Ledger Nano X

Wallet physique compatible Bluetooth

Mode d’emploi

LEDGER

Sommaire

Versions

Version	Date	Commentaires
1.0	07-03-2019	Premier numéro à paraître.
1.1	25-03-2019	Ajout de la section « Vérifier l'intégrité du matériel »

Premiers pas

Vérifier l’authenticité de l’appareil

Les produits Ledger combinent sécurité matérielle et logicielle, afin de protéger vos clés privées contre un large éventail d’attaques potentielles. Utilisez ce guide pour vous assurer que votre appareil Ledger Nano X est authentique, et pas frauduleux ou contrefait.
Quelques vérifications simples vous permettent de vérifier que votre appareil est un produit Ledger authentique :

- ✓ Origine du produit Ledger
- ✓ Contenu du coffret
- ✓ État de la feuille de récupération
- ✓ État initial de l’appareil Ledger

Les utilisateurs avancés souhaitant vérifier l’intégrité du matériel peuvent se rendre directement à la fin de cet article.

Acheter auprès d’un revendeur officiel de Ledger

Achetez votre appareil directement auprès de Ledger ou via notre réseau de distributeurs / revendeurs agréés pour vous assurer de recevoir un produit Ledger authentique. Nos canaux de vente officiels sont les suivants :

- Notre site officiel de e-commerce : Ledger.com
- Boutiques Amazon officielles : USA, Canada, Royaume-Uni, Allemagne, France, Espagne, Italie, Japon.

Les appareils Ledger achetés auprès d’autres fournisseurs ne doivent pas nécessairement faire l’objet de suspicions. Toutefois, nous vous recommandons vivement d’effectuer méticuleusement les contrôles de sécurité ci-dessous pour vous assurer que votre appareil Ledger est authentique.

Vérifier le contenu du coffret

La boîte d’un wallet physique Ledger doit contenir :

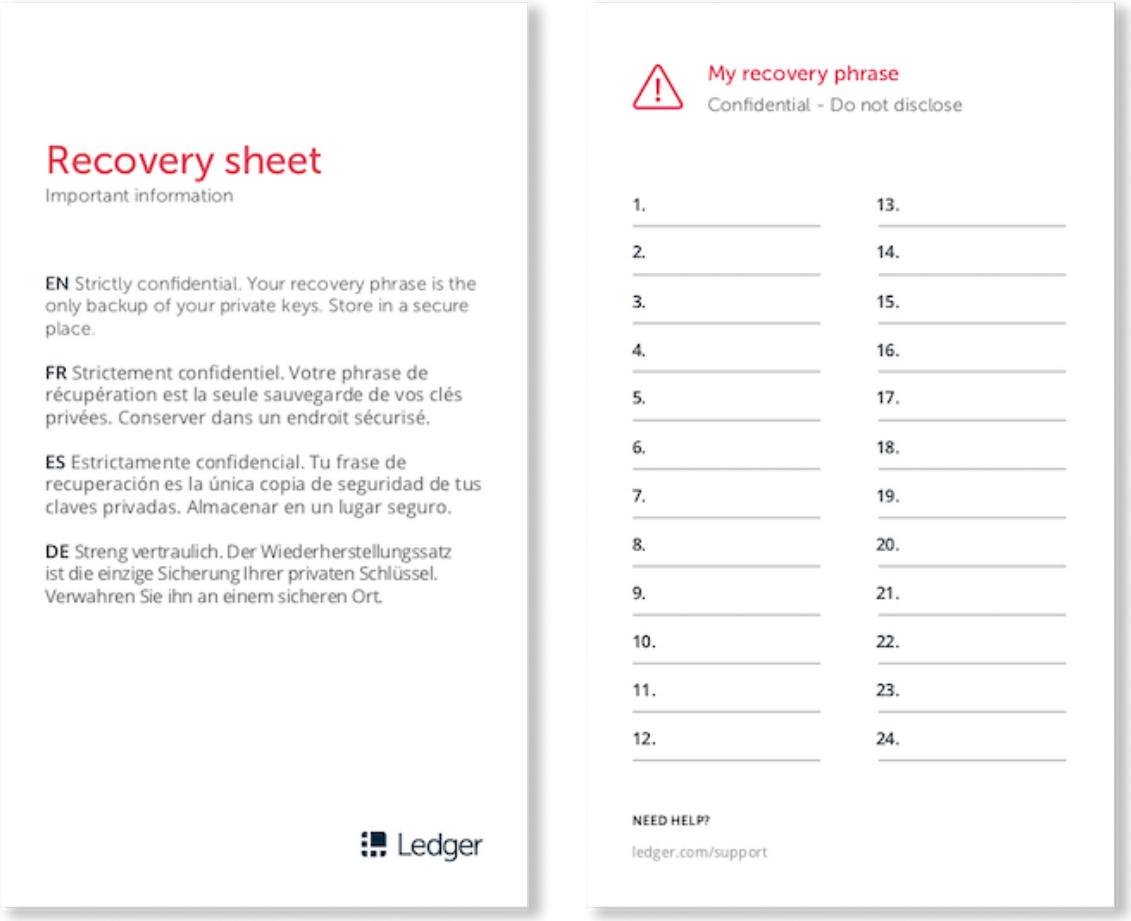
- Ledger Nano X
- Un câble USB de type C
- 3 cartes en papier dans une enveloppe, comprenant :
  - *Un fascicule "Getting started"* (Pour commencer)
  - *La déclaration d’utilisation, d’entretien et de règlementation*
  - 3 *Feuilles de récupération* vierges.
- Des accessoires : porte-clés et autocollants Ledger
- Emballage : un coffret et une pochette en carton de la marque Ledger

Contenu du coffret d'un Ledger Nano X

Vérifier que les feuilles de récupération sont vierges

Lorsque vous configurez votre appareil Ledger Nano X, celui-ci génère une nouvelle phrase de récupération de 24 mots que vous devez écrire sur votre feuille de récupération. Si une tierce personne venait à connaître votre phrase de récupération, vous pourriez perdre tous vos crypto-actifs. Suivez les consignes ci-dessous pour vous assurer que vos actifs restent sécurisés :

- Assurez-vous que vos feuilles de récupération sont toutes vierges.
- Si vos feuilles de récupération comportent déjà des mots, il est dangereux d'utiliser l'appareil.
  Veuillez contacter l'Assistance Ledger pour obtenir de l'aide.
- Ledger ne fournit jamais directement de phrase de récupération de 24 mots, de quelque manière que ce soit. Utilisez uniquement une phrase de récupération obtenue à partir de l'écran de votre appareil Ledger Nano X.



Recovery sheet

Important information

EN Strictly confidential. Your recovery phrase is the only backup of your private keys. Store in a secure place.

FR Strictement confidentiel. Votre phrase de récupération est la seule sauvegarde de vos clés privées. Conserver dans un endroit sécurisé.

ES Estrictamente confidencial. Tu frase de recuperación es la única copia de seguridad de tus claves privadas. Almacenar en un lugar seguro.

DE Streng vertraulich. Der Wiederherstellungssatz ist die einzige Sicherung Ihrer privaten Schlüssel. Verwahren Sie ihn an einem sicheren Ort.

Ledger

My recovery phrase

Confidential - Do not disclose

1.	13.
2.	14.
3.	15.
4.	16.
5.	17.
6.	18.
7.	19.
8.	20.
9.	21.
10.	22.
11.	23.
12.	24.

NEED HELP?

ledger.com/support

Feuille de récupération vierge

Vérifier les paramètres d’usine

- Lorsque vous allumez votre Ledger Nano X pour la première fois, le logo Ledger doit s’afficher. Relâchez le bouton. L’écran "Welcome to Ledger Nano X. Press right button to continue" (Bienvenue sur le Ledger Nano X. Appuyez sur le bouton droit) s’affiche.
- Ledger ne fournit jamais directement de code PIN, de quelque manière que ce soit. Choisissez toujours vous-même votre code PIN.
- Si le coffret contient un code PIN ou des instructions pour en obtenir un ailleurs, ou si votre appareil vous demande de saisir un code PIN la première fois que vous l’utilisez, il est dangereux d’utiliser l’appareil.
  Veuillez contacter l’Assistance Ledger pour obtenir de l’aide.

Ledger Nano X : *Message de bienvenue*

Vérifier l’authenticité avec les applications Ledger

- Utilisez Ledger Live pour configurer votre appareil Ledger et vérifier son authenticité.
- Les appareils Ledger authentiques contiennent une clé secrète qui est définie pendant la fabrication.
- Seul un appareil Ledger authentique peut utiliser sa clé pour fournir la preuve cryptographique requise afin de se connecter au serveur sécurisé de Ledger.

Résumé

- ✓ Vérifiez que vos feuilles de récupération sont vierges.
- ✓ Configurez vous-même votre Ledger Nano X. L’écran "Welcome" (Bienvenue) doit s’afficher lorsque vous démarrez votre appareil pour la première fois.
- ✓ Choisissez votre propre code PIN.
- ✓ Contactez l’Assistance Ledger en cas de doute.

En savoir plus

Scellés anti-fraude

Ledger a choisi de ne pas utiliser d’étiquettes anti-fraude sur ses emballages. Ces scellés sont en effet faciles à contrefaire et peuvent donc s’avérer trompeurs. Au lieu de cela, les

appareils Ledger authentiques

contiennent une puce sécurisée qui empêche toute falsification de l'appareil : cela offre une sécurité plus forte que n'importe quel autocollant.

Contrôle de l'intégrité du matériel

Les utilisateurs avancés peuvent vérifier l'intégrité du matériel à l'intérieur de leur appareil Ledger. Cet article fournit une chronologie non exhaustive des différentes révisions du build du Ledger Nano X. Notez que, dans le cadre d'une utilisation normale, il est déconseillé d'ouvrir son appareil Ledger. Si vous le faites, vous engagez votre propre responsabilité. Ledger ne saurait être tenue responsable des dommages pouvant résulter de l'ouverture de l'appareil.

Configurer comme un nouvel appareil

Pour commencer, configurez votre Ledger Nano X comme un nouvel appareil. Votre appareil générera de nouvelles clés privées : elles vous permettront de gérer vos crypto-actifs. Vous devrez également noter votre phrase unique de récupération de 24 mots.

Vous pouvez également restaurer votre appareil à partir d'une phrase de récupération. Cela vous permet de restaurer les clés privées associées à une phrase de récupération existante.

Indispensable

- ✓ Ledger Nano X
- ✓ Un smartphone iOS 9 ou Android 7 au minimum, ou un ordinateur au minimum sous Windows 8 (64 bits), macOS 10.8 ou Linux.
- ✓ L'application Ledger Live téléchargée et installée.

Instructions

Grâce à Ledger Live, vous pouvez configurer votre application de manière interactive. Pour commencer, ouvrez simplement l'application.

Étape 1. Configurer comme un nouvel appareil

1. Pour allumer votre appareil, appuyez sur le bouton à côté du port USB jusqu'à ce que le logo Ledger apparaisse.
2. Lisez les instructions à l'écran. Appuyez sur le bouton droit pour passer à l'étape suivante ou sur le bouton gauche pour revenir en arrière.
3. Appuyez simultanément sur les deux lorsque le message "Set up as a new device" (Configurer comme un nouvel appareil) s'affiche.

Étape 2. Choisir votre code PIN

1. Appuyez sur les deux boutons lorsque "Choose PIN code" (Choisissez un code PIN) s'affiche sur l'appareil.
2. Appuyez sur le bouton gauche ou droit pour choisir un chiffre. Appuyez sur les deux boutons simultanément pour confirmer.
3. Validez  pour confirmer votre code PIN composé de 4 à 8 chiffres. Choisissez  pour effacer un chiffre.

4. Saisissez à nouveau votre code PIN pour le confirmer sur l'écran "Confirm PIN code" (Confirmer le code PIN).

Conseils de sécurité

- Choisissez votre propre code PIN. Il vous permet de déverrouiller votre appareil.
- Utilisez 8 chiffres pour une sécurité optimale.
- N'utilisez jamais un appareil sur lequel le code PIN et/ou la phrase de récupération ont déjà été configurés.
- Contactez l'Assistance Ledger en cas de doute.

Étape 3. Sauvegarder votre phrase de récupération

Des instructions vont apparaître, puis votre phrase de récupération de 24 mots ("Recovery phrase") va s'afficher mot par mot sur l'écran de votre Ledger Nano X. Prêtez attention : votre phrase de récupération ne s'affichera qu'une seule fois.

1. Prenez la feuille de récupération vierge fournie dans le coffret.
2. Appuyez simultanément sur les deux boutons lorsque le message "Write down your recovery phrase" (Écrivez votre phrase de récupération) s'affiche.
3. Écrivez sur votre feuille de récupération le premier mot ("Word #1") affiché en gras et en langue anglaise sur votre appareil. Vérifiez que vous l'avez écrit et épelé correctement en position 1. Appuyez sur le bouton droit pour passer au mot suivant.
4. Faites cela jusqu'à ce que vous ayez écrit le 24e mot ("Word #24") en position 24 sur votre feuille. Appuyez sur les deux boutons de l'écran final pour valider.
5. Appuyez sur les deux boutons lorsque le message "Confirm your recovery phrase" (Confirmez votre phrase de récupération) s'affiche.
6. Trouvez le premier mot que vous avez écrit en position 1 sur votre feuille de récupération avec le bouton gauche ou droit. Validez ce mot en appuyant sur les deux boutons. Répétez cette opération pour confirmer les 24 mots de votre phrase de récupération.
7. Lorsque vous avez terminé la procédure de configuration, le message "Your device is ready" (Votre appareil est prêt) s'affiche. Appuyez sur les deux boutons pour accéder au "Dashboard" (Tableau de bord). Ce dernier va s'afficher sur votre appareil.

Conseils de sécurité

- Assurez-vous d'être bien la seule personne à connaître votre phrase de récupération. Toute personne ayant connaissance de cette phrase pourrait s'emparer de vos actifs. C'est pourquoi il est essentiel que vous la gardiez en lieu sûr.
- Ledger ne conserve pas de sauvegarde de votre phrase de récupération de 24 mots.
- N'utilisez jamais un appareil dont la phrase de récupération et/ou le code PIN ont déjà été configurés.
- Contactez l'Assistance Ledger en cas de doute.

Étapes suivantes

Vous avez bien généré de nouvelles clés privées sur votre appareil. Vous pouvez gérer un nouvel ensemble de comptes.

- Suivez ces conseils pour sécuriser votre phrase de récupération et votre code PIN.
- Installez des applications sur votre appareil et ajoutez des comptes dans Ledger Live.
- Recevez et envoyez des crypto-actifs.

Restaurer à partir d'une phrase de récupération

Utilisez votre phrase de récupération pour restaurer, remplacer ou cloner votre Ledger Nano X. Votre appareil pourra récupérer les clés privées sauvegardées grâce à votre phrase de récupération confidentielle.

Une autre solution consiste à le configurer comme un nouvel appareil pour générer de nouvelles clés privées et prendre en note votre nouvelle phrase de récupération.

Indispensable

- ✓ Un Ledger Nano X
- ✓ La phrase de récupération à restaurer. Les phrases de récupération de type BIP39 / BIP44 sont prises en charge.
- ✓ Un smartphone iOS 9 ou Android 7 au minimum, ou un ordinateur au minimum sous Windows 8 (64 bits), macOS 10.8 ou Linux.
- ✓ L'application Ledger Live téléchargée et installée.

Instructions

Grâce à Ledger Live, vous pouvez configurer votre application de manière interactive. Pour commencer, ouvrez simplement l'application.

Étape 1. Restaurer à partir d'une phrase de récupération

1. Pour allumer votre appareil, appuyez sur le bouton à côté du port USB jusqu'à ce que le logo Ledger apparaisse.
2. Lisez les instructions à l'écran. Appuyez sur le bouton droit pour passer à l'étape suivante ou sur le bouton gauche pour revenir en arrière.
3. Appuyez simultanément sur les deux boutons lorsque le message "Restore from recovery phrase" (Restaurer avec une phrase de récupération) s'affiche.

Étape 2. Choisir votre code PIN

1. Appuyez sur les deux boutons lorsque "Choose PIN code" (Choisissez un code PIN) s'affiche sur l'appareil.
2. Appuyez sur le bouton gauche ou droit pour choisir un chiffre. Appuyez sur les deux boutons simultanément pour confirmer.
3. Validez  pour confirmer votre code PIN composé de 4 à 8 chiffres. Choisissez  pour effacer un chiffre.
4. Saisissez à nouveau votre code PIN pour le confirmer sur l'écran "Confirm PIN code" (Confirmer le code PIN).

Conseils de sécurité

- Choisissez votre propre code PIN. Il vous permet de déverrouiller votre appareil.
- Utilisez 8 chiffres pour une sécurité optimale.
- N’utilisez jamais un appareil sur lequel le code PIN et/ou la phrase de récupération ont déjà été configurés.
- Contactez l’Assistance Ledger en cas de doute.

Étape 3. Saisir votre phrase de récupération

1. Choisissez la longueur de votre phrase de récupération (12, 18 ou 24 mots). Appuyez simultanément sur les deux boutons pour valider.

2. Saisissez les premières lettres du mot n°1 ("Word #1") en les sélectionnant avec le bouton droit ou gauche. Appuyez sur les deux boutons pour valider chaque lettre.
3. Choisissez le "Word #1" (Mot n°1) parmi les mots proposés. Appuyez sur les deux boutons pour le valider.
4. Faites cela jusqu'au dernier mot de votre phrase de récupération.
5. Lorsque vous avez terminé la procédure de configuration, le message "Your device is ready" (Votre appareil est prêt) s'affiche. Appuyez sur les deux boutons pour accéder au "Dashboard" (Tableau de bord). Ce dernier va s'afficher sur votre appareil.

Conseils de sécurité

- Assurez-vous d'être bien la seule personne à connaître votre phrase de récupération. Toute personne ayant connaissance de cette phrase pourrait s'emparer de vos actifs. C'est pourquoi il est essentiel que vous la gardiez en lieu sûr.
- Ledger ne conserve pas de sauvegarde de vos 24 mots. N'utilisez jamais un appareil dont la phrase de récupération et/ou le code PIN ont déjà été configurés.
- Contactez l'Assistance Ledger en cas de doute.

Phrase de récupération invalide ?

- Assurez-vous d'avoir sélectionné la bonne longueur de votre phrase de récupération. Entrez toujours tous les mots d'une phrase de récupération.
- Vérifiez que l'ordre des mots saisis sur votre appareil correspond bien à celui de votre feuille de récupération.
- Vérifiez que tous les mots de votre phrase de récupération figurent sur la liste des mots BIP39.

Étapes suivantes

Vous avez bien restauré sur votre appareil les clés privées associées à votre phrase de récupération.

- Suivez ces conseils pour sécuriser votre phrase de récupération et votre code PIN.
- Installez des applications sur votre appareil et ajoutez des comptes dans Ledger Live.
- Recevez et envoyez des crypto-actifs.

Accéder au Centre de contrôle

Accédez au "Control Center" (Centre de contrôle) sur votre Ledger Nano X pour verrouiller ou éteindre votre appareil, gérer la batterie et le Bluetooth, et ouvrir les "Settings" (Réglages) de l’appareil.

Parcourir le Centre de contrôle

1. Appuyez sur les deux boutons pendant trois secondes à tout moment pour ouvrir le "Control Center" (Centre de contrôle). Vous verrez d’abord apparaître l’état de la batterie.
2. Naviguez dans le Centre de contrôle en appuyant sur le bouton gauche ou droit.

3. Validez vos choix en appuyant sur les deux boutons.
    - "Battery" (Batterie) : niveau de charge actuel.
    - "Lock device" (Verr. appareil) : appuyez sur les deux boutons pour afficher le "Screen saver" (Écran de veille). Déverrouillez avec votre code PIN.
    - "Bluetooth" : indique le nom de votre appareil lorsque le Bluetooth est activé. Appuyez sur les deux boutons pour désactiver ("Disable") ou activer ("Enable") la connectivité Bluetooth.
    - "Settings" (Réglages) : appuyez sur les deux boutons pour accéder aux Réglages.
    - "Power Off" (Éteindre) : appuyez sur les deux boutons pour éteindre votre appareil.
    - "Close" (Sortir) : retournez à l'écran précédent.

En savoir plus

- En savoir plus sur le chargement de la batterie.
- Comment coupler votre Ledger Nano X avec votre smartphone.
- Contactez l'Assistance Ledger si vous avez besoin d'aide.

Sécuriser votre code PIN et votre phrase de récupération

Les produits Ledger sont dotés d'une combinaison de fonctionnalités de sécurité matérielle et logicielle conçue pour protéger vos crypto-actifs contre toute attaque potentielle. Pour bénéficier du niveau optimal de sécurité offert par votre Ledger Nano X, suivez les instructions ci-dessous.

Protéger son code PIN

Vous choisissez et définissez votre code PIN lors de la

configuration de votre appareil. Veuillez toujours :

- Choisir vous-même votre code PIN.
- Entrer votre code PIN à l'abri des regards indiscrets.
- Modifier votre code PIN si nécessaire. En savoir plus.
- N'oubliez pas que si vous saisissez trois fois de suite un code PIN erroné, votre appareil se réinitialisera.

Veuillez ne jamais :

- Utiliser un code PIN facile à deviner comme 0000, 123456 ou 55555555.
- Partager votre code PIN avec qui que ce soit.

- Utiliser un code PIN que vous n’avez pas choisi vous-même.
- Conserver votre code PIN sur un ordinateur ou un smartphone.

Sécuriser votre phrase de récupération de 24 mots

Votre phrase de récupération de 24 mots est la seule sauvegarde de vos

crypto-actifs. Veuillez toujours :

- Vous assurer d'obtenir votre phrase de récupération de 24 mots à partir de l'écran de votre appareil.
- Faire plusieurs copies manuscrites de votre phrase de récupération.
- Garder des copies de votre phrase de récupération en lieu sûr et à l'abri des regards indiscrets.

Veuillez ne jamais :

- Entrer votre phrase de récupération de 24 mots sur votre ordinateur ou votre téléphone.
- Prendre de photo de votre phrase de récupération de 24 mots.
- Partager votre phrase de récupération avec qui que ce soit.

En savoir plus

- Optimisez la sécurité de vos comptes en utilisant une passphrase (pour utilisateurs avancés).
- Contactez l'Assistance Ledger si vous avez besoin d'aide.

Envoyez et recevez

Recevoir des crypto-actifs

Vous pouvez recevoir des crypto-actifs sur les comptes que vous gérez avec votre Ledger Nano X, en générant une adresse de bénéficiaire dans l'application Ledger Live.

Conseil de sécurité

Commencez toujours par envoyer un petit montant. Vérifiez ensuite qu'il a été correctement reçu par le bénéficiaire avant d'envoyer des montants plus importants.

Avant de commencer

- ✓ Assurez-vous que Ledger Live est prêt à être utilisé.
- ✓ Vérifiez que les applications requises sont installées sur votre Ledger Nano X. *Exemple : installez l'application Bitcoin pour recevoir des bitcoins.*

Instructions

1. Appuyez sur les deux flèches en bas de l'application.
2. Appuyez sur Recevoir.
3. Choisissez le compte à créditer.
4. Sélectionnez le Ledger Nano X qui gère le compte à créditer.
    - Assurez-vous bien que votre appareil est allumé et déverrouillé.
    - Ouvrez l'application correspondant au type de crypto-actifs, comme indiqué.
5. Lisez les instructions à l'écran et appuyez sur "Verify" (Vérifier) pour afficher votre adresse sur votre Ledger Nano X.
6. Parcourez l'adresse et vérifiez qu'elle est identique à celle indiquée dans Ledger Live.
    - Si les adresses correspondent : appuyez sur le bouton droit pour accéder à l'écran "Approve" (Approuver).

      Appuyez ensuite sur les deux boutons pour confirmer l'adresse affichée dans Ledger Live.
7. Cliquez sur Copier ou sur Partager l'adresse, et partagez cette dernière avec l'émetteur de la transaction. Vérifiez soigneusement que l'adresse n'a pas été modifiée après l'avoir copiée et collée, ou appuyez sur le bouton Revérifier pour qu'elle s'affiche à nouveau sur votre appareil.

Les adresses ne correspondent pas ?

Sélectionnez "Reject" (Rejeter) sur votre appareil et n'y envoyez pas de crypto-actifs.

Vous n'avez pas votre appareil ?

- Sur l'écran de sélection du compte, cliquez sur « Vous n'avez pas votre appareil ? » pour générer une adresse de bénéficiaire.

- Dans ce cas, l’adresse de bénéficiaire générée sur Ledger Live ne bénéficie pas d’un niveau de sécurité optimal, car vous ne l’avez pas vérifiée sur votre wallet physique Ledger Nano X.

Pourquoi les adresses de réception changent-elles ?

Vous avez généré une adresse pour un compte et vous pouvez la partager avec l'émetteur.

- Les blockchains basées sur Bitcoin sont des réseaux publics. Pour une protection optimale de votre vie privée,
  les adresses de ces crypto-actifs ne doivent idéalement pas être réutilisées
  après une transaction.
- Ledger Live génère de nouvelles adresses pour les crypto-actifs basés sur le Bitcoin.
- Pour les crypto-actifs basés sur le Bitcoin, les adresses précédentes restent
  valables, mais elles n'offrent pas un niveau optimal de protection de la vie privée.

Envoyer des crypto-actifs

Vous pouvez envoyer des crypto-actifs à partir des adresses gérées par votre appareil Ledger Nano X, vers l'adresse d'un bénéficiaire, dans l'application Ledger Live.

Conseil de sécurité

Commencez toujours par envoyer un petit montant. Vérifiez ensuite qu'il a été correctement reçu par le bénéficiaire avant d'envoyer des montants plus importants.

Avant de commencer

- ✓ Vérifiez que Ledger Live est prêt à être utilisé et que vous avez des crypto-actifs à envoyer.
- ✓ Vérifiez que les applications requises sont installées sur votre appareil.
  Exemple : installez l'application Bitcoin pour envoyer des bitcoins.

Entrer les détails d'une transaction

1. Appuyez sur les deux flèches en bas de l'application.
2. Appuyez sur Envoyer.
3. Choisissez le Compte à débiter.
4. Appuyez sur le code QR pour le scanner ou saisissez manuellement l'adresse du bénéficiaire.
   Pour une sécurité optimale, veillez toujours à bien vérifier les adresses.
5. Saisissez le montant de cryptos à envoyer, ou l'équivalent dans la devise de contrepartie de votre choix*.
6. Appuyez sur Continuer.

Vérifier et signer

1. Vérifiez les détails de la transaction. Appuyez sur Continuer.
   - Appuyez sur Modifier sur l'écran récapitulatif pour modifier les Frais de réseau.
   - Plus les frais sont élevés, plus le traitement de la transaction est rapide. En savoir

plus.

2. Choisissez le Ledger Nano X à utiliser pour l’envoi et assurez-vous qu’il est allumé et déverrouillé.
3. Ouvrez l’application correspondant au type de crypto-actifs, comme indiqué.
4. Appuyez sur Continuer.

5. Vérifiez soigneusement tous les détails de la transaction sur votre appareil.
6. Si tout est correct, appuyez sur les deux boutons sur l'écran pour valider la transaction. La transaction est ensuite signée et diffusée au réseau pour confirmation.
7. Cliquez sur Voir les détails pour suivre la transaction jusqu'à ce qu'elle soit confirmée.

Devise de contrepartie

La devise de contrepartie que vous saisissez est convertie dans la cryptomonnaie de votre choix. Le bitcoin est utilisé comme monnaie intermédiaire lors de cette conversion. Le taux de change utilisé est celui des prestataires sélectionnés dans les Paramètres de l'application. Par défaut, les prestataires choisis sont ceux ayant les plus importants volumes de trading au cours des dernières 24 heures.

Vérifier les détails d'une transaction

Avant d'envoyer et de recevoir des crypto-actifs, familiarisez-vous avec les meilleures pratiques de sécurité offertes par votre wallet physique Ledger. En effet, les crypto-actifs que vous gérez avec votre appareil Ledger peuvent être la cible d'actes malveillants. Pour optimiser la sécurité de vos actifs, faites preuve de prudence lorsque vous effectuez vos transactions.

Adopter l'approche zéro confiance

Partez du principe que votre ordinateur ou votre smartphone est corrompu. Faites uniquement confiance aux informations qui s'affichent sur l'écran de votre appareil Ledger.

Envoyer

- Commencez toujours par envoyer un petit montant. Vérifiez ensuite que la transaction a été correctement reçue par le bénéficiaire avant d'envoyer des montants plus importants.
- Utilisez un mode de communication secondaire lorsque vous recevez une adresse ou un code QR d'un bénéficiaire.
  Exemple : si possible, vérifiez soigneusement par SMS, email ou via une application de messagerie l'adresse de dépôt fournie par une plateforme d'échange.
- Vérifiez les adresses des bénéficiaires après les avoir copiées et collées. D'éventuels logiciels malveillants sur votre ordinateur
  ou votre smartphone pourraient remplacer des adresses dans votre presse-papiers.
- Vérifiez que l'adresse du bénéficiaire, le montant et les frais sont corrects, et qu'ils sont identiques à la fois sur votre ordinateur ou sur votre smartphone et sur votre appareil lorsque vous envoyez une transaction.

Recevoir

- Vérifiez que chaque adresse utilisée pour recevoir des transactions vous appartient effectivement. Pour cela, affichez-la sur votre wallet physique. Si votre ordinateur ou votre smartphone est corrompu, les adresses affichées dans Ledger Live peuvent avoir été truquées.
- Attendez d'obtenir plusieurs confirmations avant d'accepter une transaction. Pour Bitcoin, il est généralement recommandé d'attendre six confirmations.

Adresses non vérifiées

Ledger Live peut fournir des adresses de bénéficiaire sans qu'il soit nécessaire de recourir à un appareil Ledger. Toutefois, ces adresses n'offrent pas un niveau de sécurité optimal. Utiliser des adresses non vérifiées se fait à vos risques et périls.

En savoir plus

- Apprenez à sécuriser votre code PIN et votre phrase de récupération.
- Jetez un œil aux fonctionnalités de sécurité avancée qui sont disponibles sur les appareils Ledger.
- Contactez l'Assistance Ledger en cas de doute.

Recevoir des revenus du minage

Les personnes participants à des activités de minage peuvent vouloir stocker en toute sécurité leurs revenus de minage en utilisant un appareil Ledger. Cet article explique pourquoi envoyer un grand nombre de petites transactions vers un wallet physique présente des inconvénients. Il propose également des solutions éventuelles et fournit des instructions sur la manière d'envoyer correctement les revenus de minage vers une adresse contrôlée par votre appareil Ledger.

Le non-respect de ces instructions pourrait rendre vos fonds inaccessibles sur un appareil Ledger.

Inconvénients occasionnés par la réception d'un grand nombre de petites transactions

Recevoir un grand nombre de petits paiements, ou *versements de poussière* (« dust payments » en anglais), sur une adresse contrôlée par votre wallet physique entraîne :

- La saturation de la synchronisation de vos transactions sur la blockchain.
- Une extrême lenteur dans la création ou la validation des transactions.

C'est pourquoi les wallets physiques ne sont pas particulièrement adaptés pour recevoir un nombre élevé de petites transactions, comme des revenus provenant des activités de minage.

Exemple : vous avez reçu 1 000 paiements de 0,001 BTC et vous voulez dépenser un total de 1 BTC. La puce sécurisée du wallet physique devra alors créer une transaction de 1 000 entrées et signer chacune d'elles. Cela peut prendre quelques heures ou ne pas aboutir du tout, car la puce peut surchauffer ou faire une erreur de calcul.

Que faire en cas de réception d'un grand nombre de petits

paiements ?

Si vous avez déjà envoyé un grand nombre de petits paiements sur votre wallet physique :

- Essayez de consolider vos coins en vous envoyant à vous-même quelques paiements plus importants. Par exemple : si vous avez reçu 1 000 x 0,001 BTC, consolidez ces entrées en vous envoyant à vous-même 0,1 BTC et répétez cette opération 10 fois.

- Vous pouvez également importer votre phrase de récupération de 24 mots dans un wallet applicatif, de préférence un wallet hors ligne. Videz ensuite votre wallet en transférant les fonds vers une adresse obtenue à partir d’une nouvelle phrase de récupération.

Anticiper en regroupant les transactions

- Configurez un wallet applicatif destiné à recevoir les petits paiements.
- Regroupez régulièrement ces gains en une seule transaction plus importante à envoyer à votre wallet physique.

Plus de fonctionnalités

Configurer le verrouillage et l'arrêt automatiques

Paramétrez le verrouillage automatique ou l’arrêt automatique pour verrouiller ou éteindre automatiquement votre appareil Ledger Nano X après une période d’inactivité. Vous aurez alors besoin de votre code PIN pour le déverrouiller. Pour une sécurité optimale, il est recommandé d’activer le verrouillage ou l’arrêt automatiques.

Instructions

Activer le verrouillage automatique

1. Allumez votre Ledger Nano X et déverrouillez-le.
2. Faites un appui long sur les deux boutons pour accéder au "Control Center" (Centre de contrôle).
3. Accédez aux "Settings" (Réglages). Appuyez ensuite simultanément sur les deux boutons pour valider.
4. Accédez à "Security" (Sécurité) et appuyez sur les deux boutons pour valider.
5. Appuyez sur les deux boutons pour accéder au menu "Auto-lock" (Verr. automatique).
6. Sélectionnez l’une des options suivantes :
    - "No auto lock" (Pas de verrouillage automatique)
    - 1 minute
    - 2 minutes
    - 5 minutes
    - 10 minutes
7. Appuyez sur les deux boutons pour activer l’option de verrouillage automatique choisie.

Si vous avez activé le verrouillage automatique, votre appareil va afficher des logos Ledger qui rebondissent lorsqu’il a été verrouillé automatiquement. Pour déverrouiller, appuyez sur n’importe quel bouton et saisissez votre code PIN.

Activer l'arrêt automatique

1. Allumez votre Ledger Nano X et déverrouillez-le.
2. Faites un appui long sur les deux boutons pour accéder au "Control Center" (Centre de contrôle).
3. Accédez aux "Settings" (Réglages). Appuyez ensuite simultanément sur les deux boutons pour valider.
4. Accédez à "General" (Général) et appuyez sur les deux boutons pour valider.
5. Appuyez sur les deux boutons pour accéder au menu "Auto Power Off" (Arrêt automatique).
6. Sélectionnez l’une des options suivantes :
    - Never power off (Ne jamais éteindre)

- 1 minute
- 3 minutes
- 5 minutes
- 10 minutes

7. Appuyez sur les deux boutons pour activer l’option choisie.

Si vous avez activé l’arrêt automatique, votre appareil s’éteindra automatiquement après le temps d’inactivité que vous avez configuré.

Configurer la connexion Bluetooth

Configurez la connexion Bluetooth chiffrée entre votre appareil Ledger Nano X et Ledger Live sur votre smartphone pour gérer vos crypto-actifs à tout moment. Par ailleurs, le Bluetooth peut être désactivé pour se connecter via USB uniquement.

Couplage Bluetooth

Appairez votre Ledger Nano X la première fois que vous le configurez avec votre smartphone.

1. Assurez-vous que le Bluetooth est activé sur votre smartphone et sur votre Ledger Nano X.
   Lancez le couplage dans Ledger Live pour le mobile.
2. Appuyez votre Ledger Nano X une fois qu'il apparaît dans Ledger Live pour le mobile. Le code de couplage peut prendre quelques instants avant de s'afficher sur les deux appareils.
3. Si les deux codes sont identiques, validez le couplage sur votre smartphone.
4. Appuyez sur les deux boutons de votre Ledger Nano X pour valider le couplage.
5. Appuyez sur les deux boutons pour "Allow Ledger Manager" (Autoriser le Gestionnaire Ledger). Le couplage est terminé après la vérification de l'authenticité du Ledger Nano X par le serveur sécurisé de Ledger.

Le couplage est enregistré dans les paramètres globaux de votre smartphone. Il n'est pas nécessaire de confirmer à nouveau le code de couplage tant que vous n'avez pas retiré l'appareil des paramètres Bluetooth de votre smartphone.

Désactiver la connectivité Bluetooth

Lorsque vous configurez votre Ledger Nano X, la fonction Bluetooth est activée par défaut.

1. Allumez votre Ledger Nano X et déverrouillez-le.
2. Faites un appui long sur les deux boutons pour accéder au "Control Center" (Centre de contrôle).
3. Accédez au symbole Bluetooth en vous servant du bouton droit ou gauche.
4. Appuyez sur les deux boutons pour désactiver le Bluetooth. Le mot "Disabled" (Désactivé) va s'afficher sur l'écran Bluetooth sur votre appareil Ledger.
5. Le réglage prendra effet lors du prochain démarrage de l'appareil.

Utilisez votre Ledger Nano X sans la connexion Bluetooth

Pour utiliser votre Ledger Nano X via USB :

- Ordinateur : utilisez le câble USB-C fourni avec votre Ledger Nano X pour le connecter à votre ordinateur de bureau. Gérez vos cryptos avec Ledger Live pour l'ordinateur ou avec toute autre application (Web) compatible.

- Mobile : utilisez un câble OTG pour connecter votre Ledger Nano X à votre smartphone Android (iOS non pris en charge). Gérez vos cryptos avec Ledger Live pour le mobile ou avec toute autre application (Web) compatible.

Modifier votre code PIN

Le code PIN de votre appareil Ledger Nano X empêche tout accès non autorisé à vos crypto-actifs. Vous choisissez votre code PIN lorsque vous configurez votre appareil pour la première fois, mais vous pouvez le modifier à tout moment.

Avant de commencer

- ✓ Assurez-vous que votre appareil est configuré et qu'il exécute la dernière version du micrologiciel.
- ✓ Consultez notre article sur les bonnes pratiques à adopter pour sécuriser son code PIN et sa phrase de récupération.

Instructions

1. Allumez votre Ledger Nano X et déverrouillez-le.
2. Faites un appui long sur les deux boutons pour accéder au "Control Center" (Centre de contrôle).
3. Accédez à "Settings > Security > Change PIN" (Réglages > Sécurité > Modifier le PIN).
4. Choisissez un nouveau code PIN composé de 4 à 8 chiffres.
5. Confirmez votre nouveau code PIN en le saisissant à nouveau.
6. Saisissez votre ancien code PIN pour valider.
7. Vous avez bien modifié votre code PIN.

Conseils de sécurité

- Choisissez votre propre code PIN. Il vous permet de déverrouiller votre appareil.
- Pour une sécurité optimale, créez un code PIN à 8 chiffres.
- Choisissez un code PIN difficile à deviner.

En savoir plus

- Optimisez la sécurité de vos comptes en utilisant une passphrase (pour utilisateurs avancés).
- Contactez l'Assistance Ledger si vous avez besoin d'aide.

Sécurité avancée : la passphrase

Configurez une passphrase pour ajouter un niveau de sécurité à vos crypto-actifs. Il s'agit d'une option réservée aux utilisateurs avancés. Lisez attentivement cette section avant de configurer une passphrase.

Conseil de sécurité

Les fonctionnalités de phrase de récupération et de passphrase offrent un large éventail de configurations de sécurité. Vous pouvez les utiliser pour concevoir la stratégie de sécurité qui vous convient. Attention toutefois à ne pas trop complexifier. La meilleure configuration

de sécurité est celle que vous maîtrisez et que vous pouvez exécuter en toute confiance.

Fonctionnement de la passphrase

La phrase de récupération de 24 mots enregistrée lors de la première configuration de votre wallet physique Ledger sauvegarde entièrement les clés privées permettant d'accéder à vos comptes. Vous devez la conserver en lieu sûr.

- La passphrase est comme un mot de passe qui est ajouté à votre phrase de récupération de 24 mots.
  Elle donne accès à un tout nouvel ensemble de comptes.
- La passphrase protège vos crypto-actifs au cas où votre phrase de récupération de 24 mots serait compromise. Pour accéder à un compte protégé par une passphrase, un pirate devra posséder votre phrase de récupération ainsi que votre passphrase secrète.
- Chaque passphrase déverrouille un seul ensemble de comptes. Vous pouvez donc utiliser autant de passphrases que vous le souhaitez.

Avant de commencer

✓ Assurez-vous que votre appareil est configuré et qu'il exécute la dernière version du micrologiciel.
✓ Assurez-vous d'avoir à portée de main votre phrase de récupération, par mesure de précaution.
✓ Lisez entièrement cet article avant de commencer.

Instructions

Premiers pas

1. Connectez votre Ledger Nano X et saisissez votre code PIN.
2. Faites un appui long sur les deux boutons pour accéder au "Control Center" (Centre de contrôle).
3. Accédez au menu "Settings" (Réglages).
4. Accédez à "Security" (Sécurité).
5. Accédez à Passphrase et choisissez l'une des deux options suivantes :
   - "Attach to PIN" (Lier au code PIN) : crée un code PIN secondaire pour déverrouiller les comptes protégés par passphrase.
   - "Set as temporary" (Définir temporaire) : entrez la passphrase chaque fois que vous souhaitez accéder à des comptes protégés par passphrase.
6. Continuez avec la section ci-dessous qui correspond à l'option que vous avez choisie.

Option 1 - Lier au code PIN

Fonctionnement

Lier une passphrase à un nouveau code PIN crée un nouvel ensemble de comptes sur votre Ledger Nano X, sur la base d'une passphrase secrète de votre choix. Vous pouvez accéder

aux comptes qu’elle protège en saisissant un code PIN secondaire.

- La passphrase sera stockée sur votre appareil jusqu’à ce que vous la remplaciez ou que votre appareil soit réinitialisé.
- Conservez une sauvegarde physique de votre passphrase secrète en lieu sûr. Votre appareil ne pourra plus l’afficher après avoir été configurée.

Instructions

1. Choisissez l’option "Attach to PIN" dans le menu Passphrase des "Settings" > "Security" (Réglages > Sécurité) de l’appareil.
2. Appuyez sur les deux boutons pour valider "Set up passphrase" (Définir la passphrase) sur l’écran avec la petite coche.
3. Créez un code PIN secondaire.
4. Saisissez à nouveau le code PIN secondaire pour le confirmer.
5. Choisissez et confirmez une passphrase secrète (max. 100 caractères).
6. Saisissez votre code PIN principal pour valider.
7. Votre appareil continuera à gérer les comptes liés à votre phrase de récupération sans passphrase. Veuillez éteindre votre appareil et saisir votre code PIN secondaire pour accéder aux comptes protégés par passphrase.

Option 2 - Définir une passphrase temporaire

Fonctionnement

L’utilisation d’une passphrase temporaire donne accès à un nouvel ensemble de comptes sur votre Ledger Nano X pour la durée de la session. Suivez les instructions ci-dessous chaque fois que vous souhaitez accéder à vos comptes protégés par passphrase.

- Les comptes sont liés à une passphrase secrète de votre choix.
- Conservez une sauvegarde physique de votre passphrase secrète en lieu sûr. Votre appareil ne pourra plus l’afficher une fois que vous l’avez configuré.

Instructions

1. Accédez à "Settings" > "Security" > "Passphrase" (Réglages > Sécurité > Passphrase). Choisissez l’option "Set as temporary" (Définir passphrase temporaire).
2. Appuyez sur les deux boutons pour valider "Set up passphrase" (Définir la passphrase) sur l’écran avec la petite coche.
3. Choisissez et confirmez une passphrase secrète (max. 100 caractères).
4. Saisissez votre code PIN principal pour valider.
5. Votre appareil va maintenant gérer vos comptes protégés par cette passphrase. Pour accéder à vos comptes principaux, veuillez redémarrer votre appareil et saisir votre code PIN comme d’habitude.

Récupérer des comptes protégés par passphrase

En cas de perte ou de réinitialisation de votre Ledger Nano X, vous pouvez récupérer l’accès à vos crypto-actifs sur n’importe quel appareil Ledger. Pour cela, vous devez disposer à la fois de votre phrase de récupération de 24 mots et de votre passphrase secrète.

Instructions

1. Munissez-vous de votre phrase de récupération et de votre passphrase.
2. Restaurez votre appareil Ledger à partir de votre phrase de récupération.
3. Suivez les instructions ci-dessus relatives aux options passphrase temporaire ou lier au code PIN. Notez toutefois ceci :
    a. "Temporary passphrase" (Passphrase temporaire) : saisissez simplement la passphrase que vous avez configurée précédemment pour accéder aux comptes qu’elle protège.

b. "Attach to PIN code" (Lier au code PIN) : vous pouvez choisir n'importe quel code PIN, mais vous devez saisir la passphrase que vous avez configurée plus tôt pour accéder aux comptes qu'elle protège.

Sécuriser sa passphrase

Se protéger avec le déni plausible

Pour vous protéger en cas de menace physique, organisez-vous pour que votre code PIN principal ne permette de déverrouiller qu'une petite partie de vos crypto-actifs. Ensuite, configurez une passphrase liée à un code PIN et stockez une quantité plus importante de crypto-actifs sur les comptes protégés par passphrase.
S'il vous est demandé de déverrouiller votre Ledger Nano X sous la contrainte, vous pouvez remettre votre code PIN principal à l'agresseur sans révéler le code PIN qui déverrouille vos comptes protégés par passphrase.

Protéger sa phrase de récupération

Une bonne pratique de sécurité consiste à avoir plusieurs copies de votre feuille de récupération et à les conserver dans différents endroits. Pour limiter le risque de perdre vos crypto-actifs si quelqu'un venait à mettre la main sur l'une de ces copies, vous pouvez configurer une passphrase. Si vous le faites, veillez à conserver des sauvegardes papier de votre passphrase, de préférence dans des endroits différents de ceux où vous avez conservé une sauvegarde de votre phrase de récupération.

En savoir plus

- Apprenez à optimiser la sécurité de vos comptes.
- Contactez l'Assistance Ledger si vous avez besoin d'aide.

Optimiser la durée de vie de la batterie

Le Ledger Nano X dispose d'une batterie Lithium-ion de 100 mAh capable de tenir sur plusieurs heures en utilisation. Elle peut également tenir sur quelques mois après une charge complète et lorsque l'appareil est en veille. Pour optimiser l'autonomie et la durée de vie de la batterie de votre Ledger Nano X, suivez les conseils dans cet article.

Charger la batterie

Chargez la batterie à 100 % pour bénéficier de plusieurs heures d'utilisation. Pour cela, il suffit de brancher le port USB-C de votre appareil à une source d'alimentation USB. Un symbole de charge va alors apparaître sur l'icône d'état de la batterie, en haut à droite de

votre écran.
Il n’est pas nécessaire d’attendre que la batterie soit complètement déchargée avant de la recharger. En fait, l’autonomie d’une batterie utilisée est mieux préservée lorsque vous rechargez votre appareil aussi souvent que possible. Pour vérifier le niveau de charge de la batterie, faites un appui long sur les deux boutons pour accéder au "Control Center" (Centre de contrôle).

Optimiser la durée de vie de la batterie

Si vous voulez stocker votre Ledger Nano X pendant de longues périodes sans l'utiliser, il est recommandé de recharger complètement la batterie tous les quelques mois. La durée de vie de la batterie sera ainsi mieux préservée. Dès qu'il est complètement chargé, éteignez l'appareil et placez-le dans un endroit frais et à l'abri de l'humidité.
Il est déconseillé de garder votre Ledger Nano X pendant une période prolongée à très faible charge, car cela peut détériorer la capacité de la batterie.

Fin de vie

La batterie de votre appareil est conçue pour durer 5 ans. Ledger n'offre pas de programme de remplacement des batteries. Si la capacité de votre batterie s'est dégradée au point de ne plus être utilisable, vous pouvez utiliser votre appareil en le connectant à une source d'alimentation à l'aide du câble USB.

Exporter vos comptes

Les comptes générés par un appareil Ledger Nano X peuvent être récupérés sur n'importe quel wallet tiers physique ou applicatif prenant en charge les mêmes normes que Ledger (BIP32 / BIP39 / BIP44).

Avant de commencer

- ✓ Notez bien que votre phrase de récupération de 24 mots donne un accès complet à vos comptes. Saisir votre phrase de récupération sur un ordinateur ou un smartphone présente un risque. Évitez donc de le faire.
- ✓ Choisissez soigneusement un wallet tiers, qu'il soit physique ou applicatif. Vous êtes responsable de la protection de vos comptes.
- ✓ Contactez l'Assistance Ledger en cas de doute.

Instructions

Utiliser votre phrase de récupération

1. Choisissez un wallet physique ou applicatif compatible avec les normes BIP39 / BIP44.
2. Munissez-vous de votre phrase de récupération de 24 mots.
3. Suivez les instructions relatives à l'appareil ou au service sélectionné pour importer votre phrase de récupération (également appelée *graine mnémonique*).

Appareils Ledger compatibles

- Ledger Nano X
- Ledger Nano S
- Ledger Blue
- Ledger Nano

- Ledger HW.1

Liste discrétionnaire de wallets applicatifs tiers

Sécurité des wallets applicatifs

Les wallets applicatifs sont très peu sécurisés. Ils n'ont pas été soumis à un audit de sécurité par Ledger et ne doivent être utilisés pour la récupération qu'en dernier recours. Si vous choisissez d'utiliser l'un des wallets applicatifs ci-dessous, vous assumez la responsabilité en cas de problème éventuel.

- Mycelium (pour smartphone)
- Electrum (pour ordinateur)
- Bither (pour smartphone ou ordinateur)
- Coinomi (pour smartphone)
- Jaxx Liberty (pour smartphone)
- MyEtherWallet
- MyCrypto

Générer des clés privées (niveau avancé)
Les utilisateurs avancés peuvent générer manuellement toutes les clés privées à l'aide de l'outil BIP39 de Ian Coleman. Il est préférable de télécharger cet outil pour une utilisation hors ligne, comme indiqué ci-dessous.

Générer vos clés privées

1. Téléchargez l'outil BIP39 à la fin de cette section ou consultez la source sur GitHub.
2. Double-cliquez sur le fichier téléchargé pour l'ouvrir dans un navigateur.
3. Saisissez votre phrase de récupération de 24 mots dans le champ "*BIP39 Mnemonic*" (Mnémonique BIP39). Utilisez uniquement des minuscules.
4. Saisissez votre passphrase dans le champ en dessous, si vous en avez défini une dans votre wallet physique Ledger.
5. Sélectionnez une cryptomonnaie dans le menu déroulant "Coin".
6. Laissez le champ "Internal/External" (Interne/Externe) sur la valeur 0.

Importer vos clés privées

1. Copiez la liste des clés privées générées dans la section *"Derived Addresses"* (Adresses dérivées). Utilisez les contrôles "More rows" (Plus de lignes) sous la liste pour afficher plus de lignes ou pour commencer à un certain index ("Starting from index").
2. Importez vos clés privées dans un wallet tiers qui prend en charge cette fonctionnalité, tel que MyEtherWallet ou Armory.
3. Définissez le champ "Internal/External" (Interne/Externe) sur 1 pour générer les clés privées de vos "change addresses" (adresses de différence).

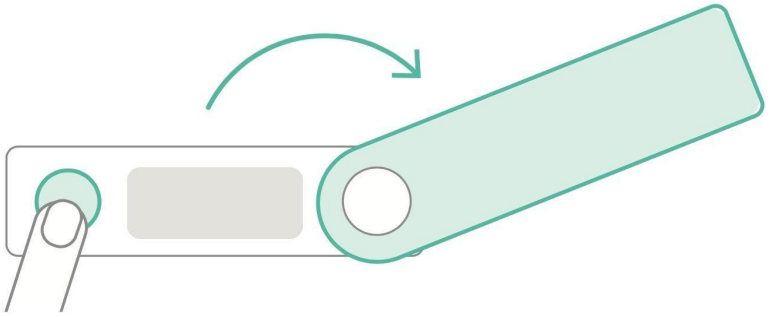
4. Importez les clés privées associées à vos "change adresses" dans votre wallet tiers.

Accéder aux mentions légales

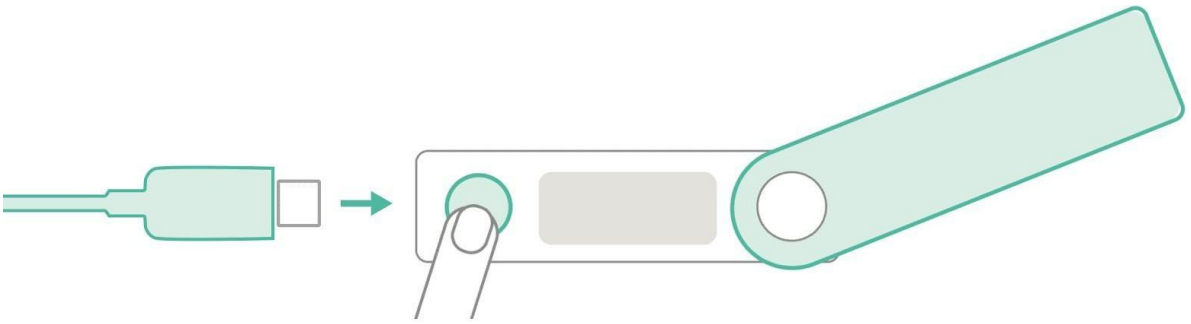
Il est possible d'accéder aux mentions légales de deux manières, selon que l'appareil a déjà été configuré ou non. Suivez les instructions de l'**Option 1** si l'appareil est encore configuré sur les paramètres d'usine. Suivez les instructions de l'**Option 2** si l'appareil a été configuré et que, en tant que propriétaire, vous connaissez le code PIN confidentiel.

Option 1 - Appareil aux paramètres d'usine

1. Faites tourner la protection pivotante.

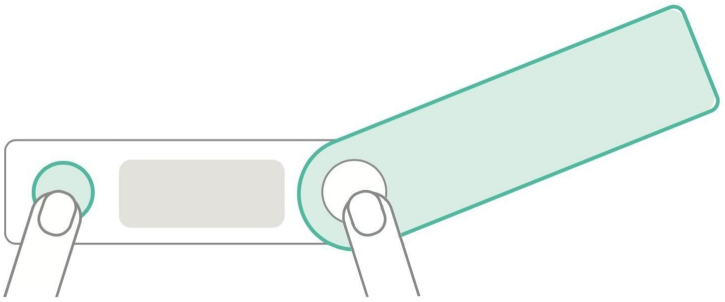


2. Faites un appui long sur le bouton à côté du port USB tout en connectant l'appareil à une source d'alimentation en utilisant le câble USB-C fourni. Le logo Ledger va alors s'afficher.



3. Appuyez une fois sur le bouton droit pour sélectionner **"Regulatory info"** (Mentions légales) dans le menu de démarrage ("Boot").

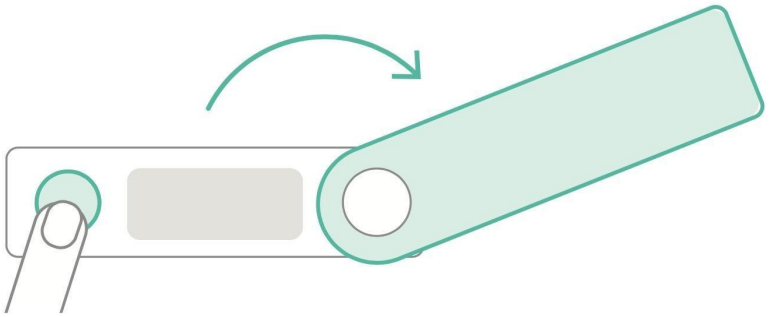
4. Appuyez simultanément sur les deux boutons pour accéder à **"Regulatory info"**.



5. Appuyez sur le bouton droit pour afficher toutes les informations.

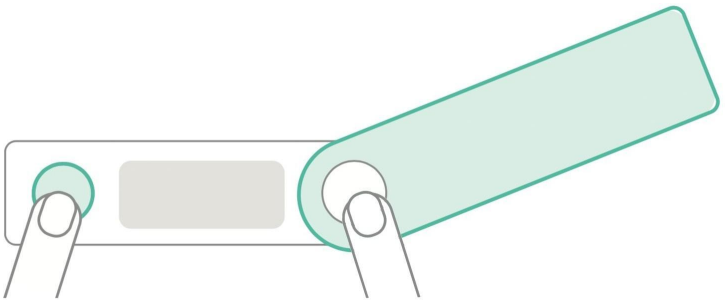
Option 2 - Appareil déja utilisé

1. Faites tourner la protection pivotante. Appuyez sur le bouton gauche pour allumer votre appareil.



2. Déverrouillez votre appareil Ledger en saisissant votre code PIN confidentiel.
3. Faites un appui long sur les deux boutons pour ouvrir le "Control Center"

   (Centre de contrôle) à partir du tableau de bord.



4. Appuyez sur le bouton droit jusqu'à sélectionner **"Settings"** (Réglages).

   Appuyez ensuite simultanément sur les deux boutons pour valider.

5. Appuyez simultanément sur les deux boutons pour accéder à **"Settings" > "General"** (Réglages > Général).

6. Appuyez sur le bouton droit pour sélectionner **"Regulatory info"** (Mentions légales). Appuyez ensuite simultanément sur les deux boutons pour valider.
7. Appuyez sur le bouton droit pour afficher toutes les informations.

Dépannage

Résoudre les problèmes de connexion

Si vous rencontrez des difficultés à connecter votre wallet physique Ledger, essayez les solutions suivantes, l'une après l'autre.

Mac, Windows ou Linux

1. Fermez toutes les autres applications *(applications Ledger, wallet de cryptos, Geth, Parity, Mist, Bitcoin Core, etc.)*
2. Désactivez votre VPN et votre antivirus.
3. Changez de câble USB si possible.
4. Essayez différents ports USB.
5. Redémarrez votre ordinateur.
6. Essayez sur un autre ordinateur.

Si le problème persiste, procédez comme suit en fonction du système d'exploitation utilisé :

Windows

- Mettez à jour les pilotes des périphériques d'entrée USB
    1. Ouvrez Périphériques et imprimantes à partir du Panneau de configuration.
    2. Double-cliquez sur Nano X et ouvrez l'onglet Appareil.
    3. Sélectionnez Périphérique d'entrée USB, puis cliquez sur Propriétés.
    4. Cliquez sur Modifier les paramètres.
    5. Cliquez sur l'onglet Pilote.
    6. Cliquez sur Mettre à jour le pilote et optez pour la recherche automatique du pilote.
    7. Exécutez cette opération pour les deux périphériques d'entrée USB.
- Si cela ne fonctionne toujours pas, veuillez essayer de connecter votre Ledger Nano X avec un Mac pour vérifier qu'il fonctionne correctement.

Mac

Si le problème de connexion persiste sur Mac, vous pouvez essayer d'accorder à Ledger Live un accès complet au disque :

1. Ouvrez les Préférences système.
2. Accédez à Sécurité et confidentialité.
3. Dans l'onglet Confidentialité, ajoutez Ledger Live à la liste Accès complet au disque.

Linux

Sous Linux, vous devez créer un ensemble de règles udev pour autoriser l'accès aux périphériques. Consultez la documentation de l'API USB de Chrome pour en savoir plus. Veuillez suivre les instructions ci-dessus.

1. Configuration

- Vérifiez si le groupe plugdev existe en saisissant la commande :

  ```
  cat /etc/group | grep plugdev
  ```

- Si la commande précédente n'a pas donné de résultat, veuillez suivre les étapes ci-dessous.
  1. Créez le groupe plugdev :

     ```
     sudo groupadd plugdev
     ```

  2. Vérifiez si vous êtes dans le groupe plugdev avec la commande :

     ```
     groups
     ```

  3. Si le résultat ne contient pas plugdev, vous n'êtes pas dans le groupe plugdev. Entrez la commande :

     ```
     sudo gpasswd -a <user> plugdev
     ```

  4. Remarque : remplacez <user> par votre nom d'utilisateur, par exemple pour l'utilisateur « paul », ce serait : sudo gpasswd -a paul plugdev.

     ```
     sudo gpasswd -a <user> plugdev
     ```

  5. Déconnectez-vous et reconnectez-vous pour que la modification prenne effet. Pour vérifier que vous êtes maintenant dans le groupe plugdev, entrez la commande :

     ```
     groups
     ```

  6. Recherchez une occurrence plugdev. S'il n'en existe pas, c'est que vous avez manqué une étape. Vous devez recommencer à l'étape 1.

2. Ajouter les règles udev

1. Pour ajouter automatiquement les règles udev et les recharger, entrez la commande suivante : `wget -q -O - https://raw.githubusercontent.com/LedgerHQ/udev-rules/master/add_udev_rules.sh | sudo bash`

2. Réessayez de connecter votre Ledger Nano X à Ledger Live.

   Si cela ne fonctionne toujours pas, passez à l'étape 3 : dépannage.

3. Dépannage

Essayez chacune des trois options suivantes :

- Option 1
  Modifiez le fichier /etc/udev/rules.d/20-hw1.rules en ajoutant le paramètre OWNER="<user>" à chaque ligne, où <user> désigne votre nom d'utilisateur Linux.
  Rechargez ensuite les règles comme suit :

  ```
  udevadm trigger
  udevadm control --reload-rules
  ```

  Réessayez de connecter l'appareil à Ledger Live. Si cela ne fonctionne pas, passez à l'option suivante.

- Option 2
  Modifiez le fichier /etc/udev/rules.d/20-hw1.rules en ajoutant les lignes suivantes :

  ```
  KERNEL=="hidraw*", SUBSYSTEM=="hidraw", MODE="0660",
  GROUP="plugdev", ATTRS{idVendor}=="2c97"
  KERNEL=="hidraw*", SUBSYSTEM=="hidraw", MODE="0660",
  GROUP="plugdev", ATTRS{idVendor}=="2581"
  ```

  Rechargez ensuite les règles avec :

  ```
  udevadm trigger
  udevadm control --reload-rules
  ```

  Réessayez de connecter l'appareil à Ledger Live. Si cela ne fonctionne pas, passez à la dernière option.

- Option 3
  Si vous utilisez Arch Linux, vous pouvez essayer les règles suivantes :
  ```
  /etc/udev/rules.d/20-hw1.rules
  SUBSYSTEMS=="usb",
  ATTRS{idVendor}=="2581",
  ATTRS{idProduct}=="1b7c", MODE="0660",
  TAG+="uaccess", TAG+="udev-acl"

  SUBSYSTEMS=="usb", ATTRS{idVendor}=="2581",
  ATTRS{idProduct}=="2b7c", MODE="0660",
  TAG+="uaccess", TAG+="udev-acl"

  SUBSYSTEMS=="usb", ATTRS{idVendor}=="2581",
  ATTRS{idProduct}=="3b7c", MODE="0660",
  TAG+="uaccess", TAG+="udev-acl"
  ```

```
SUBSYSTEMS=="usb",
ATTRS{idVendor}=="2581",
ATTRS{idProduct}=="4b7c", MODE="0660",
TAG+="uaccess", TAG+="udev-acl"

SUBSYSTEMS=="usb",
ATTRS{idVendor}=="2581",
ATTRS{idProduct}=="1807", MODE="0660", TAG+="uaccess",
TAG+="udev-acl"

SUBSYSTEMS=="usb",
ATTRS{idVendor}=="2581",
ATTRS{idProduct}=="1808", MODE="0660", TAG+="uaccess",
TAG+="udev-acl"

SUBSYSTEMS=="usb",
ATTRS{idVendor}=="2c97",
ATTRS{idProduct}=="0000", MODE="0660", TAG+="uaccess",
TAG+="udev-acl"

SUBSYSTEMS=="usb",
ATTRS{idVendor}=="2c97",
ATTRS{idProduct}=="0001", MODE="0660", TAG+="uaccess",
TAG+="udev-acl”

SUBSYSTEMS=="usb",
ATTRS{idVendor}=="2c97",
ATTRS{idProduct}=="0004", MODE="0660", TAG+="uaccess",
TAG+="udev-acl"
```

Rechargez ensuite les règles et réessayez de connecter l’appareil à Ledger Live :

```
udevadm trigger
udevadm control --reload-rules
```

iOS et Android

Si vous rencontrez des problèmes de Bluetooth avec votre Ledger Nano X, veuillez supprimer le couplage et dissocier le Ledger Nano X des périphériques Bluetooth sur votre téléphone (option « Oublier cet appareil »). Ensuite, configurez à nouveau le couplage.

Réinitialiser les couplages sur votre Ledger Nano X

1. Allumez votre Ledger Nano X et déverrouillez-le.
2. Faites un appui long sur les deux boutons pour accéder au "Control Center" (Centre de contrôle).
3. Appuyez sur les deux boutons pour accéder au menu "Security" (Sécurité).
4. Appuyez sur le bouton droit, puis accédez au menu "Reset pairings" (Réinitialiser les couplages) en appuyant sur les deux boutons.
5. Sur l’écran "Reset pairings" (Réinitialiser les couplages), confirmez votre choix en

appuyant à nouveau sur les deux boutons.

Dissocier votre Ledger Nano X sur votre smartphone

1. Ouvrez le menu des Paramètres Bluetooth de votre smartphone.
2. Sélectionnez les paramètres relatifs à votre Ledger Nano X.
3. Appuyez sur Oublier cet appareil.

Vous pouvez maintenant configurer à nouveau le couplage en sélectionnant votre Ledger Nano X à n'importe quel moment dans Ledger Live pour le mobile. Pour cela, vous devez connecter votre appareil, notamment dans l'onglet Gestionnaire.

Perte de l'appareil, du code PIN ou de la phrase de récupération

Vous ne parvenez pas à retrouver votre Ledger Nano X ? Vous avez oublié votre code PIN ? Vous avez perdu votre phrase de récupération ? Pour éviter de perdre vos crypto-actifs dans chacune de ces situations, suivez immédiatement la procédure décrite dans cet article.

Assurez-vous que votre phrase de récupération reste stockée en lieu sûr. Protégez votre code PIN confidentiel et votre phrase de récupération de 24 mots pour bénéficier du niveau de sécurité le plus élevé offert par votre wallet physique Ledger.

Instructions

Vous n'avez plus accès à votre appareil Ledger ?

1. Si votre appareil est perdu, volé ou endommagé, vous pouvez restaurer votre phrase de récupération sur tout autre wallet physique ou applicatif qui prend en charge les phrases de récupération de 24 mots.
2. Lors de la configuration, vous avez besoin de la feuille de récupération sur laquelle vous aviez écrit votre phrase de récupération.

Vous avez oublié votre code PIN ?

1. Si vous saisissez trois fois de suite un code PIN erroné, les wallets physiques Ledger se réinitialisent aux paramètres d'usine, effaçant les clés privées de leur espace de stockage sécurisé.
2. Après cette réinitialisation, il vous suffit de restaurer votre appareil à partir de votre phrase de récupération.
3. Choisissez un nouveau code PIN au cours du processus de restauration.

Vous avez perdu votre phrase de récupération ?

Votre feuille de récupération est une sauvegarde intégrale des clés privées qui donnent accès à vos clés privées. Vous devez la conserver en lieu sûr. Toute personne connaissant votre phrase de récupération pourrait s’emparer de vos actifs sans avoir besoin du code PIN de votre appareil.

Si vous perdez votre feuille de récupération :

1. Envoyez immédiatement tous vos crypto-actifs vers des comptes temporaires, comme une plateforme d'échange ou un autre wallet physique.
2. Saisissez trois codes PIN incorrects pour réinitialiser votre Ledger Nano X.
3. Configurez votre Ledger Nano X comme un nouvel appareil.
4. Ensuite, transférez vos crypto-actifs sur les comptes de votre appareil nouvellement configuré.

Réinitialiser aux paramètres d'usine

Une réinitialisation de l'appareil aux paramètres d'usine supprime toutes les clés privées, les applications et les paramètres de votre appareil Ledger Nano X. Rétablir la configuration d'usine vous permet de le configurer comme un nouvel appareil, de le restaurer à partir d'une autre phrase de récupération ou de donner votre appareil à quelqu'un d'autre en toute sécurité.

Avant de commencer

✓ Assurez-vous que vous êtes la seule personne à connaître votre phrase de récupération de 24 mots. C'est elle qui sauvegarde vos clés privées sur votre appareil.

Instructions

Avez-vous votre feuille de récupération ?

Si vous réinitialisez votre appareil sans avoir votre feuille de récupération, les clés privées qui vous permettent d'accéder à vos crypto-actifs seront effacées. Vous n'aurez plus jamais accès à vos crypto-actifs.

Votre appareil peut être réinitialisé à partir de son menu des "Settings" (Réglages) ou en saisissant trois codes PIN incorrects lors du déverrouillage. Choisissez l'une des deux options ci-dessous :

Réinitialiser à partir des réglages de l'appareil

1. Allumez votre Ledger Nano X et déverrouillez-le.
2. Faites un appui long sur les deux boutons pour accéder au "Control Center" (Centre de contrôle).
3. Accédez aux "Settings" (Réglages) et appuyez sur les deux boutons pour valider.
4. Accédez à "General" (Général) et appuyez sur les deux boutons pour valider.
5. Choisissez "Reset all" (Tout réinitialiser) en appuyant sur les deux boutons.

6. Parcourez les différents écrans et choisissez "Reset device" (Réinit. appareil) pour valider.
7. Saisissez votre code PIN pour confirmer. Votre appareil sera alors réinitialisé.

Réinitialiser à partir du code PIN

1. Allumez votre Ledger Nano X.
2. Saisissez à trois reprises un code PIN incorrect.

3. Par sécurité, votre appareil se réinitialise après le troisième code PIN erroné.

Étapes suivantes

Vous avez bien réinitialisé votre appareil aux paramètres d'usine. Vous pouvez choisir de :

- Découvrir comment le configurer comme un nouvel appareil pour générer et sauvegarder de nouvelles clés privées.
- Par ailleurs, restaurer votre appareil à partir d'une phrase de récupération vous permet de restaurer les clés privées associées à une phrase existante.

Vérifier l'intégrité du matériel

Vérifiez l'intégrité du matériel de votre Ledger Nano X pour vous assurer qu'il n'a pas été compromis. Cet article contient des informations techniques détaillées relatives à la sécurité de votre appareil.

Avertissement

Veuillez manipuler votre Ledger Nano X avec précaution pendant la vérification. Notez qu'une fois ouvert, votre appareil ne sera ni remboursable ni échangeable.

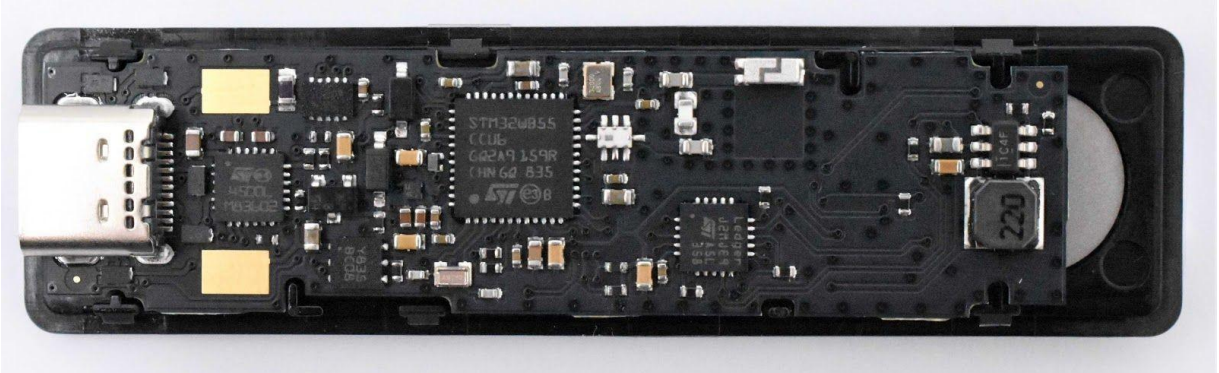
Microcontrôleur (MCU)

L'élément sécurisé (Secure Element) vérifie la totalité de la mémoire flash du microcontrôleur au démarrage, comme décrit dans cet article de blog. S'il a été modifié, vous recevrez un avertissement au démarrage. Pour effectuer un contrôle supplémentaire, vous pouvez ouvrir votre appareil et vérifier qu'aucune puce supplémentaire n'a été ajoutée. Comparez votre appareil aux photos ci-dessous, et assurez-vous que le MCU est un STM32WB55. L'élément sécurisé porte la mention J2MJE9.

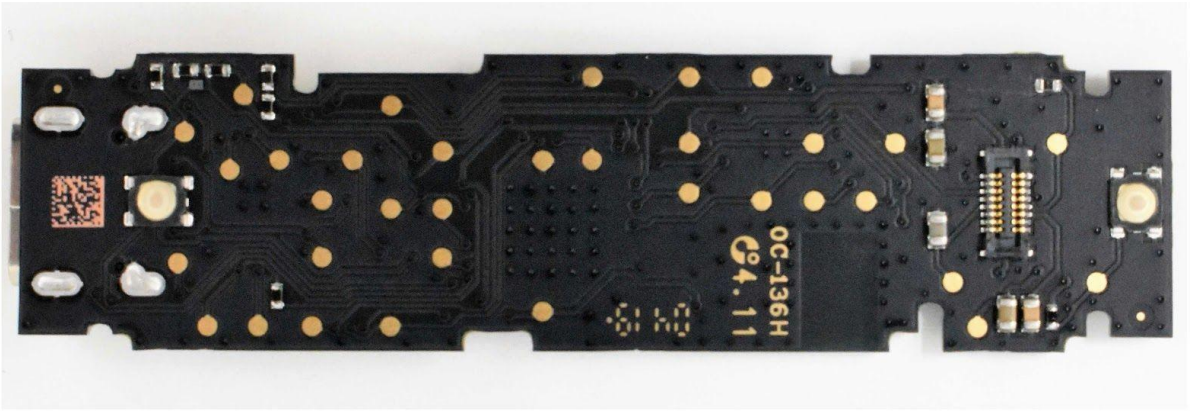
Révisions du matériel

Révision 1

- Circuit imprimé (PCB) noir



Face avant du circuit imprimé



Face arrière du circuit imprimé

Attestation de l'élément sécurisé

L'élément sécurisé est lui-même personnalisé en usine avec une attestation prouvant qu'il a été fabriqué par Ledger. Vous pouvez le vérifier en exécutant :

```
pip install --nocache-dir ledgerblue
```

Ensuite, sur la version 1.2.0 du micrologiciel

```
python -m ledgerBlue.checkGenuine --targetID 0x33000004
```

Le code source est disponible ici.

Vérification de l'application

Lors de l'ouverture d'une application, un avertissement "Non Genuine" (Non authentique) s'affiche si elle n'a pas été signée par Ledger. Une interface utilisateur modifiée (telle que celle visible à ce lien : https://github.com/LedgerHQ/nanos-ui) affichera également un message d'avertissement au démarrage.

Root of Trust

La Root of Trust (racine de confiance) pour le lot actuel est la clé publique secp256k1 suivante (vérifiable sur Genuine.py) :

```
0490f5c9d15a0134bb019d2afd0bf297149738459706e7ac5be4abc350a1f8
18057224fce12ec9a65de18ec34d6e8c24db927835ea1692b14c32e9836a75 dad609
```