

Ledger Nano X

Bluetooth-enabled hardware wallet

User Manual



Table of Contents

Table of Contents	1
Version control	5
Check if device is genuine	7
Set up as new device	11
Restore from recovery phrase	13
Access Control Center	14
Secure your PIN & recovery phrase	15
Receive crypto assets	18
Send crypto assets	19
Verify transaction details	20
Receive mining proceeds	21
Set auto-lock and power off	24
Set up Bluetooth connection	25
Change your PIN code	26
Advanced passphrase security	26
Maximize battery life	29
Export your accounts	30
Access regulatory information	32
Fix connection issues	36
Lost device, PIN code or recovery phrase	40
Reset to factory settings	41
Check hardware integrity	42
Use, Care and Regulatory Statement	45

Version control

Version	Date	Comments
1.0	07-03-2019	First issue for publication.
1.1	25-03-2019	Add chapter: Check hardware integrity
1.2	23-05-2019	Update Secure your PIN & recovery phrase section
1.3	06-06-2019	Removal firmware version: targetID is not linked to Secure Element

Getting Started

Check if device is genuine

Ledger products are built around a combination of hardware and software security, meant to protect your private keys from a wide range of attacks. Use this guide to make sure your Ledger Nano X is genuine, and not fraudulent or counterfeit.

A few simple checks will assure you that your device is a genuine Ledger product:

- ✓ Origin of the Ledger product
- ✓ Box contents
- ✓ Condition of the Recovery sheet
- ✓ Initial state of the Ledger device.

Advanced users wanting to check the hardware integrity can [jump](#) to the end of this article.

Buy from an official Ledger reseller

Purchase your device directly from Ledger or through the [authorized distributor / reseller network](#) to make sure you receive an authentic Ledger product. Our official sales channels include:

- Official e-commerce website: [Ledger.com](#)
- Official Amazon stores: [USA](#), [Canada](#), [United Kingdom](#), [Germany](#), [France](#), [Spain](#), [Italy](#), [Japan](#).

Ledger devices purchased from other vendors are not necessarily dubious. However, we do strongly recommend that you meticulously perform the safety checks below to ensure that your Ledger is genuine.

Check the box contents

The package of a Ledger hardware wallet should include:

- Ledger Nano X
- USB Type-C cable
- 3 paper cards in an envelope, including:
 - *Getting started* leaflet;
 - *Use, Care and Regulatory Statement*;
 - 3 blank *Recovery sheets*.
- Accessories: keychain and Ledger stickers
- Packaging: Ledger-branded cardboard box and sleeve



Ledger Nano X box contents

Check the Recovery sheets came blank

Once you set up your Ledger Nano X, it will generate a new 24-word recovery phrase for you to write down on a Recovery sheet. If someone else were to know your recovery phrase, you can lose all your crypto assets. Follow the guidelines below to ensure the security of your assets:

- Make sure your Recovery sheets came in blank.
- If your Recovery sheets already have words on them: The device is not safe to use.
Please contact [Ledger Support](#) for assistance.
- Ledger never provides a 24-word recovery phrase in any way, shape or form.
Only accept a recovery phrase obtained from the screen of your 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.





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

Blank Recovery sheet

Check for factory settings

- When turning on your Ledger Nano X for the first time, it should display the Ledger Logo, then release the button and then Welcome to Ledger Nano X - Press right to continue.
- Ledger never provides a PIN code in any way, shape or form. Always choose the PIN code yourself.
- If a PIN code is included in the packaging or instructions to get one elsewhere, or if the device requires a PIN code the first time you use it: the device is not safe to use.
Please contact [Ledger Support](https://support.ledger.com) for assistance.



Ledger Nano X: *Welcome*

Check authenticity with Ledger applications

- Set up your Ledger device with [Ledger Live](#) to verify its authenticity.
- Genuine Ledger devices hold a secret key that is set during manufacture.
- Only a genuine Ledger device can use its key to provide the cryptographic proof required to connect with Ledger's secure server.

Summary

- ✓ Check your Recovery sheets came in blank.
- ✓ Set up your Ledger Nano X by yourself. The Welcome screen should be displayed when first starting your device.
- ✓ Choose your own PIN code.
- ✓ Contact [Ledger Support](#) in case of doubt.

Learn more

Anti tamper seals

Ledger deliberately chooses not to use anti tamper seals on its packaging. These seals are easy to counterfeit and can therefore be misleading. Rather, genuine Ledger devices

contain a secure chip that prevents physical tampering: this provides stronger security than any sticker possibly could.

Hardware integrity check

Advanced users can check the hardware integrity on the inside of their Ledger device. This article provides a non-exhaustive chronology of the different revisions of the Ledger Nano X build. Please be aware that normal usage does not involve opening your Ledger device. Proceed to do so at your own risk. Ledger can not be held liable for any possible damage resulting from opening the device.

Set up as new device

Set up your Ledger Nano X as a new device to get started. It will generate new private keys so you can manage your crypto assets. You will also write down a new 24-word recovery phrase.

Alternatively, [restore your device from a recovery phrase](#) to recover the private keys linked to an existing recovery phrase.

What you'll need

- ✓ Ledger Nano X
- ✓ Either an iOS 9 or Android 7 smartphone or a computer with Windows 8 (64-bit), macOS 10.8, or Linux
- ✓ The Ledger Live application [downloaded](#) and installed



Instructions

Ledger Live features interactive setup instructions. Simply open the app to get started.

Step 1. Set up as new device

1. Press the button next to the USB port until the Ledger logo appears to turn on the device.
2. Read the on-screen instructions. Press the right button to proceed or the left button to go back.
3. Press both simultaneously when Set up as new device is displayed.

Step 2. Choose your PIN code

1. Press both buttons when Choose PIN code is displayed on the device.
2. Press the left or right button to select a digit. Press both buttons to validate a digit.
3. Select  to confirm your PIN code of 4 to 8 digits. Select  to erase a digit.

4. Enter the PIN code again to confirm it.

Security tips

- Choose your own PIN code. This code unlocks your device.
- Use 8 digits for optimal security.
- Never use a device supplied with a PIN code and/or a recovery phrase.
- Contact [Ledger Support](#) in case of doubt.

Step 3. Save your recovery phrase

Your 24-word recovery phrase will now be displayed word by word on the Ledger Nano X screen. Be careful, your recovery phrase will be displayed only once.

1. Take the blank Recovery sheet supplied in the box.
2. Press both buttons when Write down your recovery phrase is displayed.
3. Write down word #1 on the Recovery sheet. Verify that you have copied it correctly in position 1. Press the right button to move to the next word.
4. Repeat the process until Word #24 is written down in position 24. Press both buttons on the final screen to proceed.
5. Press both buttons when Confirm your recovery phrase is shown.
6. Select the first word that you've written down in position 1 on your Recovery sheet. with the left or right button. Validate the word by pressing both buttons. Repeat this to confirm your entire 24-word recovery phrase.
7. Your device is ready is shown once you've successfully completed the setup process. Press both buttons to Access Dashboard. You will then arrive on the Dashboard.

Security tips

- Ensure you are the only holder of your recovery phrase. Anyone with access to it could take your assets. Store it securely.
- Ledger does not keep a backup of your 24 words.
- Never use a device supplied with a recovery phrase and/or a PIN code.
- Contact [Ledger Support](#) in case of doubt.

Next steps

You've successfully generated new private keys on your device to manage a new set of accounts.

- Check [these tips](#) on how to secure your recovery phrase and PIN code.
- Install apps on your device and add accounts in Ledger Live.
- Receive and send crypto assets.

Restore from recovery phrase

Restore a [Ledger Nano X](#) device from your recovery phrase to restore, replace or clone a device. The Ledger Nano X will recover the private keys backed up by your confidential recovery phrase.

Alternatively, [set up as a new device](#) to generate new private keys and write down a new recovery phrase.

What you'll need

- ✓ Ledger Nano X.
- ✓ Get the recovery phrase to restore. BIP39/BIP44 recovery phrases are supported.
- ✓ Either at least an iOS 9 or Android 7 smartphone or a computer with at least Windows 8 (64-bit), macOS 10.8, or Linux.
- ✓ The Ledger Live application [downloaded](#) and installed.



Instructions

Ledger Live features interactive setup instructions. Simply open the app to get started.

Step 1. Restore from recovery phrase

1. Press the button next to the USB port until the Ledger logo appears to turn on the device.
2. Read the on-screen instructions. Press the right button to proceed or the left button to go back.
3. Press both simultaneously when Restore from recovery phrase is displayed.

Step 2. Choose your PIN code

1. Press both buttons when Choose PIN code is displayed on the device.
2. Press the left or right button to select a digit. Press both buttons to validate a digit.
3. Select  to confirm your PIN code of 4 to 8 digits. Select  to erase a digit.
4. Enter the PIN code again to confirm it.

Security tips

- Choose your own PIN code. This code unlocks your device.
- Use 8 digits for optimal security.
- Never use a device supplied with a PIN code and/or a recovery phrase.
- Contact [Ledger Support](#) in case of doubt.

Step 3. Enter your recovery phrase

1. Choose the length of your recovery phrase (12, 18 or 24 words). Press both buttons to validate.
2. Enter the first letters of Word #1 by selecting them with the right or left button. Press both buttons to validate each letter.
3. Choose Word #1 from the suggested words. Press both buttons to validate it.
4. Repeat the process until the last word of your recovery phrase.
5. Your device is ready is shown once you've successfully completed the setup process. Press both buttons to Access Dashboard. You will then arrive on the Dashboard.

Security tips

- Ensure you are the only holder of your recovery phrase. Anyone with access to it could take your assets. Store it securely.
- Ledger does not keep a backup of your 24 words. Never use a device supplied with a recovery phrase and/or a PIN code.
- Contact [Ledger Support](#) in case of doubt.

Invalid recovery phrase?

- Make sure the correct recovery phrase length is selected. Always enter all words of a recovery phrase.
- Verify that the order of the words entered on the device matches the order on your Recovery sheet.
- Check that all the words of your recovery phrase are on the [BIP39 word list](#).

Next steps

You've successfully restored the private keys linked to the recovery phrase on your device.

- Check [these tips](#) on how to secure your recovery phrase and PIN code.
- Install apps on your device and add accounts in Ledger Live.
- Receive and send crypto assets.

Access Control Center

Access the Control Center on your Ledger Nano X device to lock or turn off your device, to manage the battery and Bluetooth, and to access device settings.

Navigate the Control Center

1. Hold both buttons for 3 seconds at any time to open the Control Center. The battery status will be appear first.
2. Navigate the Control Center by pressing either the left or right button.

3. Validate a selection by pressing both options.
 - Battery: current charge level.
 - Lock device: Press both buttons to show screen saver. Require the PIN to unlock.
 - Bluetooth: Shows device name when Bluetooth is enabled. Press both buttons to disable or enable Bluetooth connectivity.
 - Settings: Press both buttons to enter the Settings.
 - Power off: Press both buttons to power off.
 - Close: Return to the previous activity.

Learn more

- Learn about charging the battery.
- How to pair your Ledger Nano X with your smartphone.
- Contact [Ledger Support](#) if you need assistance.

Secure your PIN & recovery phrase

Ledger products have a combination of hardware and software security features to protect your crypto assets from attacks. Follow the guidelines below to benefit from the optimal level of security offered by your Ledger Nano X device.

Secure your PIN code

During the initialization process you choose a PIN.

ALWAYS

- Choose a PIN code by yourself.
- Enter your PIN code discreetly.
- Change your PIN code if needed. [Learn more](#)
- Remember that three wrong PIN code entries in a row will reset the device.

NEVER

- Use an easy PIN code like 0000, 123456, or 55555555.
- Share your PIN code with anyone else.
- Use a PIN code you did not choose yourself.
- Store your PIN code on a computer or phone.

Secure your 24-word recovery phrase

The 24-word recovery phrase is the only backup to your crypto assets.

ALWAYS

- Ensure your 24-word recovery phrase is obtained from the device screen.
- Create multiple written copies of the recovery phrase.
- Store the copies of the recovery phrase in secure locations, out of sight.

NEVER

- Enter the 24-word recovery phrase into your computer or phone.
- Take a picture of the 24-word recovery phrase.
- Share your recovery phrase with anyone else.

Learn more

- Maximize your account security [with a passphrase](#) (advanced users).
- Contact [Ledger Support](#) in case you require assistance.

Send & Receive

Receive crypto assets

You can receive crypto assets on accounts managed by your Ledger Nano X device by generating a receive address in the Ledger Live app.

Security tip

Always send a small amount first. Then verify that the transaction was properly received by the recipient address before proceeding to send larger amounts.

Before you begin

- ✓ Ledger Live should be ready to use.
- ✓ Check that the right app is installed on your Ledger Nano X.
Ex: install the Bitcoin app to receive Bitcoin.

Instructions

1. Tap the Transact tab at the bottom of the app.
2. Tap Receive.
3. Choose the Account to credit.
4. Choose the Ledger Nano X that manages the account to credit.
 - Make sure the device is turned on and unlocked.
 - Open the crypto asset app as instructed.
5. Read the on-screen instructions and tap on Verify to display a receive address on your Ledger Nano X.
6. View the address and verify that it is the same as the address shown in Ledger Live.
 - If the addresses match: Press the right button to select Approve, then press both buttons to confirm the address shown in Ledger Live.
7. Click Copy or Share and share the address with the sender of the transaction. Carefully check that the address does not change after you copy and paste it or tap the Re-verify button to display on your device again.

Addresses don't match?

Select Reject on your device and do not send any crypto assets to it.

Don't have your device?

- On the account selection screen, click on Don't have your device? to generate a receive address.
- The generated receive address does not benefit from the optimal level of security because the receive address on Ledger Live is not verified on your Ledger Nano X.

Why receive addresses change

You've generated an address for the selected account, that you can share with the sender.

- Blockchains based on Bitcoin are public networks. For optimal privacy, the addresses of those crypto assets should generally not be re-used after a transaction.
- Ledger Live generates new addresses for crypto assets based on Bitcoin.
- For crypto assets based on Bitcoin, the previous addresses do remain valid, but they don't offer an optimal level of privacy.

Send crypto assets

You can send crypto assets from addresses controlled by your Ledger Nano X to a recipient address with the Ledger Live application.

Security tip

Always send a small amount first. Then verify that the transaction was properly received by the recipient address before proceeding to send larger amounts.

Before you begin

- ✓ Ledger Live is ready to use and you've got crypto assets to send.
- ✓ Check that the right app is installed on your device.
Ex: install the Bitcoin app to send Bitcoin.

Enter transaction details

1. Tap the Transact tab at the bottom of the app.
2. Tap Send.
3. Choose the Account to debit.
4. Tap Scan QR Code or manually enter the Recipient address.
For optimal security, always make sure to [double-check addresses](#).
5. Enter the Amount of the crypto asset to send, or its countervalue*.
6. Tap Continue.

Verify and sign

1. Check the transaction details. Tap continue to proceed.
 - Tap edit on the summary screen to change the Network fees.
 - A higher fee leads to a faster processing of the transaction. [Learn more...](#)
2. Choose the Ledger Nano X to send with while making sure it's turned on and unlocked.
3. Open the crypto asset app as instructed.
4. Tap Continue.

5. Carefully verify all transaction details on your device.
6. Press both buttons to validate the transaction if everything is correct. The transaction is then signed and sent to the network for confirmation.
7. Click View operation details to [track the transaction](#) until it gets confirmed.

Countervalue

The countervalue you enter is converted to the amount of the crypto asset to send through an intermediary exchange to Bitcoin using the exchange rate providers selected in Settings. By default, the rate providers with the highest 24h-volume are selected.

Verify transaction details

Before sending and receiving crypto assets, familiarize yourself with the secure operations enabled by your Ledger hardware wallet. Crypto assets you manage using your Ledger device can be targeted by malicious actors. Optimize your asset security by transacting with caution.

Don't trust, verify

Assume that your computer or smartphone is compromised. You should only trust information displayed on your Ledger device's screen.

Sending

- Always send a small amount first. Then verify that the transaction was properly received by the recipient before proceeding to send larger amounts.
- Use secondary communication means when obtaining a recipient address or QR code.
Example: double-check an exchange deposit address through SMS, email or a messaging app when possible.
- Check recipient addresses after you copy and paste. Malware on your computer or smartphone might replace addresses in your clipboard.
- Verify that the recipient address, amount and fees are correct and that they are the same on both your computer or smartphone and the device's screen when sending a transaction.

Receiving

- Verify that each address used to receive transactions belongs to you by displaying it on your hardware wallet. Addresses shown in Ledger Live could be manipulated if your computer or smartphone is compromised.
- Wait for a significant amount of confirmations before accepting a transaction. For Bitcoin, six confirmations are generally recommended.

Unverified addresses

Even if Ledger Live can provide receiving addresses without a Ledger device, these addresses provide suboptimal security. Choosing to use unverified addresses comes at your own risk.

Learn more

- Learn how to [secure your PIN code and recovery phrase](#).
- Check the [advanced security features](#) supported by Ledger devices.
- Contact [Ledger Support](#) when in doubt.

Receive mining proceeds

Participants in mining activities may want to securely store their mining proceeds by using a Ledger device. This article explains why sending a large amount of small transactions to a hardware wallet is troublesome, offers potential solutions and provides instructions on how to properly send mining proceeds to an address controlled by your Ledger device.

Failing to follow these instructions may lead to your funds becoming inaccessible on a Ledger device.

Receiving many small transactions is troublesome

Receiving a large number of small payments, or *dust payments*, on an address controlled by your hardware wallet causes:

- the saturation of the synchronization of your Blockchain transactions; and
- an extremely long duration of transaction construction or validation.

Therefore, hardware wallets are not directly suited for receiving a large amount of small transactions, such as the proceeds of mining activities.

Imagine that you have received 1,000 payments of 0.001 BTC and that you want to spend the total of 1 BTC. The secure chip in the hardware wallet will then have to construct a transaction of 1,000 inputs and sign each single input. This might take a few hours or might not succeed at all, since the chip may overheat or make a computation error.

If you've received a lot of small payments

If you have already sent a large number of small payments to your hardware wallet:

- Try to consolidate your coins by sending a few larger payments to yourself. For example, if you have received 1,000 times 0.001 BTC, consolidate these inputs by sending 0.1 BTC to yourself and repeat this 10 times.

- Alternatively, import your 24-word recovery phrase into a software wallet, preferably an offline one, and empty your wallet into an address that is derived from a newly generated seed.

Batch transactions to prevent problems

- Set up a software wallet that receives the small payments;
- Regularly batch these proceeds into a larger transaction to send onto a hardware wallet.

More features

Set auto-lock and power off

Set auto-lock or auto-power off to automatically lock or shutdown your Ledger Nano X device after a period of inactivity. The PIN code is then required to unlock it. It is recommended to enable auto-lock or auto-power off for optimal security.

Instructions

Enable auto-lock

1. Turn on and unlock your Ledger Nano X.
2. Hold both buttons to access Control Center.
3. Navigate to Settings. Then press both buttons to validate.
4. Go to Security and press both buttons to validate.
5. Press both buttons to enter the Auto-lock menu.
6. Select one of the following options:
 - No auto lock
 - 1 minute
 - 2 minutes
 - 5 minutes
 - 10 minutes
7. Press both buttons to activate the corresponding auto-lock option.

If you've enabled auto-lock your device will show bouncing Ledger logos when it's been locked automatically. To unlock, any button and enter your PIN code.

Enable auto power off

1. Turn on and unlock your Ledger Nano X.
2. Hold both buttons to access Control Center.
3. Navigate to Settings. Then press both buttons to validate.
4. Go to General and press both buttons to validate.
5. Press both buttons to enter the Auto power off menu.
6. Select one of the following options:
 - Never power off
 - 1 minute
 - 3 minutes
 - 5 minutes
 - 10 minutes
7. Press both buttons to activate the selected option.

If you've enabled auto power off your device will automatically turn off after the configured duration of inactivity.

Set up Bluetooth connection

Set up an [encrypted Bluetooth connection](#) between your Ledger Nano X device and Ledger Live on your smartphone to manage your crypto assets on the go. Alternatively, Bluetooth can be disabled to connect via USB only.

Bluetooth pairing

Pair your Ledger Nano X the first time you set it up with your smartphone.

1. Make sure Bluetooth is enabled on your smartphone and on your Ledger Nano X. Start the pairing in Ledger Live mobile.
2. Tap on the Ledger Nano X once it's available in Ledger Live mobile. It may take a few moments for a pairing code to be displayed on both devices.
3. If the codes are the same, confirm the pairing on your smartphone.
4. Press both buttons on your Ledger Nano X to confirm the pairing.
5. Press both buttons to Allow Ledger Manager. The pairing is complete after the authenticity of your Ledger Nano X has been checked by Ledger's secure server.

The pairing persists in your global smartphone settings. The pairing code does not have to be confirmed again until you forget the device in the Bluetooth settings of your smartphone.

Disable Bluetooth connectivity

By default, Bluetooth is enabled once you've set up your Ledger Nano X.

1. Turn on and unlock your Ledger Nano X.
2. Hold both buttons to access the Control Center.
3. Navigate to the Bluetooth symbol using the right or left button.
4. Press both buttons to disable Bluetooth. The Bluetooth status displays disabled.
5. The setting takes effect the next time you start the device.

Use your Ledger Nano X without Bluetooth

To use your Ledger Nano X via USB:

- Desktop: Use the USB-C cable that came with the Ledger Nano X to connect it to your desktop computer. Manage your crypto with Ledger Live desktop or any other compatible (web) app.
- Mobile: Use an [OTG-cable](#) to connect your Ledger Nano X to your Android smartphone (iOS not supported). Manage your crypto with Ledger Live mobile or any other compatible (web) app.

Change your PIN code

The PIN code of your Ledger Nano X device prevents unauthorized access to your crypto assets. Your PIN code is chosen when you first set up the device, but you can change it at any time.

Before you start

- ✓ Your device is [set up](#) and runs the latest firmware.
- ✓ Check our article on [PIN code and recovery phrase security](#).

Instructions

1. Turn on and unlock your Ledger Nano X.
2. Hold both buttons to access Control Center.
3. Navigate to Settings > Security > Change PIN.
4. Choose a new PIN code of 4 to 8 digits.
5. Confirm the new PIN code by entering it again.
6. Enter your old PIN code to validate.
7. The PIN code is now successfully changed.

Security tips

- Choose your own PIN code. This code unlocks your device.
- An 8-digit PIN code offers an optimum level of security.
- Choose a PIN code that's hard to guess.

Learn more

- Maximize your account security [with a passphrase](#) (advanced users).
- Contact [Ledger Support](#) in case you require assistance.

Advanced passphrase security

Set up a passphrase to add a layer of security to your crypto assets. This option is only recommended for advanced users. Carefully read this article before setting up a passphrase.

Security tip

The recovery phrase and passphrase functionalities enable a range of security setups. You may use them to design the security strategy that meets your personal situation. Please do not overcomplicate things, the best security setup is one that you master and can execute with confidence.

How the passphrase works

The 24-word recovery phrase saved during initial setup of your Ledger hardware wallet fully backs up the private keys providing access to your accounts. You must store it in a secure place.

- The passphrase is essentially a password added to your 24-word recovery phrase that provides access to a whole new set of accounts.
- The passphrase protects your crypto assets if your 24-word recovery phrase were to be compromised. To access passphrase-protected accounts, an attacker will need your recovery phrase as well as your secret passphrase.
- Each different passphrase unlocks a unique set of accounts. You can use as many passphrases as you like.

Before you start

- ✓ Your device is [set up](#) and runs the latest firmware.
- ✓ Ensure your recovery phrase is accessible, just in case.
- ✓ Read this article fully before you start.

Instructions

Getting started

1. Connect your Ledger Nano X and enter your PIN code.
2. Hold both buttons to access the Control Center.
3. Navigate to the Settings menu.
4. Go to Security.
5. Go to Passphrase and choose either of two options:
 - Attach to PIN: Creates a second PIN code to unlock passphrase-protected accounts
 - Set temporary: Enter the passphrase each time you wish to access passphrase-protected accounts
6. Continue with the section below that matches the option you've chosen

Option 1 - Attach to PIN code

How it works

Attaching a passphrase to a new PIN code creates a new set of accounts on your Ledger Nano X based on a secret passphrase of your choice. You can access the accounts protected by this passphrase by entering a secondary PIN code.

- The passphrase will be stored on the device until you overwrite it with another passphrase or until the device is reset.
- Store a physical backup of the secret passphrase in a secure place. The device cannot display it after you've set it.

Instructions

1. Choose Attach to PIN option from the Passphrase menu in the device security settings.
2. Press both buttons to validate Set secret passphrase.
3. Create a secondary PIN code.
4. Re-enter the secondary PIN code to confirm it.
5. Choose and confirm a secret passphrase (max 100 characters).
6. Enter your primary PIN code to validate.
7. Your device will continue managing the accounts based on your recovery phrase without passphrase. Please turn off the device and enter your secondary PIN code to access the passphrase-protected accounts.

Option 2 - Set temporary passphrase

How it works

Using a temporary passphrase provides access to a new set of accounts on your Ledger Nano X for the duration of the session. Follow the instructions below each time you wish to access the accounts protected by the passphrase.

- The accounts are based on a secret passphrase of your choice.
- Store a physical backup of the secret passphrase in a secure place. The device cannot display it after initial setup.

Instructions

1. Choose Set temporary option from the Passphrase menu in the device security settings.
2. Press both buttons to validate Set secret passphrase.
3. Choose and confirm a secret passphrase (max 100 characters).
4. Enter your primary PIN code to validate.
5. Your device will now manage the accounts protected by this passphrase. To access your primary accounts, please restart the device and enter your PIN code as usual.

Recover passphrase accounts

In case of loss or a reset of your Ledger Nano X, you can recover access to your crypto assets on any Ledger device as long as you have both your 24-word recovery phrase and secret passphrase.

Instructions

1. Take out your recovery phrase and passphrase.
2. Restore the Ledger device from your recovery phrase.
3. Follow the instructions above for a temporary passphrase or attach to PIN code while taking into account:
 - a. Temporary passphrase: Simply enter the passphrase you've set up earlier to access the accounts protected by that passphrase.

- b. Attach to PIN code: You can choose any PIN code, but you need to enter the passphrase you've set up earlier to access the accounts protected by that passphrase.

Passphrase security in practice

Plausible deniability

To protect yourself in case of physical threat, make sure your primary PIN code unlocks only a minor part of your crypto assets. Then set up a passphrase attached to a PIN code and store more significant amount of crypto assets on the passphrase-protected accounts.

If you are under duress to unlock your Ledger Nano X, you can surrender your main PIN code to the attacker while hiding the PIN code that unlocks your passphrase-protected accounts.

Recovery phrase protection

It's a good security practice to keep multiple copies of your Recovery sheet and to store them in different geographic locations. To mitigate the risk of losing your crypto assets if one of the copies of your recovery phrase is compromised, you can set up a passphrase. If you do so, make sure to store paper backups of your passphrase, preferably in geographic locations that are different from the locations where you keep a backup of your recovery phrase.

Learn more

- Learn how to [optimize your account security](#).
- Contact [Ledger Support](#) if you require assistance.

Maximize battery life

Ledger Nano X has a 100 mAh Lithium-ion battery that will last several hours in use and a few months when idle on a full charge. Follow the tips in this article to maximize the battery life and lifespan of your Ledger Nano X.

Charging the battery

Charge the battery to 100% to get the maximum battery life of several hours in use. Simply connect the USB-C port to a USB power source to charge it. The battery status icon in the top-right corner will display a charging symbol.

There is no need to fully discharge the battery until you charge it again. Battery life in use is best preserved by charging your device whenever you can. To check the battery charge level, hold both buttons to access the Control Center.

Maximize battery lifespan

If you intend to store your Ledger Nano X for longer periods, the battery lifespan is best preserved by charging fully once every few months. Once fully charged, turn off the device and store it in a cool, moisture-free place.

It's best not to store your Ledger Nano X for a prolonged period on a very low charge, since this may negatively affect battery capacity.

End of life

The battery is designed to last 5 years. Ledger does not provide a battery replacement program. If battery capacity has degraded beyond being practically usable, the device can be used by connecting it to a power source using the USB cable.

Export your accounts

Accounts generated by a Ledger Nano X device can be recovered on any (third-party) hardware or software wallet that supports the same standards as Ledger ([BIP32/BIP39/BIP44](#)).

Before you begin

- ✓ Note that your 24-word recovery phrase provides full access to your accounts. Entering your recovery phrase on a computer or smartphone may be insecure. Avoid doing so if possible.
- ✓ Carefully select a (third-party) hardware or software wallet. Protecting your accounts remains your own responsibility.
- ✓ Contact [Ledger Support](#) when in doubt.

Instructions

Use your recovery phrase

1. Choose a BIP39/BIP44 compatible hardware wallet or software wallet.
2. Get your 24-word recovery phrase.
3. Follow the manual of the selected device or service to import your recovery phrase (also referred to as *mnemonic seed*).

Compatible Ledger devices

- [Ledger Nano X](#)
- [Ledger Nano S](#)
- [Ledger Blue](#)
- Ledger Nano

- Ledger HW.1

Arbitrary list of third-party software wallets

Software wallet security

Software wallets are highly insecure, have not been subjected to a security audit by Ledger and they should only be used for recovery as a last resort. If you proceed to use one of the software wallets below, you accept the responsibility for any possible outcome.

- [Mycelium](#) (smartphone)
- [Electrum](#) (desktop)
- [Bither](#) (smartphone/desktop)
- [Coinomi](#) (smartphone)
- [Jaxx Liberty](#) (smartphone)
- [MyEtherWallet](#)
- [MyCrypto](#)

Generate private keys (advanced)

Advanced users can manually generate all private keys using Ian Coleman's [BIP39 tool](#). This tool is best downloaded for offline use, as instructed below.

Generate your private keys

1. Download the BIP39 tool at the bottom of this article or view the [source on GitHub](#).
2. Double-click the downloaded file to open it in a browser.
3. Type your 24-word recovery phrase in the field *BIP39 Mnemonic*. Use lowercase only.
4. Type your passphrase if you set one in your Ledger hardware wallet.
5. Select a cryptocurrency.
6. Leave the field Internal/External at 0.

Import your private keys

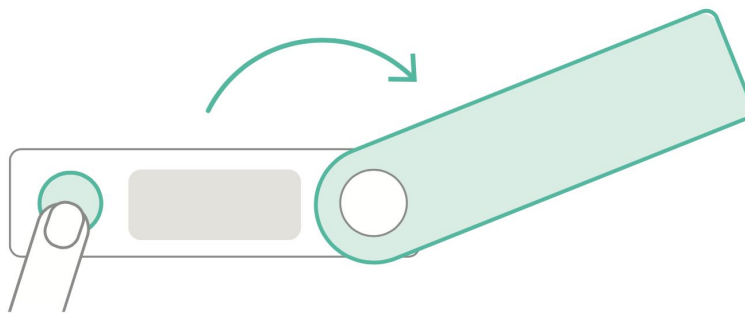
1. Copy the list of generated private keys from the *Derived Addresses* section. Use the controls below the list to show more rows or start at a certain index.
2. Import your private keys in a third-party wallet that supports this, such as [MyEtherWallet](#) or [Armory](#).
3. Set the field Internal/External to 1 to generate the private keys of your [change addresses](#).
4. Import the private keys associated with your change addresses in the third-party wallet.

Access regulatory information

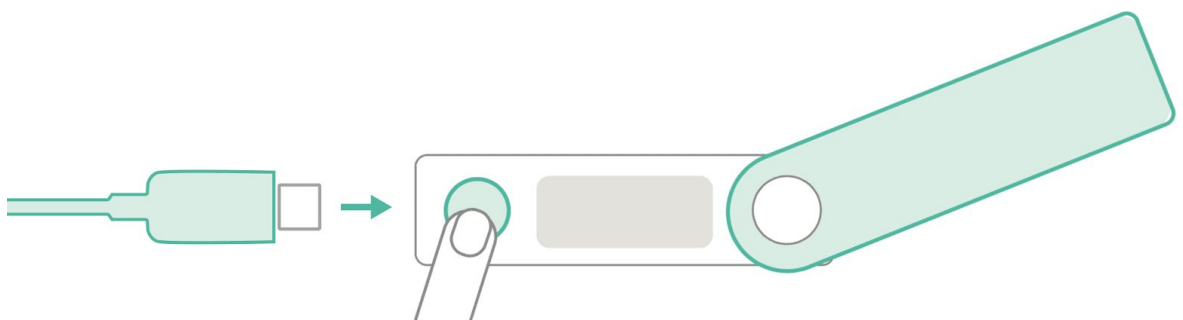
Regulatory information can be accessed in two ways, depending on whether the device has already been set up. Follow the instructions for **Option 1** if the device is still on factory settings. Alternatively, follow the instructions for **Option 2** if it has been set up and you know the confidential PIN code as the owner of the device.

Option 1 - Factory settings

1. Rotate the swivel cover.

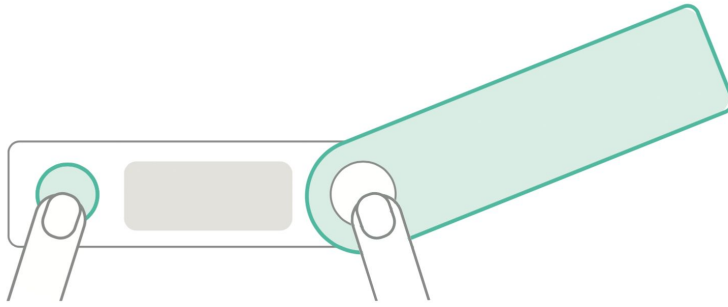


2. Press and hold the button next to the USB port while connecting the device to a power source using the included USB-C cable. The Ledger Logo is then displayed.



3. Press the right button once to select **Regulatory info** in the boot menu.

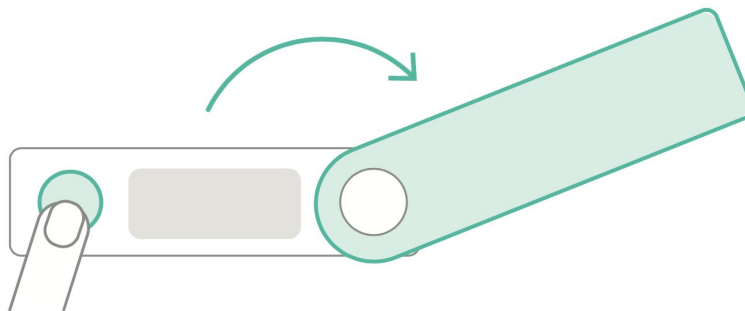
4. Press both buttons simultaneously to access **Regulatory info**.



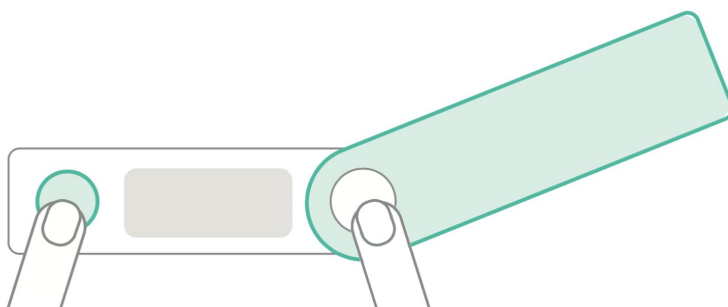
5. Press the right button to display all information.

Option 2 - Device in use

1. Rotate the swivel cover. Press the left button to turn on the device.



2. Unlock the device by entering the user's confidential PIN code.
3. Press and hold both buttons simultaneously to open the Control Center from the Dashboard.



4. Press the right button until **Settings** is selected, then press both buttons to validate.
5. Press both buttons simultaneously to enter **General** settings.

6. Press the right button to select **Regulatory info**, then press both buttons to enter.
7. Press the right button to display all information.

Troubleshooting

Fix connection issues

If you encounter connection issues when trying to connect your Ledger hardware wallet, try the following solutions one by one.

Mac, Windows or Linux

1. Close other applications (*Ledger apps, crypto wallets, Geth, Parity, Mist, Bitcoin Core, etc*).
2. Turn OFF VPN and anti-virus.
3. Change the USB cable if possible
4. Try different USB ports.
5. Restart your computer.
6. Try another computer.

If the problem persists, please select your system below.

Windows

- Update USB input device drivers
 1. Open Devices and Printers from Control Panel.
 2. Double-click Nano X and open the Hardware tab.
 3. Select USB Input Device and click Properties.
 4. Click Change Settings.
 5. Click the Driver tab.
 6. Click Update driver and select automatic driver selection.
 7. Repeat this for both USB Input Devices.
- If it still does not work, please try on a Mac to verify that your Ledger Nano X is working properly.

Mac

If you're having connection issues on a Mac, you can try giving Ledger Live full disk access:

1. Open System Preferences.
2. Go to Security & Privacy.
3. In the Privacy tab, add Ledger Live to the Full Disk Access list.

Linux

On Linux you need to create a set of udev rules to allow device access. Refer to the [Chrome USB API documentation](#) for details. Please follow the instructions below.

1. Setup

- Check if the plugdev group exists by entering the command:

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

- Follow the steps below if the previous command did not return a result
 1. Create the plugdev group:

```
sudo groupadd plugdev
```

2. Check if you are in the group plugdev with the command:

```
groups
```

3. If the output does not contain plugdev, you are not in the plugdev group. Enter the command:

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

4. Note: replace <user> by your username, e.g for user "mike", it would be:
sudo gpasswd -a mike plugdev.

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

5. Logout and login for the change to take effect. To verify you are now in the plugdev group, enter:

```
groups
```

6. and search for a plugdev occurrence. If it's not there, you've missed a step and should restart from step 1.

2. Add the udev rules

1. Enter the following command to automatically add the rules and reload udev:

```
wget -q -O -  
https://raw.githubusercontent.com/LedgerHQ/udev-rules/master/add\_udev\_rules.sh | sudo bash
```

2. Retry connecting your Ledger Nano X with Ledger Live.

If it's still not working, continue to step 3: troubleshooting.

3. Troubleshooting

Try each of the following three options.

- Option 1
Edit the file `/etc/udev/rules.d/20-hw1.rules` file by adding the `OWNER=<user>` parameter to each line, where `<user>` is your Linux user name.
Then reload the rules as follows:

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

Retry the connection with Ledger Live. If it does not work, try the next option.

- Option 2
Edit the `/etc/udev/rules.d/20-hw1.rules` file and add the following lines:

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

Then reload the rules:

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

Retry connecting with Ledger Live. If it does not work yet, try the last option.

- Option 3
If you are on Arch Linux, you can try the following rules:

```
/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"
```

Then reload the rules again and retry the connection with Ledger Live:

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

iOS and Android

If you're experiencing Bluetooth issues with your Ledger Nano X, please remove the pairing and forget the Ledger Nano X on your phone. Then set up the pairing once again.

Reset pairings on your Ledger Nano X

1. Turn on and unlock your Ledger Nano X.
2. Hold both buttons to access the Control Center.
3. Press both buttons to navigate to the Security menu.
4. Press both buttons to validate Reset pairings.
5. Confirm Reset pairings once more.

Forget Ledger Nano X on your smartphone

1. Open the Bluetooth settings of your smartphone.
2. Select specific settings for your Ledger Nano X.
3. Forget the device.

Now you can set up the pairing again by choosing your Ledger Nano X at any point in Ledger Live mobile that requires a device connection, for instance in the Manager tab.

Lost device, PIN code or recovery phrase

If you cannot access your Ledger Nano X device, you forget your PIN code or you lose the recovery phrase, you immediately need to follow the steps outlined in this article to prevent losing your crypto assets.

Make sure your recovery phrase stays securely stored. Protect your confidential PIN code and 24-word recovery phrase to guarantee the highest level of security offered by your Ledger hardware wallet.

Instructions

Can't access your Ledger device?

1. In case of loss, theft, or destruction of your device, please [restore your recovery phrase](#) on any hardware or software wallet [that supports 24-word recovery phrases](#).
2. You need the Recovery sheet on which you've saved your recovery phrase during setup.

Forgot your PIN code?

1. After three incorrect PIN code entries, Ledger hardware wallets [reset to factory settings](#), erasing the private keys from their secure storage.
2. After the reset, simply [restore the device](#) from your recovery phrase.
3. Choose a new PIN code during the restoration process.

Lost your recovery phrase?

Your Recovery sheet is a full backup of the private keys that provide access to your private keys. You must store it in a secure location. Anyone with access to your Recovery sheet can take your crypto assets without knowing the PIN code of your device.

If you do lose your Recovery sheet

1. Immediately [send all your crypto assets](#) to temporary accounts, like an exchange service or another hardware wallet.
2. Enter three wrong PIN codes to [reset your Ledger Nano X](#).
3. [Set up your Ledger Nano X](#) as a new device.
4. Then [transfer back](#) your crypto assets to your newly configured device.

Reset to factory settings

Resetting the device to factory settings removes all private keys, applications and settings from your Ledger Nano X device. You can reset to [set it up as a new device](#), to [restore another recovery phrase](#) or to safely transfer the device to someone else.

Before you start

- ✓ Ensure that you are the sole holder of the 24-word recovery phrase that backs up the private keys on your device.

Instructions

[Got your Recovery sheet?](#)

If you reset your device without holding your Recovery sheet, the private keys providing access to your crypto assets will be erased. You will permanently lose access your crypto assets.

The device can either be reset from the settings menu or by entering three incorrect PIN codes when unlocking it. Please choose one of the two options below:

Reset from device settings

1. Turn on and unlock your Ledger Nano X.
2. Hold both buttons to access the Control Center.
3. Navigate to Settings and press both buttons to validate.
4. Navigate to General and press both buttons to validate.
5. Choose Reset all by pressing both buttons.
6. Read the warnings and choose Reset device to validate.
7. Enter your PIN code to confirm. Your device will then be reset.

Reset from PIN code

1. Turn on your Ledger Nano X.
2. Enter an incorrect PIN code three times in a row.

3. The device will reset after the third incorrect attempt as a security measure.

Next steps

You've successfully reset your device to factory settings. You can either:

- Learn how to [set it up as a new device](#) to generate and backup new private keys.
- Alternatively, [restore your device from a recovery phrase](#) to restore the private keys associated to an existing recovery phrase.

Check hardware integrity

Check the hardware integrity of your Ledger Nano X device to check that it has not been tampered with. This article contains detailed technical information about the security of your device.

Caution

Please handle the Ledger Nano X device with high care while you proceed. Be aware that once opened, your device will not be refundable or exchangeable.

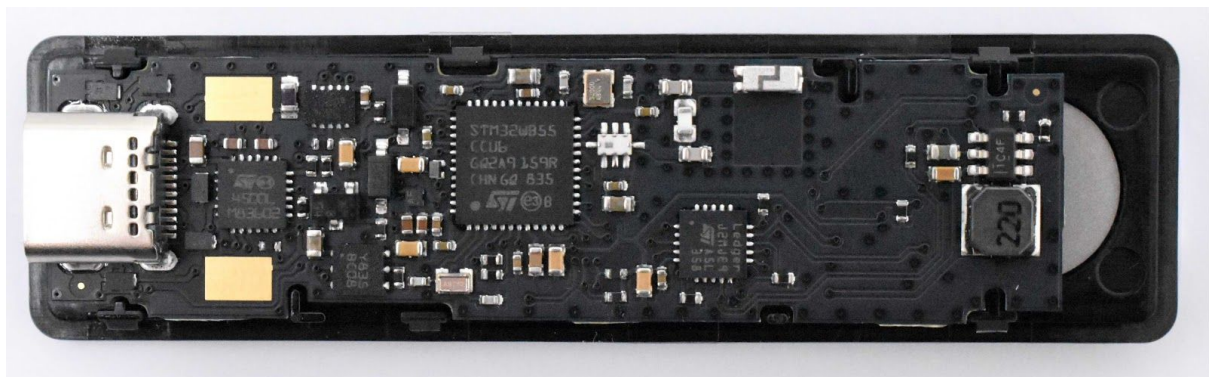
Microcontroller (MCU)

The Secure Element (SE) checks the full microcontroller flash at boot, as described in [this blog post](#). If it has been modified, you'll get a warning at boot. As an additional check, you can open the device to verify that no additional chip has been added, compared with the images below, and that the MCU is an STM32WB55. The Secure Element is marked J2MJE9.

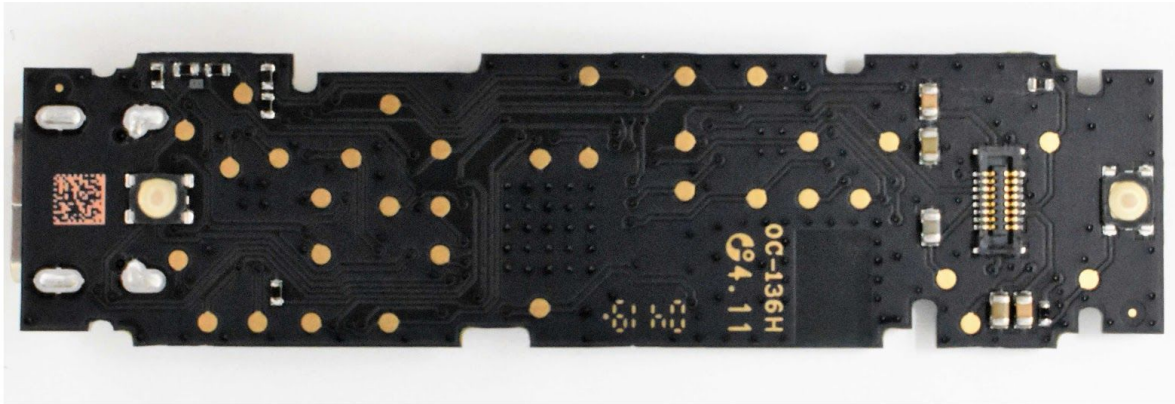
Hardware revisions

Revision 1

- Black PCB



Front of the PCB



Back of the PCB

Secure Element attestation

The Secure Element itself is personalized at factory with an attestation proving that it has been manufactured by Ledger. You can verify it by running:

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

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

The source code [is available here](#).

Application verification

When opening an application, a Non Genuine warning is displayed if the app has not been signed by Ledger. A modified User Interface (as found in <https://github.com/LedgerHQ/nanos-ui>) will also display a warning message on boot.

Root of trust

The root of trust for the current batch is the following secp256k1 public key as checked using [Genuine.py](#):

```
0490f5c9d15a0134bb019d2afd0bf297149738459706e7ac5be4abc350a1f8  
18057224fce12ec9a65de18ec34d6e8c24db927835ea1692b14c32e9836a75  
dad609
```

Use, Care and Regulatory Statement

EN Please handle your Ledger Nano X with care. It includes a battery and other sensitive components. The Ledger Nano X is not waterproof. Make sure you use it in a dry environment and keep it away from any liquids. In case it gets wet, clean it with a soft, dry, lint free cloth. This product is not a toy, make sure you keep it away from children.

The Ledger Nano X is intended to (i) operate with its pre-installed operating system (BOLOS) and the Ledger Live application and to (ii) interoperate with a compatible mobile phone with *Bluetooth®* wireless technology and with a compatible computer via the provided USB cable.

Changes or modifications to this product not expressly approved by Ledger could void its compliance to test standards and negate the user's authority to operate it.

FR Manipulez votre Ledger Nano X avec soin. Il inclut une batterie et d'autres composants sensibles. Le Ledger Nano X n'est pas étanche. À utiliser dans un environnement sec, loin de tout liquide. S'il venait à être mouillé, essuyez-le avec un linge doux et sec, sans peluche. Ce produit n'est pas un jouet, conservez-le hors de portée des enfants.

Le Ledger Nano X est conçu pour (i) fonctionner avec le système d'exploitation préinstallé (BOLOS) et l'application Ledger Live, ainsi que pour (ii) interagir avec un smartphone compatible, via la technologie sans fil *Bluetooth®* et avec un ordinateur compatible via le câble USB fourni.

Toute transformation ou modification du présent produit non expressément autorisée par Ledger pourrait le rendre non conforme aux normes de test et faire perdre à l'utilisateur son droit à l'utiliser.

DE Gehen Sie mit Ihrem Ledger Nano X sorgfältig um. Er enthält einen Akku und weitere sensible Bauteile. Der Ledger Nano X ist nicht wasserdicht. Verwenden Sie ihn ausschließlich in trockener Umgebung und halten Sie ihn von Flüssigkeiten fern. Sollte er nass werden, reinigen Sie ihn mit einem trockenen, weichen, fusselfreien Tuch. Dieses Produkt ist kein Spielzeug, halten Sie es von Kindern fern.

Der Ledger Nano X soll (i) mit dem vorinstallierten Betriebssystem (BOLOS) und der Ledger Live App betrieben werden und (ii) mit einem kompatiblen Smartphone über *Bluetooth®*-Technologie und einem kompatiblen Computer über das mitgelieferte USB-Kabel funktionieren.

Änderungen des Produkts, die von Ledger nicht ausdrücklich genehmigt wurden, können die Konformität mit den getesteten Normen zunichtemachen und die Genehmigung des Nutzers zum Betrieb des Produkts aufheben.

IT Maneggiare il Ledger Nano X con cura. Include una batteria e altri componenti sensibili. Il Ledger Nano X non è impermeabile. Assicursi di utilizzarlo in un ambiente secco e tenerlo lontano da liquidi. Nel caso in cui si bagni, asciugarlo con un panno morbido e asciutto che non lasci pelucchi. Questo prodotto non è un giocattolo, assicurarsi di tenerlo lontano dalla portata dei bambini.

Il Ledger Nano X è destinato a (i) operare con il sistema operativo preinstallato (BOLOS) e l'applicazione Ledger Live e (ii) interagire con un telefono cellulare compatibile con tecnologia wireless *Bluetooth®* e con un computer compatibile tramite il cavo USB in dotazione.

Variazioni o modifiche a questo prodotto non espressamente approvati da Ledger possono invalidare la sua conformità agli standard di prova e negare all'utente l'autorizzazione al suo utilizzo.

NL Behandel uw Ledger Nano X met gepaste zorg. Het omvat een batterij en andere gevoelige onderdelen. De Ledger Nano X is niet waterdicht. Gebruik het in een droge omgeving en houd het uit de buurt van vloeistoffen. Als het nat wordt, gebruik dan een zachte, droge, pluivrije doek. Dit product is geen speelgoed. Houd het buiten het bereik van kinderen.

De Ledger Nano X is ontworpen om (i) te werken met zijn vooraf geïnstalleerde besturingssysteem (BOLOS) en de Ledger Live-toepassing en om (ii) te werken met een compatibele mobiele telefoon via draadloze *Bluetooth*®-technologie en met een compatibele computer via de USB-kabel. Wijzigingen aan dit product die niet uitdrukkelijk door Ledger zijn goedgekeurd, kunnen de naleving van de testnormen en het gebruiksrecht van de gebruiker tenietdoen.

ES Rogamos utilice su Ledger Nano X con cuidado. Incluye una batería y varios componentes sensibles. El Ledger Nano X no es impermeable. Asegúrese de utilizarlo en un ambiente seco y manténgalo alejado de líquidos. Si se moja, límpielo utilizando un paño suave, seco y sin pelusa. El Ledger Nano X no es un juguete, manténgalo alejado de los niños. Este producto tiene por objeto (i) funcionar con su sistema operativo preinstalado (BOLOS) y con la aplicación Ledger Live e (ii) interactuar con un teléfono móvil compatible con tecnología inalámbrica *Bluetooth*®y con un ordenador compatible a través del cable USB facilitado. Cualquier cambio o modificación del producto no autorizado expresamente por Ledger puede invalidar el cumplimiento de estándares y la autoridad del usuario para utilizarlo.

PT Manuseie cuidadosamente o Ledger Nano X. Ele inclui uma pilha e outros componentes sensíveis. O Ledger Nano X não é à prova de água. Certifique-se de utilizá-lo em um ambiente seco e o mantenha longe de líquidos. Se o produto se molhar, limpe-o com um pano macio, seco e sem pelos. Este produto não é um brinquedo, mantenha-o longe de crianças. O Ledger Nano X deve (i) funcionar com o sistema operacional pré-instalado (BOLOS) e o aplicativo Ledger Live, e (ii) interagir com um celular compatível com tecnologia sem fio *Bluetooth*®e com um computador compatível através do cabo USB fornecido. As alterações ou modificações do produto que não sejam expressamente aprovadas pela Ledger podem anular a conformidade com as normas dos testes e invalidar a autorização de operação do usuário

KO Ledger Nano X를 주의하여 취급하십시오. 이 제품에는 배터리와 기타 민감한 부품이 포함되어 있습니다. Ledger Nano X는 방수가 아닙니다. 건조한 곳에서 사용하고 액체가 가까이 두지 마십시오. 젖은 경우에는 보풀이 없고 부드러운 마른 천으로 청소하십시오. 이 제품은 장난감이 아닙니다. 어린 아이의 손이 닿지 않도록 하십시오. Ledger Nano X는 (i) 사전 설치된 영체제(BOLOS)와 Ledger Live 애플리케이션으로 작동하며 (ii) *Bluetooth*®무선 기술을 통해 휴대전화와 상호 작용하고 제공된 USB 케이블을 통해 컴퓨터와 상호 작용하도록 설계되었습니다. Ledger가 승인하지 않은 제품의 변경, 개조 시 시험 기준 적합성이 무효화되고 사용자의 이용 권한이 취소될 수 있습니다.

RU Используйте Ledger Nano X с осторожностью. В устройстве есть аккумулятор и прочие хрупкие детали. Ledger Nano X неустойчив к влаге. Используйте его только в сухой среде и не допускайте воздействия влаги. При попадании влаги протрите его мягкой сухой безворсовой тканью. Храните устройство в недоступном для детей месте. Ledger Nano X (i) работает на базе предварительно установленной операционной системы (BOLOS) и с приложением Ledger Live, а также (ii) функционирует с совместимыми мобильными телефонами с помощью беспроводной технологии *Bluetooth*® и компьютерами через USB-кабель. Изменения и модификации устройства, не одобренные Ledger, могут привести к ухудшению его рабочих характеристик и невозможности его дальнейшего использования.

JA Ledger Nano X は、やさしく取り扱ってください。これにはバッテリーやその他のデリケートな部品が含まれています。Ledger Nano X は防水仕様ではありません。必ず乾燥した環境で使用し、液

体に近づけないようにして保管してください。濡れてしまった場合は、柔らかく乾いたリントフリーの布で拭いてください。この商品はおもちゃではありませんので、お子様の手の届かないところに保管してください。

Ledger Nano X は、(i) プリインストールされたオペレーティングシステム (BOLOS) と Ledger Live アプリケーションとともに使用するよう設計されており、(ii) Bluetooth®ワイヤレスを搭載し、互換性のある携帯電話、そして或いは付属のUSBケーブルで互換性のあるコンピュータとも組み合わせてご利用いただけます。

Ledgerによって明確に承認されていない方法以外の方法で本製品の変更または改造を行うと、商品テスト基準への準拠が無効となり、ユーザーの使用権限が否定される可能性があります。

ZH 由于Ledger Nano X内部包含电池和其他敏感部件，请您小心操作和使用您的Ledger Nano X。

Ledger Nano X不具备防水功能，所以请务必在干燥的环境下使用，并且远离任何液体。如被打湿，请使用柔软干燥的无绒布进行清洁。本产品非玩具，存放和使用时请务必远离儿童可触及范围。

Ledger Nano X 需(i) 使用预安装的操作系统(BOLOS) 和Ledger Live 应用程序进行操作，且(ii) 通过Bluetooth®无线技术与兼容的移动电话进行交互操作，并通过提供的USB 数据线与兼容的计算机进行交互操作。

如未经Ledger 明确批准而对本产品进行更改或修改，可能会导致本产品不符合测试标准，并会使得用户的操作权限无效。

AR يُرجى التعامل مع محفظتك Ledger Nano X بعناية. فهذه المحفظة تشتمل على بطارية ومكونات أخرى حساسة. محفظة Ledger Nano X غير مقاومة للماء. تأكد من استخدامها في بيئة جافة واحفظها بعيداً عن أي سوائل. في حالة تعرضها للبلل، نظّفها بقطعة قماش ناعمة وجافة وخالية من الوبر. هذا المنتج ليس لعبة، تأكد من إبقائه بعيداً عن متناول الأطفال.

تم تصميم محفظة العملات الرقمية (1) Ledger Nano X للعمل بنظام التشغيل المثبت مسبقاً (BOLOS) وتطبيق Ledger Live و(2) للتشغيل التفاعلي مع هاتف محمول متوافق مزود بتقنية Bluetooth® لاسلكية ومع أي جهاز كمبيوتر متوافق باستخدام كابل USB المزود معها.

يمكن أن تؤدي التغييرات أو التعديلات في هذا المنتج التي لم تتم الموافقة عليها صراحة من قبل شركة Ledger إلى إبطال الامتثال لمعايير الاختبار وإلغاء صلاحية المستخدم لتشغيله.

EU Regulatory statements



EN The manufacturer, Ledger SAS (1, rue du mail - 75002 - Paris - France), hereby declares that the Ledger Nano X complies with European RED and RoHS2 Directives. The full text of the EU declaration of conformity, including the product frequency bands and maximum radio-frequency power is available at the following address: ledger.com/legal

FR Le fabricant, Ledger SAS (1, rue du mail, 75002 Paris, France), déclare par les présentes le Ledger Nano X conforme aux Directives européennes RED et RoHS2. L'intégralité de la déclaration UE de conformité, y compris les bandes de fréquences du produit et la puissance radio maximale, est disponible à l'adresse suivante : ledger.com/legal

DE Der Hersteller, Ledger SAS (1, rue du mail – 75002 Paris – Frankreich) erklärt hiermit, dass der Ledger Nano X die Anforderungen der Richtlinien 2014/53/EU und 2011/65/EU erfüllt. Der

vollständige Text der europäischen Konformitätserklärung, einschließlich des Frequenzbands des Produkts und der höchstzulässigen Hochfrequenzleistung ist abrufbar unter: ledger.com/legal

IT Il fabbricante, Ledger SAS (1, rue du mail - 75002 - Parigi - Francia), con il presente dichiara che il Ledger Nano X è conforme alle direttive europee RED e RoHS2. Il testo completo della dichiarazione di conformità UE, comprese le bande di frequenza del prodotto e la potenza massima in radiofrequenza, è disponibile al seguente indirizzo: ledger.com/legal

NL De fabrikant, Ledger SAS (1, rue du mail – 75002 – Parijs – Frankrijk) verklaart dat de Ledger Nano X voldoet aan de Europese RED- en RoHS2-richtlijnen. De volledige tekst van de EU-conformiteitsverklaring, inclusief de frequentiebanden en het maximale radiofrequentievermogen van het product, is hier beschikbaar: ledger.com/legal

ES El fabricante, Ledger SAS (1, rue du mail - 75002 - París - Francia), declara por la presente que Ledger Nano X es conforme a las Directivas europeas RED y RoHS2. El texto íntegro de la declaración UE de conformidad, incluidas las bandas de frecuencia y la máxima potencia de radiofrecuencia del producto, puede consultarse en: ledger.com/legal

PT A fabricante, Ledger SAS (1, rue du mail - 75002 - Paris - França), declara que o Ledger Nano X está em conformidade com as Diretivas Europeias RED e RoHS2. O texto integral da Declaração de Conformidade da UE, incluindo as bandas de frequências do produto e a energia de radiofrequência máxima, está disponível no seguinte endereço: ledger.com/legal



EN This symbol indicates that your product must be disposed of according to local laws and regulations without mixing it with unsorted municipal waste. When your product reaches its end of life, contact Ledger or your local authorities to learn about recycling options. Proper treatment and recycling of your product will help conserving natural resources, protecting environment and human health.

Please note that the lithium-polymer battery included in your Ledger Nano X shall be deposited separately from the device for proper waste management. Please contact us at support@ledger.com for safe battery removal instructions.

FR Ce symbole indique que votre produit ne doit pas être jeté avec les déchets ménagers non triés, conformément aux lois et réglementations locales. Lorsque votre produit arrive en fin de vie, veuillez contacter Ledger ou les autorités locales pour en savoir plus sur les options de recyclage. Le traitement et le recyclage approprié de votre produit contribueront à la préservation des ressources naturelles, ainsi qu'à la protection de l'environnement et de la santé.

Veuillez noter que la batterie lithium-polymère incluse dans votre Ledger Nano X devra être déposée séparément de l'appareil pour une gestion appropriée des déchets. Veuillez nous contacter à support@ledger.com pour obtenir les instructions permettant le retrait de la batterie en toute sécurité.

DE Dieses Symbol zeigt an, dass Ihr Produkt gemäß den vor Ort geltenden Gesetzen nicht mit dem Hausmüll, sondern separat zu entsorgen ist. Wenn Ihr Produkt das Lebensende erreicht hat, kontaktieren Sie bitte Ledger oder die zuständigen Behörden vor Ort, um mehr über das Recycling zu erfahren. Die richtige Entsorgung und Wiederverwertung Ihres Produkts tragen zum schonenden Umgang mit den Ressourcen, dem Umweltschutz und der Gesundheit der Menschen bei.

Die Lithium-Polymer-Batterie in Ihrem Ledger Nano X ist separat und nicht mit Ihrem Gerät zu entsorgen. Bitte kontaktieren Sie uns unter support@ledger.com, wenn Sie die Batterie sicher entfernen wollen.

IT Questo simbolo indica che il prodotto deve essere smaltito secondo le leggi e le normative locali senza mescolarlo con rifiuti urbani non differenziati. Quando il prodotto raggiunge la fine della vita utile, contattare Ledger o le autorità locali per informazioni sulle opzioni di riciclaggio. Un trattamento e un riciclaggio corretti del prodotto aiuteranno a conservare le risorse naturali, proteggendo l'ambiente e la salute umana.

La batteria ai polimeri di litio inclusa nel Ledger Nano X deve essere depositata separatamente dal dispositivo per una corretta gestione dei rifiuti. Per istruzioni sulla rimozione sicura della batteria, è possibile contattarci all'indirizzo support@ledger.com.

NL Dit symbool geeft aan dat uw product moet worden verwijderd volgens de lokale wet- en regelgeving zonder het te mengen met ongesorteerd stedelijk afval. Neem aan het einde van de levensduur contact op met Ledger of uw lokale overheid voor info over recyclingmogelijkheden. Een goede verwerking en recycling draagt bij aan het behoud van natuurlijke hulpbronnen, het milieu en de menselijke gezondheid.

Merk op dat de lithium-polymeerbatterij in uw Ledger Nano X voor een correct afvalbeheer afzonderlijk van het toestel zal moeten worden verwijderd. Neem contact met ons op via support@ledger.com voor instructies om de batterij te verwijderen.

ES Este símbolo indica que este producto debe desecharse de conformidad con las leyes y normativa local sin mezclarlo con residuos municipales sin clasificar. Al final de la vida útil del producto, contacte con Ledger o la autoridad local para conocer las opciones de reciclado. El correcto tratamiento y reciclado de su producto ayudará a preservar los recursos naturales, proteger el medio ambiente y la salud.

Observe que, para la correcta gestión de residuos, la batería de polímero de litio de su Ledger Nano X debe desecharse por separado del dispositivo. Escribanos a support@ledger.com para saber cómo desechar de forma segura la batería.

PT Este símbolo indica que o seu produto deve ser descartado de acordo com a legislação e a regulamentação locais, separado de resíduos urbanos indiferenciados. Quando o produto atingir o fim da vida, entre em contato com a Ledger ou com as autoridades locais para obter informações sobre as opções de reciclagem. O tratamento adequado e a reciclagem do seu produto ajudarão a conservar recursos naturais, protegendo o meio ambiente e a saúde humana.

Observe que a pilha de polímero de lítio incluída no Ledger Nano X deve ser depositada separadamente do aparelho para gestão adequada dos resíduos. Fale conosco via support@ledger.com para obter instruções para remoção segura da pilha.

US and Canada Regulatory Statements

This equipment complies with FCC/ISED radiation exposure limits set forth for an uncontrolled environment.

Cet équipement est conforme aux limites d'exposition aux rayonnements FCC/ISDE établies pour un environnement non contrôlé.

US: This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- *Reorient or relocate the receiving antenna.*
- *Increase the separation between the equipment and receiver.*
- *Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.*
- *Consult the dealer or an experienced radio/TV technician for help.*

Canada: CAN ICES-3 (B)/NMB-3(B)

EN This device complies with Innovation, Science and Economic Development Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

FR Le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Ledger is under license.