Ledger Nano X

Bluetooth-fähige Hardware-Wallet

Benutzerhandbuch

Inhaltsverzeichnis

Versionsverwaltung

Version	Datum	Kommentare
1.0	07.03.2019	Erste Ausgabe zur Veröffentlichung.
1.1	25.03.2019	Kapitel hinzugefügt: Hardware-Integrität prüfen
1.2	23.05.2019	Aktualisierung des Abschnitts Sichern Ihrer PIN & Wiederherstellungsphrase
1.3	06.06.2019	Firmware-Version entfernen: targetID ist nicht mit Secure Element verknüpft

Ledger

Erste Schritte

Prüfen, ob das Gerät echt ist

Die Produkte von Ledger basieren auf einer Kombination aus Hardware- und Softwaresicherheit, die Ihre privaten Schlüssel vor einer Vielzahl von Angriffen schützen soll. Anhand dieses Leitfadens können Sie sicherstellen, dass Ihr Ledger Nano X echt und nicht gefälscht ist.
Einige einfache Prüfungen stellen sicher, dass Ihr Gerät ein echtes Ledger-Produkt ist:

- ✓ Ursprung des Ledger-Produkts
- ✓ Packungsinhalt
- ✓ Zustand des Wiederherstellungszettels
- ✓ Ausgangszustand des Ledger-Geräts.

Fortgeschrittene Benutzer, die die Hardware-Integrität überprüfen möchten, können zum Ende dieses Artikels springen.

Kaufen Sie bei einem offiziellen Ledger-Händler

Kaufen Sie Ihr Gerät direkt bei Ledger oder über das autorisierte Vertriebs- / Wiederverkäufernetz , um sicherzustellen, dass Sie ein authentisches Ledger-Produkt erhalten. Zu unseren offiziellen Vertriebskanälen gehören:

- Offizielle E-Commerce-Website: Ledger.com
- Offizielle Amazon-Stores: USA, Kanada, Vereinigtes Königreich, Deutschland, Frankreich, Spanien, Italien, Japan.

Ledger-Geräte, die von anderen Anbietern gekauft wurden, sind nicht unbedingt unseriös. Wir empfehlen jedoch dringend, die nachstehenden Sicherheitsprüfungen sorgfältig durchzuführen, um sicherzustellen, dass Ihr Ledger echt ist.

Prüfen Sie den Inhalt der Box

Der Lieferumfang einer Ledger-Hardware-Wallet sollte Folgendes umfassen:

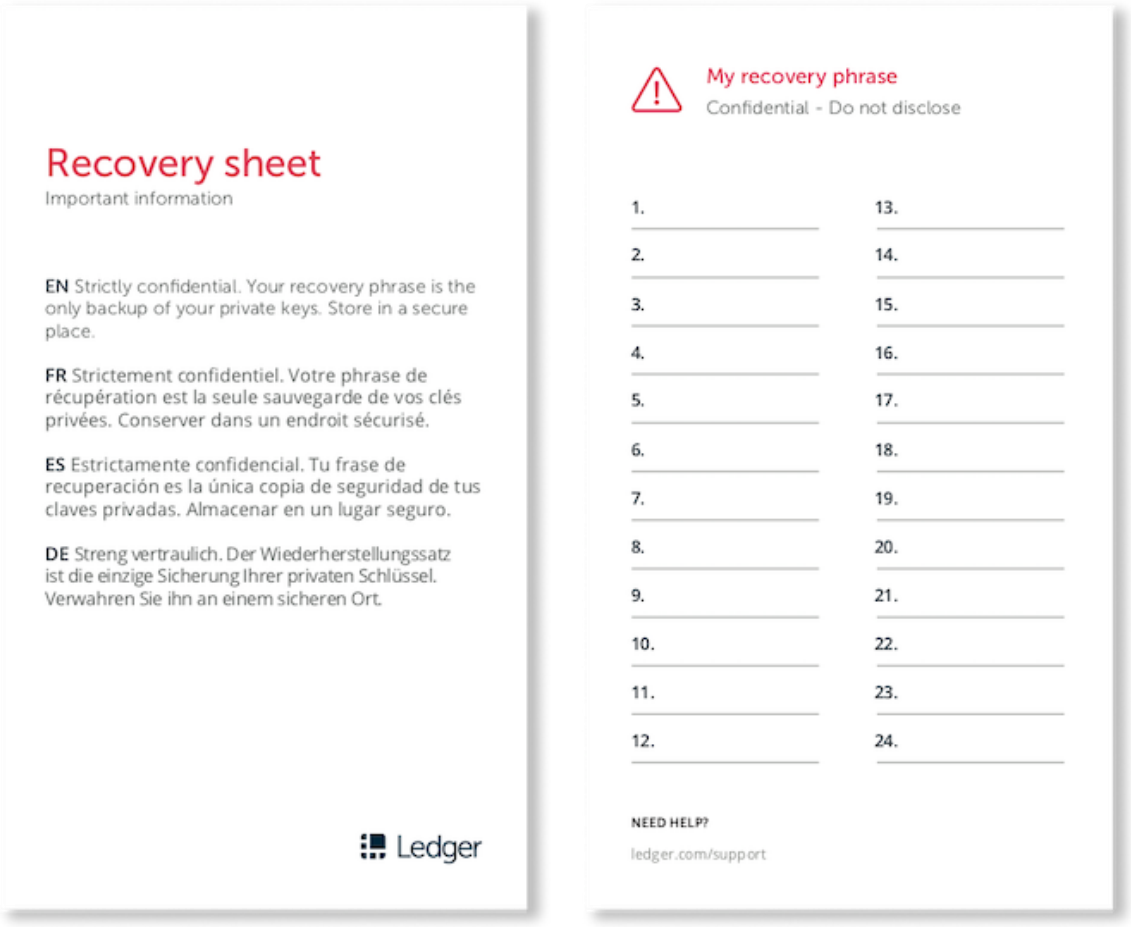
- Ledger Nano X
- USB Typ-C Kabel
- 3 Karten in einem Umschlag, einschließlich:
  - *Erste Schritte* Merkblatt;
  - *Gebrauchs-, Pflege- und Zulassungshinweise*;
  - 3 leere *Wiederherstellungszettel*.
- Zubehör: Schlüsselanhänger und Ledger-Aufkleber
- Verpackung: Karton und Banderole mit Ledger-Logo

Ledger Nano X Verpackungsinhalt

Überprüfen Sie, ob die Wiederherstellungszettel leer sind

Sobald Sie Ihren Ledger Nano X eingerichtet haben, generiert er eine neue Wiederherstellungsphrase mit 24 Wörtern, die Sie auf einen Wiederherstellungszettel schreiben sollten. Wenn jemand anderes Ihre Wiederherstellungsphrase kennt, können Sie alle Ihre Krypto-Werte verlieren. Befolgen Sie die nachstehenden Hinweise, um die Sicherheit Ihrer Vermögenswerte zu gewährleisten:

- Vergewissern Sie sich, dass Ihre Wiederherstellungszettel nicht ausgefüllt sind.
- Wenn auf Ihren Wiederherstellungszetteln bereits Wörter stehen: Das Gerät ist nicht sicher in der Anwendung.
  Bitte wenden Sie sich an den Ledger-Kundenservice, um Hilfe zu erhalten.
- Ledger stellt niemals eine 24-Wörter-Wiederherstellungsphrase in irgendeiner Form zur Verfügung. Akzeptieren Sie nur eine Wiederherstellungsphrase, die Sie auf dem Bildschirm Ihres Ledger Nano X erhalten haben.



Leerer Wiederherstellungszettel

Auf Werkseinstellungen prüfen

- Wenn Sie Ihren Ledger Nano X zum ersten Mal einschalten, sollte das Ledger-Logo angezeigt werden, und wenn Sie die Taste loslassen, erscheint die Meldung **Welcome to Ledger Nano X - Press right to continue** (Willkommen bei Ledger Nano X - Zum Fortfahren rechten Knopf drücken).
- Ledger stellt niemals einen PIN-Code in irgendeiner Weise zur Verfügung. Wählen Sie den PIN-Code immer selbst aus.
- Wenn ein PIN-Code in der Verpackung enthalten ist, oder irgendwelche Anweisungen, um diesen anderweitig zu erhalten, oder wenn das Gerät bei der ersten Verwendung bereits einen PIN-Code anfordert, bedeutet dies: Die Benutzung des Gerätes ist nicht sicher.
  Bitte wenden Sie sich an den Ledger-Kundenservice, um Hilfe zu erhalten.

Ledger Nano X: *Welcome* (Willkommen)

Authentizität mit Ledger-Anwendungen prüfen

- Richten Sie Ihr Ledger-Gerät mit Ledger Live ein, um seine Echtheit zu überprüfen.
- Echte Ledger-Geräte verfügen über einen geheimen Schlüssel, der bei der Herstellung festgelegt wird.
- Nur ein echtes Ledger-Gerät kann seinen Schlüssel verwenden, um den kryptografischen Nachweis zu erbringen, der für die Verbindung mit dem sicheren Server von Ledger erforderlich ist.

Zusammenfassung

- ✓ Überprüfen Sie, ob Ihre Wiederherstellungszettel leer sind.
- ✓ Richten Sie Ihren Ledger Nano selbst ein. Der Bildschirm **Welcome** (Willkommen) sollte beim ersten Start Ihres Geräts angezeigt werden.
- ✓ Wählen Sie Ihren eigenen PIN-Code.
- ✓ Wenden Sie sich im Zweifelsfall an den Ledger Kundenservice .

Weitere Informationen

Manipulationsschutzsiegel

Ledger verzichtet bewusst auf die Verwendung von Manipulationsschutzsiegeln auf seinen

Verpackungen. Diese Siegel sind leicht zu fälschen und können daher irreführend sein. Echte Ledger Geräte enthalten vielmehr einen sicheren Chip, der physische Manipulationen verhindert: Dies bietet eine stärkere Sicherheit als jeder Aufkleber es könnte.

Hardware-Integritätsprüfung

Fortgeschrittene Benutzer können die Hardware-Integrität auf der Innenseite ihres Ledger-Geräts überprüfen. Dieser Artikel bietet eine nicht erschöpfende Chronologie der verschiedenen Revisionen der Ledger Nano X-Version. Bitte beachten Sie, dass Sie Ihr Ledger-Gerät bei normaler Benutzung nicht öffnen müssen. Dies geschieht auf eigene Gefahr. Ledger kann nicht für mögliche Schäden haftbar gemacht werden, die durch das Öffnen des Geräts entstehen.

Als neues Gerät einrichten

Richten Sie Ihren Ledger Nano X als neues Gerät ein, um loszulegen. Ihr Gerät generiert neue private Schlüssel, die Zugriff auf Ihre Krypto-Werte bieten. Sie müssen außerdem eine neue 24-Wörter-Wiederherstellungsphrase aufschreiben.

Oder Sie können Ihr Gerät aus einer Wiederherstellungsphrase wiederherstellen, um die privaten Schlüssel wiederherzustellen, die mit einer vorhandenen Wiederherstellungsphrase verbunden sind.

Was Sie bereithalten sollten

- ✓ Ledger Nano X
- ✓ Entweder mindestens ein iOS 9- oder Android 7-Smartphone oder ein Computer mit mindestens Windows 8 (64-Bit), macOS 10.08 oder Linux
- ✓ Die Ledger Live-Anwendung,heruntergeladen und installiert

Anweisungen

Ledger Live bietet interaktive Installationshinweise. Starten Sie die App, um loszulegen.

Schritt 1. Als neues Gerät einrichten

1. Drücken Sie die Taste neben dem USB-Anschluss, bis das Ledger-Logo erscheint, um das Gerät einzuschalten.
2. Lesen Sie die Anweisungen auf dem Bildschirm. Drücken Sie die rechte Taste, um fortzufahren, oder die linke Taste, um zurückzugehen.
3. Drücken Sie beide gleichzeitig, wenn **Set up as new device** (Als neues Gerät einrichten) angezeigt wird.

Schritt 2. Wählen Sie Ihren PIN-Code aus

1. Drücken Sie beide Tasten, wenn **Choose PIN code** (PIN-Code auswählen) auf dem Gerät angezeigt wird.
2. Drücken Sie die linke oder rechte Taste, um eine Ziffer auszuwählen. Drücken Sie beide Tasten, um eine Ziffer zu bestätigen.
3. Wählen Sie , um Ihren PIN-Code aus 4 bis 8 Ziffern zu bestätigen. Wählen Sie , um eine Ziffer zu löschen.

4. Geben Sie den PIN-Code erneut ein, um ihn zu bestätigen.

Sicherheitstipps

- Wählen Sie Ihren eigenen PIN-Code. Mit diesem Code wird Ihr Gerät entsperrt.
- Verwenden Sie 8 Ziffern für optimale Sicherheit.
- Verwenden Sie niemals ein Gerät, das mit einem PIN-Code und/oder einer Wiederherstellungsphrase geliefert wurde.
- Wenden Sie sich im Zweifelsfall an den Ledger Kundenservice .

Schritt 3. Speichern Sie Ihre Wiederherstellungsphrase

Ihre 24-Wörter-Wiederherstellungsphrase wird nun Wort für Wort auf dem Bildschirm des Ledger Nano X angezeigt. Seien Sie vorsichtig, Ihre Wiederherstellungsphrase wird nur einmal angezeigt.

1. Nehmen Sie den leeren Wiederherstellungszettel, der in der Verpackung mitgeliefert wurde.
2. Drücken Sie beide Tasten, wenn **Write down your recovery phrase** (Wiederherstellungsphrase notieren) angezeigt wird.
3. Schreiben Sie **Wort #1** auf den Wiederherstellungszettel. Vergewissern Sie sich, dass Sie es korrekt in Position 1 eingetragen haben. Drücken Sie die rechte Taste, um zum nächsten Wort zu gelangen.
4. Wiederholen Sie den Vorgang, bis **Wort #24** auf Position 24 eingetragen ist. Drücken Sie beide Tasten auf dem letzten Bildschirm, um fortzufahren.
5. Drücken Sie beide Tasten, wenn **Confirm your recovery phrase** (Bestätigen Sie Ihre Wiederherstellungsphrase) angezeigt wird.
6. Wählen Sie das erste Wort, das Sie an Position 1 auf Ihrem Wiederherstellungszettel notiert haben, mit der linken oder rechten Taste aus. Bestätigen Sie das Wort durch das Drücken beider Tasten. Wiederholen Sie diesen Vorgang, um Ihre gesamte 24-Wörter-Wiederherstellungsphrase zu bestätigen.
7. **Your device is ready** (Gerät ist bereit) wird angezeigt, wenn Sie den Einrichtungsprozess erfolgreich abgeschlossen haben. Drücken Sie beide Tasten für den Dashboard-Zugang. Sie gelangen dann zum Dashboard.

Sicherheitstipps

- Stellen Sie sicher, dass Sie der einzige Inhaber Ihrer Wiederherstellungsphrase sind. Jeder, der Zugang dazu hat, kann Ihre Vermögenswerte an sich nehmen. Bewahren Sie sie deshalb sicher auf.
- Ledger speichert keine Sicherungskopie Ihrer 24 Wörter.
- Verwenden Sie niemals ein Gerät, das mit einer Wiederherstellungsphrase und/oder einem PIN-Code geliefert wurde.
- Wenden Sie sich im Zweifelsfall an den Ledger Kundenservice .

Nächste Schritte

Sie haben erfolgreich neue private Schlüssel auf Ihrem Gerät generiert, um eine neue Gruppe von Konten zu verwalten.

- Schauen Sie sich diese Tipps an, wie Sie Ihre Wiederherstellungsphrase und Ihren PIN-Code sichern können.
- Installieren Sie Apps auf Ihrem Gerät und fügen Sie Konten in Ledger Live hinzu.
- Empfangen und versenden Sie Krypto-Werte.

Wiederherstellen mit der Wiederherstellungsphrase

Stellen Sie ein Ledger Nano X Gerät anhand Ihrer Wiederherstellungsphrase wieder her, um ein Gerät wiederherzustellen, zu ersetzen oder zu klonen. Der Ledger Nano X stellt die Privaten Schlüssel wieder her, die durch Ihre vertrauliche Wiederherstellungsphrase gesichert wurden.

Alternativ dazu können Sie es auch als neues Gerät einrichten, um neue private Schlüssel zu generieren und eine neue Wiederherstellungsphrase zu notieren.

Was Sie bereithalten sollten

- ✓ Ledger Nano X.
- ✓ Halten Sie die Wiederherstellungsphrase zur Wiederherstellung bereit. BIP39/BIP44-Wiederherstellungsphrasen werden unterstützt
- ✓ Entweder mindestens ein iOS 9- oder Android 7-Smartphone oder ein Computer mit mindestens Windows 8 (64-Bit), macOS 10.8 oder Linux
- ✓ Die Ledger Live-App heruntergeladen und installiert.

Anweisungen

Ledger Live bietet interaktive Installationshinweise. Starten Sie die App, um loszulegen.

Schritt 1. Wiederherstellen mit der Wiederherstellungsphrase

1. Drücken Sie die Taste neben dem USB-Anschluss, bis das Ledger-Logo erscheint, um das Gerät einzuschalten.
2. Lesen Sie die Anweisungen auf dem Bildschirm. Drücken Sie die rechte Taste, um fortzufahren, oder die linke Taste, um zurückzugehen.
3. Drücken Sie beide Tasten gleichzeitig, wenn **Restore from recovery phrase** (Wiederherstellen aus Wiederherstellungsphrase) angezeigt wird.

Schritt 2. Wählen Sie Ihren PIN-Code aus

1. Drücken Sie beide Tasten, wenn **Choose PIN code** (PIN-Code auswählen) auf dem Gerät angezeigt wird.
2. Drücken Sie die linke oder rechte Taste, um eine Ziffer auszuwählen. Drücken Sie beide Tasten, um eine Ziffer zu bestätigen.
3. Wählen Sie , um Ihren PIN-Code aus 4 bis 8 Ziffern zu bestätigen. Wählen Sie , um eine Ziffer zu löschen.
4. Geben Sie den PIN-Code erneut ein, um ihn zu bestätigen.

Sicherheitstipps

- Wählen Sie Ihren eigenen PIN-Code. Mit diesem Code wird Ihr Gerät entsperrt.
- Verwenden Sie 8 Ziffern für optimale Sicherheit.
- Verwenden Sie niemals ein Gerät, das mit einem PIN-Code und/oder einer Wiederherstellungsphrase geliefert wurde.
- Wenden Sie sich im Zweifelsfall an den Ledger Kundenservice .

Schritt 3. Geben Sie Ihre Wiederherstellungsphrase ein

1. Wählen Sie die Länge Ihrer Wiederherstellungsphrase (12, 18 oder 24 Wörter). Drücken Sie zum Bestätigen beide Tasten.
2. Geben Sie die ersten Buchstaben von Wort #1 ein, indem Sie mit der rechten oder linken Taste auswählen. Drücken Sie beide Tasten, um jeden Buchstaben zu bestätigen.
3. Wählen Sie Wort #1 aus den vorgeschlagenen Wörtern aus. Drücken Sie beide Tasten, um das Wort zu bestätigen.
4. Wiederholen Sie den Vorgang bis zum letzten Wort Ihrer Wiederherstellungsphrase.
5. **Your device is ready** (Gerät ist bereit) wird angezeigt, wenn Sie den Einrichtungsprozess erfolgreich abgeschlossen haben. Drücken Sie beide Tasten für den Dashboard-Zugang. Sie gelangen dann zum Dashboard.

Sicherheitstipps

- Stellen Sie sicher, dass Sie der einzige Inhaber Ihrer Wiederherstellungsphrase sind. Jeder, der Zugang dazu hat, könnte Ihre Vermögenswerte an sich nehmen. Bewahren Sie sie deshalb sicher auf.
- Ledger speichert keine Sicherungskopie Ihrer 24 Wörter. Verwenden Sie niemals ein Gerät, das mit einer Wiederherstellungsphrase und/oder einem PIN-Code geliefert wurde.
- Wenden Sie sich im Zweifelsfall an den Ledger Kundenservice .

Ungültige Wiederherstellungsphrase?

- Stellen Sie sicher, dass die richtige Länge der Wiederherstellungsphrase ausgewählt ist. Geben Sie immer alle Wörter einer Wiederherstellungsphrase ein.
- Überprüfen Sie, ob die Reihenfolge der auf dem Gerät eingegebenen Wörter mit der Reihenfolge auf Ihrem Wiederherstellungszettel übereinstimmt.
- Überprüfen Sie, ob alle Wörter Ihrer Wiederherstellungsphrase in der BIP39 -Wortliste enthalten sind.

Nächste Schritte

Sie haben die privaten Schlüssel, die mit der Wiederherstellungsphrase Ihres Gerätes verknüpft sind, erfolgreich wiederhergestellt.

- Schauen Sie sich diese Tipps an, wie Sie Ihre Wiederherstellungsphrase und Ihren PIN-

Code sichern können.
- Installieren Sie Apps auf Ihrem Gerät und fügen Sie Konten in Ledger Live hinzu.
- Empfangen und versenden Sie Krypto-Werte.

Zugang zum „Control Center" (Kontrollzentrale)

Loggen Sie sich in das **Control Center** (Kontrollzentrale) auf Ihrem Ledger Nano X ein, um das Gerät zu sperren oder auszuschalten, die Akku- und Bluetooth-Einstellungen zu ändern und auf die Geräteeinstellungen zuzugreifen.

Navigieren im „Control Center" (Kontrollzentrale)

1. Halten Sie zu jeder beliebigen Zeit beide Tasten 3 Sekunden lang gedrückt, um das **Control Center** (Kontrollzentrale) zu öffnen. Der Akkustatus wird zuerst angezeigt.
2. Navigieren Sie im „Control Center" (Kontrollzentrale), indem Sie entweder die linke oder die rechte Taste drücken
3. Bestätigen Sie eine Auswahl durch das Drücken beider Optionen.
    - **Battery** (Batterie): aktueller Ladezustand.
    - **Lock device** (Gerät sperren): Drücken Sie beide Tasten, um den Bildschirmschoner anzuzeigen. Zum Freigeben ist die PIN erforderlich.
    - **Bluetooth:** Zeigt den Gerätenamen an, wenn Bluetooth aktiviert ist. Drücken Sie beide Tasten, um die Bluetooth-Verbindung zu deaktivieren oder zu aktivieren.
    - **Settings** (Einstellungen): Drücken Sie beide Tasten, um zu den **Settings** (Einstellungen) zu gelangen.
    - **Power off** (Ausschalten): Drücken Sie beide Tasten, um das Gerät auszuschalten.
    - **Close** (Schließen): Zurück zur vorherigen Aktivität.

Weitere Informationen

- Weitere Informationen zum Aufladen des Akkus.
- So koppeln Sie Ihren Ledger Nano X mit Ihrem Smartphone.
- Bitte wenden Sie sich an den Ledger-Kundenservice, um Hilfe zu erhalten.

Sichern Sie Ihre PIN und Wiederherstellungsphrase

Die Produkte von Ledger verfügen über eine Kombination aus Hardware- und Software-Sicherheitsfunktionen, die Ihre Krypto-Werte vor Angriffen schützen. Befolgen Sie die nachstehenden Richtlinien, um von dem optimalen Sicherheitsniveau Ihres Ledger Nano X-Geräts zu profitieren.

Sicheren Sie Ihren PIN-Code

Beim Konfigurieren wählen Sie eine PIN. IMMER

- Wählen Sie diesen PIN-Code selbst aus.
- Geben Sie Ihren PIN-Code diskret ein.
- Ändern Sie bei Bedarf Ihren PIN-Code. Weitere Informationen
- Denken Sie daran, dass ein dreimal nacheinander falsch eingegebener PIN-Code das Gerät automatisch zurücksetzt.

NIEMALS

- Einen einfachen PIN-Code wie 0000, 123456 oder 55555555 verwenden
- Ihren PIN-Code an andere Personen weitergeben.
- Einen PIN-Code verwenden, den Sie nicht selbst gewählt haben.
- Ihre PIN auf einem Computer oder Telefon speichern.

Sicheren Sie Ihre 24-Wörter-Wiederherstellungsphrase

Die 24-Wörter-Wiederherstellungsphrase ist die einzige Sicherheitskopie

für Ihre Krypto-Werte. IMMER

- Vergewissern Sie sich, dass Sie die 24-Wörter-Wiederherstellungsphrase dem Display des Geräts entnehmen.
- Erstellen Sie mehrere schriftliche Kopien der Wiederherstellungsphrase.
- Bewahren Sie die Kopien der Wiederherstellungsphrase an einem sicheren Ort auf, der nicht einsehbar ist.

NIEMALS

- Geben Sie die 24-Wörter-Wiederherstellungsphase auf Ihrem Computer oder Telefon ein.
- Ein Foto der 24-Wörter-Wiederherstellungsphrase machen.
- Ihre Wiederherstellungsphrase mit anderen Personen teilen.

Weitere Informationen

- Maximieren Sie die Sicherheit Ihres Kontos mit einer Passphrase (fortgeschrittene Benutzer).
- Bitte wenden Sie sich an den Ledger-Kundenservice , um Hilfe zu erhalten.

Senden und Empfangen

Kryptowährungen empfangen

Sie können Krypto-Werte auf Konten erhalten, die von Ihrem Ledger Nano X verwaltet werden, indem Sie eine Empfängeradresse in der Ledger Live App erstellen.

Sicherheitstipp

Senden Sie zuerst immer nur einen kleinen Betrag. Überprüfen Sie dann, ob die Transaktion ordnungsgemäß von der Empfängeradresse empfangen wurde, bevor Sie mit dem Senden größerer Beträge fortfahren.

Bevor Sie beginnen

- ✓ Ledger Live sollte einsatzbereit sein.
- ✓ Überprüfen Sie, ob die richtige App auf Ihrem Ledger Nano X installiert ist.
  Beispiel: Installieren Sie die Bitcoin-App, um Bitcoin zu empfangen.

Anweisungen

1. Tippen Sie unten in der App auf den Tab **Transact** (Transaktionen).
2. Tippen Sie auf **Receive** (Erhalten).
3. Wählen Sie das Konto aus, auf das Sie einzahlen möchten.
4. Wählen Sie den Ledger Nano X, auf welchem das Konto für die Gutschrift verwaltet wird.
   - Stellen Sie sicher, dass das Gerät eingeschaltet und entsperrt ist.
   - Öffnen Sie die Kryptowährungs-App wie in der Anweisung beschrieben.
5. Lesen Sie die Anweisungen auf dem Bildschirm und tippen Sie auf **Verify** (Verifizieren), um eine Empfängeradresse auf Ihrem Ledger Nano X anzuzeigen.
6. Sehen Sie sich die Adresse an und überprüfen Sie, ob sie mit der in Ledger Live angezeigten Adresse übereinstimmt.
   - Wenn die Adressen übereinstimmen: Drücken Sie die rechte Taste, um **Approve** (Genehmigen) zu wählen, dann
     drücken Sie beide Tasten, um die in Ledger Live angezeigte Adresse zu bestätigen.
7. Klicken Sie auf **Copy** (Kopieren) oder **Share** (Teilen) und geben Sie die Adresse an den Absender der Transaktion weiter. Achten Sie sorgfältig darauf, dass sich die Adresse nach dem Kopieren und Einfügen nicht ändert, oder tippen Sie auf die Schaltfläche **Re-verify** (Erneut verifizieren), um sie auf Ihrem Gerät erneut anzuzeigen.

Adressen stimmen nicht überein?

Wählen Sie **Reject** (Ablehnen) auf Ihrem Gerät und senden Sie keine Krypto-Werte an das Gerät.

Sie haben Ihr Gerät nicht dabei?

- Klicken Sie auf dem Bildschirm zur Auswahl des Kontos auf **Don't have your**

device? (Sie haben Ihr Gerät nicht dabei?) um eine Empfangsadresse zu generieren.

- Die generierte Empfangsadresse profitiert nicht von der optimalen Sicherheit, da die Adresse auf Ledger Live nicht auf Ihrem Ledger Nano X verifiziert ist

Warum sich Empfangsadressen ändern

Sie haben eine Adresse für das ausgewählte Konto erstellt, die Sie dem Absender mitteilen können.

- Blockchains, die auf Bitcoin basieren, sind öffentliche Netzwerke. Um einen optimalen Schutz der Privatsphäre zu gewährleisten, sollten die Adressen dieser Krypto-Werte nach einer Transaktion generell nicht wiederverwendet werden.
- Ledger Live generiert neue Adressen für Kryptowährungen, die auf Bitcoin basieren.
- Bei Kryptowährungen, die auf Bitcoin basieren, bleiben die bisherigen Adressen zwar gültig, bieten aber kein optimales Maß an Privatsphäre.

Kryptowährungen senden

Sie können Krypto-Werte von Adressen, die von Ihrem Ledger Nano X kontrolliert werden, mit der Ledger Live-Anwendung an eine Empfängeradresse senden.

Sicherheitstipp

Senden Sie zuerst immer nur einen kleinen Betrag. Überprüfen Sie dann, ob die Transaktion ordnungsgemäß von der Empfängeradresse empfangen wurde, bevor Sie mit dem Senden größerer Beträge fortfahren.

Bevor Sie beginnen

✓ Ledger Live ist einsatzbereit und Sie haben Krypto-Werte zu versenden.
✓ Überprüfen Sie, ob die richtige App auf Ihrem Gerät installiert ist.
Beispiel: Installieren Sie die Bitcoin-App, um Bitcoin zu versenden.

Transaktionsdetails eingeben

1. Tippen Sie unten in der App auf den Tab **Transact** (Transaktionen).
2. Tippen Sie auf **Send** (Senden).
3. Wählen Sie unter **Account** (Konto) das Konto aus, auf das Sie einzahlen möchten.
4. Tippen Sie auf **Scan QR-Code** (QR-Code scannen) oder geben Sie die **Recipient address** (Empfängeradresse) manuell ein.
   Für eine optimale Sicherheit sollten Sie immer darauf achten, dass Sie die Adressen doppelt überprüfen.
5. Geben Sie unter Amount den Betrag der zu sendenden Krypto-Werte oder den entsprechenden Gegenwert* *ein.*
6. Tippen Sie auf **Continue** (Weiter).

Verifizieren und signieren

1. Überprüfen Sie die Transaktionsdetails. Tippen Sie auf **Weiter**, um fortzufahren.
    - Tippen Sie auf **Edit** (Bearbeiten) in der Übersichtsanzeige, um die Netzwerkgebühren zu ändern.
    - Eine höhere Gebühr führt zu einer schnelleren Bearbeitung der Transaktion. Mehr erfahren...
2. Wählen Sie den Ledger Nano X, mit dem Sie senden möchten, und vergewissern Sie sich, dass er eingeschaltet und entsperrt ist.
3. Öffnen Sie die Kryptowährungs-App wie in der Anweisung beschrieben.
4. Tippen Sie auf **Continue** (Weiter).
5. Überprüfen Sie sorgfältig alle Transaktionsdetails auf Ihrem Gerät.
6. Drücken Sie beide Tasten, um die Transaktion zu validieren, wenn alles korrekt ist. Die Transaktion wird dann signiert und zur Bestätigung an das Netzwerk gesendet.
7. Klicken Sie auf View operation details (Vorgangsdetails anzeigen), um die Transaktion zu verfolgen, bis sie bestätigt wird.

Gegenwert

Der von Ihnen eingegebene Gegenwert wird in den Betrag des Krypto-Wertes konvertiert, der über einen Zwischenhändler in Bitcoin gesendet werden soll, wobei die in den Einstellungen ausgewählten Anbieter für den Wechselkurs verwendet werden. Standardmäßig werden die Anbieter von Wechselkursen mit dem höchsten 24h-Volumen ausgewählt.

Verifizieren der Transaktionsdetails

Bevor Sie Krypto-Werte senden und empfangen, machen Sie sich mit den sicheren Vorgängen vertraut, die Ihre Ledger Hardware-Wallet ermöglicht. Krypto-Werte, die Sie mit Ihrem Ledger-Gerät verwalten, können von böswilligen Akteuren ins Visier genommen werden. Optimieren Sie die Sicherheit Ihres Vermögens durch vorsichtiges Handeln bei Transaktionen.

Nicht vertrauen, verifizieren

Gehen Sie davon aus, dass Ihr Computer oder Smartphone kompromittiert ist. Sie sollten nur den Informationen vertrauen, die auf dem Bildschirm Ihres Ledger-Geräts angezeigt werden.

Senden

- Schicken Sie immer zuerst einen kleinen Betrag. Verifizieren Sie dann, ob die Transaktion ordnungsgemäß von der Empfängeradresse empfangen wurde, bevor Sie mit dem Senden größerer Beträge fortfahren.
- Verwenden Sie sekundäre Kommunikationsmittel, wenn Sie eine Adresse oder einen QR-Code des Empfängers erhalten.
  Beispiel: Überprüfen Sie die Einzahlungsadresse einer Börse per SMS, E-Mail oder einer Messaging-App, wenn möglich.
- Überprüfen Sie die Empfängeradressen, nachdem Sie sie kopiert und eingefügt haben. Schadsoftware auf Ihrem Computer
  oder Smartphone kann Adressen in Ihrer Zwischenablage ersetzen.
- Verifizieren Sie, dass die Adresse des Empfängers, der Betrag und die Gebühren korrekt sind und dass sie sowohl auf Ihrem Computer oder Smartphone als auch auf dem Display des Geräts übereinstimmen, wenn Sie eine Transaktion senden.

Empfangen

- Verifizieren Sie, ob jede Adresse, die für den Empfang von Transaktionen verwendet wird, Ihre eigene ist, indem Sie sie auf Ihrer Hardware-Wallet anzeigen lassen. Die in Ledger Live angezeigten Adressen könnten manipuliert werden, wenn Ihr Computer oder Smartphone kompromittiert ist.
- Warten Sie eine größere Menge an Bestätigungen ab, bevor Sie eine Transaktion akzeptieren.
  Für Bitcoin werden im Allgemeinen sechs Bestätigungen empfohlen.

Nicht verifizierte Adressen

Selbst wenn Ledger Live Empfängeradressen ohne ein Ledger-Gerät bereitstellen kann, bieten diese Adressen nur suboptimale Sicherheit. Die Verwendung ungeprüfter Adressen erfolgt auf Ihr eigenes Risiko.

Weitere Informationen

- Erfahren Sie, wie Sie Ihren PIN-Code und Ihre Wiederherstellungsphrase schützen können.
- Prüfen Sie die https://support.ledger.com/hc/en-us/articles/360019010313 erweiterten Sicherheitsfunktionen, die von Ledger-Geräten unterstützt werden.
- Wenden Sie sich im Zweifelsfall an den Ledger-Kundenservice.

Mining-Erlöse erhalten

Teilnehmer an Mining-Aktivitäten möchten ihre Mining-Erlöse möglicherweise sicher verstauen, indem sie ein Ledger-Gerät verwenden. Dieser Artikel erklärt, warum das Senden einer großen Menge kleinerer Transaktionen an eine Hardware-Wallet problematisch ist, bietet mögliche Lösungen an und liefert eine Anleitung, wie Sie Mining-Erlöse ordnungsgemäß an eine Adresse senden, die von Ihrem Ledger-Gerät kontrolliert wird.

Die Nichtbeachtung dieser Anweisungen kann dazu führen, dass Ihr Guthaben auf einem Ledger-Gerät nicht mehr zugänglich ist.

Das Empfangen von vielen kleinen Transaktionen ist problematisch

Der Empfang einer großen Anzahl von kleinen Zahlungen oder sogenannten *Dust-Payments*, auf einer Adresse, die von Ihrer Hardware-Wallet kontrolliert wird, verursacht folgendes:

- die Überlastung der Synchronisierung Ihrer Blockchain-Transaktionen; und
- eine extrem lange Dauer der Transaktionserstellung oder -validierung.

Daher eignen sich Hardware-Wallets nicht direkt für den Empfang einer großen Menge kleinerer Transaktionen, wie z.B. der Erlöse aus Mining-Aktivitäten.

Stellen Sie sich vor, Sie haben 1.000 Zahlungen von jeweils 0.001 BTC erhalten und Sie möchten insgesamt 1 BTC ausgeben. Der sichere Chip in der Hardware-Wallet muss dann eine Transaktion mit 1.000 Eingaben zusammenstellen und jede einzelne Eingabe signieren. Dies kann einige Stunden dauern oder gar nicht gelingen, da der Chip überhitzen oder einen Berechnungsfehler machen könnte.

Wenn Sie viele kleine Zahlungen erhalten haben

Wenn Sie bereits eine große Anzahl kleiner Zahlungen an Ihre Hardware-Wallet gesendet haben:

- Versuchen Sie Ihre Coins zu konsolidieren, indem Sie ein paar größere Zahlungen an sich selbst durchführen. Wenn Sie beispielsweise 1.000 Mal 0.001 BTC erhalten haben, konsolidieren Sie diese Eingaben, indem Sie 0.1 BTC an sich selbst senden und dies 10 Mal wiederholen.
- Alternativ dazu können Sie Ihre 24-Wörter-Wiederherstellungsphrase in eine Software-Wallet importieren, vorzugsweise eine Offline-Wallet, und Ihre komplette Wallet an eine Adresse senden, die von einem neu generierten Seed abgeleitet ist.

Batch-Transaktionen zur Vermeidung von Problemen

- Richten Sie eine Software-Wallet ein, die alle kleinen Zahlungen empfängt;
- Fassen Sie diese Erlöse regelmäßig zu einer größeren Transaktion zusammen, um sie an eine Hardware-Wallet zu senden.

Weitere Funktionen

Auto-Sperrung und Abschaltung einstellen

Aktivieren Sie die Funktionen **Auto-Lock** (Auto-Sperrung) oder **Auto-Power Off** (Auto-Abschaltung), um Ihr Ledger Nano X-Gerät nach einer gewissen Zeit der Inaktivität automatisch zu sperren oder abzuschalten. Zum Entsperren ist dann der PIN-Code erforderlich. Es wird empfohlen, die Auto-Sperrung oder Auto-Abschaltung für optimale Sicherheit zu aktivieren.

Anweisungen

Auto-Sperrung aktivieren

1. Schalten Sie Ihren Ledger Nano X ein und entsperren Sie das Gerät.
2. Halten Sie beide Tasten gedrückt, um das **Control Center**(Kontrollzentrale) aufzurufen.
3. Navigieren Sie zu **Settings** (Einstellungen). Drücken Sie dann beide Tasten zur Bestätigung.
4. Gehen Sie auf **Security** (Sicherheit) und drücken Sie zur Bestätigung auf beide Tasten.
5. Drücken Sie beide Tasten, um das Menü **Auto-lock** (Auto-Sperrung) aufzurufen.
6. Wählen Sie eine der folgenden Optionen:
    - „No auto lock“ (Keine Auto-Sperrung)
    - „1 minute“ (1 Minute)
    - „2 minutes“ (2 Minuten)
    - „5 minutes“ (5 Minuten)
    - „10 minutes“ (10 Minuten)
7. Drücken Sie beide Tasten, um die entsprechende Option für die Auto-Sperrung zu aktivieren.

Falls die Auto-Sperrung aktiviert ist, zeigt Ihr Gerät springende Ledger-Logos an, wenn das Gerät automatisch gesperrt wurde. Um das Gerät zu entsperren, drücken Sie eine beliebige Taste und geben Ihren PIN-Code ein.

Auto-Abschaltung aktivieren

1. Schalten Sie Ihren Ledger Nano X ein und entsperren Sie das Gerät.
2. Halten Sie beide Tasten gedrückt, um das **Control Center**(Kontrollzentrale) aufzurufen.
3. Navigieren Sie zu **Settings** (Einstellungen). Drücken Sie dann beide Tasten zur Bestätigung.
4. Gehen Sie auf **General** (Allgemein) und drücken Sie zur Bestätigung auf beide Tasten.
5. Drücken Sie beide Tasten, um das Menü **Auto power off** (Auto-Abschaltung) aufzurufen.
6. Wählen Sie eine der folgenden Optionen:
    - „Never power off“ (Niemals abschalten)
    - „1 minute“ (1 Minute)

- „3 minutes“ (3 Minuten)
- „5 minutes“ (5 Minuten)
- „10 minutes“ (10 Minuten)

7. Drücken Sie beide Tasten, um die ausgewählte Option zu aktivieren.

Wenn Sie die Auto-Abschaltung aktiviert haben, schaltet sich Ihr Gerät nach der eingestellten Dauer der Inaktivität automatisch ab.

Bluetooth-Verbindung einrichten

Richten Sie eine verschlüsselte Bluetooth-Verbindung zwischen Ihrem Ledger Nano X-Gerät und Ledger Live auf Ihrem Smartphone ein, um Ihre Krypto-Werte unterwegs zu verwalten. Alternativ kann Bluetooth deaktiviert werden, um die Verbindung nur über USB herzustellen.

Bluetooth-Verbindung

Verbinden Sie Ihren Ledger Nano X beim ersten Einrichten mit Ihrem Smartphone.

1. Vergewissern Sie sich, dass Bluetooth auf Ihrem Smartphone und auf Ihrem Ledger Nano X aktiviert ist.
   Starten Sie die Verbindung in Ledger Live Mobile.
2. Tippen Sie auf den Ledger Nano X, sobald es in Ledger Live Mobile verfügbar ist.
   Es kann einige Augenblicke dauern, bis auf beiden Geräten ein Kopplungscode angezeigt wird.
3. Wenn die Codes identisch sind, bestätigen Sie die Verbindung auf Ihrem Smartphone.
4. Drücken Sie beide Tasten an Ihrem Ledger Nano X, um die Kopplung zu bestätigen.
5. Drücken Sie beide Tasten, um Ledger Manager zuzulassen. Der Kopplungsvorgang ist abgeschlossen, sobald die Authentizität Ihres Ledger Nano X durch den sicheren Server von Ledger verifiziert wurde.

Die Verbindung bleibt in den globalen Einstellungen Ihres Smartphones erhalten. Der Pairing-Code muss erst dann erneut bestätigt werden, wenn Sie das Gerät in den Bluetooth-Einstellungen Ihres Smartphones vergessen haben.

Deaktivieren der Bluetooth-Verbindung

Standardmäßig ist Bluetooth aktiviert, sobald Sie Ihren Ledger Nano X eingerichtet haben.

1. Schalten Sie Ihren Ledger Nano X ein und entsperren Sie das Gerät.
2. Halten Sie beide Tasten gedrückt, um das **Control Center** (Kontrollzentrale) aufzurufen.
3. Navigieren Sie mit der rechten oder linken Taste zum Bluetooth-Symbol.
4. Drücken Sie beide Tasten, um Bluetooth zu deaktivieren. Der Bluetooth-Status wird als **disabled** (deaktiviert) angezeigt.
5. Die Einstellung wird beim nächsten Starten des Geräts wirksam.

Ledger Nano X ohne Bluetooth verwenden

So verwenden Sie ihren Ledger Nano X über USB:

- Desktop: Verwenden Sie das USB-C-Kabel, das mit dem Ledger Nano X geliefert wurde, um ihn an Ihren Desktop-Computer anzuschließen. Verwalten Sie Ihre Krypto mit Ledger Live Desktop oder einer anderen kompatiblen (Web-)App.
- Mobil: Verwenden Sie ein OTG-Kabel , um Ihren Ledger Nano X mit Ihrem Android zu verbinden
  Smartphone zu verbinden (iOS wird nicht unterstützt). Verwalten Sie Ihre Kryptowährungen mit Ledger Live Mobile oder einer anderen kompatiblen (Web-)App.

Ändern Sie Ihren PIN-Code

Der PIN-Code Ihres Ledger Nano X-Geräts verhindert den unbefugten Zugriff auf Ihre Kryptowährungen. Ihr PIN-Code wird bei der Ersteinrichtung des Geräts festgelegt, Sie können ihn jedoch jederzeit ändern.

Bevor Sie starten

✓ Ihr Gerät ist eingerichtet, und die neueste Firmware wurde installiert.
✓ Lesen Sie unseren Artikel über Sicherheit für PIN Codes und Wiederherstellungsphrasen .

Anweisungen

1. Schalten Sie Ihren Ledger Nano X ein und entsperren Sie das Gerät.
2. Halten Sie beide Tasten gedrückt, um das **Control Center** (Kontrollzentrale) aufzurufen.
3. Navigieren Sie zu **Settings** > **Security** > **Change PIN** (Einstellungen > Sicherheit > PIN ändern).
4. Wählen Sie einen neuen PIN-Code mit 4 bis 8 Ziffern aus.
5. Bestätigen Sie den neuen PIN-Code, indem Sie ihn erneut eingeben.
6. Geben Sie Ihren alten PIN-Code ein, um ihn zu bestätigen.
7. Der PIN-Code wurde nun erfolgreich geändert.

Sicherheitstipps

- Wählen Sie Ihren eigenen PIN-Code. Mit diesem Code wird Ihr Gerät entsperrt.
- Ein 8-stelliger PIN-Code bietet ein Höchstmaß an Sicherheit.
- Wählen Sie einen PIN-Code, der schwer zu erraten ist.

Weitere Informationen

- Maximieren Sie die Sicherheit Ihres Kontos mit einer Passphrase (fortgeschrittene Benutzer).
- Bitte wenden Sie sich an den Ledger-Kundenservice , um Hilfe zu erhalten.

Erweiterte Passphrasen-Sicherheit

Richten Sie eine Passphrase ein, um eine zusätzliche Sicherheitsebene für Ihre Krypto-Werte zu bilden. Diese Option wird nur fortgeschrittenen Benutzern empfohlen. Lesen Sie sich diesen Artikel vor dem Einrichten einer Passphrase sorgfältig durch.

Sicherheitstipp

Die Funktionen für Wiederherstellungs- und Passphrase ermöglichen die Einrichtung verschiedener Sicherheitsszenarien. Sie können so eine Sicherheitsstrategie entwerfen, die für Ihre persönliche Situation maßgeschneidert ist. Bitte vermeiden Sie dabei unnötige Komplexität. Eine Sicherheitsstrategie ist dann am besten, wenn Sie sie beherrschen und kompetent umsetzen können.

Wie die Passphrase funktioniert

Die 24-Wörter-Wiederherstellungsphrase, die bei der Ersteinrichtung Ihrer Ledger-Hardware-Wallet gespeichert wird, sichert die privaten Schlüssel, die Zugriff auf Ihre Konten ermöglichen. Sie müssen sie an einem sicheren Ort aufbewahren.

- Die Passphrase ist im Wesentlichen ein Passwort, das zu Ihrer 24-Wörter-Wiederherstellungsphrase hinzugefügt wird,
  das den Zugriff auf eine ganze Reihe neuer Konten ermöglicht.
- Diese Passphrase schützt Ihre Krypto-Werte, falls Ihre 24-Wörter-Wiederherstellungsphrase kompromittiert werden sollte. Um auf Konten zuzugreifen, die durch Passphrasen geschützt sind, benötigt ein Angreifer Ihre Wiederherstellungsphrase sowie Ihre geheime Passphrase.
- Jede einzelne Passphrase schaltet eine einzigartige Reihe von Konten frei. Sie können so viele
  Passphrasen verwenden, wie Sie möchten.

Bevor Sie starten

✓ Ihr Gerät ist eingerichtet, und die neueste Firmware wurde installiert.
✓ Stellen Sie sicher, dass Ihre Wiederherstellungsphrase wenn nötig verfügbar ist.
✓ Lesen Sie diesen Artikel vollständig, bevor Sie beginnen.

Anweisungen

Erste Schritte

1. Schließen Sie Ihr Ledger Nano X an und geben Sie Ihren PIN-Code ein.
2. Halten Sie beide Tasten gedrückt, um das **Control Center** (Kontrollzentrale) aufzurufen.
3. Navigieren Sie zum Menü **Settings** (Einstellungen).
4. Gehen Sie zu **Security** (Sicherheit).
5. Gehen Sie zu **Passphrase** und wählen Sie eine der beiden Optionen:
    - **Attach to PIN** (An PIN anhängen): Erstellt einen zweiten PIN-Code, um durch Passphrasen geschützte Konten zu entsperren.
    - **Set temporary** (Temporäre Einstellung): Geben Sie die Passphrase jedes Mal ein, wenn Sie auf Passphrasen-geschützte Konten zugreifen möchten.
6. Fahren Sie unten mit dem Abschnitt fort, der Ihrer gewählten Option entspricht

Option 1 - An den PIN-Code anhängen

Wie es funktioniert

Durch das Anhängen einer Passphrase an einen neuen PIN-Code werden neue Konten auf Ihrem Ledger Nano X erstellt, die auf einer geheimen Passphrase Ihrer Wahl basieren. Sie können nach Eingabe eines sekundären PIN-Codes auf die mit dieser Passphrase geschützten Konten zugreifen.

- Die Passphrase wird auf dem Gerät gespeichert, bis Sie sie mit einer anderen Passphrase überschreiben oder bis das Gerät zurückgesetzt wird.
- Bewahren Sie ein physisches Backup der geheimen Passphrase an einem sicheren Ort auf. Das Gerät kann sie nicht mehr anzeigen, nachdem Sie sie festgelegt haben.

Anweisungen

1. Wählen Sie die Option **Attach to PIN** (An PIN anhängen) aus dem Menü **Passphrase** in den Sicherheitseinstellungen des Geräts.
2. Drücken Sie beide Tasten, um die Option **Set secret passphrase** (Geheime Passphrase festlegen) auszuwählen.
3. Erstellen Sie einen zweiten PIN-Code.
4. Geben Sie den zweiten PIN-Code erneut ein, um ihn zu bestätigen.
5. Wählen und bestätigen Sie eine geheime Passphrase (max. 100 Zeichen).
6. Geben Sie Ihren primären PIN-Code ein, um ihn zu bestätigen.
7. Ihr Gerät verwaltet die Konten weiterhin basierend auf Ihrer

Wiederherstellungsphrase ohne Passphrase. Bitte schalten Sie das Gerät aus und geben Sie Ihren zweiten PIN-Code ein, um auf die Passphrase-geschützten Konten zuzugreifen.

Option 2 - Temporäre Passphrase festlegen

Wie es funktioniert

Die Verwendung einer temporären Passphrase ermöglicht den Zugang zu einer neuen Reihe von Konten auf Ihrem Ledger Nano X für die Dauer der Sitzung. Befolgen Sie die nachstehenden Anweisungen jedes Mal, wenn Sie auf die durch die Passphrase geschützten Konten zugreifen möchten.

- Die Konten basieren auf einer geheimen Passphrase Ihrer Wahl.
- Bewahren Sie ein physisches Backup der geheimen Passphrase an einem sicheren Ort auf. Das Gerät kann sie nach der Ersteinrichtung nicht mehr anzeigen.

Anweisungen

1. Wählen Sie im Menü **Passphrase** in den Sicherheitseinstellungen des Geräts die Option **Set temporary** (Temporäre Einstellung festlegen) aus.
2. Drücken Sie beide Tasten, um die Option **Set secret passphrase** (Geheime Passphrase festlegen) auszuwählen.
3. Wählen und bestätigen Sie eine geheime Passphrase (max. 100 Zeichen).
4. Geben Sie Ihren primären PIN-Code ein, um ihn zu bestätigen.
5. Ihr Gerät verwaltet nun die durch diese Passphrase geschützten Konten. Um auf Ihre primären Konten zuzugreifen, starten Sie bitte das Gerät neu und geben Sie wie gewohnt Ihren PIN-Code ein.

Passphrase-Konten wiederherstellen

Bei Verlust oder Zurücksetzen Ihres Ledger Nano X können Sie den Zugriff auf Ihre Kryptowährungen auf jedem Ledger-Gerät wiederherstellen, solange Sie sowohl Ihre 24-Wörter-Wiederherstellungsphrase als auch Ihre geheime Passphrase kennen.

Anweisungen

1. Nehmen Sie Ihre Wiederherstellungsphrase und Ihre Passphrase heraus.
2. Stellen Sie das Ledger-Gerät mithilfe Ihrer Wiederherstellungsphrase wieder her.
3. Befolgen Sie die obigen Anweisungen für eine temporäre Passphrase oder das Anhängen an einen PIN-Code, wobei Sie Folgendes beachten müssen:
    a. Temporäre Passphrase: Geben Sie einfach die Passphrase ein, die Sie zuvor eingerichtet haben, um auf die von dieser Passphrase geschützten Konten zuzugreifen.
    b. An PIN-Code anhängen: Sie können einen beliebigen PIN-Code wählen, aber Sie müssen die Passphrase eingeben, die Sie zuvor eingerichtet haben, um auf die durch diese Passphrase geschützten Konten zuzugreifen.

Passphrasen-Sicherheit in der Praxis

Glaubhafte Abstreitbarkeit

Um sich im Falle einer physischen Bedrohung zu schützen, sollten Sie sicherstellen, dass Ihr primärer PIN-Code nur einen kleinen Teil Ihrer Kryptowährungen freigibt. Richten Sie dann eine Passphrase ein, die mit einem PIN-Code verbunden ist, und sicheren Sie eine größere Menge an Kryptowährungen auf den Passphrasen-geschützten Konten.
Wenn Sie Ihren Ledger Nano X entsperren möchten, können Sie Ihren PIN-Hauptcode an den Angreifer aushändigen, während Sie den PIN-Code verstecken, der Ihre Passphrasen-geschützten Konten entsperrt.

Schutz der Wiederherstellungsphrase

Es ist eine gute Sicherheitspraxis, mehrere Kopien Ihres Wiederherstellungszettels aufzubewahren und diesen an verschiedenen geografischen Standorten sicher aufzubewahren. Um das Risiko zu mindern, Ihre Kryptowährungen zu verlieren, wenn eine der Kopien Ihres Wiederherstellungszettels kompromitiert wurde, können Sie eine weitere Passphrase einrichten. Wenn Sie dies tun, sollten Sie sicherstellen, dass Sie Papier-Sicherheitskopien Ihrer Passphrase an geografischen Orten aufbewahren, die sich von den Standorten unterscheiden, an denen Sie eine Sicherheitskopie Ihrer Wiederherstellungsphrase aufbewahren.

Weitere Informationen

- Erfahren Sie,wie Sie Ihre Kontosicherheit optimieren.
- Bitte wenden Sie sich an den Ledger-Kundenservice, wenn Sie Hilfe benötigen.

Maximierung der Akkulaufzeit

Der Ledger Nano X verfügt über einen 100-mAh-Lithium-Ionen-Akku, der bei voller Aufladung mehrere Stunden und im Leerlauf einige Monate hält. Befolgen Sie die Tipps in diesem Artikel, um die Akkulaufzeit und die Lebensdauer Ihres Ledger Nano X zu verlängern.

Aufladen des Akkus

Laden Sie den Akku 100 % auf, um die maximale Akkulaufzeit von mehreren Stunden zu erhalten. Schließen Sie den USB-C-Anschluss einfach an eine USB-Stromquelle an, um ihn aufzuladen. Das Batteriestatussymbol in der oberen rechten Ecke zeigt ein Ladesymbol

an.
Es ist nicht notwendig, den Akku vollständig zu entladen, bevor Sie ihn wieder aufladen. Die Lebensdauer des Akkus wird am besten dadurch verlängert, dass Sie Ihr Gerät aufladen, wann immer Sie können. Um den Ladezustand des Akkus zu überprüfen, halten Sie beide Tasten gedrückt, um das **Control Center** (die Kontrollzentrale) aufzurufen.

Maximieren der Akkulebensdauer

Wenn Sie Ihren Ledger Nano X länger aufbewahren möchten, wird die Akkulebensdauer am besten erhalten, indem Sie ihn alle paar Monate vollständig aufladen. Wenn das Gerät vollständig aufgeladen ist, schalten Sie es aus und bewahren Sie es an einem kühlen, trockenen Ort auf.
Am besten lagern Sie Ihren Ledger Nano X nicht für einen längeren Zeitraum mit sehr geringer Ladung, da sich dies negativ auf die Batteriekapazität auswirken kann.

Lebensdauer

Die Batterie ist für eine Lebensdauer von 5 Jahren ausgelegt. Ledger bietet kein Batterieaustauschprogramm an. Wenn die Akkukapazität so gering ist, dass sie praktisch nicht mehr genutzt werden kann, kann das Gerät über das USB-Kabel an eine Stromquelle angeschlossen werden.

Ihre Konten exportieren

Konten, die von einem Ledger Nano X erstellt wurden, können auf jeder Hardware- oder Software-Wallet (eines Drittanbieters) wiederhergestellt werden, die die gleichen Standards wie Ledger unterstützt (BIP32/BIP39/BIP44).

Bevor Sie beginnen

- ✓ Beachten Sie bitte, dass Ihre 24-Wörter-Wiederherstellungsphrase vollen Zugriff auf Ihre Konten bietet. Die Eingabe Ihrer Wiederherstellungsphrase auf einem Computer oder Smartphone kann unsicher sein. Vermeiden Sie dies, wenn möglich.
- ✓ Seien Sie vorsichtig bei der Auswahl einer Hardware- oder Software-Wallet (eines Drittanbieters). Der Schutz Ihrer Konten liegt in Ihrer eigenen Verantwortung.
- ✓ Wenden Sie sich im Zweifelsfall an den Ledger-Kundenservice.

Anweisungen

Verwenden Sie Ihre Wiederherstellungsphrase

1. Wählen Sie eine BIP39/BIP44-kompatible Hardware-Wallet oder Software-Wallet.
2. Halten Sie Ihre 24-Wort-Wiederherstellungphrase bereit.
3. Folgen Sie dem Handbuch des ausgewählten Geräts oder Dienstes, um Ihre Wiederherstellungsphrase (auch als *Mnemonic Seed* bezeichnet) zu importieren.

Kompatible Ledger-Geräte

- Ledger Nano X
- Ledger Nano S
- Ledger Blue
- Ledger Nano
- Ledger HW.1

Beliebige Liste von Drittanbieter-Software-Wallets

Software-Wallet Sicherheit

Software-Wallets sind höchst unsicher, wurden von Ledger keiner Sicherheitsprüfung unterzogen und sollten nur als letzter Ausweg zur Wiederherstellung verwendet werden. Wenn Sie weiter eine der unten aufgeführten Software-Wallets verwenden, übernehmen Sie Verantwortung für mögliche Auswirkungen.

- Mycelium (Smartphone)
- Electrum (desktop)
- Bither (Smartphone/Desktop)
- Coinomi (Smartphone)
- Jaxx Liberty (Smartphone)
- MyEtherWallet
- MyCrypto

Private Schlüssel generieren (fortgeschritten)
Fortgeschrittene Benutzer können alle privaten Schlüssel mit dem BIP39-Tool von Ian Coleman manuell generieren. Dieses Tool wird am besten für die Offline-Nutzung heruntergeladen, wie unten beschrieben.

Erstellen Sie Ihre privaten Schlüssel

1. Laden Sie das BIP39-Tool am Ende dieses Artikels herunter oder sehen Sie sich den Quellcode https://github.com/iancoleman/bip39 auf GitHub an.
2. Doppelklicken Sie auf die heruntergeladene Datei, um sie in einem Browser zu öffnen.
3. Geben Sie Ihre 24-Wörter-Wiederherstellungsphrase in das Feld*BIP39 Mnemonic* ein. Verwenden Sie nur Kleinbuchstaben.
4. Geben Sie Ihre Passphrase ein, wenn Sie eine in Ihrer Ledger-Hardware-Wallet festgelegt haben.
5. Wählen Sie eine Kryptowährung.
6. Lassen Sie das Feld **Internal/External** (Intern/Extern) auf 0 stehen.

Importieren Sie Ihre privaten Schlüssel

1. Kopieren Sie die Liste der generierten privaten Schlüssel aus dem Abschnitt *Derived Addresses* (Abgeleitete Adressen). Verwenden Sie die Steuerelemente unterhalb der Liste, um mehr Zeilen anzuzeigen oder bei einem bestimmten Index zu beginnen.
2. Importieren Sie Ihre privaten Schlüssel in eine Wallet eines Drittanbieters, die dies unterstützt, so wie MyEtherWallet oder Armory.
3. Setzen Sie das Feld **Internal/External** (Intern/Extern) auf 1 um die privaten Schlüssel Ihrer Wechselgeld-Adressen zu generieren.

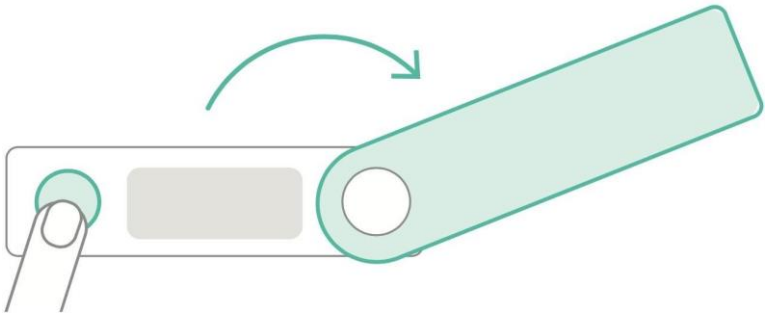
4. Importieren Sie die privaten Schlüssel, die mit Ihren Wechselgeldadressen verbunden sind, in die Wallet des Drittanbieters.

Zugang zu regulatorischen Informationen

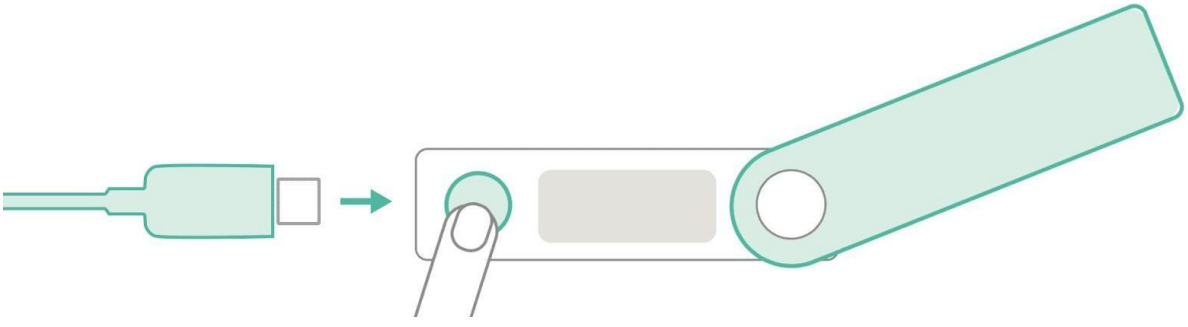
Es gibt zwei Möglichkeiten für den Zugriff auf regulatorische Informationen, je nachdem, ob das Gerät bereits eingerichtet wurde. Folgen Sie den Anweisungen für **Option 1,** wenn das Gerät noch auf Werkseinstellungen steht. Befolgen Sie alternativ die Anweisungen für **Option 2,** wenn das Gerät bereits eingerichtet wurde und Sie den vertraulichen PIN-Code als Besitzer des Geräts kennen.

Option 1 - Werkseinstellungen

1. Drehen Sie die Abdeckung des Gehäuses.

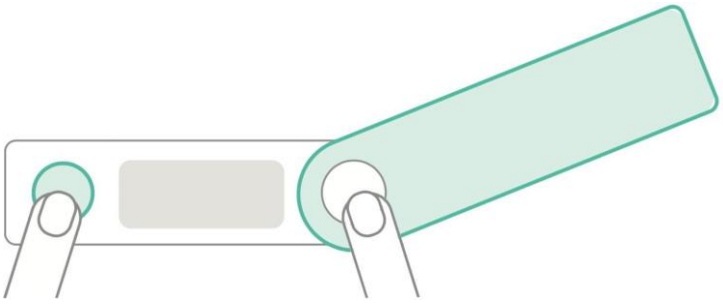


2. Halten Sie die Taste neben dem USB-Anschluss gedrückt, während Sie das Gerät über das mitgelieferte USB-C-Kabel an eine Stromquelle anschließen. Daraufhin wird das Ledger-Logo angezeigt.



3. Drücken Sie einmal die rechte Taste, um im Boot-Menü die Option **Regulatory info** (Regulatorische Informationen) auszuwählen**.**

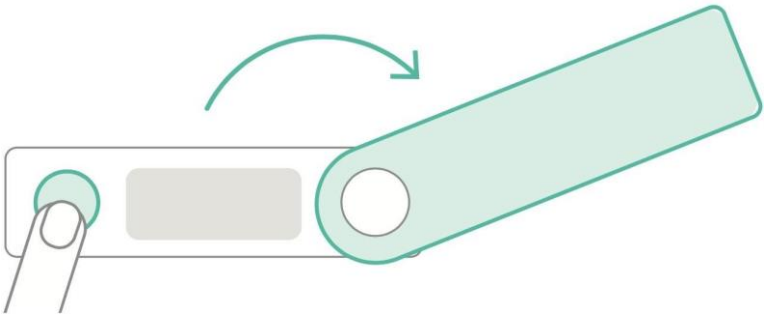
4. Drücken Sie beide Tasten gleichzeitig, um auf die **Regulatory info** (Regulatorische Informationen) zuzugreifen.



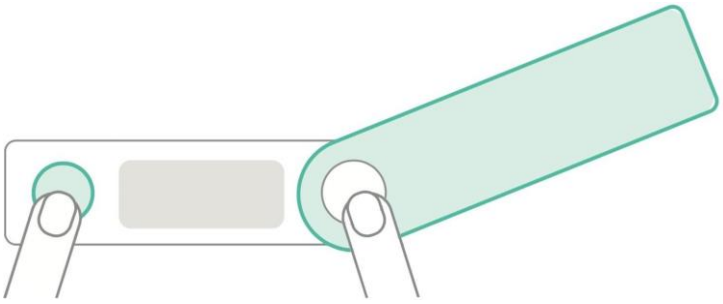
5. Drücken Sie die rechte Taste, um alle Informationen anzuzeigen.

Option 2 - Gerät in Betrieb

1. Drehen Sie die Abdeckung des Gehäuses. Drücken Sie die linke Taste, um das Gerät einzuschalten.



2. Geben Sie zum Freigeben des Geräts den vertraulichen PIN-Code des Nutzers ein.
3. Halten Sie beide Tasten gleichzeitig gedrückt, um das Control Center (Kontrollzentrale) vom Dashboard aus zu öffnen.



4. Drücken Sie die rechte Taste, bis **Settings** (Einstellungen) ausgewählt ist, und drücken Sie dann beide Tasten zur Validierung.

5. Drücken Sie beide Tasten gleichzeitig, um die **General Settings** (allgemeinen Einstellungen) aufzurufen.
6. Wählen Sie mit der rechten Taste die Option **Regulatory info** (Regulatorische Informationen) und drücken Sie dann zur Bestätigung beide Tasten.
6. Drücken Sie die rechte Taste, um alle Informationen anzuzeigenWählen Sie mit der rechten Taste die Option **Regulatory info** (Regulatorische Informationen) und drücken Sie dann zur Bestätigung beide Tasten.
7. Drücken Sie die rechte Taste, um alle Informationen anzuzeigen

Fehlersuche

Behebung von Verbindungsproblemen

Wenn Sie beim Versuch, Ihre Ledger Hardware-Wallet zu verbinden, auf Verbindungsprobleme stoßen, versuchen Sie die folgenden Lösungen der Reihe nach.

Mac, Windows oder Linux

1. Schließen Sie andere Anwendungen*(Ledger Apps, Krypto-Wallets, Geth, Parity, Mist, Bitcoin Core, etc).*
2. Schalten Sie VPN und Anti-Virus-Software aus.
3. Tauschen Sie, wenn möglich, das USB-Kabel aus.
4. Versuchen Sie es mit anderen USB-Anschlüssen.
5. Starten Sie Ihren Computer neu.
6. Versuchen Sie es auf einem anderen Computer.

Wenn das Problem weiterhin besteht, wählen Sie bitte unten Ihr System aus.

Windows

- Aktualisierung der Treiber für USB-Eingabegeräte
    1. Öffnen Sie **Devices and Printers** (Geräte und Drucker) in der Systemsteuerung.
    2. Doppelklicken Sie auf **Nano X** und öffnen Sie den Tab **Hardware**.
    3. Wählen Sie **USB Input Device** (USB-Eingabegerät) aus und klicken Sie auf **Properties** (Eigenschaften).
    4. Klicken Sie auf **Change Settings** (Einstellungen ändern).
    5. Klicken Sie auf den Tab **Driver** (Treiber).
    6. Klicken Sie auf **Update driver** (Treiber aktualisieren) und wählen Sie **automatic driver selection** (automatische Treiberauswahl) aus.
    7. Wiederholen Sie diesen Vorgang für beide USB-Eingabegeräte.
- Wenn es immer noch nicht funktioniert, versuchen Sie es bitte auf einem Mac, um zu verifizieren, dass Ihr Ledger Nano X richtig funktioniert.

Mac

Wenn Sie auf einem Mac Probleme mit der Verbindung haben, können Sie versuchen, Ledger Live vollen Zugriff auf die Festplatte zu geben:

1. Öffnen Sie die **System Preferences** (Systemeinstellungen).
2. Gehen Sie zu **Security & Privacy** (Sicherheit und Privatsphäre).
3. Fügen Sie auf dem Tab **Privacy** (Privatsphäre) Ledger Live auf der Liste **Full Disk Access** (Vollständiger Datenzugriff) hinzu.

Linux

Unter Linux müssen Sie eine Reihe von udev-Regeln erstellen, um den Zugriff auf Geräte zu ermöglichen. Einzelheiten dazu empfehlen wir Ihnen in der Chrome USB API Dokumentation. . Bitte folgen Sie den unten stehenden Anweisungen.

1. Einrichten

Prüfen Sie, ob die plugdev-Gruppe existiert, indem Sie den Befehl eingeben:

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

- Führen Sie die folgenden Schritte aus, wenn der vorherige Befehl kein Ergebnis geliefert hat
    1. Erstellen Sie die Gruppe plugdev:

       ```
       sudo groupadd plugdev
       ```

    2. Prüfen Sie mit dem Befehl, ob Sie in der Gruppe plugdev sind:

       ```
       groups
       ```

    3. Wenn die Ausgabe nicht plugdev enthält, befinden Sie sich nicht in der Gruppe plugdev. Geben Sie den folgenden Befehl ein:

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

    4. Hinweis: Ersetzen Sie <user> durch Ihren Nutzernamen, z.B. für den Nutzer „mike“ wäre das: sudo gpasswd -a mike plugdev.

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

    5. Melden Sie sich ab und wieder an, damit die Änderung wirksam wird. Um zu verifizieren, dass Sie jetzt in der plugdev-Gruppe sind, geben Sie ein:

       ```
       groups
       ```

    6. und suchen Sie nach dem Eintrag plugdev. Wenn er nicht vorhanden ist, haben Sie einen Schritt übersehen und sollten wieder bei Schritt 1 beginnen.

2. Fügen Sie die udev-Regeln hinzu

1. Geben Sie den folgenden Befehl ein, um die Regeln automatisch hinzuzufügen und udev neu zu laden: `wget -q -O - https://raw.githubusercontent.com/LedgerHQ/udev-rules/master/add_udev_rules.sh | sudo bash`

2. Versuchen Sie erneut, Ihren Ledger Nano X mit Ledger Live zu verbinden.

   Wenn es immer noch nicht funktioniert, fahren Sie mit Schritt 3 fort: Fehlersuche.

1. Fehlersuche

Probieren Sie jede der folgenden drei Optionen aus.

- Option 1
  Bearbeiten Sie die Datei /etc/udev/rules.d/20-hw1.rules, indem Sie den Parameter OWNER="<user>" zu jeder Zeile hinzufügen, wobei <user> Ihr Linux-Benutzername ist. Laden Sie dann die Regeln wie folgt neu:

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

  Versuchen Sie die Verbindung mit Ledger Live erneut. Wenn das nicht funktioniert, versuchen Sie die nächste Option.

- Option 2
  Bearbeiten Sie die Datei /etc/udev/rules.d/20-hw1.rules und fügen Sie die folgenden Zeilen hinzu:

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

  Laden Sie dann die Regeln neu:

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

  Versuchen Sie erneut, sich mit Ledger Live zu verbinden. Wenn es immer noch nicht funktioniert, versuchen Sie die letzte Option.

```
SUBSYSTEMS=="usb", ATTRS{idVendor}=="2c97",
SUBSYSTEMS=="usb", ATTRS{idVendor}=="2581",
```

- Option 3

  Wenn Sie mit Arch Linux arbeiten, können Sie die folgenden Regeln ausprobieren:

  ```
  /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"

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

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

  ATTRS{idProduct}=="0000", MODE="0660", TAG+="uaccess",
  TAG+="udev-acl"

  ATTRS{idProduct}=="0001", MODE="0660", TAG+="uaccess",
  TAG+="udev-acl”

  ATTRS{idProduct}=="0004", MODE="0660", TAG+="uaccess",
  TAG+="udev-acl"
  ```

  Laden Sie dann die Regeln neu und versuchen Sie erneut, eine Verbindung mit Ledger Live herzustellen:

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

iOS und Android

Wenn Sie Bluetooth-Probleme mit Ihrem Ledger Nano X haben, entfernen Sie bitte die

Kopplung und entfernen Sie den Ledger Nano X von Ihrem Telefon. Koppeln Sie die Geräte anschließend erneut.

Verbindungen auf Ihrem Ledger Nano X zurücksetzen

1. Schalten Sie Ihren Ledger Nano X ein und entsperren Sie das Gerät.
2. Halten Sie beide Tasten gedrückt, um das **Control Center** (Kontrollzentrale) aufzurufen.
3. Drücken Sie beide Tasten, um zum Menü **Security** (Sicherheit) zu navigieren.
4. Drücken Sie beide Tasten, um Reset Pairings (Pairings zurücksetzen) zu bestätigen.
5. Bestätigen Sie Reset Pairings (Pairings zurücksetzen) noch einmal.

Löschen Sie Ledger Nano X auf Ihrem Smartphone

1. Öffnen Sie die Bluetooth-Einstellungen Ihres Smartphones.
2. Wählen Sie die spezifischen Einstellungen für Ihren Ledger Nano X.
3. Das Gerät entfernen.

Jetzt können Sie die Verbindung wieder herstellen, indem Sie Ihren Ledger Nano X an jeder Stelle in Ledger Live Mobile auswählen, die eine Geräteverbindung erfordert, z.B. auf dem Tab Manager.

Verlorenes Gerät, PIN-Code oder Wiederherstellungsphrase

Wenn Sie keinen Zugriff auf Ihr Ledger Nano X-Gerät haben, Ihren PIN-Code vergessen oder die Wiederherstellungsphrase verloren haben, müssen Sie sofort die in diesem Artikel beschriebenen Schritte befolgen, um zu verhindern, dass Sie Ihre Kryptowährungen verlieren.

Stellen Sie sicher, dass Ihre Wiederherstellungsphrase sicher verwahrt bleibt. Schützen Sie Ihren vertraulichen PIN-Code und Ihre 24-Wörter-Wiederherstellungsphrase, um ein Höchstmaß an Sicherheit für Ihre Ledger-Hardware-Wallet zu gewährleisten.

Anweisungen

Sie können nicht auf Ihr Ledger-Gerät zugreifen?

1. Bei Verlust, Diebstahl oder Zerstörung Ihres Geräts stellen Sie bitte Ihre

Wiederherstellungsphrase https://support.ledger.com/hc/articles/360015132494auf einer beliebigen Hardware- oder Software-Wallet wieder her, die 24-Wörter-Wiederherstellungsphrasen unterstützt https://support.ledger.com/hc/en-us/articles/360019254093.

2. Sie brauchen den Wiederherstellungszettel, auf welchem Sie Ihre Wiederherstellungsphrase während der Einrichtung vermerkt haben.

Sie haben Ihren PIN-Code vergessen?

1. Ledger-Hardware-Wallets werden durch dreimalige Falscheingabe des PIN-Codes auf die Werkseinstellungen https://support.ledger.com/hc/en-us/articles/360019095214zurückgesetzt. Hierdurch werden die privaten Schlüssel aus ihrem sicheren Speicher gelöscht.
2. Nach dem Zurücksetzen können Sie einfach das Gerät wiederherstellen , indem Sie die Wiederherstellungsphrase verwenden.
3. Wählen Sie während des Wiederherstellungsvorgangs einen neuen PIN-Code.

Sie haben Ihre Wiederherstellungsphrase verloren?

Ihr Wiederherstellungszettel ist eine vollständige Sicherheitskopie der privaten Schlüssel, die Ihnen die Zugänglichkeit zu Ihren privaten Schlüsseln ermöglicht. Sie müssen sie an einem sicheren Ort aufbewahren. Jeder, der Zugriff auf Ihren Wiederherstellungszettel hat, kann Ihre Krypto-Werte verwenden, ohne den PIN-Code Ihres Geräts kennen zu müssen.

Wenn Sie Ihren Wiederherstellungszettel verloren haben:

1. Senden Sie alle Ihre Krypto-Werte sofort auf temporäre Konten, z. B. zu einem Börsendienst oder einer anderen Hardware-Wallet.
2. Geben Sie dreimal den falschen PIN-Code ein, um Ihren Ledger Nano X zurückzusetzen.
3. Richten Sie Ihren Ledger Nano X als neues Gerät ein.
4. Dann können Sie Ihre Krypto-Werte auf Ihr neu konfiguriertes Gerät zurück übertragen.

Zurücksetzen auf Werkseinstellungen

Wenn Sie das Gerät auf die Werkseinstellungen zurücksetzen, werden alle privaten Schlüssel, Anwendungen und Einstellungen von Ihrem Ledger Nano X entfernt. Sie können das Gerät zurücksetzen, um es als neues Gerät einzurichten, https://support.ledger.com/hc/en-us/articles/360015132494 um eine andere Wiederherstellungsphrase wiederherzustellen oder um das Gerät sicher an eine andere Person zu übertragen.

Bevor Sie starten

✓ Vergewissern Sie sich, dass Sie der alleinige Inhaber der aus 24 Wörtern bestehenden Wiederherstellungsphrase sind, mit der die privaten Schlüssel auf Ihrem Gerät gesichert werden.

Anweisungen

Haben Sie Ihren Wiederherstellungszettel?

Wenn Sie Ihr Gerät zurücksetzen, ohne den Wiederherstellungszettel zu besitzen, werden die privaten Schlüssel, die den Zugang zu Ihren Krypto-Werten ermöglichen, gelöscht. Sie werden dauerhaft den Zugriff auf Ihre Krypto-Werte verlieren.

Das Gerät kann entweder über das Einstellungsmenü oder durch Eingabe von drei falschen PIN-Codes zurückgesetzt werden, wenn es entsperrt wird. Bitte wählen Sie eine der beiden folgenden Optionen:

Zurücksetzen aus den Geräteeinstellungen

1. Schalten Sie Ihren Ledger Nano X ein und entsperren Sie das Gerät.
2. Halten Sie beide Tasten gedrückt, um das **Control Center** (Kontrollzentrale) aufzurufen.
3. Navigieren Sie zu **Settings** (Einstellungen)und drücken Sie beide Tasten, um zu bestätigen.
4. Navigieren Sie zu **General** (Allgemein) und drücken Sie beide Tasten, um zu validieren.

5. Wählen Sie **Reset all** (Alle zurücksetzen) aus, indem Sie beide Tasten drücken.
6. Lesen Sie die Warnungen, und wählen **Reset device** (Gerät zurücksetzen) aus, um es zu überprüfen.
7. Geben Sie zur Bestätigung Ihren PIN-Code ein. Ihr Gerät wird dann zurückgesetzt.

Zurücksetzen mit dem PIN-Code

1. Schalten Sie Ihren Ledger Nano X ein.
2. Geben Sie dreimal hintereinander einen falschen PIN-Code ein.
3. Als Sicherheitsmaßnahme wird das Gerät nach dem dritten falschen Versuch zurückgesetzt.

Nächste Schritte

Sie haben Ihr Gerät erfolgreich auf die Werkseinstellungen zurückgesetzt. Sie können nun entweder:

- Erfahren, wie Sie es als neues Gerät einrichten, um neue private Schlüssel zu erzeugen und zu sichern.
- Alternativ können Sie Ihr Gerät aus einer Wiederherstellungsphrase wiederherstellen, um die privaten Schlüssel wiederherzustellen, die mit einer vorhandenen Wiederherstellungsphrase verbunden sind.

Hardware-Integrität prüfen

Überprüfen Sie die Hardware-Integrität Ihres Ledger Nano X, um sicherzustellen, dass keine Manipulationen vorgenommen wurden. Dieser Artikel enthält detaillierte technische Informationen über die Sicherheit Ihres Geräts.

Achtung

Bitte behandeln Sie den Ledger Nano X mit hoher Sorgfalt, während Sie fortfahren. Beachten Sie bitte, dass Ihr Gerät nach dem Öffnen nicht mehr erstattungsfähig oder umtauschbar ist.

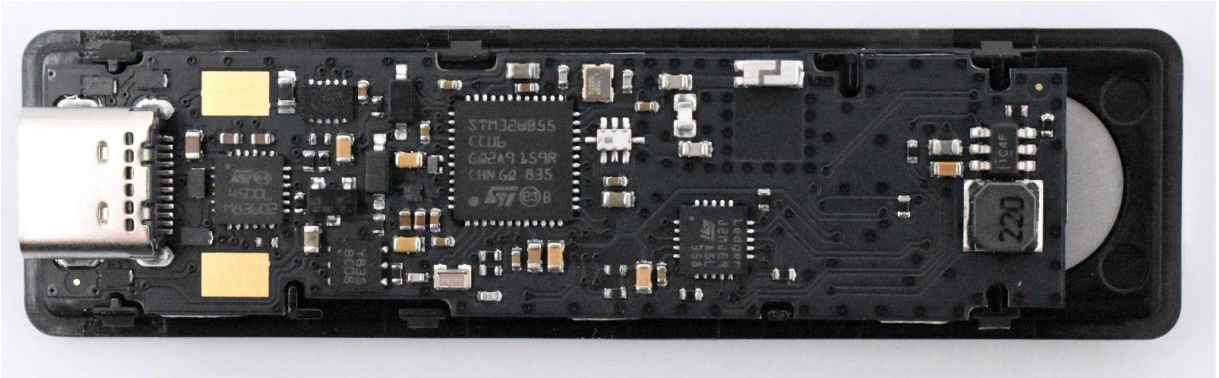
Microcontroller (MCU)

Das sichere Element (SE) überprüft den gesamten Flash-Speicher des Mikrocontrollers beim Hochfahren, wie in diesem Blog-Beitrag beschrieben. Wenn es verändert wurde, erhalten Sie beim Hochfahren eine Warnung. Als zusätzliche Prüfung können Sie das Gerät öffnen, um zu verifizieren, dass kein zusätzlicher Chip hinzugefügt wurde (siehe Bilder unten) und dass es sich bei der MCU um einen STM32WB55 handelt. Das Secure Element ist mit J2MJE9 gekennzeichnet.

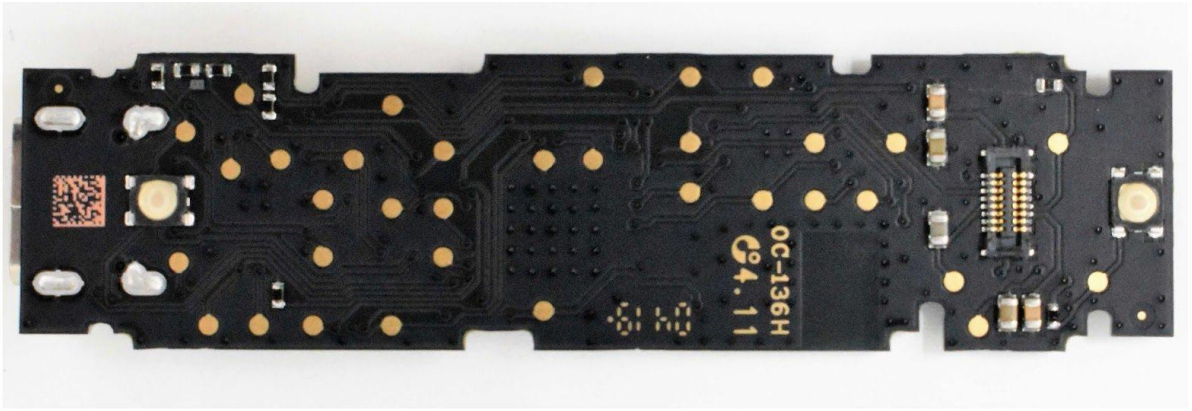
Hardware-Überarbeitungen

Revision 2

- Schwarzes PCB



Vorderseite des PCB



Rückseite des PCB

Bescheinigung des Secure Element

Das Secure Element selbst wird im Werk mit einer Bescheinigung personalisiert, die belegt, dass es von Ledger hergestellt wurde. Sie können dies überprüfen, indem Sie folgende Befehle ausführen:

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

```
python -m ledgerblue.checkGenuine --targetId 0x33000004
```

Der Quellcode ist hier verfügbar .

Überprüfung der Anwendung

Beim Öffnen einer Anwendung wird die Warnung Non Genuine (Nicht echt) angezeigt, wenn die App nicht von Ledger signiert wurde. Eine geänderte Benutzeroberfläche (wie unter https://github.com/LedgerHQ/nanos-ui zu finden) wird beim Booten ebenfalls eine Warnmeldung anzeigen.

Root of Trust

Die Root of Trust (Vertrauensgrundlage) für den aktuellen Batch ist der folgende öffentliche Schlüssel secp256k1, der mit Genuine.py überprüft wurde:

```
0490f5c9d15a0134bb019d2afd0bf297149738459706e7ac5be4abc350a1f818057224fce12ec9a65de18ec34d6e8c24db927835ea1692b14c32e9836a75dad609
```