CUVEX

CUVEX ACADEMY · 0.1

Apprenez. Comprenez. Prenez le contrôle.

Bitcoin et la garde en propre, expliqués pas à pas. Le cours, le manuel, le glossaire et les exercices sont gratuits et accessibles sans inscription. À vous de choisir par où commencer.

Gratuit · sans inscription

Toutes les sections

1. Préparer votre espace d’apprentissage
2. L’argent numérique et la question de la confiance
3. Histoire et limites de Bitcoin
4. Calculer sans erreur avec les satoshis
5. Votre modèle de menace
6. Nœuds, minage et consensus
7. Les UTXO et la monnaie rendue lors d’une transaction
8. Mempool, confirmations et réorganisations
9. Frais, taille virtuelle et remplacement
10. Réseaux, adresses et demandes de paiement
11. Hachage, signatures et chiffrement
12. Graine, phrase secrète et mot de passe
13. Dérivation, xpub et descripteurs
14. Choisir un portefeuille et un mode de garde
15. Des sauvegardes permettant une restauration
16. Découvrir Original et BIT
17. Créer une graine à partir d’une source physique d’entropie
18. Chiffrer et déchiffrer un secret avec Cuvex
19. Seuils de chiffrement et biométrie
20. Cloner, conserver et vérifier les copies
21. Installer et protéger Cuvex Desk
22. Associer des cryptogrammes et organiser WOW
23. Associer Mirror à Desk
24. NFC via Mirror, USB-C et lecture des codes QR
25. Prestataires publics et nœud personnel
26. Recevoir des bitcoins et vérifier l’adresse
27. Étiqueter, geler et sélectionner des UTXO
28. Préparer et vérifier un paiement
29. Signer avec Original et BIT
30. Finaliser, diffuser et résoudre les incidents
31. Ce qui est observable sur Bitcoin
32. Séparer les contextes et gérer la monnaie rendue
33. Confidentialité du réseau, Tor et VPN
34. CoinJoin, Payjoin et leurs limites actuelles
35. Leçons tirées d’incidents réels

36. Créer une identité de messagerie et vérifier ses contacts
37. Demander et payer des satoshis depuis la messagerie
38. Partager des cryptogrammes en connaissance de cause
39. Récupérer la messagerie et comprendre ses métadonnées
40. Réglages du quotidien et vérification des autorisations
41. Concevoir un portefeuille multisignature
42. Créer des invitations et fournir des clés
43. Vérifier les politiques avec Mirror dans l’ordre de votre choix
44. Coordonner les signatures et diffuser une transaction multisignature
45. Récupérer et modifier un portefeuille multisignature
46. Mettre à jour le micrologiciel sans improviser
47. Perte, panne et récupération d’urgence
48. Hameçonnage, assistance et fraudes vocales
49. Confidentialité, obligations légales et documents personnels
50. Succession, continuité et exercice annuel
51. Cours, épargne et analyse fondamentale
52. Choisir où acquérir des bitcoins
53. Comptes, ordres et coûts d’exécution
54. Bougies, indicateurs et biais de l’analyse technique
55. Marge, contrats à terme et automatisation
56. Lightning et les autres couches
57. Taproot, MuSig2 et l’avenir post-quantique
58. Interopérabilité et indépendance vis-à-vis du fabricant
59. Laboratoire technique avec regtest
60. Projet final et plan de continuité
61. Manuel de l’élève
62. Glossaire de Bitcoin et de la garde en propre
63. Vérifiez vos acquis

M01

Préparer votre espace d’apprentissage

Objectif

Préparer le cours, distinguer les trois appareils et convenir des informations à ne jamais communiquer au tuteur.

Comprendre

Vous apprendrez à recevoir, conserver, dépenser et récupérer des bitcoins en exerçant votre propre jugement. L’objectif final est de savoir expliquer une décision avant de l’autoriser. Vous pouvez lire le cours sans assistance. Le tuteur vocal vous propose des explications, des questions et un accompagnement. Il n’a besoin ni de connaître votre patrimoine ni de contrôler vos appareils.

Cuvex est l’appareil qui protège les secrets et sur l’écran duquel vous autorisez les opérations. Sur l’ordinateur, Desk organise les cryptogrammes, les portefeuilles en lecture seule, les paiements et leur coordination. Mirror sert de passerelle locale pour les opérations compatibles et permet de comparer des données. Il ne signe pas et ne fonctionne pas comme un portefeuille autonome. Le parcours disponible dépend de votre version et de votre modèle.

Réservez un écran au cours et un autre à Desk. Gardez le téléphone et Cuvex à portée de main. Si vous n’avez qu’un écran, passez de l’un à l’autre sans partager votre écran en visioconférence pendant la saisie de secrets. Un appel peut prendre fin avant que vous ayez terminé un exercice. Faire une pause n’est pas un échec. Conservez uniquement l’identifiant de la leçon, l’étape atteinte et la difficulté rencontrée.

Ni le formateur humain ni l’IA ne doivent recevoir vos phrases de récupération, phrases secrètes BIP39, mots de passe, Clé de chat, codes PIN, fichiers privés ou codes d’achat complets. Ils n’ont pas non plus besoin de votre xpub, de votre véritable descripteur ou de votre adresse. Même si ces données ne permettent pas de dépenser, elles révèlent votre activité. Décrivez les messages d’erreur et utilisez les données fictives du laboratoire.

Mise en pratique

1. Identifiez physiquement l’ordinateur, le téléphone et le modèle de Cuvex. Notez leurs versions dans votre carnet privé.

2. Séparez votre environnement d’apprentissage, sans fonds, de celui où vous détenez réellement des bitcoins. N’importez pas une phrase de récupération réelle pour vous entraîner.
3. Ouvrez cette leçon et repérez la commande de pause, l’aide et le glossaire. Si quelqu’un vous demande un secret, mettez fin à cet échange.

À vous de l’expliquer

Expliquez qui signe, qui interroge le réseau et qui transporte les données. Vous pouvez poursuivre quand vous savez distinguer ces fonctions sans aide.

Question fréquente

Faut-il parler au tuteur tous les jours ? Non. Vous pouvez étudier en autonomie, refaire une séance et demander de l’aide pour une procédure précise. L’accès au cours et le crédit du service vocal sont deux droits distincts.

Point de pause

L01 terminée. Appareils identifiés. Aucun secret consigné dans le cours.

Le tuteur vous demande votre phrase de récupération pour vérifier que vous l’avez bien notée. Que faites-vous ?

1. Je la dicte lentement.
2. Je mets fin à la demande et vérifie la phrase uniquement dans mon environnement sécurisé.
3. Je n’envoie que les premiers mots.

> **Afficher la réponse: Je mets fin à la demande et vérifie la phrase uniquement dans mon environnement sécurisé.**
> Aucun fragment d’un secret ne doit être communiqué au service de formation.

M01

L’argent numérique et la question de la confiance

Objectif

Comprendre le problème que Bitcoin tente de résoudre avant d’ouvrir un portefeuille.

Comprendre

Un solde bancaire est une écriture gérée par un établissement. Celui-ci authentifie son client, décide quels virements il traite et tient sa comptabilité. Un fichier numérique ordinaire se copie facilement. Envoyer une photo n’empêche pas d’en conserver une copie. Pour qu’une unité numérique serve de monnaie, il faut pouvoir éviter qu’elle soit dépensée deux fois.

Bitcoin combine des règles de validation, des signatures et un historique partagé des transactions. Au lieu de confier l’intégralité du registre à un seul organisme, il permet à des participants indépendants de vérifier si une transaction respecte les règles. La rareté tient au fait que ces règles continuent d’être vérifiées et acceptées. Elle ne découle ni de l’image d’une pièce ni du cours affiché par une plateforme d’échange.

La garde en propre modifie vos responsabilités. Vous pouvez conserver la capacité de dépenser sans l’autorisation d’un dépositaire, mais vous pouvez aussi la perdre en détruisant toutes vos sauvegardes ou en signant un paiement erroné. Cette liberté d’action exige toujours de la sécurité, de la coordination, une connexion pour diffuser les transactions et le respect des obligations applicables.

Distinguez Bitcoin, le réseau et le protocole, de BTC, son unité monétaire. D’autres réseaux utilisent le mot blockchain tout en présentant des propriétés différentes. Une promesse d’entreprise libellée en « bitcoin » n’équivaut pas non plus à une sortie Bitcoin contrôlée par vos propres clés.

Mise en pratique

1. Comparez trois situations : un solde en banque, un solde sur une plateforme d’échange et un UTXO contrôlé par vos clés.
2. Pour chacune, indiquez qui peut vous empêcher de déplacer le solde et qui peut vous aider si vous oubliez comment y accéder.
3. Décrivez ce qui se passerait si vous copiiez une photo et si vous tentiez de dépenser deux fois la même sortie.

À vous de l’expliquer

Expliquez avec vos propres mots pourquoi un solde et la capacité de signer sont deux notions distinctes. Vous n’avez pas besoin de mémoriser les termes techniques.

Question fréquente

La garde en propre fait-elle disparaître tous les intermédiaires ? Vous pouvez choisir des services pour acheter, effectuer des consultations ou communiquer. L’important est de savoir quel pouvoir ils conservent et quelles données ils reçoivent.

Point de pause

Conservez votre comparaison des responsabilités sans nommer de comptes réels.

Quel problème monétaire la signature numérique ne résout-elle pas à elle seule ?

1. Empêcher une tentative de double dépense de la même sortie.
2. Prouver une autorisation à l’aide d’une clé.
3. Détecter la modification du message signé.

> **Afficher la réponse: Empêcher une tentative de double dépense de la même sortie.** Les signatures autorisent la dépense. Les règles et le consensus ordonnent les dépenses incompatibles.

M01

Histoire et limites de Bitcoin

Objectif

Situer les origines de Bitcoin et distinguer les faits historiques des récits commerciaux.

Comprendre

Le document de Satoshi Nakamoto a été diffusé en 2008, et le réseau a démarré en 2009. Il proposait une monnaie électronique de pair à pair, fondée sur des travaux antérieurs en cryptographie, en preuve de travail et en monnaie numérique. Il n’est pas nécessaire de connaître l’identité civile de Satoshi pour vérifier le logiciel ou une transaction.

Bitcoin n’a pas évolué par le remplacement unilatéral des règles par une entreprise. Les développeurs proposent et examinent des changements, les opérateurs choisissent leurs logiciels, les mineurs construisent les blocs et les utilisateurs comme les services décident de ce qu’ils acceptent. Cette répartition peut occasionner des désaccords. Une bifurcation du réseau et une mise à jour d’application sont deux événements différents.

Un nœud peut rejeter un bloc qui enfreint ses règles même si sa production a demandé un travail considérable. Le consensus ne se réduit pas à un vote par nombre d’ordinateurs. Exécuter des milliers de copies d’un nœud ne donne pas automatiquement davantage de pouvoir de décision. De même, une majorité de mineurs n’obtient pas pour autant la clé privée d’un utilisateur.

Bitcoin comporte des limites et des compromis délibérés : capacité des blocs, coût de vérification, délais de confirmation variables et registre public. Par défaut, il n’offre ni annulation administrative des paiements ni confidentialité intégrale. Les couches et applications répondent à des usages particuliers en introduisant de nouvelles dépendances.

Mise en pratique

1. Placez sur une frise le document initial, le démarrage du réseau, l’adoption de SegWit et l’activation de Taproot. Avant publication, vérifiez les dates auprès de sources fiables.
2. Classez « une entreprise garantit le cours », « un nœud valide » et « un mineur propose un bloc » parmi les promesses commerciales ou les fonctions techniques.
3. Expliquez un avantage et un inconvénient de l’absence d’administrateur pouvant annuler les paiements.

À vous de l’expliquer

Distinguez règle de consensus, politique locale et décision commerciale. L’application utilisée ne représente qu’une partie du réseau.

Question fréquente

La dernière version d’un logiciel change-t-elle toujours les règles monétaires ? Non. Une version peut aussi corriger des anomalies, améliorer les performances ou modifier des politiques locales. Lisez les notes de version et de compatibilité.

Point de pause

Notez une propriété vérifiable et une affirmation qui exigerait d’autres preuves.

Un bloc contient une dépense sans autorisation valide. Une majorité de mineurs peut-elle la rendre valide ?

1. Oui, si elle dépasse 51 %.
2. Seulement si la plateforme d’échange l’annonce.
3. Pas pour un nœud qui applique les règles conduisant à la rejeter.

> **Afficher la réponse: Pas pour un nœud qui applique les règles conduisant à la rejeter.**
> Le travail cumulé est comparé entre les historiques valides selon les règles du nœud.

Calculer sans erreur avec les satoshis

Objectif

Convertir des BTC en satoshis et inversement, et vérifier les montants indépendamment d’une cotation.

Comprendre

Un BTC vaut 100 000 000 satoshis. « sat » désigne une unité de bitcoin, pas une autre monnaie. Sur la chaîne de base, les montants s’expriment en nombres entiers de satoshis. 0,001 BTC vaut 100 000 sat et 0,00001000 BTC vaut 1 000 sat. Le séparateur décimal affiché dépend de la langue de l’interface. N’ajoutez pas de zéros au jugé.

Une cotation convertit momentanément les BTC dans une devise telle que l’EUR ou l’USD. Elle ne change pas le nombre de satoshis que vous contrôlez. Si vous détenez 100 000 sat et que le cours varie, vous détenez toujours autant de satoshis. Dans Desk, le cours de référence porte une source et une date. Une donnée ancienne peut conduire à une mauvaise décision économique même si le solde en BTC est juste.

Pour un paiement, distinguez le montant versé au destinataire, les frais de réseau et le total dépensé. Si vous envoyez 50 000 sat avec 600 sat de frais, 50 600 sat quittent votre portefeuille, compte tenu des éventuelles sorties qui vous reviennent. La commande « Envoyer la totalité » verse normalement au destinataire un montant net inférieur au solde disponible puisqu’il faut couvrir les frais.

Les exemples du cours sont des exercices de calcul. Ils ne donnent ni cours de marché ni barèmes recommandés. Avant de signer, vérifiez l’unité, le réseau, le destinataire et le coût total sur l’écran prévu. L’interface vocale peut prononcer « cinquante mille satoshis » tout en affichant « 50 000 sat ». Elle ne doit jamais choisir un montant sur la foi d’une transcription incertaine.

Mise en pratique

1. Convertissez 250 000 sat en BTC : 0,0025 BTC. Convertissez 0,00025000 BTC en satoshis : 25 000 sat.
2. Calculez la dépense totale pour un envoi de 75 000 sat assorti de 900 sat de frais : 75 900 sat.
3. Dans le simulateur, partez de 120 000 sat, envoyez 70 000 sat et fixez les frais à 1 000 sat. Vérifiez que la monnaie rendue est de 49 000 sat.

À vous de l’expliquer

Lisez un montant en BTC puis en sat et indiquez quel chiffre inclut les frais. En cas de doute, suspendez l’opération.

Question fréquente

Dois-je acheter un bitcoin entier ? Non. Vous pouvez en acheter une fraction, sous réserve des minimums et frais du prestataire.

Point de pause

Ne conservez que les résultats de l’exercice.

Vous disposez de 80 000 sat et souhaitez envoyer la totalité avec 1 200 sat de frais. Combien le destinataire reçoit-il ?

1. 80 000 sat.
2. 78 800 sat.
3. 81 200 sat.

> **Afficher la réponse: 78 800 sat.**
> En l’absence d’autres sorties dans cet exemple, le destinataire reçoit le solde disponible moins les frais.

M01

Votre modèle de menace

Objectif

Choisir des mesures proportionnées contre la perte, le vol, la tromperie et l’exposition des données.

Comprendre

La sécurité consiste à conserver la capacité d’agir selon ses intentions. La confidentialité consiste à maîtriser qui connaît ses données et ses relations. La disponibilité consiste à pouvoir accéder aux éléments nécessaires au moment voulu. Une boîte inaccessible à tous peut aussi vous être inaccessible. À l’inverse, une copie très commode peut trop en révéler.

Identifiez les biens à protéger, les adversaires et les accidents. Les biens comprennent clés, sauvegardes, historique, emplacement des copies et identité des contacts. Les risques comprennent logiciels malveillants, hameçonnage, incendie, oubli, contrainte, panne, décès et erreurs personnelles. Ils ne se réduisent pas tous avec le même outil.

Dressez un tableau simple : probabilité approximative, impact et mesure concrète. Un long mot de passe résiste mieux aux tentatives de devinette. Il ne corrige pas un destinataire frauduleux que vous autorisez vous-même. Deux copies dans le même sac ne protègent pas contre la perte du sac. Si une même personne contrôle tous les appareils et sauvegardes d’un portefeuille multisignature, il peut subsister un point de défaillance commun.

Intégrez aussi le cours et le tuteur au modèle : achats, appels, horaires de connexion et progression peuvent produire des métadonnées. Le site du cours ne doit pas demander vos adresses ou soldes pour personnaliser une leçon. L’absence d’inscription classique dans Desk ou Mirror ne signifie pas que la boutique, un prestataire vocal ou un service tiers interrogé ignore votre activité.

Mise en pratique

1. Notez vos trois risques principaux sans indiquer de montants patrimoniaux ni d’emplacements exacts.
2. Pour chacun, choisissez des mesures de prévention, de détection et de récupération. Par exemple, pour la perte d’une carte : deux copies séparées, un inventaire et un essai de restauration.
3. Identifiez qui peut observer un achat, un appel, une consultation du solde et une transaction publique.

À vous de l’expliquer

Expliquez quel risque précis réduit votre prochaine mesure. Évitez une complexité que vous ne pourriez ni maintenir ni expliquer à vos héritiers.

Question fréquente

Davantage d’appareils signifie-t-il toujours davantage de sécurité ? Seulement s’ils réduisent les dépendances communes et si vous pouvez tester la récupération. Ajouter des appareils augmente aussi la maintenance et les possibilités de confusion.

Point de pause

Gardez le plan dans votre documentation privée. Inscrivez uniquement « modèle de menace vérifié » dans le cours.

Quelle mesure réduit le mieux le risque de perdre toutes les copies dans un incendie local ?

1. Changer la couleur de la carte.
2. Placer deux copies dans le même tiroir.
3. Conserver des copies vérifiées dans des lieux exposés à des risques indépendants.

> **Afficher la réponse: Conserver des copies vérifiées dans des lieux exposés à des risques indépendants.**
> La redondance doit résister à l’incident qui menace l’original.

M02

Nœuds, minage et consensus

Objectif

Expliquer ce que valident les nœuds et ce qu’apporte le minage.

Comprendre

Un nœud complet reçoit les blocs et transactions, vérifie les règles et conserve une vue de la chaîne. Il n’a pas besoin de faire confiance au solde annoncé par un site. Le minage consiste à proposer des blocs par preuve de travail. Les mineurs sélectionnent des transactions valides et rivalisent pour trouver un bloc admissible.

La preuve de travail rend coûteuse la réécriture de l’historique. Parmi des chaînes valides concurrentes, c’est le travail cumulé qui compte. On ne peut se borner à compter les blocs sans tenir compte de la difficulté. L’intervalle entre blocs varie : dix minutes est une moyenne visée, pas un rendez-vous pour le prochain paiement.

La rémunération du mineur associe une subvention de bloc et des frais. La subvention diminue selon un calendrier lié à la hauteur de bloc. Les frais dépendent des transactions incluses. Payer davantage de frais ne rend pas valide une signature incorrecte. La sécurité économique et le coût d’une attaque ne rendent pas un paiement récent mathématiquement irréversible.

Un nœud personnel permet de vérifier soi-même les données et limite les consultations envoyées à des prestataires externes. Il faut encore protéger son système, son accès et sa connexion. Un nœud allumé mais non synchronisé, ou une application qui interroge un autre serveur, ne procure pas automatiquement ces avantages.

Mise en pratique

1. Attribuez les responsabilités suivantes : vérifier une signature, sélectionner les transactions d’un bloc, protéger votre graine et décider d’accepter un paiement.
2. Expliquez pourquoi « le mineur garde mes bitcoins » est inexact.
3. Sur un réseau de laboratoire, observez la hauteur et la synchronisation sans publier d’identifiants RPC.

À vous de l’expliquer

Décrivez la différence entre vérifier et proposer. Vous pouvez commencer par une analogie, puis terminer par la fonction technique exacte.

Question fréquente

Faut-il miner pour utiliser Bitcoin ? Non. Vous pouvez aussi commencer sans nœud personnel, mais vous devez comprendre la confiance accordée à votre prestataire.

Point de pause

Notez le type de prestataire du laboratoire sans révéler son URL privée.

Que permet un nœud complet correctement configuré ?

1. Vérifier le respect des règles par la chaîne qu’il accepte.
2. Récupérer n’importe quelle clé perdue.
3. Garantir une hausse du cours.

> **Afficher la réponse: Vérifier le respect des règles par la chaîne qu’il accepte.**
> La validation et la garde sont deux fonctions distinctes.

Les UTXO et la monnaie rendue lors d’une transaction

Objectif

Lire une transaction en distinguant les sorties dépensées et celles qu’elle crée.

Comprendre

Un UTXO est une sortie d’une transaction antérieure qui reste non dépensée. Un portefeuille calcule son solde en recensant les sorties qu’il contrôle. Il n’existe pas de compte universel débité comme sur un relevé bancaire. Une entrée désigne une sortie antérieure par l’identifiant de la transaction et la position de la sortie.

Un UTXO se dépense en entier. Pour payer moins que sa valeur, vous créez normalement une sortie pour le destinataire et une sortie de monnaie rendue que vous contrôlez. Avec une entrée de 120 000 sat, un paiement de 70 000 et des frais de 1 000, la monnaie rendue est de 49 000. La somme des entrées doit égaler la somme des sorties augmentée des frais.

Une adresse est distincte d’un UTXO. Elle peut recevoir plusieurs sorties et ne représente pas nécessairement une personne. Un identifiant de transaction peut être public. Le relier à votre identité ou expliquer à qui appartient chaque sortie ajoute des renseignements que la chaîne ne fournit pas à elle seule.

Cette structure compte pour la confidentialité. Regrouper des entrées peut suggérer un contrôle commun et la monnaie rendue peut relier des paiements futurs. Cette déduction n’est pas universelle, car il existe des transactions collaboratives. Le coin control consiste à choisir les sorties à dépenser en connaissant les conséquences de leur regroupement.

Mise en pratique

1. Dessinez trois entrées fictives de 40 000, 60 000 et 200 000 sat. Avec les deux premières uniquement, payez 70 000 sat avec 1 000 sat de frais.
2. Vérifiez que la monnaie rendue est de 29 000 sat et que la troisième entrée reste inutilisée.
3. Recommencez en utilisant uniquement l’entrée de 200 000 sat. La monnaie rendue serait de 129 000. Comparez les coûts possibles et les liens créés sans supposer des tailles identiques.

À vous de l’expliquer

Repérez entrée, destinataire, monnaie rendue et frais dans le schéma du cours. Si vous ne pouvez pas identifier une sortie, ne signez pas d’opération réelle.

Question fréquente

Tout ce qui revient dans mon portefeuille est-il de la monnaie rendue ? Non. Il peut s’agir d’un transfert vers une autre de vos adresses. Pour classer la sortie, il faut connaître la politique et la dérivation plutôt que deviner d’après son montant.

Point de pause

Conservez le schéma fictif, jamais une capture de vos avoirs.

Une entrée de 100 000 sat produit deux sorties de 30 000 et 69 200 sat. Quels sont les frais ?

1. 69 200 sat.
2. 800 sat.
3. 30 000 sat.

> **Afficher la réponse: 800 sat.**
> 100 000 moins 99 200 font 800 sat.

M02

Mempool, confirmations et réorganisations

Objectif

Distinguer une transaction préparée, diffusée et confirmée.

Comprendre

Le mempool est l’ensemble local des transactions non confirmées que conserve un nœud selon sa politique. Il n’existe pas de mempool mondial identique pour tous. Si un explorateur affiche un paiement, cela prouve que ce service en a connaissance, sans garantir son acceptation par tous les nœuds ni sa confirmation dans un délai précis.

Préparer une PSBT ne diffuse rien. Signer donne une autorisation. Finaliser construit la transaction susceptible d’être diffusée. Diffuser tente de la transmettre. Une confirmation signifie qu’elle est incluse dans un bloc de la chaîne acceptée par votre source de vérification. Une deuxième confirmation correspond à un bloc supplémentaire au-dessus du précédent, pas à une seconde signature du destinataire.

Lors d’une réorganisation, un tronçon de la chaîne change. Une opération peut perdre des confirmations ou redevenir en attente. Les parties demandent généralement davantage de confirmations pour les paiements dont l’enjeu est plus élevé. Aucun nombre n’élimine tout risque pour tous les montants et toutes les situations.

Si Desk présente un état enregistré, regardez la date de synchronisation. « Confirmé » dans un ancien instantané ne décrit pas forcément l’état actuel. Si un paiement n’apparaît pas, gardez son identifiant local et vérifiez sa diffusion et son historique avant de le préparer à nouveau. Une répétition précipitée peut créer un second paiement valide.

Mise en pratique

1. Mettez ces cartes dans l’ordre : brouillon, PSBT, signature, transaction finale, diffusion, inclusion dans un bloc.
2. Simulez une déconnexion après la diffusion. Décidez quoi vérifier avant de payer de nouveau.
3. Expliquez à un commerçant pourquoi un message « payé » ne remplace pas une vérification sur le réseau.

À vous de l’expliquer

Indiquez l’état d’une opération ainsi que la source et la date de cette information, sans la confondre avec une garantie.

Question fréquente

Fermer Desk annule-t-il une transaction diffusée ? Non. D’autres nœuds ou participants peuvent la conserver. Annuler un brouillon local a une portée différente.

Point de pause

Notez l’état de la simulation. Ne communiquez pas d’identifiants réels au tuteur.

L’ordinateur se déconnecte juste après que vous avez appuyé sur Diffuser. Que faites-vous en premier ?

1. Repréparer le même paiement depuis le début.
2. Supprimer le portefeuille.
3. Se reconnecter et vérifier la transaction et ses entrées.

> **Afficher la réponse: Se reconnecter et vérifier la transaction et ses entrées.**
> L’absence de réponse ne prouve pas que la diffusion a échoué.

M02

Frais, taille virtuelle et remplacement

Objectif

Estimer les coûts, interpréter les satoshis par octet virtuel et comprendre RBF et CPFP.

Comprendre

Les frais de réseau sont la différence entre la valeur des entrées et celle des sorties. Leur compétitivité s’exprime généralement en sat/vB, c’est-à-dire en satoshis par octet virtuel. Elle ne dépend pas directement du montant envoyé. De nombreuses entrées peuvent rendre coûteux un petit paiement, alors qu’un gros paiement comprenant peu d’entrées peut occuper moins d’espace.

À titre d’exemple, 200 vB à 5 sat/vB coûtent 1 000 sat. Avant la signature, les frais peuvent rester une estimation, car la taille finale dépend parfois des signatures et de la structure. Desk propose des vitesses indicatives et un taux manuel. Une mention « rapide » ne promet pas une confirmation à heure fixe.

RBF est une politique de remplacement de transactions non confirmées sous certaines conditions. Elle permet de proposer une dépense incompatible avec la précédente et assortie de frais supérieurs. Les politiques des nœuds ont évolué : une indication de non-remplacement ne garantit pas l’encaissement. Tout remplacement demande une nouvelle vérification et les signatures nécessaires.

CPFP consiste à dépenser une sortie de la transaction en attente afin de rendre intéressante l’inclusion de la transaction parente avec son enfant. Il faut contrôler une sortie dépensable, respecter les politiques et acquitter le coût. Cette technique Bitcoin ne suppose pas la présence d’un bouton CPFP dans la version de Cuvex de l’élève.

Une sortie dite « dust » est jugée trop petite selon les politiques applicables et le coût estimé de sa dépense. Il n’existe pas de seuil universel pour tous les scripts. N’enseignez pas un chiffre fixe comme une règle de consensus. Si une sortie de monnaie rendue n’est pas viable, revoyez le montant, les entrées ou le balayage du solde, ainsi que les frais effectifs.

Mise en pratique

1. Calculez les frais pour 180 vB à 8 sat/vB : 1 440 sat. Vérifiez s’ils dépassent votre budget de laboratoire.

2. Comparez une transaction à une entrée et une transaction à dix entrées. Expliquez pourquoi le montant envoyé ne suffit pas pour estimer les frais.
3. Simulez une transaction en attente et choisissez entre attendre, utiliser RBF ou étudier CPFP, sans présumer de leur prise en charge.

À vous de l’expliquer

Justifiez le taux de frais, les frais absolus et leur proportion par rapport au montant envoyé. Refusez des frais que vous ne pouvez pas expliquer.

Question fréquente

RBF annule-t-il avec certitude le paiement précédent ? Non. Les versions restent en concurrence jusqu’à confirmation et leur propagation compte. Ne remettez pas de marchandises sur une promesse d’annulation.

Point de pause

Gardez la décision de l’exercice et son motif.

À combien s’élèvent les frais pour 250 vB à 4 sat/vB ?

1. 1 000 sat.
2. 254 sat.
3. 4 % du montant envoyé.

> **Afficher la réponse: 1 000 sat.**
> La taille virtuelle multipliée par le taux donne une estimation des frais.

Réseaux, adresses et demandes de paiement

Objectif

Reconnaître le réseau, le format de l’adresse et les instructions de paiement avant de copier ou de scanner.

Comprendre

Mainnet transfère des bitcoins de valeur économique réelle. Les réseaux d’essai servent au développement et à l’apprentissage, sans être interchangeables. Regtest est un réseau local contrôlé par la personne qui installe le laboratoire. Signet et testnet ont leurs propres règles et écosystèmes. La prise en charge d’une signature unique sur signet ne signifie pas que le profil multisignature de Cuvex y fonctionne.

Les adresses encodent des conditions de réception. Sur mainnet, on trouve des formats commençant par 1, 3, bc1q ou bc1p. Le préfixe aide à reconnaître une famille, mais il n’authentifie pas le destinataire, ne garantit pas la compatibilité de l’appareil de signature et ne remplace pas la vérification du format complet.

Un code QR est un conteneur visuel. Il peut transporter une adresse, une demande de paiement, un descripteur ou du texte malveillant. Le scanner n’authentifie pas son auteur. Un lien bitcoin: peut aussi préciser un montant et un message. BIP321 est la référence moderne qui remplace BIP21. L’implémentation de Desk examinée conserve la terminologie et la compatibilité BIP21. L’évolution de la norme n’étend pas automatiquement les capacités de l’application.

Une demande de paiement Lightning se distingue d’une adresse sur la chaîne. Elle peut comporter une expiration et d’autres champs. Ne la collez pas dans un envoi sur la chaîne en l’absence d’un parcours compatible. Un jeton nommé BTC sur un autre réseau n’est pas non plus automatiquement du bitcoin natif.

Mise en pratique

1. Classez les exemples étiquetés du cours sans utiliser d’adresses réellement dépensables : adresse, URI bitcoin:, demande Lightning et descripteur.
2. Identifiez le réseau sélectionné dans le laboratoire. Le profil multisignature Cuvex examiné prend en charge mainnet/regtest.
3. Avant une opération réelle, comparez sur un canal authentifié le texte complet demandé par le destinataire.

À vous de l’expliquer

Refusez une demande dont vous ne connaissez pas le réseau ou le mode de paiement et expliquez ce qu’il faut vérifier.

Question fréquente

Puis-je envoyer des BTC par tout réseau proposé par une plateforme d’échange ? Non. Le réseau de retrait doit être compatible avec la réception prévue. Ne choisissez pas uniquement en fonction des frais les plus bas.

Point de pause

Notez seulement le type de réseau d’apprentissage.

Une adresse de réception bc1 ne permet pas à elle seule un retrait de BTC sur un autre réseau de jetons. Que manque-t-il ?

1. Changer le pseudonyme du destinataire.
2. Confirmer que le retrait passe par la chaîne Bitcoin et que toutes les données concordent.
3. Saisir la graine sur la plateforme d’échange.

> **Afficher la réponse: Confirmer que le retrait passe par la chaîne Bitcoin et que toutes les données concordent.**
> L’actif, le réseau et le mode de réception doivent être compatibles.

M03

Hachage, signatures et chiffrement

Objectif

Distinguer intégrité, autorisation et confidentialité.

Comprendre

Une fonction de hachage transforme des données en une empreinte de longueur fixe. La comparaison avec une empreinte connue aide à détecter des changements. Elle ne chiffre pas le fichier et n’identifie pas à elle seule son éditeur. Si vous téléchargez le fichier et son empreinte depuis la même page compromise, l’attaquant a pu remplacer les deux.

Une clé privée permet de créer des signatures, et la clé publique correspondante permet de les vérifier. Selon l’algorithme et ses règles, la signature lie une autorisation à un message précis. Elle n’en masque pas le contenu. Dans Bitcoin, une signature valide peut constituer l’une des conditions requises pour dépenser une sortie.

Le chiffrement vise à réserver la lecture aux personnes disposant de la capacité appropriée. Le chiffrement authentifié permet aussi de détecter des modifications. Dans l’écosystème Cuvex, les cryptogrammes protègent des secrets, les transactions signées autorisent des dépenses et les canaux chiffrés transportent des messages. Tous utilisent la cryptographie, mais ce sont des objets différents.

Un mot de passe saisi par une personne passe généralement par une fonction de dérivation avant de servir de clé cryptographique. « AES-256 » indique l’algorithme et la longueur de clé. Cela ne rend pas robuste un mot de passe prévisible. La génération, la mise en œuvre, le stockage, l’affichage et la récupération contribuent tous à la sécurité de l’ensemble.

Un code QR d’apparence complexe n’est pas pour autant sûr. Il faut savoir ce qu’il contient, qui l’a créé et ce que l’application en fera. Avant d’accepter une action, demandez au tuteur d’en expliquer la finalité sans solliciter la donnée privée.

Mise en pratique

1. Associez « détecter la modification d’un fichier », « masquer une graine » et « autoriser un paiement » au hachage, au chiffrement et à la signature.
2. Changez une lettre d’un texte fictif et observez la modification de son empreinte. N’utilisez pas de secret pour la démonstration.
3. Expliquez comment une transaction peut être publique et signée à la fois.

À vous de l’expliquer

Nommez la garantie recherchée et le mécanisme qui la procure, sans appeler « chiffré » tout ce qui est sécurisé.

Question fréquente

L’empreinte d’un micrologiciel certifie-t-elle l’absence de défauts ? Non. Elle identifie des octets si la référence est fiable. Un audit, une signature de fabricant et un essai physique répondent à des questions différentes.

Point de pause

Conservez les trois associations de l’exercice.

Quel mécanisme masque le contenu d’un secret ?

1. Publier son nom de fichier.
2. Le signer sans le chiffrer.
3. Le chiffrer correctement avec une clé protégée.

> **Afficher la réponse: Le chiffrer correctement avec une clé protégée.**
> Une signature ou une empreinte ne garantit pas à elle seule la confidentialité.

M03

Graine, phrase secrète et mot de passe

Objectif

Éviter de confondre les différents moyens d’accès du système.

Comprendre

Une phrase mnémonique BIP39 représente de l’entropie et une somme de contrôle au moyen de mots d’un dictionnaire. Les longueurs standard sont de 12, 15, 18, 21 ou 24 mots. Choisir une phrase facile à retenir, des paroles de chanson ou des mots qui semblent aléatoires ne reproduit pas une génération sûre. La somme de contrôle détecte certaines erreurs. Elle ne prouve ni qui a créé la graine ni que personne d’autre ne la connaît.

La phrase secrète BIP39 intervient dans la dérivation de la graine binaire. Une autre phrase secrète peut ouvrir un portefeuille entièrement différent et apparemment vide, sans message « phrase secrète incorrecte ». Elle n’a pas à être un mot du dictionnaire et ne constitue pas littéralement un vingt-cinquième mot.

Le mot de passe du cryptogramme Cuvex protège le secret stocké. Celui de Desk protège le stockage local de l’ordinateur. Le PIN d’association autorise une session de communication. La Clé de chat sert à récupérer une identité de messagerie. Tous diffèrent de la graine, et connaître l’un ne permet pas de reconstituer tous les autres.

Réunir graine et phrase secrète dans un cryptogramme peut simplifier la récupération. Mais quiconque le déchiffre accède alors aux deux. Les séparer accroît les exigences pour vous et vos héritiers. Documentez et testez votre choix. Ne le faites pas simplement parce que le tuteur juge une option « plus avancée ».

Mise en pratique

1. Préparez cinq cartes en papier portant les mentions graine, phrase secrète, mot de passe Cuvex, mot de passe Desk et Clé de chat, sans y inscrire aucune valeur secrète.
2. Indiquez ce que chaque élément permet de récupérer et ce que vous perdriez en l’oubliant.
3. Concevez un test sur un portefeuille vide. Saisissez les mots et la phrase secrète en privé. Communiquez au tuteur uniquement le résultat.

À vous de l’expliquer

Expliquez pourquoi le cours ne doit jamais demander un mot de passe pour « valider » votre apprentissage. Identifiez le secret nécessaire à votre procédure de récupération.

Question fréquente

Puis-je réinitialiser la phrase secrète par e-mail ? BIP39 ne prévoit pas ce mécanisme. Un dépositaire peut proposer une récupération de compte, mais il s’agit d’un autre modèle.

Point de pause

Consignez « moyens d’accès distingués », sans inscrire leurs valeurs.

Vous changez une lettre de votre phrase secrète BIP39 et voyez un solde nul. Quelle interprétation est correcte ?

1. Il peut s’agir d’un autre portefeuille valide, dérivé d’une autre phrase secrète.
2. Le réseau a effacé vos fonds.
3. Desk doit deviner la phrase secrète d’origine.

> **Afficher la réponse: Il peut s’agir d’un autre portefeuille valide, dérivé d’une autre phrase secrète.**
> Une phrase secrète différente peut produire un autre portefeuille sans signaler d’erreur.

Dérivation, xpub et descripteurs

Objectif

Comprendre comment décrire un portefeuille sans transmettre la capacité de dépenser.

Comprendre

Un portefeuille hiérarchique dérive de nombreuses clés d’une racine. Le chemin indique quelle branche est utilisée. Sur mainnet, BIP84 emploie généralement m/84'/0'/0' pour le premier compte SegWit à signature unique. BIP48 P2WSH utilise m/48'/0'/0'/2' pour le premier compte multisignature. L’apostrophe indique une dérivation renforcée. Modifier le compte, le réseau ou le type de script peut produire d’autres adresses à partir de la même phrase mnémonique.

Une xpub est une clé publique étendue qui permet de dériver certaines clés publiques descendantes. Ce n’est pas un mot de passe de dépense, mais elle peut permettre d’observer une famille d’adresses. L’empreinte maîtresse est un identifiant court qui aide à relier des enregistrements. Elle ne garantit pas l’identité à elle seule et n’exclut pas les collisions.

Un descripteur indique comment construire les scripts et les adresses à partir du type de script, des clés, de leurs origines et des dérivations. Un descripteur en lecture seule muni de clés publiques permet d’observer sans signer. Le mot « descripteur » ne garantit pas que tout son contenu soit public : certains formats peuvent contenir des clés privées. N’importez jamais de véritable descripteur dans le cours.

La récupération d’un portefeuille multisignature exige généralement sa politique complète, au-delà des mots d’un seul signataire. Conservez seuil, participants, xpub, chemins, réseau, type de script et données de découverte. La somme de contrôle du descripteur aide à détecter les erreurs de transcription, sans authentifier les participants.

Mise en pratique

1. Lisez un chemin fictif et expliquez son objet, sa monnaie, son compte et sa branche. Ne saisissez pas de clés réelles.
2. Distinguez l’adresse de réception, la xpub d’un participant et le descripteur complet.
3. Préparez une fiche de récupération privée avec les intitulés de champs laissés vides et un endroit séparé où conserver la documentation.

À vous de l’expliquer

Expliquez pourquoi un portefeuille vide après restauration ne prouve pas une perte. Vérifiez réseau, phrase secrète, script, compte, chemin et découverte.

Question fréquente

Peut-on publier une xpub sans conséquence ? Seule, elle ne permet normalement pas de dépenser, mais elle expose des données privées et peut aggraver d’autres risques dans certaines combinaisons cryptographiques particulières.

Point de pause

Ne conservez dans le cours qu’une fiche sans valeurs sensibles.

Quelles informations peuvent manquer si vous tentez de récupérer un portefeuille multisignature avec une seule graine ?

1. La couleur de l’appareil.
2. La politique et les clés publiques des autres participants.
3. Le mot de passe d’un réseau social.

> **Afficher la réponse: La politique et les clés publiques des autres participants.**
> La reconstruction des scripts exige la politique complète, en plus du nombre de clés privées requis par le seuil.

M03

Choisir un portefeuille et un mode de garde

Objectif

Comparer les outils selon leurs fonctions, la confiance qu’ils exigent et leur récupération.

Comprendre

Un portefeuille regroupe des outils pour décrire et observer les fonds et, le cas échéant, autoriser leur dépense. Un portefeuille à chaud peut signer dans un environnement connecté. Un appareil de signature isolé vise à séparer les secrets de l’ordinateur qui interroge le réseau. Un portefeuille en lecture seule possède les données publiques nécessaires pour observer et préparer les opérations, mais dépend d’un autre système pour signer.

Dans un régime de garde par un tiers, le solde d’un compte peut représenter une créance sur une entreprise. En garde en propre, vous conservez la capacité technique de dépenser, seul ou conjointement. La récupération par e-mail et la possibilité de bloquer un retrait caractérisent généralement le premier modèle. Évaluez chaque option en fonction de ses responsabilités propres.

Comparez les réseaux et scripts pris en charge, la vérification sur écran, les sauvegardes, les mises à jour, l’interopérabilité, la maintenance, les consultations de prestataires et la clarté des erreurs. Une liste de monnaies ou une belle finition ne suffit pas. Un appareil de signature ne vous protège pas contre l’approbation d’une adresse erronée que vous n’avez pas vérifiée.

Cuvex sépare les secrets protégés dans les cryptogrammes des fonctions d’organisation et de consultation de Desk. Ce modèle exige de conserver le cryptogramme et ses moyens de déverrouillage. La protection contre la perte de l’appareil ne garantit pas la récupération si toutes les copies ou tous les mots de passe disparaissent aussi. Apprenez le processus complet avant de déplacer vos avoirs.

Mise en pratique

1. Comparez Cuvex, un portefeuille à chaud et une plateforme d’échange dans un tableau indiquant qui signe, qui voit les consultations, qui peut rétablir l’accès et ce qui se passe si l’entreprise ferme.
2. Choisissez deux critères que vous devez vérifier à l’aide de preuves indépendantes de la publicité.

3. Vérifiez que l’environnement d’exercice n’emploie aucune clé de votre épargne réelle.

À vous de l’expliquer

Justifiez le choix d’un outil pour un cas précis sans le qualifier d’invulnérable.

Question fréquente

Un portefeuille matériel rend-il toutes mes transactions privées ? Non. Il protège principalement la capacité de signature et une partie de la vérification. La chaîne, les consultations et les contreparties continuent de produire des informations.

Point de pause

Conservez votre tableau sans noms de comptes.

Que peut faire un portefeuille en lecture seule correctement configuré avec des clés publiques ?

1. Observer l’activité et préparer des opérations sans pouvoir les signer seul.
2. Modifier une graine perdue.
3. Garantir l’anonymat.

> **Afficher la réponse: Observer l’activité et préparer des opérations sans pouvoir les signer seul.**
> Les capacités d’observation et d’autorisation peuvent être séparées.

Des sauvegardes permettant une restauration

Objectif

Concevoir une sauvegarde complète et démontrer sa récupération avant d’en dépendre.

Comprendre

Une sauvegarde utile restaure une capacité, au-delà d’un simple fichier. Pour un portefeuille à signature unique, il peut falloir la phrase mnémonique, la phrase secrète et les données de dérivation. En multisignature, il faut aussi la politique et des signataires en nombre suffisant. Desk peut nécessiter une copie chiffrée et son mot de passe. Dans la messagerie, récupérer l’identité n’équivaut pas à retrouver l’historique des messages.

La redondance protège contre la perte accidentelle, et la séparation contre la compromission simultanée de plusieurs éléments. Deux copies sur des supports et dans des lieux différents peuvent réduire les défaillances corrélées. Chaque copie supplémentaire exige aussi des contrôles d’accès, un inventaire et des vérifications. Les noms de fichiers et les étiquettes ne doivent ni révéler vos avoirs ni faciliter la localisation de tous les composants.

Un essai doit confirmer une adresse vérifiée au préalable et, dans un environnement d’apprentissage, la capacité de signer une opération contrôlée. Un fichier qui s’ouvre n’appartient pas forcément au bon portefeuille. Ne testez pas une copie en saisissant votre graine réelle dans un ordinateur quelconque.

Documentez ce que chaque copie couvre et exclut. Changer le mot de passe actuel ne modifie pas automatiquement les anciennes copies. Si un ancien mot de passe a été exposé, les sauvegardes qu’il protégeait restent concernées. Supprimer un fichier d’un stockage moderne ne garantit pas non plus l’effacement de toutes ses copies ou versions.

Mise en pratique

1. Remplissez un tableau privé avec l’objet, le contenu, le mot de passe associé, l’emplacement indépendant, la date d’essai et le responsable.
2. Restaurez une sauvegarde d’apprentissage dans un environnement séparé. Vérifiez le réseau, la première adresse et la dérivation.
3. Simulez la perte de l’ordinateur, puis celle de l’appareil. Identifiez la procédure qui change.

À vous de l’expliquer

Récupérez votre scénario de test sans aide improvisée et expliquez quelles informations manqueraient pour un autre scénario.

Question fréquente

La sauvegarde globale de Desk reprend-elle tout ? Ne le supposez pas. Dans l’implémentation examinée, l’historique et les sessions de messagerie sont exclus. La politique multisignature et les clés privées ont par ailleurs des fonctions distinctes.

Point de pause

Notez la date et le résultat du test, jamais le contenu de la sauvegarde dans le cours.

Vous changez le mot de passe de Desk. Que devient une sauvegarde antérieure ?

1. Elle se met à jour toute seule.
2. Elle perd automatiquement son chiffrement.
3. Elle conserve la protection et le mot de passe employés à sa création.

> **Afficher la réponse: Elle conserve la protection et le mot de passe employés à sa création.**
> Les sauvegardes antérieures sont des objets indépendants.

M04

Découvrir Original et BIT

Objectif

Choisir le parcours adapté au modèle et à sa version.

Comprendre

Original utilise des cartes NFC pour transporter cryptogrammes et opérations compatibles. Bluetooth intervient dans sa mise à jour et, sur le modèle documenté, USB-C sert à l’alimentation. BIT utilise USB-C pour échanger des fichiers et ajoute la biométrie pour les cryptogrammes qui l’exigent. Ne transposez pas à BIT les consignes NFC ou Bluetooth d’Original.

L’appareil propose chiffrement, déchiffrement, création de portefeuilles, signature et réglages. Original sait cloner des cartes, tandis que BIT travaille sur les fichiers du support USB. Les libellés, les langues et les accès peuvent varier selon la version. Le nouvel accès « Vérifier les politiques » de BIT ouvre le parcours compatible sans changer qui donne l’autorisation.

Les références éditoriales examinées sont Original 1.2.2 Final, BIT 1.2.3 Final, Desk beta.9.21 et Mirror beta.12.12. Il s’agit de références documentaires. La signature, la distribution et l’acceptation physique de chaque combinaison sont à vérifier avec l’équipe. N’installez pas à la place de votre micrologiciel un binaire non signé destiné à l’ingénierie.

Avant utilisation, vérifiez la provenance, les scellés, l’aspect et la version. La traçabilité et la signature d’une mise à jour répondent à certaines menaces sans remplacer toutes les vérifications. En cas de signes de manipulation ou de version inattendue, suspendez l’initialisation et contactez l’assistance par un canal que vous avez vérifié.

Mise en pratique

1. Identifiez votre modèle et notez la version affichée sans photographier de secret.
2. Repérez Chiffrer, Déchiffrer, Créer un portefeuille, PSBT et Réglages. Ne lancez pas un effacement ou une mise à jour pour explorer les menus.
3. Choisissez la branche Original ou BIT dans le cours et conservez-la pour la durée de l’exercice.

À vous de l’expliquer

Expliquez par où entre et ressort une opération sur votre modèle et quel support il faut protéger contre l’écrasement.

Question fréquente

BIT est-il automatiquement plus sûr pour tout le monde ? Les modèles impliquent des choix d’utilisation différents. La réponse dépend des menaces, de la récupération et du bon usage.

Point de pause

Conservez modèle et version dans votre carnet local. Le cours n’a besoin que du modèle choisi.

Vous avez un BIT et un guide demande d’écrire sur une carte NFC avec l’appareil lui-même. Que faites-vous ?

1. Je vérifie à quel modèle s’applique le guide et j’utilise le parcours USB compatible.
2. Je force la mise à jour d’Original.
3. J’envoie la graine au téléphone.

> **Afficher la réponse: Je vérifie à quel modèle s’applique le guide et j’utilise le parcours USB compatible.**
> Les instructions doivent correspondre au moyen de transport réellement utilisé par le modèle.

M04

Créer une graine à partir d’une source physique d’entropie

Objectif

Comprendre la génération et pratiquer le parcours sans utiliser des données du cours comme clés personnelles.

Comprendre

L’entropie est l’imprévisibilité. Des dés adaptés peuvent en fournir si leur ordre est fixé avant le lancer et si l’algorithme de conversion est correct. Un résultat rejeté doit être reproduit conformément aux consignes. Le remplacer par le maximum ou choisir un autre mot introduit un biais.

Le parcours Cuvex examiné combine une pièce et quatre dés. La conversion calcule le résultat de la pièce multiplié par 1 296, puis y ajoute le nombre en base six formé par les résultats des dés diminués chacun de un. Les indices de 0 à 2 047 sont admis. Si le résultat dépasse le dictionnaire, il faut relancer la pièce et les quatre dés. Garder la pièce et ne relancer que les dés biaise le résultat. Cela décrit le code source examiné : l’écran et le parcours complet sont à valider sur chaque micrologiciel distribué.

Cette méthode ne revient pas à choisir des mots préférés. N’utilisez pas une démonstration publique pour produire des données destinées à protéger de l’argent. Toute graine apparaissant dans un support pédagogique doit être considérée comme connue. L’algorithme complet de l’appareil doit produire le dernier mot et en effectuer la vérification. Ne complétez pas la phrase mnémonique à la main.

Préparez un espace sans caméra, assistant vocal actif à proximité, capture d’écran ni observateur. Le tuteur doit s’interrompre pendant la saisie et l’examen du secret. Il peut expliquer avant et poser des questions ensuite sans entendre ni les résultats des lancers ni les mots.

Après la génération, vérifiez la sauvegarde, chiffrez-la selon le modèle et testez la récupération d’un portefeuille vide. Une adresse de contrôle aide à vérifier la cohérence sans exposer la graine à l’ordinateur. Si le parcours accepte des valeurs contraires aux consignes ou affiche des mots inattendus, arrêtez-vous et notez uniquement la version, l’écran et l’erreur.

Mise en pratique

1. Pendant l’exercice, suivez les étapes de l’appareil avec des données sans fonds. Fixez l’ordre des dés et ne modifiez aucun résultat.
2. Recommencez les saisies rejetées selon l’écran, sans les corriger pour qu’elles soient acceptées.
3. Examinez le contenu en privé, créez une copie et confirmez que vous pouvez reconstituer le même portefeuille d’apprentissage.

À vous de l’expliquer

Expliquez pourquoi l’entropie physique, la justesse de la conversion et le secret du résultat sont trois exigences distinctes.

Question fréquente

Puis-je communiquer mes lancers à l’IA pour qu’elle vérifie l’algorithme ? Pas pour une graine que vous comptez utiliser. L’assistance travaille sur des exemples synthétiques distincts.

Point de pause

Terminez dans un état sûr de l’appareil. Ne laissez pas de graine visible pendant la pause.

Le micrologiciel rejette une saisie de dés. Quelle action respecte la procédure ?

1. Choisir un mot manuellement.
2. Recommencer comme l’indique l’appareil sans biaiser le résultat.
3. Réduire le nombre jusqu’à ce qu’il soit accepté.

> **Afficher la réponse: Recommencer comme l’indique l’appareil sans biaiser le résultat.** Les rejets font partie de la conversion de l’entropie. Il ne faut pas remplacer arbitrairement les résultats rejetés.

M04

Chiffrer et déchiffrer un secret avec Cuvex

Objectif

Créer un cryptogramme d’apprentissage et vérifier sa récupération.

Comprendre

Choisissez le bon type de contenu : BIP39, SLIP39, Monero ou texte si votre parcours le permet. Ce sont des formats différents. Chiffrer du texte SLIP39 ne transforme pas Cuvex en signataire de tous les réseaux susceptibles de l’utiliser. Le stockage des secrets et la mise en œuvre de protocoles de signature ont des portées distinctes.

Pour garder le contenu hors des appareils connectés, saisissez-le directement sur l’appareil. Une importation depuis un téléphone ou un PC a pu exposer le secret à la source, même s’il est ensuite chiffré. L’écran de vérification préalable sert à repérer les erreurs de mots, d’ordre, de casse ou de champs.

Le mot de passe du cryptogramme doit être long, unique et récupérable selon votre plan. Le clavier de création examiné accepte jusqu’à 40 caractères. Le validateur en exige au moins 12, dont une majuscule et une minuscule ASCII, un chiffre et un symbole reconnu. La règle de 12 à 1 024 caractères de Desk ne s’applique pas automatiquement au clavier de Cuvex. D’autres champs de récupération peuvent avoir d’autres limites : vérifiez le parcours et la version.

Sur Original, écrivez sur une carte vide et adaptée, maintenue en position jusqu’à confirmation. Sur BIT, gardez les fichiers produits par le parcours USB, y compris les composants biométriques nécessaires le cas échéant. Ne renommez ni ne combinez les fichiers au jugé. Testez ensuite la lecture et le déchiffrement sur l’appareil, sans communiquer le secret au tuteur.

Mise en pratique

1. Chiffrez un texte pédagogique créé pour l’exercice, sans identifiant secret ni valeur économique.
2. Identifiez le support et l’objet obtenu. Notez en privé l’alias et son rôle.
3. Relancez le déchiffrement, vérifiez le texte sur l’écran de confiance et fermez l’affichage à la fin.

À vous de l’expliquer

Distinguez l’exactitude du contenu, la réussite de l’écriture et celle de la récupération. « Fichier copié » ne prouve pas les trois.

Question fréquente

L’alias d’une carte est-il un mot de passe ? Non. Il sert à l’organisation. Évitez les soldes ou descriptions qui permettraient d’identifier vos avoirs.

Point de pause

Ne laissez pas de contenu déchiffré visible. Notez seulement le succès ou l’échec de l’essai.

Comment démontrer au mieux qu’un cryptogramme de test permet de récupérer son contenu ?

1. Lui donner un joli nom.
2. Constater que le fichier existe dans deux dossiers.
3. Le lire et le déchiffrer par le bon parcours, puis vérifier le contenu en privé.

> **Afficher la réponse: Le lire et le déchiffrer par le bon parcours, puis vérifier le contenu en privé.**
> L’existence d’une copie ne prouve ni son utilité ni sa correspondance avec les données attendues.

M04

Seuils de chiffrement et biométrie

Objectif

Distinguer la protection partagée d’un secret de la multisignature Bitcoin.

Comprendre

Un cryptogramme protégé par plusieurs mots de passe détermine qui peut déchiffrer le contenu. Un portefeuille Bitcoin multisignature détermine quelles clés doivent autoriser une dépense sur le réseau. Un secret protégé conjointement peut correspondre à un portefeuille à signature unique. Inversement, chaque signataire d’une politique multisignature peut avoir son propre cryptogramme individuel.

Si plusieurs personnes déverrouillent ensemble une graine qui permet ensuite de dépenser seule, le seuil sur la chaîne reste d’une clé. Une fois la graine révélée, quelqu’un peut la conserver. Ne présentez pas ce dispositif comme imposant plusieurs signatures pour chaque paiement.

La biométrie de BIT ajoute une condition d’accès pour les formats qui l’emploient. Un doigt n’est ni une graine ni un substitut universel au mot de passe. Prévoyez les blessures, l’évolution de l’empreinte, les pannes, la disponibilité de l’appareil et la succession. Conservez et testez la voie de récupération documentée pour ce cryptogramme avant d’en dépendre.

Un export de récupération peut révéler le secret sur un ordinateur pour résoudre une urgence. Cette possibilité ne rend pas le PC équivalent à l’appareil isolé. Conservez l’isolation en usage normal. Étudiez délibérément la récupération locale et prévoyez une migration ultérieure en cas d’exposition.

Mise en pratique

1. Dessinez deux politiques : « deux mots de passe pour ouvrir une graine » et « deux clés sur trois pour dépenser ».
2. Dans un essai sans fonds, identifiez les fichiers nécessaires à une copie biométrique et l’endroit où vérifier sa récupération.
3. Simulez l’indisponibilité d’une personne. Déterminez si le seuil retenu permet de poursuivre.

À vous de l’expliquer

Expliquez qui peut connaître le secret et qui peut autoriser une dépense après déchiffrement.

Question fréquente

Puis-je retirer un participant en changeant une étiquette ? Non. Distinguez une modification d’organisation, une nouvelle protection du secret et une nouvelle politique de dépense.

Point de pause

Conservez le schéma sans noms réels ni données biométriques.

Trois personnes utilisent deux mots de passe pour ouvrir un cryptogramme contenant une seule graine à signature unique. Combien de clés Bitcoin exige-t-il pour dépenser ?

1. Une, si telle est la politique du portefeuille.
2. Deux, parce que le fichier exigeait deux mots de passe.
3. Trois, parce qu’il y a trois personnes.

> **Afficher la réponse: Une, si telle est la politique du portefeuille.**
> Le seuil de chiffrement ne modifie pas le script qui contrôle les fonds.

M04

Cloner, conserver et vérifier les copies

Objectif

Créer de la redondance sans détruire l’unique copie valide.

Comprendre

Cloner un cryptogramme copie des données chiffrées. Cela ne crée ni un nouveau solde ni une autre graine et ne protège pas contre l’exposition d’un mot de passe. Des copies identiques répondent à la perte d’un support sans réparer la compromission du secret d’origine. Une restauration et une migration vers de nouvelles clés répondent donc à des situations différentes.

Sur Original, distinguez la carte du cryptogramme de celle qui transporte la PSBT. Une carte d’opérations peut être réutilisée conformément au parcours, mais une carte contenant votre sauvegarde ne doit pas devenir ce support de transport. Si l’opération refuse une carte qui contient un cryptogramme, ne contournez pas la protection et n’effacez pas l’en-tête à la main.

Sur BIT, une copie doit préserver tous les fichiers nécessaires et leur association. Un gestionnaire de fichiers peut afficher un transfert terminé avant que l’appareil ait validé le contenu ou fini son opération. Attendez les états indiqués et vérifiez la copie par une récupération contrôlée.

Gardez un inventaire privé avec des identifiants discrets, la version du format, la date et le résultat du dernier essai. Séparez au moins deux copies pour résister aux incidents de votre modèle de menace. N’envoyez pas les sauvegardes à l’assistance pour un diagnostic. Fournissez des métadonnées expurgées et les codes d’erreur.

Mise en pratique

1. Créez sur un autre support une copie de votre cryptogramme pédagogique par le bon parcours.
2. Déconnectez le support original et récupérez le texte de test à partir de la copie.
3. Documentez ce que vous feriez en cas de perte, de fichier endommagé ou de mot de passe exposé. Les procédures diffèrent.

À vous de l’expliquer

Identifiez la copie testée et expliquez pourquoi l’original n’a pas été écrasé.

Question fréquente

Puis-je effacer l’original dès que je vois un second fichier ? Vérifiez d’abord la récupération et la couverture. L’effacement doit suivre un plan et non le simple décompte des copies.

Point de pause

Rangez les supports avant de terminer la séance. Ne mélangez pas cartes de sauvegarde et cartes d’essais de paiement.

Quelqu’un connaît le mot de passe et obtient une copie du cryptogramme. À quoi sert la création de trois clones supplémentaires ?

1. Elle révoque la copie de l’attaquant.
2. Elle ajoute de la redondance sans révoquer cet accès.
3. Elle change automatiquement la graine Bitcoin.

> **Afficher la réponse: Elle ajoute de la redondance sans révoquer cet accès.**
> La duplication ne met pas fin à une compromission existante.

M05

Installer et protéger Cuvex Desk

Objectif

Ouvrir une installation de provenance vérifiée et protéger son stockage local.

Comprendre

Choisissez le paquet adapté au système et à l’architecture : macOS Intel ou Apple Silicon, Windows x64 ou ARM64, Linux x64 ou ARM64 selon les distributions disponibles. Un ZIP de code source, un paquet pour le Manager et un installateur client sont des livrables distincts. Le cours ne doit pas orienter l’élève vers un paquet privé de signature.

Vérifiez la provenance et les contrôles du système. Une signature d’ingénierie Windows n’établit pas à elle seule la confiance publique envers l’éditeur. Sur Mac, la signature de l’application, la notarisation et l’évaluation à l’ouverture sont des contrôles distincts. Ne désactivez pas les protections générales à la demande d’un prétendu agent d’assistance. En cas d’avertissement inattendu, conservez son texte et utilisez le canal officiel.

Desk crée un stockage local chiffré protégé par mot de passe. Dans l’implémentation examinée, les nouveaux mots de passe acceptent de 12 à 1 024 caractères. Lorsque la confirmation est demandée, les deux champs doivent être identiques. Ces limites ne suffisent pas à assurer la robustesse : choisissez une phrase unique et ne la réutilisez pas. La biométrie du PC, lorsqu’elle est disponible, facilite l’accès mais nécessite sa propre configuration.

Configurez le verrouillage pour inactivité et, si nécessaire, lors du passage en arrière-plan. Le manuel traite du délai après échec et de l’effacement facultatif. N’activez pas l’effacement automatique pendant une démonstration. L’application peut fonctionner sans compte utilisateur classique. Ses services de consultation, de messagerie ou de téléchargement ont néanmoins leurs propres exigences et communications.

Mise en pratique

1. Vérifiez la plateforme, la version visible et la provenance du paquet sans communiquer d’identifiants privés au tuteur.
2. Créez un stockage d’apprentissage et testez le verrouillage puis la réouverture. Saisissez le mot de passe en privé.
3. Prévoyez une sauvegarde chiffrée et conservez son mot de passe selon votre plan. N’enchaînez pas des blocages de test dans l’environnement réel.

À vous de l’expliquer

Distinguez mot de passe local, compte commercial et moyens d’accès aux services que vous ajoutez.

Question fréquente

Changer le mot de passe de Desk change-t-il aussi celui de mes cartes ? Non. Ces protections sont indépendantes. Les anciennes copies ne changent pas non plus d’elles-mêmes.

Point de pause

Verrouillez Desk et notez l’identifiant de la leçon sans information d’accès.

L’installateur ne correspond pas à votre architecture. Quelle est la première étape ?

1. Désactiver les protections pour en forcer l’exécution.
2. Obtenir le bon paquet officiel et vérifier ses prérequis.
3. Importer la graine sur un site pour continuer.

> **Afficher la réponse: Obtenir le bon paquet officiel et vérifier ses prérequis.**
> La compatibilité et la provenance se vérifient avant d’utiliser les données qui protègent vos avoirs.

Associer des cryptogrammes et organiser WOW

Objectif

Associer une copie chiffrée et la distinguer d’un compte en lecture seule.

Comprendre

Desk organise les cryptogrammes associés via NFC, USB ou un fichier de sauvegarde compatible. Un habillage visuel et un alias aident à les reconnaître sans prouver cryptographiquement leur identité. La fiche affiche la provenance et les propriétés interprétées par l’application, comme le format, la taille et les conditions d’accès.

L’association importe ou organise l’objet compatible. Elle ne le déchiffre pas sur le PC et ne vérifie pas son secret. WOW est un portefeuille en lecture seule associé au moyen de données publiques compatibles. Un même ensemble de secrets peut donner lieu à des comptes ou dérivations différents. L’association doit correspondre au portefeuille que vous voulez gérer.

Activez ou importez le compte avec le descripteur ou les informations publiques exportées par le parcours de l’appareil. Vérifiez réseau, type de script, empreinte, chemin et adresse de contrôle. Le nom du compte sert à l’organisation. Un identifiant dérivé d’un nom prévisible peut être deviné et ne constitue pas une anonymisation forte.

L’implémentation de Desk examinée conserve les comptes en attente d’association et propose d’exporter des copies, de cloner et de supprimer des enregistrements locaux. Supprimer une carte de l’interface ne détruit pas les copies externes et ne déplace aucun fonds. « Aucune sauvegarde » signifie que l’application ne reconnaît pas de copie selon ses critères. Une sauvegarde peut exister ailleurs.

Mise en pratique

1. Associez le cryptogramme pédagogique par le transport choisi et examinez sa fiche.
2. Importez un compte d’apprentissage compatible et vérifiez son réseau et son adresse de contrôle sans montrer de clé au tuteur.
3. Distinguez l’enregistrement du cryptogramme, le compte WOW et le support physique. Indiquez ce qui disparaîtrait lors d’une suppression locale.

À vous de l’expliquer

Expliquez de quelles données Desk a besoin pour observer et lesquelles doivent normalement rester hors de l’ordinateur.

Question fréquente

Associer un fichier .bin garantit-il qu’il contient ma graine ? Non. Vérifiez sa provenance et sa récupération. Une extension de fichier ne certifie pas son contenu.

Point de pause

Conservez uniquement la mention « association de test vérifiée ».

Supprimer localement un compte WOW déplace-t-il ses bitcoins ?

1. Non. Le parcours supprime des informations locales sans dépenser les UTXO.
2. Oui. Les bitcoins sont envoyés au fabricant.
3. Cela annule toute signature conservée par quelqu’un d’autre.

> **Afficher la réponse: Non. Le parcours supprime des informations locales sans dépenser les UTXO.**
> L’état local et l’état de la chaîne sont distincts.

M05

Associer Mirror à Desk

Objectif

Établir puis terminer une association locale autorisée sans confondre ses codes.

Comprendre

Mirror réalise des opérations locales avec Desk par le parcours d’association, de PIN et de codes QR affiché dans les applications. Le PIN à six chiffres appartient à cette session. Il diffère du mot de passe de Desk, de celui du cryptogramme et des mots de récupération. Vérifiez quel écran le génère et où le saisir. N’utilisez pas de code envoyé par un inconnu.

Lancez l’action depuis le bon contexte de Desk. Associer, lire un code QR, transporter une PSBT et mettre à jour le micrologiciel ont des finalités différentes. La fenêtre rend compte de la recherche, de la connexion, de la détection, du PIN, du code QR puis de l’action sur carte ou fichier. La présence de l’appareil dans les résultats de recherche ne prouve pas que l’opération a abouti.

Accordez les autorisations nécessaires selon le système : caméra pour la lecture optique, Bluetooth ou NFC si le parcours l’exige. Installer un logiciel ne confère pas une capacité physique absente du téléphone. Les adaptateurs et les validations diffèrent sur iOS. Un projet compilable ne doit pas être présenté comme déjà distribué et testé sur tous les iPhone.

En cas d’échec, repérez le stade précis : appareil introuvable, appareil détecté mais non connecté, PIN refusé, code QR illisible, carte non lue ou réponse non reçue. Fermez les anciennes sessions, vérifiez versions et autorisations, puis réessayez de façon contrôlée. Un PIN erroné ne justifie ni de changer de micrologiciel ni de saisir une graine ailleurs.

Mise en pratique

1. Lancez une lecture de test depuis Desk et connectez Mirror en suivant les écrans locaux.
2. Vérifiez la finalité avant de présenter une carte ou un code QR pédagogique.
3. Annulez la session et confirmez qu’une lecture tardive du contexte précédent n’est pas appliquée. Ouvrez une nouvelle session.

À vous de l’expliquer

Décrivez l’étape en échec et les appareils concernés sans communiquer de code actif ni de contenu sensible.

Question fréquente

Mirror doit-il rester connecté en permanence ? Cela dépend de l’opération. Ne le traitez pas comme un service permanent et ne supposez pas que la session demeure autorisée après la fermeture ou le passage en arrière-plan.

Point de pause

Fermez la session d’association et verrouillez les applications inutilisées.

Que doit faire le tuteur si l’association échoue avant l’affichage du PIN ?

1. Demander la graine.
2. Vérifier la détection, les autorisations, la session et les versions avant de poursuivre.
3. Considérer que la connexion a réussi.

> **Afficher la réponse: Vérifier la détection, les autorisations, la session et les versions avant de poursuivre.**
> Le diagnostic doit partir de l’étape observée sans supposer que la connexion a abouti.

NFC via Mirror, USB-C et lecture des codes QR

Objectif

Utiliser chaque moyen de transport selon sa finalité et en effectuer les vérifications.

Comprendre

Les parcours NFC de Cuvex Desktop nécessitent Cuvex Mirror sur un smartphone compatible, associé à l’ordinateur par Bluetooth. Cuvex Desktop ne prend pas en charge les lecteurs NFC USB externes. La carte, son format et sa capacité doivent également convenir. Une petite carte qui peut contenir un cryptogramme n’aura pas forcément assez de place pour une PSBT incluant les transactions antérieures. La limite dépend de l’ensemble du contenu, pas seulement du nombre de destinataires. N’utilisez jamais une carte de sauvegarde comme carte de transport.

Avec Original, Mirror peut écrire une requête sur une carte d’opérations. L’appareil la traite et écrit une réponse que Mirror ramène à Desk. La confirmation d’écriture ne prouve pas que Desk a reçu la réponse. Maintenez la carte immobile jusqu’à l’affichage du résultat. Si le système refuse une opération pour protéger un cryptogramme reconnu, respectez ce refus.

BIT échange des fichiers au moyen d’un volume ou dossier USB. Le volume peut être démonté puis présenté à nouveau pendant l’échange. Desk doit sélectionner le bon support, valider la réponse et en accuser réception selon le protocole. Copier un fichier dans un dossier du PC portant le même nom ne le remet pas à l’appareil.

La mise au point, un reflet, la taille du code QR, son mouvement ou sa densité peuvent empêcher la caméra de le lire. Agrandissez le code, ajustez l’éclairage et la distance. N’abrégez pas un identifiant long à ses premières lettres et n’acceptez aucune transcription partielle. Une lecture réussie n’est que la première étape de validation du sens des données.

Mise en pratique

1. À l’aide des supports du cours, identifiez sur le schéma la requête, le support et la réponse pour Original et pour BIT.
2. Essayez d’annuler la lecture d’un code QR sans enregistrer de valeur reçue tardivement. Recommencez avec un autre objectif.
3. Simulez un fichier trop volumineux. Expliquez comment réduire la complexité de l’opération ou choisir un support compatible tout en conservant les vérifications.

À vous de l’expliquer

Indiquez quel appareil a confirmé chaque étape : lecture, écriture, validation, réception ou accusé de réception.

Question fréquente

Une empreinte ou un message de copie réussie prouve-t-il que le destinataire Bitcoin est le bon ? Non. Vérifiez l’opération et ses sorties sur l’appareil qui signe.

Point de pause

Retirez et rangez les cartes de sauvegarde. Identifiez clairement le support de transport.

Original indique avoir écrit la réponse sur la carte. Que manque-t-il pour pouvoir dire que Desk l’a reçue ?

1. Repeindre la carte d’une autre couleur.
2. Créer une nouvelle graine.
3. Lire la réponse et la valider dans Desk en suivant le parcours approprié.

> **Afficher la réponse: Lire la réponse et la valider dans Desk en suivant le parcours approprié.**
> La réussite de l’écriture et celle de la réception sont deux événements distincts.

Prestataires publics et nœud personnel

Objectif

Choisir une source de consultation et comprendre ses limites et les informations qu’elle peut révéler.

Comprendre

Desk peut interroger des prestataires publics compatibles ou un nœud Bitcoin Core configuré par l’utilisateur. Un prestataire peut connaître les requêtes qu’il reçoit, leur ordre et les données de connexion. Ne pas transmettre de xpub complète réduit une exposition précise. Des scripts ou leurs empreintes peuvent néanmoins être reliés entre eux.

Desk 9.21 propose explicitement Blockstream Electrum via TLS, en plus des options REST et du nœud personnel. TLS protège le canal contre certains observateurs du réseau, mais le prestataire continue de recevoir les requêtes. Aucune rotation silencieuse ne garantit l’anonymat. Choisissez en comprenant le compromis entre confidentialité et commodité.

Pour Core, configurez le point de connexion, l’authentification et le portefeuille en lecture seule selon le guide correspondant. Ne publiez pas le port RPC et ne l’exposez pas à Internet pour que l’application « le voie ». Limitez l’accès aux environnements de confiance et utilisez un transport protégé approprié. Ne dictez pas le mot de passe RPC au tuteur.

La synchronisation initiale et une nouvelle analyse peuvent prendre du temps. La progression indique un travail en cours, pas un succès anticipé. Desk poursuit le travail en arrière-plan : fermer la vue n’arrête pas le nœud. La fenêtre historique minimale documentée ne garantit pas la découverte d’une activité plus ancienne. Pour un portefeuille ancien, vérifiez la date d’import et la période réellement analysée.

La découverte repose sur l’historique, non sur un solde positif. Une adresse dont le solde a été dépensé jusqu’à zéro a tout de même servi. En multisignature dans l’implémentation examinée, le seuil est de 20 adresses consécutives sans historique par branche et par participant, avec des limites d’émission. N’extrapolez pas une limite globale à tous les portefeuilles.

Mise en pratique

1. Choisissez une source d’apprentissage et indiquez les informations qu’elle peut voir.

2. Vérifiez la date de dernière synchronisation, le réseau et la progression. En cas de HTTP 429, respectez la pause et ne changez de prestataire que délibérément.
3. Simulez un portefeuille au solde nul avec un ancien historique. Expliquez en quoi « zéro » diffère de « jamais utilisé ».

À vous de l’expliquer

Déterminez si la source répond à vos besoins de vérification et de confidentialité et reconnaissez un état incomplet.

Question fréquente

Mon propre nœud me rend-il anonyme ? Non. Il réduit la dépendance aux services interrogés, mais il faut aussi considérer la connexion, les contreparties, la diffusion et les autres métadonnées.

Point de pause

Notez uniquement le type de prestataire et si l’analyse doit être terminée.

Une adresse a un solde nul, mais elle a déjà reçu puis dépensé des fonds. Comment faut-il la traiter lors de la découverte du portefeuille ?

1. Comme une adresse avec un historique.
2. Comme une adresse jamais utilisée.
3. Comme une adresse invalide.

> **Afficher la réponse: Comme une adresse avec un historique.**
> L’historique détermine si elle a été utilisée, indépendamment de son solde actuel.

Recevoir des bitcoins et vérifier l’adresse

Objectif

Créer une demande de réception et la vérifier avant de la transmettre.

Comprendre

Ouvrez le bon compte WOW et confirmez réseau et politique. Générez ou retrouvez une demande de réception. Pour votre organisation, vous pouvez ajouter un motif, un observateur et le montant attendu. Ces champs décrivent des informations locales : le montant attendu n’empêche pas quelqu’un d’en envoyer un autre.

Vérifiez l’adresse par le parcours disponible sur l’appareil, dans le contexte du portefeuille. Si cette combinaison n’a pas été validée physiquement, limitez l’exercice à la simulation et faites examiner le cas avant de recevoir des fonds importants. Comparer deux écrans alimentés par la même source ne crée pas de vérification indépendante.

Lorsque le parcours le permet, utilisez une nouvelle adresse pour une nouvelle relation d’encaissement. Dans la multisignature examinée, les adresses déjà affichées ne sont pas réattribuées et n’expirent pas, car le payeur peut les utiliser plus tard. Si la limite de nouvelles adresses consécutives sans historique est atteinte, retrouvez la demande antérieure adéquate et comprenez la raison de la limite. Ne rembobinez pas les indices.

Après le partage, surveillez la réception auprès de votre source de vérification. Un e-mail, un justificatif de plateforme ou une capture du payeur ne prouve pas le règlement. Vérifiez réseau, txid, sortie, montant et confirmations en fonction de l’enjeu. N’ouvrez pas votre adresse dans un explorateur public par commodité si votre plan exige la confidentialité des consultations.

Mise en pratique

1. Générez une demande dans le laboratoire, vérifiez le compte et le réseau, puis expliquez comment vous contrôleriez l’adresse.
2. Inscrivez une étiquette fictive et retrouvez la même demande après fermeture de la vue.
3. Simulez un encaissement d’un montant différent et décidez comment le rapprocher de la demande sans modifier l’historique.

À vous de l’expliquer

Distinguez adresse générée, adresse vérifiée, demande partagée et encaissement confirmé.

Question fréquente

Une ancienne adresse cesse-t-elle de fonctionner si j’en crée une autre ? Normalement non. Conserver la découverte et l’historique des demandes permet de garder les paiements tardifs visibles.

Point de pause

Gardez l’état de la demande du laboratoire sans en communiquer le contenu au tuteur.

Le payeur envoie une capture indiquant « retrait terminé ». Que vérifiez-vous avant d’accepter le paiement ?

1. Uniquement la qualité de la capture.
2. La sortie correspondante et les confirmations nécessaires auprès d’une source réseau fiable.
3. Le mot de passe du payeur.

> **Afficher la réponse: La sortie correspondante et les confirmations nécessaires auprès d’une source réseau fiable.**
> Un justificatif commercial ou une capture ne remplace pas la vérification du paiement.

Étiqueter, geler et sélectionner des UTXO

Objectif

Préparer les entrées sans mélanger par accident des origines différentes.

Comprendre

Les étiquettes conservent un contexte absent de la chaîne : origine, contrepartie, finalité et restrictions d’usage. Dans Desk, l’étiquette d’un UTXO et la note d’une adresse peuvent avoir des longueurs et fonctions différentes. « Client A » peut suffire. Inscrire une pièce d’identité ou un nom complet peut créer un dossier inutilement sensible.

Geler un UTXO dans Desk l’exclut de certaines sélections locales. Cela ne bloque pas sa dépense sur Bitcoin, ne modifie pas son script et n’empêche pas une autre application munie des clés de l’utiliser. Le solde total et le solde dépensable peuvent donc différer. Vérifiez si une sortie est gelée, réservée par un brouillon ou effectivement dépensée.

La sélection automatique optimise selon son algorithme et son contexte, sans forcément connaître vos relations privées. Pour un paiement donné, examinez s’il vaut mieux utiliser une sortie du même contexte au lieu de regrouper épargne, salaire et activité commerciale. La séparation exige des choix cohérents dans le temps, au-delà du nom des étiquettes.

Exporter les étiquettes au format BIP329 facilite leur conservation ou leur migration. Le format ne chiffre pas les données à lui seul. Desk propose une enveloppe chiffrée : distinguez le fichier protégé du texte en clair compatible. Avant un import qui écrase des données, vérifiez la correspondance avec le portefeuille et le traitement des gels.

Mise en pratique

1. Étiquetez trois UTXO synthétiques « épargne », « activité » et « don ».
2. Gelez l’un d’eux et comparez le solde observé et celui disponible pour sélection.
3. Exportez les étiquettes du laboratoire avec un mot de passe, importez-les dans une copie et vérifiez le résultat sans données privées réelles.

À vous de l’expliquer

Justifiez votre sélection d’entrées selon le coût et l’exposition. Reconnaissez que le gel est une préférence locale.

Question fréquente

Une étiquette est-elle envoyée au destinataire avec le paiement ? Sa simple présence locale ne la transmet pas. Elle peut fuiter lors d’un export, du partage de fichiers, de l’utilisation d’un autre service ou de son ajout à un message.

Point de pause

Gardez les étiquettes d’exercice et les états de gel.

Que se passe-t-il lorsqu’un UTXO est gelé dans Desk ?

1. Un verrou de consensus est créé sur le réseau.
2. L’UTXO est transféré sur un compte spécial.
3. L’application lui applique une restriction locale de sélection.

> **Afficher la réponse: L’application lui applique une restriction locale de sélection.**
> Cela ne révoque pas la capacité de dépense des autres copies des clés.

M06

Préparer et vérifier un paiement

Objectif

Construire une PSBT compréhensible et reconnaître tous ses coûts et toutes ses sorties.

Comprendre

Sélectionnez le compte, les entrées dépensables, les destinataires et les montants. Vérifiez l’origine de la demande. Après collage ou lecture d’un code, examinez l’adresse complète et le réseau : le presse-papiers ou l’image peuvent être remplacés. Ne vous fiez pas uniquement aux premiers et derniers caractères lorsque la procédure offre une vérification complète.

Choisissez le taux de frais, puis examinez les frais absolus, la taille estimée, le total et la monnaie rendue. Avec « Envoyer la totalité », Desk déduit les frais du montant disponible. Si la demande vient de la messagerie et que le montant net est insuffisant, tout paiement partiel doit être intentionnel. La demande d’origine ne change pas pour masquer l’écart.

Vérifiez s’il existe une petite sortie de monnaie rendue ou aucune. Une sortie désignée comme étant à vous se vérifie avec la politique et non d’après le nom donné par le coordinateur. Si la monnaie rendue n’est pas viable, revoyez le balayage du solde ou ajoutez une entrée compatible. N’acceptez pas que le reliquat devienne silencieusement des frais disproportionnés.

La PSBT transporte des informations et des signatures. Ce format n’assure par lui-même ni confidentialité ni authenticité de l’origine. Il peut inclure transactions antérieures, clés publiques, chemins et métadonnées. Dans les micrologiciels Final examinés, le profil multisignature utilise PSBT v0/BIP174. « Transaction version 2 » ne signifie pas « PSBT version 2 ».

Mise en pratique

1. Dans le simulateur, préparez un paiement avec une entrée de 120 000 sat, un montant destinataire de 70 000 sat et des frais de 1 000 sat.
2. Énumérez toutes les sorties et expliquez la monnaie rendue de 49 000 sat. Recommencez avec un balayage du solde.
3. Annulez le brouillon et expliquez ce qui a été annulé localement. N’utilisez pas ce simulateur pour signer ou diffuser quoi que ce soit.

À vous de l’expliquer

Avant l’export, expliquez ce qui entre, ce qui sort, qui reçoit, combien coûte l’opération et quelle autorisation manque.

Question fréquente

Puis-je envoyer la totalité du solde affiché ? Seulement si l’application calcule un montant net viable et si les frais sont couverts. Le solde peut inclure des sorties indisponibles.

Point de pause

Enregistrez ou annulez un brouillon pédagogique. Ne déposez jamais de PSBT réelle sur le portail du cours.

Un écran indique « transaction version 2 ». Cela prouve-t-il que le fichier est une PSBT v2 ?

1. Non. Il s’agit de champs de version différents.
2. Oui, toujours.
3. Cela prouve que la transaction utilise Taproot.

> **Afficher la réponse: Non. Il s’agit de champs de version différents.**
> BIP370 distingue la version du conteneur de celle de la transaction.

Signer avec Original et BIT

Objectif

Mener à terme le parcours de signature de chaque modèle et recevoir une réponse liée à la bonne opération.

Comprendre

Avec Original, transmettez la PSBT sur la carte de transport du parcours compatible, en utilisant Cuvex Mirror. Sur l’appareil, lisez la requête, fournissez le cryptogramme et déverrouillez-le en privé. Vérifiez toutes les sorties, les montants, la monnaie rendue et les frais. La réponse est écrite sur la carte, puis elle doit être lue et validée dans Desk. Une écriture réussie sur la carte ne remplace pas cette étape de retour.

Avec BIT, sélectionnez le bon volume et transmettez la requête par USB-C. Le service local de Desk gère l’échange prévu pendant que vous manipulez l’appareil. Fournissez le cryptogramme selon les indications et vérifiez l’opération sur BIT. « Recevoir de BIT » importe la réponse. Desk la valide et l’enregistre avant de confirmer l’accusé de réception. Après une déconnexion, reprenez la même opération. N’en choisissez pas une autre au motif qu’elle lui ressemble.

Pour une signature multisignature avec les micrologiciels Final, vérifiez le récapitulatif, les sorties obligatoires, les avertissements applicables et les trois confirmations finales « Signer la PSBT ». L’examen approfondi facultatif permet d’explorer davantage de paramètres. Choisir « Non » ne supprime pas les vérifications obligatoires. La vérification indépendante d’une politique suit un autre parcours et sa portée se limite à cet examen précis.

La signature exige un cryptogramme compatible dont l’authenticité est vérifiable. Une ancienne copie peut encore permettre de récupérer le secret sans être utilisable pour signer. Si l’appareil signale une ancienne copie dont l’authenticité n’est pas vérifiée, récupérez et vérifiez le secret, puis créez une nouvelle copie avant de signer. Ne modifiez pas les en-têtes et ne contournez pas le refus.

Annulez si une adresse diffère, si les frais sont inattendus, si une donnée manque, si un autre réseau apparaît ou si l’appareil rejette la politique. Ne laissez pas la pression de terminer l’appel vous pousser à approuver l’opération. L’IA n’appuie pas sur les boutons, ne donne pas la confirmation finale et ne déclare pas signée une opération que vous n’avez pas vérifiée.

Mise en pratique

1. Suivez le parcours de votre modèle avec un portefeuille sans fonds ou un laboratoire ayant fait l’objet de tests d’acceptation physiques.
2. Simulez un arrêt avant les confirmations finales et expliquez pourquoi cela ne vaut pas autorisation.
3. Vérifiez le retour de la réponse, sa correspondance avec le brouillon et, pour BIT, l’état de la réception et de son accusé.

À vous de l’expliquer

Décrivez le parcours sans divulguer d’identifiants secrets. Distinguez l’approbation sur l’appareil, la réponse importée et la transaction diffusée.

Question fréquente

L’appareil hors ligne sait-il si mes entrées restent disponibles ? Il ne peut pas vérifier seul l’état actuel de la chaîne. L’application doit vérifier la transaction finale auprès de sa source réseau.

Point de pause

Si vous interrompez la signature, annulez ou laissez une opération en attente clairement identifiée selon le parcours, sans aucun secret visible.

BIT signe, mais Desk ne confirme pas la réception. Quel état devez-vous retenir ?

1. Le paiement a été diffusé avec certitude.
2. La réponse reste à recevoir ou à valider. Reprenez la même opération.
3. Le portefeuille est perdu.

> **Afficher la réponse: La réponse reste à recevoir ou à valider. Reprenez la même opération.**
> La signature, la réception et la diffusion sont trois étapes distinctes.

Finaliser, diffuser et résoudre les incidents

Objectif

Terminer le paiement sans le dupliquer et diagnostiquer les échecs selon leur étape.

Comprendre

Après l’import d’une signature, Desk doit vérifier sa correspondance avec le brouillon et le maintien de l’intention. En multisignature, le seuil peut ne pas être atteint. En signature unique, l’import ne dispense pas non plus de vérification. Lorsque toutes les conditions sont réunies, la finalisation produit la transaction prête à diffuser.

Ne diffusez qu’après la vérification finale. Une réponse du serveur ou un txid indique le résultat de la requête, mais le suivi doit confirmer l’acceptation et l’état sur la chaîne. En l’absence de réponse de l’application, vérifiez avant de recommencer. Ne créez pas un nouveau paiement pour résoudre un problème d’affichage.

Pour un paiement en attente, vérifiez le taux de frais, la validité, les conflits et la possibilité effective d’utiliser RBF. Toute modification de la politique ou du destinataire requiert une nouvelle proposition et les signatures adéquates. Une annulation locale ne détruit pas une signature ou une transaction déjà conservée par quelqu’un d’autre et ne révoque pas ce qui est confirmé.

Distinguez les phases de préparation, transport, déverrouillage, vérification, signature, retour, validation, finalisation, diffusion et confirmation. Notez système, version, modèle, étape, heure approximative et code d’erreur. Les diagnostics de l’application sont conçus pour exclure les données sensibles. Vérifiez-les néanmoins avant partage et ne joignez ni copies, ni codes QR, ni Clé de chat, ni identifiants secrets.

Mise en pratique

1. Ordonnez les états d’un paiement fictif et indiquez où il est possible de s’arrêter sans risque.
2. Traitez trois incidents : un solde insuffisant, une réponse USB absente et une interruption de connexion pendant la diffusion.
3. Rédigez un ticket avec des données synthétiques et un résultat attendu vérifiable.

À vous de l’expliquer

Déterminez si l’action suivante incombe à l’élève, à l’appareil, au coordinateur ou au réseau, sans créer un second paiement inutile.

Question fréquente

Faut-il changer de micrologiciel à l’aveugle pour corriger FIRMWARE_CAPABILITY_REQUIRED ? Non. Dans l’incident documenté de Desk, la reconnaissance de la version Final exigeait une correction du catalogue de Desk. Vérifiez version et profil avant de modifier les appareils.

Point de pause

Notez l’état et l’action suivante. Si vous avez diffusé une transaction réelle hors laboratoire, gardez sa trace dans votre documentation privée.

Quelle action peut à elle seule révoquer une transaction déjà confirmée ?

1. Supprimer le brouillon local.
2. Fermer Mirror.
3. Aucune de ces actions.

> **Afficher la réponse: Aucune de ces actions.**
> La suppression locale ne réécrit pas la chaîne et ne retire pas les autorisations déjà en circulation.

M07

Ce qui est observable sur Bitcoin

Objectif

Identifier les données publiques, les déductions et les données que vous ajoutez hors chaîne.

Comprendre

Sur la chaîne Bitcoin, les scripts et adresses représentables, les montants, les relations entre entrées et sorties et la position dans les blocs sont publics et analysables. Votre nom n’y apparaît pas nécessairement, mais un achat identifié, une facture publiée ou une adresse partagée peuvent vous relier à cet historique.

Le pseudonymat consiste à utiliser des identifiants qui ne constituent pas en eux-mêmes votre identité civile. L’anonymat exigerait un ensemble et des conditions dans lesquels un observateur ne peut pas vous distinguer. Installer une application ne suffit pas. La confidentialité dépend du contexte : un commerçant connaît votre paiement, une plateforme peut connaître votre retrait, un serveur voit les requêtes et une personne peut observer vos appareils.

Distinguez faits et déductions. « Cette sortie a été dépensée dans cette transaction » est vérifiable sur la chaîne. « Toutes ces entrées appartiennent à la même personne » est une heuristique parfois erronée. Une identification hors chaîne peut renforcer une hypothèse sans rendre toutes les interprétations certaines.

Réutiliser une adresse facilite le regroupement des activités observées. Combiner des UTXO issus de contextes différents peut les relier. Divulguer une xpub permet d’observer davantage que la communication d’une seule adresse. Partager un txid peut aussi exposer d’autres sorties et relations que le destinataire n’avait pas besoin de connaître.

Mise en pratique

1. Sur une transaction fictive, indiquez quelles données sont publiques et quelles étiquettes vous appartiennent.
2. Ajoutez une facture portant un nom et décrivez le nouveau lien créé.
3. Rédigez une demande d’assistance permettant de résoudre une erreur sans fournir d’adresse, de descripteur ni de solde.

À vous de l’expliquer

Dites « cela s’observe » ou « cela se déduit » et précisez quelle preuve manque.

Question fréquente

Si je ne réutilise jamais d’adresse, suis-je anonyme ? Non. La sélection des entrées, la monnaie rendue, les consultations, les contreparties et les autres métadonnées comptent toujours.

Point de pause

Gardez une carte des observateurs sans identité ni transaction réelle.

Quelles données permettent généralement d’observer toute une famille d’adresses d’un compte ?

1. La couleur de l’icône.
2. Sa xpub et un contexte de dérivation suffisant.
3. La marque du câble.

> **Afficher la réponse: Sa xpub et un contexte de dérivation suffisant.**
> Les données publiques étendues sont sensibles pour la vie privée, même si elles ne permettent pas à elles seules d’autoriser une dépense.

Séparer les contextes et gérer la monnaie rendue

Objectif

Prendre des décisions de dépense cohérentes avec l’origine des UTXO.

Comprendre

La séparation des contextes commence avant le paiement. Décidez si une réception correspond à l’épargne, à l’activité professionnelle, aux dépenses courantes ou à une relation précise. Conservez ce contexte dans des étiquettes privées pour éviter qu’une sélection future efface une distinction par ignorance.

Une étiquette ne sépare pas les sorties sur le plan cryptographique. Dépenser ensemble deux UTXO de contextes différents publie leur relation. La consolidation réduit le nombre d’entrées de paiements futurs mais renforce le lien entre les sorties réunies. Profiter de frais bas peut être économique tout en étant contraire à votre objectif de confidentialité.

La monnaie rendue est une nouvelle sortie contrôlée par la même politique, et non de « l’argent invisible ». Son usage ultérieur peut prolonger des liens antérieurs. Ne désignez pas une adresse comme monnaie rendue au vu d’un montant inhabituel : lors d’une vérification réelle, l’appareil doit contrôler son appartenance au portefeuille.

Évitez de transformer vos pratiques de confidentialité en séries mécaniques de montants, d’horaires ou de virements répétés. Ces habitudes peuvent aussi être reconnues et occasionner des frais. Évaluez ce que sait chaque partie et ce que l’opération publierait de nouveau. Aucune série de transactions n’efface l’historique déjà publié.

Mise en pratique

1. Créez cinq UTXO fictifs de trois contextes et préparez un paiement employant le moins de contextes nécessaire.
2. Identifiez la monnaie rendue et choisissez son étiquette.
3. Comparez le coût et l’exposition d’une consolidation de toutes les sorties avec leur maintien séparé.

À vous de l’expliquer

Justifiez ou refusez une consolidation pour une raison concrète, sans imposer une règle absolue à tous les cas.

Question fréquente

Transférer tout vers une autre de mes adresses rompt-il l’historique ? Non. Le transfert publie un lien supplémentaire et peut ajouter des frais sans réduire la menace qui vous concerne.

Point de pause

Conservez le raisonnement de l’exercice et la politique de sélection choisie.

Que peut entraîner la consolidation d’un salaire et de dons dans une même transaction ?

1. Rendre visible un lien entre ces entrées.
2. Effacer leur provenance publique.
3. Les transformer en espèces dont l’anonymat est garanti.

> **Afficher la réponse: Rendre visible un lien entre ces entrées.**
> Réduire le nombre d’UTXO peut multiplier les liens observables.

M07

Confidentialité du réseau, Tor et VPN

Objectif

Distinguer la confidentialité de la connexion de celle de la chaîne.

Comprendre

Un serveur de consultation peut relier des requêtes à une connexion. Selon le transport, votre fournisseur d'accès peut observer des destinations ou des schémas de trafic. Un VPN transfère une partie de cette confiance à son opérateur. Il n'efface pas les informations publiques de Bitcoin et n'empêche pas un compte identifié de vous reconnaître.

Tor achemine le trafic dans un réseau pour réduire certains liens entre source et destination. Il ne rend pas une adresse Bitcoin privée et ne protège pas une application dont le trafic ne passe pas par Tor. Ouvrir Tor Browser ne configure pas automatiquement Desk, Bitcoin Core ni tous les services de l'ordinateur.

Avant d'affirmer qu'une connexion est protégée, vérifiez son trajet et sa configuration. L'implémentation examinée ne présume pas de l'existence d'un interrupteur Tor dans Desk. Un déploiement avec nœud ou proxy exige des consignes techniques et la validation du trafic réel. La présence d'un champ dans un autre portefeuille ne justifie pas de l'inventer dans Desk.

Le DNS, la synchronisation de comptes, les liens d'explorateur et les services de prix peuvent également révéler des informations. Un dispositif qui protège les requêtes de solde peut encore exposer l'activité lors de l'ouverture d'un explorateur public. Définissez la portée de chaque mesure et le comportement en cas de panne de connexion. Évitez une bascule silencieuse vers une source moins privée.

Mise en pratique

1. Dessinez le trajet depuis l'ordinateur à travers le fournisseur d'accès et le proxy éventuel, puis le nœud ou service et le réseau Bitcoin.
2. Indiquez qui reçoit les requêtes et qui connaît votre identité commerciale.
3. Simulez l'absence de réponse du nœud privé. Choisissez entre suspendre et changer explicitement de source en connaissant l'exposition.

À vous de l’expliquer

Expliquez quelle menace votre configuration réduit et quelle menace subsiste.

Question fréquente

Tor garantit-il que personne ne pourra me relier à un paiement ? Non. Les contreparties, l’identification commerciale, les habitudes et les erreurs d’utilisation peuvent encore permettre ce rapprochement.

Point de pause

Notez la portée du dispositif, sans points de connexion privés ni mots de passe.

Ouvrir Tor Browser oblige-t-il Desk à effectuer ses consultations par Tor ?

1. Oui, puisqu’ils partagent le même ordinateur.
2. Oui, si l’icône est visible.
3. Non. Il faut configurer et vérifier le chemin réseau de chaque application.

> **Afficher la réponse: Non. Il faut configurer et vérifier le chemin réseau de chaque application.**
> La protection d’une application ne s’étend pas automatiquement aux autres.

CoinJoin, Payjoin et leurs limites actuelles

Objectif

Comprendre les techniques collaboratives sans leur attribuer anonymat ou compatibilité inexistants.

Comprendre

CoinJoin regroupe les apports de plusieurs personnes dans une transaction pour compliquer certaines déductions sur ses entrées et ses sorties. Il se distingue de la remise de fonds à un dépositaire promettant d'en rendre d'autres. Chaque conception exige d'examiner la coordination, la garde, les frais, la résistance aux participants malveillants et l'utilisation ultérieure.

Payjoin intègre des entrées du payeur et du bénéficiaire dans un paiement collaboratif, ce qui affaiblit certaines heuristiques de propriété commune. Il exige une prise en charge compatible aux deux extrémités et un protocole précis. C'est ici une notion technique : les sources examinées n'établissent pas l'existence d'un parcours Payjoin ou CoinJoin intégré et opérationnel dans Cuvex Desk.

La disponibilité et le contexte juridique évoluent. La documentation de Wasabi signale l'arrêt du coordinateur de zkSNACKs le 1er juin 2024. Un ancien bouton ne doit pas être enseigné comme une garantie de service aujourd'hui. En 2025, le ministère américain de la Justice a annoncé les plaidoyers de culpabilité puis les condamnations des fondateurs de Samourai. Cette affaire ne permet pas de conclure que toute technique de confidentialité est illégale dans toute juridiction.

Un outil peut réduire une déduction sans en affecter d'autres. Une origine identifiée reste dans les dossiers d'une contrepartie. Des regroupements ultérieurs, les métadonnées et les défaillances du groupe de participants peuvent dégrader la confidentialité. Certains services peuvent aussi appliquer des politiques commerciales différentes selon l'historique des fonds.

Mise en pratique

1. Comparez une transaction ordinaire, une transaction collaborative et un service qui prend les fonds en garde, sans réaliser d'opérations réelles.
2. Avant de proposer un outil, vérifiez sa version, son mainteneur, l'état du service et sa documentation actuelle.

3. Identifiez séparément risques techniques, risques de garde et risques juridiques. Le tuteur ne doit ni concevoir de contournement des contrôles ni promettre des « fonds impossibles à tracer ».

À vous de l’expliquer

Présentez un avantage limité et au moins deux risques ou conditions d’une technique de confidentialité.

Question fréquente

Cuvex a-t-il besoin d’un mixeur pour protéger la confidentialité de la garde ? Non. Maîtriser les requêtes, les données, les clés et la sélection des UTXO répond déjà à des risques précis, sans promettre de dissimulation intégrale.

Point de pause

Notez qu’un outil a été « étudié ». Ne le dites « compatible » qu’avec des preuves.

Quelle affirmation est défendable ?

1. CoinJoin garantit un anonymat permanent.
2. Une technique collaborative peut compliquer certaines déductions, sous certaines conditions et dans certaines limites.
3. Tout service appelé « mixeur » préserve la garde en propre.

> **Afficher la réponse: Une technique collaborative peut compliquer certaines déductions, sous certaines conditions et dans certaines limites.**
> Les propriétés dépendent du protocole, de sa mise en œuvre, des participants et de l’usage ultérieur.

Leçons tirées d’incidents réels

Objectif

Tirer des décisions vérifiables d’incidents documentés, sans attaquer de concurrents ni exagérer une protection.

Comprendre

Mt. Gox. Un acte d’accusation de 2023 du ministère américain de la Justice décrit un accès non autorisé à des serveurs et à des clés, puis la disparition de fonds de clients. Un acte d’accusation énonce des allégations et ne constitue pas un jugement. Pour la garde, demandez qui contrôle réellement les clés et ce qui se passe en cas de défaillance de l’entreprise.

Ledger Connect Kit, décembre 2023. Ledger a documenté la publication malveillante d’une bibliothèque employée par des applications décentralisées, après compromission de l’accès d’un ancien salarié. L’incident a touché la distribution du logiciel et trompé des utilisateurs de DApps EVM pour les faire signer. Il ne démontre ni rupture du matériel Ledger ni rupture du consensus Bitcoin.

Bybit, février 2025. Le FBI a attribué à la Corée du Nord le vol d’environ 1,5 milliard de dollars d’actifs virtuels. L’incident concernait une plateforme d’échange et des actifs d’autres réseaux. Il ne constitue pas une rupture de la cryptographie de Bitcoin. Pour l’élève, il importe de vérifier l’intention d’une signature et d’éviter que plusieurs personnes fassent aveuglément confiance au même écran.

Coinbase, mai 2025. L’entreprise a annoncé un vol de données par des agents d’assistance soudoyés pour faciliter l’ingénierie sociale. Elle a indiqué qu’aucun mot de passe ni aucune clé privée n’avaient été exposés. Un escroc peut connaître des renseignements exacts sans être pour autant un interlocuteur légitime.

Bitcoin Core publie aussi des défauts logiciels. L’avis CVE-2024-35202 décrivait un arrêt déclenchable à distance dans les versions antérieures à 25.0. Vérifier les règles ne dispense pas d’entretenir le logiciel. Cet avis ne permet pas de conclure à un vol de clés.

En janvier 2026, The Register a signalé une exposition de données de commande et de contact d’acheteurs de Ledger via Global-e. Le journal a attribué des confirmations aux deux entreprises, dont les déclarations indiquaient que les clés de récupération n’étaient pas touchées. Un achat peut révéler la possession d’un appareil sans que celui-ci ait été compromis.

En avril 2026, The Record a rapporté l’attaque contre Drift et la suspension des dépôts et retraits annoncée par la plateforme. Il s’agit d’un protocole de finance décentralisée sur Solana, sans rupture de Bitcoin. Ne présentez pas les premières estimations de pertes comme définitives ni les démarches de récupération ultérieures comme une garantie de remboursement.

Mise en pratique

1. Classez les incidents selon la garde, l’interface ou la distribution, les données personnelles, les protocoles d’autres réseaux et la disponibilité.
2. Pour chacun, proposez une mesure préventive et indiquez-en une limite.
3. Simulez un appel frauduleux : « Je connais votre achat. Déplacez vos fonds vers cette adresse sûre. » Raccrochez et vérifiez par un canal que vous avez vous-même ouvert.

À vous de l’expliquer

Expliquez pourquoi aucun incident ne prouve qu’une autre marque est invulnérable. Chaque preuve a une portée précise.

Question fréquente

S’agit-il de tous les derniers piratages ? Non. C’est une sélection vérifiée pour l’édition du 17 novembre 2026, et non un inventaire exhaustif ni une veille en direct.

Point de pause

Notez quelle habitude vous allez changer et comment vous vérifierez que vous la conservez.

Un interlocuteur connaît votre achat et vous demande de transférer des fonds vers un « portefeuille de secours ». Que prouve sa connaissance de l’achat ?

1. L’information a pu fuiter. Elle n’authentifie ni l’interlocuteur ni l’adresse.
2. Il s’agit forcément de l’assistance légitime.
3. Vous devez communiquer la graine.

> **Afficher la réponse: L’information a pu fuiter. Elle n’authentifie ni l’interlocuteur ni l’adresse.**
> Des informations exactes peuvent servir à construire une escroquerie convaincante.

Créer une identité de messagerie et vérifier ses contacts

Objectif

Activer une identité de messagerie sans exposer sa clé et vérifier son interlocuteur.

Comprendre

Dans Desk, la messagerie est liée au cryptogramme par une Clé de chat générée sur Cuvex. Son apparence peut rappeler une xpub, mais elle est secrète et ne doit pas être traitée comme la clé publique d’un compte WOW. Le tuteur n’a jamais besoin de la lire ni de voir son code QR.

Le parcours distingue la création d’un alias, le transfert ou la récupération d’un alias existant. Dans l’implémentation examinée, il faut choisir le profil mobile iOS ou Android correspondant. Ne supposez pas que les identités dérivées historiquement sont interchangeables. DEV et Production sont des environnements séparés. Changer d’environnement ne transfère pas automatiquement les conversations ou les alias.

Ajouter un alias ne vérifie pas une identité. Comparez l’empreinte par un canal indépendant et authentifié. Si l’application propose des questions de reconnaissance, utilisez des renseignements non publics sans révéler de mots de passe dans les réponses. Une voix familière peut être imitée. Dans les situations à risque, combinez des méthodes convenues à l’avance.

Si l’identité d’un contact change, suspendez paiements et coordination jusqu’à éclaircissement. Il peut s’agir d’une récupération légitime ou d’une substitution malveillante. Le chiffrement de bout en bout protège le canal selon son protocole et sa mise en œuvre. Il ne prouve pas qui utilise l’appareil à l’autre extrémité.

Mise en pratique

1. Dans un environnement de test, expliquez la création ou la récupération sans fournir la Clé de chat.
2. Ajoutez un contact de laboratoire et convenez sur un autre canal de la vérification d’empreinte.
3. Simulez un changement d’identité. Définissez comment vous le confirmeriez avant de payer.

À vous de l’expliquer

Distinguez alias, empreinte publique, Clé de chat secrète et confiance personnelle accordée à un individu.

Question fréquente

Un ancien alias garantit-il qu’il s’agit de la même personne ? Non. Vérifiez la continuité et les changements de clés selon le parcours prévu.

Point de pause

Inscrivez uniquement « contact de test vérifié » et la méthode, sans clé ni question privée.

Une chaîne de caractères nommée « Clé de chat » ressemble à une xpub. Comment faut-il la traiter dans Desk ?

1. Comme une donnée publiable sur un forum.
2. Comme un secret de récupération d’identité.
3. Comme une adresse de réception Bitcoin.

> **Afficher la réponse: Comme un secret de récupération d’identité.**
> L’apparence d’une donnée ne détermine ni sa confidentialité ni son usage.

M08

Demander et payer des satoshis depuis la messagerie

Objectif

Passer d’une conversation à un paiement en conservant les vérifications et le contexte.

Comprendre

La messagerie permet de demander une adresse, de répondre avec une adresse de réception, de solliciter un paiement et d’ouvrir sa préparation depuis un compte WOW. Conserver le contexte dans un même canal réduit les erreurs de copie entre applications, sans transformer chaque message en ordre de dépense authentifié.

Avant de répondre ou de payer, vérifiez le contact authentifié, le réseau, le montant et la demande d’origine. Le formulaire partagé conserve la sélection d’UTXO et les frais. Si un montant est demandé et que vous choisissez « Envoyer la totalité », le montant net après frais peut être inférieur. Indiquez alors explicitement qu’il s’agit d’un paiement partiel.

L’autorisation reste sur Cuvex. La messagerie véhicule l’intention et la coordination, sans permission de signer automatiquement. La confirmation envoyée au contact doit distinguer la réception d’un message de l’existence d’une transaction confirmée. Le destinataire vérifie avec son propre compte ou sa propre source.

Liens externes, codes QR joints et adresses restent non fiables jusqu’à validation. « Voir dans Mempool » peut ouvrir un service tiers et révéler des consultations. Si votre politique prévoit un nœud personnel, utilisez de préférence la vérification compatible dans WOW et évaluez tout passage vers un service public.

Mise en pratique

1. Jouez deux rôles : le destinataire demande 50 000 sat et le payeur prépare l’opération sans la diffuser.
2. Simulez un solde net disponible de 48 000 sat. Expliquez quels accord et rapprochement manquent pour un paiement partiel.
3. Modifiez délibérément le réseau dans un message de test et interrompez la procédure.

À vous de l’expliquer

Retracez les liens entre demande, adresse, brouillon, signature et confirmation sans vous limiter à « la messagerie indique OK ».

Question fréquente

Envoyer des sats depuis la messagerie implique-t-il l’utilisation de Lightning ? Non. Le parcours documenté de WOW prépare des paiements sur la chaîne Bitcoin. Le mot « sats » désigne une unité, pas un réseau de transport.

Point de pause

Annulez le brouillon de laboratoire ou notez son état. Ne diffusez pas un paiement pour démontrer une interface.

Vous recevez une confirmation dans la messagerie. Quelle vérification est décisive pour constater le paiement ?

1. L’icône du message est verte.
2. L’interlocuteur écrit « confirmé ».
3. Vérifier la transaction et ses sorties sur le réseau auprès d’une source appropriée.

> **Afficher la réponse: Vérifier la transaction et ses sorties sur le réseau auprès d’une source appropriée.**
> L’état du message et celui de la transaction sont distincts.

Partager des cryptogrammes en connaissance de cause

Objectif

Comprendre les conséquences de la remise d’une copie chiffrée à une autre personne.

Comprendre

Partager un cryptogramme transmet une copie de l’objet chiffré. Cela n’envoie pas nécessairement des bitcoins et n’ajoute pas à lui seul un nouveau signataire. Si le destinataire obtient aussi suffisamment de moyens de déverrouillage, il peut accéder au contenu selon le schéma prévu. Décidez à l’avance quelle capacité vous transférez.

Le chiffrement de bout en bout de la messagerie et le chiffrement du fichier protègent des couches différentes. Une fois le fichier téléchargé, le destinataire peut le garder en dehors de la discussion. Supprimer votre message ou votre enregistrement local ne garantit pas la disparition de toutes les copies. Partager le mot de passe par le même canal peut réunir les composants nécessaires en un seul endroit.

Avant l’envoi, vérifiez identité, format et finalité. Si l’application permet d’associer un cryptogramme reçu, elle organise ainsi une copie sans garantir qu’un fichier quelconque peut être déchiffré sans risque. N’utilisez pas de pièce jointe qui exige la saisie d’une graine ou d’un mot de passe sur une page externe.

La récupération suppose un accord pratique : qui conserve chaque composant, qui peut l’ouvrir, comment détecter une exposition et comment modifier la garde si la relation cesse. Pour un paiement ordinaire, une adresse validée suffit généralement. Il n’est pas nécessaire de partager votre cryptogramme.

Mise en pratique

1. Concevez le transfert d’un texte pédagogique chiffré vers un contact de laboratoire.
2. Énumérez ce que sait le destinataire et ce qu’il pourrait faire avant et après avoir appris le mot de passe.
3. Simulez la fin de la relation. Expliquez pourquoi supprimer le message ne révoque ni la copie ni les clés.

À vous de l’expliquer

Distinguez « j’ai partagé des données », « j’ai donné accès à un secret » et « j’ai signé une dépense ».

Question fréquente

Un fichier chiffré peut-il circuler sans conséquence ? Il peut révéler des métadonnées, faciliter des tentatives de découverte du mot de passe et être conservé indéfiniment. Évaluez la nécessité de le partager.

Point de pause

Ne laissez pas de pièces jointes de garde dans le cours. Notez uniquement la conclusion de l’exercice.

Partager un cryptogramme dans la messagerie revient-il à envoyer des bitcoins ?

1. Non. Cela transmet un objet dont le contenu et les conditions d’accès ont une autre portée.
2. Oui, si le nom se termine par .bin.
3. Cela active automatiquement un nouveau portefeuille multisignature.

> **Afficher la réponse: Non. Cela transmet un objet dont le contenu et les conditions d’accès ont une autre portée.**
> Transporter des secrets et déplacer des UTXO sont des opérations distinctes.

Récupérer la messagerie et comprendre ses métadonnées

Objectif

Préparer un changement d’appareil en distinguant la récupération de l’identité de celle des messages.

Comprendre

Desk indique que l’historique et les sessions sont chiffrés localement et exclus de sa sauvegarde globale. La Clé de chat permet de récupérer l’identité, sans garantir le retour de toutes les anciennes conversations. L’application comporte des états et des commandes pour l’activation en attente, l’entretien des clés et la récupération locale lorsque les éléments compatibles existent.

Le guide de l’implémentation examinée prévoit un seul appareil à la fois par alias. N’activez pas l’alias simultanément sur deux appareils pour « tester la synchronisation » si cet usage n’est pas pris en charge. Tout transfert doit suivre la procédure et donner lieu à une vérification de continuité avec les contacts.

« En attente », « accepté par le serveur », « reçu » et « déchiffrement impossible » décrivent des étapes distinctes. En l’absence de confirmation, ne renvoyez pas le message à l’aveugle : établissez d’abord s’il est arrivé. Si une clé de session manque ou si l’identité change, conserver le message en attente ne signifie pas l’avoir lu.

Le chiffrement du contenu ne cache pas forcément à tous les systèmes concernés les horaires, la taille, les relations de distribution, les alias ou les données de connexion. La voix présente une limite comparable : le chiffrement du transport ne rend pas un appel ordinaire adapté à la transmission de secrets. Utilisez uniquement les données nécessaires à l’apprentissage ou au diagnostic.

Mise en pratique

1. Simulez la perte du PC et expliquez ce que chaque élément disponible permet de récupérer.
2. Classez les états des messages et décidez quand il ne faut pas renvoyer une demande de paiement.
3. Préparez un avis de changement d’appareil que vos contacts pourront vérifier par un canal indépendant.

À vous de l’expliquer

Expliquez quelle conversation serait perdue et quelle identité pourrait être restaurée, sans promettre une restauration au-delà du périmètre de la sauvegarde.

Question fréquente

Supprimer ma discussion locale efface-t-il les messages à l’autre extrémité ? Ne le supposez pas. Le destinataire peut conserver ses messages et fichiers indépendamment.

Point de pause

Gardez un plan de transfert avec des intitulés de champs vides, sans Clé de chat.

D’après le guide examiné, que garantit à elle seule la Clé de chat ?

1. Toutes les conversations passées sur n’importe quel PC.
2. La récupération de l’identité par le parcours compatible, sans garantie de retrouver tous les anciens messages.
3. L’accès automatique aux clés Bitcoin des contacts.

> **Afficher la réponse: La récupération de l’identité par le parcours compatible, sans garantie de retrouver tous les anciens messages.**
> La récupération d’une identité et celle des archives de messages sont deux capacités distinctes.

Réglages du quotidien et vérification des autorisations

Objectif

Maîtriser les réglages de Desk et distinguer confort d’utilisation et protection.

Comprendre

Desk propose les thèmes Nuit, Jour ou Système, la synchronisation automatique par périodes de 3 ou 5 minutes, les sons de transaction, le fond de la messagerie, la langue et la devise de référence. Ces préférences changent la présentation ou la fréquence des consultations. Elles ne modifient pas une signature Bitcoin et n’ajoutent pas d’anonymat.

Les réglages de sécurité examinés permettent le verrouillage après inactivité ou passage en arrière-plan, un délai maximal après échecs et un effacement facultatif. Le schéma d’inactivité admet de 30 à 86 400 secondes. L’interface peut proposer des choix plus restreints. Vérifiez les valeurs par défaut dans la version exécutée plutôt que de les déduire d’une leçon enregistrée.

L’intégration des liens bitcoin: ouvre une demande exigeant déverrouillage, choix du compte et vérification. Elle n’autorise pas un paiement automatique. Sous Linux, le guide distingue l’installation intégrée de l’AppImage pour l’enregistrement des liens. Une demande Lightning nécessite un autre parcours compatible. Déclarer Desk application par défaut ne suffit pas.

La cotation, le graphique de cours et les liens d’information peuvent consulter des services externes. Ils renseignent sans constituer des signaux d’achat. Vérifiez date et source avant de convertir des montants. Ni le mode sombre ni une petite fenêtre ne doivent masquer les commandes finales, l’adresse ou les frais. Dans ce cas, suspendez l’opération et signalez le problème d’affichage.

Mise en pratique

1. Réglez l’apparence et le verrouillage dans le stockage d’apprentissage. Vérifiez que vous pouvez vous reconnecter.
2. Passez en revue les automatismes activés : synchronisation, sons et vérification du micrologiciel ont des effets différents.
3. Ouvrez une demande fictive par lien bitcoin: et annulez avant de préparer une opération réelle.

À vous de l’expliquer

Expliquez l’effet de chaque réglage et repérez ceux qui impliquent des consultations ou des actions sensibles.

Question fréquente

La biométrie du PC remplace-t-elle ma sauvegarde de récupération ? Non. Elle peut dépendre de l’appareil et du stockage sécurisé du système. Conservez une méthode indépendante.

Point de pause

Verrouillez Desk et notez uniquement les préférences modifiées.

Que modifie le choix d’une synchronisation toutes les trois minutes ?

1. La fréquence prévue des consultations lorsque la fonction est active.
2. La politique de signature sur la chaîne.
3. La graine de l’appareil.

> **Afficher la réponse: La fréquence prévue des consultations lorsque la fonction est active.**
> C’est un réglage de fonctionnement, sans modification de la garde.

M09

Concevoir un portefeuille multisignature

Objectif

Choisir un seuil qui résiste à des pertes et compromissions plausibles.

Comprendre

Dans une politique M sur N, N représente le nombre de participants aux clés distinctes et M le nombre de signatures exigées. Une politique 2 sur 3 tolère l'indisponibilité d'une clé, mais deux clés compromises permettent d'autoriser une dépense. Si les trois graines se trouvent au même endroit ou ont subi la même exposition, leur indépendance diminue.

Le profil multisignature Cuvex examiné utilise P2WSH natif avec sortedmulti et une dérivation BIP48. Original admet structurellement jusqu'à six clés de politique, et BIT jusqu'à quinze. Si les deux participent, respectez le modèle le plus limité et la taille réelle du moyen de transport. Les limites structurelles ne garantissent pas qu'une politique avec de nombreuses clés et entrées puisse tenir sur le support.

L'application accepte des seuils respectant les relations de la politique, mais une politique 1 sur N n'exige pas de collaboration pour dépenser. Le micrologiciel conserve des avertissements spécifiques à ce risque. Choisir un plus grand nombre n'améliore pas tout : coordination, coûts, données de récupération et risque de blocage augmentent.

MuSig2 est un autre schéma d'agrégation de signatures Schnorr. À lui seul, il fonctionne en N sur N, et non selon un seuil arbitraire 3 sur 5. Les micrologiciels Final examinés ne prennent en charge ni la signature d'entrées Taproot, ni MuSig2, ni Miniscript. Accepter un destinataire P2TR ne prouve pas que l'on peut signer depuis un portefeuille Taproot.

Mise en pratique

1. Concevez une politique fictive 2 sur 3 avec des risques indépendants pour chaque participant.
2. Simulez la perte d'une clé et la compromission d'une clé. Expliquez ce qui reste possible ou impossible.
3. Vérifiez les limites de chaque modèle avant de choisir une politique plus large.

À vous de l’expliquer

Indiquez la tolérance à la perte, le seuil de compromission et les dépendances communes de votre conception.

Question fréquente

La multisignature exige-t-elle que les participants connaissent les graines des autres ? Non. Chacun doit conserver sa capacité privée tout en partageant les informations publiques qui permettent de construire et de récupérer la politique.

Point de pause

Gardez le schéma avec des participants fictifs et leurs responsabilités.

Pour une politique 2 sur 3 à clés indépendantes, combien de clés privées suffisent à autoriser une dépense valide selon cette politique ?

1. Une.
2. Deux.
3. Toujours les trois.

> **Afficher la réponse: Deux.**
> Le seuil en exige deux. Les autres conditions et vérifications doivent également être satisfaites.

Créer des invitations et fournir des clés

Objectif

Construire une politique avec des participants vérifiés sans partager les graines.

Comprendre

Le créateur choisit le nom, le réseau, M, N, les contacts, ses propres données publiques et les conditions pratiques de l’invitation. Le schéma examiné accepte mainnet et regtest, de 2 à 15 participants avant application des limites matérielles, et une expiration opérationnelle de 1 à 720 heures. Ces limites n’autorisent pas à omettre une vérification de capacité.

Chaque participant examine l’invitation, décide de l’accepter ou de la refuser et fournit sa clé publique étendue avec empreinte et chemin BIP48 par le parcours compatible. Il ne fournit ni graine, ni clé privée, ni adresse isolée, ni descripteur complet d’un autre portefeuille. Une clé utilisée dans le mauvais contexte peut produire une autre politique tout en ressemblant à une xpub valide.

Le créateur coordonne sans remplacer la validation de chaque signataire. Avant de recevoir des fonds, tous doivent pouvoir reconstruire et vérifier les mêmes paramètres et une adresse de contrôle. Accepter un contact dans la messagerie n’approuve pas automatiquement les politiques qu’il envoie.

L’expiration de l’invitation est une règle de coordination de l’application. Elle ne modifie pas à elle seule un script déjà financé, n’efface pas les signatures conservées par d’autres et ne fonctionne pas comme un verrou temporel de consensus. Annuler une proposition et retirer des fonds d’une politique existante sont des actions distinctes.

Mise en pratique

1. Dans un laboratoire regtest préparé, créez une proposition 2 sur 3 avec des contacts de test.
2. Jouez une acceptation, un refus et une contribution sur le mauvais réseau. Vérifiez que la dernière est bloquée.
3. Énumérez ce que tous doivent conserver avant de financer : réseau, seuil, clés publiques, origines, script et adresse vérifiée.

À vous de l’expliquer

Reconnaissez une invitation incomplète et expliquez quelle approbation manque sans la déduire de la seule existence d’une discussion.

Question fréquente

Une échéance rend-elle impossible toute dépense ultérieure ? Pas s’il s’agit d’un simple champ d’invitation. Une restriction temporelle de Bitcoin exige des conditions spécifiques dans le script ou la transaction et une prise en charge effective.

Point de pause

Gardez l’identifiant pédagogique de la proposition et l’approbation en attente.

Que demande le parcours documenté lorsque vous apportez votre contribution au portefeuille multisignature ?

1. La graine de tous les participants.
2. Une adresse de réception quelconque.
3. Votre clé publique étendue avec une empreinte et une origine BIP48 compatibles.

> **Afficher la réponse: Votre clé publique étendue avec une empreinte et une origine BIP48 compatibles.**
> Les données publiques adéquates permettent de construire la politique sans divulguer de clés privées.

Vérifier les politiques avec Mirror dans l’ordre de votre choix

Objectif

Comparer les champs complets et comprendre précisément ce qu’atteste le résultat.

Comprendre

La vérification indépendante présente le seuil, le réseau, le profil, SIGHASH, l’identifiant de politique, la première adresse, la position de l’utilisateur et les données de chaque participant. Elle contrôle l’intention et la cohérence. Elle ne suppose pas que l’appareil a enregistré une politique de façon permanente. La portée documentée est limitée à « cet examen ».

Dans Mirror 12.12, vous pouvez lire d’abord le code QR de Cuvex ou celui de Desk et choisir n’importe quel champ. Il n’est pas obligatoire de commencer à l’étape 1, de tout scanner ou de suivre un ordre. Si vous vérifiez un texte à la main et omettez son scan, Mirror ne l’indique pas comme vérifié par lui.

Le comparateur affiche le texte littéral complet. Espaces, sauts de ligne, casse et différences Unicode comptent. « Correspondance » signifie que les deux valeurs de la paire sont égales. Cela n’authentifie pas leur provenance, ne prouve pas leur appartenance à la même politique et n’active pas le portefeuille. L’approbation finale et sa réponse associée passent toujours par le parcours Cuvex et Desk.

Les codes QR actuels de Desk ne contiennent que la valeur, sans numéro d’étape ni session. Mirror ne peut donc pas toujours déduire l’étape. « Indiquer l’étape de Desk » ajoute un contexte manuel qui doit être affiché comme tel. Pour N participants, le plan documenté comporte 7 + 4N champs : 8+4k pour l’empreinte, 9+4k pour le chemin, 10+4k pour la xpub et 11+4k pour l’identifiant de clé, avec k commençant à zéro. Pour N=2, l’étape 15 est l’identifiant de la deuxième clé et peut être comparée en premier.

Mise en pratique

1. Avec des données synthétiques, comparez d’abord un identifiant étiqueté étape 15, puis le réseau et le seuil.
2. Introduisez un écart d’un caractère. Vérifiez la mention « Pas de correspondance » et commencez une autre paire sans conserver ce résultat.
3. Comparez « 2 / 3 » et expliquez pourquoi le texte seul ne permet pas toujours de savoir s’il désigne le seuil ou la position de l’utilisateur.

À vous de l’expliquer

Indiquez quel champ vous avez vérifié, comment vous en avez déterminé le contexte et ce qui reste à approuver. Des correspondances partielles ne valent pas approbation globale.

Question fréquente

Faut-il scanner tous les codes QR pour poursuivre l’apprentissage ? Non. La comparaison est libre. Les vérifications et autorisations obligatoires du signataire gardent leur propre parcours.

Point de pause

Fermez le comparateur. Selon la conception examinée, quitter l’outil ou le placer en arrière-plan doit effacer les valeurs.

Mirror compare deux codes QR de l’étape 15 et affiche « Correspondance ». Qu’est-ce que cela atteste ?

1. L’égalité littérale des deux valeurs, dans le contexte identifié ou indiqué.
2. L’approbation de toute la politique.
3. L’authenticité de la provenance des deux codes QR.

> **Afficher la réponse: L’égalité littérale des deux valeurs, dans le contexte identifié ou indiqué.**
> La comparaison ne remplace ni l’authentification, ni l’examen global, ni la réponse de l’appareil.

Coordonner les signatures et diffuser une transaction multisignature

Objectif

Amener une proposition jusqu’au seuil de signatures sans perdre de vue l’intention ni le contrôle.

Comprendre

Une opération multisignature précise les entrées, destinataires, montants, taux de frais, modalités de remplacement et notes de coordination. Le créateur peut demander les signatures des participants compatibles. Avant d’autoriser sur son appareil, chacun vérifie lui-même le réseau, la politique, les entrées, toutes les sorties et les frais.

Si le seuil n’est pas atteint, une signature partielle ne déplace pas à elle seule les fonds. Une fois le seuil atteint, le coordinateur peut combiner les signatures et finaliser selon le parcours prévu. Les rapports des autres participants ou du coordinateur sont des informations de coordination distinctes d’une vérification locale menée par vous. L’application doit distinguer ces provenances.

L’implémentation propose la nouvelle tentative, la réception et l’accusé de signature, le refus et le transfert de coordination. Un transfert ne change ni les clés ni le seuil sur la chaîne. Une réponse enregistrée doit être reliée à la requête et au profil effectif utilisés. Ne choisissez pas une autre politique au seul motif qu’elle ressemble ou apparaît en tête du catalogue.

Si quelqu’un change les destinataires ou des conditions importantes, vérifiez une nouvelle proposition et obtenez les signatures correspondantes. Ne « réparez » pas une PSBT à la main en supprimant des données de sécurité pour la faire tenir sur le support NFC. Les micrologiciels exigent un profil et des validations compatibles, avec des limites d’entrées, de sorties et de taille.

Avant de diffuser, vérifiez que l’opération correspond à l’accord et qu’aucune version n’a déjà été diffusée. Suivez ensuite les confirmations par la source choisie. Un refus dans votre application ne révoque pas automatiquement les signatures conservées par d’autres et n’empêche pas toute action encore possible avec le seuil restant.

Mise en pratique

1. Jouez un scénario 2 sur 3 avec trois rôles fictifs : l’un signe, un autre refuse et le troisième demande une précision.
2. Changez l’adresse du paiement de test et expliquez pourquoi un ancien accord verbal ne peut pas être réutilisé.
3. Simulez l’échec de l’accusé de réception après enregistrement de la signature. Reprenez le même travail sans dupliquer le paiement ni changer le profil.

À vous de l’expliquer

Indiquez qui coordonne, qui signe, qui finalise et quelle preuve existe pour chaque étape.

Question fréquente

Deux OK dans la messagerie valent-ils deux signatures ? Non. Le seuil exige des autorisations cryptographiques valides selon la politique et ne se satisfait pas de messages.

Point de pause

Notez l’état, les signatures attendues et le prochain responsable sans contenu privé.

Une opération 2 sur 3 a une signature valide et deux messages indiquant « d’accord ». Le seuil est-il atteint ?

1. Oui, car il y a trois participants.
2. Non. Il manque une autre signature cryptographique valide.
3. Oui, si le coordinateur l’annonce.

> **Afficher la réponse: Non. Il manque une autre signature cryptographique valide.**
> Un accord donné dans une discussion et une signature valide sont des preuves distinctes.

Récupérer et modifier un portefeuille multisignature

Objectif

Récupérer la politique et prévoir la perte ou le remplacement de participants.

Comprendre

La récupération exige deux catégories d'éléments : les données qui reconstruisent la politique et des capacités privées suffisantes pour dépenser. Une copie de politique munie de xpub peut révéler l'historique sans contenir de graines. Le chiffrement protège le fichier mais impose de conserver le mot de passe. L'extension .cuvexms ne prouve pas à elle seule le chiffrement : vérifiez le format et l'export concrets.

Dans Desk 9.21, la récupération demande la clé publique étendue du participant avec l'empreinte et le chemin BIP48 exportés depuis son appareil. Le parcours compatible permet sa lecture par webcam ou Mirror. Ne la remplacez pas par une adresse de réception et n'envoyez pas la graine à l'assistance.

En cas de perte d'une clé dans une politique 2 sur 3, les deux autres peuvent conserver la capacité de dépense. L'ancienne politique reste en vigueur. Pour retirer effectivement un participant et établir d'autres clés, on crée généralement une nouvelle politique et l'on transfère les fonds avec les autorisations requises. Changer un alias ou supprimer un portefeuille dans Desk ne modifie pas les UTXO existants.

Les sauvegardes doivent permettre de reconstruire les deux branches et d'en découvrir l'historique. Conservez les indices, les demandes émises et le contexte nécessaire pour éviter la réutilisation d'adresses ou l'interprétation d'un portefeuille comme vide après une analyse incomplète. Restaurer et reprendre une opération en attente doit respecter le profil conservé lors de sa création.

Mise en pratique

1. Exportez et restaurez une politique de laboratoire au moyen de la fonction documentée. Vérifiez le réseau et une adresse connue.
2. Simulez la perte d'un participant et préparez un plan de rotation sans déplacer de fonds réels.
3. Simulez des pertes laissant moins de clés que le seuil requis. Reconnaissez que ni l'assistance ni l'IA ne peuvent fabriquer les signatures manquantes.

À vous de l’expliquer

Récupérez le scénario de test et distinguez la restauration d’informations d’un changement de contrôle des fonds.

Question fréquente

Supprimer le portefeuille multisignature dans Desk le désactive-t-il pour tous ? Non. Le parcours supprime son état local. D’autres personnes ou copies peuvent conserver une capacité compatible avec la politique.

Point de pause

Gardez la copie testée et le plan privé. Notez uniquement le résultat dans le cours.

Vous souhaitez retirer une personne d’une politique qui contrôle déjà des fonds. Suffit-il d’effacer son nom dans Desk ?

1. Oui.
2. Oui, si la discussion est également supprimée.
3. Non. Il faut prévoir une nouvelle politique et, le cas échéant, un transfert autorisé des fonds.

> **Afficher la réponse: Non. Il faut prévoir une nouvelle politique et, le cas échéant, un transfert autorisé des fonds.**
> Modifier des données locales ne change pas les scripts des UTXO existants.

Mettre à jour le micrologiciel sans improviser

Objectif

Préparer une mise à jour compatible et vérifier son résultat sur l’appareil.

Comprendre

Une mise à jour modifie un logiciel auquel vous faites confiance. Vérifiez modèle, révision matérielle, version, provenance et mécanisme d’authentification du fabricant. Un téléchargement complet ou une empreinte identique à celle d’une page ne remplace pas la vérification de la signature et de la compatibilité. N’installez jamais une application de micrologiciel non signée destinée à l’ingénierie comme s’il s’agissait d’une distribution client.

Selon le parcours documenté, Original se met à jour par Bluetooth et BIT par USB-C. Mirror offre des parcours compatibles de préparation et de transport. Le fonctionnement d’une combinaison précise de PC, téléphone et appareil ne peut pas être promis avant son acceptation physique. L’ancien incident de mise à jour d’Original sous Windows exige un diagnostic spécifique. Prétendre au succès à 99 % ne le résout pas.

Avant de commencer, vérifiez que les sauvegardes sont récupérables, que l’alimentation est stable et qu’aucune autre opération n’est en cours. Préparez le fichier officiel ou une copie déjà vérifiée selon l’application. Pendant l’envoi, distinguez transfert, validation, installation, redémarrage et vérification de la version. La barre de progression n’est pas une preuve finale.

À la fin, vérifiez la version visible sur l’appareil, puis consignez date et résultat. Le catalogue de compatibilité de Desk ne mesure pas le micrologiciel à distance : firmwareAttestation reste à false. Sélectionner un profil Final ne prouve pas quels octets sont réellement installés. En cas d’échec, suivez la récupération documentée et gardez l’étape et l’erreur, sans débrancher au hasard à un moment critique.

Mise en pratique

1. Passez en revue la liste de préparation sans lancer de mise à jour réelle pendant l’exercice.
2. Ordonnez les états et expliquez la différence entre « transféré » et « installé ».
3. Rédigez un rapport fictif d’échec à 99 % avec le modèle, la version, le système, l’étape et le message final.

À vous de l’expliquer

Identifiez le fichier adapté, son transport et le critère final de réussite.

Question fréquente

Faut-il mettre à jour le micrologiciel seulement pour faire disparaître une erreur de Desk ? Identifiez d’abord son origine. Une incompatibilité du catalogue peut exiger de corriger Desk tout en gardant le micrologiciel validé.

Point de pause

Une mise à jour réelle ne se suspend qu’à un stade expressément sûr de la procédure. La fin d’un appel ne constitue pas ce critère.

Que vérifie à lui seul le catalogue explicite de Desk ?

1. Les références de compatibilité prises en charge, sans mesure à distance du micrologiciel installé.
2. Une attestation physique de tous les appareils connectés.
3. L’absence de vulnérabilités.

> **Afficher la réponse: Les références de compatibilité prises en charge, sans mesure à distance du micrologiciel installé.**
> Compatibilité, signature, mesure et acceptation physique constituent des preuves distinctes.

Perte, panne et récupération d’urgence

Objectif

Choisir une récupération proportionnée à l’incident et préserver les éléments de preuve utiles.

Comprendre

Commencez par déterminer ce qui a été perdu ou exposé : ordinateur, appareil, carte, fichier, mot de passe, graine, phrase secrète ou politique. « Je ne peux plus accéder » ne signifie pas nécessairement « on m’a volé ». Si vous soupçonnez une compromission, cessez de saisir des secrets sur l’appareil suspect.

La perte de l’appareil peut se résoudre avec des supports et des moyens de récupération compatibles. La perte de l’ordinateur peut nécessiter la restauration du stockage de Desk et la reconstruction de la lecture seule. Si tous les moyens de déverrouillage ont disparu ou s’il reste moins de clés que le seuil requis, aucune solution technique n’existe nécessairement. Aucune IA ne peut garantir de retrouver des clés inexistantes.

Desk comprend une récupération locale pour les formats pris en charge et permet d’exporter les données nécessaires. Déchiffrer sur PC peut exposer le secret au système d’exploitation ou à un logiciel malveillant. C’est une décision exceptionnelle. Utilisez un environnement préparé, des composants compatibles et un plan de transfert vers de nouvelles clés si le secret a pu être compromis. Cette opération n’équivaut pas à l’isolation habituelle de Cuvex.

Si une graine a fuité, changer le mot de passe de Desk ne la révoque pas. Évaluez un transfert autorisé vers un nouveau portefeuille et protégez-le depuis un appareil fiable. Évitez de publier des détails qui aideraient l’attaquant et de payer des services qui promettent une récupération contre une autre graine ou une avance frauduleuse.

Mise en pratique

1. Traitez quatre scénarios fictifs : PC perdu, carte cassée avec copie valide, mot de passe oublié et graine exposée.
2. Pour chacun, identifiez les données nécessaires, le risque de l’intervention et le critère de récupération.
3. Entraînez-vous exclusivement avec des données pédagogiques. Ne transmettez aucun fichier d’urgence réel au tuteur.

À vous de l’expliquer

Choisissez entre restaurer, reconfigurer la lecture seule, migrer le contrôle ou faire appel à un spécialiste sans promettre de solution impossible.

Question fréquente

Changer le mot de passe chiffre-t-il à nouveau tous les secrets que quelqu’un a déjà vus ? Non. Une copie en clair ou une graine déjà connue reste connue.

Point de pause

Notez la catégorie de l’incident et la prochaine action sûre. Interrompez la voix avant de travailler avec des secrets.

Votre graine a été publiée et vous changez le mot de passe du PC. L’attaquant a-t-il perdu sa capacité de dépense ?

1. Oui.
2. Non. La graine contrôle toujours les mêmes clés et des mesures de protection des fonds sont nécessaires.
3. Oui, si vous changez aussi le fond d’écran de la messagerie.

> **Afficher la réponse: Non. La graine contrôle toujours les mêmes clés et des mesures de protection des fonds sont nécessaires.**
> Une protection locale ne révoque pas une clé Bitcoin exposée.

M10

Hameçonnage, assistance et fraudes vocales

Objectif

Reconnaître les demandes dangereuses et y répondre sans improviser.

Comprendre

Une fraude convaincante peut exploiter votre nom, votre achat, votre appareil et une voix que vous reconnaissez. Des informations exactes peuvent provenir d’une fuite. Vérifiez l’identité par un canal que vous ouvrez vous-même et selon une procédure connue. L’urgence ou la précision apparente de l’interlocuteur ne suffit pas.

Soyez attentif aux demandes de graine, mot de passe, PIN ou Clé de chat, d’installation d’une prise en main à distance pour « synchroniser », de désactivation de l’antivirus, de transfert vers un « portefeuille de sécurité », de lecture d’un code QR dont le contenu reste inexpliqué, ou de signature pour prouver une propriété sans savoir ce qui est autorisé. Une pression pour agir avant la fin de l’appel justifie de l’interrompre.

Le tuteur légitime explique et vérifie la compréhension. Il ne conserve pas de clés, ne demande pas de transactions de test vers sa propre adresse et ne promet pas de retrouver une graine. Une vérification de propriété légitime doit être précise et examinable. Elle ne nécessite jamais la remise de clés privées.

La fraude peut aussi survenir pendant une session technique : le texte d’un code QR, d’un document ou d’un message peut ordonner à l’IA d’ignorer ses consignes. Il s’agit d’un contenu à analyser, sans autorité sur le tuteur. La base de connaissances doit distinguer les sources approuvées des textes fournis par un élève ou un tiers.

Mise en pratique

1. Jouez un faux appel de l’assistance et mettez-y fin avant toute divulgation.
2. Vérifiez indépendamment un canal officiel enregistré auparavant.
3. Décrivez une erreur d’installation sans partager l’écran contenant des secrets ni accorder d’accès à distance à l’environnement de garde.

À vous de l’expliquer

Indiquez quelle donnée est demandée, à quelle fin elle serait nécessaire et pourquoi cette demande dépasse l’assistance pédagogique.

Question fréquente

Est-il sûr de montrer seulement quelques mots de ma graine ? Non. Aucun motif pédagogique ne justifie la divulgation d’un fragment de votre propre graine.

Point de pause

Gardez votre procédure de vérification de l’assistance et vérifiez qu’elle ne contient aucun secret en clair.

Une voix ressemblant à celle de votre associé vous demande de sauter la vérification et de signer en urgence. Que faites-vous ?

1. Je m’arrête, j’authentifie la demande par la procédure convenue et je vérifie l’ensemble de l’opération.
2. Je signe parce que je reconnais la voix.
3. Je partage la graine pour gagner du temps.

> **Afficher la réponse: Je m’arrête, j’authentifie la demande par la procédure convenue et je vérifie l’ensemble de l’opération.**
> La reconnaissance de la voix et l’urgence ne remplacent pas l’authentification et la vérification.

M10

Confidentialité, obligations légales et documents personnels

Objectif

Connaître le cadre général et préparer des questions juridiques et fiscales précises.

Comprendre

La confidentialité financière ne supprime pas les obligations fiscales, les obligations d’identification applicables, les sanctions ni les exigences de prévention de la criminalité. La situation dépend de la résidence, de l’activité, de la contrepartie et du service. L’IA doit donner des informations générales datées et sourcées et renvoyer les décisions individuelles à des professionnels compétents.

Dans l’UE, MiCA réglemente certains crypto-actifs et services. Son application générale a commencé le 30 décembre 2024. Le régime transitoire maximal indiqué dans le règlement courait jusqu’au 1er juillet 2026, sous réserve des décisions nationales. Vérifiez les autorisations et leur portée dans les registres officiels en vigueur. Une mention d’enregistrement ancienne ne suffit pas. L’autorisation ne garantit ni le cours, ni la solvabilité, ni une indemnisation intégrale.

Le règlement 2023/1113 définit les informations accompagnant les transferts lorsque des prestataires assujettis interviennent. Pour les transferts de plus de 1 000 euros avec des adresses auto-hébergées, il prévoit des mesures visant à évaluer la propriété ou le contrôle. Ce seuil ne crée pas de dispense générale d’identification en dessous de ce montant. Les transferts de personne à personne sans prestataire sont exclus du champ de ce règlement, mais d’autres obligations demeurent.

Conservez, en les protégeant contre les accès inutiles, des justificatifs suffisants des achats, ventes, frais et origines des fonds selon votre situation. Il n’est pas nécessaire de publier tout l’historique pour tenir des registres privés. Le cours n’enseigne ni à fractionner des opérations pour contourner des contrôles, ni à falsifier des informations, ni à dissimuler des revenus.

En cas d’enregistrement ou de transcription de la voix et de progression identifiable, le service doit définir la finalité, la base juridique, la conservation, les accès, les sous-traitants et les droits applicables. Les dispositions commerciales de confidentialité doivent être validées avant la vente, sans improvisation pendant un appel.

Mise en pratique

1. Rédigez pour un conseiller un cas fictif avec résidence, activité et opérations, sans clés.
2. Identifiez où vérifier l’autorisation du prestataire et la date de l’information.
3. Concevez un registre privé des mouvements et une politique minimale de données de l’élève.

À vous de l’expliquer

Distinguez une règle de droit, une politique de plateforme d’échange et une capacité technique de Bitcoin.

Question fréquente

Toute garde en propre est-elle interdite dans l’UE ? Les textes cités ne permettent pas cette conclusion. Évitez les titres absolus et vérifiez la disposition précise et son champ d’application.

Point de pause

Gardez les questions pour votre conseiller sans déposer de documents personnels auprès du tuteur.

Le seuil de 1 000 euros cité pour certaines vérifications de contrôle d’adresse supprime-t-il toute obligation en dessous de ce montant ?

1. Oui.
2. Seulement si vous fractionnez l’opération.
3. Non. Il ne s’agit pas d’une dispense générale d’identification ou d’autres obligations.

> **Afficher la réponse: Non. Il ne s’agit pas d’une dispense générale d’identification ou d’autres obligations.**
> La règle s’interprète selon la mesure concernée et son champ d’application. Le seuil n’est pas une dispense universelle.

Succession, continuité et exercice annuel

Objectif

Créer un plan permettant aux personnes autorisées d’agir sans tout exposer prématurément.

Comprendre

La succession combine légitimité juridique, localisation des matériaux et capacité technique. Une personne peut avoir le droit d’hériter sans savoir reconstruire un portefeuille. Une autre peut détenir une clé sans avoir le droit de l’utiliser. Le plan doit résoudre ces deux dimensions avec les conseils appropriés.

Séparez les instructions communicables de l’accès aux secrets. L’inventaire décrit ce qui existe, qui contacter et quelles vérifications faire, sans regrouper clés et mots de passe dans un document largement accessible. N’inscrivez pas de graine dans un testament ou un dossier qui pourrait circuler hors de votre contrôle.

En multisignature, déterminez qui conserve la politique et les copies, quel seuil reste accessible après une perte et ce qui arrive si un participant essentiel décède. Un dépositaire unique possédant suffisamment de composants peut devenir un point d’abus. À l’inverse, une distribution trop complexe peut rendre les avoirs irrécupérables.

Intégrez la récupération des mots de passe du cryptogramme et de la phrase secrète éventuelle, les données de dérivation, la compatibilité des appareils et la procédure à suivre si le fabricant cesse son activité. Ne supposez pas qu’un fichier propriétaire ou une empreinte biométrique seront utilisables sans préparation. Vérifiez l’interopérabilité avec des données d’essai et des formats documentés.

Révisez le plan après un changement familial, d’adresse, de politique, de logiciel ou de participants. Réalisez périodiquement un exercice. Il doit établir qu’une personne de confiance comprend les instructions sans dévoiler votre patrimoine ni déplacer inutilement de fonds.

Mise en pratique

1. Complétez un modèle privé avec responsables, composants, accès autorisés et remplaçants.
2. Remettez les instructions de laboratoire à une autre personne sans commentaire oral et observez où elle se bloque.

3. Corrigez les ambiguïtés et fixez une date de révision. Le cours ne crée pas automatiquement de rappels.

À vous de l’expliquer

Expliquez ce qui se passe en votre absence et ce dont chaque rôle a besoin à chaque étape.

Question fréquente

Un portefeuille 2 sur 3 remplace-t-il un plan de succession ? Non. C’est un outil technique. Les héritiers ont toujours besoin de contexte, de matériaux, de coordination et de légitimité.

Point de pause

Gardez le plan hors du cours et inscrivez seulement « exercice de succession vérifié ».

Quel critère permet d’évaluer utilement un plan de succession ?

1. Une personne autorisée peut réaliser un exercice documenté sans improviser ni recevoir de secrets prématurément.
2. Le plan comporte beaucoup de pages.
3. Il dépend uniquement de la mémorisation d’un mot de passe.

> **Afficher la réponse: Une personne autorisée peut réaliser un exercice documenté sans improviser ni recevoir de secrets prématurément.**
> La capacité de récupération et le contrôle d’accès doivent être vérifiés en pratique.

Cours, épargne et analyse fondamentale

Objectif

Analyser des arguments d’investissement sans les confondre avec les propriétés techniques vérifiables.

Comprendre

Le cours résulte d’échanges sur des marchés particuliers et peut varier d’une plateforme à l’autre. Liquidité, devise de cotation, profondeur du marché, horaires des prestataires bancaires et demande influencent ce que vous pouvez réellement exécuter. Un prix affiché ne constitue pas une offre garantie pour le volume de votre ordre.

L’analyse fondamentale étudie notamment l’adoption, la demande, la concurrence, la sécurité économique, la réglementation et l’offre. Un calendrier d’émission connu ne détermine pas à lui seul le prix futur. Les appréciations de l’utilité monétaire ou de la « valeur intrinsèque » reposent sur des hypothèses. L’IA ne dispose pas d’un chiffre objectif qui constituerait une certitude universelle.

Une stratégie d’achats périodiques répartit les dates d’entrée, sans garantir de bénéfice ni éviter les pertes prolongées. L’épargne de long terme nécessite aussi des liquidités pour les obligations, une tolérance à la volatilité et un plan de garde. Le cours ne prescrit pas de proportion de votre patrimoine et ne décide pas à votre place.

Posez séparément trois questions : est-ce que je comprends l’actif ? Puis-je le protéger et le récupérer ? Puis-je assumer son risque économique ? Maîtriser les clés ne répond pas automatiquement à la troisième. La formation ne transforme pas une projection de cours ou un graphique historique en conseil personnalisé.

Mise en pratique

1. Formulez une thèse d’investissement fictive avec ses hypothèses et les faits qui l’invalideraient.
2. Simulez une baisse de 50 % accompagnée de besoins de liquidités simultanés, sans saisir vos avoirs réels.
3. Repérez les éléments vérifiables dans l’argument et ceux qui relèvent d’anticipations.

À vous de l’expliquer

Discutez d’investissement sans promettre de rendement ni confondre conviction et preuve.

Question fréquente

La rareté garantit-elle une hausse du prix ? Non. La demande et d’autres conditions restent décisives pour le prix de marché.

Point de pause

Conservez les hypothèses du laboratoire, sans instruction automatique d’achat.

Que garantit un achat périodique ?

1. Un bénéfice à long terme.
2. Aucun rendement. Les achats sont répartis dans le temps selon une règle choisie.
3. Une protection contre la perte de clés.

> **Afficher la réponse: Aucun rendement. Les achats sont répartis dans le temps selon une règle choisie.**
> Répartir les achats ne supprime pas les risques économiques ou opérationnels.

Choisir où acquérir des bitcoins

Objectif

Évaluer un prestataire selon son autorisation, son coût, ses retraits, sa confidentialité et son risque de garde.

Comprendre

Comparez des critères vérifiables : entité juridique et juridiction, services autorisés, réseau de retrait, frais, écart de prix, limites, assistance, authentification et traitement des données. Un nom commercial ou un parrainage ne prouve pas l’autorisation pour le service considéré.

Le coût total peut inclure dépôt, conversion, spread, négociation, retrait et frais bancaires. Une opération « sans commission » peut comporter un écart de prix supérieur. Vérifiez les montants nets et la devise de référence. Si votre objectif est la garde en propre, intégrez le retrait au budget.

Tant que votre solde est détenu par le prestataire, vous en dépendez. Une preuve des réserves n’établit pas à elle seule l’ensemble des passifs, la propriété des fonds ou la solvabilité future. Vérifiez les restrictions et effectuez un petit retrait que vous pouvez vous permettre avant de dépendre d’un parcours nouveau.

L’identification commerciale peut associer votre identité à un retrait. Protéger ensuite ces données n’efface pas ce que le prestataire connaît. Ne falsifiez pas de renseignements et n’utilisez pas le cours pour contourner des obligations. L’achat d’un code de formation crée aussi une trace commerciale distincte de votre portefeuille.

Mise en pratique

1. Dressez un tableau fictif de deux prestataires avec coût total, réseau, retrait minimal, autorisation et données exigées.
2. Calculez le montant net d’une opération d’apprentissage en tenant compte de tous les frais indiqués.
3. Concevez un retrait d’essai vers une adresse vérifiée auparavant, sans l’exécuter depuis ce site.

À vous de l’expliquer

Justifiez un choix adapté à votre cas et reconnaissez quelles informations sont périmées ou non vérifiées.

Question fréquente

Le cours recommande-t-il une plateforme comme la meilleure pour tous ? Non. Les autorisations, tarifs, pays desservis et conditions évoluent. La comparaison dépend d’une date et d’un usage.

Point de pause

Conservez le tableau sans identifiants secrets ni documents d’identité.

Quelle comparaison est plus utile que le seul examen des frais de négociation ?

1. Le coût total jusqu’à la réception des BTC sur le réseau et à l’adresse souhaités.
2. Le nombre d’abonnés du prestataire.
3. La couleur de son application.

> **Afficher la réponse: Le coût total jusqu’à la réception des BTC sur le réseau et à l’adresse souhaités.**
> Le coût final inclut des éléments qui peuvent être absents des frais annoncés.

Comptes, ordres et coûts d’exécution

Objectif

Comprendre les types d’ordres et protéger le compte sans transformer le cours en terminal de négociation.

Comprendre

Un ordre au marché privilégie l’exécution disponible, avec un risque de glissement du prix. Un ordre à cours limité fixe un maximum à l’achat ou un minimum à la vente, mais il peut ne pas être exécuté ou ne l’être qu’en partie. Un ordre stop déclenche une autre action selon les règles du prestataire, sans garantir à lui seul le prix final.

Le carnet d’ordres affiche les offres disponibles sans promettre le maintien de tous les volumes. En cas de baisse ou de faible liquidité, le résultat peut différer de la dernière cotation. Un ordre stop-market risque une exécution à un prix moins favorable, tandis qu’un stop-limit peut ne pas être exécuté.

Protégez l’accès au moyen d’un mot de passe unique, d’une authentification résistante au hameçonnage si elle est proposée, d’un examen des sessions et de contrôles de retrait adaptés. Conservez séparément le moyen de récupération du second facteur. Une clé API d’automatisation peut disposer d’autorisations plus dangereuses que ne l’exige la lecture des données. Ne la saisissez ni dans le tuteur ni sur le site du cours.

Avant de retirer, vérifiez l’actif, le réseau Bitcoin, l’adresse de votre portefeuille et les montants nets. Une plateforme peut utiliser les mêmes symboles pour des produits différents. Conservez les justificatifs d’achat, d’exécution, de frais et de retrait adaptés à votre cas. Un retrait vers votre portefeuille ne constitue pas un nouvel achat.

Mise en pratique

1. Simulez un carnet fictif avec 1 unité à 100 et une autre à 102. Expliquez pourquoi acheter les deux au marché ne garantit pas un prix moyen de 100.
2. Concevez un ordre à cours limité et décrivez un scénario où il ne sera pas entièrement exécuté.
3. Examinez les autorisations d’une API fictive et retirez la permission de retrait si seule la consultation est nécessaire.

À vous de l’expliquer

Indiquez pour chaque ordre sa priorité, le prix recherché et le risque de non-exécution.

Question fréquente

Un stop-loss limite-t-il toujours la perte au chiffre exact ? Non. Les écarts de cotation, la liquidité, le glissement et les règles du prestataire peuvent l’en empêcher.

Point de pause

Gardez le résultat de l’exercice sans ordres réels ni clés API.

Quel risque subsiste pour un ordre d’achat à cours limité à 100 ?

1. Il peut ne jamais être exécuté ou ne l’être qu’en partie.
2. Il doit être exécuté à n’importe quel prix.
3. Il crée automatiquement une sauvegarde.

> **Afficher la réponse: Il peut ne jamais être exécuté ou ne l’être qu’en partie.**
> La maîtrise du prix a pour contrepartie un risque de non-exécution.

Bougies, indicateurs et biais de l’analyse technique

Objectif

Lire les graphiques comme des données historiques et évaluer une stratégie sans confondre motifs et prédiction.

Comprendre

Une bougie résume le cours d’ouverture, le plus haut, le plus bas et le cours de clôture d’une période. Le volume dépend de la source. Changer de plateforme, de devise, de fuseau horaire ou de période peut modifier ce que vous voyez. Une bougie ne révèle pas l’ordre de tous les mouvements à l’intérieur de son intervalle.

Une moyenne mobile lisse les cours passés. Un indicateur de momentum transforme les données observées selon une formule. Aucun des deux ne connaît l’avenir. Deux indicateurs issus de la même série peuvent apporter des informations très corrélées malgré des noms et des couleurs différents.

Avant de consulter les résultats, définissez l’entrée, la sortie, les critères d’invalidation, les coûts, la taille et les données. Évitez de ne sélectionner que les exemples gagnants, d’ajuster les paramètres jusqu’à obtenir le résultat voulu ou d’utiliser des données futures dans une décision passée. Distinguez les données d’entraînement de la validation sur une période ultérieure.

Un test rétrospectif doit intégrer le spread, les frais, le glissement, la disponibilité des données et la possibilité réelle d’exécution. Rendement brut, taux de réussite, perte maximale et distribution des pertes répondent à des questions distinctes. Un système qui gagne souvent peut perdre de l’argent si ses échecs coûtent cher. Aucun signal d’achat ou de vente ne doit être enseigné comme une certitude.

Mise en pratique

1. Lisez une bougie fictive et expliquez quelles informations chronologiques lui manquent.
2. Écrivez une règle avant d’évaluer dix résultats synthétiques, en intégrant les frais et un critère d’échec.
3. Comparez 9 gains de 1 à une perte de 15 : le résultat brut est de -6 malgré un taux de réussite de 90 %.

À vous de l’expliquer

Examinez de manière critique un résultat attrayant en considérant la sélection, les coûts et le risque sans devoir réaliser d’opérations.

Question fréquente

Combiner de nombreux indicateurs garantit-il un meilleur signal ? Non. Cela peut accroître le surajustement et la complexité sans apporter d’information indépendante.

Point de pause

Gardez la règle et les résultats du laboratoire, sans passer d’ordre au marché.

Neuf opérations gagnent chacune 1 et une en perd 15. Quel est le résultat avant frais ?

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

> **Afficher la réponse: -6.**
> Neuf unités gagnées moins quinze perdues donnent une perte de six.

Marge, contrats à terme et automatisation

Objectif

Reconnaître l’exposition, le risque de liquidation et les défaillances d’automatisation avant d’envisager des produits complexes.

Comprendre

L’effet de levier augmente l’exposition par rapport au capital apporté. Dans un exemple simplifié, 100 de marge pour une exposition de 1 000 signifie qu’un mouvement défavorable de 5 % du sous-jacent représente une perte de 50 avant frais, soit la moitié de la marge initiale. Les règles réelles de marge de maintien, de liquidation, de collatéral et de frais peuvent aggraver le résultat et se déclencher plus tôt que prévu.

Les contrats à terme et perpétuels peuvent comporter une échéance, un règlement par différence, des taux de financement et des prix de référence différents du dernier échange. Ils ne sont pas équivalents au retrait de bitcoins natifs vers Cuvex. Protéger une graine ne protège pas une position contre la liquidation ou la défaillance d’une contrepartie.

Un robot automatise des règles, y compris leurs erreurs. Il lui faut des limites de position, des autorisations minimales, des ordres idempotents, un rapprochement des opérations, un contrôle des pertes, un arrêt d’urgence et une supervision. Répéter une requête après expiration du délai peut doubler l’exposition si le résultat précédent est inconnu.

L’IA peut expliquer des notions et repérer des incohérences dans un cas fictif. Elle ne doit pas recevoir de clés API, lancer des opérations de marché ou promettre une stratégie rentable. Pour l’objectif principal du cours, comprendre les risques permet de décider de ne pas utiliser les produits que l’on ne comprend pas.

Mise en pratique

1. Résolvez l’exemple de marge et d’exposition sans supposer que le seuil de liquidation correspond exactement à 10 %.
2. Simulez une API qui exécute un ordre mais perd la réponse. Expliquez pourquoi il faut effectuer un rapprochement avant de réessayer.
3. Concevez un bouton d’arrêt qui empêche de nouveaux ordres et vérifie les ordres ouverts, sans connexion à un courtier.

À vous de l’expliquer

Décrivez un risque qui subsiste malgré un stop, un autre malgré un robot et un autre malgré la garde en propre de fonds extérieurs.

Question fréquente

L’automatisation élimine-t-elle les émotions et garantit-elle donc les résultats ? Non. Elle peut réduire une intervention impulsive tout en multipliant les erreurs de conception ou d’exécution.

Point de pause

Marquez cet approfondissement comme compris sans activer de produits complexes.

Avec une exposition de 1 000 et une marge de 100, une perte de 5 % sur l’exposition représente, avant frais :

1. Une perte de 5.
2. Une perte de 50, soit 50 % de la marge.
3. Aucune perte si un robot est utilisé.

> **Afficher la réponse: Une perte de 50, soit 50 % de la marge.**
> L’effet de levier et les frais font que le résultat rapporté à la marge diffère de la variation de l’actif.

M12

Lightning et les autres couches

Objectif

Comprendre les paiements par canaux et reconnaître les fonctions absentes du parcours Cuvex examiné.

Comprendre

Lightning utilise des canaux et des mécanismes de mise à jour pour payer sans enregistrer chaque échange individuel sur la chaîne de base. L’ouverture ou la fermeture de canaux et certains scénarios de récupération peuvent cependant exiger des transactions sur la chaîne. La disponibilité, la liquidité entrante et sortante et la surveillance dépendent de la conception du portefeuille et des services utilisés.

Une demande de paiement Lightning, ou invoice, peut inclure un montant, une description et une échéance. Selon le contexte, l’unité est le satoshi ou le millisatoshi. Ce dernier n’implique pas de sorties inférieures au satoshi sur la chaîne de base. Il faut une prise en charge compatible et une route disponible pour payer la demande. Un code QR ne garantit pas qu’une application quelconque puisse la régler.

Les services avec et sans garde reposent sur des modèles très différents. La rapidité habituelle ne démontre pas l’absence de risques. Lightning ne doit pas non plus être présenté comme entièrement anonyme. Les observateurs, les routes, les contreparties et les métadonnées restent pertinents.

La messagerie de Cuvex peut coordonner des demandes de sats payées sur la chaîne depuis le compte WOW. Cette édition n’attribue à Desk ni nœud Lightning, ni gestion de canaux, ni signature de demandes Lightning. Lorsqu’une demande propose plusieurs modalités, vérifiez celle que vous comprenez et celle que l’application exécutera.

Mise en pratique

1. Classez les exemples pédagogiques suivants : adresse sur la chaîne, URI bitcoin: et demande de paiement Lightning.
2. Comparez paiement sur la chaîne et paiement par canal en matière de confirmation, de liquidité, de garde et de récupération.
3. Expliquez pourquoi une demande expirée doit être réexaminée avec le destinataire et ne doit pas être réinterprétée comme une adresse.

À vous de l’expliquer

Refusez une modalité incompatible sans exposer de clés ni attribuer à tort une panne à Cuvex.

Question fréquente

Tous les paiements en sats passent-ils par Lightning ? Non. Les satoshis expriment une valeur. La modalité dépend du protocole employé.

Point de pause

Notez la modalité de l’exercice sans conserver de demande réelle.

À quoi reconnaît-on qu’une demande se paie sur Lightning ?

1. Elle emploie le mot « sats ».
2. Elle arrive dans la messagerie.
3. Son format et son mode de paiement sont compatibles. L’unité ou le canal du message ne suffit pas.

> **Afficher la réponse: Son format et son mode de paiement sont compatibles. L’unité ou le canal du message ne suffit pas.**
> L’unité de compte et le réseau de paiement sont deux éléments distincts.

Taproot, MuSig2 et l’avenir post-quantique

Objectif

Distinguer les normes, les propositions et les capacités effectivement mises en œuvre.

Comprendre

Taproot permet des conditions de dépense par chemin de clé ou de script. Les signatures Schnorr et l’agrégation peuvent améliorer certaines constructions, mais le résultat en matière de confidentialité dépend de la configuration et de la façon de dépenser. Une adresse bc1p ne prouve pas l’absence d’autres participants et ne révèle pas toutes les conditions cachées.

Avec MuSig2, plusieurs signataires peuvent agréger leurs clés et interagir pour produire une signature Schnorr compatible. Le schéma de base est N sur N. Un seuil arbitraire M sur N nécessite une autre construction ou un protocole supplémentaire. La gestion des nonces et des sessions est cruciale. Un échange informel de messages ne suffit pas à la mettre en œuvre.

PSBT v2 réorganise des informations par rapport à v0. Il ne s’agit pas d’une mise à niveau automatique d’un fichier contenant une transaction en version 2. Pour le profil multisignature, les micrologiciels Final de cette édition conservent PSBT v0, P2WSH/sortedmulti et SIGHASH_ALL. Les capacités futures nécessitent une spécification et une validation qui leur soient propres.

En 2024, le NIST a publié ses premières normes post-quantiques définitives. Cela ne modifie pas en soi les signatures de Bitcoin. Employer un algorithme post-quantique pour authentifier un micrologiciel protégerait cette couche sans transformer automatiquement les signatures ECDSA ou Schnorr d’un UTXO en signatures post-quantiques. Le tuteur ne peut pas non plus annoncer avec certitude la date d’une future attaque.

Mise en pratique

1. Classez cinq affirmations comme norme, mise en œuvre vérifiée, proposition ou publicité.
2. Expliquez pourquoi « accepte un destinataire Taproot » ne prouve pas « signe une entrée Taproot ».
3. Dessinez des couches distinctes pour la signature du micrologiciel, le chiffrement des secrets, la messagerie et la signature des dépenses Bitcoin.

À vous de l’expliquer

Demandez une preuve propre à une couche et évitez de transposer des garanties d’un protocole à un autre.

Question fréquente

Dois-je déplacer mes fonds à cause d’un titre sur l’informatique quantique ? Une décision réelle exige des données techniques actuelles, une prise en charge vérifiable, une évaluation des risques et un plan de migration sûr. Le cours ne prescrit pas de mouvements de fonds sur la foi d’un titre.

Point de pause

Notez vos questions techniques sans créer de plan de dépense automatique.

Si elle était mise en œuvre et validée, une signature post-quantique dans le chargeur de démarrage modifierait-elle les conditions de signature d’un UTXO existant ?

1. Non. Il s’agit de couches distinctes.
2. Oui. Elle fait passer tout le réseau à un autre algorithme.
3. Elle rend les sauvegardes inutiles.

> **Afficher la réponse: Non. Il s’agit de couches distinctes.**
> Authentifier une mise à jour ne réécrit pas les conditions de dépense de Bitcoin.

Interopérabilité et indépendance vis-à-vis du fabricant

Objectif

Prévoir la continuité en cas de changement de logiciel, d’appareil ou de prestataire.

Comprendre

Une liste de sigles ne suffit pas à vérifier l’interopérabilité. Il faut préserver le réseau, le script, la dérivation, les clés, la politique, le format des transactions et le sens des signatures. Deux applications peuvent comprendre BIP174 sans accepter les mêmes champs, tailles ou types d’entrées.

Pour sortir de la dépendance à une interface, conservez des informations de récupération documentées et entraînez-vous avec des portefeuilles pédagogiques. Une phrase mnémonique standard peut permettre de dériver les clés, mais la récupération en multisignature exige la politique complète. Les étiquettes BIP329 ajoutent un contexte sensible pour la vie privée. L’historique de messagerie a une autre portée.

Ne transformez pas un test de compatibilité en exposition d’une graine réelle. Vérifiez d’abord l’export des descripteurs publics et la récupération en lecture seule. Si une urgence impose la reconstruction des clés, utilisez un environnement prévu à cet effet et envisagez ensuite une migration. Un portefeuille incompatible qui affiche zéro ne démontre pas à lui seul la perte des fonds.

Conservez des copies vérifiables de la documentation, de la version du cours et des outils nécessaires. La signature des applications, l’expiration des certificats et l’évolution des systèmes peuvent affecter l’installation. Un code source ouvert et disponible ne garantit pas que n’importe qui puisse le compiler des années plus tard sans avoir préservé les dépendances et les connaissances.

Mise en pratique

1. Concevez un test de sortie avec un compte vide : même réseau, même politique et même adresse de contrôle dans deux implémentations compatibles.
2. Indiquez quels composants sont normalisés et lesquels nécessitent un convertisseur ou la documentation d’un format Cuvex.
3. Définissez le résultat qui établit la compatibilité et ce qui reste à vérifier avec du matériel ou une signature réelle.

À vous de l’expliquer

Décrivez une voie de récupération qui ne dépende pas du maintien du même service par une entreprise.

Question fréquente

Le code ouvert rend-il le fabricant sans importance ? Non. La distribution, la maintenance, les composants physiques et l’expérience opérationnelle comptent toujours. Le code ouvert permet l’examen et une continuité possible, sans garantie automatique.

Point de pause

Gardez les résultats de laboratoire, les versions et les limites observées.

Quelle preuve d’interopérabilité est la plus solide ?

1. Les deux applications affichent « Bitcoin ».
2. Reconstruire et vérifier en laboratoire la même politique et la même adresse avec des versions identifiées.
3. Les icônes se ressemblent.

> **Afficher la réponse: Reconstruire et vérifier en laboratoire la même politique et la même adresse avec des versions identifiées.**
> Le test doit préserver les conditions pertinentes et produire un résultat vérifiable.

Laboratoire technique avec regtest

Objectif

Comprendre un laboratoire reproductible sans confondre essais synthétiques et usage physique.

Comprendre

Regtest permet de créer une chaîne locale contrôlée, de générer des blocs et d'essayer des transactions sans valeur économique. Utilisez des répertoires et des identifiants distincts et n'importez pas de données réelles. Les résultats ne prouvent pas à eux seuls la compatibilité USB, NFC, Bluetooth ou caméra d'un appareil physique.

Un laboratoire complet enregistre versions, configuration du réseau, politique, entrées de test, PSBT, signatures, transaction finale et résultat d'acceptation. Il peut vérifier l'équilibre des montants, le rejet d'une signature modifiée et l'inclusion d'un paiement valide dans un bloc local. Testez aussi les échecs et pas seulement le parcours réussi.

La validation de Desk 9.21 fait état de tests avec Bitcoin Core 31 sur regtest, ainsi que de tests automatisés du moteur et d'une interface simulée. Cette édition les utilise comme preuves documentaires. Elle n'affirme pas les avoir répétés ni avoir opéré avec des appareils physiques. Vérifier un paquet ne prouve pas davantage son installation sur tous les systèmes.

Avant un cours technique, l'ingénieur doit fournir le laboratoire installé et une procédure compatible avec la version de l'élève. N'exposez pas RPC à Internet pour en donner le contrôle au tuteur. L'IA peut guider l'interprétation de résultats synthétiques, sans recevoir d'identifiants secrets ni d'autorisations d'administration.

Mise en pratique

1. Dans le laboratoire préparé, observez une transaction valide et une autre dont la signature a été modifiée. Notez l'acceptation ou le rejet.
2. Vérifiez un cas de monnaie rendue incorrecte et un autre de réseau incompatible.
3. Dans votre rapport, distinguez « test du moteur », « interface simulée » et « matériel physique ».

À vous de l'expliquer

Décrivez précisément ce qui a été testé et ce qui reste en attente, sans présenter une simulation comme une certification.

Question fréquente

Si regtest fonctionne, peut-on vendre le cours comme validé pour tous les appareils ? Non. Les parcours physiques, l’installation, l’accessibilité, la récupération et le service commercial nécessitent encore des essais.

Point de pause

Arrêtez et sauvegardez le laboratoire selon ses instructions. Ne gardez que les données synthétiques.

Un test du moteur sur regtest démontre-t-il la lecture NFC réelle sur un téléphone donné ?

1. Oui, car les deux utilisent Bitcoin.
2. Oui, si la PSBT est petite.
3. Non. Un essai physique distinct est nécessaire.

> **Afficher la réponse: Non. Un essai physique distinct est nécessaire.**
> Les environnements de validation n’ont pas la même portée.

Projet final et plan de continuité

Objectif

Démontrer votre autonomie depuis la préparation jusqu’à la récupération et à la protection de la vie privée.

Comprendre

L’objectif est de savoir expliquer l’intention, vérifier le résultat et interrompre une opération que vous ne comprenez pas. Mémoriser un menu ne suffit pas. L’évaluation combine notions, pratique guidée et cas autonome. Elle ne dépend jamais de la divulgation de graines, d’avoirs ou d’adresses personnelles à l’évaluateur.

Cas A. Configurez un environnement d’apprentissage, identifiez modèles et versions, protégez Desk, associez un cryptogramme pédagogique et reconstruisez un compte en lecture seule. Expliquez les sauvegardes nécessaires et les données que le prestataire peut observer.

Cas B. Concevez un paiement avec des UTXO fictifs de contextes différents, justifiez leur sélection, vérifiez destinataire, monnaie rendue et frais, puis décrivez le parcours de signature de votre modèle. Résolvez une interruption au retour de la réponse et une autre lors de la diffusion sans dupliquer le paiement. Si le matériel n’a pas fait l’objet d’une acceptation physique, indiquez que cette partie est simulée et que l’essai physique reste en attente.

Cas C. Concevez une politique 2 sur 3, jouez l’invitation et la vérification, comparez dans Mirror un champ de votre choix dans l’ordre qui vous convient et expliquez la portée du OK. Récupérez la politique d’apprentissage, simulez la perte d’un participant et préparez la continuité et la succession.

Le seuil de réussite proposé exige au moins 80 % à l’évaluation des connaissances et la réussite de tous les contrôles critiques : ne pas révéler de secrets, vérifier réseau et sorties, distinguer les étapes et préserver la récupération. Une erreur critique appelle un nouvel examen et de la pratique. De bonnes réponses sur les marchés ne la compensent pas. Tout certificat commercial éventuel doit préciser ce qui a été évalué et si l’évaluation relève d’une observation physique ou seulement d’une simulation.

Mise en pratique

1. Traitez les trois cas avec des données synthétiques et vos propres explications.
2. Passez l’évaluation finale en annexe et reprenez chaque réponse incorrecte.

3. Remettez uniquement une feuille de résultats sans secrets, en y précisant le périmètre des preuves et les éléments en attente.

À vous de l’expliquer

Arrêtez-vous de votre propre initiative quand les preuves manquent pour une opération et identifiez ce qu’il faut pour poursuivre.

Question fréquente

Lire toutes les pages signifie-t-il que je suis prêt à conserver n’importe quel montant ? Non. La capacité doit être démontrée et le risque évalué selon votre situation. La lecture et les exercices ne garantissent pas les résultats futurs.

Point de pause

Conservez votre plan de révision et les exercices en attente. Vous pouvez revenir au chapitre nécessaire sans refaire tout le cours.

Quelle exigence est essentielle pour conclure la formation pratique ?

1. Avoir ouvert toutes les pages.
2. Démontrer la récupération et la vérification des opérations dans un périmètre documenté, sans divulguer de secrets.
3. Prédire le cours du mois prochain.

> **Afficher la réponse: Démontrer la récupération et la vérification des opérations dans un périmètre documenté, sans divulguer de secrets.**
> L’apprentissage s’évalue par les capacités et les limites vérifiées, et non par la navigation ou les prédictions.

Manuel de l’élève

Manuel d’utilisation de Cuvex

Ce manuel accompagne les leçons. Chaque procédure décrit le parcours relevé dans les sources examinées, les vérifications à effectuer et le point d’arrêt. Il s’agit d’une édition candidate pour un pilote. Elle n’atteste pas d’essais physiques indépendants avec Original, BIT, les téléphones ou toutes les plateformes de bureau. Avant tout enseignement avec des fonds réels, l’équipe doit compléter la matrice d’acceptation et corriger les libellés ou écrans qui diffèrent.

Références : Original 1.2.2 Final, BIT 1.2.3 Final, Desk 1.0.0-beta.9.21 et Mirror 1.0.0-beta.12.12. Sélectionner un profil dans Desk déclare une compatibilité sans mesurer à distance le micrologiciel. Les captures de Mirror incluses proviennent de l’émulateur Android du paquet 12.12. Les photographies de produits fournies par l’entreprise ne prouvent pas la version affichée sur un appareil actuel.

P01 | Vérifier la provenance et la version | Cuvex | L16,L21 | C01,C02

Préparation : Munissez-vous des renseignements relatifs à l’achat et d’un canal officiel que vous pouvez vérifier de manière indépendante. Ne saisissez encore aucun secret.

1. Examinez l’emballage et les scellés. En présence de signes de manipulation, arrêtez la mise en service et conservez des éléments de preuve non sensibles.
2. Suivez le parcours de vérification d’intégrité et des scellés dans l’application compatible avec votre livraison. N’y saisissez les codes qu’à cet endroit, jamais auprès du tuteur.
3. Identifiez le modèle, Original ou BIT, et la révision disponible. Vérifiez les versions visibles sur l’appareil et dans les applications.
4. Comparez-les à la matrice publiée par l’équipe. Ni un catalogue ni une empreinte ne remplacent l’authentification du micrologiciel ou l’acceptation physique.

Résultat : Le modèle et les versions sont identifiés, la provenance vérifiée sans exposition de secrets. Si les codes ne sont pas valides ou si l’interface diffère, ne forcez pas l’utilisation en suivant un ancien guide.

Pause : Arrêtez-vous avant de charger les données de garde. La traçabilité commerciale ne garantit pas à elle seule l’absence de manipulation sophistiquée.

P02 | Mettre à jour Original par Bluetooth | Original | L46 | C01,C02,C03

Préparation : Prévoyez des sauvegardes récupérables, une alimentation stable, un paquet officiel compatible et un parcours validé pour votre système. Ce cours n’atteste pas du fonctionnement physique complet sur chaque plateforme.

1. Dans la rubrique appareils ou micrologiciels de l’application, sélectionnez Original et le téléchargement officiel ou le fichier local authentique correspondant.
2. Placez l’appareil en mode de mise à jour depuis son menu, puis connectez-vous par le parcours de l’application. Restez à proximité et évitez les sessions concurrentes.
3. Saisissez dans le champ indiqué le code affiché sur Original. Ne le confondez pas avec le mot de passe du cryptogramme.
4. Suivez le transfert, la validation, l’installation et le redémarrage. Le pourcentage affiché ne prouve pas l’installation.
5. Après le redémarrage, vérifiez la version finale sur Original et enregistrez-la dans l’application si ce champ existe.

Résultat : La version a été vérifiée sur l’écran après redémarrage et la fin du parcours est confirmée. En cas d’échec avant le PIN, pendant le transfert des paquets ou à la fin, notez l’étape et le code. N’improvisez pas une déconnexion ou un changement de logiciel pour « dépasser 99 % ».

P03 | Mettre à jour BIT par USB | BIT | L46 | C01,C02,C03

Préparation : Identifiez le support réel de BIT, l’alimentation et le paquet officiel compatible. Conservez des copies avant de changer de logiciel.

1. Sélectionnez BIT dans le parcours de mise à jour compatible de Desk ou de Mirror.
2. Connectez l’appareil avec le câble et l’adaptateur de données appropriés. Autorisez l’accès au volume ou au dossier à la demande de l’application.
3. Sélectionnez le micrologiciel authentique du modèle. Vérifiez la version et les informations de compatibilité avant de le transmettre.
4. Attendez les phases de transfert et de validation par l’appareil. Le volume peut disparaître puis être monté à nouveau conformément au protocole.
5. Après le redémarrage, vérifiez la version sur BIT et le résultat final dans l’application.

Résultat : L’installation a été vérifiée sur l’appareil même. Si le volume n’apparaît pas, contrôlez le mode de l’appareil, le câble de données, les autorisations, le montage et les éventuelles sessions concurrentes. Ne créez pas de dossier du même nom sur le PC en remplacement. La récupération après l’échec d’une mise à jour exige la procédure officielle de ce matériel.

P04 | Générer un portefeuille avec une pièce et des dés | Cuvex | L17 | C01

Préparation : Prévoyez un espace privé, des dés appropriés et une pièce, sans caméra et avec le microphone du tuteur coupé. Utilisez un portefeuille d'apprentissage.

1. Ouvrez la création de portefeuille et le parcours d'entropie du micrologiciel. Définissez à l'avance l'ordre des quatre dés.
2. Saisissez le résultat de la pièce et de chaque dé selon les indications de l'écran, sans modifier un résultat par préférence.
3. Le code source examiné calcule indice = pièce × 1 296 + (d1−1) × 216 + (d2−1) × 36 + (d3−1) × 6 + (d4−1). Seuls les indices de 0 à 2 047 sont acceptés.
4. En cas de rejet, relancez la pièce et tous les dés. L'avertissement conserve les mots précédents et demande un nouveau lancer de l'ensemble.
5. Menez à terme l'algorithme de l'appareil, y compris la validation finale, protégez la phrase mnémonique et vérifiez la récupération en privé.

Résultat : Le portefeuille a été généré par le parcours complet, sans choisir manuellement les mots. Si l'écran et le code source divergent, arrêtez l'utilisation. N'utilisez jamais comme données personnelles un exemple public de dés, de graine ou de clé.

P05 | Chiffrer un secret | Cuvex | L18,L19 | C01

Préparation : Choisissez le modèle, le format du contenu et sa protection. Une saisie sur PC ou téléphone expose le secret à la source, même si la destination est chiffrée.

1. Sélectionnez le chiffrement et le type compatible : BIP39, SLIP39, Monero ou texte. Ne mélangez pas les dictionnaires. Le clavier de texte en clair examiné accepte jusqu'à 500 caractères. Stocker un autre format ne signifie pas pouvoir signer sur son réseau.
2. Saisissez le contenu directement sur l'appareil pour conserver son isolation. Vérifiez l'ordre, les caractères et les champs auxiliaires sur son écran.
3. Choisissez la protection individuelle ou partagée prévue par le parcours et, le cas échéant, la biométrie sur BIT. Distinguez ce seuil de celui de Bitcoin.
4. Saisissez et confirmez les mots de passe en privé selon le validateur du micrologiciel. N'appliquez pas automatiquement les règles de Desk.
5. Sur Original, écrivez sur une carte vide compatible. Sur BIT, conservez les objets exportés par le parcours USB. Attendez la confirmation.
6. Lancez un essai de récupération pour vérifier le contenu et fermez l'affichage du secret à la fin.

Résultat : La récupération du cryptogramme a été vérifiée. En cas d'échec d'écriture ou de lecture, protégez l'original et suivez la procédure de nouvelle tentative à l'écran. N'effacez pas d'en-tête et ne forcez pas l'écrasement.

P06 | Déchiffrer sur l’appareil | Cuvex | L18 | C01,C02

Préparation : Assurez-vous de disposer d’un espace physiquement privé et de suffisamment de moyens de déverrouillage. Désactivez microphones et captures d’écran à proximité du secret.

1. Lancez le déchiffrement sur le bon modèle et fournissez le cryptogramme par NFC sur Original ou par le parcours USB de BIT.
2. Vérifiez l’alias et l’identification de l’objet avant de saisir les informations d’accès.
3. Fournissez les mots de passe nécessaires et les données biométriques si le format les exige. Ne multipliez pas automatiquement les tentatives après un échec : des contrôles d’accès et de blocage s’appliquent.
4. Vérifiez le contenu uniquement sur l’écran prévu. Un code QR contenant le secret est aussi sensible que le texte.
5. Fermez ou terminez le processus conformément aux indications de l’appareil. Rangez séparément support et moyens d’accès selon votre plan.

Résultat : Le contenu a été récupéré en privé et la session est terminée. Si le format n’est pas reconnu, si l’authentification échoue ou si le contenu est inattendu, ne tentez pas de le « corriger » avec une application inconnue. Décrivez à l’assistance la version, le format et l’erreur sans joindre le secret.

P07 | Préparer la récupération d’un cryptogramme biométrique | BIT | L19,L47 | C01,C02

Préparation : Utilisez un cryptogramme d’apprentissage et la documentation de son format. La simple possession d’une copie .bin ne garantit pas sa récupération.

1. Dans la fiche de Desk, repérez les éventuels composants biométriques et l’export de récupération disponible.
2. Conservez l’ensemble de fichiers associés par le parcours et une copie indépendante, avec des identifiants discrets.
3. Testez le déverrouillage normal sur BIT et documentez les mots de passe et conditions nécessaires.
4. Étudiez la voie exceptionnelle de récupération locale et les formats qu’elle prend en charge. Vérifiez la présence des éléments nécessaires avant d’en avoir besoin.
5. Avec des données sans fonds, simulez un appareil en panne ou une empreinte indisponible.

Résultat : Vous disposez d’un plan testé, avec ses limites, pour ce format précis. Cela ne signifie pas que toute condition biométrique peut être contournée ni qu’une empreinte remplace les copies. Si un secret est récupéré sur PC, évaluez l’exposition et la nécessité d’un transfert ultérieur du contrôle.

P08 | Créer et vérifier une copie de cryptogramme | Cuvex et Desk | L20 | C01,C02

Préparation : Identifiez la copie originale et une destination compatible qui ne contient aucune donnée à préserver.

1. Pour Original, utilisez le clonage de l’appareil ou la fonction compatible de Desk. Présentez la source et la destination dans l’ordre indiqué.
2. Gardez les cartes immobiles et respectez le refus d’un support contenant déjà un cryptogramme.
3. Pour BIT ou un fichier, exportez l’ensemble des composants prévus et préservez les noms ou les associations nécessaires.
4. Isolez l’original et testez la lecture et la récupération depuis la nouvelle copie.
5. Notez en privé la date, le format et le résultat. Rangez les copies dans des lieux exposés à des risques physiques indépendants.

Résultat : Une deuxième copie a été testée. Elle ne crée pas un autre portefeuille, ne révoque pas les mots de passe et ne protège pas une graine déjà divulguée. Si la destination échoue, conservez l’original sans essayer de le « réparer » pour le faire correspondre à la copie.

P09 | Créer et déverrouiller le stockage de Desk et changer son mot de passe | Desk | L21,L40 | C02

Préparation : Prévoyez un installateur vérifié, une architecture adaptée et un plan de sauvegarde du stockage.

1. Créez le stockage avec un mot de passe unique de 12 à 1 024 caractères et une confirmation identique.
2. Verrouillez puis rouvrez-le pour vérifier l’accès. Saisissez le mot de passe exclusivement dans Desk.
3. Dans Sécurité, puis Accès et verrouillage, vérifiez les réglages d’inactivité et de passage en arrière-plan. N’activez pas l’effacement facultatif pendant une démonstration.
4. Pour changer le mot de passe, fournissez l’actuel et confirmez le nouveau dans le parcours prévu.

5. Si vous utilisiez la biométrie du PC, configurez-la à nouveau suivant les indications. Faites une sauvegarde à jour en conservant le lien avec les anciennes copies.

Résultat : L’accès a été vérifié. Les anciennes copies conservent leurs mots de passe et chiffrements d’origine. La biométrie du PC et celle de BIT sont des mécanismes distincts. En cas d’échec, arrêtez les essais répétés et examinez la récupération sans demander au tuteur de conserver les informations d’accès.

P10 | Associer et examiner un cryptogramme dans Desk | Desk | L22 | C02

Préparation : Utilisez un cryptogramme de test de provenance connue et un moyen de transport disponible.

1. Ouvrez Cryptogrammes ou Cartes et choisissez l’association par NFC, USB ou copie compatible.
2. Sélectionnez la présentation et la source. Pour le NFC, utilisez Cuvex Mirror associé à l’ordinateur par Bluetooth. Vous pouvez aussi utiliser le volume d’un Cuvex BIT connecté en USB-C. Cuvex Desktop ne prend pas en charge les lecteurs NFC USB externes.
3. Consultez la fiche : alias, origine, taille, format et conditions d’accès interprétées. Il s’agit de métadonnées et non du contenu déchiffré.
4. Vérifiez si des comptes conservés sont en attente d’association et n’associez que le compte vérifié.
5. Si la couverture de sauvegarde est insuffisante, exportez une copie et testez sa récupération séparément.

Résultat : L’objet est organisé localement. La mention « associé » ne prouve ni l’authenticité de la graine ni le solde. Si un objet n’est pas reconnu, vérifiez format et version sans changer l’extension ni effacer de données pour forcer son acceptation.

P11 | Activer un compte WOW en lecture seule | Desk et Cuvex | L13,L22 | C01,C02

Préparation : Munissez-vous des données publiques issues du parcours de l’appareil et vérifiez en privé leur provenance.

1. Depuis le bon cryptogramme, ouvrez Activer WOW ou Ajouter un compte.
2. Importez le descripteur ou les données publiques acceptées au moyen d’un fichier, d’une webcam ou de Mirror, selon la fonction.
3. Vérifiez réseau, script, origine, empreinte, chemin et somme de contrôle le cas échéant. Ne saisissez ni graine ni xprv.
4. Nommez le compte et choisissez en connaissance de cause la source de consultation.

5. Vérifiez une adresse de contrôle et le périmètre de découverte avant d’interpréter le solde.

Résultat : Le portefeuille en lecture seule est associé. Si le solde affiché est nul, vérifiez réseau, phrase secrète d’origine, dérivation, compte, prestataire et analyse avant de conclure que les fonds ont disparu. Les réseaux acceptés par une interface générale ne le sont pas nécessairement par le profil multisignature. Respectez chaque contexte.

P12 | Configurer le nœud et la synchronisation | Desk | L25,L33 | C02

Préparation : Définissez vos exigences de confidentialité et, si vous utilisez Core, disposez d’un accès à un nœud protégé et synchronisé.

1. Dans Sécurité, puis Confidentialité et nœuds, choisissez le compte WOW et examinez son prestataire.
2. Choisissez explicitement un prestataire public compatible ou Core. Pour Core, saisissez le point de connexion, le portefeuille et les identifiants uniquement dans l’application.
3. Autorisez la consultation en comprenant quelles données reçoit chaque service. TLS ne masque pas la requête au prestataire.
4. Synchronisez et vérifiez la date, la tête de chaîne, la progression et l’état d’achèvement. Pour une nouvelle analyse, vérifiez l’ancienneté couverte et la continuité du travail.
5. En cas de code 429, respectez la pause. En cas d’échec, ne supposez pas qu’un autre nœud a pris le relais : le système ne change pas silencieusement de source.

Résultat : La source et l’état sont connus. N’exposez pas RPC à Internet, ne communiquez pas le mot de passe et ne limitez pas la découverte aux adresses dont le solde est positif. Un historique vide peut être un résultat partiel.

P13 | Générer et retrouver une demande de réception | Desk et Cuvex | L26 | C01,C02

Préparation : Vérifiez le compte, le réseau et la politique.

1. Ouvrez Recevoir et générez ou retrouvez la demande appropriée.
2. Ajoutez un observateur, un motif et un montant attendu uniquement si vous avez besoin de ces métadonnées locales.
3. Vérifiez l’adresse par le parcours compatible de l’appareil avant un encaissement important. Si l’acceptation physique manque, limitez l’exercice à la simulation.
4. Partagez exclusivement les données nécessaires par le canal authentifié du destinataire.
5. Vérifiez la réception, le montant et les confirmations auprès de votre source réseau.

Résultat : Le paiement est rapproché de la demande, au-delà de sa simple émission. En multisignature, les adresses déjà affichées sont conservées pour les paiements tardifs et ne sont pas réattribuées. Si la limite de nouvelles adresses sans historique est atteinte, retrouvez les demandes antérieures sans forcer les indices manuellement.

P14 | Étiquettes, gel et BIP329 | Desk | L27 | C02,B13

Préparation : Prévoyez un compte de laboratoire contenant des UTXO et un mot de passe pour l'export protégé.

1. Étiquetez une entrée selon son contexte sans données personnelles superflues.
2. Gelez ou dégelez délibérément et vérifiez le solde disponible pour la dépense. La restriction est locale.
3. Exportez les étiquettes avec la fonction protégée. Distinguez BIP329, le format, du chiffrement du fichier.
4. Importez-les dans une copie compatible. Vérifiez la correspondance des références, étiquettes et états de gel.
5. Conservez une sauvegarde à jour des métadonnées avec son mot de passe conformément à votre plan.

Résultat : Le contexte est préservé et la sélection comprise. Une importation ne doit pas dégeler automatiquement des sorties sans vérification. Ne communiquez pas au tuteur le fichier d'étiquettes, car il peut révéler les contreparties et leurs relations même sans clés de dépense.

P15 | Préparer un paiement et envoyer la totalité | Desk | L28 | C02

Préparation : Disposez d'une demande vérifiée et d'un compte contenant suffisamment d'entrées dépensables.

1. Ouvrez Payer depuis WOW, les UTXO ou la messagerie, puis confirmez le compte et le réseau.
2. Sélectionnez entrées, destinataires et montants. Examinez les contextes que vous allez relier.
3. Choisissez le taux de frais, puis vérifiez les frais absolus, la monnaie rendue et les avertissements. En présence de dust, étudiez les solutions sans accepter de frais cachés.
4. Pour envoyer la totalité, vérifiez le montant net après frais. Dans la messagerie, confirmez explicitement tout paiement partiel qui ne couvre pas la demande.
5. Préparez le brouillon et vérifiez toutes les données avant de l'exporter pour signature.

Résultat : L’intention est claire et la PSBT correspond à l’opération. Un formulaire général peut accepter plus d’entrées ou de destinataires que le matériel : appliquez les limites réelles de l’appareil de signature et du transport. Toute modification des sorties ou des conditions ouvre une nouvelle vérification.

P16 | Signer et retourner une PSBT avec Original | Original et Mirror | L29 | C01,C02,C03

Préparation : Prévoyez le bon brouillon, une carte de transport compatible, un cryptogramme compatible authentifié et un moyen de déverrouillage privé. Une ancienne copie d’authenticité non vérifiée peut nécessiter une récupération vérifiée puis la création d’une nouvelle copie avant la signature. Modifier son en-tête ne la corrige pas.

1. Exportez la requête par le parcours NFC compatible depuis Desk/Mirror.
2. Portez-la à Original. Fournissez le cryptogramme lorsque l’appareil le demande et déverrouillez-le sans dicter vos informations d’accès.
3. Vérifiez réseau, récapitulatif, sorties complètes, frais, monnaie rendue et avertissements obligatoires.
4. Pour une multisignature Final, décidez si vous souhaitez examiner les paramètres étendus. Ne donnez les trois confirmations finales que si tout concorde.
5. Attendez l’écriture puis la relecture de la réponse sur la carte.
6. Lisez la réponse avec Cuvex Mirror et validez-la dans l’opération correspondante de Desk.

Résultat : La signature a été reçue et reliée au brouillon, sans que cela constitue une diffusion. Si l’écriture échoue, conservez l’état et suivez le parcours de nouvelle tentative. N’utilisez jamais la carte de sauvegarde comme support de paiement que l’on peut écraser.

P17 | Signer, recevoir et accuser réception avec BIT | BIT et Desk | L29 | C01,C02

Préparation : Prévoyez le bon brouillon, un cryptogramme authentifié compatible et le volume réel de BIT sélectionné. Si une ancienne copie est refusée pour la signature, suivez la récupération et le renouvellement indiqués sans forcer le format.

1. Transmettez la requête par USB-C au moyen du service de Desk, puis suivez les indications de l’écran de l’appareil pour le cryptogramme.
2. Déverrouillez en privé et vérifiez le récapitulatif, toutes les sorties, les frais et les avertissements.
3. Pour une multisignature Final, examinez si vous le souhaitez les détails étendus. Autorisez l’opération par les confirmations finales obligatoires.
4. Dans Desk, choisissez Recevoir de BIT pour importer et valider la réponse correspondant à ce travail.

5. Vérifiez l’enregistrement et l’accusé de réception. Si l’accusé échoue après réception, réessayez pour la même opération, sans laisser le modèle en choisir une autre.

Résultat : La signature est vérifiée et l’état de l’échange est cohérent. En cas de déconnexion avant réception ou après enregistrement, conservez le profil de la requête. Ne sélectionnez pas un autre micrologiciel du catalogue pour faire correspondre une réponse en attente.

P18 | Finaliser, diffuser et suivre une opération | Desk | L30,L44 | C02

Préparation : Disposez de signatures vérifiées et, le cas échéant, d’un seuil atteint.

1. Vérifiez à nouveau l’intention, les entrées, les sorties, les frais et le réseau.
2. Finalisez avec la commande prévue et vérifiez qu’aucune signature ni condition ne manque.
3. Autorisez la diffusion et conservez le résultat local. Si la réponse du réseau se perd, vérifiez avant de réessayer.
4. Suivez le mempool et les confirmations auprès du prestataire choisi, avec la date de synchronisation.
5. Si vous envisagez RBF, vérifiez la nouvelle opération et obtenez les signatures requises. Ne supposez pas qu’une fonction CPFP est intégrée.

Résultat : L’état de la chaîne a été vérifié auprès de sa source. Annuler un brouillon ne révoque pas les signatures déjà exportées et ne réécrit pas les paiements confirmés. Un message ou une capture d’écran ne remplace pas le suivi.

P19 | Comparer librement deux codes QR de politique | Mirror | L43 | C03,C02

Préparation : Affichez le champ dans Desk et sur Cuvex. Pour l’exercice, utilisez uniquement les exemples synthétiques du cours.

1. Ouvrez Comparer les politiques et lisez en premier le côté de votre choix.
2. Choisissez la donnée que vous voulez vérifier. Vous pouvez commencer par l’étape 15 et sauter des champs vérifiés manuellement.
3. Lisez la valeur correspondante et vérifiez les deux textes complets. Si l’étape est ambiguë, utilisez Indiquer l’étape de Desk en gardant à l’esprit que le contexte est saisi manuellement.
4. Interprétez « Correspondance » ou « Pas de correspondance » uniquement pour cette paire de valeurs littérales. Les espaces, la casse et l’encodage comptent.
5. Commencez une autre paire dans l’ordre de votre choix. Quittez l’outil ou passez en arrière-plan pour terminer selon le comportement d’effacement examiné.

Résultat : Il s’agit d’une comparaison locale ponctuelle. Elle n’atteste ni la source, ni la session, ni l’approbation globale, ni l’activation. Élucidez toute différence auprès de ses sources sans normaliser le texte pour obtenir artificiellement un OK.

P20 | Activer, récupérer et transférer la messagerie | Desk et Cuvex | L36,L39 | C02

Préparation : Choisissez l’environnement DEV ou Production. Gardez l’alias et la Clé de chat sur l’appareil, jamais dans le cours.

1. Ouvrez l’activation ou la récupération de la messagerie dans le contexte du cryptogramme.
2. Choisissez un nouvel alias ou le transfert d’un alias existant, ainsi que le profil mobile compatible indiqué par l’application.
3. Saisissez ou lisez la Clé de chat exclusivement dans le parcours privé. N’employez ni graine, ni PIN, ni clé de WOW.
4. Vérifiez l’activation auprès du service. Si elle reste en attente, utilisez la commande de finalisation ou de vérification avant de conclure au succès.
5. Après un transfert, vérifiez la continuité avec les contacts. Évitez d’utiliser simultanément le même alias sur plusieurs appareils.

Résultat : L’identité est activée ou récupérée dans le bon environnement. Ni la Clé de chat ni la sauvegarde globale de Desk ne restaurent automatiquement l’historique et les anciennes sessions. Respectez les limites des éléments disponibles.

P21 | Vérifier l’identité d’un contact | Desk | L36,L48 | C02

Préparation : Prévoyez un canal indépendant convenu à l’avance avec la personne.

1. Ajoutez l’alias et consultez son identité publique dans l’application.
2. Comparez l’empreinte sur le canal authentifié, sans vous limiter à la discussion que vous venez de créer.
3. Si vous utilisez des questions de reconnaissance, évitez les informations publiques et les secrets réutilisés sur d’autres services.
4. Ne confirmez qu’après avoir résolu toutes les différences. En cas de changement d’identité, suspendez paiements et coordination jusqu’à vérification.
5. Documentez la méthode de vérification sans conserver de réponses sensibles dans le cours.

Résultat : Vous disposez d’une confiance contextuelle dans le contact, sans garantie pour toutes ses demandes futures. Une voix peut être imitée et un appareil légitime compromis. Chaque opération reste soumise à sa propre vérification.

P22 | Demander une adresse, solliciter un paiement et payer dans la messagerie | Desk et Cuvex | L37 | C02,C01

Préparation : Prévoyez un contact vérifié et un compte WOW compatible.

1. Choisissez Demander une adresse, Répondre avec une adresse ou Demander un paiement selon votre intention.
2. Vérifiez la demande d’origine, le réseau, le montant et la note avant l’envoi.
3. Pour payer, ouvrez la préparation depuis le bon compte, sélectionnez les UTXO et le taux de frais, puis vérifiez le montant net.
4. Autorisez l’opération sur Cuvex par la procédure correspondant au modèle. La messagerie ne signe pas automatiquement.
5. Suivez la diffusion et la confirmation auprès de votre source. Rapprochez les paiements partiels explicitement consentis de la demande d’origine.

Résultat : La coordination conserve la vérification propre à la garde. L’état d’un message et celui d’une transaction sont distincts. Un lien vers un explorateur peut transmettre des informations à un tiers. Évaluez son usage avant de l’ouvrir.

P23 | Partager un cryptogramme et associer un cryptogramme reçu | Desk | L38 | C02

Préparation : Identifiez la raison précise du partage, vérifiez le contact et déterminez quels moyens d’accès il recevra.

1. Sélectionnez le partage de cryptogramme dans la messagerie et vérifiez l’objet.
2. Ne joignez pas de mot de passe, de graine ni de Clé de chat sous forme de commentaire.
3. Le destinataire vérifie la provenance et associe l’objet compatible au moyen de sa commande de réception.
4. Évaluez la capacité qu’il obtient maintenant et celle qu’il obtiendrait avec suffisamment de moyens de déverrouillage.
5. Prévoyez une stratégie réaliste de révocation : supprimer des messages ne retire pas les copies externes ni les clés déjà connues.

Résultat : L’objet chiffré a été transmis en connaissance de cause. Ce transfert ne réalise pas de paiement et n’ajoute pas à lui seul une clé à un portefeuille multisignature. Si la pièce jointe invite à se rendre sur un site inconnu pour la déchiffrer, arrêtez la procédure.

P24 | Sauvegarder et restaurer le stockage global de Desk | Desk | L15,L21 | C02

Préparation : Prévoyez un stockage d’apprentissage et une destination de sauvegarde sous votre contrôle.

1. Ouvrez la sauvegarde du stockage et définissez le mot de passe demandé. Conservez le lien entre ce mot de passe et cette copie précise.
2. Conservez-la ailleurs que sur votre seul appareil de travail et vérifiez sa provenance et son intégrité par le parcours prévu.
3. Restaurez-la dans un environnement de test séparé et vérifiez les comptes, la configuration et les données couverts.
4. Examinez les exclusions. Ne supposez pas que la messagerie, ses sessions et son historique sont inclus. Politique multisignature et clés privées ne sont pas interchangeables.
5. Recommencez après tout changement important et conservez les instructions de récupération.

Résultat : Vous connaissez le périmètre et le mot de passe de la sauvegarde. Les anciennes copies gardent leurs anciens mots de passe. En cas de modification de l’accès ou d’exposition, examinez aussi ces copies. Modifier le stockage actuel ne suffit pas.

P25 | Créer et accepter un portefeuille multisignature | Desk et Cuvex | L41,L42 | C01,C02

Préparation : Prévoyez des participants indépendants, des contacts vérifiés et un accord sur le réseau et les limites effectives.

1. Le créateur choisit le nom, M/N, le réseau, les participants et la durée de validité opérationnelle.
2. Fournissez la bonne clé publique étendue avec son empreinte et son chemin BIP48 par le parcours compatible.
3. Chaque participant examine l’invitation, l’accepte ou la refuse et fournit ses données publiques. Il ne partage jamais sa graine.
4. Construisez la politique complète et préparez sa vérification sur chaque appareil.
5. Gardez des copies de la politique avant d’y transférer des fonds. Vérifiez l’adresse de contrôle et la capacité de récupération.

Résultat : La proposition est complète et vérifiable. Accepter l’invitation ne remplace pas la vérification sur l’appareil. Si Original participe, respectez sa limite de six clés et la taille disponible en NFC. BIT n’étend pas les capacités des autres participants.

P26 | Vérifier une politique et recevoir la confirmation | Desk et Cuvex | L43 | C01,C02,C03

Préparation : Prévoyez la même politique complète pour tous, le bon profil de micrologiciel et un appareil sans opérations concurrentes.

1. Lancez Vérifier les politiques dans le contexte compatible. Original exige la sélection explicite du profil installé. BIT négocie ses capacités selon sa spécification.
2. Selon le modèle, transmettez la requête par NFC/Mirror ou USB-C.
3. Vérifiez les champs de la politique sur l’appareil. Mirror peut servir de comparateur facultatif pour des paires de votre choix, sans ordre imposé.
4. Terminez la confirmation sur l’appareil et retournez sa réponse par le moyen de transport correspondant.
5. Dans Desk, validez la réponse associée à la requête. Un OK visuel du comparateur ne remplace pas cette étape.

Résultat : La réponse se rapporte à l’examen effectué et sa portée se limite à cet examen. Le catalogue n’atteste pas le micrologiciel à distance, et l’appareil n’est pas présenté comme un stockage persistant des politiques. Face à FIRMWARE_CAPABILITY_REQUIRED, vérifiez d’abord la version de Desk et la combinaison modèle/build.

P27 | Demander et recevoir des signatures, puis transférer la coordination | Desk et Cuvex | L44 | C01,C02

Préparation : Prévoyez une politique vérifiée, une opération identifiée et des destinataires convenus.

1. Préparez entrées, sorties, frais et notes, puis demandez la signature des participants compatibles.
2. Chaque participant vérifie et signe sur son appareil par le parcours de transport de son modèle.
3. Recevez, validez et enregistrez chaque signature. Résolvez les accusés de réception en attente sans changer le profil conservé.
4. En cas de transfert de la coordination, le destinataire accepte le parcours et vérifie l’état. Ni M/N ni la propriété des clés ne changent.
5. Une fois le seuil atteint, vérifiez et finalisez avant de diffuser. Suivez la transaction sur le réseau.

Résultat : Chaque étape de coordination possède sa propre preuve. Un rapport de progression du coordinateur n’est pas une vérification locale effectuée par vous. Annuler ou refuser dans une application ne détruit pas nécessairement les signatures déjà conservées par des tiers.

P28 | Exporter, restaurer et supprimer localement un portefeuille multisignature | Desk | L45 | C02

Préparation : Prévoyez une politique connue et une sauvegarde chiffrée avec un mot de passe unique.

1. Exportez les données de récupération avec la commande de Desk. Le parcours actuel utilise un conteneur authentifié CVXMSBK1 pour cet export.
2. Conservez la copie et le mot de passe dans des conditions qui les exposent à des risques indépendants. Ne déduisez pas le chiffrement de l’extension des anciens fichiers.
3. Pour restaurer, fournissez la copie, le mot de passe et la clé publique du participant avec la bonne origine, au moyen de la webcam ou de Mirror le cas échéant.
4. Vérifiez politique, réseau, adresse et découverte avant toute opération.
5. Pour supprimer localement, lisez la portée de l’action et sa confirmation. Gardez une copie si vous souhaitez pouvoir restaurer. Une restauration ultérieure nécessite une action explicite.

Résultat : La politique est récupérable ou la suppression locale a été décidée en connaissance de cause. La suppression ne déplace pas les fonds, n’efface pas les clés des autres signataires et n’annule pas à elle seule les opérations conservées par d’autres personnes.

P29 | Effectuer une récupération exceptionnelle sur PC | Desk | L47 | C02

Préparation : Prévoyez des données dans un format pris en charge, un environnement propre préparé et une sauvegarde. Cette opération peut exposer un secret au PC. Utilisez des données d’apprentissage dans le cours.

1. Ouvrez la récupération locale dans le bon contexte et lisez les limitations du format et les avertissements.
2. Acceptez le risque en connaissance de cause et déconnectez le réseau comme l’exige la procédure. La fenêtre vérifie l’état de connexion avant d’autoriser la suite.
3. Saisissez exclusivement les informations nécessaires dans la fenêtre privée. Ne les dictez pas, ne les collez pas dans le cours et ne les partagez pas avec l’assistance.
4. N’activez l’affichage que dans un espace sans caméra ni assistant à l’écoute. Respectez le minuteur et la fermeture.
5. Terminez, examinez l’exposition possible et planifiez une migration vers de nouvelles clés si nécessaire.

Résultat : Il s’agit d’une récupération exceptionnelle. Elle ne garantit pas un effacement forensique et n’équivaut pas au travail sur du matériel isolé. En l’absence d’authentification, de format compatible ou de moyens d’accès, ne testez pas d’outils trouvés sur Internet avec votre copie réelle.

P30 | Vérifier les préférences, la biométrie et le verrouillage | Desk | L40 | C02

Préparation : Avant de modifier la sécurité, vérifiez que vous connaissez le mot de passe et que la sauvegarde a été testée.

1. Dans Accès et verrouillage, vérifiez le mot de passe, la biométrie disponible, l’inactivité et le verrouillage lors du passage en arrière-plan.
2. Comprenez le délai après les échecs et le maximum configuré avant de les modifier.
3. Laissez l’effacement facultatif désactivé tant que vous n’en comprenez pas les conditions, le seuil et la récupération. Ne le testez pas en production.
4. Dans Préférences, réglez la langue, le thème, la devise, la synchronisation toutes les 3 ou 5 minutes et les sons.
5. Si vous enregistrez les liens bitcoin:, vérifiez que l’ouverture d’une demande conserve les étapes de déverrouillage, de sélection et d’examen. Elle ne déclenche pas à elle seule le paiement.

Résultat : La configuration est comprise. La biométrie du système d’exploitation dépend de l’appareil et ne remplace ni le mot de passe ni la sauvegarde. Les préférences visuelles ne modifient pas la politique Bitcoin.

P31 | Supprimer des enregistrements en tenant compte de leur portée | Desk | L22,L45 | C02

Préparation : Identifiez l’objet à supprimer, qu’il s’agisse d’un cryptogramme local, d’un compte, de WOW, d’une discussion ou d’un portefeuille multisignature, et la copie que vous conserverez.

1. Lisez le nom de l’objet sélectionné et son avertissement. Confirmez l’alias exact ou la condition explicite lorsque l’application le demande.
2. Exportez et testez une sauvegarde si vous devez pouvoir retrouver cet état ultérieurement.
3. Supprimez uniquement l’objet prévu et vérifiez quelles associations le parcours conserve ou retire.
4. Vérifiez s’il reste des opérations ou des participants externes. Ne supposez pas que les messages, signatures ou fichiers disparaissent des autres appareils.
5. Documentez le changement dans votre inventaire privé sans déposer de données sensibles dans le cours.

Résultat : L’état local a été géré en connaissance de cause. Aucune de ces actions ne modifie à elle seule le script d’un UTXO financé, ne détruit une graine connue de tiers ou n’annule une transaction confirmée.

P32 | Diagnostiquer un problème sans exposer de secrets | Desk et Mirror | L23,L30,L48 | C02,C03

Préparation : Notez l’heure approximative, le système, l’architecture, la version et l’étape. Évitez de répéter une opération sensible sans connaître son état.

1. Déterminez si l’échec concerne la recherche, l’association, la lecture, l’écriture, la validation, la signature, le retour, le réseau ou l’affichage.
2. Copiez le code et le texte de l’erreur sans inclure de code QR ou de donnée privée. Utilisez les diagnostics de l’application si nécessaire.
3. Examinez le fichier avant de le partager. Ne joignez ni sauvegarde du stockage, ni cryptogramme, ni graine, ni Clé de chat, ni descripteur, ni identifiant RPC.
4. Pour un problème d’interface, relevez la taille de la fenêtre, le zoom et les commandes masquées dans une scène synthétique.
5. Transmettez par le canal officiel le résultat attendu et les étapes reproductibles. Le cours n’envoie pas automatiquement de message à l’assistance.

Résultat : Le rapport permet d’enquêter avec un minimum de données. En l’absence de preuve pour une étape, indiquez « en attente » et non « terminée ». L’assistance vocale n’a pas besoin d’accéder à distance à votre appareil de garde.

Glossaire de Bitcoin et de la garde en propre

Bitcoin

Réseau et ensemble de règles permettant de transférer de la valeur et d’en vérifier l’historique sans administrateur unique du registre.

BTC

Unité monétaire de Bitcoin. Un BTC vaut cent millions de satoshis.

Satoshi

Unité de la chaîne de base égale à un cent-millionième de BTC.

Blockchain

Historique de blocs reliés et vérifiés selon des règles. Ce terme ne décrit pas à lui seul toutes les propriétés d’un réseau.

Bloc

Ensemble de données comprenant des transactions et un en-tête vérifiable.

Nœud complet

Logiciel qui vérifie le respect des règles par les blocs et les transactions qu’il accepte.

Minage

Construction de blocs par preuve de travail conformément aux règles du réseau.

Preuve de travail

Mécanisme exigeant un travail de calcul vérifiable pour proposer un bloc.

Consensus

Accord des participants sur les règles et l’historique valide qu’ils acceptent.

Politique du mempool

Règles locales d’acceptation et de retransmission, qui ne coïncident pas nécessairement avec les règles de consensus.

Mempool

Ensemble local des transactions non confirmées conservées par un nœud.

Confirmation

Inclusion dans un bloc de la chaîne acceptée, puis profondeur de ce bloc dans la chaîne.

Réorganisation

Modification d’une partie de la chaîne acceptée susceptible de changer les confirmations.

UTXO

Sortie de transaction non dépensée, utilisable dans les conditions qu’elle prévoit.

Entrée

Référence à une sortie antérieure et données nécessaires pour autoriser sa dépense.

Sortie

Valeur et condition de dépense créées par une transaction.

Monnaie rendue

Sortie qui rend à l’utilisateur le contrôle d’une partie des entrées après le paiement et les frais.

Frais

Différence entre la valeur totale des entrées et celle des sorties d’une transaction.

vbyte

Unité de taille virtuelle servant à exprimer le coût relatif d’une transaction.

sat par vbyte

Taux de frais exprimé en satoshis par unité de taille virtuelle.

Dust

Sortie jugée petite au regard des politiques et du coût de sa dépense. Le seuil dépend du contexte et du script.

RBF

Remplacement d’une transaction non confirmée selon des politiques compatibles. L’annulation n’est pas garantie.

CPFP

Utilisation d’une transaction enfant pour accroître l’incitation à l’inclure avec sa transaction parente.

Hachage

Empreinte de données utile pour vérifier leur intégrité. À elle seule, elle ne chiffre pas les données et n’en identifie pas l’auteur.

Clé privée

Capacité cryptographique de produire des autorisations selon le schéma concerné.

Clé publique

Donnée permettant de vérifier des signatures et de construire certaines conditions sans exposer la clé privée.

Signature numérique

Preuve cryptographique d’autorisation d’un message déterminé. Elle n’en cache pas le contenu.

Chiffrement

Protection de la confidentialité au moyen d’une clé et d’un algorithme.

Chiffrement authentifié

Chiffrement qui, selon sa conception, permet aussi de détecter des modifications.

AES GCM

Famille de chiffrements authentifiés employée dans certains formats de l’écosystème. Ses propriétés dépendent de la mise en œuvre et de la gestion des clés.

Phrase mnémonique

Représentation sous forme de mots des données de génération et de vérification selon un format précis.

Graine

Donnée à partir de laquelle les clés sont dérivées. Dans l’usage courant, ce terme peut aussi désigner les mots de récupération, d’où l’importance du contexte.

Entropie

Imprévisibilité des données de génération. Choisir des mots faciles à retenir ne la garantit pas.

Somme de contrôle

Valeur permettant de détecter certaines erreurs. Elle n’authentifie pas l’auteur.

BIP39

Spécification des phrases mnémoniques et de la dérivation d’une graine avec une phrase secrète facultative.

Phrase secrète BIP39

Donnée supplémentaire de dérivation. Une autre phrase peut produire un autre portefeuille valide et apparemment vide.

BIP32

Spécification de la dérivation hiérarchique des clés.

Chemin de dérivation

Suite de branches permettant d’obtenir des clés à partir d’une racine.

Dérivation renforcée

Étape de dérivation généralement signalée par une apostrophe ou un h. Ses propriétés diffèrent de celles de la dérivation publique ordinaire.

xpub

Clé publique étendue comportant le contexte nécessaire à la dérivation. Elle est sensible pour la vie privée.

xprv

Clé privée étendue. Elle ne doit être ni partagée ni importée dans un cours.

Empreinte maîtresse

Identifiant court d’une racine, utile pour établir une association. Il ne constitue pas une preuve d’identité suffisante.

Descripteur

Expression décrivant la construction de scripts avec des clés et des chemins de dérivation. Elle peut être publique ou contenir des données privées.

Lecture seule

Portefeuille d’observation qui ne dispose pas des données privées suffisantes pour signer seul.

WOW

Nom donné aux comptes d’observation et à la gestion des portefeuilles dans l’écosystème Cuvex.

Portefeuille à chaud

Outil capable de signer dans un environnement connecté.

Garde en propre

Mode de garde dans lequel l’utilisateur conserve la capacité technique de dépenser, seul ou avec d’autres, selon sa politique.

Dépositaire

Entité qui contrôle la capacité de dépense pour le compte du client et applique ses conditions d’accès.

Cryptogramme Cuvex

Objet chiffré protégeant un secret. Il ne constitue en lui-même ni une transaction ni un solde.

Mot de passe de Desk

Protection de l’accès au stockage local. Il diffère de la graine et du mot de passe du cryptogramme.

Clé de chat

Secret de récupération d’une identité de messagerie. Son apparence peut laisser croire à tort qu’il s’agit d’une donnée publique.

PIN d’association

Code temporaire d’une session de connexion, distinct d’un mot de passe protégeant les avoirs.

Air gap

Séparation opérationnelle des environnements. Les données transportées entre eux doivent toujours être validées.

NFC

Technologie de communication à courte portée utilisée par les cartes et lecteurs compatibles.

USB Mass Storage

Interface d’échange de fichiers du modèle BIT, avec son propre protocole, ses validations et ses accusés de réception.

PSBT

Conteneur de données et de signatures servant à coordonner la construction et l’autorisation des transactions.

PSBT v0

Version du format définie par BIP174 et utilisée par le profil multisignature Final examiné.

PSBT v2

Version définie par BIP370. Le fait qu’une transaction soit en version 2 ne renseigne pas sur la version de sa PSBT.

SIGHASH ALL

Mode d’engagement de la signature employé dans le profil examiné. La validation de l’opération comprend la vérification des éléments couverts.

P2WPKH

Condition de dépense SegWit à clé unique, couramment associée aux comptes BIP84.

P2WSH

Condition SegWit qui engage un script. Le profil multisignature Final examiné l’utilise.

P2TR

Type de sortie Taproot. Le prendre en charge comme destination ne signifie pas que l’on puisse signer une dépense à partir de cette sortie.

sortedmulti

Construction multisignature qui ordonne les clés de façon déterministe pour générer des scripts.

Seuil M sur N

Nombre M d’autorisations requises parmi N participants selon une politique donnée.

MuSig2

Protocole d’agrégation de signatures Schnorr dont le schéma de base exige N signatures sur N, et non un seuil arbitraire.

Taproot

Ensemble de mécanismes de dépense et d’engagement de Bitcoin comportant des chemins par clé et par script.

Miniscript

Langage permettant de décrire et d’analyser certaines politiques de script. Le profil Final examiné ne le met pas en œuvre.

Regtest

Réseau de laboratoire local contrôlé par la personne qui le met en place, sans valeur économique.

Signet

Réseau de test présentant ses propres caractéristiques. Il n’est pas interchangeable par défaut avec regtest.

Mainnet

Réseau Bitcoin utilisé pour des opérations à valeur économique réelle.

Gap limit

Nombre d’adresses consécutives sans historique utilisé comme critère de découverte. Sa portée dépend du portefeuille.

Coin control

Sélection délibérée des UTXO à dépenser.

Consolidation

Regroupement de sorties pour réduire la fragmentation, avec des conséquences sur les coûts et la confidentialité.

Pseudonymat

Usage d’identifiants qui ne sont pas directement des noms d’état civil, sans garantie automatique d’anonymat.

Anonymat

Propriété, dépendante du contexte, de ne pas pouvoir être distingué par des observateurs définis. Une application ne peut pas le garantir par une simple étiquette.

Métadonnées

Informations sur les communications ou l’activité, notamment les horaires, les tailles et les relations, distinctes du contenu.

CoinJoin

Construction collaborative qui complique certaines déductions sans garantir un anonymat permanent.

Payjoin

Paiement collaboratif utilisant des entrées du payeur et du bénéficiaire selon un protocole compatible.

Tor

Réseau et outils de protection des connexions. Leur utilisation doit être configurée et vérifiée pour chaque application.

VPN

Canal qui transfère une partie de la confiance accordée à la connexion vers son opérateur. Il ne masque pas la chaîne.

Lightning

Système de paiement par canaux dont les conditions et les risques diffèrent de ceux d’une transaction sur la chaîne.

Invoice

Demande de paiement structurée dont il faut identifier le format et le mode de paiement.

RPC

Interface d’appel d’un service tel que Bitcoin Core. Elle doit être authentifiée et protégée.

TLS

Protection du transport contre certaines menaces. Le serveur destinataire voit toujours les requêtes.

SRTP

Protection de l’audio sur certains segments VoIP. Elle n’implique pas automatiquement que l’opérateur ne puisse pas accéder au contenu.

Idempotence

Propriété qui évite de produire deux fois un effet lorsqu’une requête identifiée est répétée.

Webhook

Événement transmis entre serveurs dont il faut vérifier l’authenticité ainsi que les éventuelles répétitions.

RAG

Recherche d’extraits de connaissances destinés à fonder une réponse sur le contexte et la version pertinents.

Reformulation par l’élève

Vérification de l’apprentissage en demandant à l’élève d’expliquer avec ses propres mots ce qu’il a compris.

Hameçonnage

Tromperie qui associe usurpation d’identité et contexte convaincant pour obtenir un accès ou provoquer une action.

Ingénierie sociale

Manipulation de décisions humaines qui peut s’appuyer sur des informations vraies et un sentiment d’urgence.

Notarisation

Contrôle de distribution d’Apple, distinct d’un audit du produit ou d’essais physiques de tous ses parcours.

Attestation

Preuve d’un état selon un mécanisme précis. Le catalogue de compatibilité de Desk ne constitue pas une mesure à distance.

MiCA

Cadre européen applicable à certains crypto-actifs et services. Il ne garantit ni rendement ni indemnisation intégrale.

Travel Rule

Obligations d’information relatives aux transferts entrant dans son champ d’application. La garde en propre ne permet pas de s’y soustraire.

Point de reprise

Repère permettant de reprendre l’apprentissage avec un minimum de données et sans information sur le portefeuille.

Vérifiez vos acquis

Entraînez-vous sans fonds réels. L’évaluation est en libre accès et ne nécessite aucun compte.

Qui autorise la dépense dans le cadre d’une utilisation habituelle de Cuvex ?

1. L’appareil, après vérification par l’utilisateur
2. Le tuteur vocal
3. Le serveur du cours

> **Afficher la réponse: L’appareil, après vérification par l’utilisateur**
> L’autorisation passe toujours par Cuvex.

À combien de satoshis correspondent 0,001 BTC ?

1. 1 000
2. 100 000
3. 1 000 000

> **Afficher la réponse: 100 000**
> Un BTC vaut 100 000 000 sat.

Les entrées totalisent 120 000 sat et les sorties 119 000 sat. À combien s’élèvent les frais ?

1. 1 000 sat
2. 119 000 sat
3. 1 sat/vB, sans autre information

> **Afficher la réponse: 1 000 sat**
> La différence entre les montants donne les frais absolus.

Une transaction signée qui n’a pas encore été diffusée est :

1. Confirmée
2. Irréversible du fait de sa signature
3. Autorisée mais pas nécessairement publiée

> **Afficher la réponse: Autorisée mais pas nécessairement publiée**
> La signature et la diffusion sont deux étapes distinctes.

Combien coûtent 200 vB à 6 sat/vB ?

1. 206 sat
2. 1 200 sat
3. 6 % de la somme envoyée

> **Afficher la réponse: 1 200 sat**
> Multipliez la taille virtuelle par le taux de frais.

Avant un retrait depuis une plateforme d’échange, que devez-vous vérifier ?

1. Uniquement les frais les plus bas
2. La compatibilité de l’actif, du réseau, de l’adresse et du montant net
3. La graine de la contrepartie

> **Afficher la réponse: La compatibilité de l’actif, du réseau, de l’adresse et du montant net**
> Certains réseaux affichent le symbole BTC sans être la chaîne Bitcoin.

Que fait une signature numérique à elle seule ?

1. Elle cache tout le message
2. Elle autorise un message vérifiable selon son schéma de signature
3. Elle efface les données publiées

> **Afficher la réponse: Elle autorise un message vérifiable selon son schéma de signature**
> La confidentialité nécessite un autre mécanisme.

Changer une phrase secrète BIP39 peut :

1. Produire un autre portefeuille valide et apparemment vide
2. Toujours être annulé par e-mail
3. Modifier le registre public des paiements précédents

> **Afficher la réponse: Produire un autre portefeuille valide et apparemment vide**
> La phrase secrète intervient dans la dérivation.

Comment devez-vous traiter la xpub d’un compte ?

1. Comme une donnée sans conséquence
2. Comme une donnée identique à la graine privée
3. Comme une information sensible pour la vie privée

> **Afficher la réponse: Comme une information sensible pour la vie privée**
> Elle peut permettre d’observer une plus grande partie de votre activité.

Pourquoi une seule graine peut-elle être insuffisante pour récupérer un portefeuille multisignature ?

1. Il manque la politique et les autorisations requises pour atteindre le seuil
2. Bitcoin ne permet aucune récupération
3. Il faut connaître la couleur d’origine de l’application

> **Afficher la réponse: Il manque la politique et les autorisations requises pour atteindre le seuil**
> Conserver la politique et disposer des moyens privés de signature sont deux exigences distinctes.

Si l’algorithme Final examiné rejette un lancer, que devez-vous faire ?

1. Relancer uniquement la pièce jusqu’à l’acceptation
2. Relancer la pièce et les quatre dés
3. Choisir un mot connu

> **Afficher la réponse: Relancer la pièce et les quatre dés**
> Ne relancer qu’une partie de l’ensemble peut biaiser la correspondance entre résultats et mots.

Que signifient deux mots de passe servant à accéder à une graine à signature unique ?

1. Deux clés sont obligatoires sur la chaîne
2. Il s’agit d’un portefeuille multisignature Taproot
3. Le seuil d’accès au secret est distinct du seuil de dépense sur Bitcoin

> **Afficher la réponse: Le seuil d’accès au secret est distinct du seuil de dépense sur Bitcoin**
> Le chiffrement ne modifie pas le script.

Quel élément faut-il prendre en compte pour évaluer une sauvegarde globale de Desk ?

1. Elle inclut nécessairement toute la messagerie
2. Son périmètre comporte des exclusions et l’inclusion de la messagerie ne va pas de soi
3. Elle met à jour toutes les anciennes copies

> **Afficher la réponse: Son périmètre comporte des exclusions et l’inclusion de la messagerie ne va pas de soi**
> Récupérer une identité et récupérer les messages sont deux choses distinctes.

Que permet un nœud personnel correctement configuré ?

1. Éliminer toutes les fuites d’information
2. Réduire la dépendance aux consultations de services tiers et vérifier soi-même les données
3. Récupérer les clés perdues

> **Afficher la réponse: Réduire la dépendance aux consultations de services tiers et vérifier soi-même les données**
> Il ne garantit ni l’anonymat ni la récupération des secrets.

Que se passe-t-il lorsque vous gelez un UTXO dans Desk ?

1. L’application applique une restriction locale
2. La condition de consensus change
3. Les autres copies de la graine sont révoquées

> **Afficher la réponse: L’application applique une restriction locale**
> Le gel local ne bloque pas la dépense partout.

Que faire en cas de perte de connexion au moment précis de la diffusion ?

1. Payer de nouveau immédiatement
2. Supprimer le portefeuille
3. Vérifier d’abord si le paiement a déjà été diffusé

> **Afficher la réponse: Vérifier d’abord si le paiement a déjà été diffusé**
> L’expiration du délai de réponse ne prouve pas que rien ne s’est passé.

Que peuvent entraîner la réutilisation d’adresses ou le regroupement d’UTXO provenant de contextes différents ?

1. Des liens plus faciles à observer
2. L’effacement de l’historique
3. La garantie de l’anonymat

> **Afficher la réponse: Des liens plus faciles à observer**
> La confidentialité dépend du contexte et des usages ultérieurs.

Ouvrir Tor Browser configure-t-il automatiquement Desk ?

1. Oui
2. Non
3. Seulement si le thème sombre est activé

> **Afficher la réponse: Non**
> Le chemin réseau de chaque application doit être vérifié.

Qu’est-ce qu’une Clé de chat qui ressemble à une xpub ?

1. Une donnée que l’on peut publier
2. Une adresse de réception
3. Un secret qui contrôle une identité

> **Afficher la réponse: Un secret qui contrôle une identité**
> L’usage de la clé détermine son caractère sensible.

Que signifie un message de discussion marqué « payé » ?

1. Il remplace les confirmations
2. Le paiement nécessite encore une vérification indépendante sur le réseau
3. Il change le réseau de la demande

> **Afficher la réponse: Le paiement nécessite encore une vérification indépendante sur le réseau**
> Le statut du message est distinct de celui du paiement.

Que prévoit le profil multisignature Final examiné ?

1. MuSig2 et PSBT v2
2. P2WSH sortedmulti BIP48 PSBT v0
3. N’importe quel script Bitcoin

> **Afficher la réponse: P2WSH sortedmulti BIP48 PSBT v0**
> Une fonctionnalité souhaitée ou une appellation commerciale ne suffit pas à établir sa prise en charge.

Par où peut-on commencer une comparaison dans Mirror 12.12 ?

1. Uniquement par l’étape 1
2. Par toute donnée choisie, y compris celle de l’étape 15
3. Uniquement par la dernière étape, après toutes les autres

> **Afficher la réponse: Par toute donnée choisie, y compris celle de l’étape 15**
> Les paires se comparent indépendamment et dans l’ordre de votre choix.

Qu’atteste la mention « Correspondance » dans Mirror ?

1. Une approbation globale
2. L’authenticité de la provenance des deux codes QR
3. L’égalité littérale des deux valeurs

> **Afficher la réponse: L’égalité littérale des deux valeurs**
> Le reste de la vérification et la réponse sont encore en attente.

Si une graine a été exposée, quel effet a le changement du mot de passe de Desk ?

1. Il révoque l’accès de l’attaquant
2. Il ne révoque pas les clés dérivées de cette graine
3. Il efface toutes les copies

> **Afficher la réponse: Il ne révoque pas les clés dérivées de cette graine**
> Il faut étudier un transfert sécurisé du contrôle.

Que doit indiquer le bilan final de la formation pratique ?

1. Ce qui relevait de la lecture, de la simulation et des essais physiques, ainsi que ce qui reste à faire
2. Seulement les heures vendues
3. Une promesse de garde invulnérable

> **Afficher la réponse: Ce qui relevait de la lecture, de la simulation et des essais physiques, ainsi que ce qui reste à faire**
> Chaque type de preuve a sa propre portée.