldo num banco, saldo numa plataforma de câmbio e uma UTXO controlada pelas tuas chaves.
2. Para cada uma, escreve quem te pode impedir de movimentar o saldo e quem te pode ajudar se te esqueceres de como aceder.
3. Descreve o que aconteceria ao copiar uma fotografia e ao tentar gastar duas vezes a mesma saída.

Mostra o que aprendeste

Explica por palavras tuas a diferença entre um saldo e a capacidade de assinar. Não precisas de decorar termos técnicos.

Pergunta frequente

Na autocustódia desaparecem todos os intermediários? Podes escolher serviços para comprar, consultar ou comunicar. O que importa é o poder que conservam e os dados que recebem.

Ponto de pausa

Guarda a tua comparação das responsabilidades sem nomes de contas reais.

Que problema monetário uma assinatura digital não resolve por si só?

1. Impedir que se tente gastar duas vezes a mesma saída.
2. Comprovar a autorização através de uma chave.
3. Detetar uma alteração da mensagem assinada.

> **Ver resposta: Impedir que se tente gastar duas vezes a mesma saída.**
> As assinaturas autorizam. As regras e o consenso determinam a ordem de gastos incompatíveis.

M01

História e limites do Bitcoin

Objetivo

Situar a origem do Bitcoin e distinguir os factos históricos dos discursos comerciais.

Compreender

O documento de Satoshi Nakamoto foi divulgado em 2008 e a rede entrou em funcionamento em 2009. Propôs dinheiro eletrónico entre pares, recorrendo a ideias anteriores da criptografia, da prova de trabalho e do dinheiro digital. Não é necessário conhecer a identidade civil de Satoshi para verificar o software ou uma transação.

A evolução não se fez por substituição unilateral das regras por uma empresa. Os programadores propõem e analisam alterações, os operadores escolhem o software e os mineiros constroem blocos. Os utilizadores e os serviços decidem o que aceitam. Esta distribuição de decisões pode gerar desacordos. Uma bifurcação e uma atualização de uma aplicação são coisas diferentes.

Um nó pode rejeitar um bloco que infrinja as suas regras, mesmo que tenha sido feito muito trabalho para o produzir. O consenso não é uma simples votação pelo número de computadores. Executar milhares de cópias de um nó não dá automaticamente maior poder de decisão. Do mesmo modo, uma maioria de mineiros não obtém por esse facto a chave privada de um utilizador.

O Bitcoin tem limites deliberados e implica escolhas quanto à capacidade dos blocos, ao custo da verificação, aos tempos variáveis de confirmação e ao registo público. Não oferece reversão administrativa de pagamentos nem confidencialidade integral por predefinição. As camadas e as aplicações procuram satisfazer necessidades específicas em troca de novas dependências.

Prática

1. Coloca numa cronologia o documento inicial, o arranque da rede, a adoção do SegWit e a ativação do Taproot. Confirma as datas nas fontes antes de as publicares.
2. Classifica «uma empresa garante o preço», «um nó valida» e «um mineiro propõe um bloco» como promessa comercial ou função técnica.
3. Explica uma vantagem e um custo da ausência de um administrador que reverta pagamentos.

Mostra o que aprendeste

Distingue uma regra de consenso, uma política local e uma decisão empresarial. A aplicação que utilizas não representa toda a rede.

Pergunta frequente

O software mais recente altera sempre as regras monetárias? Não. As novas versões também corrigem erros, melhoram o desempenho ou alteram políticas locais. Lê as notas da versão e verifica a compatibilidade.

Ponto de pausa

Anota uma propriedade verificável e uma afirmação que exija provas adicionais.

Um bloco contém um gasto sem autorização válida. Uma maioria de mineiros torna-o válido?

1. Sim, se ultrapassar os 51 %.
2. Só se a plataforma de câmbio o anunciar.
3. Não para um nó que aplique regras que o rejeitam.

> **Ver resposta: Não para um nó que aplique regras que o rejeitam.**
> Compara-se o trabalho acumulado entre históricos válidos de acordo com as regras do nó.

M01

Satoshis e cálculos sem erros

Objetivo

Converter BTC em satoshis e vice-versa, e conferir montantes sem depender de uma cotação.

Compreender

Um BTC equivale a 100.000.000 de satoshis. «sat» é uma unidade e não uma moeda diferente. Na cadeia de base, os montantes são contabilizados em números inteiros de satoshis. 0,001 BTC correspondem a 100.000 sat e 0,00001000 BTC a 1.000 sat. O separador decimal apresentado depende do idioma da interface. Não acrescentes zeros a olho.

Uma cotação converte BTC numa moeda como o EUR ou o USD num determinado momento. Não altera o número de satoshis que controlas. Se tiveres 100.000 sat e o preço mudar, o número de satoshis mantém-se. No Desk, a cotação é uma referência com fonte e data. Um dado desatualizado pode levar a uma decisão económica errada mesmo com o saldo em BTC correto.

Num pagamento, distingue o montante para o destinatário, a comissão de rede e a despesa total. Se enviares 50.000 sat com uma comissão de 600 sat, saem da tua carteira 50.600 sat, salvo outras saídas próprias. «Enviar o total» normalmente calcula um montante líquido para o destinatário inferior ao saldo disponível, porque é preciso pagar a comissão.

Os exemplos do curso são exercícios de aritmética, não cotações de mercado nem comissões recomendadas. Antes de assinar, verifica a unidade, a rede, o destinatário e o custo total no ecrã correspondente. A voz pode dizer «cinquenta mil satoshis» enquanto se mostra «50.000 sat». Uma transcrição duvidosa nunca deve determinar o montante.

Prática

1. Converte 250.000 sat em BTC: 0,0025 BTC. Converte 0,00025000 BTC em sat: 25.000 sat.
2. Calcula o custo de enviar 75.000 sat com uma comissão de 900 sat: 75.900 sat.
3. No simulador, usa 120.000 sat, um envio de 70.000 e uma comissão de 1.000. Confirma um troco de 49.000 sat.

Mostra o que aprendeste

Lê um montante em BTC e em sat e explica qual inclui a comissão. Em caso de dúvida, faz uma pausa na operação.

Pergunta frequente

Preciso de comprar um bitcoin inteiro? Não. Podes comprar uma fração, sujeita aos montantes mínimos e aos custos do prestador.

Ponto de pausa

Conserva apenas os teus resultados do exercício.

Tens 80.000 sat e queres enviar o total com uma comissão de 1.200 sat. Quanto recebe o destinatário?

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

> **Ver resposta: 78.800 sat.**
> Neste exemplo sem outras saídas, o destinatário recebe o saldo que se pode gastar menos a comissão.

M01

O teu modelo de ameaças

Objetivo

Escolher medidas proporcionais contra perda, roubo, engano e exposição de dados.

Compreender

Segurança é conservar a capacidade de agir segundo a tua intenção. Privacidade é controlar quem conhece os teus dados e as tuas relações. Disponibilidade é conseguires aceder quando precisas. Uma caixa inacessível a todos também pode ser inacessível para ti. Uma cópia muito cómoda pode expor demasiada informação.

Identifica os ativos, os adversários e os acidentes. Os ativos incluem chaves, cópias de segurança, histórico, localização das cópias e identidade dos contactos. Os riscos incluem malware, phishing, incêndio, esquecimento, coação, avaria, morte e erros teus. Não há uma ferramenta que reduza todos estes riscos.

Usa uma matriz simples com probabilidade aproximada, impacto e medida concreta. Uma palavra-passe longa dificulta as tentativas de adivinhação, mas não corrige um destinatário fraudulento que tu próprio autorizaste. Duas cópias no mesmo saco não resolvem a perda desse saco. Uma carteira multiassinatura cujos equipamentos e cópias de segurança são controlados por uma só pessoa pode manter um ponto comum de falha.

O curso e o tutor também integram o modelo. Compras, chamadas, tempos de ligação e progresso podem gerar metadados. O minissite não deve pedir endereços nem saldos para personalizar uma aula. A ausência de um registo convencional no Desk ou no Mirror não significa que a loja, o prestador do serviço de voz ou um terceiro consultado desconheçam a tua atividade.

Prática

1. Escreve os teus três riscos mais importantes sem indicar valores patrimoniais nem localizações exatas.
2. Para cada um, escolhe medidas de prevenção, deteção e recuperação. Por exemplo, para a perda de um cartão, duas cópias separadas, um inventário e um teste de restauro.
3. Distingue quem ou que sistema pode observar a compra, a chamada, a consulta de saldo e a transação pública.

Mostra o que aprendeste

Justifica como a tua próxima medida resolve um risco concreto. Não acumules complexidade que não possas manter ou explicar aos teus herdeiros.

Pergunta frequente

Mais dispositivos significam sempre mais segurança? Só se reduzirem dependências comuns e puderes testar a recuperação. Mais equipamentos também exigem manutenção e aumentam as possibilidades de confusão.

Ponto de pausa

Guarda o plano na tua documentação privada e regista no curso apenas «modelo de ameaças revisto».

Que medida reduz melhor o risco de perder todas as cópias num incêndio local?

1. Mudar a cor do cartão.
2. Pôr duas cópias na mesma gaveta.
3. Manter cópias verificadas em locais com riscos independentes.

> **Ver resposta: Manter cópias verificadas em locais com riscos independentes.**
> A redundância deve resistir ao mesmo incidente que ameaça o original.

M02

Nós, mineração e consenso

Objetivo

Explicar o que os nós validam e qual o contributo da mineração.

Compreender

Um nó completo recebe blocos e transações, verifica regras e mantém a sua visão da cadeia. Não precisa de confiar no saldo anunciado por uma página. A mineração consiste em propor blocos mediante prova de trabalho. Os mineiros selecionam transações válidas e competem para encontrar um bloco admissível.

A prova de trabalho torna dispendioso reescrever o histórico. Quando existem alternativas válidas, o que conta é o trabalho acumulado. Contar blocos sem considerar a dificuldade não basta. Os intervalos entre blocos variam. Dez minutos é a média pretendida e não uma hora marcada para o próximo pagamento.

A recompensa da mineração combina o subsídio com as comissões. O subsídio diminui segundo um calendário definido pela altura do bloco. As comissões dependem das transações incluídas. Pagar mais numa transferência não torna válida uma assinatura incorreta. A segurança económica e o custo de um ataque não tornam um pagamento recente matematicamente irreversível.

Um nó próprio permite verificar e reduz a necessidade de enviar consultas a terceiros. Continua a ser necessário proteger o sistema operativo, o acesso e a ligação. Um nó ligado mas não sincronizado, ou associado a uma aplicação que consulta outro servidor, não oferece automaticamente essas vantagens.

Prática

1. Atribui estas tarefas: verificar a assinatura, escolher as transações de um bloco, guardar a tua frase-semente e decidir se aceitas um pagamento.
2. Explica por que razão «o mineiro guarda os meus bitcoins» é uma descrição incorreta.
3. Numa rede de laboratório, observa a altura e a sincronização. Não publiques credenciais RPC.

Mostra o que aprendeste

Descreve a diferença entre verificar e propor. Podes usar uma analogia, mas termina por indicar a função técnica correta.

Pergunta frequente

Preciso de minerar para usar o Bitcoin? Não. Também não precisas de ter um nó próprio para começar, embora devas saber até que ponto tens de confiar no teu prestador.

Ponto de pausa

Anota o tipo de prestador do laboratório, sem indicar um URL privado.

O que dá um nó completo bem configurado ao seu utilizador?

1. A possibilidade de verificar as regras da cadeia que aceita.
2. A possibilidade de recuperar qualquer chave perdida.
3. Uma garantia de subida de preço.

> **Ver resposta: A possibilidade de verificar as regras da cadeia que aceita.**
> A validação e a custódia são funções diferentes.

M02

UTXO e o troco de uma transação

Objetivo

Interpretar uma transação como consumo e criação de saídas.

Compreender

Uma UTXO é uma saída de uma transação anterior que ainda não foi gasta. Uma carteira calcula o saldo identificando as saídas que pode controlar. Não existe uma conta universal a debitar como num registo bancário. Uma entrada referencia uma saída anterior pelo identificador da transação e pela posição.

Uma UTXO é sempre gasta por inteiro. Se precisares de pagar menos do que o seu valor, normalmente crias uma saída para o destinatário e uma saída de troco que controlas. Com uma entrada de 120.000 sat, 70.000 para o destinatário e uma comissão de 1.000, o troco é 49.000. A soma das entradas tem de ser igual à soma das saídas mais a comissão.

Um endereço não é uma UTXO. Pode receber várias saídas e também não corresponde necessariamente a uma pessoa. O identificador da transação pode ser público, mas associá-lo à tua identidade ou explicar a quem pertence cada saída acrescenta informação que a cadeia, por si só, não fornece.

Esta estrutura afeta a privacidade. Combinar entradas pode sugerir controlo comum e o troco pode ligar pagamentos futuros. A inferência não é prova universal, porque existem transações colaborativas. O controlo de moedas (coin control) consiste em escolher as saídas a gastar, conhecendo as consequências de as combinar.

Prática

1. Desenha três entradas fictícias de 40.000, 60.000 e 200.000 sat. Paga 70.000 com uma comissão de 1.000 usando apenas as duas primeiras.
2. Confirma que o troco é de 29.000 sat e que a terceira entrada não participa.
3. Repete usando apenas 200.000. O troco seria de 129.000. Compara o custo potencial e as ligações sem presumir que os tamanhos são iguais.

Mostra o que aprendeste

Localiza a entrada, o destinatário, o troco e a comissão no diagrama do curso. Se não conseguires identificar uma saída, não assines uma operação real.

Pergunta frequente

Tudo o que volta para a minha carteira é troco? Não. Pode ser uma transferência para outro endereço teu. A classificação exige conhecer a política e a derivação, e não tentar adivinhar pelo montante.

Ponto de pausa

Guarda o esquema fictício, nunca uma captura de ecrã do teu património.

Uma entrada de 100.000 sat gera uma saída de 30.000 e outra de 69.200. Qual é a comissão?

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

> **Ver resposta: 800 sat.**
> A diferença entre 100.000 e 99.200 é de 800 sat.

M02

Mempool, confirmações e reorganizações

Objetivo

Distinguir uma transação preparada, publicada e confirmada.

Compreender

A mempool é o conjunto local de transações não confirmadas que um nó conserva de acordo com a sua política. Não existe uma mempool única e idêntica em todo o mundo. Se um explorador mostra um pagamento, significa que esse serviço o conhece. Não garante que todos os nós o aceitem ou que seja confirmado num prazo específico.

Preparar uma PSBT não publica nada. Assinar produz a autorização. Finalizar constrói a transação que pode ser difundida. Publicar é tentar transmiti-la. A confirmação indica que foi incluída num bloco da cadeia aceite pela tua fonte de verificação. Uma segunda confirmação acrescenta outro bloco por cima, não uma segunda assinatura do destinatário.

Podem ocorrer reorganizações que alteram parte da cadeia. Uma operação pode perder confirmações ou voltar ao estado pendente. Para pagamentos com maior exposição, as partes costumam exigir mais confirmações. Nenhum número elimina todos os riscos para todos os montantes e situações.

Se o Desk mostrar um estado guardado, verifica a data de sincronização. «Confirmado» num registo antigo não descreve necessariamente o estado atual. Se um envio não aparecer, conserva o identificador local e verifica a publicação e o histórico antes de o preparares de novo. Repetir por impaciência pode criar outro pagamento válido.

Prática

1. Ordena estes cartões: rascunho, PSBT, assinatura, transação final, difusão, inclusão num bloco.
2. Simula uma perda de ligação logo após a publicação. Decide o que verificar antes de voltares a pagar.
3. Explica a um comerciante por que motivo uma mensagem de chat a dizer «pago» não substitui a verificação na rede.

Mostra o que aprendeste

Consegues indicar o estado de uma operação, a fonte e a data da informação sem a confundires com uma garantia.

Pergunta frequente

Fechar o Desk cancela uma transação publicada? Não. Outros nós e participantes podem conservá-la. Cancelar um rascunho local tem um alcance diferente.

Ponto de pausa

Anota o estado da simulação. Não forneças identificadores reais ao tutor.

O computador perde a ligação logo após clicares em publicar. O que fazes primeiro?

1. Preparo o mesmo pagamento de raiz.
2. Apago a carteira.
3. Volto a ligar e verifico a transação e as respetivas entradas.

> **Ver resposta: Volto a ligar e verifico a transação e as respetivas entradas.**
> A ausência de resposta não demonstra que a difusão falhou.

M02

Comissões, tamanho virtual e substituição

Objetivo

Estimar custos, interpretar sat por vbyte e compreender RBF e CPFP.

Compreender

A comissão de rede corresponde à diferença entre entradas e saídas. A sua competitividade expressa-se habitualmente em sat/vB, satoshis por byte virtual. Não depende diretamente do valor económico enviado. Muitas entradas podem encarecer um pagamento pequeno, enquanto um pagamento grande com poucas entradas pode ocupar menos espaço.

Num exemplo de 200 vB a 5 sat/vB, a comissão é de 1.000 sat. Antes da assinatura, só tens uma estimativa porque o tamanho final pode depender das assinaturas e da estrutura. O Desk oferece velocidades indicativas e permite definir a taxa manualmente. A indicação «rápida» não promete confirmação a uma hora exata.

RBF é uma política de substituição de transações não confirmadas em determinadas condições. Permite propor um gasto incompatível com uma comissão superior. As políticas dos nós evoluíram e um sinal de não substituição não deve ser considerado garantia de recebimento. Uma substituição exige nova revisão e as assinaturas necessárias.

CPFP consiste em gastar uma saída da transação pendente para tornar atrativo o conjunto das transações mãe e filha. Exige controlo de uma saída que se possa gastar, cumprimento das políticas e pagamento do respetivo custo. É um conceito do Bitcoin. Não se presume que a versão do Cuvex do aluno tenha um botão CPFP.

«Dust» é uma saída demasiado pequena segundo as políticas aplicáveis e os custos estimados para a gastar. Não há um limiar universal para todos os tipos de script. Evita ensinar um valor fixo como regra de consenso. Se o troco não for viável, revê o montante, as entradas ou a transferência da totalidade do saldo e a comissão efetiva.

Prática

1. Calcula 180 vB a 8 sat/vB: 1.440 sat. Verifica se excede o orçamento do laboratório.
2. Compara uma entrada com dez entradas. Explica por que razão o montante enviado é insuficiente para estimar o custo.
3. Simula uma transação pendente e decide entre esperar, usar RBF ou estudar CPFP sem presumir compatibilidade automática.

Mostra o que aprendeste

Justifica a taxa, a comissão absoluta e o custo em relação ao montante enviado. Rejeita uma comissão que não compreendas.

Pergunta frequente

O RBF cancela seguramente o pagamento anterior? Não. As versões competem até à confirmação e a propagação é importante. Não entregues bens com base numa promessa de cancelamento.

Ponto de pausa

Guarda a decisão do exercício e a justificação.

Qual é a comissão para 250 vB a 4 sat/vB?

1. 1.000 sat.
2. 254 sat.
3. 4 % do montante enviado.

> **Ver resposta: 1.000 sat.**
> O tamanho virtual multiplicado pela taxa dá a comissão estimada.

M02

Redes, endereços e faturas

Objetivo

Reconhecer a rede, o formato do endereço e as instruções de pagamento antes de copiar ou digitalizar.

Compreender

A mainnet movimenta bitcoin com valor económico. As redes de teste servem para desenvolver e aprender, mas não são intercambiáveis. A regtest é uma rede local controlada por quem monta o laboratório. A signet e a testnet têm regras e ecossistemas próprios. Uma função de assinatura única na signet não implica que o perfil multiassinatura do Cuvex suporte essa rede.

Os endereços codificam condições de receção. Na mainnet há formatos que começam por 1, 3, bc1q ou bc1p. O prefixo ajuda a reconhecer uma família, mas não verifica o destinatário, não garante a compatibilidade de quem assina nem substitui a validação completa do formato.

Um QR é um suporte visual. Pode transportar um endereço, uma fatura, um descritor ou texto malicioso. Lê-lo não autentica o autor. Uma ligação bitcoin: pode incluir montante e mensagem. A BIP321 é a referência moderna que substitui a BIP21. Na implementação analisada, o Desk mantém a terminologia e a compatibilidade BIP21. Uma melhoria da norma, por si só, não alarga o que a aplicação interpreta.

Uma fatura Lightning não é um endereço on-chain. Pode incluir um prazo de validade e outros campos. Não a coloques num envio na cadeia se a aplicação não oferecer um procedimento compatível. Um token denominado BTC noutra rede também não é automaticamente bitcoin nativo.

Prática

1. Classifica exemplos identificados do curso sem usar endereços com fundos que se possam gastar: endereço, URI bitcoin:, fatura Lightning e descritor.
2. Identifica a rede selecionada no laboratório. No perfil multiassinatura do Cuvex analisado, as redes compatíveis são mainnet/regtest.
3. Compara por um canal autenticado o texto completo pedido pelo destinatário antes de uma operação real.

Mostra o que aprendeste

Consegues rejeitar um pedido cuja rede ou modalidade desconheças e explicar o que precisas de verificar.

Pergunta frequente

Posso enviar BTC por qualquer rede apresentada por uma plataforma de câmbio? Não. A rede de levantamento deve coincidir com a de receção efetiva. Não escolhas apenas pela comissão mais baixa.

Ponto de pausa

Regista apenas o tipo de rede de aprendizagem.

Um endereço de receção bc1 não autoriza por si só o levantamento de BTC por uma rede de tokens diferente. O que falta?

1. Alterar o nome alternativo do destinatário.
2. Confirmar que o levantamento utiliza Bitcoin on-chain e que todos os dados coincidem.
3. Introduzir a frase-semente na plataforma de câmbio.

> **Ver resposta: Confirmar que o levantamento utiliza Bitcoin on-chain e que todos os dados coincidem.**
> O ativo, a rede e o método de receção têm de ser compatíveis.

Funções de hash, assinaturas e cifragem

Objetivo

Distinguir integridade, autorização e confidencialidade.

Compreender

Um hash transforma dados numa impressão digital de comprimento fixo. Comparar uma impressão digital conhecida ajuda a detetar alterações. Não cifra o ficheiro nem identifica por si só quem o publicou. Se descarregares o ficheiro e o hash da mesma página comprometida, o atacante poderá ter substituído ambos.

Uma chave privada permite criar assinaturas; a chave pública correspondente permite verificá-las. A assinatura vincula uma autorização a uma mensagem específica de acordo com o algoritmo e suas regras. Não esconde o conteúdo assinado. Em Bitcoin, uma assinatura válida é uma parte das condições necessárias para gastar uma saída.

A criptografia busca que um conteúdo só possa ser lido com a capacidade adequada. A criptografia autenticada adiciona deteção de alterações. No ecossistema Cuvex existem criptogramas que protegem segredos, transações assinadas que autorizam despesas e canais cifrados que transportam mensagens. Não são objetos equivalentes, embora todos usem criptografia.

Uma palavra-passe humana geralmente passa por uma função de derivação antes de ser usada como chave criptográfica. AES-256 descreve o algoritmo e o tamanho da chave, mas não transforma uma palavra-passe previsível numa escolha forte. A geração, implementação, armazenamento, ecrã e recuperação fazem parte da segurança total.

Também não se deduz que um QR seja seguro porque parece complexo. É preciso saber o que contém, quem o produziu e o que a aplicação vai fazer com ele. Antes de aceitar uma ação, peça ao tutor que explique sua finalidade sem solicitar a informação privada.

Prática

1. Associa «detetar uma alteração num ficheiro», «ocultar uma frase-semente» e «autorizar um pagamento» a hash, cifragem e assinatura.
2. Muda uma letra de um texto fictício e observa que seu hash muda; não use segredos para esta demonstração.
3. Explica por que uma transação pode ser pública e ser assinada ao mesmo tempo.

Mostra o que aprendeste

Consegues explicar que garantia procuras e que mecanismo a proporciona, sem usar «cifrado» como sinónimo de tudo o que é seguro.

Pergunta frequente

Um hash de firmware garante que não há erros? Não. Identifica bytes se a referência é fiável. Uma auditoria, uma assinatura de fabricante e uma prova física respondem a perguntas diferentes.

Ponto de pausa

Mantém as três correspondências do exercício.

Qual destes mecanismos oculta o conteúdo de um segredo?

1. Publicar o nome do ficheiro.
2. Assiná-lo sem o cifrar.
3. Cifrá-lo corretamente com uma chave protegida.

> **Ver resposta: Cifrá-lo corretamente com uma chave protegida.**
> Uma assinatura ou uma impressão digital, por si só, não garante a confidencialidade.

Frase-semente, passphrase e palavra-passe

Objetivo

Evitar a confusão entre as diferentes credenciais do sistema.

Compreender

Uma mnemónica BIP39 representa a entropia e uma soma de verificação por meio de palavras de um dicionário. Os comprimentos normalizados são 12, 15, 18, 21 ou 24 palavras. Escolher uma frase fácil de recordar, a letra de uma canção ou palavras ao acaso segundo o teu critério não equivale a uma geração segura. A soma de verificação deteta alguns erros. Não prova quem criou a semente nem que ninguém mais a conheça.

A passphrase BIP39 participa na derivação da semente binária. Uma passphrase diferente pode abrir uma carteira completamente diferente e aparentemente vazia. Não aparece necessariamente uma mensagem a indicar «passphrase incorreta». Não tem de ser uma palavra do dicionário nem é literalmente uma vigésima quinta palavra.

A palavra-passe do criptograma Cuvex protege o segredo armazenado. A palavra-passe do Desk protege o armazenamento local do computador. O PIN de ligação permite uma sessão de comunicação. A Chave de Chat permite recuperar a identidade usada nas mensagens. Nenhuma destas credenciais deve ser confundida com a frase-semente. Conhecer uma não implica conseguir reconstruir as restantes.

Guardar a frase-semente e a passphrase juntas num criptograma pode facilitar a recuperação, mas elimina a separação entre ambas perante quem o consiga decifrar. Mantê-las separadas exige mais de ti e dos teus herdeiros. A decisão deve ser documentada e testada. Não a tomes só porque o tutor considera uma opção «mais avançada».

Prática

1. Cria cinco cartões de papel sem valores secretos: frase-semente, passphrase, palavra-passe do Cuvex, palavra-passe do Desk e Chave de Chat.
2. Escreve o que cada credencial permite recuperar e o que perderias se te esquecesses dela.
3. Desenha uma prova numa carteira vazia. Introduz as palavras e a passphrase em privado e informa o tutor apenas do resultado.

Mostra o que aprendeste

Explica por que o curso nunca deve pedir uma palavra-passe para «validar» teu aprendizado. Identifica o segredo que o teu procedimento de recuperação exige.

Pergunta frequente

Posso repor a passphrase por email? Não existe esse mecanismo no BIP39. Um fornecedor custodial pode ter recuperação de conta, mas é outro modelo.

Ponto de pausa

Regista «credências diferenciadas», sem escrever os seus valores.

Alteras uma letra da passphrase BIP39 e vês saldo zero. Qual é a interpretação correta?

1. Pode ser outra carteira válida, derivada de outra passphrase.
2. A rede apagou os teus fundos.
3. O Desk deve adivinhar a passphrase original.

> **Ver resposta: Pode ser outra carteira válida, derivada de outra passphrase.**
> Uma passphrase diferente pode produzir outra carteira sem indicar um erro.

M03

Derivação, xpub e descritores

Objetivo

Compreender como se descreve uma carteira sem entregar capacidade de gasto.

Compreender

Uma carteira hierárquica deriva muitas chaves de uma raiz. Uma rota indica qual ramo é usado. Em mainnet, o BIP84 geralmente usa m/84'/0'/0' para a primeira conta SegWit de assinatura única; o BIP48 P2WSH usa m/48'/0'/0'/2' na primeira conta multiassinatura. A plica indica derivação reforçada. Mudar conta, rede ou tipo de script pode dar outros endereços da mesma mnemónica.

Uma xpub é uma chave pública estendida que permite derivar certas chaves públicas descendentes. Não é uma palavra-passe de gasto, mas pode permitir que observes uma família de endereços. A pegada mestre é um identificador curto útil para relacionar registos; não garante identidade por si só nem evita colisões.

Um descritor expressa como construir scripts e endereços: tipo de script, chaves, origens e derivações. Um descritor watch-only com chaves públicas permite observar, não assinar. A palavra «descritor» não garante que contenha apenas informação pública. Alguns formatos podem incluir chaves privadas. Nunca coloques uma descrição real no curso.

Para recuperar uma multiassinatura geralmente é necessário a política completa, não apenas as palavras de um dos signatários. Conserva um limiar, participantes, xpubs, rotas, rede, tipo de script e dados de descoberta. A soma de verificação do descritor ajuda a detetar erros de transcrição; não autentica seus participantes.

Prática

1. Lê uma rota fictícia e explica propósito, moeda, conta e ramo. Não introduzas chaves reais.
2. Distinguir o endereço de receção, o xpub de participante e o descritor completo.
3. Faz uma ficha privada de recuperação com nomes de campos vazios e localização documental separada.

Mostra o que aprendeste

Consegues explicar por que razão uma carteira vazia após o restauro não prova a perda dos fundos. É necessário verificar a rede, a passphrase, o script, a conta, o caminho de derivação e a descoberta de endereços.

Pergunta frequente

Um xpub pode ser publicado sem consequências? Não dá por si só a capacidade normal de gastar, mas expõe privacidade e pode aumentar outros riscos em combinações criptográficas particulares.

Ponto de pausa

Mantém a ficha sem valores sensíveis no curso.

Que informação pode faltar ao tentar recuperar uma carteira multiassinatura só com uma frase-semente?

1. A cor do dispositivo.
2. A política e as chaves públicas dos restantes participantes.
3. A palavra-passe de uma rede social.

> **Ver resposta: A política e as chaves públicas dos restantes participantes.**
> Para reconstruir os scripts é necessária a política completa, além do número de chaves privadas exigido pelo limiar.

M03

Escolher uma carteira e um modelo de custódia

Objetivo

Compare ferramentas por funções, confiança e recuperação.

Compreender

Uma carteira é um conjunto de ferramentas para descrever, observar e, quando apropriado, autorizar despesas. Uma carteira quente mantém a capacidade de assinatura num ambiente ligado. Um dispositivo de assinatura isolado procura manter os segredos separados do equipamento que consulta a rede. Uma carteira watch-only conserva informação pública suficiente para observar e preparar, mas precisa de outro sistema para assinar.

Em custódia de terceiros, uma conta pode representar um direito em relação a uma empresa. Em autocustódia manténs a capacidade técnica de gasto, de forma individual ou partilhada. A recuperação por e-mail e o poder de bloquear uma retirada geralmente refletem o primeiro modelo. Não deves avaliar ambas as opções com o mesmo suposto de responsabilidade.

Compara suporte de rede e script, verificação de ecrã, cópias, atualização, interoperabilidade, manutenção, consultas de fornecedores e clareza de erros. Uma lista de moedas ou um acabamento físico não é suficiente. Um dispositivo de assinatura também não evita que aceites um endereço errado se não o revisares.

O Cuvex separa a proteção dos segredos em criptogramas das funções de organização e consulta no Desk. Este modelo exige que o criptograma e seus meios de desbloqueio sejam mantidos. A proteção contra a perda do dispositivo não implica recuperação se todas as cópias ou palavras-passe desaparecerem também. Aprende o processo completo antes de transferir património.

Prática

1. Compara Cuvex com uma carteira quente e uma troca numa matriz: quem assina, quem vê consultas, quem pode recuperar acesso e o que acontece ao fechar a empresa.
2. Escolhe dois critérios que deves verificar com evidência e não com publicidade.
3. Certifica-se de que o ambiente de prática não partilha chaves com o teu dinheiro real.

Mostra o que aprendeste

Justifica uma escolha para um caso concreto sem declarar uma ferramenta invulnerável.

Pergunta frequente

Uma carteira de hardware faz todas as transações privadas? Não. Protege principalmente a capacidade de assinatura e parte da revisão; a cadeia, consultas e contrapartes continuam gerando informações.

Ponto de pausa

Mantém tua matrícula de critérios sem nomes de contas.

O que pode fazer uma carteira watch-only configurada corretamente com chaves públicas?

1. Observar e preparar operações sem as poder assinar por si só.
2. Alterar uma frase-semente perdida.
3. Garantir o anonimato.

> **Ver resposta: Observar e preparar operações sem as poder assinar por si só.**
> Observar e autorizar são capacidades separáveis.

Cópias de segurança que permitem a recuperação

Objetivo

Desenhar uma cópia completa e demonstrar recuperação antes de depender dela.

Compreender

Um cópia de segurança útil recupera uma capacidade, não apenas um ficheiro. Para uma de assinatura única pode exigir mnemônica, passphrase e dados de derivação. Para uma multiassinatura exige também política e suficientes signatários. Para o Desk pode ser necessário uma cópia cifrada e sua palavra-passe. Para o chat, recuperar identidade não equivale a recuperar mensagens históricas.

A redundância protege contra a perda acidental. A separação protege contra o comprometimento simultâneo dos elementos. Duas cópias em diferentes suportes e locais podem reduzir falhas correlacionadas. Cada cópia adicional também precisa de controlo de acesso, inventário e revisão. Os nomes de ficheiro e etiquetas não devem revelar património nem facilitar a localização de todos os componentes.

Um teste deve confirmar uma direção previamente verificada e, num ambiente de aprendizagem, a capacidade de assinar uma operação controlada. Ver que o ficheiro está aberto não demonstra que pertence à carteira correta. Também não testes uma cópia de segurança introduzindo a tua frase-semente em uso num computador qualquer.

Documenta o que cobre e o que exclui cada cópia. Mudar a palavra-passe atual não altera automaticamente as cópias antigas. Se uma palavra-passe anterior for exposta, esses suporte continuarão afectados. Eliminar um ficheiro em armazenamento moderno também não garante a eliminação de todas as suas cópias ou versões.

Prática

1. Completa uma tabela privada: objeto, conteúdo, palavra-passe associada, localização independente, data de teste e responsável.
2. Restaura uma cópia de aprendizagem num ambiente separado. Verifica rede, primeira direção e derivação.
3. Simula a perda do computador e depois a do dispositivo. Identificar qual procedimento muda.

Mostra o que aprendeste

Podes recuperar teu cenário de testes sem ajuda improvisada e explicar quais informações ainda faltariam para outro cenário.

Pergunta frequente

A cópia global de Desk é uma cópia de tudo? Não deve ser assumido. Na base analisada, histórico e sessões de chat não estão incluídos. A política multiassinatura e as chaves privadas têm funções diferentes.

Ponto de pausa

Regista a data e o resultado da prova; nunca o conteúdo da cópia.

Alteras a palavra-passe do Desk. O que acontece a uma cópia de segurança anterior?

1. Atualiza-se sozinha.
2. Perde automaticamente a cifragem.
3. Conserva a proteção e a palavra-passe com que foi criada.

> **Ver resposta: Conserva a proteção e a palavra-passe com que foi criada.**
> As cópias anteriores são objetos independentes.

M04

Conhecer o Original e o BIT

Objetivo

Escolha o caminho certo de acordo com o dispositivo e sua versão.

Compreender

O Original utiliza cartões NFC para transportar criptogramas e operações compatíveis. O Bluetooth intervém na sua atualização. Seu USB-C é usado como alimentação no modelo documentado. O BIT utiliza USB-C para trocar ficheiros e acrescenta biometria para os criptogramas que a exigem. Não mudes as instruções NFC ou Bluetooth de Original para BIT.

No dispositivo encontrarás funções para cifrar, decifrar, criar carteiras e assinar, além de ajustes. Original incorpora clonado de cartões; BIT trabalha com ficheiros de suporte USB. Os rótulos, idiomas e acessos podem variar por versão. No BIT, a nova opção «Verificar políticas» conduz ao procedimento compatível e não altera quem autoriza a operação.

A referência editorial analisada é Original 1.2.2 Final, BIT 1.2.3 Final, Desk beta.9.21 e Mirror beta.12.12. São referências de fontes: a assinatura, distribuição e aceitação física de cada combinação devem ser verificadas com o equipamento. Não substituas teu firmware por um binário sem assinatura incluído num pacote de engenharia.

Antes de utilizar o equipamento, verifica a proveniência, os selos, o aspeto e a versão. A traçabilidade e uma assinatura de atualização ajudam com ameaças concretas, mas não substituem todas as verificações. Se observares uma manipulação ou uma versão inesperada, pare a inicialização e consulte suporte por um canal que verificaste.

Prática

1. Identifica o teu modelo e registra uma versão visível sem fotografar segredos.
2. Localiza cifrar, decifrar, criar carteiras, PSBT e ajustes. Não inicies um excluído ou uma atualização para explorar menus.
3. Escolhe no curso o percurso correspondente ao Original ou ao BIT. Mantém essa seleção durante a prática.

Mostra o que aprendeste

Explica como uma operação de teu modelo entra e sai e que suporte deves proteger de sobrescrições.

Pergunta frequente

O BIT é automaticamente mais seguro para qualquer pessoa? Os modelos oferecem decisões operacionais diferentes. A resposta depende de ameaças, recuperação e uso correto.

Ponto de pausa

Mantém o modelo e a versão no teu catálogo local; o curso só precisa do modelo escolhido.

Tens um BIT e um guia pede-te que graves um cartão NFC com o próprio dispositivo. O que fazes?

1. Verifico se o guia corresponde ao meu modelo e uso o procedimento USB compatível.
2. Forço a atualização do Original.
3. Envio a frase-semente para o telemóvel.

> **Ver resposta: Verifico se o guia corresponde ao meu modelo e uso o procedimento USB compatível.**
> As instruções devem corresponder ao meio de transporte de dados realmente utilizado pelo modelo.

Criar uma semente com entropia física

Objetivo

Entender a geração e ensaiar o fluxo sem converter dados do curso em chaves próprias.

Compreender

A entropia é imprevisibilidade. Alguns dados podem trazer entropia se forem adequados, a ordem é fixada antes de lançar e o algoritmo de conversão é correto. Quando o procedimento rejeita um resultado, é preciso repetir o lançamento exatamente como indicado. Substituir o resultado pelo número máximo ou escolher outra palavra introduz enviesamento.

O fluxo Cuvex analisado combina uma moeda e quatro dados. A função de conversão multiplica o valor da moeda por 1.296 e soma o número em base seis formado pelos valores dos quatro dados depois de se subtrair um a cada valor. Aceita índices de 0 a 2.047. Se o resultado cair fora do dicionário, tens que repetir a moeda e os quatro dados. Manter o resultado da moeda e voltar a lançar apenas os dados introduz enviesamento. É isso que descreve o código-fonte analisado. O ecrã e o procedimento completo são validados em cada versão de firmware distribuída.

Não é equivalente a escolher palavras favoritas. Não convertas uma demonstração pública em material para custodiar dinheiro. Qualquer semente que apareça em material didático é considerada conhecida. A palavra final e a sua verificação devem ser produzidos através do algoritmo completo do dispositivo, sem completar uma mnemónica à mão.

Prepara um espaço sem câmeras, assistentes de voz ativos perto, gravação de ecrã ou pessoas observando. O tutor deve deter-se durante a entrada e revisão do segredo. Podes explicar antes e avaliar depois por meio de perguntas sobre o processo, sem ouvir os resultados dos lançamentos nem as palavras.

Depois de gerar, precisas verificar a cópia de segurança, cifrá-lo de acordo com o modelo e provar a recuperação de uma carteira vazia. Um endereço de verificação ajuda a confirmar a consistência sem expor a semente ao computador. Se o fluxo aceitar valores que contradizem as instruções ou exibir palavras inesperadas, pare de usar e registra apenas versão, ecrã e erro.

Prática

1. No ensaio, siga os passos do dispositivo com material sem fundos. Fica na ordem dos dados e não mude os resultados.
2. Repete as entradas rejeitadas segundo o ecrã, sem corrigir para que elas encaixem.
3. Revisa o conteúdo em privado, crie cópia e confirme que podes reconstruir o mesmo carteira de aprendizagem.

Mostra o que aprendeste

Explica por que entropia física, conversão correta e segredo do resultado são três requisitos diferentes.

Pergunta frequente

Posso contar as minhas tiras para a IA para que comprove o algoritmo? Não para uma semente que vais usar. A assistência trabalha com exemplos sintéticos diferentes.

Ponto de pausa

Finaliza num estado seguro do dispositivo; não deixe uma semente visível durante o descanso.

O firmware rejeita um resultado dos dados. Que ação respeita o procedimento?

1. Escolher manualmente uma palavra.
2. Repetir segundo a indicação do dispositivo, sem enviesar o resultado.
3. Reduzir o número até ser aceite.

> **Ver resposta: Repetir segundo a indicação do dispositivo, sem enviesar o resultado.**
> A rejeição de resultados faz parte da conversão da entropia. Não se devem substituir os resultados arbitrariamente.

M04

Cifrar e decifrar um segredo com o Cuvex

Objetivo

Criar um criptograma de aprendizagem e verificar sua recuperação.

Compreender

Escolhe o tipo de conteúdo correto: BIP39, SLIP39, Monero ou texto, se estiver disponível no teu procedimento. São formatos diferentes. Cifrar um texto SLIP39 não torna a Cuvex um signatário de todas as redes que possam usar esse texto. Armazenar segredos e executar protocolos de assinatura têm alcances diferentes.

Introduz o conteúdo diretamente no dispositivo quando estás procurando mantê-lo fora de dispositivos ligados. Um método de importação do telefone ou PC pode ter exposto o segredo em origem, embora depois esteja cifrado. A ecrã de revisão prévia é o lugar para detetar palavras, ordem, majúsculas e campos errados.

A palavra-passe do criptograma deve ser longa, única e recuperável de acordo com o teu plano. O teclado de criação analisado tem capacidade para 40 caracteres e o validador exige pelo menos 12, maior e menor ASCII, número e símbolo reconhecido. Não apliques automaticamente os 12 a 1.024 caracteres de Desk ao teclado de Cuvex: Desk aplica uma política diferente. Outros campos de recuperação podem ter limites diferentes; verifica o fluxo e a versão.

Em Original escreva num cartão adequado e vazio; mantém a posição até receber a confirmação. O BIT conserva os ficheiros que produzem o fluxo USB, incluindo os componentes biométricos necessários quando necessário. Não renomee ou combine ficheiros por intuição. Em seguida, ele faz uma leitura e descriptografia de teste no dispositivo, sem comunicar o segredo ao tutor.

Prática

1. Cifra um texto didático criado para esta prática, sem credenciais nem valor econômico.
2. Identifica o suporte e o objeto resultante; anota em privado o alias e a sua função.
3. Reiniciar o processo de descriptografia, verificar o texto no ecrã de confiança e fechar a visualização quando terminar.

Mostra o que aprendeste

Podes distinguir conteúdo correto, escrita correta e recuperação correta. A mensagem «Arquivo copiado» não prova os três.

Pergunta frequente

O alias do cartão é uma palavra-passe? Não. É informação organizacional. Evita incluir saldos ou descrições que facilitem a identificação do teu património.

Ponto de pausa

Não deixes conteúdo decifrado visível. Regista apenas o sucesso ou falha do ensaio.

O que demonstra melhor que um criptograma de teste permite recuperar o seu conteúdo?

1. Ter um nome bonito.
2. O ficheiro existir em duas pastas.
3. Lê-lo e decifrá-lo pelo procedimento correto e verificar o conteúdo em privado.

> **Ver resposta: Lê-lo e decifrá-lo pelo procedimento correto e verificar o conteúdo em privado.**
> A existência de uma cópia não prova que seja utilizável nem que corresponda ao conteúdo esperado.

M04

Limiares de cifragem e biometria

Objetivo

Separar a proteção partilhada do segredo da multiassinatura de Bitcoin.

Compreender

Um criptograma protegido por várias palavras-passe regula quem pode decifrar o conteúdo. Uma carteira Bitcoin multiassinatura regula quais chaves devem autorizar uma despesa na rede. Podes ter um segredo cifrado de forma partilhada que corresponda a uma carteira de assinatura única, ou cada signatário de uma multiassinatura com seu próprio criptograma individual.

Se várias pessoas desbloquearem conjuntamente uma única semente e essa semente permite gastar sozinha, o limiar da cadeia continua a ser uma chave. Uma vez revelada, alguém poderia mantê-la. Não descrevas esse esquema como se forçasse a coordenar várias assinaturas para cada pagamento.

A biometria BIT adiciona uma condição de acesso nos formatos que a utilizam. Um dedo não é uma semente nem um substituto universal da palavra-passe. Planifica lesões, mudanças de pegada, falhas, disponibilidade do equipamento e herança. Conserva e teste a via de recuperação documentada desse criptograma antes de depender dele.

Uma exportação de recuperação pode revelar o segredo num computador, precisamente para resolver uma emergência. A existência dessa função não transforma o PC num ambiente equivalente ao dispositivo. A prática normal deve manter o isolamento; a recuperação local é estudada de forma consciente e com um plano posterior de migração se houve exposição.

Prática

1. Desenha duas políticas: «duas palavras-passe para abrir uma frase-semente» e «duas chaves de três para gastar».
2. Num teste sem fundos, identificas quais ficheiros requer uma cópia biométrica e onde sua recuperação é verificada.
3. Simula que uma pessoa não está disponível. Determina se o limite do teu esquema permite continuar.

Mostra o que aprendeste

Podes explicar quem pode conhecer o segredo e quem pode autorizar uma despesa depois de decifrá-lo.

Pergunta frequente

Posso retirar um participante mudando uma etiqueta? Não. Deves distinguir mudanças de organização de uma nova proteção do segredo e de uma nova política de despesa.

Ponto de pausa

Mantém o esquema sem nomes reais ou dados biométricos.

Três pessoas usam duas palavras-passe para abrir um criptograma com uma única frase-semente de uma carteira de assinatura única. Quantas chaves exige o Bitcoin para gastar?

1. Uma, se for essa a política da carteira.
2. Duas, porque o ficheiro exigia duas palavras-passe.
3. Três, por serem três pessoas.

> **Ver resposta: Uma, se for essa a política da carteira.**
> O limiar de cifragem não altera o script que controla as moedas.

M04

Clonar, conservar e verificar cópias

Objetivo

Construir redundância sem destruir a única cópia válida.

Compreender

Clonar um criptograma copia dados cifrados; não cria um saldo novo, outra semente ou independência em relação a uma palavra-passe exposta. Cópias idênticas permitem enfrentar a perda do suporte, mas não resolvem a exposição do segredo original. Portanto, uma restauração e uma migração para novas chaves respondem a situações diferentes.

No Original, distingue o cartão com o criptograma do cartão de transporte da PSBT. Um suporte de operações pode ser reutilizado de acordo com o fluxo; um cartão com o teu suporte não deve se tornar esse suporte. Se uma operação rejeita um cartão que contém um criptograma, não tente saltar a proteção ou apagar a mão a sua cabeça.

Em BIT, uma cópia deve conservar o conjunto necessário e a relação entre ficheiros. Um administrador de ficheiros pode exibir uma transferência completa sem garantir que o dispositivo tenha validado conteúdo ou terminado sua operação. Espera os estados indicados e confira uma cópia através de recuperação controlada.

Mantém um inventário privado com identificadores discretos, versão de formato, data e resultado de última prova. Separa pelo menos duas cópias em relação aos incidentes que definiste. Evita subindo suporte a canais de suporte para diagnosticar problemas; facilita metadados depurados e códigos de erro.

Prática

1. Cria uma cópia do teu criptograma didático em outro suporte usando o fluxo correto.
2. Desliga o suporte original e recupera o texto de teste a partir da cópia.
3. Documenta o que farias diante de perda, dano de ficheiro e exposição de palavra-passe. Não são o mesmo procedimento.

Mostra o que aprendeste

Consegues identificar a cópia que testaste e explicar por que motivo o original não foi substituído.

Pergunta frequente

Posso apagar o original depois de ver um segundo ficheiro? Primeiro, verifica a recuperação e cobertura. A eliminação deve responder a um plano, não ao simples número de cópias.

Ponto de pausa

Guarda os suporte antes de fechar a sessão; não deixe cartões misturados com os de teste de pagamento.

Se alguém conhecer a palavra-passe e obtiver uma cópia do criptograma, para que serve criar mais três clones?

1. Revoga a cópia do atacante.
2. Aumenta a redundância, mas não revoga esse acesso.
3. Altera automaticamente a semente do Bitcoin.

> **Ver resposta: Aumenta a redundância, mas não revoga esse acesso.**
> Criar duplicados não resolve um comprometimento que já ocorreu.

M05

Instalar e proteger o Cuvex Desk

Objetivo

Abrir uma instalação de origem verificada e proteger seu armazém local.

Compreender

Selecione o pacote do teu sistema e arquitetura: macOS Intel ou Apple Silicon, Windows x64 ou ARM64 e Linux x64 ou ARM64 de acordo com a distribuição disponível. Um ZIP de fontes, um pacote para o Manager e um instalador para o cliente são entregas diferentes. O curso não deve dirigir um aluno a um pacote privado de assinatura.

Verifica a origem e as verificações do sistema. Uma empresa de engenharia do Windows não traz por si só a confiança pública do editor. No Mac, assinatura de aplicação, notarização e avaliação ao abrir são controlos diferentes. Não desabilite proteções gerais seguindo uma chamada de suposto suporte. Se uma versão dá um aviso inesperado, guarda o texto e usa o canal oficial.

Desk cria um armazenamento local cifrado com palavra-passe. Na base analisada, as novas palavras-passe admitem de 12 a 1.024 caracteres; a coincidência de campos é exigida onde há confirmação. Esses limites não são uma medida de qualidade suficiente: usa uma frase única e evita reutilização. A biometria do computador, quando disponível, é uma comodidade de acesso que exige sua própria configuração.

Configura bloqueio por inatividade e, se for caso disso, ao passar para o segundo plano. O atraso após falhas e o apagamento opcional são estudados no manual: não ativar um apagamento automático durante uma demonstração. A aplicação pode funcionar sem uma conta de utilizador convencional, mas seus serviços de consulta, chat ou download têm requisitos e comunicações específicas.

Prática

1. Verifica a plataforma, a versão visível e a origem do pacote sem fornecer identificadores privados ao tutor.
2. Cria um armazém de aprendizagem e confira bloqueio e reabertura. Introduz a palavra-passe em privado.
3. Programar uma cópia cifrada e manter sua palavra-passe conforme o seu plano. Não tentes bloqueio repetido no ambiente real.

Mostra o que aprendeste

Podes diferenciar palavra-passe local, conta comercial e credenciais dos serviços que adicionas.

Pergunta frequente

Mudar a palavra-passe do Desk muda a minha cartão? Não. São proteções independentes. As cópias antigas também não mudam sozinhas.

Ponto de pausa

Bloqueia o Desk e guarda o identificador da lição, sem credenciais.

O instalador não corresponde à arquitetura do teu computador. Qual é o primeiro passo?

1. Forçar a execução desativando as proteções.
2. Obter o pacote oficial adequado e verificar os requisitos.
3. Importar a frase-semente num site para continuar.

> **Ver resposta: Obter o pacote oficial adequado e verificar os requisitos.**
> Verifica a compatibilidade e a proveniência antes de usar material de custódia.

M05

Associar criptogramas e organizar as contas WOW

Objetivo

Vincular uma cópia cifrada e distinguir-a de uma conta de observação.

Compreender

O Desk organiza os criptogramas associados por NFC, USB ou ficheiro de cópia compatível. Um design visual e um alias ajudam a reconhecê-los, mas não são uma prova criptográfica de identidade. Na ficha podes consultar origem e propriedades interpretadas pela app, como formato, tamanho e características de acesso.

Vincular importa ou organiza o objeto compatível; não significa descriptografá-lo no PC nem verificar o seu segredo. WOW é uma carteira de observação associada através de informações públicas compatíveis. Um mesmo conjunto de segredos pode ter diferentes contas ou derivações: a associação deve corresponder à carteira que pretendes gerir.

Ativa ou importa a conta com o descritor ou informações públicas exportadas pelo fluxo do dispositivo. Revisa rede, tipo de script, pegada, rota e endereço de controlo. O nome da conta é organizativo; o identificador derivado de um nome não deve ser tratado como uma forte anonimização, porque um nome previsível pode ser adivinhado.

Na base de Desk, contas pendentes de associação e funções são mantidas para exportar cópias, clonar e eliminar registos locais. Eliminar um cartão da interface não destrói cópias externas nem mova os fundos. "Não há cópia de segurança" significa que a aplicação não acredita uma cópia sob seu critério, não que nenhum cópia de segurança exista no mundo.

Prática

1. Vincula o criptograma didático pelo transporte escolhido e revisa sua ficha.
2. Importa uma conta de aprendizagem compatível e verifica sua rede e endereço de verificação sem mostrar chaves ao tutor.
3. Distingue o registo do criptograma, a conta WOW e o suporte físico. Identifica o que desapareceria com uma eliminação local.

Mostra o que aprendeste

Podes explicar quais dados Desk precisa para observar e quais devem ser seguidos fora do computador durante o uso habitual.

Pergunta frequente

Vincular um ficheiro.bin garante que seja a minha semente? Não. Deves verificar sua origem e recuperação. Uma extensão de ficheiro não certifica conteúdo.

Ponto de pausa

Conserva apenas o estado de «vinculação de prova verificada».

Eliminar localmente uma conta WOW movimenta os respetivos bitcoins?

1. Não. Elimina informação local de acordo com o procedimento, sem gastar as UTXO.
2. Sim. Envia-os ao fabricante.
3. Cancela qualquer assinatura que outra pessoa conserve.

> **Ver resposta: Não. Elimina informação local de acordo com o procedimento, sem gastar as UTXO.**
> O estado local e o estado da cadeia são distintos.

M05

Ligar o Mirror ao Desk

Objetivo

Estabelecer e terminar um link local autorizado sem confundir seus códigos.

Compreender

O Mirror permite operações locais com o Desk através do fluxo de ligação, PIN e QR que apresentam as aplicações. O PIN de seis dígitos pertence a essa sessão. Não é a palavra-passe do Desk, nem a do criptograma, nem uma palavra de recuperação. Verifica qual ecrã gerou e onde deve ser introduzido; não use um código enviado por uma pessoa desconhecida.

Inicia a ação do contexto correto de Desk: vincular, ler QR, transportar PSBT ou firmware são finalidades diferentes. A janela informa de pesquisa, ligação, descoberta, PIN, QR e ação sobre cartão ou ficheiro. O fato de um dispositivo aparecer na pesquisa não mostra que a operação completa tenha terminado.

Concede permissões relevantes de acordo com o sistema: câmera de leitura óptica e Bluetooth ou NFC quando o fluxo os requer. Um telefone sem uma capacidade física necessária não a obtém instalando software. No iOS há diferenças de adaptador e validação; não deve ser apresentado um projeto compilable como se já estivesse distribuído e testado em todos os iPhones.

Se falhar, identifica a fase exata: não aparece, aparece mas não liga, PIN rejeitado, QR ilegível, cartão não lido ou resposta não recebida. Fecha as sessões antigas, verifica as versões compatíveis e as permissões, e volta a tentar de forma controlada. Um PIN incorreto não justifica a mudança de firmware ou a introdução de sementes em outro lugar.

Prática

1. Começa uma leitura de teste a partir do Desk e ligue o Mirror através de seus ecrãs locais.
2. Verifica a finalidade antes de apresentar um QR ou um cartão didático.
3. Cancelar a sessão e confirmar que uma leitura de um contexto anterior não é aplicada depois. Reabre uma nova sessão.

Mostra o que aprendeste

Consegues descrever a fase que falhou e os equipamentos envolvidos sem comunicar códigos ativos nem conteúdo sensível.

Pergunta frequente

O Mirror tem que permanecer ligado sempre? Depende da operação. Não o considere como um serviço permanente nem suponha que uma sessão continue autorizada após fechar ou passar a fundo.

Ponto de pausa

Fecha a sessão de link e bloqueie as aplicações que não estás usando.

O que deve fazer o tutor se a ligação falhar antes de aparecer o PIN?

1. Pedir a frase-semente.
2. Verificar a deteção dos dispositivos, as permissões, a sessão e as versões antes de avançar.
3. Dar a ligação por concluída.

> **Ver resposta: Verificar a deteção dos dispositivos, as permissões, a sessão e as versões antes de avançar.**
> O diagnóstico deve seguir a fase observada, sem presumir que a ligação foi bem-sucedida.

NFC através do Mirror, USB-C e leitura de códigos QR

Objetivo

Utilizar cada transporte conservando seu propósito e suas verificações.

Compreender

Os procedimentos NFC do Cuvex Desktop exigem o Cuvex Mirror num smartphone compatível ligado por Bluetooth ao computador. O Cuvex Desktop não suporta leitores NFC USB externos. O cartão, o seu formato e a sua capacidade também têm de ser compatíveis. Um cartão pequeno suficiente para um criptograma pode não ter espaço para uma PSBT com transações anteriores. O limite efetivo depende do conteúdo integral, e não apenas do número de destinatários. Não uses um cartão de cópia de segurança como cartão de transporte.

No Original, o Mirror pode escrever uma solicitação num cartão de operações; o dispositivo o processará e escreverá uma resposta que o Mirror retorna ao Desk. A confirmação de escrita não significa receção de Desk. Mantém o cartão imóvel até que o equipamento indique o resultado. Se o sistema proteger um criptograma reconhecido, respeita esse rejeição.

BIT utiliza um volume ou cartão USB de troca. O procedimento pode desmontar o volume ou apresentá-lo novamente. O Desk deve selecionar o suporte correto, validar a resposta e emitir a confirmação de receção prevista. Copiar um ficheiro para um ficheiro do PC com o mesmo nome não é como entregá-lo ao dispositivo.

Uma câmera que não lê um QR pode falhar por foco, reflexo, tamanho, movimento ou densidade. Amplia a data e melhora a luz e a distância. Não substituas um identificador longo por suas primeiras letras ou aceite uma transcrição parcial. A leitura bem-sucedida é apenas o começo da sua validação semântica.

Prática

1. Com material didático identifica solicitação, suporte e resposta para Original e BIT no diagrama.
2. Tenta cancelar uma leitura QR sem guardar valores atrasados. Repete com outra finalidade.
3. Simula um ficheiro muito grande e explica por que deves reduzir a complexidade da operação ou escolher um meio compatível, sem retirar validações.

Mostra o que aprendeste

Consegues dizer que equipamento confirmou que fase: leitura, gravação, validação, receção ou confirmação de receção.

Pergunta frequente

Um hash ou um OK de cópia mostra que o destinatário do Bitcoin é correto? Não. Deves revisar a operação e suas saídas no signatário.

Ponto de pausa

Retira e guarda cartões de apoio; deixa identificado o suporte de transporte.

O Original indica que gravou a resposta no cartão. O que falta para afirmar que o Desk a recebeu?

1. Pintar o cartão de outra cor.
2. Criar uma frase-semente nova.
3. Ler a resposta e validá-la no Desk pelo procedimento correspondente.

> **Ver resposta: Ler a resposta e validá-la no Desk pelo procedimento correspondente.**
> O êxito da gravação e o êxito da receção são eventos diferentes.

Prestadores públicos e nó próprio

Objetivo

Escolha uma fonte de consulta e compreender suas fugas e limites.

Compreender

A Desk pode consultar fornecedores públicos compatíveis ou um Bitcoin Core configurado pelo utilizador. Um fornecedor pode conhecer as consultas que recebe, sua sequência e dados de ligação. Não enviar um xpub completo reduz uma exposição concreta, mas os scripts ou seus hashes também podem se vincular entre si.

Em Desk 9.21 aparece a escolha explícita de Blockstream Electrum por TLS, além de alternativas REST e nó próprio. O TLS protege o canal contra certos observadores de rede; o próprio fornecedor continua recebendo consultas. Não há rotação silenciosa que garanta anonimato. A escolha exige compreender esse intercâmbio de privacidade por comodidade.

Para Core, configura endpoint, autenticação e carteira de observação de acordo com o guia correspondente. Não publiques o portão RPC nem deixe exposto à Internet para que a app "verá". Limita o acesso a ambientes fiáveis e utiliza um transporte protegido adequado. Uma palavra-passe RPC não é ditada ao tutor.

A sincronização inicial e um resgate podem atrasar. O progresso deve ser interpretado como estado de trabalho, não como sucesso antecipado. Desk mantém trabalho em segundo plano; fechar a vista não equivale a deter o nó. A janela mínima histórica documentada não garante a descoberta da atividade anterior: se o teu carteira é mais antigo, verifique a data de importação e o alcance real do leitura.

A descoberta é baseada em histórico, não em saldo positivo. Um endereço gastado até zero continua sendo usado. Em multiassinatura analisada, aplica-se um buraco de 20 direções consecutivas sem histórico por ramo e participante, com limites de emissão. Não extrapoles um limite global para todas as carteiras.

Prática

1. Selecione uma fonte de aprendizagem e explique quais informações podes ver.
2. Verifica a data da última sincronização, rede e progresso. Se houver HTTP 429, respeite a pausa e não mude de fornecedor sem decidir.
3. Simula uma carteira com saldo zero e histórico antigo. Vê por que «nulo» e «não usar» são diferentes.

Mostra o que aprendeste

Podes decidir se tua fonte cobre tua necessidade de verificação e privacidade, e reconhecer um estado incompleto.

Pergunta frequente

Um nó próprio faz-me anônimo? Não. Reduz as dependências de consulta, mas deves considerar ligação, contrapartes, publicação e outros metadados.

Ponto de pausa

Registra apenas o tipo de fornecedor e a necessidade de completar o leitura.

Um endereço tem saldo zero, mas já recebeu e gastou fundos. Como deve ser tratado na descoberta da carteira?

1. Como endereço com histórico.
2. Como endereço nunca utilizado.
3. Como endereço inválido.

> **Ver resposta: Como endereço com histórico.**
> É o histórico, e não o saldo atual, que mostra se o endereço foi utilizado.

Receber bitcoin e verificar o endereço

Objetivo

Crie uma solicitação de receção e verificar antes de entregá-la.

Compreender

Abre a conta WOW correta e confira rede e política. Gerar ou recuperar uma solicitação de receção. Podes adicionar motivo, observador e valor esperado para tua organização. Esses campos descrevem tuas informações locais; o montante esperado não impede que alguém envia outra quantidade.

Verifica o endereço usando o fluxo disponível no dispositivo e no contexto de carteira. Se esse percurso ainda não está fisicamente validado em tua combinação, a prática fica em simulação e é escalada antes de receber fundos importantes. Comparar dois ecrãs alimentados pela mesma fonte não traz uma independência que não existe.

Usa um novo endereço para uma nova relação de cobrança quando o fluxo o permite. Na multiassinatura analisada, os endereços já mostrados não são reassignados nem expirados porque um pagador pode usá-los mais tarde. Ao chegar ao limite de novas direções consecutivas sem histórico, recupera a solicitação prévia adequada e compreende o motivo do limite; não rebobines índices.

Depois de partilhar, observe a entrada na tua fonte de verificação. Um e-mail, um justificante do exchange ou uma captura do pagador não demonstram liquidação. Verifica rede, txid, saída, montante e confirmações de acordo com a exposição. Não abras um explorador público com o teu endereço por comodidade se o teu plano exige manter essas consultas privadas.

Prática

1. Gerar uma solicitação no laboratório, revisar conta e rede e explicar como verificarias o endereço.
2. Regista uma etiqueta fictícia e recupera a mesma solicitação depois de fechar a vista.
3. Simula uma cobrança por um montante diferente e decide como conciliá-la sem mudar o histórico.

Mostra o que aprendeste

Podes distinguir endereço gerado, endereço verificado, solicitação partilhada e cobro confirmado.

Pergunta frequente

Um endereço velho deixa de funcionar ao criar outro? Normalmente não. Manter o descobrimento e o registo de solicitações evita perder visibilidade de pagamentos atrasados.

Ponto de pausa

Guarda o estado da solicitação de laboratório, não seu conteúdo no tutor.

O pagador envia uma captura de ecrã que diz «levantamento concluído». O que verificas para aceitar o pagamento?

1. Apenas a qualidade da captura.
2. A saída correspondente numa fonte de rede fiável e as confirmações necessárias.
3. A palavra-passe do pagador.

> **Ver resposta: A saída correspondente numa fonte de rede fiável e as confirmações necessárias.**
> Um comprovativo comercial ou uma captura de ecrã não substitui a verificação do pagamento.

Etiquetar, congelar e selecionar UTXO

Objetivo

Preparar entradas sem misturar origens por acidente.

Compreender

As etiquetas permitem manter um contexto que não figura na cadeia: origem, contraparte, finalidade e restrições de uso. Em Desk, uma etiqueta UTXO e uma nota de endereço podem ter longitudes e funções diferentes. Anotando «cliente A» é útil; usar seu documento ou nome completo pode criar um registo inesquecível sensível.

Congelar um UTXO em Desk exclui-o de certas seleções locais. Não bloqueia sua despesa em Bitcoin, não muda o script e não impede que outra aplicação com as chaves a utilize. Também pode fazer com que o saldo total e o saldo gastável sejam diferentes. Verifica se uma moeda está congelada, reservada por um rascunho ou realmente gasto.

A seleção automática otimiza de acordo com o algoritmo e seu contexto; não necessariamente conhece suas relações privadas. Para um pagamento concreto revisa se convém usar uma saída desse mesmo contexto em vez de unir poupança, salário e atividade comercial. A separação útil requer consistência futura, não apenas bonitas etiquetas.

Exportar etiquetas com formato BIP329 facilita a conservação ou a migração. O formato, por si só, não cifra os dados. O Desk oferece um envelope cifrado para sua exportação; distingue o ficheiro protegido de um texto plano compatível. Na importação, confira a coincidência com a carteira e o tratamento de congelamentos antes de sobrescrever informações.

Prática

1. Etiqueta três UTXOs sintéticos como poupança, atividade e doação.
2. Congela uma e veja a diferença entre o saldo observado e disponível para selecionar.
3. Exporta etiquetas de laboratório com palavra-passe, importa numa cópia e revisa resultados sem dados pessoais reais.

Mostra o que aprendeste

Justifica a escolha das entradas em função do custo e da exposição. Reconhece que congelar é uma preferência local.

Pergunta frequente

Uma etiqueta viaja ao destinatário ao pagar? Não apenas por ser uma etiqueta local. Poda ser filtrado ao exportar, partilhar ficheiros, usar outro serviço ou adicioná-lo a uma mensagem.

Ponto de pausa

Mantém as etiquetas de prática e o estado de congelamento.

Que efeito tem congelar uma UTXO no Desk?

1. Cria um bloqueio de consenso na rede.
2. Transfere a UTXO para uma conta especial.
3. Aplica uma restrição local à seleção na aplicação.

> **Ver resposta: Aplica uma restrição local à seleção na aplicação.**
> Não revoga a capacidade de gastar através de outras cópias das chaves.

Preparar e rever um pagamento

Objetivo

Construir uma PSBT compreensível e reconhecer todos os seus custos e saídas.

Compreender

Selecione conta, entradas gastáveis, destinatários e montantes. Verifica a origem da solicitação. Ao pegar ou ler, revise o endereço completo e rede; a carteira e uma imagem podem ser substituídos. Não confies apenas nos primeiros e últimos caracteres se o procedimento permite uma verificação completa.

Escolhe a taxa e verifica a comissão absoluta, o tamanho estimado, o total e o troco. Com "Enviar o total", a Desk descontina a comissão do montante disponível. Se a ação nasce do chat e o neto não cobre o solicitado, um pagamento parcial deve ser consciente; a solicitação original não se transforma para esconder a diferença.

Verifica se o troco é pequeno ou se não existe saída de troco. Uma saída marcada como própria exige comprovação com a política, não com o nome que o coordenador lhe dá. Se o troco não for viável, revê a opção de transferir a totalidade do saldo ou acrescenta uma entrada compatível. Não aceites que o troco se transforme silenciosamente numa comissão desproporcionada.

PSBT é um formato para transportar informações e assinaturas. Não contém necessariamente privacidade ou autenticidade de origem. Poda incluir transações anteriores, chaves públicas, rotas e metadados. Nos firmwares Final analisados, o perfil multiassinatura usa PSBT v0/BIP174; «transacção versão 2» não significa «PSBT versão 2».

Prática

1. Prepara no simulador um pagamento com uma entrada de 120.000 sat, 70.000 para o destinatário e 1.000 de comissão.
2. Enumera todas as saídas e explica o troco de 49.000 sat. Repete a operação transferindo a totalidade do saldo.
3. Cancelar o rascunho e explicar o que cancelaste localmente. Não uses este simulador para assinar ou publicar nada.

Mostra o que aprendeste

Antes de exportar podes explicar o que entra, o que sai, quem recebe, quanto custa e que autorização falta.

Pergunta frequente

Posso enviar toda a quantidade que mostra o saldo? Somente se a aplicação calcular um envio líquido viável e as comissões forem cobertas. O saldo pode incluir moedas não disponíveis.

Ponto de pausa

Mantém um rascunho de aprendizagem ou cancelá-lo; nunca um PSBT real no portal do curso.

Um ecrã indica «transaction version 2». Isso prova que o ficheiro é uma PSBT v2?

1. Não. São campos de versão distintos.
2. Sim, sempre.
3. Prova que usa Taproot.

> **Ver resposta: Não. São campos de versão distintos.**
> A BIP370 distingue a versão do contentor da versão da transação.

Assinar com o Original e com o BIT

Objetivo

Completar cada ramo de assinatura e receber uma resposta vinculada à operação correta.

Compreender

No Original, entrega a PSBT através do cartão de transporte do procedimento compatível, com o Cuvex Mirror. No dispositivo, lê o pedido, apresenta o criptograma e desbloqueia-o em privado. Revê todas as saídas, os montantes, o troco e a comissão. A resposta é gravada no cartão e depois lida e validada no Desk. O êxito da gravação no cartão não substitui este retorno.

BIT: seleciona o volume correto e entrega a solicitação por USB-C. O serviço local da Desk atende o intercâmbio previsto enquanto operas o dispositivo. Apresenta o criptograma conforme indicado no ecrã e verifica os dados no BIT. «Receber do BIT» importa a resposta. O Desk valida-a e guarda-a antes de confirmar a receção. Uma perda de ligação exige recuperar a mesma operação, não outra escolhida por semelhante.

Na assinatura de uma transação multiassinatura nos firmwares Final, revê o resumo, as saídas obrigatórias, os avisos aplicáveis e as três confirmações finais de «Assinar PSBT». A revisão ampliada opcional permite explorar mais parâmetros; escolher "Não" não elimina as revisões obrigatórias. A verificação independente de uma política é outro percurso e conserva o seu alcance dessa revisão.

A assinatura requer um criptograma compatível cuja autenticidade pode ser verificada. Uma cópia histórica que ainda permite recuperar o segredo não fica por isso habilitada para assinar. Se o dispositivo avisa de cópia antiga sem autenticidade verificada, siga o percurso de recuperação e verificação do segredo e crie uma nova cópia antes de assinar. Não mudes as cabeças nem omite o rejeição.

Se um endereço não coincide, há uma comissão inesperada, faltam dados, aparece outra rede ou o dispositivo rejeita política, cancelar. Não convertas a pressão para terminar a chamada em aprovação. A IA não pulsa botões, não realiza a confirmação final e não declara assinado o que não verificaste.

Prática

1. Segue o percurso do teu modelo com uma carteira sem fundos ou num laboratório já aceite em testes físicos.

2. Simula deter-se antes das confirmações finais e explica por que não equivale a autorizar.
3. Verifica o retorno, a correspondência com o rascunho e, no BIT, o estado da receção e da respetiva confirmação.

Mostra o que aprendeste

Podes narrar o percurso sem revelar credenciais e distinguir aprovação no dispositivo, resposta importada e operação publicada.

Pergunta frequente

O dispositivo offline sabe se as minhas entradas continuam por gastar? Por si só, não pode verificar o estado atual da cadeia. A app deve verificar a transação final contra sua fonte de rede.

Ponto de pausa

Se interromperes a assinatura, cancelar ou deixar uma operação pendente identificada segundo o fluxo, sem segredos visíveis.

O BIT assina, mas o Desk não confirma a receção. Que estado deves assumir?

1. O pagamento foi definitivamente publicado.
2. A resposta aguarda receção ou validação. Retoma a mesma operação.
3. A carteira perdeu-se.

> **Ver resposta: A resposta aguarda receção ou validação. Retoma a mesma operação.**
> Assinar, receber e publicar são etapas distintas.

Finalizar, publicar e resolver problemas

Objetivo

Feche o ciclo de pagamento sem duplicá-lo e diagnostique falhas por etapa.

Compreender

Depois de importar uma assinatura, a Desk deve verificar que corresponde ao rascunho e manter a intenção. Em multiassinatura pode faltar o limiar; em de assinatura única uma assinatura importada também não exime de revisão. Finalizar produz a transação pronta para ser divulgada quando as suas condições estão completas.

Publica somente após a revisão final. Uma resposta do servidor ou um txid indica um resultado do pedido. É necessário acompanhar a operação para verificar a aceitação e a cadeia. Se a app não recebeu resposta, consulte antes de repetir. Não inventes um novo pagamento para resolver um problema de visualização.

Para um pagamento pendente, revise tarifa, validade, conflitos e possibilidade real de RBF. Se houver uma mudança de política ou destinatário, a nova proposta requer novas assinaturas apropriadas. Cancelar localmente não destrói uma assinatura ou transação que já conserve outra pessoa; também não revoga o confirmado.

Diagnóstico por fases: preparação, transporte, desbloqueio, revisão, assinatura, retorno, validação, finalização, difusão e confirmação. Regista sistema, versão, modelo, fase, hora aproximada e código de erro. Os diagnósticos da aplicação foram concebidos para excluir dados sensíveis. Verifica-os antes de os partilhar e não anexes cópias, códigos QR, a Chave de Chat ou credenciais.

Prática

1. Ordena os estados de um pagamento fictício e identifica onde farias uma pausa segura.
2. Resolve três incidentes: saldo insuficiente, resposta USB não recebida e publicação com ligação interrompida.
3. Redige um pedido de assistência com dados sintéticos e um resultado esperado que se possa verificar.

Mostra o que aprendeste

Podes decidir se falta ação do aluno, do dispositivo, do coordenador ou da rede, e evitar um segundo pagamento desnecessário.

Pergunta frequente

Um erro FIRMWARE_CAPABILITY_REQUIRED é corrigido ao mudar o firmware para cegos?
Não. Na incidência documentada de Desk, o reconhecimento do build Final requeria corrigir o catálogo de Desk. Verifica a versão e o perfil antes de modificar equipamentos.

Ponto de pausa

Mantém o estado e a próxima ação. Se publicaste uma operação real fora do laboratório, mantém seu registo em sua documentação privada.

Que ação pode revogar por si só uma transação já confirmada?

1. Apagar o rascunho local.
2. Fechar o Mirror.
3. Nenhuma dessas ações.

> **Ver resposta: Nenhuma dessas ações.**
> A eliminação local não reescreve a cadeia nem retira autorizações que já circulam.

M07

O que se pode observar no Bitcoin

Objetivo

Identificar dados públicos, inferências e dados que adicionas fora da cadeia.

Compreender

Bitcoin on-chain é público: scripts e endereços representáveis, valores, relações entre entradas e saídas e posição em blocos podem ser analisados. O teu nome não aparece necessariamente, mas uma compra identificada, uma fatura publicada ou um endereço partilhado podem ligar-te a esse histórico.

Pseudonimato significa operar com identificadores que não são por si próprios tua identidade civil. Anonimato exigiria um conjunto e condições de indistinguibilidade que não são obtidos simplesmente instalando uma app. A privacidade depende do contexto: um comerciante conhece o teu pagamento, uma plataforma de câmbio pode conhecer o teu levantamento, um servidor conhece as consultas e uma pessoa pode observar os teus dispositivos.

Distinguem fatos e inferências. «Esta saída foi gasta nessa transação» é uma afirmação verificável na cadeia. «Todas essas entradas pertencem à mesma pessoa» é uma inferência heurística que pode falhar. A identificação fora da cadeia pode aumentar a confiança de uma hipótese sem converter todas as interpretações em certeza.

Reutilizar um endereço facilita a adição de atividade. Combinando UTXOs de contextos diferentes pode relacioná-los. Revelar um xpub permite uma observação mais ampla do que ensinar uma única direção. Partilhar um txid pode também mostrar outras saídas e relações que o receptor não precisava conhecer.

Prática

1. Marca numa transação fictícia quais dados são públicos e quais etiquetas são seus.
2. Adiciona uma fatura com nome e descreva qual novo link aparece.
3. Redire uma solicitação de suporte que resolve um erro sem incluir endereço, descritor ou saldo.

Mostra o que aprendeste

Podes dizer «isto é observado» ou «isto é infectado» e explicar quais evidências faltam.

Pergunta frequente

Se eu nunca reutilizo endereços já sou anônimo? Não. A seleção das entradas, o troco, as consultas, as contrapartes e outros metadados continuam a ser importantes.

Ponto de pausa

Mantém um mapa de observadores sem identidades ou transações reais.

Que dado costuma permitir observar uma família de endereços de uma conta?

1. A cor do ícone.
2. A respetiva xpub com contexto de derivação suficiente.
3. A marca do cabo.

> **Ver resposta: A respetiva xpub com contexto de derivação suficiente.**
> A informação pública alargada é sensível para a privacidade, mesmo sem autorizar gastos por si só.

M07

Separar contextos e gerir o troco

Objetivo

Tomar decisões de gasto coerentes com a origem de teus UTXOs.

Compreender

A separação de contextos começa antes do pagamento. Decide se uma receção corresponde a poupança, atividade profissional, despesa diária ou uma relação concreta. Mantém essas informações em etiquetas privadas para que a seleção futura não a apague por desconhecimento.

Uma etiqueta não separa criptograficamente saídas. Se gastares juntos dois UTXOs de contextos diferentes, a transação publica sua relação. Consolidar reduz o número de entradas de futuros pagamentos, mas aumenta o vínculo entre as saídas consolidadas. Fazer isso com comissões baixas pode ser eficiente e ao mesmo tempo contrário ao teu objetivo de privacidade.

O troco é uma nova saída controlada pela mesma política, não «dinheiro invisível». Seu uso posterior pode estender relações anteriores. Não identifiques um endereço como troco por ter um montante estranho. Numa revisão real, o dispositivo deve verificar se o endereço pertence à carteira.

Evita converter a privacidade em padrões mecânicos de montantes, tempos ou transferências repetidas. Esses padrões também podem ser reconhecíveis e gerar mais comissões. Avaliar quais dados cada parte conhece e quais novas informações a operação proposta publicaria. Nenhuma seqüência apaga a história já publicada.

Prática

1. Cria cinco UTXOs ficções de três contextos e prepare um pagamento que use o menor número de contextos necessários.
2. Identifica o troco resultante e decide como o etiquetar.
3. Compara o custo e a exposição de consolidar todas as saídas em vez de mantê-las separadas.

Mostra o que aprendeste

Podes justificar uma consolidação ou rejeitá-la com um motivo concreto, sem aplicar uma regra absoluta para todos os casos.

Pergunta frequente

Transferir tudo para outra direção minha rompe o histórico? Não. A transferência publica uma relação adicional e pode adicionar custos sem resolver tua ameaça.

Ponto de pausa

Conserva o raciocínio do laboratório e a política de seleção escolhida.

Que consequência pode ter a consolidação de salários e donativos numa única transação?

1. Tornar visível uma relação entre essas entradas.
2. Apagar a sua proveniência pública.
3. Transformá-los em dinheiro garantidamente anónimo.

> **Ver resposta: Tornar visível uma relação entre essas entradas.**
> Reduzir o número de UTXO pode aumentar as ligações observáveis.

M07

Privacidade na rede, Tor e VPN

Objetivo

Distinguir a privacidade da ligação da privacidade na cadeia.

Compreender

Um servidor de consulta pode relacionar pedidos com uma ligação. teu provedor de Internet pode observar destinos ou padrões de acordo com o transporte. Uma VPN transfere parte dessa confiança para o operador da VPN; não elimina a informação pública do Bitcoin nem impede que uma conta identificada o reconheça.

O Tor encaminha o tráfego através de uma rede para reduzir determinadas ligações entre a origem e o destino. Não transforma uma endereço Bitcoin em privada e não protege uma aplicação cujo tráfego não passa por Tor. Abrir Tor Browser não configura automaticamente Desk, Bitcoin Core nem todos os serviços do computador.

Antes de afirmar que uma ligação está protegida, precisas verificar sua rota e configuração. Nesta base não se pressupõe um interruptor Tor integrado em Desk. Um deslocamento com nó ou proxy requer guia de engenharia e validação de tráfego real. Não se inventou um campo de interface porque outra carteira o tem.

Há também fugas por DNS, sincronização de contas, links de navegador e serviços de preço. Um esquema pode proteger as consultas de saldo e continuar revelando atividade ao abrir um explorador público. Define o alcance de cada medida e o comportamento quando a ligação falha; evite mudanças silenciosas a um fornecedor menos privado.

Prática

1. Descrição do percurso de computador, fornecedor de ligação, proxy se existe, nó ou serviço e rede Bitcoin.
2. Indica quem recebe consultas e quem vê tua identidade comercial.
3. Simula que o nó privado não responde. Decide entre parar ou mudar explicitamente de fonte com conhecimento da exposição.

Mostra o que aprendeste

Podes explicar quais ameaças reduzem tuas configurações e quais ameaças ainda existem.

Pergunta frequente

Tor garante que ninguém pode associar um pagamento comigo? Não. Contractantes, identificação comercial, padrões e erros operacionais podem continuar vinculando.

Ponto de pausa

Regista o alcance do design, não endpoints privados ou palavras-passe.

Abrir o Tor Browser obriga o Desk a fazer consultas através do Tor?

1. Sim, porque partilham o computador.
2. Sim, se o ícone estiver visível.
3. Não. É preciso configurar e verificar o percurso de rede de cada aplicação.

> **Ver resposta: Não. É preciso configurar e verificar o percurso de rede de cada aplicação.**
> As outras aplicações não herdam automaticamente a proteção de uma delas.

CoinJoin, Payjoin e limites atuais

Objetivo

Entender ferramentas colaborativas sem atribuir-lhes anonimato ou compatibilidade inexistentes.

Compreender

CoinJoin reúne contribuições de várias pessoas numa transação para dificultar certas inferências sobre entradas e saídas. Não é sinónimo de entregar moedas a um serviço custodial que promete devolver outras. Diferentes desenhos exigem revisar coordenação, custódia, comissões, resistência a participantes maliciosos e tratamento posterior.

O Payjoin inclui entradas do pagador e do destinatário num pagamento colaborativo, enfraquecendo algumas heurísticas de propriedade comum. Requer suporte compatível em ambos os extremos e um protocolo específico. É material de compreensão técnica: não foi acreditado em fontes analisadas um fluxo Payjoin ou CoinJoin integrado e operativo em Cuvex Desk.

A disponibilidade e o contexto jurídico mudam. A documentação de Wasabi registra o fechamento do coordenador do zkSNACKs em 1 de junho de 2024; não deve ser ensinado um botão histórico como se fosse garantido hoje um serviço. O Departamento de Justiça dos EUA comunicou em 2025 a declaração de culpabilidade e posteriores condenações dos fundadores do Samourai. Este caso não permite concluir que qualquer técnica de privacidade é ilegal em qualquer jurisdição.

Uma ferramenta pode reduzir uma inferência e deixar outras intactas. A origem identificada não desaparece dos registos de uma contraparte. As recombinações posteriores, metadados e falhas do conjunto de participantes podem degradar a privacidade. Além disso, certos serviços podem aplicar políticas comerciais diferentes a moedas com determinadas histórias.

Prática

1. Compara uma transação corrente, uma colaborativa e um serviço que recebe custódia, sem executar operações reais.
2. Para uma ferramenta concreta, procure versão, manutenção, estado do serviço e documentação atual antes de propor seu uso.
3. Identifica riscos técnicos, de custódia e jurídicos por separado. O tutor não deve projetar evasão de controlos nem prometer «fundos impossíveis de rastrear».

Mostra o que aprendeste

Podes explicar uma vantagem limitada e pelo menos dois riscos ou requisitos de uma técnica de privacidade.

Pergunta frequente

Cuvex precisa de um misturador para servir de guarda privada? Não. Controle de consultas, dados, chaves e seleção de UTXOs já resolvem riscos concretos, sem prometer ocultação total.

Ponto de pausa

Regista uma ferramenta como «estudada», não como «compatível» sem evidência.

Que afirmação se pode sustentar?

1. O CoinJoin garante anonimato permanente.
2. Uma técnica colaborativa pode dificultar certas inferências, com requisitos e limites.
3. Qualquer serviço chamado mixer mantém a autocustódia.

> **Ver resposta: Uma técnica colaborativa pode dificultar certas inferências, com requisitos e limites.**
> As propriedades dependem do protocolo, da implementação, dos participantes e da utilização posterior.

O que nos ensinam incidentes reais

Objetivo

Transformar incidentes documentados em decisões comprováveis, sem atacar concorrentes ou exagerar proteção.

Compreender

e Mt. Gox: uma acusação do Departamento de Justiça de 2023 descreve o acesso não autorizado a servidores e chaves, e a posterior desaparição de fundos de clientes. Uma acusação expressa alegações, não uma sentença. A lição de guarda é perguntar quem realmente controla as chaves e o que acontece se a empresa falhar.

Ledger Connect Kit, dezembro de 2023: Ledger documentou uma publicação maliciosa de uma biblioteca usada por aplicações descentralizados, após comprometer o acesso de um antigo funcionário. O incidente afetou a cadeia de distribuição de software e enganou utilizadores da DApps EVM para assinar. Não demonstra uma ruptura do hardware de Ledger nem do consenso de Bitcoin.

Bybit, fevereiro de 2025: o FBI atribuiu à Coreia do Norte um roubo de cerca de US $ 1.500 milhões em ativos virtuais. Foi um incidente de um intercâmbio e ativos de outras redes; não se apresenta como uma ruptura da criptografia de Bitcoin. Para o aluno é importante verificar a intenção de uma assinatura e evitar que várias pessoas confie cegamente na mesma ecrã.

Coinbase, maio de 2025: a empresa comunicou roubo de dados por agentes de suporte sobornados para facilitar engenharia social. Ele disse que não havia palavras-passe ou chaves privadas. O risco educacional é que um estafador conheça dados verdadeiros e ainda assim seja um estafador.

Bitcoin Core também publica falhas de software: o aviso CVE-2024-35202 descreveu um possível fechamento remoto em versões anteriores a 25.0. Verificar regras não elimina a necessidade de manter software. Não se deduza desse aviso um roubo de chaves.

Em janeiro de 2026, The Register informou de uma exposição de dados de encomendas e contacto de compradores da Ledger através da Global-e, com confirmações atribuídas a ambas as empresas e sem afetação de chaves de recuperação de acordo com essas declarações. O caso lembra que uma compra pode revelar que possuis um dispositivo mesmo que o hardware não tenha sido vulnerável.

Em abril de 2026, The Record informou do ataque a Drift e a suspensão de depósitos e retiradas anunciada pela plataforma. Trata-se de um protocolo de finanças descentralizadas sobre Solana, não de uma ruptura de Bitcoin. As perdas inicialmente estimadas e os processos posteriores de recuperação não devem ser apresentadas como uma cifra definitiva nem como um reembolso garantido.

Prática

1. Classifica cada incidente por custódia, interface ou distribuição, dados pessoais, protocolos de outras redes e disponibilidade.
2. Para cada um propõe uma prevenção e uma limitação dessa prevenção.
3. Tente uma chamada fraudulenta: «Eu conheço a tua compra; mova teus fundos para esta direção segura». Desliga a chamada e verifica o pedido através de um canal que tenhas iniciado.

Mostra o que aprendeste

Podes explicar por que nenhum incidente prova que uma marca alternativa seja invulnerável. A evidência apoia um alcance concreto.

Pergunta frequente

São os últimos hackers que existem? Não. É uma seleção verificada para a edição de 17 de novembro de 2026, não um inventário exaustivo nem uma monitorização em directo.

Ponto de pausa

Nota o hábito que vais mudar e como verás que manténs.

Alguém conhece a tua compra e pede uma transferência para uma «carteira de resgate». O que prova o conhecimento da compra?

1. Pode tratar-se de informação divulgada indevidamente. Não autentica a identidade da pessoa nem o endereço.
2. A pessoa pertence necessariamente ao apoio oficial.
3. Deves partilhar a frase-semente.

> **Ver resposta: Pode tratar-se de informação divulgada indevidamente. Não autentica a identidade da pessoa nem o endereço.**
> Dados verdadeiros podem ser usados para construir um engano convincente.

Criar uma identidade e verificar contactos de chat

Objetivo

Activar uma identidade de chat sem expor sua chave e verificar a contraparte.

Compreender

Em Desk, o chat é ligado ao criptograma através de uma Chave de Chat gerada em Cuvex. Embora sua representação possa parecer uma xpub, ela é secreta e não deve ser tratada como uma chave pública de uma conta WOW. O tutor nunca precisa ler ou ver por QR.

O fluxo distingue alias novo e transferência ou recuperação de um existente. Na implementação analisada é escolhido o perfil móvel iOS ou Android correspondente, porque as identidades derivadas históricas não são intercambiáveis por intuição. DEV e Produção são ambientes separados: mudar de ambiente não migra conversas ou alias automaticamente.

Adicionar um alias não verifica identidade. Verifica a pegada através de um canal independente e autenticado. Se a aplicação oferece perguntas de reconhecimento, utiliza informações que não são públicas e evita respostas que revelam palavras-passe. Uma voz conhecida pode ser imitada; para situações de risco combina métodos previamente acordados.

Se mudares a identidade de um contacto, pare pagamentos e coordenação até resolvê-lo. Poda ser uma recuperação legítima ou uma substituição maliciosa. A cifragem de ponta a ponta protege um canal segundo o protocolo e a implementação, mas não prova quem está a utilizar o dispositivo do outro lado.

Prática

1. Num ambiente de testes, explica o fluxo de criação ou recuperação sem facilitar a Chave de Chat.
2. Adiciona um contacto de laboratório e acorde por outro canal uma verificação de impressão.
3. Simula uma mudança de identidade. Define como confirmarias o troco antes de pagar.

Mostra o que aprendeste

Podes distinguir alias, pegada pública, Chave de Chat secreta e confiança humana numa pessoa.

Pergunta frequente

Um antigo alias garante que é a mesma pessoa? Não. A continuidade e as mudanças de chaves devem ser verificadas de acordo com o fluxo.

Ponto de pausa

Regista apenas «contacto de teste verificado» e o método utilizado, sem chaves nem perguntas privadas.

Uma sequência de caracteres chama-se Chave de Chat e tem o aspeto de uma xpub. Como é tratada no Desk?

1. Como dado que se pode publicar em fóruns.
2. Como segredo para recuperar a identidade.
3. Como endereço de receção Bitcoin.

> **Ver resposta: Como segredo para recuperar a identidade.**
> O aspeto não determina a confidencialidade nem a finalidade do dado.

M08

Pedir e pagar satoshis pelo chat

Objetivo

Passar de uma conversa a um pagamento sem perder revisão ou contexto.

Compreender

O chat permite solicitar endereço, responder com um endereço de receção, solicitar pagamento e abrir a preparação de uma conta WOW. Manter o contexto no canal reduz erros de copiar informações entre aplicações, mas não transforma cada mensagem numa ordem de gasto autenticada.

Antes de responder ou pagar, revise contacto verificado, rede, montante e solicitação original. O formulário partilhado conserva seleção de UTXOs e comissão. Se a mensagem solicita uma quantia e escolheres "Enviar o total", o net depois de comissões pode ser inferior; deve ser identificado como pagamento parcial quando corresponde.

A autorização permanece em Cuvex. O chat transporta intenção e coordenação; não tem permissão para assinar automaticamente. A confirmação de pagamento enviada ao contacto deve distinguir que uma mensagem foi recebida de que existe uma transação confirmada. O receptor verifica com sua própria conta ou fonte.

Os links externos, os anexos QR e os endereços continuam a ser dados não fiáveis até que eles sejam validados. "Ver em Mempool" pode abrir um serviço de terceiros e revelar consultas. Se a tua política usa teu próprio nó, prefira a verificação compatível no WOW e avalia qualquer saída para serviços públicos.

Prática

1. Representa dois papéis: o receptor solicita 50.000 sat; o pagador prepara sem publicar.
2. Simula um saldo disponível neto de 48.000 sat. Explica o consentimento e conciliação que faltam para um pagamento parcial.
3. Muda deliberadamente a rede numa mensagem de teste e pare o fluxo.

Mostra o que aprendeste

Consegues acompanhar a relação entre o pedido, o endereço, o rascunho, a assinatura e a confirmação sem a reduzir a «o chat diz OK».

Pergunta frequente

Enviar sats desde chat implica usar Lightning? Não. O fluxo WOW documentado prepara pagamentos Bitcoin em cadeia. A palavra sats significa uma unidade, não uma rede de transporte.

Ponto de pausa

Cancelar o rascunho de laboratório ou registar o estado; não publicar para demonstrar uma interface.

Recebes uma confirmação no chat. Qual é a verificação decisiva para aceitar o pagamento?

1. O ícone da mensagem estar verde.
2. O interlocutor dizer «confirmado».
3. Verificar a operação e as suas saídas na rede através da fonte apropriada.

> **Ver resposta: Verificar a operação e as suas saídas na rede através da fonte apropriada.**
> O estado da mensagem e o estado da transação são diferentes.

Partilhar criptogramas de forma consciente

Objetivo

Entender o que implica entregar uma cópia cifrada a outra pessoa.

Compreender

Partilhar um criptograma transmite uma cópia do objeto cifrado. Não envia necessariamente bitcoins nem incorpora por si só um novo signatário. Se o receptor também obter meios de desbloqueio suficientes, ele pode acessar o conteúdo de acordo com o esquema; portanto, tens que decidir com antecedência que capacidade estás transferindo.

A cifragem de ponta a ponta do chat e a cifragem do ficheiro protegem camadas diferentes. Uma vez baixado, o receptor pode manter o objeto fora do chat. Eliminar tua mensagem ou registo local não garante retirar todas as cópias. Uma palavra-passe partilhada pelo mesmo canal pode concentrar os componentes numa única via.

Antes de enviar, verifique a identidade, o formato e a finalidade. Se a aplicação permite ligar um criptograma recebido, que organiza uma cópia, não acredita que é seguro descriptar qualquer ficheiro. Não uses anexos que exijam a introdução de semente ou palavra-passe numa página externa.

A recuperação requer um acordo operacional: quem conserva cada componente, quem pode abri-lo, como uma exposição é detectada e como a guarda é mudada se a relação termina. Para um pagamento corrente, geralmente basta um endereço validado; não é necessário partilhar o teu criptograma.

Prática

1. Desenha uma transferência de um texto didático cifrado para um contacto de laboratório.
2. Enumera o que sabe e o que o receptor poderia fazer antes e depois de conhecer a palavra-passe.
3. Simula que a relação termina. Descreve por que apagar a mensagem não revoga a cópia ou as chaves.

Mostra o que aprendeste

Podes distinguir «Compartilhei dados», «Compartilhei acesso a um segredo» e «Firmou uma despesa».

Pergunta frequente

Um ficheiro cifrado pode circular sem nenhuma consequência? Poda revelar metadados, facilitar tentativas de palavra-passe e ser mantido indefinidamente. Avalia a necessidade de partilhar.

Ponto de pausa

Não deixes adjuntos de guarda no curso. Regista apenas a conclusão do exercício.

Partilhar um criptograma no chat equivale a enviar bitcoins?

1. Não. Transmite um objeto cujo conteúdo e acesso têm outro alcance.
2. Sim, desde que termine em .bin.
3. Ativa automaticamente uma nova carteira multiassinatura.

> **Ver resposta: Não. Transmite um objeto cujo conteúdo e acesso têm outro alcance.**
> Transportar segredos e movimentar UTXO são operações distintas.

Recuperar o chat e compreender os seus metadados

Objetivo

Planear a mudança de equipamento e distinguir a recuperação da identidade da recuperação das mensagens.

Compreender

Desk indica que histórico e sessões são cifrados localmente e não fazem parte de sua cópia global. A Chave de Chat permite recuperar a identidade; não garante recuperar todas as conversas antigas. A aplicação inclui estados e ações para ativação pendente, manutenção de chaves e recuperação local quando há material compatível.

Cada alias deve ser usado num único dispositivo ao mesmo tempo, de acordo com o guia da base analisada. Não o ative simultaneamente em dois equipamentos para «testar a sincronização» se esse uso não for suportado. Um transferência deve seguir o procedimento e verificar a continuidade com os contactos.

«Pendente», «aceite pelo servidor», «recebido» e «não foi possível decifrar» descrevem fases diferentes. Um envio não confirmado não é enviado automaticamente para cegos: primeiro tens que resolver se ele chegou. Se falta uma chave de sessão ou muda identidade, manter a mensagem pendente não é igual a ter lido.

O conteúdo cifrado não oculta necessariamente horários, tamanho, relações de entrega, alias ou dados de ligação em relação a todos os sistemas envolvidos. Na voz acontece algo semelhante: a criptografia do transporte não converte uma chamada convencional num canal apropriado para segredos. Usa o mínimo de dados necessários para aprender e resolver incidentes.

Prática

1. Simula perder o PC e explica o que recupera cada material disponível.
2. Classifica os estados de mensagens e decide quando uma solicitação de pagamento não deve ser reenviada.
3. Prepara um aviso de mudança de equipamento para que os contactos possam verificar por um canal independente.

Mostra o que aprendeste

Podes explicar que conversa seria perdida e que identidade poderia ser restaurada sem prometer restaurações que a cópia de segurança não cobre.

Pergunta frequente

Apagar o chat local apaga também as mensagens do outro lado? Não deves assumir isso. O receptor pode armazenar mensagens e ficheiros de forma independente.

Ponto de pausa

Mantém um plano de transferência com nomes de campos vazios, sem Chave de Chat.

Segundo o guia analisado, o que garante por si só a Chave de Chat?

1. Todo o histórico de conversas em qualquer PC.
2. A possibilidade de recuperar a identidade através do procedimento compatível, mas não todas as mensagens antigas.
3. Acesso automático às chaves Bitcoin dos contactos.

> **Ver resposta: A possibilidade de recuperar a identidade através do procedimento compatível, mas não todas as mensagens antigas.**
> A identidade e o arquivo histórico são capacidades diferentes.

Configuração do dia a dia e revisão das permissões

Objetivo

Controlar parâmetros de Desk sem confundir conforto com proteção.

Compreender

Desk oferece tema Noite, Dia ou Sistema; sincronização automática e períodos de 3 ou 5 minutos; sons de transação; fundo do chat; idioma e moeda de referência. Estas preferências alteram a apresentação ou a frequência de consulta. Eles não alteram uma assinatura de Bitcoin nem adicionam anonimato.

A configuração de segurança analisada permite bloqueio por inatividade, bloqueio ao passar para o segundo plano, atraso máximo após falhas e apagamento opcional. O esquema de inatividade admite um intervalo de 30 a 86.400 segundos. A interface pode oferecer opções mais restritas. Os valores por padrão devem ser lidos da versão que executas, não supostamente por uma classe gravada.

A integração de ligações bitcoin: abre uma solicitação para desbloquear, selecionar conta e revisar. Não permite um pagamento automático. No Linux, o guia diferencia instalação integrada e AppImage para registar links. Uma fatura Lightning requer um fluxo compatível diferente; não é resolvido declarando Desk aplicação padrão.

A cotação, o gráfico de preço e os links informativos podem consultar serviços externos. Sua função é informativa e não um sinal de compra. Verifica a data e a fonte antes de usar os dados para traduzir montantes. Um modo escuro ou uma janela pequena não deve ocultar botões finais, direção ou comissão; se ocorrer, pare e relate o problema de geometria.

Prática

1. Ajusta a aparência e o bloqueio no armazenamento de aprendizagem. Verifica se podes entrar novamente.
2. Verifica quais os automatismos ativos: sincronização, som e verificação de firmware não são o mesmo.
3. Abre uma fictícia solicitação de ligação bitcoin: e cancelar antes de preparar qualquer operação real.

Mostra o que aprendeste

Podes explicar o efeito de cada ajuste e localizar os que implicam consultas ou ações sensíveis.

Pergunta frequente

A biometria do PC substitui minha cópia de recuperação? Não. Poda depender do equipamento e do armazenamento seguro do sistema. Conserva a recuperação independente.

Ponto de pausa

Bloqueia o Desk e regista apenas as preferências que alteraste.

O que muda ao escolher uma sincronização de três em três minutos?

1. A frequência prevista das consultas quando a função está a ser executada.
2. A política de assinaturas na cadeia.
3. A frase-semente do dispositivo.

> **Ver resposta: A frequência prevista das consultas quando a função está a ser executada.**
> É uma preferência operacional que não altera a custódia.

M09

Conceber uma carteira multiassinatura

Objetivo

Escolha um limiar que resiste a perdas e compromissos razoáveis.

Compreender

Numa política M de N, N é o número de participantes com chaves diferentes e M é o número de assinaturas necessárias. Uma 2 de 3 resiste à indisponibilidade de uma chave, mas duas chaves comprometidas podem autorizar gasto. Se as três sementes estão no mesmo lugar ou nascem da mesma exposição, a independência é reduzida.

O perfil multiassinatura analisado de Cuvex é P2WSH nativo com sortedmulti e derivação BIP48. Original admite estrutural até seis chaves de política e BIT até quinze. Se ambos intervirem, o fluxo deve respeitar o participante mais limitado e o tamanho real do transporte. Os limites máximos da estrutura não garantem que haja espaço para uma política com muitas chaves e entradas.

A aplicação admite prazos que devem cumprir as relações de política, mas uma 1 de N não exige colaboração para gastar. O firmware mantém avisos específicos sobre esse risco. Escolher um número maior não melhora tudo: aumenta a coordenação, os custos, o material de recuperação e a possibilidade de bloqueio.

MuSig2 é um esquema diferente de agregação de assinaturas Schnorr e, por si mesmo, é N de N, não uma 3 de 5 arbitrária. Nos firmwares Final estudados não está implementada assinatura de entradas Taproot, MuSig2 nem Miniscript. Receber um destinatário P2TR não demonstra a capacidade de assinar a partir de uma carteira Taproot.

Prática

1. Deseja uma 2 de 3 ficção com riscos independentes para cada participante.
2. Simula a perda de uma chave e, noutro cenário, o comprometimento de uma chave. Explica o que pode e o que não pode ser feito.
3. Verifica limites por modelo antes de escolher uma política de tamanho maior.

Mostra o que aprendeste

Podes expressar tolerância à perda, um limiar de ataque e dependências partilhadas do teu design.

Pergunta frequente

A multiassinatura exige que as pessoas conheçam as sementes das outras? Não. O propósito é que cada uma conserve sua capacidade privada e partilhe a informação pública necessária para construir e recuperar a política.

Ponto de pausa

Mantém o design com participantes fictícios e suas responsabilidades.

Numa política 2 de 3 com chaves independentes, quantas chaves privadas bastam para autorizar um gasto válido segundo essa política?

1. Uma.
2. Duas.
3. Sempre as três.

> **Ver resposta: Duas.**
> O limiar exige duas. As restantes condições e validações também têm de ser cumpridas.

Criar convites e fornecer chaves

Objetivo

Construir uma política com participantes verificados sem partilhar sementes.

Compreender

O criador escolhe nome, rede, M, N, contactos, informação pública própria e condições operacionais da convite. No esquema analisado aceitam redes mainnet e regtest para este fluxo, de 2 a 15 participantes antes de aplicar limites do dispositivo, e expiração operacional de 1 a 720 horas. Não uses esses limites como autorização para saltar uma verificação de capacidade.

Cada participante revisa a convite, decide aceitar ou rejeitar e fornece a chave pública estendida do participante com pegada e rota BIP48 mediante o fluxo compatível. Não fornece semente, chave privada, endereço separado ou descritor inteiro de outra carteira. Uma chave mal contextualizada pode produzir uma política diferente, mesmo que tenha uma aparência de xpub válida.

O criador coordena; não substitui a validação de cada signatário. Antes de receber fundos, todos devem ser capazes de reconstruir e verificar os mesmos parâmetros e um endereço de controlo. Um contacto aceito no chat não implica a aprovação automática de qualquer política que envias.

A caducidade de uma convite é uma regra de coordenação da app. Não muda por si só um script já financiado, não apaga assinaturas guardadas por outras pessoas e não funciona como timelock de consenso. Cancelar uma proposta e retirar fundos de uma política existente são ações diferentes.

Prática

1. Em laboratório regtest preparado, crie uma proposta 2 de 3 com contactos de teste.
2. Representa uma aceitação, um rejeição e uma contribuição com rede incorrecta. Verifica se a última se detém.
3. Enumera os dados que todos devem conservar antes de financiar: rede, Limiar, chaves públicas, origens, script e endereço comprovado.

Mostra o que aprendeste

Podes reconhecer uma convite incompleta e explicar que aprovação falta sem assumir-la pela existência do chat.

Pergunta frequente

Uma data de expiração torna impossível gastar depois? Não por ser um campo de convite. Uma restrição temporária de Bitcoin requer condições específicas de script ou transação e suporte real.

Ponto de pausa

Mantém o identificador didático da proposta e a aprovação pendente.

Para participares numa carteira multiassinatura, o que pede o procedimento documentado?

1. A frase-semente de todos os participantes.
2. Um endereço de receção qualquer.
3. A tua chave pública alargada com impressão digital e origem BIP48 compatíveis.

> **Ver resposta: A tua chave pública alargada com impressão digital e origem BIP48 compatíveis.**
> O material público correto permite construir a política sem divulgar chaves privadas.

Verificar políticas com o Mirror pela ordem que escolheres

Objetivo

Compare campos completos e entenda exatamente o que acredita o resultado.

Compreender

A verificação independente apresenta um limite, rede, perfil, SIGHASH, ID de política, primeiro endereço, posição do utilizador e dados de cada participante. É um controlo de intenção e consistência. Não se presume que o dispositivo tenha registado a política de forma permanente. O alcance documentado limita-se a «esta revisão».

No Mirror 12.12 podes primeiro ler o QR de Cuvex ou o de Desk e escolher quaisquer dados. Não há obrigação de começar pelo passo 1, ler todos ou manter uma ordem. Se revisares um texto manualmente, omitir seu scan não o marca como comprovado por Mirror.

O comparador mostra texto literal completo. Espaços, saltos de linha, majúsculas e diferenças Unicode contam. "Coincide" significa que os dois valores desse par são iguais; não autentica origem, não prova que correspondem à mesma política e não activa a carteira. A aprovação final e sua resposta correlacionada seguem o circuito Cuvex e Desk.

Os QR atuais da Desk contêm apenas o valor, sem ordinal nem sessão. Mirror não pode sempre deduzir o passo. "Indicar passo de Desk" adiciona contexto manual e deve ser mostrado como tal. Com N participantes há 7 + 4N campos do mapa documentado: 8+4k pegada, 9+4k rota, 10+4k xpub e 11+4k ID de chave, para k começando em zero. Com N=2, o passo 15 é o ID da segunda chave e pode ser comparado primeiro.

Prática

1. Usa dados sintéticos e compare primeiro um ID marcado como passo 15; depois rede e limiar.
2. Introduz uma discrepância de um caráter. Verifica "Não coincide" e comece outro par sem trazer o resultado.
3. Compara «2 / 3» e explica por que o texto não permite saber sempre se é um limiar ou posição do utilizador.

Mostra o que aprendeste

Podes descrever quais campos verificaste, como o contextualizou e o que resta para aprovar. Não convertas coincidências parciais em aprovação global.

Pergunta frequente

Preciso ler todos os QR para continuar aprendendo? Não. A comparação é livre. As revisões e autorizações obrigatórias do signatário mantêm o seu próprio fluxo.

Ponto de pausa

Pede o comparador; os valores devem ser apagados ao sair ou passar para o segundo plano de acordo com o design analisado.

O Mirror compara dois códigos QR do passo 15 e indica uma correspondência. O que atesta isso?

1. A igualdade literal dos elementos desse par, no contexto identificado ou indicado.
2. A aprovação de toda a política.
3. A autenticidade da origem dos dois QR.

> **Ver resposta: A igualdade literal dos elementos desse par, no contexto identificado ou indicado.**
> A comparação não substitui a autenticação, a revisão global ou a resposta do equipamento.

Coordenar assinaturas e publicar uma transação multiassinatura

Objetivo

Levar uma proposta a um limiar de assinaturas sem perder intenção ou controlo.

Compreender

Uma operação multiassinatura especifica entradas, destinatários, montantes, tarifas, substituição e notas operacionais. O criador pode solicitar assinaturas a participantes compatíveis. Cada signatário revisa por sua conta de rede, política, entradas, todas as saídas e comissão antes de autorizar em seu dispositivo.

Uma assinatura parcial não move fundos por si só se falta o limiar. Quando alcançado, o coordenador pode combinar e terminar de acordo com o fluxo. Os relatórios de outros participantes ou do coordenador são informações de coordenação, não uma verificação local que fizeste. A app deve distinguir essas origens.

A implementação de referência permite repetir a tentativa, receber a assinatura, confirmar a receção, rejeitar e transferir a coordenação. Um transpaso não muda as chaves nem o seu limiar. Uma resposta guardada deve ser correlacionada com a solicitação e o perfil efetivo que foi usado; não é escolhida outra política por ser semelhante ou por ser a primeira do catálogo.

Se alguém altera destinatários ou condições relevantes, precisas revisar uma nova proposta e obter as assinaturas que correspondem. Não «arrigue» uma PSBT à mão eliminando dados de segurança para que ele faça em NFC. Os firmwares exigem o perfil e validações compatíveis, com limites de entradas, saídas e tamanho.

Antes de publicar, certifique-se de que a operação é a acordada e que não existe uma versão já difundida. A seguir, a confirmação da fonte escolhida. Rejeitar no teu aplicação não revoga automaticamente assinaturas que outros já conservaram ou impede qualquer ação compatível com o limite restante.

Prática

1. Representa uma política 2 de 3 com três participantes fictícios. Um assinou, o outro rejeitou e o terceiro pede esclarecimento.
2. Muda o endereço do pagamento de teste e explica por que uma aprovação verbal anterior não é reutilizada.

3. Simula uma falha na confirmação de receção depois de guardar a assinatura. Recupera o mesmo trabalho, sem duplicar o pagamento ou mudar o perfil.

Mostra o que aprendeste

Podes indicar quem coordena, quem assina, quem termina e que prova existe de cada etapa.

Pergunta frequente

Dois OK do chat equivale a duas assinaturas? Não. O limiar é satisfeito com autorizações criptográficas válidas sob a política, não com mensagens.

Ponto de pausa

Registra estado, assinaturas pendentes e seguinte responsável sem conteúdo privado.

Uma operação 2 de 3 tem uma assinatura válida e duas mensagens a dizer «concordo». O limiar foi atingido?

1. Sim, porque há três participantes.
2. Não. Falta outra assinatura criptográfica válida.
3. Sim, se o coordenador o anunciar.

> **Ver resposta: Não. Falta outra assinatura criptográfica válida.**
> O consentimento numa conversa e uma assinatura válida constituem evidências diferentes.

Recuperar e alterar uma carteira multiassinatura

Objetivo

Recuperar a política e planejar perda ou substituição de participantes.

Compreender

A recuperação precisa de duas categorias: dados que reconstruem a política e capacidade privada suficiente para gastar. Uma cópia de política com xpubs pode revelar histórico sem incluir sementes. Uma cópia cifrada adiciona proteção ao ficheiro, mas exige que sua palavra-passe seja mantida. A extensão.cuvexms não mostra por si só que está cifrada: o formato e a sua exportação concreta devem ser verificados.

Em Desk 9.21 a recuperação solicita a chave pública estendida do participante com pegada e rota BIP48 exportada do seu dispositivo. Aceita a leitura por webcam ou Mirror do fluxo compatível. Não substituas essa contribuição por um endereço de receção nem envia a semente ao suporte.

Se uma chave for perdida numa 2 de 3, as outras duas podem manter a capacidade de gasto. A política anterior continua a ser a mesma; para retirar de forma efetiva um participante e estabelecer outras chaves, geralmente se cria uma nova política e se transfere fundos com as autorizações necessárias. Mudar um alias ou remover uma carteira do Desk não altera o UTXOs existente.

As cópias de segurança devem permitir reconstruir ambos os ramos e descobrir o histórico. Conserva índices, solicitações emitidas e o contexto necessário para não reutilizar endereços ou interpretar uma carteira vazia por um leitura incompleta. Restaurar e reiniciar uma operação pendente deve respeitar o perfil que foi guardado ao criá-la.

Prática

1. Exporta e restaura uma política de laboratório através da função documentada. Verifica rede e endereço conhecido.
2. Simula perda de um participante e prepara um plano de rotação, sem mover fundos reais.
3. Simula perda por debaixo do limiar. Reconhece que suporte ou IA não podem produzir as assinaturas faltantes.

Mostra o que aprendeste

Podes recuperar o cenário de testes e distinguir restaurar informações de mudar controlo sobre moedas.

Pergunta frequente

Eliminar a multiassinatura no Desk desativa a carteira para todos? Não. Elimina o estado local de acordo com o fluxo. Outras pessoas e cópias podem continuar a manter a capacidade compatível com a política.

Ponto de pausa

Conserva cópia comprovada e plano privado; registra no curso apenas o resultado.

Queres retirar uma pessoa de uma política que já recebeu fundos. Basta apagar o nome no Desk?

1. Sim.
2. Sim, se o chat também for eliminado.
3. Não. É necessário planear uma nova política e a movimentação autorizada dos fundos quando aplicável.

> **Ver resposta: Não. É necessário planear uma nova política e a movimentação autorizada dos fundos quando aplicável.**
> Editar registos locais não altera os scripts das UTXO existentes.

Atualizar o firmware sem improvisar

Objetivo

Preparar uma atualização compatível e verificar seu resultado no dispositivo.

Compreender

Uma atualização muda software fiável. Verifica modelo, revisão de hardware, versão, origem e mecanismo de autenticação do fabricante. Uma descarga completa ou um hash igual ao de uma página não substituem a verificação de assinatura e compatibilidade. Nunca instales uma aplicação de firmware sem assinatura para o engenheiro como se fosse uma publicação para clientes.

Original atualiza por Bluetooth no fluxo documentado. BIT usa USB-C. Mirror incorpora percursos de preparação e transporte compatíveis. Não se promete que uma combinação concreta de PC, telefone e dispositivo funcione até completar a aceitação física dessa combinação. A incidência histórica de atualização de Original em Windows exige diagnóstico específico; não é resolvido ficando um sucesso no 99 %.

Antes de começar, verifique os suportes recuperáveis, alimentação estável e ausência de outras operações. Prepara o ficheiro oficial ou cópia previamente verificada de acordo com a app. Durante o envio, diferencia transferência, validação, instalação, reinicio e verificação de versão. A barra não é uma prova final.

Ao terminar, verifique a versão visível no computador e registre data e resultado. O catálogo de compatibilidade do Desk não mede o firmware à distância: firmwareAttestation mantém o valor false. Selecionar um perfil Final não acredita quais bytes estão realmente instalados. Se a atualização falhar, segue o procedimento de recuperação documentado e anota a fase e o erro. Não desligues o equipamento às cegas numa etapa crítica.

Prática

1. Revisa uma lista de preparação sem iniciar uma atualização real durante o ensaio.
2. Ele ordena estados e explica por que «transferido» e «instalado» são diferentes.
3. Redie um relatório fictício de falha para o 99 % com modelo, versão, sistema, fase e mensagem final.

Mostra o que aprendeste

Podes identificar o artefato adequado, o transporte e o critério final de sucesso.

Pergunta frequente

Devo atualizar apenas para que um erro de Desk desaparece? Em primeiro lugar, identificar a origem. Uma incompatibilidade do catálogo pode exigir que o Desk seja corrigido e que o firmware seja validado.

Ponto de pausa

Uma atualização real só é interrompida num estado expressamente seguro do procedimento, não por chegar ao fim da chamada.

O que verifica, por si só, o catálogo explícito do Desk?

1. As referências de compatibilidade admitidas, sem medir remotamente o firmware instalado.
2. A atestação física de todos os dispositivos ligados.
3. A ausência de vulnerabilidades.

> **Ver resposta: As referências de compatibilidade admitidas, sem medir remotamente o firmware instalado.**
> Compatibilidade, assinatura, medição e aceitação física são evidências diferentes.

M10

Perda, avaria e recuperação de emergência

Objetivo

Escolher uma recuperação proporcional ao incidente e preservar evidências úteis.

Compreender

Perante um incidente, identifica primeiro o que se perdeu ou ficou exposto: computador, dispositivo, cartão, ficheiro, palavra-passe, frase-semente, passphrase ou política. «Não posso entrar» não significa necessariamente «me roubaram». Se suspeitares que um equipamento foi comprometido, não continues a introduzir segredos nesse equipamento.

A perda do dispositivo pode ser resolvida com suportes e credenciais de recuperação compatíveis. A perda do computador pode exigir restaurar o armazém de Desk e reconstruir observação. Perder todos os meios de desbloqueio ou todas as chaves necessárias debaixo do limiar pode não ter solução técnica. Nenhuma IA pode garantir o resgate de chaves inexistentes.

Desk inclui uma recuperação local para formatos admitidos e exportação do material de recuperação correspondente. Decifrar no PC pode expor o segredo ao sistema operacional ou malware. É uma decisão excepcional: utiliza um ambiente preparado, material compatível e plano de transferência para novas chaves se o segredo pudesse ficar comprometido. Não o descreva como uma operação equivalente ao isolamento habitual de Cuvex.

Se uma semente foi filtrada, mudar a palavra-passe de Desk não revoga essa semente. Deves avaliar a transferência autorizada para uma nova carteira e protegê-la de um equipamento fiável. Evita publicar detalhes do incidente que ajudem o atacante ou pagar serviços que prometem recuperação em troca de outra semente ou antecipos fraudulentos.

Prática

1. Resolve quatro situações fictícias: PC perdido, cartão danificado com cópia válida, palavra-passe esquecida e frase-semente exposta.
2. Para cada uma, identifica material necessário, risco de ação e critério de recuperação.
3. Tente o procedimento apenas com dados de aprendizagem; não carregue ficheiros de emergência reais ao tutor.

Mostra o que aprendeste

Podes escolher entre restaurar, reconfigurar observação, migrar controlo ou escalar para um especialista, sem afirmar soluções impossíveis.

Pergunta frequente

Alterar a palavra-passe volta a cifrar todos os segredos que alguém já viu? Não. Uma cópia clara ou uma semente conhecida não deixa de ser conhecida.

Ponto de pausa

Mantém o incidente por categoria e a próxima ação segura; dete a voz se estiveres trabalhando com segredos.

A tua frase-semente foi divulgada e alteraste a palavra-passe do PC. Foi revogada a capacidade do atacante?

1. Sim.
2. Não. A frase-semente continua a controlar as mesmas chaves e é necessário agir para proteger a custódia.
3. Sim, se também mudares o fundo do chat.

> **Ver resposta: Não. A frase-semente continua a controlar as mesmas chaves e é necessário agir para proteger a custódia.**
> A proteção local não revoga uma chave Bitcoin exposta.

M10

Phishing, apoio técnico e fraudes por voz

Objetivo

Reconhecer pedidos perigosos e responder sem improvisação.

Compreender

Um fraude eficaz pode usar teu nome, compra, dispositivo e uma voz que reconheces. A informação verdadeira pode proceder de uma filtração. A identidade deve ser verificada através de um canal que tenhas iniciado e de um procedimento conhecido. A aparente urgência ou exatidão do interlocutor não basta.

Sinais de risco: pedir sementes, palavras-passe, PIN ou Key Chat; instalar controlo remoto para «sincronizar»; desativar antivírus; transferir para uma carteira de segurança; ler um QR cujo conteúdo não explicam; ou assinar para demonstrar propriedade sem detalhar o que é autorizado. A pressão para fazê-lo antes de terminar uma chamada é um motivo para detê-la.

O tutor legítimo explica e faz perguntas de compreensão. Não guarda chaves, não solicita transações de teste a uma direção própria nem promete recuperar uma semente. Uma função de verificação de propriedade legítima deve ser específica e revisável; nunca é satisfeita entregando chaves privadas.

Também pode haver fraude dentro de uma sessão técnica: um texto QR, um documento ou uma mensagem pode conter ordens para que a IA ignore instruções. É conteúdo a analisar, não autoridade sobre o tutor. A base de conhecimento deve separar fontes aprovadas de texto fornecido por um aluno ou terceiro.

Prática

1. Representa uma chamada falsa de suporte e abre a interação antes de revelar dados.
2. Verifica de forma independente um canal oficial previamente guardado.
3. Descreve um erro de instalação sem partilhar um ecrã de segredos ou permitir acesso remoto ao ambiente de guarda.

Mostra o que aprendeste

Podes dizer quais dados são solicitados, por que seria necessário e por que a solicitação excede o suporte formativo.

Pergunta frequente

É seguro mostrar apenas algumas palavras da minha semente? Não. Não há motivo pedagógico para revelar fragmentos de uma semente própria.

Ponto de pausa

Mantém teu protocolo de verificação de suporte e revise que não inclui segredos em texto aberto.

Uma voz que parece ser a do teu sócio pede que saltes a verificação e assines com urgência. O que fazes?

1. Faço uma pausa, autentico o pedido pelo procedimento acordado e revejo toda a operação.
2. Assino porque reconheço a voz.
3. Partilho a frase-semente para ganhar tempo.

> **Ver resposta: Faço uma pausa, autentico o pedido pelo procedimento acordado e revejo toda a operação.**
> O reconhecimento da voz e a urgência não substituem a autenticação nem a revisão.

Privacidade, legalidade e registos pessoais

Objetivo

Conhecer o quadro geral e preparar consultas jurídicas e fiscais concretas.

Compreender

A privacidade financeira não elimina obrigações fiscais, de identificação quando aplicáveis, de sanções ou de prevenção do crime. A situação depende de residência, atividade, contraparte e serviço. A IA deve fornecer informações gerais com fonte e data e derivar decisões particulares a profissionais competentes.

Na UE, a MiCA regula certas criptomoedas e serviços. A sua aplicação geral começou em 30 de dezembro de 2024 e o regime transitório máximo indicado no regulamento chegou a 1 de julho de 2026, sujeito a decisões nacionais. Verifica autorização e alcance em registos oficiais em vigor; não basta uma menção antiga de registo. A autorização não garante preço, solvência ou compensação total.

O Regulamento 2023/1113 estabelece informações que acompanham transferências quando os fornecedores obrigados intervêm. Para transferências superiores a 1.000 euros com direcções autocustodiadas contempla medidas para avaliar propriedade ou controlo. Esse limiar não cria uma isenção geral de identificação abaixo. As transferências entre pessoas sem fornecedor têm uma exclusão de alcance nesse regulamento; ainda existem outras obrigações.

Conserva documentação suficiente de compras, vendas, comissões e origem segundo o teu caso, protegida de acessos desnecessários. Não precisas publicar o histórico completo para levar registos privados. Também não se ensina fragmentar operações para eludir controlos, falsificar informações ou ocultar rendimentos.

Se houver gravação ou transcrição de voz e progresso identificável, o serviço deve definir finalidade, base jurídica, conservação, acesso, encarregados e direitos aplicáveis. A configuração de privacidade comercial é válida antes de vender, não é improvisada durante uma chamada.

Prática

1. Redige para um consultor um caso fictício que indique a residência, a atividade e as operações, sem incluir chaves.

2. Verifica onde verificar a autorização do fornecedor e a data da informação.
3. Desenvolve um registo privado de movimentos e uma política mínima de dados do aluno.

Mostra o que aprendeste

Podes distinguir uma regra jurídica, uma política de câmbio e uma capacidade técnica de Bitcoin.

Pergunta frequente

Qualquer autodistribuição é proibida na UE? Isso não se deduz das regras citadas. Evita titulares absolutos e comprove a disposição concreta e o seu alcance.

Ponto de pausa

Mantém questões pendentes para o teu conselheiro sem introduzir documentos pessoais no tutor.

O limiar de 1.000 euros referido para certas medidas de controlo do endereço elimina todas as obrigações abaixo desse valor?

1. Sim.
2. Só se dividires a operação.
3. Não. Não é uma isenção geral de identificação ou de outras obrigações.

> **Ver resposta: Não. Não é uma isenção geral de identificação ou de outras obrigações.** A norma deve ser interpretada de acordo com a medida e o seu âmbito. Um limiar não constitui uma isenção universal.

Herança, continuidade e simulação anual

Objetivo

Criar um plano que permita que pessoas autorizadas atuem sem expor tudo antecipadamente.

Compreender

A herança combina legitimidade jurídica, localização de materiais e capacidade técnica. Uma pessoa pode ter direito a herdar e não saber reconstruir uma carteira; outra pode ter uma chave e não ter autorização para usá-la. O plano deve resolver ambas as dimensões com aconselhamento adequado.

Separa instruções públicas de acesso a segredos. O inventário descreve o que existe, a quem entrar em contacto e quais verificações fazer, sem colocar todas as chaves e palavras-passe juntas num documento amplamente acessível. Evita publicar sementes em testamentos ou expedientes que possam circular fora do teu controlo.

Em multiassinatura desenha quem conserva política e cópias, que faixa está disponível após uma perda e o que acontece se uma pessoa-chave morrer. Um mesmo guarda-chuva guardando componentes suficientes pode se tornar um ponto único de abuso. Uma distribuição muito complexa pode tornar o património irreversível.

Inclui a recuperação das palavras-passe do criptograma e da passphrase, se existir, os dados de derivação, a compatibilidade dos dispositivos e o procedimento caso o fabricante deixe de operar. Não presuma que um ficheiro proprietário ou uma pegada biométrica sejam usáveis sem preparação. A interoperabilidade deve ser testada com dados de teste e formatos documentados.

Revisa após mudanças familiares, de domicílio, de política, de software ou de participantes, e realiza um simulacro periódico. O exercício deve provar que uma pessoa de confiança entende as instruções sem revelar o património ou mover dinheiro desnecessariamente.

Prática

1. Completa uma equipe privada com responsáveis, componentes, acesso autorizado e substitutos.
2. Dá instruções de laboratório a outra pessoa sem explicá-las oralmente e observa onde ele está bloqueado.

3. Corre ambigüidades e registra uma data de revisão. O curso não cria lembranças automaticamente.

Mostra o que aprendeste

Podes explicar o que acontece se não estiveres disponível e quais informações cada rol precisa em cada etapa.

Pergunta frequente

Uma 2 de 3 substitui um plano de herança? Não. É uma ferramenta técnica. Os herdeiros ainda precisam de contexto, materiais, coordenação e legitimidade.

Ponto de pausa

Mantém o plano fora do curso e marque apenas "simulacro analisado".

Qual é um critério útil para avaliar um plano de sucessão?

1. Uma pessoa autorizada conseguir executar uma simulação documentada sem improvisar nem receber segredos antes do tempo.
2. Ter muitas páginas.
3. Depender apenas da memorização de uma palavra-passe.

> **Ver resposta: Uma pessoa autorizada conseguir executar uma simulação documentada sem improvisar nem receber segredos antes do tempo.**
> A capacidade de recuperação e o controlo de acesso têm de ser testados na prática.

Preço, poupança e análise fundamental

Objetivo

Analisar argumentos de investimento sem confundir com propriedades técnicas verificáveis.

Compreender

Preço é o resultado de trocas em mercados específicos e pode diferir entre plataformas. Liquidez, moeda de cotização, profundidade, horário de fornecedores bancários e demanda influenciam o resultado que podes executar. Uma nota de ecrã não é uma oferta garantida para o teu volume.

A análise fundamental estuda fatores como adoção, demanda, competência, segurança econômica, regulação e oferta. Um calendário de emissão conhecido não determina por si só o preço futuro. As avaliações sobre utilidade monetária ou «valor intrínseco» dependem de supostos; não há uma cifra objetiva que a IA possa apresentar como certeza universal.

Uma estratégia de compras periódicas distribui o momento de entrada, mas não garante lucro nem evita perdas prolongadas. O poupança a longo prazo também precisa de liquidez para obrigações, tolerância à volatilidade e um plano de custódia. O curso não define uma percentagem do teu património nem toma decisões por ti.

Separa três perguntas: entendendo o ativo?, posso custodi-lo e recuperá-lo?, posso assumir o seu risco econômico? Dominar chaves não responde automaticamente à terceira. A formação não converte uma projeção de preço ou um gráfico histórico numa recomendação personalizada.

Prática

1. Escreve uma tese fictícia, os seus pressupostos e os factos que a invalidariam.
2. Simula uma queda do 50 % e necessidades de liquidez simultâneas, sem introduzir teu património real.
3. Identifica quais dados do argumento são verificáveis e quais são as expectativas.

Mostra o que aprendeste

Podes discutir investimento sem prometer rentabilidade ou confundir convicção com evidência.

Pergunta frequente

A escassez garante que o preço sobe? Não. A demanda e outras condições continuam a ser decisivas para o preço de mercado.

Ponto de pausa

Guarda supostos de laboratório, não uma instrução automática de compra.

O que garante uma compra periódica?

1. Lucro a longo prazo.
2. Nenhuma rentabilidade. Apenas distribui os momentos de compra segundo uma regra escolhida.
3. Proteção contra a perda de chaves.

> **Ver resposta: Nenhuma rentabilidade. Apenas distribui os momentos de compra segundo uma regra escolhida.**
> Distribuir as entradas no mercado não elimina o risco económico nem o operacional.

M11

Escolher onde adquirir bitcoin

Objetivo

Avaliar um fornecedor por autorização, custo, retirada, privacidade e risco de custódia.

Compreender

Compara fornecedores através de critérios verificáveis: entidade jurídica e jurisdição, serviços autorizados, rede de retirada, comissões, diferencial de preço, limites, suporte, autenticação e tratamento de dados. O nome comercial ou um patrocínio não demonstram autorização para o serviço específico.

O custo total pode incluir depósito, conversão, spread, comissão de negociação, retirada e custo bancário. Uma negociação «sem comissão» pode ter um diferencial de preços mais elevado. Verifica quantidades líquidas e moeda de referência. O orçamento deve incluir retirar-se a autodistribuição quando esse é o teu objetivo.

Enquanto manténs um saldo custodial dependes do fornecedor. Uma prova de reservas não demonstra por si só todos os passivos, propriedade de fundos ou solvência futura. Verifica restrições e faça uma pequena retirada que podes permitir antes de depender de um novo fluxo.

A identificação comercial pode associar tua identidade a uma retirada. Proteger essas informações posteriormente não equivale a apagar o que o fornecedor conhece. Não falseie dados nem use o curso para evitar obrigações. A compra de um código de treinamento também gera um registo comercial separado da tua carteira.

Prática

1. Preenche uma matriz fictícia para dois prestadores com o custo total, a rede, o levantamento mínimo, a autorização e os dados exigidos.
2. Calcula o neto para uma operação de aprendizagem com todos os cargos especificados.
3. Deseja uma retirada de teste para uma direcção previamente verificada, sem executá-la a partir deste minisite.

Mostra o que aprendeste

Podes justificar uma escolha para o teu caso e reconhecer quais informações estão expiradas ou não verificadas.

Pergunta frequente

O curso recomenda um intercâmbio como o melhor para todos? Não. As permissões, tarifas, países atendidos e condições mudam. A comparação exige data e caso de uso.

Ponto de pausa

Mantém a matriz sem credenciais ou documentos de identificação.

Que comparação é mais útil do que olhar apenas para a comissão de negociação?

1. O custo total até receber BTC na rede e no endereço pretendidos.
2. O número de seguidores do prestador.
3. A cor da sua aplicação.

> **Ver resposta: O custo total até receber BTC na rede e no endereço pretendidos.**
> O preço final inclui componentes que podem ficar fora da comissão anunciada.

Contas, ordens e custos de execução

Objetivo

Entender ordens básicas e proteger a conta sem converter o curso num terminal de negociação.

Compreender

Uma ordem de mercado prioriza execução disponível, com risco de deslizamento. Uma ordem limitada fixa um preço máximo de compra ou mínimo de venda, mas pode não ser executada ou parcialmente. Uma ordem stop activa outra ação de acordo com as regras do fornecedor; não garante por si só o preço final.

O livro de encomendas mostra ofertas disponíveis, não compromissos de que todos os volumes permanecerão. Numa queda ou baixa liquidez, o resultado pode diferir da última cotização. As ordens stop-market e stop-limit têm riscos diferentes: execução a pior preço em comparação com possível não execução.

Protege o acesso com uma palavra-passe única, autenticação resistente ao phishing quando suportada, revisão de sessões e controlos de retirada adequados. Mantém a recuperação de segundo fator de forma independente. Uma chave API para automatizar pode ter permissões mais perigosas do que aquelas que precisam de uma leitura de dados; não a introduza no tutor nem no minisite.

Antes de retirar, verifique ativo e rede Bitcoin, endereço de tua carteira e quantidades líquidas. Uma plataforma pode usar os mesmos símbolos para produtos diferentes. Ao terminar, conserva documentação de compra, execução, comissões e retirada conforme o teu caso; não confunda retirada à tua própria carteira com uma nova compra.

Prática

1. Simula um livro fictício com 1 unidade a 100 e outra a 102. Explica por que comprar dois no mercado não garante preço médio 100.
2. Desenha uma ordem limitada e descreva o cenário em que não se completa.
3. Revê as permissões de uma API fictícia e remove a de levantamento se só forem necessárias consultas.

Mostra o que aprendeste

Podes descrever prioridade, preço e risco de não execução para cada pedido.

Pergunta frequente

Um stop-loss sempre limita a perda exatamente? Não. Gaps, liquidez, deslizamento e regras do fornecedor podem impedir isso.

Ponto de pausa

Guarda o resultado do exercício sem ordens reais ou chaves API.

Que risco mantém uma ordem limitada de compra a 100?

1. Nunca ser executada ou sê-lo apenas em parte.
2. Ter de ser executada a qualquer preço.
3. Criar automaticamente uma cópia de segurança.

> **Ver resposta: Nunca ser executada ou sê-lo apenas em parte.**
> O controlo do preço tem como contrapartida a possibilidade de a ordem não ser executada.

Velas, indicadores e enviesamentos da análise técnica

Objetivo

Leia gráficos como dados históricos e avaliar uma estratégia sem confundir padrões com previsão.

Compreender

Uma vela resume abertura, máximo, mínimo e fechamento de um período. O volume depende da fonte. Mudar plataforma, moeda, fuso horário ou período pode mudar o que vês. Uma vela não mostra toda a ordem temporal de movimentos dentro de seu intervalo.

Uma média móvel suaviza preços passados. Um indicador de momento transforma dados observados sob uma fórmula. Ninguém conhece o futuro. Dois indicadores derivados da mesma série podem fornecer informações muito correlacionadas, embora suas cores e nomes sejam diferentes.

Para avaliar uma regra define entrada, saída, invalidez, custos, tamanho e dados antes de olhar para o resultado. Evita selecionar apenas exemplos ganhadores, ajustar parâmetros até que eles encaixem ou usar dados futuros numa decisão passada. Distinguir dados de treinamento e validação temporária.

Um backtest deve considerar espalhamento, comissões, deslizamento, disponibilidade de dados e execução possível. Rentabilidade bruta, taxa de correcto, perda máxima e distribuição de perdas respondem a perguntas diferentes. Um sistema com muitos bons pode perder dinheiro se seus erros são grandes. Não é ensinado um sinal de compra ou venda como certeza.

Prática

1. Lê uma vela fictícia e explica quais informações temporárias não contêm.
2. Escreve uma regra antes de avaliar dez resultados sintéticos, com custos e critério de falha.
3. Compara 9 ganhos de 1 com uma perda de 15: o resultado bruto é -6 apesar do 90 % certo.

Mostra o que aprendeste

Podes criticar um resultado atraente por seleção, custo ou risco sem ter que executar operações.

Pergunta frequente

Combinar muitos indicadores garante um melhor sinal? Não. Poda aumentar a sobreajustamento e complexidade sem fornecer informações independentes.

Ponto de pausa

Mantém a regra e os resultados de laboratório, não uma ordem de mercado.

Nove operações ganham 1 cada e uma perde 15. Qual é o resultado antes de custos?

1. +90 %.
2. +6.
3. −6.

> **Ver resposta: −6.**
> Nove unidades ganhas menos quinze perdidas dão um prejuízo de seis unidades.

M11

Margem, futuros e automatização

Objetivo

Reconhecer exposição, liquidação e falhas de automatização antes de considerar produtos complexos.

Compreender

A alavancagem aumenta a exposição em relação ao capital investido. Num exemplo simplificado, a margem 100 para uma exposição de 1.000 implica que um movimento adverso do 5 % do subjacente equivale a 50 antes de custos: metade da margem inicial. As regras reais de manutenção, liquidação, colateral e comissões podem piorar o resultado e ativar-se antes do esperado.

Futuros e perpétuos podem incluir vencimento, liquidação por diferenças, taxas de financiamento e preços de referência diferentes do último intercâmbio. Eles não são equivalentes a retirar bitcoin nativo a Cuvex. Custodiar uma semente não protege uma posição contra liquidação ou falha de contraparte.

Um bot automatiza regras, incluindo seus erros. Precisa de limites de posição, permissões mínimas, idempotência de ordens, reconciliação, controlo de perdas, interrupção de emergência e supervisão. Duplicar uma solicitação após um timeout pode duplicar uma exposição se o resultado anterior não for conhecido.

A IA pode explicar conceitos e detetar incoerências num caso fictício. Não deves receber chaves API, ativar negociação ou prometer uma estratégia rentável. Para o objetivo principal deste curso, entender esses riscos permite decidir não usar produtos que não são entendidos.

Prática

1. Resolve o exemplo de exposição e margem sem assumir que o nível de liquidação é exatamente um 10 %.
2. Simula uma API que executa uma ordem, mas perde a resposta. Explica por que antes de repetir precisas reconciliar.
3. Desenha um botão de parada que impede novas encomendas e verifica as já abertas, sem ligar um corretor.

Mostra o que aprendeste

Podes descrever um risco que sobrevive ao stop, outro que sobrevive ao bot e outro que sobrevive à autocustódia de fundos externos.

Pergunta frequente

Automatizar elimina emoções e por isso garante resultados? Não. Poda reduzir uma intervenção impulsiva e multiplicar erros de design ou execução.

Ponto de pausa

Marca esta ampliação como compreendida sem habilitar produtos complexos.

Com uma exposição de 1.000 e uma margem de 100, a quanto equivale uma perda de 5 % da exposição, antes de custos?

1. Uma perda de 5.
2. Uma perda de 50, ou seja, 50 % da margem.
3. Nenhuma perda se for usado um bot.

> **Ver resposta: Uma perda de 50, ou seja, 50 % da margem.**
> A alavancagem e os custos fazem com que o resultado sobre a margem seja diferente da variação do ativo.

M12

Lightning e outras camadas

Objetivo

Entender pagamentos por canais e reconhecer as funções que o fluxo Cuvex analisado não oferece.

Compreender

A Lightning utiliza canais e mecanismos de atualização para realizar pagamentos sem registar cada troca individual na cadeia de base. Abrir ou fechar canais e certos cenários de recuperação podem implicar transações on-chain. A disponibilidade, liquidez de entrada e saída e vigilância dependem do design da carteira e dos serviços utilizados.

Uma fatura pode incluir montante, descrição e caducidade. A unidade pode ser expressa em satoshis ou milisatoshis segundo o contexto, sem que estes últimos impliquem saídas sub-satoshi na cadeia base. Pagar uma fatura requer compatibilidade e rota disponíveis; um QR não garante que possas pagar com qualquer aplicação.

Há serviços custodiais e não custodiais com modelos muito diferentes. A velocidade habitual não mostra a ausência de riscos. Lightning também não deve ser apresentado como anonimato completo: existem observadores, rotas, contrapartes e metadados relevantes.

O chat de Cuvex pode coordenar pedidos de sats que são pagos pela conta WOW em cadeia. Nesta edição não se atribui a Desk um nó Lightning, gestão de canais ou assinatura de facturas Lightning. Se uma solicitação inclui várias modalidades, verifique qual entendes e qual irá executar tua aplicação.

Prática

1. Classifica um endereço on-chain, um URI bitcoin: e uma invoice Lightning didácticas.
2. Compara pagar por cadeia e por canal em termos de confirmação, liquidez, custódia e recuperação.
3. Explica por que uma fatura expirada deve ser analisada com o receptor e não reinterpretada como endereço.

Mostra o que aprendeste

Podes rejeitar uma modalidade incompatível sem expor chaves ou atribuir uma falha a Cuvex.

Pergunta frequente

Todos os pagamentos em sats são Lightning? Não. Os satoshis expressam valor; a modalidade depende do protocolo utilizado.

Ponto de pausa

Guarda a modalidade do exercício, sem facturas reais.

Que informação permite saber se um pedido é pago através da Lightning?

1. O uso da palavra sats.
2. O pedido chegar por chat.
3. O formato e a modalidade compatíveis, para além da unidade ou do canal da mensagem.

> **Ver resposta: O formato e a modalidade compatíveis, para além da unidade ou do canal da mensagem.**
> A unidade de conta e a rede de pagamento são aspetos distintos.

Taproot, MuSig2 e o futuro pós-quântico

Objetivo

Distinguir padrões, propostas e capacidades implementadas.

Compreender

Taproot permite condições de gasto com caminhos de chave e de script. As firmas Schnorr e a agregação podem melhorar certas construções, mas o resultado de privacidade depende de como é configurado e gasto. Que um endereço seja bc1p não demonstra que não há outros participantes nem revela todas as suas condições ocultas.

MuSig2 permite que um conjunto de signatários adicione chaves e produza uma assinatura Schnorr compatível por interação. O padrão base é N de N. Um limiar arbitrário M de N requer outra construção ou protocolo adicional. A gestão dos nonces e das sessões é fundamental e não se faz por troca informal de mensagens.

PSBT v2 reorganiza informações sobre v0; não é uma atualização automática de qualquer ficheiro que contém uma transação de versão 2. Os firmwares Final desta edição conservam PSBT v0, P2WSH/sortedmulti e SIGHASH_ALL para o perfil multiassinatura. As futuras capacidades requerem contrato e validação próprias.

A NIST publicou em 2024 os seus primeiros padrões pós-quânticos finalizados. Isso não muda por si só as assinaturas de Bitcoin. Usar um algoritmo pós-quântico para autenticar firmware protegeria essa camada; não converteria automaticamente ECDSA ou Schnorr de um UTXO em assinaturas pós-quânticas. Também não há uma data de ataque futuro que o tutor possa prometer com certeza.

Prática

1. Classifica cinco afirmações como padrão, implementação verificada, proposta ou publicidade.
2. Explica por que "accepta um destinatário Taproot" não prova "firma uma entrada Taproot".
3. Desenha camadas separadas: firmware, criptografia de segredo, chat e Bitcoin expendimento assinatura.

Mostra o que aprendeste

Podes pedir evidências específicas de uma camada e evitar transferir garantias entre protocolos.

Pergunta frequente

Devo migrar meus fundos por um titular sobre computação quântica? Uma decisão real exige evidência técnica atual, suporte verificável, avaliação de riscos e um plano de migração seguro; o curso não ordena movimentos por titulares.

Ponto de pausa

Regista perguntas técnicas sem criar um plano de despesa automático.

Uma assinatura pós-quântica no bootloader, se implementada e validada, altera as condições de assinatura de uma UTXO existente?

1. Não. São camadas diferentes.
2. Sim. Converte toda a rede para outro algoritmo.
3. Elimina a necessidade de cópias de segurança.

> **Ver resposta: Não. São camadas diferentes.**
> Autenticar uma atualização não reescreve as condições de gasto do Bitcoin.

Interoperabilidade e independência do fabricante

Objetivo

Planejar continuidade se mudares o software, o dispositivo ou o fornecedor.

Compreender

A interoperabilidade não é verificada com uma lista de siglas. Deve conservar rede, script, derivação, chaves, política, formato de transação e semântica de assinaturas. Duas aplicações podem entender BIP174 e, no entanto, não admitir os mesmos campos, tamanhos ou tipos de entrada.

Para sair de uma dependência de interface, conserve informações de recuperação documentadas e ensai com carteiras de aprendizagem. Uma mnemônica padrão pode permitir derivar chaves, mas a recuperação de uma multiassinatura requer sua política completa. As etiquetas BIP329 adicionam um contexto de privacidade; o histórico de chat tem um alcance diferente.

Não convertas uma prova de compatibilidade em exposição de uma semente real. Primeiro, verifica a exportação pública de descritores e recuperação watch-only. Se uma emergência exige reconstruir chaves, use um ambiente projetado para isso e considere migrar depois. Uma carteira incompatível que mostra zero não mostra por si só que os fundos se perderam.

Mantém uma cópia verificável da documentação, versão do curso e ferramentas necessárias. A assinatura de aplicações, certificados caducados e mudanças de sistemas podem afetar a instalação. Um código aberto disponível não garante que qualquer pessoa possa compilá-lo anos depois sem conservar dependências e conhecimento.

Prática

1. Desenha uma prova de saída com uma conta vazia: a mesma rede, política e endereço de controlo em duas implementações compatíveis.
2. Indica quais os componentes normalizados e quais exigem um conversor ou a documentação do formato Cuvex.
3. Define qual resultado permite afirmar compatibilidade e o que fica pendente de hardware ou assinatura real.

Mostra o que aprendeste

Podes descrever uma rota de recuperação sem depender de que uma empresa continue a oferecer o mesmo serviço.

Pergunta frequente

O código aberto significa que o fabricante não importa mais? Não. Distribuição, manutenção, componentes físicos e experiência operacional continuam importando. Permite inspeção e continuidade potencial, não uma garantia automática.

Ponto de pausa

Guarda resultados de laboratório com versões e limites observados.

Qual é a evidência mais forte de interoperabilidade?

1. As duas aplicações dizerem «Bitcoin».
2. Reconstruir e verificar no laboratório a mesma política e o mesmo endereço com versões identificadas.
3. Terem ícones semelhantes.

> **Ver resposta: Reconstruir e verificar no laboratório a mesma política e o mesmo endereço com versões identificadas.**
> O teste deve preservar as condições relevantes e produzir um resultado verificável.

M12

Laboratório técnico com regtest

Objetivo

Entender um laboratório reprodutor sem confundir testes sintéticos e uso físico.

Compreender

A regtest permite criar uma cadeia local controlada para gerar blocos e testar transações sem valor económico. Deves usar diretórios e credenciais separados, independentemente do material real. Seus resultados não demonstram por si só compatibilidade USB, NFC, Bluetooth ou câmera de um dispositivo físico.

Um laboratório completo registra versões, configuração de rede, política, entradas de teste, PSBT, assinaturas, transação final e resultado de aceitação. Podes verificar que a soma quadrada, que uma assinatura alterada é rejeitada e que um pagamento válido entra num bloco local. O ensaio deve incluir falhas, não apenas o caminho certo.

A validação do Desk 9.21 informa de testes com o Bitcoin Core 31 regtest e de testes automatizados de motor e UI simulado. Esta edição usa-as como evidência documental, não afirma ter repetido essas provas nem executado operações com dispositivos. A verificação de um pacote também não prova sua instalação em todos os sistemas.

Antes de uma classe técnica, o engenheiro deve entregar o laboratório montado e o procedimento compatível com a versão do aluno. Não abras RPC para a Internet para que o tutor o controlo. A IA pode guiar a interpretação de resultados sintéticos, mas não deve obter credenciais ou permissões de administração.

Prática

1. Com o laboratório preparado, observa uma transação válida e outra com uma assinatura alterada. Regista aceitação ou rejeição.
2. Verifica um caso de mudança incorrecta e outro de rede incompatível.
3. Separa no teu relatório «teste de motor», «interface simulada» e «hardware físico».

Mostra o que aprendeste

Podes descrever exatamente o que foi testado e o que fica pendente, sem apresentar uma simulação como certificação.

Pergunta frequente

Se regtest funciona, posso vender o curso como validado para todos os dispositivos? Não. Faltam testes de percursos físicos, instalação, acessibilidade, recuperação e serviço comercial.

Ponto de pausa

Detém e guarda o laboratório de acordo com as suas instruções, conservando apenas dados sintéticos.

Um teste do motor na regtest demonstra a leitura NFC real num telemóvel específico?

1. Sim, porque ambos usam Bitcoin.
2. Sim, se a PSBT for pequena.
3. Não. Exige um teste físico separado.

> **Ver resposta: Não. Exige um teste físico separado.**
> Os ambientes de validação têm âmbitos diferentes.

Projeto final e plano de continuidade

Objetivo

Demonstrar autonomia desde a preparação até a recuperação e privacidade.

Compreender

O resultado do curso não é memorizar um menu: é poder explicar a intenção, verificar o resultado e deter uma operação que não entendes. A avaliação combina conceitos, prática guiada e um caso independente. Nunca depende de revelar sementes, património ou endereços pessoais ao avaliador.

Caso A: Configura um ambiente de aprendizagem, identifica modelos e versões, protege o Desk, liga um criptograma didático e reconstrui uma conta watch-only. Explica quais os dados de suporte são necessários e quais os dados que o teu fornecedor pode observar.

Caso B: concebe um pagamento com UTXOs fictícias de contextos diferentes. Justifica a seleção, verifica o destinatário, o troco e a comissão e descreve o procedimento de assinatura correspondente ao teu dispositivo. Resolve uma interrupção de devolução e outra de publicação sem duplicar o pagamento. Se não houver hardware fisicamente aceito, a parte é registada como simulada e fica pendente.

Caso C: desenha uma 2 de 3, representa convite e verificação, compara em Mirror um campo escolhido em ordem livre e explica o alcance do OK. Recupera a política de aprendizagem, simula perda de um participante e prepara continuidade e herança.

A superação proposta exige pelo menos 80 % em conhecimentos e todos os controlos críticos corretos: não revelar segredos, verificar rede e saídas, não confundir etapas e conservar recuperação. Um erro crítico exige revisão e nova prática; não é compensado por perguntas de mercado corretas. Um certificado comercial, se emitido, deve indicar o que foi avaliado e se houve observação física ou apenas simulação.

Prática

1. Completa os três casos com dados sintéticos e uma explicação própria.
2. Resolve a avaliação final do anexo e revisa cada resposta falha.
3. Entrega apenas uma folha de resultados sem segredos, com evidências de alcance e pendentes.

Mostra o que aprendeste

Podes parar por iniciativa própria quando uma operação não tem evidência suficiente e sabes o que precisas para continuar.

Pergunta frequente

Terminar as páginas equivale a estar preparado para custodiar qualquer montante? Não. A capacidade deve ser testada e o risco deve ser avaliado de acordo com a tua situação. A leitura e os ensaios não garantem resultados futuros.

Ponto de pausa

Mantém o teu plano de revisão e as práticas pendentes. Podes voltar ao capítulo necessário sem repetir todo o curso.

Qual é um requisito crítico para concluir a formação prática?

1. Ter aberto todas as páginas.
2. Demonstrar a recuperação e a revisão de operações dentro de um âmbito documentado sem revelar segredos.
3. Prever o preço do próximo mês.

> **Ver resposta: Demonstrar a recuperação e a revisão de operações dentro de um âmbito documentado sem revelar segredos.**
> A aprendizagem comprova-se pelas capacidades e limites verificados, e não pela navegação ou por previsões.

Manual do aluno

Manual de utilização do Cuvex

Este manual acompanha as lições. Cada procedimento descreve o fluxo encontrado nas fontes analisadas, suas verificações e seu ponto de parada. Esta edição destina-se a um projeto-piloto. Não atesta testes físicos próprios com o Original, o BIT, telemóveis ou cada plataforma de computador. Antes de ensinar com fundos reais, o equipamento deve completar a matrícula de aceitação e ajustar qualquer rótulo ou ecrã que difira.

Referências: Original 1.2.2 Final, BIT 1.2.3 Final, Desk 1.0.0-beta.9.21 e Mirror 1.0.0-beta.12.12. A seleção de um perfil em Desk é compatibilidade declarada, não medição remota de firmware. As capturas reais incluídas do Mirror vêm do emulador Android do pacote 12.12. As fotografias de produto são materiais corporativos e não testam a versão mostrada num dispositivo atual.

P01 | Verificar a proveniência e a versão | Cuvex | L16,L21 | C01,C02

Preparação: dispõe da compra e do canal oficial que podes verificar de forma independente. Não introduzas segredos ainda.

1. Inspeciona a embalagem e os selos. Se houver sinais de manipulação, dete o lançamento e conserve evidência não sensível.
2. Usa o fluxo de integridade e selos da aplicação compatível com a tua entrega; introduza os códigos apenas lá, nunca ao tutor.
3. Identifica Original ou BIT e a revisão disponível. Verifica a versão visível do dispositivo e das apps.
4. Compara com a matrícula publicada pela equipe. Um catálogo ou um hash não substituem a autenticação de firmware ou a aceitação física.

Resultado: modelo e versões identificadas, e origem analisada sem exposição de segredos. Se os códigos não forem válidos ou a interface é diferente, não siga um guia histórico para forçar o uso.

Pausa: antes de carregar material de guarda. A traçabilidade comercial não garante por si só a ausência de manipulação avançada.

P02 | Atualizar o Original por Bluetooth | Original | L46 | C01,C02,C03

Preparação: cópias recuperáveis, alimentação estável, pacote oficial compatível e percurso aceito para o teu sistema. A disponibilidade física completa em cada plataforma não é acreditada por este curso.

1. Em dispositivos ou firmware da aplicação, selecione Original e download oficial ou ficheiro local autêntico correspondente.
2. Mantém o dispositivo atualizado de acordo com o seu menu e ligue-se pelo fluxo da aplicação. Mantém a proximidade e evite sessões competitivas.
3. Introduz o código do ecrã Original no campo indicado. Não o confundas com a palavra-passe do criptograma.
4. Seguem transferência, validação, instalação e reinição. Não tomes o percentual como prova de instalação.
5. Verifica a versão final em Original e registre-a na app se esse campo existe.

Resultado: versão verificada no ecrã após reiniciar e fluxo final confirmado. Se falhares antes do PIN, durante pacotes ou no final, registre essa fase e o código. Não desligues ou troque software de forma improvisada para «passar o 99 %».

P03 | Atualizar o BIT por USB | BIT | L46 | C01,C02,C03

Preparação: identifica o suporte real de BIT, alimentação e pacote oficial compatível. Mantém cópias antes de alterar o software.

1. Selecione o BIT no percurso de firmware Desk ou Mirror compatível.
2. Ligue o dispositivo pelo cabo e adaptador de dados adequados. Autoriza o acesso ao volume ou cartão quando a app o solicita.
3. Selecione o firmware autêntico do modelo. Verifica a versão e os dados de compatibilidade antes de enviá-lo.
4. Espera as etapas de transferência e validação do dispositivo. Um volume pode desaparecer ou reinstalar-se conforme o protocolo.
5. Depois de reiniciar, verifique a versão em BIT e o resultado final da aplicação.

Resultado: instalação comprovada no próprio equipamento. Se o volume não aparecer, verifique o modo do dispositivo, o cabo de dados, os permissões, a montagem e outra sessão ativa. Não cries uma pasta com o mesmo nome no PC como substituto. A recuperação de uma atualização falha requer o procedimento oficial desse hardware.

P04 | Gerar uma carteira com uma moeda e dados | Cuvex | L17 | C01

Preparação: espaço privado, dados adequados e moeda; sem microfone do tutor ativo nem câmeras. Usa uma carteira de aprendizagem.

1. Abre a criação de carteira e fluxo de entropia do firmware. Fica previamente a ordem dos quatro dados.
2. Introduz moeda e cada dado como indicado no ecrã, sem alterar resultados por preferência.
3. O código-fonte analisado calcula o índice = moeda × 1.296 + (d1−1) × 216 + (d2−1) × 36 + (d3−1) × 6 + (d4−1). Só aceita índices 0..2.047.
4. Antes de recusar, ele lançou novamente moeda e todos os dados. O aviso mantém as palavras anteriores e pede que o conjunto seja repetido.
5. Completa o algoritmo do dispositivo, incluindo a validação final, protege a mnemónica e verifica a recuperação em privado.

Resultado: carteira gerada pelo percurso completo, não palavras escolhidas manualmente. Se o ecrã e a fonte não concordam, pare de usar. Não uses um exemplo público de dados, sementes ou chaves como material próprio.

P05 | Cifrar um segredo | Cuvex | L18,L19 | C01

Preparação: escolha modelo, formato de conteúdo e proteção. A entrada num PC ou telefone expõe a origem mesmo que o destino esteja cifrado.

1. Seleciona a opção de cifragem e o tipo compatível: BIP39, SLIP39, Monero ou texto. Não troques dicionários. O teclado de texto plano analisado admite até 500 caracteres; armazenar outro formato não implica poder assinar sua rede.
2. Introduz o conteúdo diretamente no dispositivo para manter esse isolamento. Verifica ordem, caracteres e campos auxiliares na seu ecrã.
3. Escolhe proteção individual ou partilhada de acordo com o fluxo, e biometria em BIT, se necessário. Diferença este limiar do limiar Bitcoin.
4. Introduz e confirma as palavras-passe em privado de acordo com o validador do firmware. Não reutilize automaticamente as regras do Desk.
5. Em Original grava em cartão vazio compatível; em BIT conserva os objetos de exportação do fluxo USB. Aguardando a confirmação.
6. Abre uma recuperação de teste para verificar o conteúdo e feche o segredo ao terminar.

Resultado: criptograma com recuperação verificada. Se a gravação ou a leitura falhar, protege o original e segue as instruções no ecrã para voltar a tentar. Não apagues cabeçalhos nem forces a substituição de dados.

P06 | Decifrar no dispositivo | Cuvex | L18 | C01,C02

Preparação: privacidade física e componentes de desbloqueio suficientes; microfone e captura de ecrã desativados perto do segredo.

1. Começa a decifrar no modelo correto e entrega o criptograma por NFC em Original ou o fluxo USB do BIT.
2. Verifica o alias e a identificação do objeto antes de introduzir credenciais.
3. Fornece as palavras-passe necessárias e a biometria quando o formato a exigir. Não insiste automaticamente em falhas: há controlo de acesso e bloqueio.
4. Verifica o conteúdo apenas no ecrã prevista. Um QR de segredo tem a mesma sensibilidade que o texto.
5. Pede ou termina o processo de acordo com o dispositivo e guarda suporte e credenciais separadamente de acordo com o teu plano.

Resultado: conteúdo recuperado em privado e sessão terminada. Se o formato não for reconhecido, a autenticação falha ou o conteúdo inesperado aparece, não o «corre» com uma aplicação desconhecido. Descreve o suporte versão, formato e erro, sem adicionar o segredo.

P07 | Preparar a recuperação de um criptograma biométrico | BIT | L19,L47 | C01,C02

Preparação: criptograma de aprendizagem e documentação do seu formato. Não deduzas uma recuperação pelo simples fato de ter uma cópia.bin.

1. Na ficha de Desk identifica se existem componentes biométricos e que exportação de recuperação está disponível.
2. Conserva o conjunto de ficheiros que o fluxo associa e uma cópia independente, com identificadores discretos.
3. Teste o desbloqueio normal no BIT e documenta quais palavras-passe e condições requerem.
4. Estuda a via excepcional de recuperação local e seus formatos admitidos. Verifica se o material necessário existe antes de precisar.
5. Teste com dados sem fundo o cenário de dispositivo errado ou pegada não disponível.

Resultado: um plano testado, com seus limites, para esse formato concreto. Não se afirma que qualquer biometria possa ser omitida nem que uma pegada substitua as cópias. Se um segredo é recuperado num PC, avaliar sua exposição e a necessidade de migrar controlo depois.

P08 | Criar e verificar uma cópia de um criptograma | Cuvex e Desk | L20 | C01,C02

Preparação: uma cópia original identificada e um destino compatível sem dados a preservar.

1. Para Original, use o clonamento do dispositivo ou a função compatível do Desk e apresenta origem e destino na ordem indicada.
2. Mantém as cartas estáveis e respeite o rejeição de suporte que já contém criptogramas.
3. Para BIT ou ficheiro, exporta o conjunto de componentes do fluxo e conserva nomes ou associação necessários.
4. Separa a cópia original e testa a leitura e a recuperação a partir da nova cópia.
5. Regista privadamente data, formato e resultado; guarda as cópias com riscos físicos independentes.

Resultado: uma segunda cópia comprovada. Não implica uma carteira diferente, revogação de palavras-passe ou proteção contra uma semente que já foi filtrada. Se o destino falhar, conserve o original sem tentar «repará-lo» para que ambos coincidem.

P09 | Criar o armazenamento do Desk, desbloqueá-lo e alterar a palavra-passe | Desk | L21,L40 | C02

Preparação: instalador verificado, arquitetura adequada e um plano de cópia de segurança do armazém.

1. Cria o armazém com uma palavra-passe única de 12 a 1.024 caracteres e confirmação coincidente.
2. Bloqueia e volta a abrir para confirmares que continuas a ter acesso. A palavra-passe só é inserida no Desk.
3. Em Segurança e acesso e bloqueio revisa inatividade e passo a segundo plano. Não activar excluído opcional durante uma demonstração.
4. Para alterar a palavra-passe, adicionas a atual e confirma a nova pelo seu fluxo.
5. Se usaste a biometria do PC, configure-a novamente de acordo com a indicação. Cria uma cópia atual e conserve a relação com cópias anteriores.

Resultado: acesso comprovado. As cópias prévias conservam sua palavra-passe e criptografia originais. Biometria de PC e biometria de BIT são mecanismos diferentes. Se o acesso for falso, dete tentativas repetidas e revise recuperação sem pedir ao tutor que guarda credenciais.

P10 | Associar e verificar um criptograma no Desk | Desk | L22 | C02

Preparação: criptograma de prova de origem conhecida e transporte disponível.

1. Abre a área de criptogramas ou cartões e seleciona a associação por NFC, USB ou cópia compatível.
2. Seleciona o design e a origem. Para NFC, usa o Cuvex Mirror ligado por Bluetooth ao computador. Para o Cuvex BIT, usa o volume do dispositivo ligado por USB-C. O Cuvex Desktop não suporta leitores NFC USB externos.
3. Revisa a ficha: alias, origem, tamanho, formato e condições interpretadas. É metadato, não contém decifrado.
4. Verifica se há contas mantidas pendentes de associação e relaciona apenas a conta verificada.
5. Exporta uma cópia se falta cobertura e teste recuperação por separado.

Resultado: o objeto ficou organizado no armazenamento local. «Vinculado» não demonstra autenticação da semente ou saldo. Um objeto não reconhecido exige verificar formato e versão, sem alterar extensão ou apagar dados até que a aplicação o aceite.

P11 | Ativar uma conta WOW watch-only | Desk e Cuvex | L13,L22 | C01,C02

Preparação: informação pública obtida do fluxo do dispositivo e controlo privado da sua origem.

1. Abre ativar WOW ou adicionar uma conta do criptograma correto.
2. Importa o descritor ou material público admitido por ficheiro, webcam ou Mirror segundo a função.
3. Revisa rede, script, origem, pegada, rota e checksum quando apropriado. Não introduzas sementes ou xprv.
4. Nome a conta e escolha a fonte de consulta com o seu consentimento.
5. Verifica uma direção de controlo e o alcance da descoberta antes de interpretar o saldo.

Resultado: Carteira de observação associado. Se vires saldo zero, verifica a rede, a passphrase original, a derivação, a conta, o prestador e a pesquisa de endereços antes de concluíres que as moedas desapareceram. Uma interface admite redes gerais que não necessariamente admite o perfil multiassinatura: respeita cada contexto.

P12 | Configurar o nó e a sincronização | Desk | L25,L33 | C02

Preparação: Decisão de privacidade e, se usares Core, acesso a um nó protegido e sincronizado.

1. Em Segurança e Privacidade e nós, escolha a conta WOW e revise o seu fornecedor.
2. Escolhe expressamente um fornecedor público compatível ou Core. Para Core introduza endpoint, carteira e credenciais apenas na aplicação.
3. Autoriza a consulta compreendendo quais dados cada serviço recebe. O TLS não esconde a consulta ao fornecedor.
4. Sincroniza e revisa data, ponta, progresso e estado completo. Para resgatar, confira a antiguidade coberta e a continuidade do trabalho.
5. A 429 respeita a pausa. Antes de falha, não suponha que outro nó foi ativado: a configuração não se rompe silenciosamente.

Resultado: fonte e estado conhecidos. Não abras RPC para a Internet, partilhe palavra-passe ou reduza a descoberta para endereços com saldo. Um histórico vazio pode ser um resultado parcial.

P13 | Gerar e recuperar um pedido de receção | Desk e Cuvex | L26 | C01,C02

Preparação: conta, rede e política comprovadas.

1. Abre receber e gera ou recupera a solicitação adequada.
2. Adiciona observador, motivo e valor esperado apenas se precisares desses metadados locais.
3. Verifica o endereço pelo percurso compatível do dispositivo antes de uma cobrança relevante. Se falta aceitação física, pare a prática em simulação.
4. Partilhe exclusivamente os dados necessários através do canal autenticado do receptor.
5. Verifica ingresso, montante e confirmações em tua fonte de rede.

Resultado: cobro conciliado, não apenas solicitação emitida. Em multiassinatura, os endereços mostrados são conservados para pagamentos atrasados e não são reassignados. Se o limite de novos endereços sem histórico for alcançado, recupera solicitações anteriores; não forças índices manualmente.

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

Preparação: conta de laboratório com UTXOs e uma palavra-passe para a exportação protegida.

1. Etique uma entrada com o seu contexto sem dados pessoais desnecessários.
2. Congela ou descongele conscientemente e revise o saldo gasto. A restrição é local.
3. Exporta etiquetas através da função protegida. Distingue a BIP329, que define o formato, da cifragem do ficheiro.
4. Importa numa cópia compatível; revisa coincidência de referências, etiquetas e congelamentos.
5. Mantém uma cópia de segurança de metadados atualizado junto com sua palavra-passe, de acordo com seu plano.

Resultado: contexto conservado e seleção entendida. Uma importação não deve ser usada para desbloquear automaticamente moedas congeladas sem revisão. Não envies o ficheiro de etiquetas para o tutor: ele pode revelar contrapartes e relacionamentos, mesmo que não inclua chaves de despesa.

P15 | Preparar um pagamento e enviar a totalidade do saldo | Desk | L28 | C02

Preparação: solicitação verificada e conta com entradas gastáveis suficientes.

1. Abre o pagamento a partir de WOW, UTXOs ou chat e confira conta e rede.
2. Selecione entradas, destinatários e montantes, e revise os contextos relacionados.
3. Escolhe a taxa e verifica a comissão absoluta, o troco e os avisos. Se houver poeira, revise alternativas sem aceitar uma comissão oculta.
4. Para enviar total, confira o neto após comissão. Em chat confirma de forma explícita um pagamento parcial se não cobre a solicitação.
5. Prepara o rascunho e revise todos os dados antes de exportar para assinatura.

Resultado: intenção compreensível e PSBT dessa operação. Um formulário geral pode admitir mais entradas ou destinatários do que o hardware: aplica os limites efetivos do signatário e transporte. Se as saídas ou as condições mudarem, uma nova revisão será iniciada.

P16 | Assinar e devolver uma PSBT com o Original | Original y Mirror | L29 | C01,C02,C03

Preparação: rascunho correto, cartão de transporte compatível, criptograma autenticado e compatível e meios de desbloqueio mantidos em privado. Uma cópia histórica sem autenticidade verificada pode requerer recuperação verificada e criação de uma nova cópia antes de assinar; não é corrigida editando sua cabeçalho.

1. Exporta a solicitação pelo fluxo NFC compatível a partir do Desk/Mirror.
2. Leva-a a Original; ele fornece o criptograma quando solicitado e desbloqueia sem ditar credenciais.
3. Verifica a rede, o resumo, todas as saídas, a comissão, o troco e os avisos obrigatórios.
4. Em multiassinatura Final, decide se examinar parâmetros ampliados; completa as três confirmações finais apenas se tudo coincidir.
5. Espera escrita e relectura da resposta no cartão.
6. Lê a resposta com o Cuvex Mirror e valida-a na operação do Desk.

Resultado: assinatura recebida e vinculada ao rascunho, ainda diferente de publicação. Se a gravação falhar, conserva o estado e segue as instruções para voltar a tentar. Nunca uses o cartão de suporte como suporte de pagamento prescindível.

P17 | Assinar, receber e confirmar a receção com o BIT | BIT y Desk | L29 | C01,C02

Preparação: rascunho correto, criptograma autenticado e compatível e volume real do BIT selecionado. Se uma cópia histórica for rejeitada para assinatura, siga a recuperação e renovação indicada, sem forçar o formato.

1. Entrega o pedido por USB-C através do serviço do Desk e segue as indicações do dispositivo para apresentar o criptograma.
2. Desbloqueia em privado e revise resumo, todas as saídas, comissão e avisos.
3. Em multiassinatura Final, revisa opcionalmente detalhes ampliados e autoriza com as confirmações finais obrigatórias.
4. A Desk usa o BIT para importar e validar a resposta a esse trabalho.
5. Confirma que a resposta foi guardada e que a receção foi confirmada. Se a confirmação falhar depois da receção, volta a tentar a mesma operação, sem escolher uma nova com base no modelo.

Resultado: assinatura verificada e estado de troca coerente. Se desligares antes de receber ou depois de guardar, mantenha o perfil da solicitação. Não mudes para outro firmware de catálogo para fazer uma resposta pendente encaixar.

P18 | Finalizar, publicar e acompanhar uma operação | Desk | L30,L44 | C02

Preparação: assinaturas verificadas e um limite suficiente quando apropriado.

1. Revisa de novo intenção, entradas, saídas, comissão e rede.
2. Finaliza através da ação correspondente e verifica que não faltam assinaturas ou condições.
3. Autoriza a difusão e conserva o resultado local. Se a resposta de rede for perdida, consulte antes de repetir.
4. Acompanha a mempool e as confirmações no prestador escolhido, verificando a data de sincronização.
5. Se o RBF for apresentado, revise a nova operação e obtenha as assinaturas necessárias. Não supõe uma função CPFP integrada.

Resultado: estado da cadeia verificado através da respetiva fonte. Cancelar um rascunho não revoga assinaturas já exportadas e não reescreve pagamentos confirmados. Uma mensagem de chat ou uma captura não substitui o rastreio.

P19 | Comparar livremente dois códigos QR de uma política | Mirror | L43 | C03,C02

Preparação: campo visível em Desk e Cuvex; na prática utiliza apenas as amostras sintéticas do curso.

1. Abre Comparar políticas e leia primeiro qualquer pessoa dos dois lados.
2. Escolhe a data que desejas verificar; podes começar com o passo 15 e omitir outros analisados manualmente.
3. Lê o seu contraparte e revise os dois textos completos. Se o passo é ambíguo, use Indicar passo de Desk e entenda que o contexto é manual.
4. Interpreta Coincide ou Não coincide apenas para esse par literal. Espaços, majúsculas e codificação contam.
5. Começa um novo par em qualquer ordem. Sair ou passar para segundo plano para terminar de acordo com o comportamento de borracha analisado.

Resultado: comparação local num momento específico. Não acredita origem, sessão, aprovação global ou ativação. Uma diferença deve ser esclarecida com suas fontes, sem normalizar o texto para forçar um OK.

P20 | Ativar, recuperar e transferir o chat | Desk e Cuvex | L36,L39 | C02

Preparação: ambiente DEV ou Produção escolhido, um alias e Chave de Chat no dispositivo, nunca no curso.

1. Abrir para ativar ou recuperar o chat do contexto do criptograma.
2. Escolhe um novo alias ou transferência existente e o perfil móvel compatível indicado pela app.
3. Introduz ou leia a Chave de Chat exclusivamente no fluxo privado. Não uses semente, PIN ou chave WOW.
4. Verifica a ativação com o serviço; se estiver pendente, use a ação de completar ou verificar, sem dar-a por correta.
5. Verifica a continuidade com os contactos após a transferência e evita utilizar o mesmo nome alternativo em vários equipamentos ao mesmo tempo.

Resultado: identidade ativada ou recuperada no ambiente correto. Histórico e sessões anteriores não são automaticamente recuperados com a Chave de Chat ou com a cópia global de Desk. Manter os limites do material disponível.

P21 | Verificar a identidade de um contacto | Desk | L36,L48 | C02

Preparação: canal independente acordado previamente com a pessoa.

1. Adiciona o alias e consulte sua identidade pública através da app.
2. Compara a pegada pelo canal autenticado, não apenas dentro da conversa recentemente criada.
3. Se usares o reconhecimento, evite informações públicas ou segredos reutilizados em outros serviços.
4. Confirmando somente após resolver diferenças. Se a identidade mudar, suspende os pagamentos e a coordenação até a verificares.
5. Documenta o método de verificação sem armazenar respostas sensíveis no curso.

Resultado: confiança contextual no contacto, não uma garantia de todas as suas solicitações futuras. Uma voz pode ser imitada e um equipamento legítimo pode estar comprometido. Cada operação mantém sua revisão.

P22 | Pedir um endereço, solicitar e efetuar um pagamento por chat | Desk e Cuvex | L37 | C02,C01

Preparação: contacto verificado e conta WOW compatível.

1. Selecione solicitar endereço, responder com endereço ou solicitar pagamento conforme a intenção.
2. Verifica a solicitação original, rede, montante e nota antes de enviá-la.
3. Para pagar, abra a preparação da conta adequada, selecione UTXOs e tarifa e revise o montante líquido.
4. Autoriza em Cuvex pelo procedimento do modelo. O chat não assina automaticamente.
5. Siga publicação e confirmação por tua fonte; concilia pagamentos parciais explícitos com a solicitação original.

Resultado: coordenação conservando a revisão de custódia. Estado de mensagem e estado de transação não são equivalentes. Um link para o navegador pode enviar informações para um terceiro: avaliar seu uso antes de abrir.

P23 | Partilhar e associar um criptograma recebido | Desk | L38 | C02

Preparação: necessidade concreta de partilhar, contacto verificado e definição de meios de acesso que receberá.

1. Seleciona a opção de partilhar um criptograma no chat e verifica o objeto.
2. Não adiciones palavras-passe, sementes ou Chave de Chat como comentário.
3. O receptor verifica a origem e vincula o objeto compatível através da sua ação de receção.
4. Avalia qual a capacidade que obténs agora e o que obterias se conseguires credenciais de desbloqueio suficientes.
5. Manter um plano de revogação realista: apagar mensagens não remove cópias externas ou chaves conhecidas.

Resultado: transferência consciente de um objeto cifrado. Não é um pagamento nem incorpora por si só uma chave para uma multiassinatura. Se o anexo pedir que abras uma página desconhecida para o decifrar, interrompe o procedimento.

P24 | Cópia de segurança global e restauro do Desk | Desk | L15,L21 | C02

Preparação: armazenamento de aprendizagem e destino de cópia controlado.

1. Abre a função de cópia do armazém e define a palavra-passe indicada; conserva sua relação com esta cópia concreta.
2. Guarda fora do único equipamento de uso e verifica a origem e integridade pelo fluxo.
3. Restaura num ambiente de teste separado e verifica contas, configurações e dados cobertos.
4. Revisa exclusões: chat, suas sessões e histórico não devem ser assumidos incluídos; política multiassinatura e chaves privadas não são intercambiáveis.
5. Repete após mudanças importantes e guarda as instruções de recuperação.

Resultado: suporte cujo alcance e palavra-passe são conhecidos. As cópias antigas conservam palavras-passe anteriores. Se o acesso for alterado ou existir exposição, avaliar também essas cópias; não basta modificar o armazenamento atual.

P25 | Criar e aceitar uma carteira multiassinatura | Desk e Cuvex | L41,L42 | C01,C02

Preparação: participantes independentes, contactos verificados, rede e limites efetivos acordados.

1. O criador escolhe nome, M/N, rede, participantes e vigência operacional.
2. Fornece a chave pública alargada correta com a impressão digital e o caminho BIP48 através do procedimento compatível.
3. Cada participante revisa, aceita ou rejeita e fornece seu material público. Nunca partilhe sementes.
4. Constrói a política completa e prepara sua verificação em cada dispositivo.
5. Mantém cópias de política antes de financiar. Verifica a direção de controlo e a capacidade de recuperação.

Resultado: proposta completa e verificável. A aceitação de convite não substitui a revisão de hardware. Se o Original intervém, aplica o máximo de seis chaves e o tamanho NFC; o BIT não amplia as capacidades dos outros participantes.

P26 | Verificar a política e receber a confirmação | Desk e Cuvex | L43 | C01,C02,C03

Preparação: a mesma política completa para todos, perfil de firmware correto e dispositivo sem operações competitivas.

1. Começa a verificar políticas no contexto compatível. Original requer seleção explícita do perfil instalado; BIT negocia capacidades de acordo com seu contrato.
2. Entrega a solicitação por NFC/Mirror ou USB-C segundo modelo.
3. Verifica os campos de política no dispositivo. Usa o Mirror como comparador opcional de pares escolhidos sem ordem obrigatória.
4. Completa a confirmação do equipamento e devolva sua resposta pelo transporte correspondente.
5. Em Desk valida a resposta vinculada à solicitação. Não substituas este passo por um OK visual do comparador.

Resultado: revisão correlacionada com o alcance desta revisão. O catálogo não atesta remotamente firmware e o dispositivo não é apresentado como um armazenamento persistente de políticas. Antes de FIRMWARE_CAPABILITY_REQUIRED, consulte primeiro a versão do Desk e a combinação modelo/build.

P27 | Pedir assinaturas, recebê-las e transferir a coordenação | Desk e Cuvex | L44 | C01,C02

Preparação: política verificada, operação identificada e destinatários acordados.

1. Prepara as entradas, as saídas, a comissão e as notas e pede as assinaturas aos participantes compatíveis.
2. Cada participante verifica e assina no seu equipamento, seguindo o respetivo procedimento de transporte.
3. Recebe, valida e guarda cada assinatura; resolve acusações pendentes sem mudar o perfil conservado.
4. Se a coordenação for interrompida, o receptor aceita o fluxo e verifica o estado. Não muda por isso M/N nem propriedade de chaves.
5. Ao alcançar um limiar, revise e finaliza antes de publicar. Siga a transação pela rede.

Resultado: Coordenação com evidências diferenciadas. O relatório de progresso do coordenador não substitui a tua verificação local. Cancelar ou rejeitar uma app não necessariamente destrói assinaturas já mantidas por terceiros.

P28 | Exportar, restaurar e eliminar a carteira multiassinatura local | Desk | L45 | C02

Preparação: política conhecida e cópia cifrada com uma palavra-passe única.

1. Exporta recuperação através da ação de Desk. O fluxo atual usa um recipiente autenticado CVXMSBK1 para essa exportação.
2. Conserva cópia e palavra-passe com riscos independentes. Não deduzas criptografia por extensão de ficheiros históricos.
3. Para restaurar fornece cópia, palavra-passe e chave pública do participante com origem correta por webcam ou Mirror se for caso disso.
4. Verifica política, rede, direção e descoberta antes de operar.
5. Para remover localmente, leia alcance e confirmação e guardar cópia se quiseres manter recuperação. Restaurar depois é explícito.

Resultado: política recuperável ou eliminação local consciente. A eliminação não movimenta fundos, não apaga chaves de outros signatários nem cancela por si só as operações que outras pessoas conservam.

P29 | Recuperação excecional num PC | Desk | L47 | C02

Preparação: material de formato admitido, ambiente limpo preparado e cópia de segurança. Esta operação pode revelar um segredo para o PC; utiliza dados de aprendizagem no curso.

1. Inicia a recuperação local do contexto correto e leia as limitações do formato e os avisos.
2. Aceita conscientemente o risco e desligue a rede como o fluxo exige; a janela verifica o estado antes de permitir que continue.
3. Insere apenas as credenciais necessárias na janela privada. Não se ditam, pegam no curso nem partilham com apoio.
4. Ativa a visualização apenas num espaço sem câmeras ou assistentes ouvindo; respeita temporizador e feche.
5. Termina, revisa qual exposição poderia existir e planeja migração para novas chaves se for caso disso.

Resultado: recuperação excepcional, não garantia de apagamento forense ou equivalência com hardware isolado. Se falta autenticação, formato ou material de acesso, não tente ferramentas da Internet com tua cópia real.

P30 | Rever as preferências, a biometria e o bloqueio | Desk | L40 | C02

Preparação: palavra-passe conhecida e suporte provado antes de alterar a segurança.

1. No Access e bloqueio, revise a palavra-passe, a biometria disponível, a inatividade e o bloqueio ao passar para o fundo.
2. Compreende o atraso após falhas e o máximo configurado antes de trocar.
3. Mantém o apagamento opcional desativado até compreender condições, limite e recuperação. Não tente em produção.
4. Em Preferências ajusta idioma, tema, moeda, sincronização de 3 ou 5 minutos e sons.
5. Se registares links bitcoin:, certifique-se de que abrir uma solicitação mantém o desbloqueio, seleção e revisão; não paga por si só.

Resultado: configuração entendida. A biometria do sistema operacional depende do equipamento e não substitui palavra-passe ou suporte. As preferências visuais não alteram a política do Bitcoin.

P31 | Eliminar registos sem confundir o alcance da eliminação | Desk | L22,L45 | C02

Preparação: identifica se vais eliminar o criptograma local, a conta, a WOW, o chat ou a carteira multiassinatura, e decide que cópia vais conservar.

1. Lê o objeto selecionado e seu aviso. Confirmar alias exato ou condição explícita quando o app o solicita.
2. Exporta e teste uma cópia se precisares recuperar esse estado mais tarde.
3. Elimina apenas o objeto previsto e verifica as associações que conserva ou retira o fluxo.
4. Verifica se existem operações ou participantes externos. Não presumas que serão eliminadas mensagens, assinaturas ou ficheiros de outros equipamentos.
5. Documenta a mudança em teu inventário privado sem dados sensíveis no curso.

Resultado: estado local gerido conscientemente. Nenhuma dessas ações muda por si só scripts de UTXOs financiados, destrói uma semente conhecida por terceiros ou reverte transações confirmadas.

P32 | Diagnosticar problemas sem expor segredos | Desk e Mirror | L23,L30,L48 | C02,C03

Preparação: anota hora aproximada, sistema, arquitetura, versão e fase. Evita repetir uma operação sensível sem saber seu estado.

1. Identifica se a falha é busca, ligação, leitura, escrita, validação, assinatura, retorno, rede ou visualização.
2. Copia o código e texto do erro sem incluir QR ou dados privados. Usa o diagnóstico da app quando necessário.
3. Revê o ficheiro antes de o partilhar. Não anexes uma cópia do armazenamento local, um criptograma, uma frase-semente, a Chave de Chat, um descritor ou credenciais RPC.
4. Numa incidência de interface, registra tamanho de janela, zoom e controlos ocultos com uma cena sintética.
5. Envia pelo canal oficial um resultado esperado e passos reprodutíveis. O curso não envia mensagens de suporte automaticamente.

Resultado: relatório que permite pesquisar com mínimo de dados. Se não houver evidência de uma etapa, é registado «pendente», não «completada». A assistência de voz não requer acesso remoto ao teu equipamento de guarda.

Glossário de Bitcoin e autocustódia

Bitcoin

Rede e conjunto de regras para transferir valor e verificar o respetivo histórico sem um administrador único do registo.

BTC

Unidade monetária do Bitcoin. Um BTC equivale a cem milhões de satoshis.

Satoshi

Unidade da cadeia de base que equivale a uma de cem milhões de partes iguais de um BTC.

Blockchain

Histórico de blocos ligados entre si e verificados segundo determinadas regras. Por si só, o termo não descreve todas as propriedades de uma rede.

Bloco

Conjunto de dados que inclui transações e um cabeçalho que pode ser validado.

Nó completo

Software que verifica o cumprimento das regras pelos blocos e transações que aceita.

Mineração

Construção de blocos mediante prova de trabalho segundo as regras da rede.

Prova de trabalho

Mecanismo que exige trabalho computacional verificável para propor um bloco.

Consenso

Concordância dos participantes quanto às regras e ao histórico válido que aceitam.

Política da mempool

Regras locais de aceitação e retransmissão que não correspondem necessariamente a regras de consenso.

Mempool

Conjunto local das transações não confirmadas que um nó conserva.

Confirmação

Inclusão num bloco da cadeia aceite e profundidade que esse bloco alcança depois.

Reorganização

Alteração de um segmento da cadeia aceite que pode afetar as confirmações.

UTXO

Saída de uma transação ainda não gasta, que pode ser consumida se as respetivas condições forem satisfeitas.

Entrada

Referência a uma saída anterior e dados necessários para autorizar o respetivo gasto.

Saída

Valor e condição de gasto criados por uma transação.

Troco

Saída que devolve ao teu controlo parte do valor das entradas depois do pagamento e da comissão.

Comissão

Diferença entre o valor das entradas e o das saídas de uma transação.

vbyte

Unidade de tamanho virtual utilizada para expressar o custo relativo de uma transação.

sat por vbyte

Taxa de comissão expressa em satoshis por unidade de tamanho virtual.

Dust

Saída pequena segundo as políticas aplicáveis e o custo de a gastar. O limiar depende do contexto e do script.

RBF

Substituição de uma transação não confirmada ao abrigo de políticas compatíveis. Não garante o cancelamento.

CPFP

Utilização de uma transação filha para aumentar o incentivo à inclusão do conjunto formado com a transação mãe.

Hash

Impressão digital dos dados, útil para verificar a integridade. Não cifra os dados nem identifica por si só o seu autor.

Chave privada

Permite produzir autorizações criptográficas segundo o esquema aplicável.

Chave pública

Dado que permite verificar assinaturas e construir determinadas condições sem expor a chave privada.

Assinatura digital

Prova criptográfica da autorização de uma mensagem específica. Não oculta o seu conteúdo.

Cifragem

Proteção da confidencialidade por meio de uma chave e de um algoritmo.

Cifragem autenticada

Cifragem que permite verificar alterações de acordo com a sua conceção.

AES GCM

Família de cifragem autenticada utilizada em formatos do ecossistema. As suas propriedades dependem da implementação e do tratamento das chaves.

Mnemónica

Representação por palavras do material de geração e verificação segundo um formato determinado.

Semente

Material a partir do qual se derivam chaves. O termo também é usado informalmente para a sequência de palavras, pelo que importa clarificar o contexto.

Entropia

Imprevisibilidade do material de geração. Não se obtém escolhendo palavras fáceis de recordar.

Checksum

Soma de verificação que deteta determinados erros. Não autentica o autor.

BIP39

Especificação de mnemónicas e de derivação de uma semente com passphrase opcional.

Passphrase BIP39

Dado adicional da derivação. Uma passphrase diferente pode produzir outra carteira válida e vazia.

BIP32

Especificação da derivação hierárquica de chaves.

Caminho de derivação

Sequência de ramos utilizada para obter chaves a partir de uma raiz.

Derivação reforçada

Passo de derivação habitualmente indicado por uma plica ou por h, com propriedades diferentes das da derivação pública normal.

xpub

Chave pública alargada que inclui o contexto de derivação. É sensível do ponto de vista da privacidade.

xprv

Chave privada alargada. Não deve ser partilhada nem importada para um curso.

Impressão digital da chave-mestra

Identificador curto de uma raiz. É útil para estabelecer associações, mas é insuficiente como prova de identidade.

Descritor

Expressão que descreve como construir scripts a partir de chaves e derivações. Pode ser pública ou conter material privado.

Watch only

Carteira de observação sem capacidade privada suficiente para assinar por si só.

WOW

Designação das contas de observação e gestão de carteiras no ecossistema Cuvex.

Carteira quente

Ferramenta com capacidade de assinatura num ambiente ligado à rede.

Autocustódia

Modelo em que o utilizador conserva, individualmente ou em conjunto, a capacidade técnica de gastar de acordo com a sua política.

Custodiante

Entidade que controla a capacidade de gastar por conta do cliente e aplica as suas condições de acesso.

Criptograma Cuvex

Objeto cifrado que protege um segredo. Por si só, não é uma transação nem um saldo.

Palavra-passe do Desk

Protege o acesso ao armazenamento local. É distinta da frase-semente e da palavra-passe do criptograma.

Chave de Chat

Segredo para recuperar a identidade do chat. Pode ter a aparência de um dado público sem o ser.

PIN de ligação

Código temporário de uma sessão de ligação. Não é uma palavra-passe de custódia.

Air gap

Separação operacional entre ambientes. Os dados transportados continuam a exigir validação.

NFC

Tecnologia de comunicação de curto alcance utilizada com cartões e leitores compatíveis.

USB Mass Storage

Interface de troca de ficheiros do modelo BIT, com protocolo, validação e confirmações próprios.

PSBT

Formato que reúne informações e assinaturas para coordenar a construção e a autorização de transações.

PSBT v0

Versão do formato definida na BIP174 e utilizada pelo perfil multiassinatura Final analisado.

PSBT v2

Versão definida na BIP370. Uma transação ser de versão 2 não implica que a PSBT seja v2.

SIGHASH ALL

Modo que determina a que dados a assinatura se vincula no perfil analisado. O seu alcance técnico faz parte da validação da operação.

P2WPKH

Tipo de condição SegWit com uma chave, habitualmente associado a contas BIP84.

P2WSH

Condição SegWit que vincula um script. É utilizada pela multiassinatura Final analisada.

P2TR

Tipo de saída Taproot. Aceitá-la como destino não implica ser possível assinar um gasto a partir dela.

sortedmulti

Construção multiassinatura que gera scripts ordenando as chaves de forma determinística.

Limiar M de N

Número M de autorizações necessárias entre N participantes de acordo com a política em causa.

MuSig2

Protocolo de agregação Schnorr cujo esquema de base é N de N, diferente de um limiar arbitrário.

Taproot

Conjunto de mecanismos de gasto e vinculação do Bitcoin com caminhos por chave e por script.

Miniscript

Linguagem para descrever e analisar determinadas políticas de script. Não está implementada no perfil Final analisado.

Regtest

Rede local de laboratório sem valor económico, controlada por quem prepara o ambiente.

Signet

Rede de teste com características próprias. Não é intercambiável com a regtest por predefinição.

Mainnet

Rede Bitcoin utilizada com valor económico real.

Gap limit

Critério de descoberta baseado no número de endereços consecutivos sem histórico. O seu âmbito depende da carteira.

Coin control

Seleção consciente das UTXO que serão gastas.

Consolidação

Combinação de saídas para reduzir a fragmentação, com consequências para o custo e a privacidade.

Pseudonimato

Uso de identificadores que não correspondem diretamente a um nome civil. Não implica anonimato automático.

Anonimato

Propriedade, dependente do contexto, de não se ser distinguível perante observadores definidos. Uma aplicação não a garante com um rótulo.

Metadados

Informações sobre as comunicações ou a atividade, como horários, tamanhos e relações, distintas do conteúdo.

CoinJoin

Construção colaborativa que dificulta certas inferências sem garantir anonimato permanente.

Payjoin

Pagamento colaborativo com entradas do pagador e do destinatário ao abrigo de um protocolo compatível.

Tor

Rede e ferramentas de proteção da ligação. A sua utilização deve ser configurada e verificada em cada aplicação.

VPN

Canal que transfere parte da confiança na ligação para o seu operador. Não oculta a cadeia.

Lightning

Sistema de pagamentos por canais com requisitos e riscos diferentes dos de um envio on-chain.

Invoice

Pedido estruturado de pagamento cujo formato e modalidade é necessário identificar.

RPC

Interface de chamadas a um serviço como o Bitcoin Core. Deve ser autenticada e protegida.

TLS

Proteção do transporte contra determinadas ameaças. O servidor destinatário continua a ver os pedidos.

SRTP

Proteção do áudio em determinados segmentos VoIP. Não implica automaticamente sigilo perante o operador.

Idempotência

Propriedade que evita duplicar um efeito ao repetir um pedido identificado.

Webhook

Evento enviado entre servidores. É necessário verificar a sua autenticidade e detetar repetições.

RAG

Recuperação de excertos de conhecimento para fundamentar uma resposta com contexto e versão.

Teach back

Verificação da aprendizagem pedindo ao aluno que explique por palavras suas o que compreendeu.

Phishing

Engano que recorre à usurpação de identidade e a um contexto convincente para obter acesso ou induzir uma ação.

Engenharia social

Manipulação de decisões humanas que pode recorrer a dados verdadeiros e à urgência.

Notarização

Controlo de distribuição da Apple, distinto de uma auditoria ao produto ou de testes físicos de todos os seus procedimentos.

Atestação

Evidência de um estado obtida por determinado mecanismo. O catálogo de compatibilidade do Desk não é uma medição remota.

MiCA

Enquadramento europeu para determinados criptoativos e serviços. Não garante rentabilidade nem compensação integral.

Travel Rule

Obrigações de informação nas transferências abrangidas. A utilização de autocustódia não as afasta.

Checkpoint

Ponto de retoma da aprendizagem com dados mínimos e sem informações sobre a carteira.

Verifica o que aprendeste

Pratica sem fundos reais. A avaliação é de acesso livre e não exige conta.

No uso habitual do Cuvex, quem autoriza o gasto?

1. O dispositivo, após verificação pelo utilizador
2. O tutor de voz
3. O servidor do curso

> **Ver resposta: O dispositivo, após verificação pelo utilizador**
> A autorização segue o seu percurso no Cuvex.

A quantos satoshis correspondem 0,001 BTC?

1. 1.000
2. 100.000
3. 1.000.000

> **Ver resposta: 100.000**
> Um BTC equivale a 100.000.000 sat.

As entradas somam 120.000 sat e as saídas 119.000 sat. Qual é a comissão?

1. 1.000 sat
2. 119.000 sat
3. 1 sat/vB, sem mais dados

> **Ver resposta: 1.000 sat**
> A diferença entre os valores é a comissão absoluta.

Em que estado está uma transação assinada que ainda não foi difundida?

1. Confirmada
2. Irreversível por estar assinada
3. Autorizada, mas não necessariamente publicada

> **Ver resposta: Autorizada, mas não necessariamente publicada**
> Assinar e publicar são etapas distintas.

A quanto correspondem 200 vB a 6 sat/vB?

1. 206 sat
2. 1.200 sat
3. 6 % do valor enviado

> **Ver resposta: 1.200 sat**
> Multiplica-se o tamanho virtual pela taxa.

Que deves verificar antes de efetuar um levantamento numa plataforma de câmbio?

1. Apenas a comissão mais baixa
2. A compatibilidade do ativo, da rede, do endereço e do montante líquido
3. A frase-semente da contraparte

> **Ver resposta: A compatibilidade do ativo, da rede, do endereço e do montante líquido**
> Nem todas as redes com o símbolo BTC são Bitcoin on-chain.

O que faz, por si só, uma assinatura digital?

1. Oculta toda a mensagem
2. Autoriza uma mensagem que pode ser verificada segundo o seu esquema de assinatura
3. Apaga dados publicados

> **Ver resposta: Autoriza uma mensagem que pode ser verificada segundo o seu esquema de assinatura**
> A confidencialidade exige outro mecanismo.

Que efeito pode ter alterar uma passphrase BIP39?

1. Criar outra carteira válida e aparentemente vazia
2. Permitir sempre a reposição por email
3. Alterar o registo público de pagamentos anteriores

> **Ver resposta: Criar outra carteira válida e aparentemente vazia**
> A passphrase participa na derivação.

Como deves tratar a xpub de uma conta?

1. Como um dado sem consequências
2. Como a própria frase-semente privada
3. Como informação sensível para a privacidade

> **Ver resposta: Como informação sensível para a privacidade**
> A xpub permite observar mais atividade.

Porque pode uma só frase-semente ser insuficiente numa carteira multiassinatura?

1. Faltam a política e as autorizações necessárias para atingir o limiar
2. O Bitcoin não permite recuperar nada
3. É necessário saber a cor original da aplicação

> **Ver resposta: Faltam a política e as autorizações necessárias para atingir o limiar**
> Conservar a política e manter a capacidade de usar as chaves privadas são requisitos distintos.

O que fazes se o algoritmo Final analisado rejeitar o resultado dos dados?

1. Volto a lançar apenas a moeda até o resultado ser aceite
2. Volto a lançar a moeda e os quatro dados
3. Escolho uma palavra conhecida

> **Ver resposta: Volto a lançar a moeda e os quatro dados**
> Repetir apenas parte do conjunto pode enviesar a correspondência entre resultados e palavras.

O que significa usar duas palavras-passe para abrir a frase-semente de uma carteira de assinatura única?

1. São necessárias duas chaves na cadeia
2. Trata-se de uma multiassinatura Taproot
3. O limiar de acesso ao segredo é independente do limiar do Bitcoin

> **Ver resposta: O limiar de acesso ao segredo é independente do limiar do Bitcoin**
> A cifragem não altera o script.

O que se deve ter em conta ao avaliar uma cópia de segurança global do Desk?

1. Inclui necessariamente todo o chat
2. Tem um âmbito e exclusões. Não se deve presumir que inclui o chat
3. Atualiza todas as cópias antigas

> **Ver resposta: Tem um âmbito e exclusões. Não se deve presumir que inclui o chat**
> Recuperar a identidade e recuperar as mensagens são coisas diferentes.

O que permite um nó próprio bem configurado?

1. Eliminar todas as fugas de informação
2. Reduzir a dependência de consultas a terceiros e fazer verificações
3. Recuperar chaves perdidas

> **Ver resposta: Reduzir a dependência de consultas a terceiros e fazer verificações**
> Não garante anonimato nem recuperação de segredos.

O que acontece ao congelar uma UTXO no Desk?

1. Aplica-se uma restrição local da aplicação
2. Altera-se a condição de consenso
3. Revogam-se outras cópias da frase-semente

> **Ver resposta: Aplica-se uma restrição local da aplicação**
> O congelamento não impede o gasto de forma global.

Que fazes se perderes a ligação no momento da publicação?

1. Pago outra vez imediatamente
2. Apago a carteira
3. Verifico primeiro se o pagamento já foi difundido

> **Ver resposta: Verifico primeiro se o pagamento já foi difundido**
> Um tempo limite excedido não prova que a ação não teve efeito.

Que consequência pode ter reutilizar endereços ou juntar UTXO de contextos distintos?

1. Facilitar a identificação de relações observáveis
2. Apagar o histórico
3. Garantir anonimato

> **Ver resposta: Facilitar a identificação de relações observáveis**
> A privacidade depende do contexto e da utilização posterior.

Abrir o Tor Browser configura automaticamente o Desk?

1. Sim
2. Não
3. Só se o tema for escuro

> **Ver resposta: Não**
> É preciso verificar o percurso de rede de cada aplicação.

O que é a Chave de Chat com aspeto de xpub?

1. Um dado que se pode publicar
2. Um endereço para receber pagamentos
3. Um segredo associado à identidade

> **Ver resposta: Um segredo associado à identidade**
> A finalidade determina a sensibilidade.

O que significa uma mensagem de chat a dizer «pago»?

1. Substitui as confirmações
2. O pagamento precisa de verificação independente na rede
3. Altera a rede do pedido

> **Ver resposta: O pagamento precisa de verificação independente na rede**
> O estado da mensagem é diferente do estado do pagamento.

O que utiliza o perfil multiassinatura Final analisado?

1. MuSig2 e PSBT v2
2. P2WSH, sortedmulti, BIP48 e PSBT v0
3. Qualquer script de Bitcoin

> **Ver resposta: P2WSH, sortedmulti, BIP48 e PSBT v0**
> As funcionalidades suportadas não se alargam por vontade do utilizador nem pelo nome comercial.

Por onde podes começar a comparação no Mirror 12.12?

1. Apenas pelo passo 1
2. Por qualquer dado que escolheres, incluindo o 15
3. Apenas pelo último, depois de todos os outros

> **Ver resposta: Por qualquer dado que escolheres, incluindo o 15**
> A comparação é livre e cada par é comparado de forma independente.

O que atesta a indicação de correspondência no Mirror?

1. Aprovação global
2. Origem autêntica dos dois QR
3. Igualdade literal dos elementos do par

> **Ver resposta: Igualdade literal dos elementos do par**
> A restante revisão e a resposta continuam pendentes.

Se uma frase-semente tiver sido exposta, o que acontece ao alterar a palavra-passe do Desk?

1. Revoga-se o acesso do atacante
2. Não são revogadas as chaves derivadas dessa frase-semente
3. Apagam-se todas as cópias

> **Ver resposta: Não são revogadas as chaves derivadas dessa frase-semente**
> É necessário avaliar como transferir o controlo em segurança.

Que deve indicar o encerramento da formação prática?

1. O que foi leitura, simulação e teste físico, e o que falta
2. Apenas as horas vendidas
3. Uma promessa de custódia invulnerável

> **Ver resposta: O que foi leitura, simulação e teste físico, e o que falta**
> Cada tipo de evidência tem um alcance próprio.