Openloop

User Manual

Openloop Hardware Wallet & Security Key

Haudi Crypto, Inc.

Version 1.1.1
2026-08-13

Contents

---

1. Introduction

1.1 What is Openloop?

Openloop is a hardware wallet for crypto assets, a FIDO2 security key, and a PKCS#11 signer all in one. It keeps your private keys safe and signs in an environment completely isolated from the internet.

Three ways to use it:

- 🔐 **Hardware wallet**: private key management and signing for crypto assets (Bitcoin / Ethereum / XRP / Solana / TRON)
- 🔑 **FIDO2 security key (passkeys)**: passwordless authentication to web services and apps from a PC or smartphone (USB on PC, BLE on mobile — Openloop Connect required)
- 📝 **PKCS#11 signer (PIV)**: SSH authentication, PDF signing, GPG signing, TLS client authentication (over USB, with Openloop Connect)

Key features:

- Encrypted storage: private keys protected with AES-256-GCM
- Touchscreen: an intuitive 320×240 pixel display

- Three connection methods: Air Gap (QR code) / USB / Bluetooth USB and Bluetooth are the standard methods for everyday use; Air Gap is the option for operating without any electronic communication
- Multi-currency support: Bitcoin / Ethereum (215 networks) / XRP / Solana / TRON
- FIDO2/CTAP2: passkey support (ES256 / EdDSA)
- PIV/PKCS#11: SSH / PDF signing / TLS authentication (P-256 / Ed25519 / RSA-2048)
- Multilingual: Japanese / English

★ **Secure element**: an NXP SE050 secure element (EAL6+ certified) protects your private keys in hardware.

1.2 How to Use This Manual

- ℹ **Tip**: handy techniques and supplementary information
- ▲ **Warning**: important cautions and security-related information
- Checkpoint: items you should verify

Suggested reading order:

1. First time: Ch. 1 → 2 → 3 → 4 → 7
2. To send funds: Ch. 5 → 6
3. To use it as a security key: Ch. 9
4. To use it as a PKCS#11 signer: Ch. 10
5. To change settings: Ch. 11
6. When you run into trouble: Ch. 13

1.3 Important Safety Information

▲ Your recovery phrase is your most important asset

Why the recovery phrase (12 or 24 words) matters:

- With it, **you can restore your assets even if you lose the device**
- Lose it and **your assets are gone forever** (nobody can help you)
- If it is stolen, **your assets will be stolen** (you cannot get them back)

Things you must not do casually:

- ✗ Photograph it with your phone and store it in the cloud (the cloud can be hacked)
- ✗ Type it into a computer (malware can steal it)
- ✗ Show or tell it to anyone (be careful)

- ✗ Save it in online storage
- ✗ Send it by email or messaging

Things you must do:

- ✓ Write it down on paper by hand
- ✓ Make several copies (2–3)
- ✓ Store them separately, for example in a fireproof safe
- ✓ Tell your family where they are (for inheritance)

⚠ Managing your PIN

- PIN: required to unlock the device (4–6 digits)
- Get it wrong 10 times: ⚠ **the device automatically erases all data** (see below)
- If you forget it: you will need to restore from your recovery phrase

⚠ **Getting the PIN wrong 10 times in a row makes the device automatically perform a factory reset.** In addition to your wallet (recovery phrase), PIN, and all settings, **your FIDO2 passkeys and PIV keys and certificates are also completely erased and can never be recovered.** Crypto assets can be restored from your recovery phrase, but passkeys must be registered again at each service, and PIV keys must be regenerated with new certificates issued. After nine failures, wait for the lockout to clear and then enter the correct PIN calmly.

⚠ Beware of phishing

- Use official software only: trusted applications such as Sparrow Wallet and MetaMask
- Suspicious emails and DMs: messages like “please verify your wallet” are scams
- Support scams: official support will **never** ask you for your private key or recovery phrase

1.4 Terms of Use and Disclaimer

Please read the following terms of use and disclaimer before using this product. By using this product, you are deemed to have agreed to them.

Software license

The Openloop firmware and software are provided “AS IS.”

- No warranty: the software is provided without warranty
- Copyright: all software copyrights belong to the manufacturer

Your responsibilities

What you are responsible for:

- Storing your recovery phrase safely
- Managing your PIN appropriately
- Verifying transaction details (destination address, amount, fee)
- Physically protecting the device (preventing theft and loss)
- Updating the firmware regularly
- Creating and storing backups

The manufacturer and developers accept no responsibility whatsoever for:

1. Losses relating to crypto assets
   - Losses from price volatility
   - Loss of assets due to a lost or stolen recovery phrase
   - Device lockout due to a forgotten PIN
   - User error (sending to the wrong address, mistyping an address)
   - Damage from fraud or phishing
   - Blockchain network failures or delays
   - Failures or bankruptcy of exchanges or third-party services
2. Technical problems
   - Losses caused by software bugs
   - Hardware compatibility problems
   - Interoperability problems with third-party wallet software
   - Trouble during firmware updates
   - Connection errors on any transport (QR / USB / BLE)
3. Legal and regulatory matters
   - Changes to laws and regulations in any country
   - Changes to the legal status of crypto assets
   - Tax matters (calculating and filing taxes is your responsibility)
   - Compliance with anti-money-laundering law
4. Other
   - Damage to the device from natural disasters or accidents
   - Unauthorized access or hacking by third parties
   - Loss or corruption of data
   - Errors or omissions in this manual

Important points to understand

▲ Crypto assets are extremely high-risk:

- Prices can move dramatically
- Once sent, a transaction cannot be reversed
- Losing your private key means losing your assets forever
- No government or company will compensate you

▲ Openloop is a signing-only device:

- It does not connect to the internet (air gap)
- It cannot check the state of the blockchain
- It has no balance display (check with third-party wallet software)
- Broadcasting a transaction is done by third-party wallet software

Before you use it, always:

- Back up your recovery phrase in several places
- Test with a small transfer first
- Verify the details (address, amount, fee) on the device screen
- Use only wallet software you trust

1.5 Warranty

Hardware warranty

Warranty period: 6 months from the date of purchase

Covered:

- Failures caused by manufacturing defects
- Component failures under normal use
- Touchscreen malfunctions (manufacturing defects only)
- USB/BLE communication failures (manufacturing defects only)

Not covered:

- Damage caused by the user (drops, water damage, disassembly, and so on)
- Failures caused by improper use or storage
- Problems caused by modification or repair
- Natural battery degradation
- Minor scratches or marks on the screen
- Software and firmware defects

- Compatibility problems with third-party products

Scope of the warranty:

- Covered failures will be repaired or replaced free of charge
- **Loss of crypto assets is not covered**
- We do not offer data recovery or migration services
- Shipping in both directions is at your expense

Software warranty

⚠ **The software is provided without warranty (AS IS)**

- Firmware and software are provided “as is”
- Losses caused by bugs or defects are not covered
- We carry out ongoing security review and improvement
- Security updates are provided on a **best-effort** basis

Asset guarantee

There is no guarantee of any kind regarding crypto assets

- Even when the device works correctly, asset losses are not compensated
- Loss of assets due to a lost recovery phrase is not covered
- User error (sending to the wrong place) is not covered
- Losses caused by software bugs are not covered
- Problems with third-party services (exchanges, wallet software) are not covered

How to make a warranty claim

If a failure or defect occurs:

1. Prepare proof of purchase: have your receipt ready
2. Describe the symptoms: note the specifics (steps to reproduce, error messages, and so on)
3. Contact support: get in touch through the official support channel
4. Diagnosis: the support team determines whether it is covered
5. Repair or replacement: handled free of charge if covered

⚠ **Important**: when a device is repaired or replaced, **all data on it is erased**. Make sure you can restore from your recovery phrase first.

Acknowledgement of the disclaimer

By using this product, you are deemed to understand and agree that:

- Managing crypto assets is **entirely at your own risk**
- Losing your recovery phrase means **permanently losing your assets**
- The manufacturer and developers accept **no responsibility whatsoever for asset losses**
- The hardware warranty covers **physical device failures only**
- The software is provided **without warranty (AS IS)**

1.6 Privacy Policy

Openloop respects your privacy and keeps data collection to an absolute minimum.

Basic principles

Openloop is an offline device

- It does not connect to the internet
- It does not send user data to any server
- It does not track how you use it
- It collects no data for advertising or marketing

Data stored on the device

The following data is stored **only on the device** and is never transmitted:

Data type	Storage	Purpose	How to erase
Private keys	Secure element (SE050)	Signing	Erase Wallet
Entropy	Secure element (SE050)	Recovery phrase generation	Erase Wallet
Seed	Secure element (SE050)	Private key derivation	Erase Wallet
FIDO2 master key	Secure element (SE050)	Passkey authentication	Passkey reset
PIV key pairs	Secure element (SE050)	PIV signing	PIV reset
Passkey data	NVS (non-volatile memory)	Passkey management	Passkey reset
PIV certificates	NVS (non-volatile memory)	PIV authentication	PIV reset

Data type	Storage	Purpose	How to erase
PIN	NVS (non-volatile memory)	Device lock	Delete PIN
PIV PIN	NVS (non-volatile memory)	PIV signing authentication	PIV reset
Settings	NVS (non-volatile memory)	Language, volume, and so on	Factory Reset
BLE pairing data	NVS (non-volatile memory)	Bluetooth connection	Unpair

★ **Secure element**: the device carries an NXP SE050 secure element (EAL6+ certified). Private keys are protected by the dual-secure mechanism and stored safely inside the secure element.

▲ **Important**: running “Erase Wallet” or “Factory Reset” **completely deletes** the private keys, entropy, and seed. Without a backup of your recovery phrase, **your assets are lost forever**. A factory reset also deletes your FIDO2 passkeys and PIV keys.

Data in transit

Air Gap (QR code):

- The only data is what appears on screen as a QR code
- No network communication
- The most private method

USB:

- A direct connection to your PC
- Data travels over the USB cable only
- Nothing is sent over the internet
- Security depends on the PC you connect to

Bluetooth Low Energy (BLE):

- Encrypted communication with paired devices
- A range of about 10 m
- Pairing data is stored on the device
- Connection history is never transmitted

Sharing data with third parties

We never provide user data to third parties

- No data sold to advertisers
- No data sent to analytics services
- No voluntary disclosure to government agencies
- No data shared with business partners

⚠ **Exception**: if we receive a legally binding request (such as a court order), we may respond within the limits of the law. Because Openloop is an offline device, however, the manufacturer has no means of accessing user data.

Privacy of companion wallets

The wallet software you pair with Openloop (Sparrow Wallet, MetaMask, and so on) each has its own privacy policy.

- Sparrow Wallet: open source, privacy-focused
- MetaMask: governed by ConsenSys's privacy policy
- Other software: check each application's policy

ℹ **Tip**: for maximum privacy, we recommend combining QR-code communication, your own node, and Sparrow Wallet.

Deleting your data

To completely delete your data:

1. Settings → **Security** → **Factory Reset**
2. Choose "Yes" on the confirmation screen
3. All data is completely deleted

⚠ **Warning**: this **cannot be undone**. Make sure you have a backup of your recovery phrase first.

1.7 Export Controls and Compliance

Openloop contains cryptographic technology and may be subject to import/export controls in some countries and regions.

Cryptographic technology used

Openloop uses the following cryptographic technology:

Technology	Purpose	Standard
ECDSA (secp256k1)	Bitcoin/Ethereum/TRON signing	SEC 2
ECDSA (P-256)	FIDO2/PIV signing	FIPS 186-4
EdDSA (Ed25519)	XRP/Solana/FIDO2/PIV signing	RFC 8032
RSA-2048	PIV signing	PKCS#1 v1.5
SHA-256	Hashing	FIPS 180-4
SHA-512	XRP key derivation	FIPS 180-4
Keccak-256	Ethereum signature hashing	FIPS 202
RIPEMD-160	Bitcoin address generation	ISO/IEC 10118-3
AES-256-GCM	Encrypting private keys and the recovery phrase	FIPS 197 / SP 800-38D
PBKDF2	Deriving the seed from a BIP39 mnemonic	RFC 8018
HMAC-SHA512	BIP32 key derivation	RFC 2104
ECDH key exchange	Dual-secure key derivation with the SE050	SEC 1
AES-CTR	Encryption on the SE050	SP 800-38A
BLE encryption	Bluetooth communication	Bluetooth 4.2+ LE Secure Connections

About export controls

Export from Japan:

- Cryptographic products are subject to the Foreign Exchange and Foreign Trade Act
- As a consumer product, an export licence is likely **not required**
- Bulk exports or shipments to particular countries need to be checked individually

United States (EAR):

- Cryptographic products fall under the Export Administration Regulations (EAR)
- Consumer cryptographic products are classified as **EAR99** or **5A992.c**
- Export to embargoed countries (North Korea, Iran, Syria, Cuba, and others) is prohibited

EU regulation:

- Subject to the Dual-Use Regulation (EU 2021/821)
- Consumer products are normally **out of scope**

Prohibited uses

Using Openloop for the following purposes is **prohibited**:

- ✗ Money laundering
- ✗ Terrorist financing
- ✗ Evading economic sanctions
- ✗ Illegal transfers of funds
- ✗ Concealing assets to evade tax
- ✗ Any other illegal activity

Your responsibilities

You are responsible for complying with the following:

1. The laws of your country of residence
   - Laws governing holding and trading crypto assets
   - Tax law (capital gains tax, income tax, and so on)
   - Reporting obligations (for example, reporting transactions above a threshold)
2. Import and export controls
   - Checking the rules before taking this product to another country
   - Not bringing it into embargoed countries
3. Cooperation with KYC
   - Meeting KYC/AML requirements when using exchanges
   - Keeping transaction records as required
4. Tax filing
   - Keeping proper records of crypto-asset transactions
   - Filing accurately with the tax authorities

Disclaimer

⚠ **Important: your responsibility**

The manufacturer and developers make no warranty whatsoever that Openloop meets the export-control conditions of any given country. If you import or export this product,

you must check the applicable laws and regulations yourself and obtain any necessary permits.

- The manufacturer and developers are not liable if you break the law
- Laws and regulations can change in any country
- Deciding whether import or export is permitted is your responsibility
- If anything is unclear, consult a legal professional

Tip: tax treatment of crypto assets is complex. If you are making large transactions, we recommend consulting a tax accountant.

---

2. Unboxing and Initial Setup

2.1 What's in the box

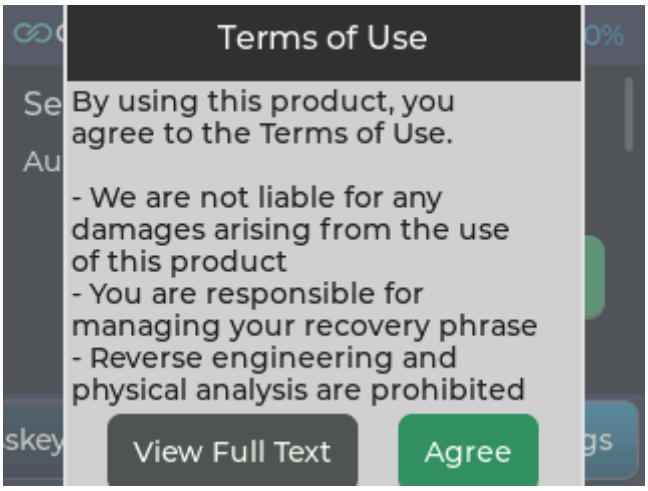
When you open the box, check that you have:

- The Openloop device

Note: a USB-C cable is not included. You will need to supply your own USB-C cable (USB 2.0 or later) for charging and firmware updates.

2.2 First Boot

1. Charge: connect to power with a USB-C cable (a PC or a USB charger)
2. Power on: the device starts automatically
3. Splash screen: the Openloop logo appears
4. Choose a language: the "Select Language / 言語を選択" dialog appears. Tap "English" or "日本語" (you can change this later under Settings → Language)
5. Accept the terms: on first boot the end-user licence agreement (EULA) is displayed. Read it and tap "Agree." Tapping "View full text" shows a QR code so you can read the full agreement on your smartphone
6. Setup begins: after you accept the terms, the setup dialog appears automatically



The licence agreement screen shown on first boot

Splash screen

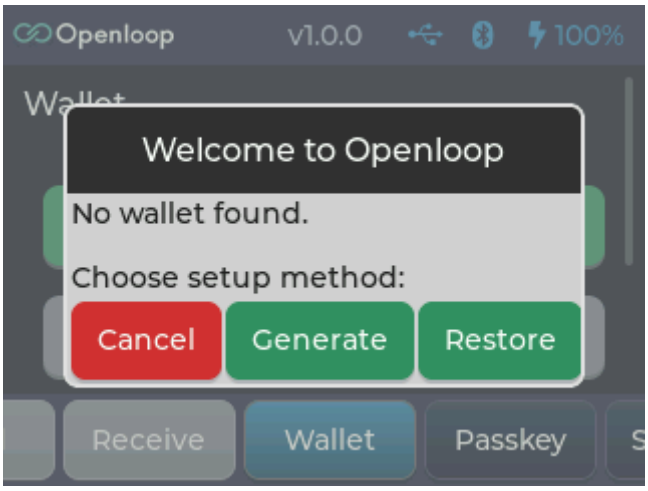
2.3 Creating or Restoring a Wallet (most important)

On first boot, if no wallet exists, the **setup dialog appears automatically**.

⚠ **On firmware v1.1.0 and earlier**: this dialog may be replaced by a screen that says "Wallet Corrupted". **Nothing is wrong with your device.** Go ahead and choose "Generate" or "Restore" (see 13.2). **This false alarm is fixed in v1.1.1** — updating to v1.1.1 or later stops it appearing (see chapter 12).

The automatic dialog on first boot

The "Welcome to Openloop" dialog:



Setup dialog

Options:

- "Generate": create a new wallet (→ go to Step 1)
- "Restore": restore a wallet from an existing recovery phrase (→ see section 8.4)
- "Cancel": set up later

Tip: this dialog also appears automatically after you erase a wallet. You can open the same screen from the "Wallet" screen → "Create Wallet" button.

Creating a new wallet

Step 1: Choose the mnemonic length

Tapping "Generate" brings up the **mnemonic length selection screen**.

The "Select mnemonic length" dialog:

Recovery phrase length selection

Which should you choose?

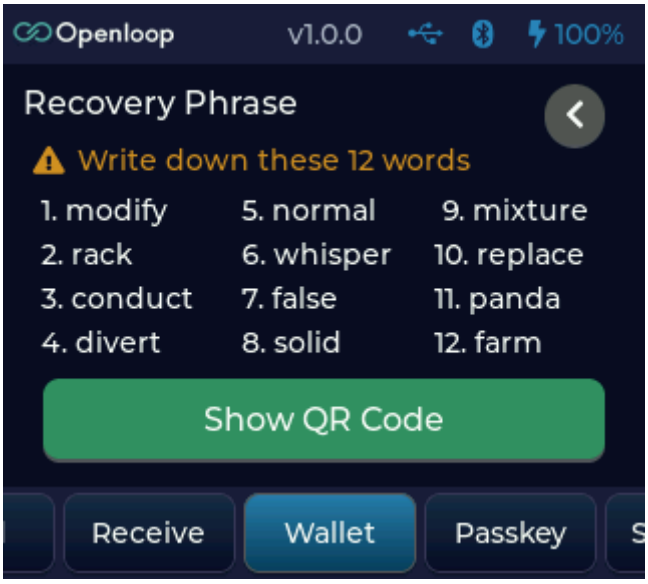
Length	Security	Entropy	Recommended for
12 words	High	128 bits	General use, easier to record
24 words	Very high	256 bits	Large holdings, maximum security

Step 2: Record the recovery phrase

⚠ **This is the single most important step. Concentrate and do it accurately.**

Once you choose 12 or 24 words, a new recovery phrase is generated, and you can view it on the “Wallet” → “Recovery Phrase” screen.

1. Write down the words shown on screen
   - Use the included record sheet
   - **The order matters** (1st, 2nd, and so on)
   - Watch for spelling mistakes (for example, “work” and “word” are different words)
2. Store it somewhere safe
   - A fireproof safe, a safe deposit box, and so on
   - Keep multiple copies in different places (recommended)



Recovery phrase display

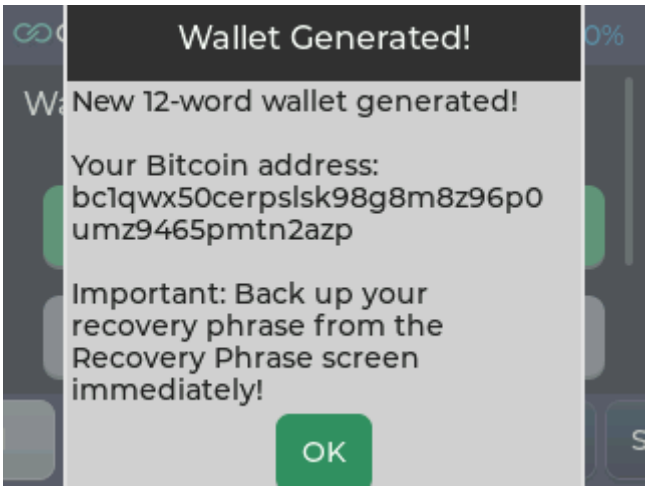
Example recovery phrase (12 words):

```
1. modify     5. normal      9. mixture
2. rack       6. whisper    10. replace
3. conduct    7. false      11. panda
4. divert     8. solid      12. farm
```

⚠️ **Warning**: this is a **sample**. Never use it for a real wallet.

Step 3: Wallet creation complete

- Tap the “Done” button
- The message “Wallet created!” appears
- You can see the generated Bitcoin address
- Your wallet is now ready



Wallet created

Checkpoints:

- I wrote the recovery phrase down on paper
- I checked the spelling and the order
- I stored it somewhere safe
- I told my family where it is (optional)

Operations on the “Wallet” screen

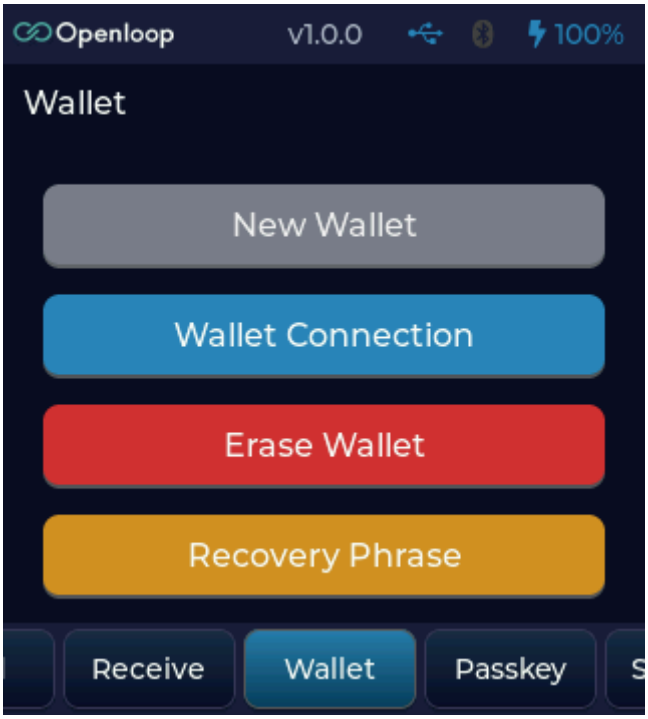
On the Wallet screen, buttons are enabled or disabled according to the current wallet state:

Button	No wallet	Wallet exists	Colour
Create Wallet	✓ Enabled	✗ Disabled	Blue / grey

Button	No wallet	Wallet exists	Colour
Recovery Phrase	✗ Disabled	✓ Enabled	Yellow / grey
Erase Wallet	✗ Disabled	✓ Enabled	Red / grey

What the button colours mean:

- Blue: a normal operation
- Yellow: an operation with a warning (showing secret information)
- Red: a dangerous operation (deleting data)
- Grey: disabled



Wallet screen

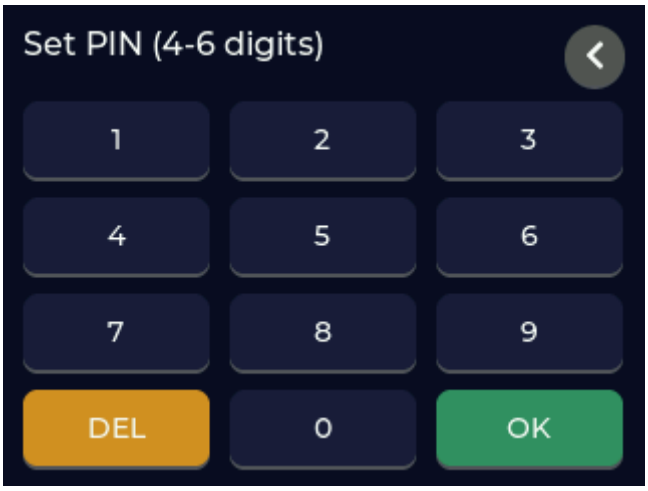
Tip: after you erase a wallet, the “Welcome to Openloop” dialog appears again the next time you access it.

2.4 Setting a PIN

After creating a wallet, set a PIN to protect the device.

Step 1: Go to the PIN screen

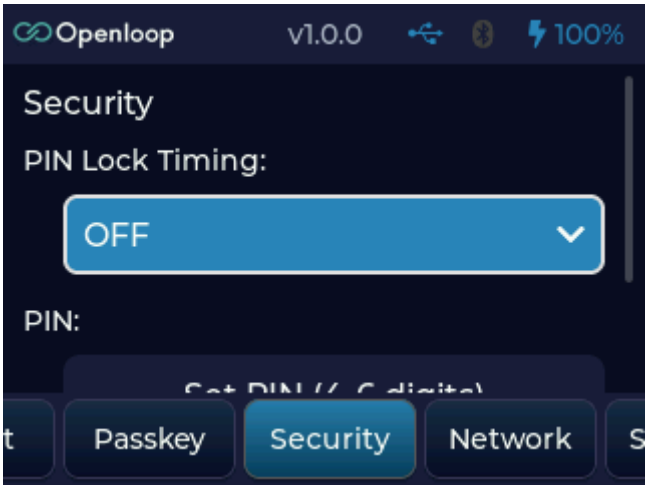
1. Tap “Security” in the navigation bar → “Set PIN (4-6 digits)”



PIN entry screen

Step 2: Enter the PIN

1. Enter a new PIN (4–6 digits)
   - Recommended: 6 digits or more
   - Avoid: 1234, 0000, your birthday, or anything else easy to guess
2. Enter it again to confirm
   - Type the same PIN
3. Done
   - The message “PIN set” appears



PIN lock timing setting

Tip: write your PIN down so you do not forget it (and store it **somewhere separate** from your recovery phrase).

⚠ PIN entry limits (lockout)

For security, entering the PIN incorrectly several times in a row temporarily locks the device:

Failed attempts	Lockout
1–2	None (retry immediately)
3	30 seconds
4	1 minute
5	5 minutes
6–9	10 minutes
10	⚠ The device automatically erases all data

⚠ **Most important**: getting it wrong 10 times in a row makes the device **automatically perform a factory reset**. In addition to your wallet (recovery phrase), PIN, and all settings, **your FIDO2 passkeys and PIV keys and certificates are also completely erased and can never be recovered.**

Crypto assets can be restored from your recovery phrase, but passkeys must be registered again at each service, and PIV keys must be regenerated with new certificates issued (see also 8.1, 9.4, and 10.7).

After nine failures, wait for the lockout to clear and then enter the correct PIN calmly. Powering the device off does not cancel the pending erase — the confirmation screen reappears on the next boot.

2.5 Language

You can choose Japanese or English.

1. Tap “Settings” → “Language”
2. Choose “日本語” or “English”
3. The whole interface switches to the language you chose

Language setting

Tip: you can change the language at any time.

2.6 Sound

You can configure the click sound and other tones.

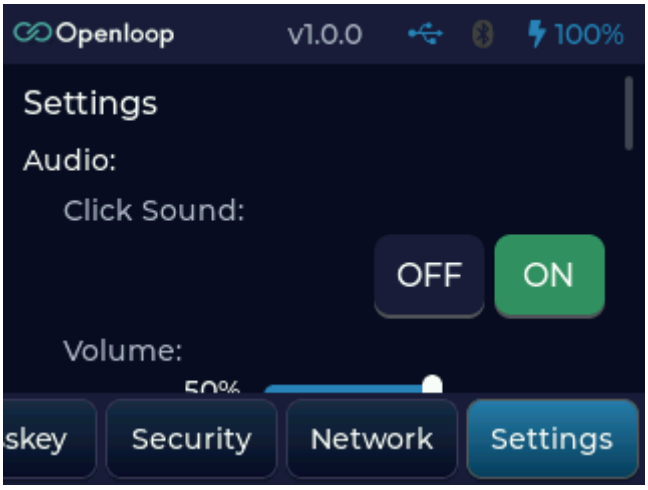
Turning the click sound on and off

1. “Settings” → “Sound” → “Click sound”
2. Use the toggle to turn it on or off

Tip: you can turn the click sound off when using the device somewhere quiet.

Adjusting the volume

1. “Settings” → “Sound” → “Volume”
2. Adjust with the slider
   - 0% (silent) to 100% (maximum)



Sound settings

Tip: the confirmation tone played when signing a transaction also follows the volume setting.

---

3. Reading the Screen and Basic Operation

3.1 Screen layout

The Openloop screen consists of three areas:

```
┌──────────────────────────────────────────────────────┐
│                  [ Status bar ]                      │  ←  Battery / BLE / USB
├──────────────────────────────────────────────────────┤
│                                                      │
│                [ Content area ]                      │  ←  Main information and buttons
│                                                      │
├──────────────────────────────────────────────────────┤
│ Home Send Receive Wallet Passkey Security Coin Set   │  ←  Navigation bar (scrolls sideways)
└──────────────────────────────────────────────────────┘
```

Screen layout

Status bar (top)

- Left: menu icon, application title
- Right: battery level, BLE connection status, USB connection status

Navigation bar (bottom)

The navigation bar **scrolls horizontally** and gives direct access to eight screens:

Label	Screen	Function
Home	Home screen	Check wallet information
Send	Send screen	Transaction signing
Receive	Receive screen	Show addresses and QR codes
Wallet	Wallet screen	Create, erase, and export a wallet
Passkey	Passkey & PIV screen	Manage FIDO2 passkeys and PIV keys
Security	Security screen	PIN lock settings
Coin	Coin & network screen	Coin and network settings
Settings	Settings screen	Sound, language, USB, BLE, factory reset

Tip: swipe the navigation bar left and right to reach the items that are hidden.

3.2 Touch basics

- **Tap**: press the screen lightly with a finger (to select a button)
- **Swipe left/right**: swiping the content area sideways switches to the adjacent screen, so you can move intuitively between the eight screens in the navigation bar
- **Swipe right (back)**: while an overlay such as a QR code display or the camera is showing, swiping right returns to the previous screen
- **Swipe up/down**: scrolls long content
- **Long press**: not used at present

Tip: tapping a button plays a click sound (which you can turn on or off in Settings).

Working with dialogs

In confirmation dialogs and signing approval screens, buttons are laid out like this:

- **Right side**: the affirmative button (OK, Agree, Sign, and so on)
- **Left side**: the negative button (Cancel, Reject, and so on)

3.3 Home screen

Shows the current state of your wallet at a glance.

What it shows:

- The Openloop logo
- Wallet type: the current connection mode (`Air Gap` / `Air Gap / USB` / `Air Gap / BLE` / `Air Gap / USB / BLE`)
- Mainnet addresses for five currencies (scroll up and down):
  - BTC: Bitcoin mainnet address
  - ETH: Ethereum mainnet address
  - XRP: XRP mainnet address
  - SOL: Solana mainnet address
  - TRX: TRON mainnet address

Home screen

Tip: the home screen always shows mainnet addresses. To check a testnet address, switch networks on the “Receive” screen.

Default coin

Scrolling the address card on the home screen (headed “Default coin”) up and down highlights the selected currency in the accent colour. That is the “default coin,” and it becomes the app mode reported to wallet software on your PC over USB. This is equivalent to Ledger’s “app switching.”

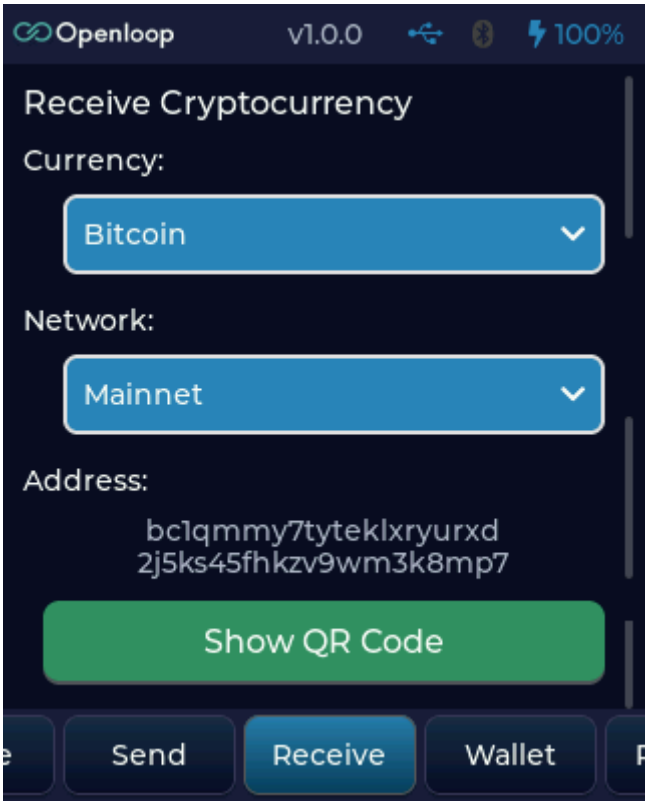
Normally it switches automatically in response to requests from the wallet software, but some wallet software requires you to select it manually.

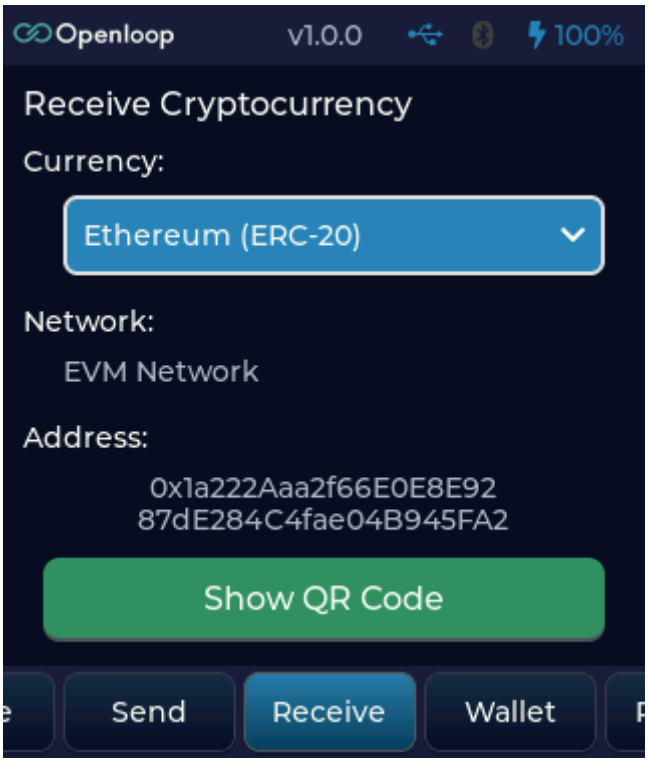
3.4 Receive screen

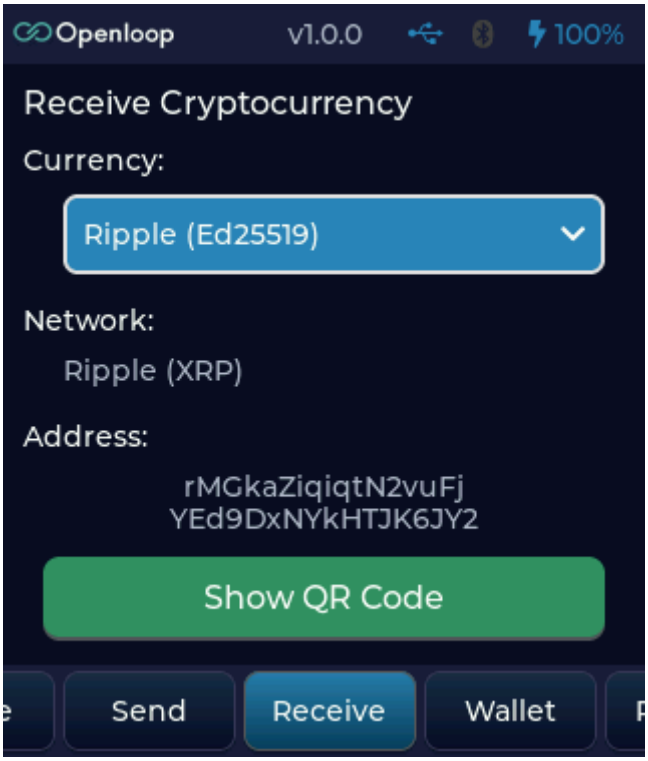
Shows the address and QR code for receiving crypto assets.

Openloop is a **hierarchical deterministic (HD) wallet**: following BIP32/BIP44, it derives many keys hierarchically from a single master seed. Any derived key can be used, and changing the key for each transaction helps protect your privacy.

The Receive screen can show representative addresses for Bitcoin, Ethereum, XRP, Solana, and TRON, as well as any public-key address your wallet holds by specifying a BIP44 custom path.




Openloop
v1.0.0
100%
Receive Cryptocurrency
Currency:
Ethereum (ERC-20)
Network:
EVM Network
Address:
0x1a222Aaa2f66E0E8E92
87dE284C4fae04B945FA2
Show QR Code
Send
Receive
Wallet

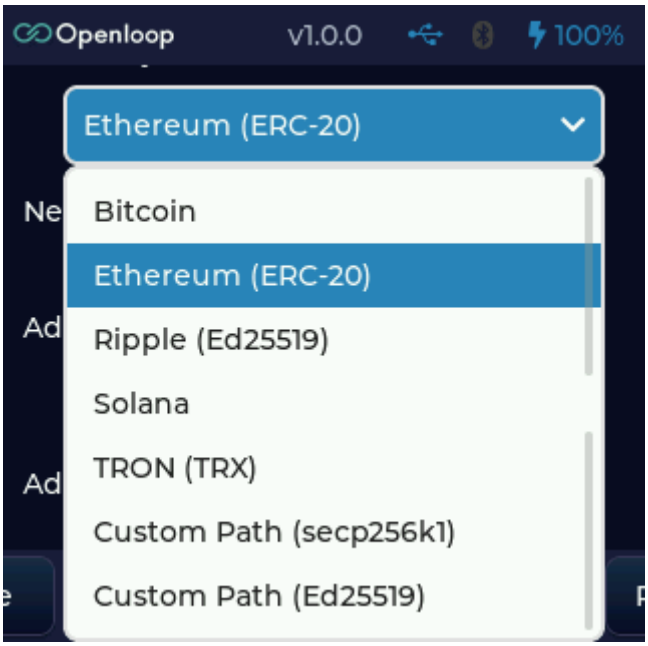

Openloop
v1.0.0
100%
Receive Cryptocurrency
Currency:
Ripple (Ed25519)
Network:
Ripple (XRP)
Address:
rMGkaZiqiqtN2vuFj
YEd9DxNYkHTJK6JY2
Show QR Code
Send
Receive
Wallet

How to use it:

1. Tap “Receive” in the navigation bar
2. Choose a currency (Bitcoin / Ethereum / XRP / Solana / TRON / custom path)
3. The receiving address appears
4. Tap “Show QR” to display the QR code

What each currency choice does:

Choice	Behaviour
Bitcoin	Shows the Bitcoin address at Account 0, Index 0
Ethereum (ERC-20)	Shows the Ethereum address at Account 0, Index 0
Ripple (Ed25519)	Shows the XRP address at Account 0, Index 0
Solana	Shows the Solana address at Account 0. “BIP32 Path” lets you choose the derivation depth (2 / 3 / 4 levels; 3 is the default)
TRON (TRX)	Shows the TRON address at Account 0, Index 0
Custom path (secp256k1)	Specify any Account/Index under BIP44 (secp256k1 curve)
Custom path (Ed25519)	Specify any Account/Index under BIP44 (Ed25519 curve)



Receive screen dropdown

If you choose a custom path (BIP32/BIP44):

1. Select “Custom path (secp256k1)” or “Custom path (Ed25519)”
2. Choose the “Coin” (BTC / ETH / XRP / SOL / TRX)
3. Choose the “Account” (0–9)
4. Choose the “Change” value ((none) / 0 (Ext) / 1 (Int); the default is `0 (Ext)`)
5. Choose the “Index” ((none) / 0–99)
6. The “Full path” field at the bottom shows the derivation path (for example `m/84'/0'/0'/0/0`), with the corresponding address below it

This lets you display and verify on Openloop any address your companion wallet is using.

Parameter	Description	Choices
Account	The account number within the wallet	0–9
Change	External (receiving) or internal (change)	(none) / 0 (Ext) / 1 (Int)
Index	The address number within the account	(none) / 0–99

Tip: choosing “(none)” for Change or Index omits that level, making the path shallower. Use this when you need a three-level path, as Solana does.

BIP32 derivation path format:

```
m / purpose' / coin_type' / account' / change / index
```

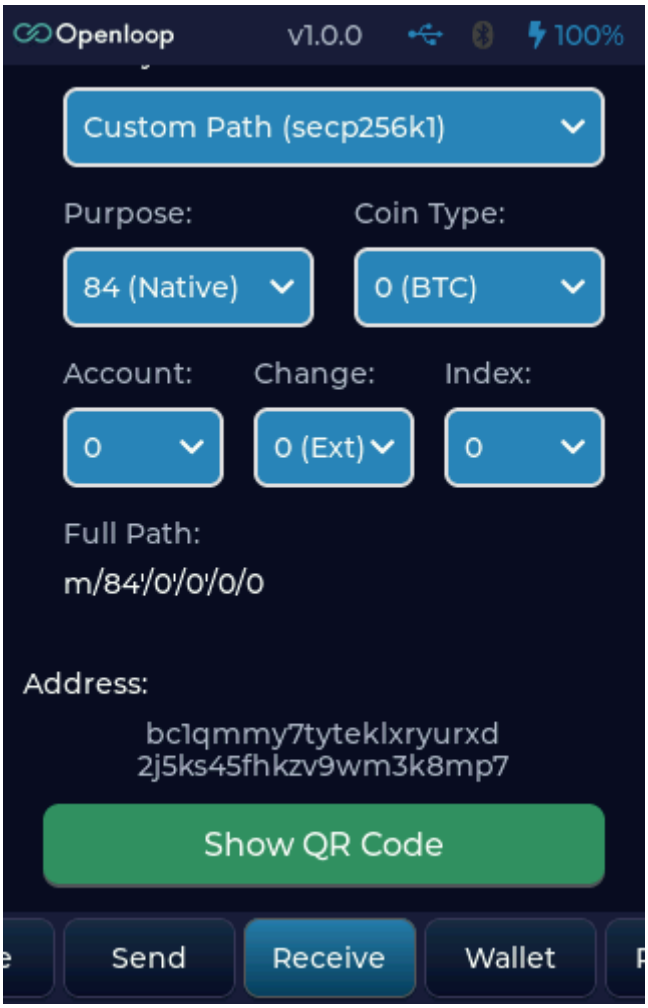
Standard paths by currency:

Currency	Standard path	Standard	Curve
Bitcoin	m/84’/0’/0’/0/0	BIP84 (Native SegWit)	secp256k1
Ethereum	m/44’/60’/0’/0/0	BIP44	secp256k1
XRP (Ed25519)	m/44’/144’/0’/0’/0’	BIP44 (all levels hardened)	Ed25519
XRP (secp256k1)	m/44’/144’/0’/0/0	BIP44	secp256k1
Solana	m/44’/501’/0’ (Receive screen default) m/44’/501’/0’/0’ (when signing)	SLIP-0010 (all levels hardened)	Ed25519
TRON	m/44’/195’/0’/0/0	BIP44	secp256k1

⚠ **Note**: for XRP the derivation path changes with the curve you select (Ed25519 hardens every level). Set the curve on the “Connect Wallet” screen (see 4.1).

ℹ **Example**: if you want to use several receiving addresses for different purposes (work and personal, say), use addresses with different indexes.

For details, see “5. Receiving Crypto Assets”



Receive screen

Tip: scanning the QR code with a phone app avoids address typos.

3.5 Send screen

Signs transactions so you can send crypto assets.

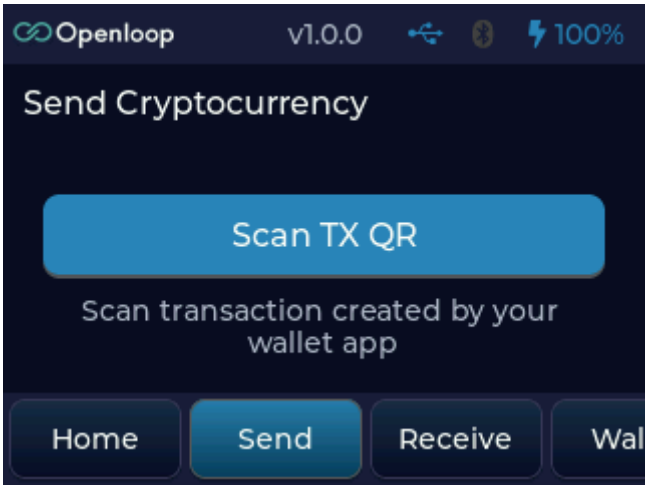
Important: this screen is for signing transactions using the **Air Gap method (QR codes)**.

Air Gap (QR code):

- Tap the “Scan transaction QR” button
- Scan the transaction QR code shown by your companion wallet (Sparrow Wallet, for example)
- The signing confirmation screen appears
- For details see “6. Sending Crypto Assets”

USB / BLE:

- You do not need to press anything on this screen
- When your companion wallet (MetaMask, for example) sends a signing request, **the confirmation screen appears automatically**
- You must set up the companion wallet connection in advance (see "4. Pairing with a Companion Wallet")



Send screen

⚠ **Important**: Openloop only signs. The actual send (broadcast) is performed by your companion wallet.

3.6 Other screens

An overview of the screens you can reach directly from the navigation bar. See the relevant chapter for details.

Screen	Contents	Details
Wallet	Create, export, erase, recovery phrase	Ch. 8
Passkey	FIDO2 passkey management, PIV key management	Ch. 9, Ch. 10
Security	PIN lock timing, set/change/delete PIN	8.1
Coin	View and configure coins and networks	Ch. 14
Settings	Sound, language, USB, BLE, factory reset, version	Ch. 7, Ch. 11

Tip: the wallet pairing feature is reached from “Connect Wallet” on the “Wallet” screen. See “4.1 The Connect Wallet screen” for details.

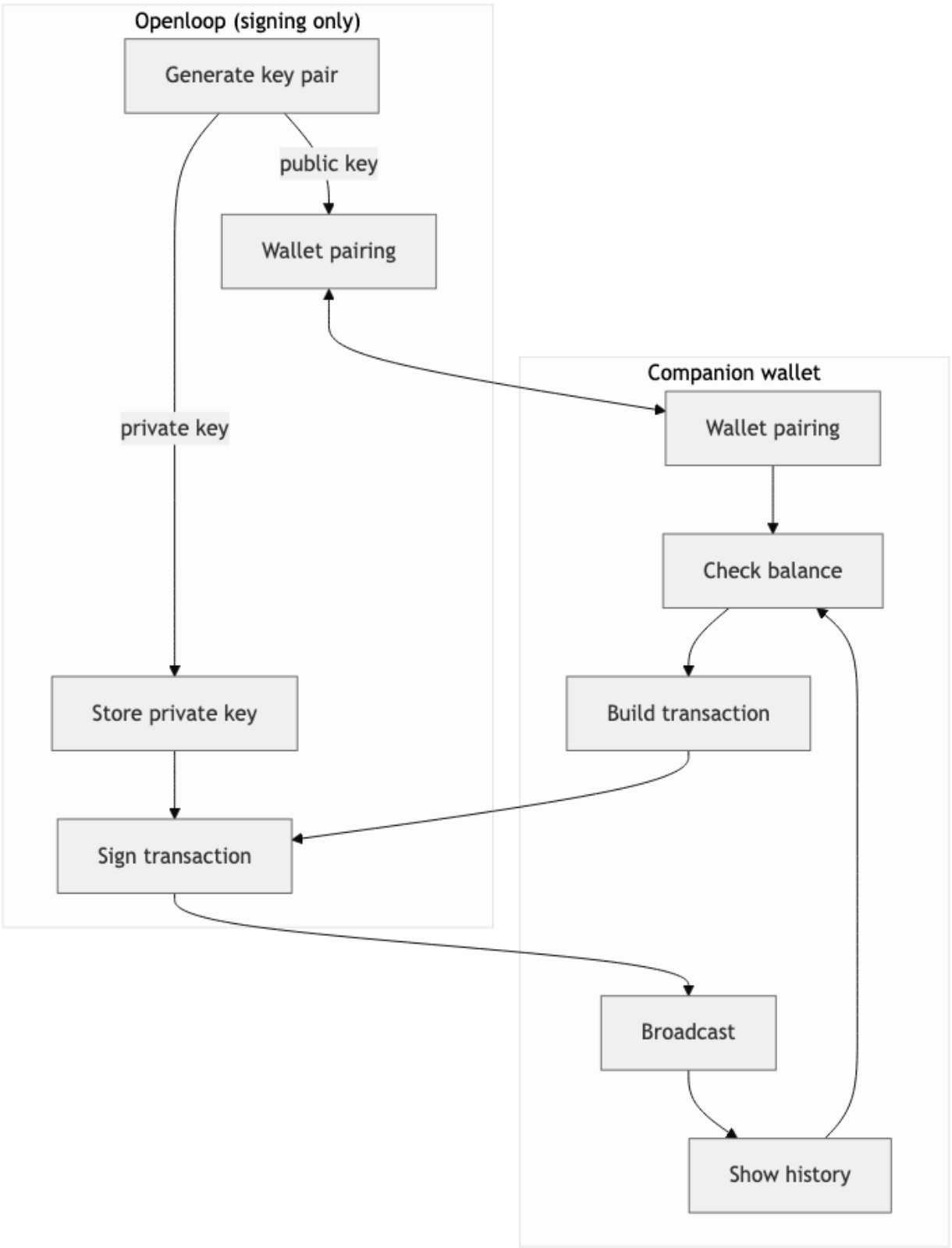
---

4. Pairing with a Companion Wallet

Important: before you use Openloop, always set up the connection with your wallet software (your companion wallet).

Openloop is a signing-only device. To actually send and receive crypto assets, you need to pair it with wallet software (a companion wallet).

How wallet pairing works



Choosing a connection method

Method	Currencies	Example wallets	Recommendation
Air Gap	BTC/ETH/XRP/SOL	Sparrow Wallet and others	★★ For those who want no electronic communication
USB	BTC/ETH/XRP/SOL/ TRX	Sparrow/MetaMask/ Rabby and others	★★★ Recommended for everyday use
BLE	ETH	MetaMask Mobile	★★★ Recommended for everyday use

About security: with every method, the private key never leaves the Openloop device, and by design you must always approve the signature on the device itself.

4.1 The Connect Wallet Screen

How to get there: “Wallet” in the navigation bar → “Connect Wallet”

This screen displays the public-key information needed to pair with a companion wallet, as a QR code.

When you need it

Connection	Is this screen needed?	Explanation
Air Gap	**Yes**	Displays the public-key QR code for your companion wallet to scan
USB	No	Turn USB on in Openloop, then connect from the companion wallet side
BLE	No	Turn BLE on in Openloop and complete pairing, then connect from the companion wallet side

Tip: for USB and BLE, as long as the transport is enabled on Openloop, you can pair without going through this public-key QR screen. In MetaMask and similar wallets, choose “Connect hardware wallet.”

Choosing a currency

Select the currency to pair from the dropdown menu:

- **Bitcoin**: pair with Sparrow Wallet and others over Air Gap
- **Ethereum**: pair with a companion wallet over Air Gap
- **XRP (Ripple)**: pair over Air Gap, or change the curve setting
- **Solana**: pair with a companion wallet over Air Gap

Options by currency

Bitcoin

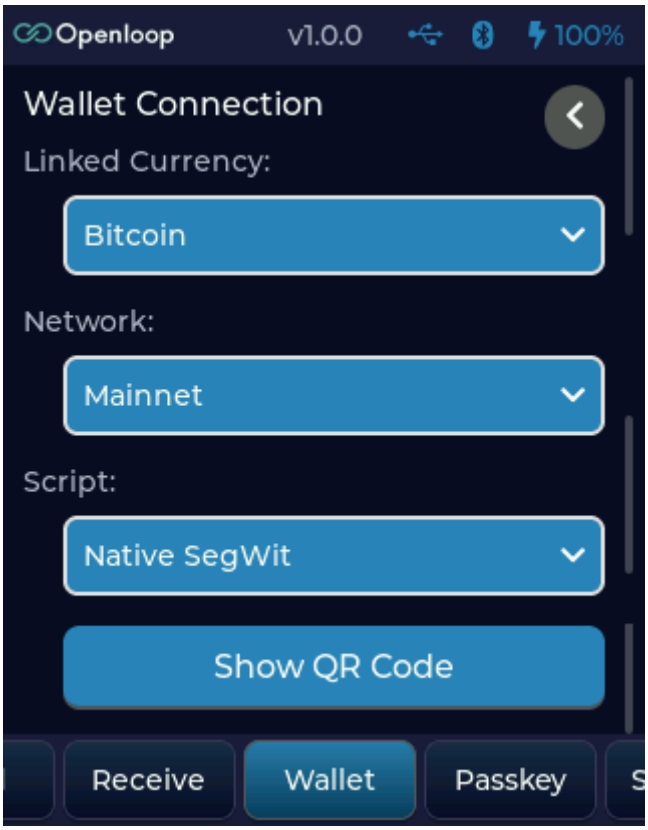
Option	Description
Mainnet	Show the public key for the production network
Testnet	Show the public key for the test network
Script	Choose the script type for the derived key (see below)

Script choices:

Choice	Derivation path	Wallet type in Sparrow
Native SegWit (default)	m/84’/0’/0’ (zpub)	Native SegWit (P2WPKH)
Nested SegWit	m/49’/0’/0’ (ypub)	Nested SegWit (P2SH-P2WPKH)
Legacy	m/44’/0’/0’ (xpub)	Legacy (P2PKH)
Multisig	m/48’/0’/0’/2’ (Zpub)	Multi Signature (P2WSH)

⚠ **Important**: the script type you choose here must match the wallet type you create in your companion wallet. If they do not match, the addresses will differ.

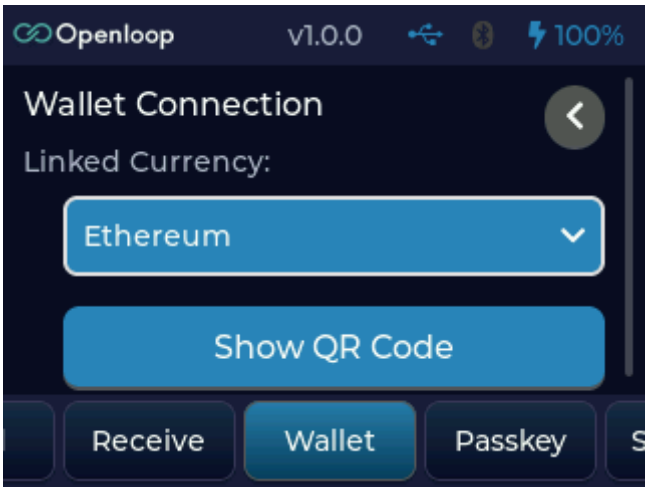
Tapping “Show QR” displays the extended public key for the selected script (zpub / ypub / xpub / Zpub) as a QR code.



Bitcoin Connect Wallet screen

Ethereum

There are no options. Tapping “Show QR” displays the address information as a QR code.

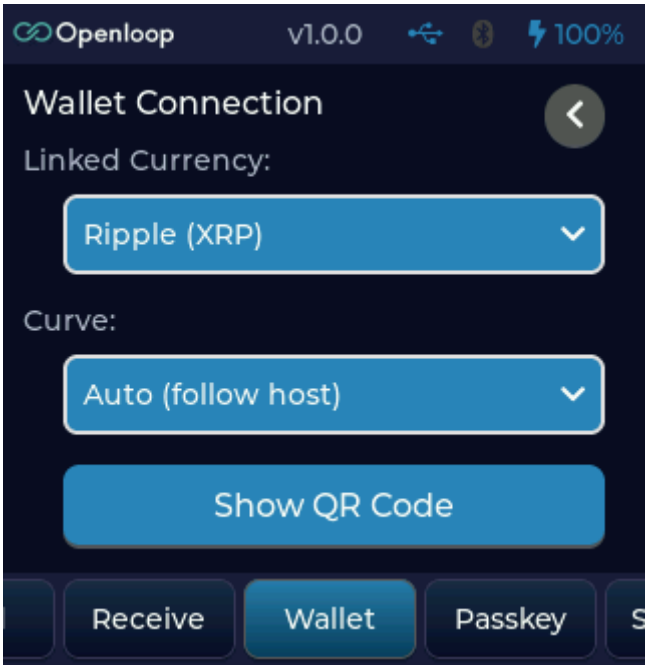


Ethereum Connect Wallet screen

XRP (Ripple)

Option	Description
Auto	

Option	Description
	Choose the curve according to the P2 parameter from the host (default)
Ed25519	Always use the Ed25519 curve (ignore the P2 parameter)
secp256k1	Always use the secp256k1 curve (ignore the P2 parameter)



XRP Connect Wallet screen

⚠ An important note about the XRP curve setting

The XRP curve setting affects **all three transports — Air Gap, USB, and BLE**. This is different from the other currencies.

Background:

XRP Toolkit (via the hw-app-xrp library) has a bug: it always sends P2=0x40 (secp256k1), even when you are using an Ed25519 address.

Setting	Behaviour	Recommendation
Auto	Follow the host's P2	✗ with XRP Toolkit (signing fails)
Ed25519	**Always Ed25519**	✓ **Recommended when using XRP Toolkit**

Setting	Behaviour	Recommendation
secp256k1	Always secp256k1	When Ledger compatibility is required

Recommended settings:

- **Using XRP Toolkit**: set it to “Ed25519”
- **Other wallets**: “Auto” works fine

Tip: Ed25519 is the newer format and the default for software wallets. Unless you have a specific reason not to, we recommend “Ed25519.”

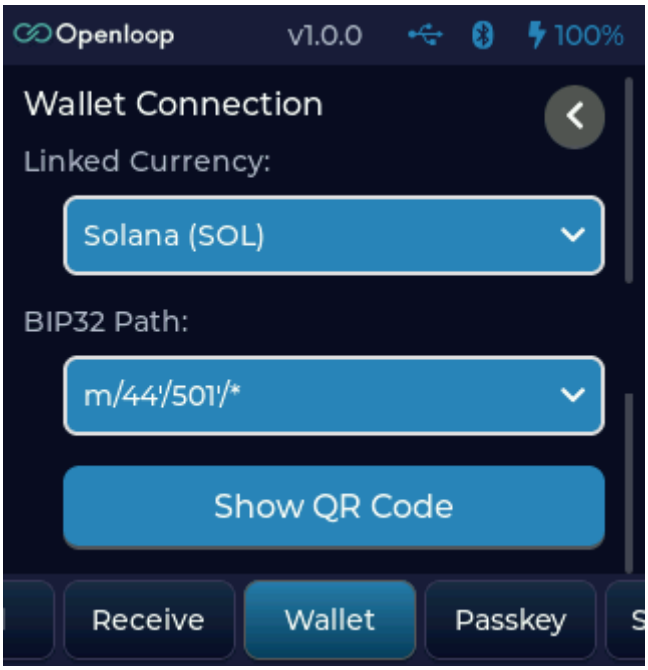
Solana

“BIP32 Path” lets you choose how deep the derivation path goes.

Option	Path	What it means
`m/44'/501'`	2 levels	A single address with no account number
`m/44'/501'/*`	3 levels (default)	A separate address per account number
`m/44'/501'/*/0'`	4 levels	One more level below the account number

Important: a different depth derives a different address. Match it to the path format your companion wallet uses. If they do not match, the addresses will differ. If you are unsure, leave it at the default of 3 levels.

Tapping “Show QR” displays the Solana public-key information for the selected depth as a QR code.



Solana Connect Wallet screen

Pairing at a glance

1. **Air Gap pairing (Bitcoin + Sparrow Wallet)**
    1. In Sparrow Wallet, choose “New Wallet” → “Airgapped Hardware Wallet”
    2. Display the QR code on Openloop (“Wallet” → “Connect Wallet” → “Bitcoin”)
    3. Scan the QR in Sparrow → paired
2. **USB pairing (Ethereum + MetaMask)**
    1. In MetaMask, choose “Add account” → “Hardware wallet” → “Ledger”
    2. Connect Openloop over USB
    3. Select an address → paired
3. **BLE pairing (Ethereum + MetaMask Mobile)**
    1. Pair over BLE on Openloop first (see “7.4 BLE (Bluetooth) in detail”)
    2. In MetaMask Mobile, choose “Hardware wallet” → “Bluetooth”
    3. Select Openloop → paired

▲ **Note**: for step-by-step instructions on each method, see “6. Sending Crypto Assets.”

▲ A caution when using several wallets

Do not run several wallet applications at the same time.

- ✗ Running Sparrow Wallet and MetaMask simultaneously

- ✗ Opening different wallets in several browsers

What goes wrong:

- Contention for the USB port
- Confusion between signing requests
- Unexpected errors

The right way:

- ✓ Sending Bitcoin: run only Sparrow Wallet
- ✓ Sending Ethereum: run only MetaMask
- ✓ When you are done, quit the wallet software before working with another currency

---

5. Receiving Crypto Assets

⚠ **Important**: Openloop **has no balance display**. To check whether funds have arrived, use your companion wallet (Sparrow Wallet, MetaMask, and so on) or a blockchain explorer.

5.1 How receiving works

To receive crypto assets, you need to give the sender your **receiving address**.

There are two ways to obtain a receiving address:

Method	Description	When to use it
From the companion wallet	Use the address shown in the paired wallet software (Sparrow Wallet, MetaMask, and so on)	Everyday receiving
From Openloop itself	Show the QR code on the “Receive” screen for the sender to scan	When no companion wallet is connected, or when verifying for security

ℹ **Security tip**: checking that the address shown in your companion wallet matches the one on Openloop lets you detect address tampering by malware.

The basic flow:

1. Confirm the currency and network
2. Obtain the receiving address (from the companion wallet or from Openloop)

3. Have the funds sent from an exchange or another wallet
4. Confirm the transaction (on the blockchain)

5.2 Checking which crypto assets are supported

Openloop supports several crypto assets and networks. Check that the currency you want to receive is supported.

Note: you do not have to do this before every transaction. As long as the correct currency and network are configured in your companion wallet, they are determined automatically at signing time.

Getting to the Coin & Network screen

Tap “Coin” in the navigation bar

Supported currencies

Currency	Description	Typical use
Bitcoin (BTC)	The most widely used crypto asset	Store of value, transfers
Ethereum (ETH)	Smart-contract capable	DeFi, NFTs, tokens
XRP (Ripple)	Fast, low-fee transfers	International remittance
Solana (SOL)	A fast, low-fee blockchain	DeFi, NFTs
TRON (TRX)	A high-throughput blockchain	DeFi, stablecoins

Broad Ethereum support:

Openloop supports **every EVM-compatible network** and **every ERC-20 token**.

Built-in data:

- **2,599 major tokens** and **215 networks** are built in
- Token names and network names are shown on the signing confirmation screen

When something is not built in:

- Tokens that are not built in: instead of a token name, the screen shows “ERC-20 Token” or “Unknown ERC-20,” together with an orange warning, “Unknown token - verify contract!” The contract address is shown in full
- Networks that are not built in: instead of a network name, the screen shows something like “Chain ID 12345,” and the currency symbol for the amount and fee becomes “ETH?”
- **Signing is still possible** in both cases

For details, see “14. Supported Crypto Assets and Networks.”


Openloop
v1.0.0
100%
Currency & Network
Bitcoin
Supported Networks:
• Mainnet
• Testnet
Air Gap Format
BBQr
USB/BLE Format
• APDU
Ethereum
Supported Networks:
All EVM networks (excerpt)
• Ethereum Mainnet
• Optimism
• Flare Network
• Songbird
• Elastos
• KardiaChain
• Cronos
• Rootstock RSK
Supported Tokens:
All ERC-20 tokens (excerpt)
• USDC (USDC)
• USDT (Tether)
• DAI (Dai)
• LINK (Chainlink)
• UNI (Uniswap)
• AAVE (Aave)
• ARB (Arbitrum)
• JPYC (JPY Coin)
Air Gap Format
• UR
USB/BLE Format
• APDU
Ripple (XRP)
Supported Networks:
• XRP Mainnet
Air Gap Format
• UR
USB/BLE Format
• APDU
Solana (SOL)
Supported Networks:

Mainnet vs. testnet

⚠️ **Important**: choosing the wrong network can cost you your assets.

Network	Purpose	Value
Mainnet	Real transactions (production)	Has real value
Testnet	Development and testing	No value (for practice)

ℹ️ **If you are new to this**: we strongly recommend practising on **testnet** first, then moving to mainnet.

Networks per currency:

Currency	Mainnet	Testnet
Bitcoin	BTC Main	BTC Test
Ethereum	ETH Main	ETH Sep (Sepolia)
XRP	XRP Main	XRP Test

Additional Ethereum networks (layer 2 and so on):

- Arbitrum One / Arbitrum Sepolia
- Optimism / Optimism Sepolia
- Base / Base Sepolia
- And many more

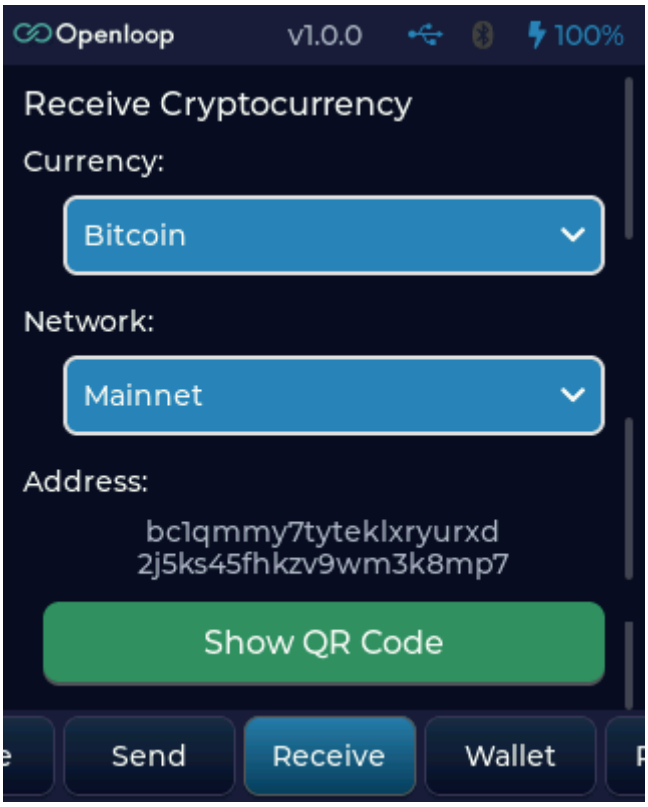
⚠️ **Warning**: always confirm that the sending and receiving networks are correct.

5.3 Displaying a receiving address on Openloop

Use the “Receive” screen on Openloop when you want an address without using a companion wallet, or when you want to verify that the address shown in your companion wallet is correct.

Step 1: Go to the Receive screen

1. Tap “Receive” in the navigation bar
2. The receiving address for the current currency and network appears



Receive screen

Address verification tip: when you pick a currency on the Openloop Receive screen, the address for “Account 0, Index 0” is shown by default.

Using a custom derivation path (BIP32/BIP44)

If your companion wallet uses a different account or index, you can specify a custom BIP32/BIP44 path on Openloop to display the same address.

How to do it:

1. On the Receive screen, choose “Custom path (secp256k1)” or “Custom path (Ed25519)” from the currency dropdown
2. Select “Coin,” “Account,” “Change,” and “Index” (see 3.4)
3. The “Full path” field shows the derivation path, with the corresponding address below it

Example 1: Sparrow Wallet is using the second address

- Sparrow: the address at Account 0, Index 1
- Openloop: specify Account=0, Index=1, Coin=BTC on the custom path → the same address appears

Example 2: MetaMask with several accounts

- MetaMask: the address of “Account 2” (MetaMask’s second account)

- Openloop: specify Account=1, Index=0, Coin=ETH on the custom path → the same address appears

Note: MetaMask's "Account 1" corresponds to Openloop's Account=0 (because counting starts at zero).

Example addresses:

- Bitcoin: `bc1q...` or `tb1q...` (testnet)
- Ethereum: `0x...`

Step 2: Show the QR code

1. Tap the "Show QR" button
2. The QR code fills the screen
3. Scan it with a phone or similar to read the address

Receive QR code

Tip: tapping the QR code returns to the address display.

Step 3: Ways to copy the address

Option 1: Type it manually

- Type the displayed address exactly (not recommended — risk of typos)

Option 2: Scan the QR code

- Scan the QR code with a wallet app on your phone (recommended)

Option 3: USB / BLE

- Retrieve it automatically from the companion wallet (easiest)

5.4 Having funds sent from an exchange or another wallet

Example: sending from an exchange (Bitcoin)

1. Sign in to the exchange
2. Go to the withdrawal screen
   - Choose the “Withdraw” or “Send” menu
3. Choose the currency: Bitcoin (BTC)
4. Enter the receiving address
   - Scan the QR code on Openloop’s Receive screen, or copy the address
5. Enter the amount
   - How much BTC you want to send
6. Check the network fee
   - The exchange calculates it automatically
7. Confirm and send
   - Complete any security checks such as two-factor authentication
8. Wait for the transaction to confirm
   - Minutes to hours (for Bitcoin)

⚠ **Warning**: test with a small amount the first time. Confirm the address is correct before sending a real amount.

ℹ **Tip**: if you want to practise on testnet, you can obtain coins from a testnet faucet.

5.5 Confirming a deposit

Openloop itself has only limited balance display. You can check in these ways:

Option 1: A blockchain explorer

- Bitcoin: blockstream.info
- Ethereum: etherscan.io
- XRP: xrpscan.com

Search for your address to see the transaction history and balance.

Option 2: Your companion wallet

- Check the balance in Sparrow Wallet, MetaMask, and so on

5.6 Receiving ERC-20 tokens

ERC-20 tokens are tokens that run on the Ethereum blockchain (USDT, USDC, DAI, JPYC, and so on).

The key point

The receiving address for ERC-20 tokens is the same as your ETH address

⚠ **Important**: you use your ordinary Ethereum address (`0x...`) to receive ERC-20 tokens too. You do not need a separate address per token.

About the differences between networks (chains)

⚠ **Important**: ERC-20 tokens differ **by network (chain)**. The same token name on a different network is a different thing.

EVM networks supported by Openloop (215 networks: 129 mainnets + 86 testnets)

Category	Example mainnets	Example testnets
Ethereum	Ethereum	Sepolia, Holesky
Optimistic L2	Optimism, Arbitrum One, Base, Mantle, Blast	Various Sepolia versions
ZK rollup L2	zkSync Era, Linea, Scroll, Polygon zkEVM, Taiko	Various Sepolia versions
Alt L1	BNB Smart Chain, Avalanche, Fantom, Cronos	Various testnet/Fuji versions
Gaming/NFT	Ronin, Immutable zkEVM, ApeChain	Various testnets
Emerging chains	Berachain, Monad, Sonic, Abstract, Morph	Various testnets

Major networks (excerpt):

Network	Chain ID	Purpose
Ethereum	1	Mainnet (production)
Optimism	10	Layer 2
Arbitrum One	42161	Layer 2
Base	8453	Layer 2 (Coinbase)
Polygon	137	Sidechain
zkSync Era	324	zkRollup
Linea	59144	zkRollup
Scroll	534352	zkRollup

Network	Chain ID	Purpose
BNB Smart Chain	56	EVM-compatible chain
Avalanche C-Chain	43114	EVM-compatible chain
Berachain	80094	Emerging chain
Blast	81457	Layer 2

See the product specification for the complete network list.

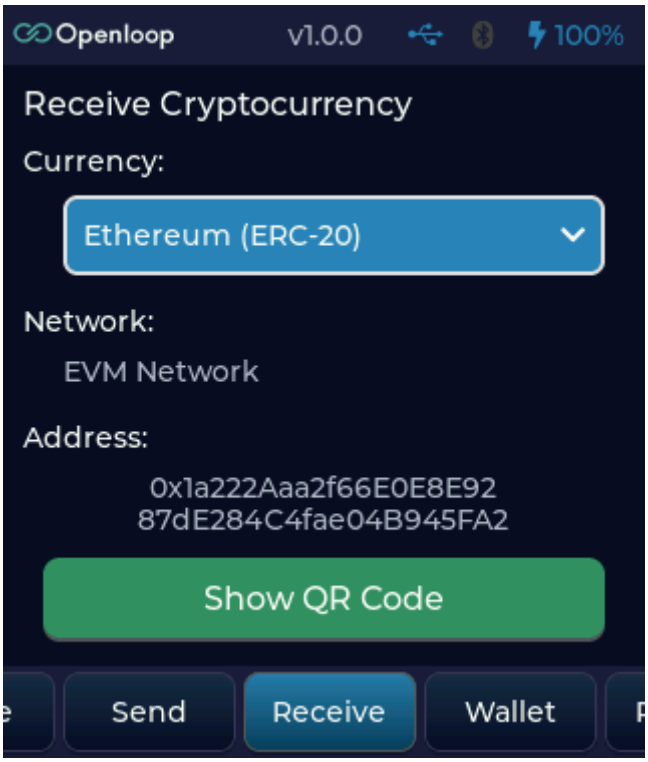
Characteristics of the major networks:

1. Ethereum Mainnet:
   - The most common; almost every exchange supports it
   - Fees (gas) are high (sometimes $5–$50 or more)
   - The highest security
2. Base (Coinbase L2): ⭐ **newly supported**
   - A layer 2 operated by Coinbase
   - Very cheap fees (under $0.01)
   - Easy to use alongside Coinbase
3. Arbitrum One / Optimism:
   - Ethereum layer-2 solutions
   - Extremely cheap fees ($0.01–$1)
   - Fast processing (seconds)

How to receive

1. Choose the network:
   - Withdrawing from an exchange → **choose a network the exchange supports**
   - Receiving from a personal wallet → **choose the same network as the sender**
2. Check the address: confirm your Ethereum address (`0x...`) on the “Receive” screen
3. Request the transfer: have the exchange or wallet send ERC-20 tokens to that address

⚠️ **Important: the address may be the same, but if the network differs the funds will not arrive.** Sender and receiver must always choose the same network.



ETH receive screen

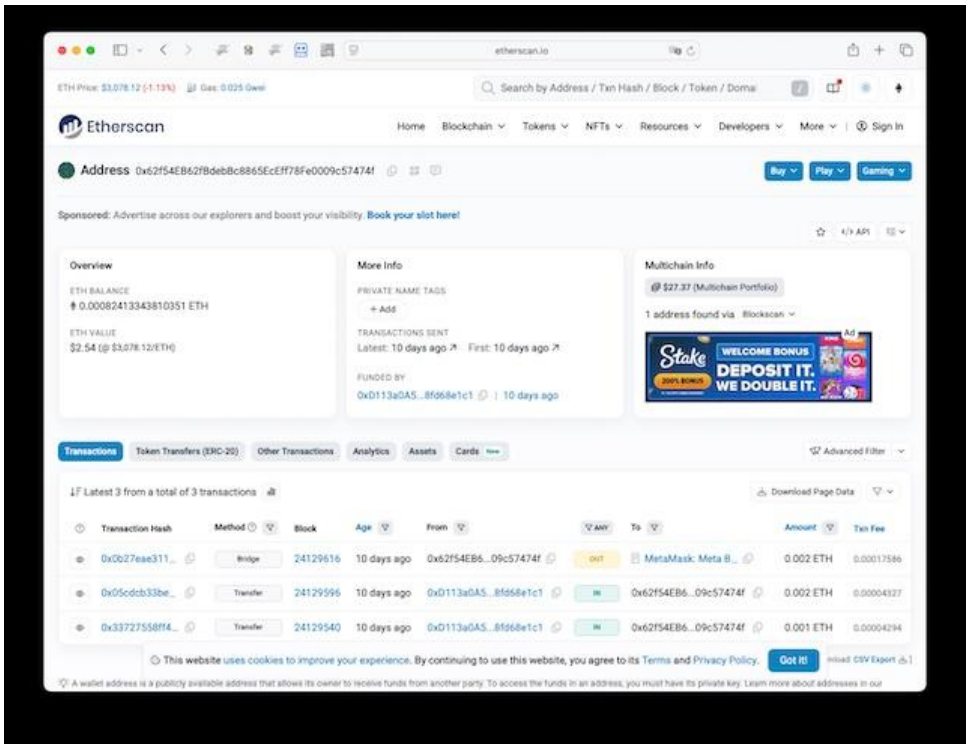
Frequently asked questions

Q: Do I need a dedicated address for USDT? A: No. A single Ethereum address receives ETH and every ERC-20 token (USDT, USDC, DAI, and so on).

Q: My exchange asks me to choose a "network." What should I pick? A: Choose as follows:

- Choose **ERC-20** or **Ethereum** (correct)
- ✗ Do not choose **TRC-20** (the Tron network) or **BEP-20** (BSC)
- ✗ Choosing the wrong network loses your assets

Q: How do I check whether the tokens arrived? A: Search for your address on Etherscan (https://etherscan.io/) to see your ETH and ERC-20 balances.



Examples of supported ERC-20 tokens

Openloop supports the major ERC-20 tokens:

Token	Contract address (mainnet)	Purpose
AAVE	`0x7Fc66500c84A76Ad7e9c93437bFc5Ac33E2DDaE9`	DeFi lending
ARB	`0xB50721BCf8d664c30412Cfbc6cf7a15145234Ad1`	Layer 2 governance
DAI	`0x6B175474E89094C44Da98b954EedeAC495271d0F`	Decentralized stablecoin
JPYC	`0xE7C3D8C9a439feDe00D2600032D5dB0Be71C3c29`	Japanese yen stablecoin
LINK	`0x514910771AF9Ca656af840dff83E8264EcF986CA`	Oracle
UNI	`0x1f9840a85d5aF5bf1D1762F925BDADdC4201F984`	DEX governance
USDC	`0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48`	Stablecoin
USDT	`0xdAC17F958D2ee523a2206206994597C13D831ec7`	Stablecoin

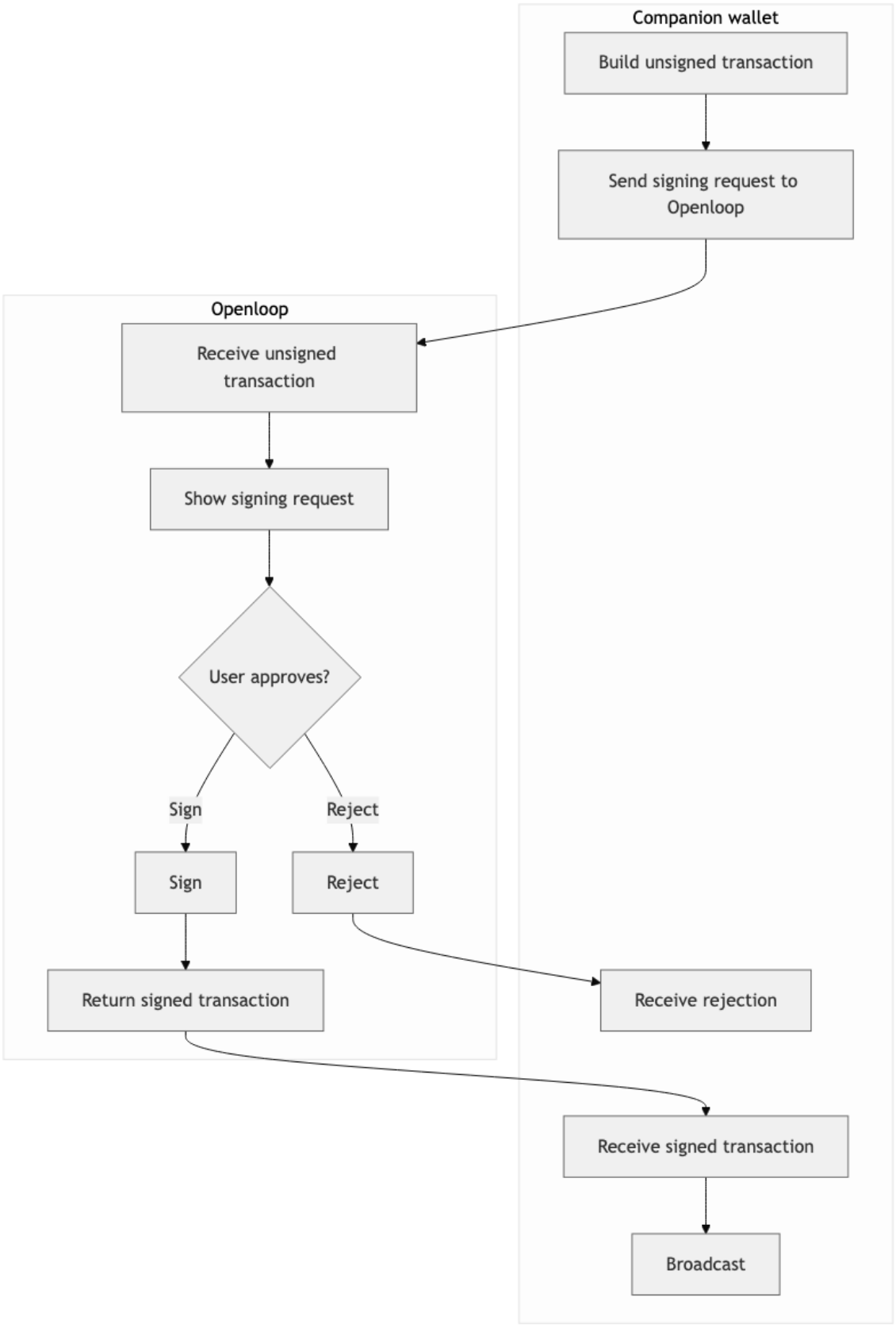
Tip: because ERC-20 tokens run on the Ethereum network, transfer fees (gas) are paid in ETH.

---

6. Sending Crypto Assets

6.1 The basics of sending

Openloop is a **signing-only device**. The actual sending process works like this:



What "Air Gap" means: exchanging data purely through QR codes, without USB or BLE. Choose it when you do not want any electronic communication between devices.

6.2 Preparing your wallet software

The main wallet applications that work with Openloop:

Wallet	Currencies	Transport	Verified
MetaMask Mobile	Ethereum / ERC-20	BLE (recommended)	✓ Verified
MetaMask (PC)	Ethereum / ERC-20	USB (WebHID)	✓ Verified
Sparrow Wallet	Bitcoin	Air Gap (QR code)	✓ Verified
Safe	Ethereum / ERC-20	USB (WebHID)	✓ Verified
Rabby	Ethereum / ERC-20	USB (WebHID)	✓ Verified
XRP Toolkit	XRP	USB	✓ Verified
Other Ledger-compatible apps	Various	USB / BLE	✓ Many supported
Other KeyStone-compatible apps	Various	QR code	✓ Many supported

> **About compatibility**: Openloop uses the Ledger-compatible protocol over USB and BLE, and the KeyStone-compatible protocol over QR codes. Ledger-compatible applications other than Ledger Live, and KeyStone-compatible applications, generally work.

Installing MetaMask Mobile (for Ethereum, recommended):

1. Install “MetaMask” from the App Store (iOS) or Google Play (Android)
2. Create (or import) a wallet
3. Set up BLE pairing with Openloop (see 6.5)

Installing Sparrow Wallet (for Bitcoin):

1. Official site: sparrowwallet.com
2. Download the version for your OS
3. After installing, pair it with Openloop (see Appendix 15.5)

6.3 Air Gap (scanning QR codes)

This method exchanges everything through QR codes, without USB or BLE. It suits anyone who wants to operate without electronic communication between devices. For everyday use we recommend USB or BLE (sections 6.4 and 6.5).

Supported wallets (KeyStone-compatible)

- Sparrow Wallet (Bitcoin) — verified
- MetaMask Mobile (Ethereum) — verified
- AirGap Vault (multi-chain) — verified
- Many other KeyStone-compatible wallets

The basic Air Gap flow

1. Export the public key: Openloop → QR code → companion wallet
2. Build an unsigned transaction: companion wallet → QR code
3. Sign: scan on Openloop → review the details → sign
4. Return the signed data: Openloop → QR code → companion wallet
5. Broadcast: the companion wallet sends it to the network

What BBQr is: a format that splits large data across several QR codes. Openloop scans all the frames automatically.

Detailed tutorial: for step-by-step Air Gap instructions, see "15.5 Tutorial: Sparrow Wallet (Bitcoin Air Gap)."

Advantages and disadvantages of Air Gap

Advantages:

- The highest security (no internet connection)
- Zero risk of malware infection
- Privacy protection (no IP address leakage)

Disadvantages:

- Slightly more complex to operate
- Requires QR code scanning (a camera is essential)

6.4 USB

With USB you connect your PC and Openloop directly and sign. It works with HID-capable wallet software.

Choosing a USB mode

Mode	Purpose	Wallets
Native	Uses Openloop's own extensions	Openloop-aware wallets
Compatible	Prioritizes compatibility with existing wallets	MetaMask, Rabby, XRP Toolkit, and so on

Recommended: choose **Compatible mode** to use anything other than an Openloop-aware companion wallet.

Supported wallets (compatible mode)

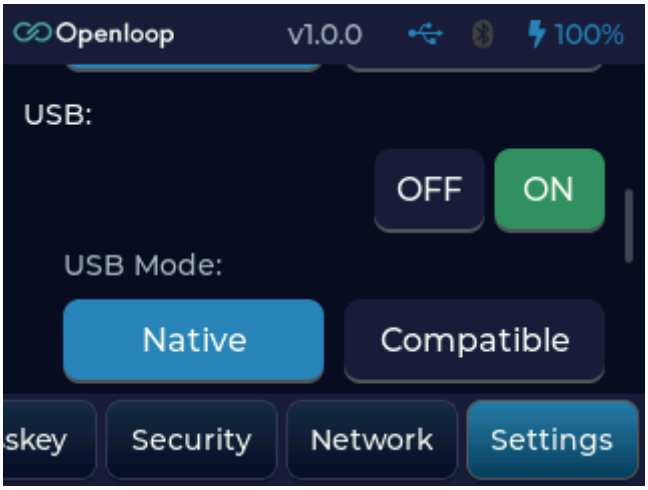
- MetaMask (Ethereum / ERC-20) — verified
- Rabby (Ethereum / ERC-20) — verified
- XRP Toolkit (XRP) — verified
- Many other WebHID-capable wallets

> **Tip**: MetaMask supports Ethereum and ERC-20 tokens. To send Bitcoin, use the QR-code method (Sparrow Wallet).

Sending (example: MetaMask × Ethereum)

Step 1: Turn USB on in compatible mode

1. On Openloop
   - "Settings" → "USB"
   - Switch it to "ON"
   - Choose "Compatible" mode (when pairing with an existing wallet such as MetaMask)



Settings screen

Step 2: Connect your PC and Openloop

1. Connect with a USB-C cable
2. Open MetaMask (the browser extension)
3. Choose “Connect hardware wallet”

Step 3: Connect the device in MetaMask

1. Choose “Ledger”
2. WebHID detects Openloop
3. It appears in the list as “Openloop” or “Ledger Nano S”
4. Click to connect
5. The account selection screen appears

Step 4: Send

1. Click “Send”
2. Enter the destination address
3. Enter the amount
4. Check the gas fee
5. “Next” → “Confirm”

Step 5: Review and sign on Openloop

1. The confirmation screen appears on Openloop
   - Destination (the recipient’s address)
   - Amount (how much ETH is being sent)
   - Gas fee
   - Network (chain ID)
2. Choose “Sign” (right) rather than “Reject” (left)
3. If the device was locked, you will be asked for your PIN (when you are asked depends on the “PIN lock timing:” setting on the Security screen. Setting it to “On sleep” requires a PIN for every signature, which is the most secure)
4. Signing complete

For details of the confirmation screen, see “6.7 The signing confirmation screen in detail.”

ETH signing confirmation

Step 6: Broadcast

- MetaMask sends the transaction automatically
- The transfer appears in your history as “Confirmed”

Done: the transaction has been sent to the Ethereum network from MetaMask.

Advantages and disadvantages of USB

Advantages:

- Simple to operate (no QR codes)
- Fast (quick data transfer)
- Access to MetaMask’s rich DeFi and NFT features

Disadvantages:

- Requires a USB connection (you need a cable)
- Slightly less secure than Air Gap
- Exposed to malware risk on the PC side

6.5 BLE (Bluetooth)

Connect to a phone or tablet over Bluetooth.

Openloop implements the Ledger-compatible BLE protocol, so it works wirelessly with compatible apps.

Supported wallets (compatible mode)

- MetaMask Mobile (iOS / Android) — verified
- Many other Ledger-compatible mobile apps

> **Note**: Ledger Live Mobile is not supported because it checks for genuine Ledger devices.

⚠ Pairing in advance is mandatory

Important: to use BLE, **you must complete pairing beforehand.** Without pairing, BLE will not connect.

Recommended: pair while registering the device in Openloop Connect

The clearest way to pair is to **register the device in Openloop Connect (mobile)**. The registration flow completes your phone's BLE pairing at the same time.

1. Install Openloop Connect (mobile) (see the Connect manual)
2. Turn BLE on in Openloop's settings
3. Tap "Add device" in Openloop Connect
4. The BLE scan finds nearby Openloop devices → tap "Connect"
5. Tap "Pair" in your phone's BLE pairing dialog
6. Registration complete

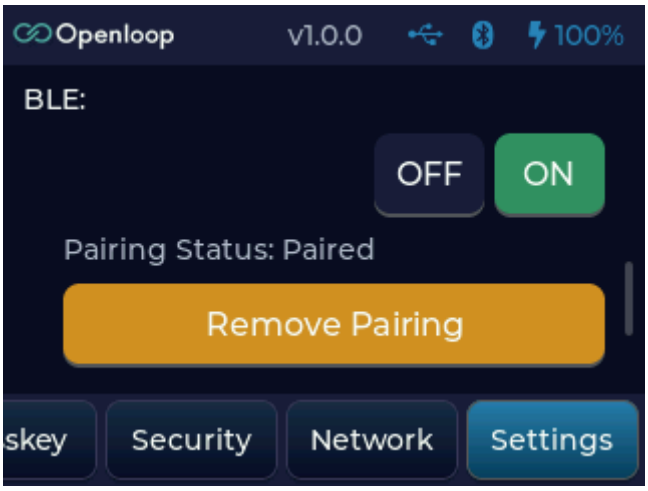
From then on, when you connect to Openloop from another app such as MetaMask Mobile, pairing is already done at the OS level — just choose "Connect hardware wallet" in that app.

Pairing directly from MetaMask Mobile and similar apps

You can also pair directly from a companion wallet such as MetaMask Mobile, without using Openloop Connect (mobile).

Step 1: Turn BLE on

1. On Openloop
   - "Settings" → "BLE"
   - Switch it to "ON"



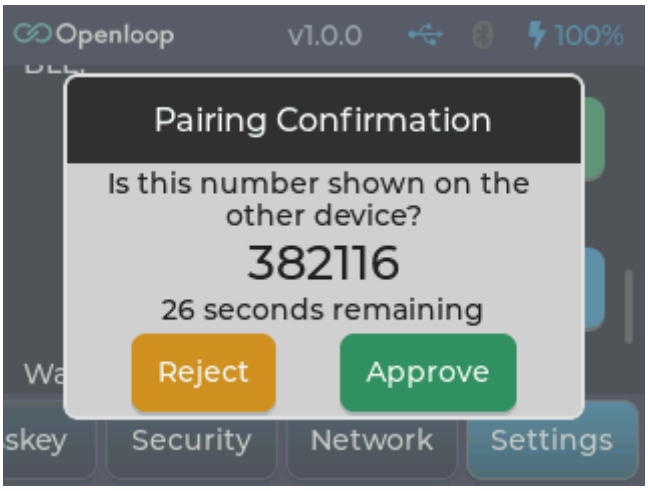
BLE settings

Step 2: Start pairing

1. Scroll down the “Settings” screen and tap the “Start pairing” button below the BLE toggle
2. Openloop shows “Waiting···” and enters pairing mode
3. There is a 30-second timeout

Step 3: Pair from your phone

1. Launch MetaMask Mobile or another compatible app
2. “Settings” → “Security” → “Hardware wallet”
3. Search for “Openloop-XXXX” (XXXX is four alphanumeric characters unique to the device)
   - If you have several Openloop devices, these four characters tell them apart
   - Some apps simply show “Openloop”
4. Pairing request
   - A six-digit code appears on your phone
5. The same code appears on Openloop
   - Check that the codes match
   - The device asks, “Is this number shown on the other device?”
6. Tap “Approve” on Openloop
   - If the codes do not match, tap “Reject”



Pairing code

Step 4: Pairing complete

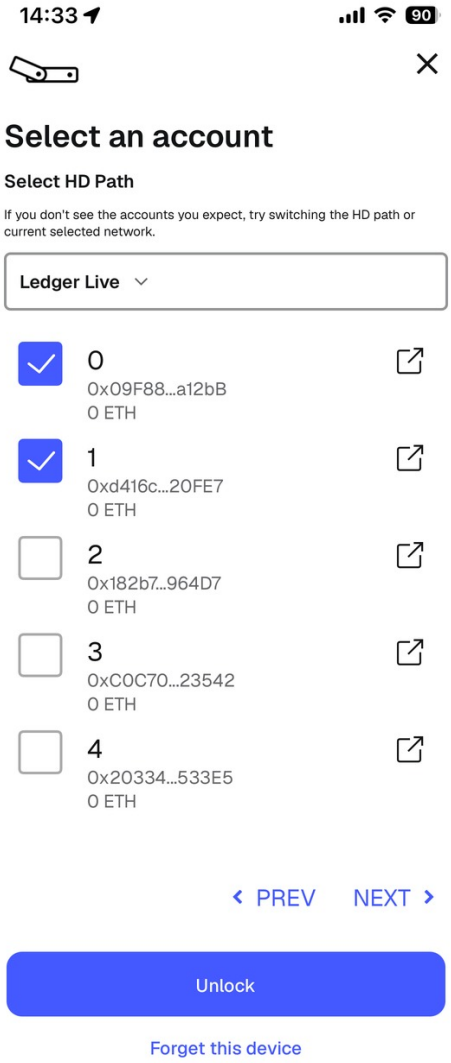
- A tone plays
- Your phone and Openloop are connected
- They connect automatically from now on

Sending (example: MetaMask Mobile × Ethereum)

Once pairing is done, here is how to send Ethereum using MetaMask Mobile.

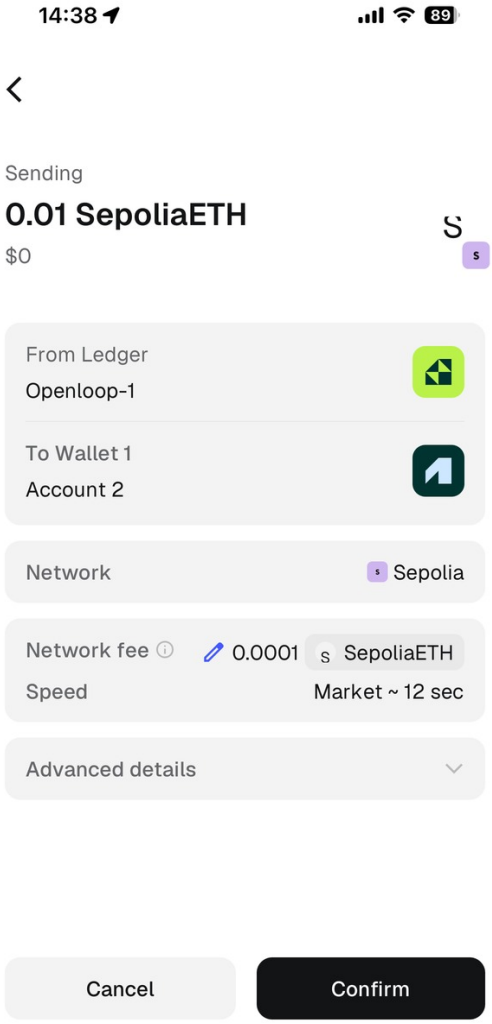
Step 1: Add the account in MetaMask Mobile

1. Launch MetaMask Mobile
2. Tap the account name at the top of the wallet screen
3. “Add account” → “Connect hardware wallet”
4. Choose “Ledger”
5. The connected Openloop appears
6. Select the account (address) to import
7. Tap “Unlock”



Step 2: Start the transfer

1. Select the imported account in MetaMask Mobile
2. Tap “Send”
3. Enter the destination address (or use “Scan QR code”)
4. Enter the amount
5. Check the gas fee
6. Tap “Confirm”



Step 3: Confirm the signature on Openloop

When MetaMask Mobile sends the signing request, the confirmation screen appears on Openloop. If the device is locked, you will be asked for your PIN.

Openloop signing confirmation

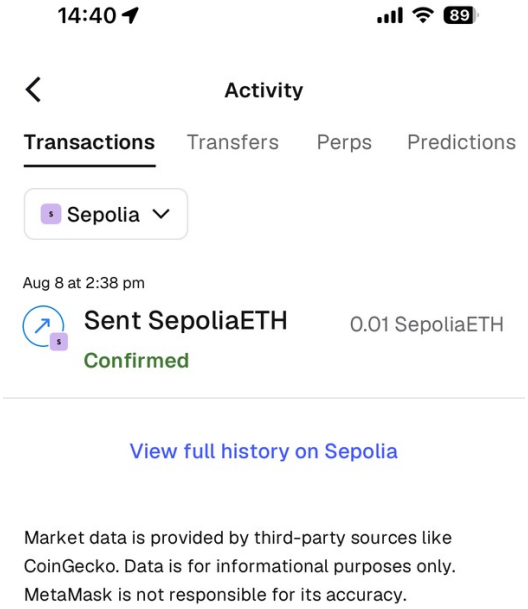
For details of the confirmation screen, see "6.7 The signing confirmation screen in detail."

Step 4: Sign

1. Review the details
2. Tap "Sign"
3. Signing completes inside the secure element

Step 5: Send the transaction

- Once signing finishes, the result is returned to MetaMask Mobile
- MetaMask Mobile broadcasts the transaction automatically
- The transfer appears in your history as "Confirmed"



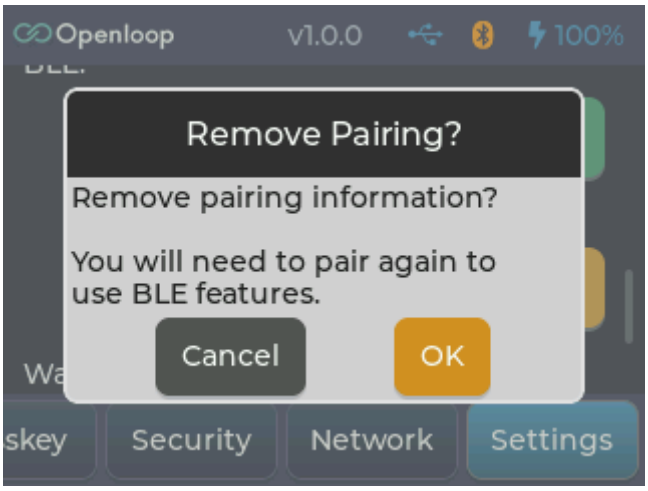
Done: the transaction has been sent to the Ethereum network.

Tip: opening the transaction details from your history gives you a link to a block explorer.

Removing pairing data

To unpair:

1. Go to the “Settings” screen
2. Tap the “Unpair” button
3. Tap “OK” on the confirmation screen



Unpair

⚠ **Note**: after unpairing you will need to pair again.

Advantages and disadvantages of BLE

Advantages:

- No cable (wireless)
- Works with phones and tablets
- Usable while you are out

Disadvantages:

- Requires pairing
- Depends on radio conditions
- Less secure than Air Gap

6.6 Sending ERC-20 tokens

Sending ERC-20 tokens (USDT, USDC, DAI, and so on) works essentially the same way as sending ETH, but there are a few important differences.

Essential background

⚠ **Gas fees must be paid in ETH**

When you send an ERC-20 token, the fee is paid in ETH. So:

- Before sending, make sure your Ethereum address holds enough ETH
- Holding only USDT is not enough — without ETH you cannot send
- ℹ Rule of thumb: keep $5–$50 worth of ETH on hand (on mainnet)

How to send (essentially the same as ETH)

You can send ERC-20 tokens using the same three methods as ETH:

1. Air Gap (QR code)

- Wallets: Sparrow Wallet (partial support for USDT and others), BlueWallet
- Steps: the same as 6.3 (sending in PSBT form)

1. USB (compatible mode)

- Wallets: MetaMask (via WebHID)
- Steps: the same as 6.4 (turn on USB compatible mode)

1. BLE (Bluetooth)

- Wallets: MetaMask Mobile (iOS / Android)
- Steps: the same as 6.5

What Openloop shows you

For details of the confirmation screen, see “6.7 The signing confirmation screen in detail.”

ERC-20 confirmation

Frequently asked questions

Q: Why do I need ETH to send an ERC-20 token? A: Because the fee (gas) paid to the miners (validators) who process transactions on the Ethereum network is denominated in ETH.

Q: How much gas do I need? A: It depends on network congestion:

- Ethereum Mainnet: $5–$50 (over $100 when congested)
- Arbitrum One: $0.01–$1 (very cheap)

Q: I tried to send USDT and got an "insufficient gas" error A: Your ETH balance is too low. Send a small amount of ETH ($10–$50) from an exchange.

Q: My exchange withdrawal screen asks me to "select a network" A: Choose the same network you selected on Openloop:

- Openloop on "Ethereum Mainnet" → choose "ERC-20" or "Ethereum" at the exchange

- Openloop on “Arbitrum One” → choose “Arbitrum” at the exchange

Q: Do you support TRC-20 or BEP-20 USDT? A: For sending tokens such as USDT with Openloop, only **ERC-20 (Ethereum-family networks)** is supported. TRC-20 tokens are not supported, although sending TRON’s native currency (TRX) is. BEP-20 is an ERC-20-compatible token on BNB Smart Chain and is supported as an EVM-compatible chain.

Troubleshooting

Checklist when a token will not send:

1. Is your ETH balance sufficient? ($10 or more recommended)
2. Is the network correct? (sender and receiver must match)
3. Is the contract address correct? (is it a scam token?)
4. Does your wallet software support ERC-20?

6.7 The signing confirmation screen in detail

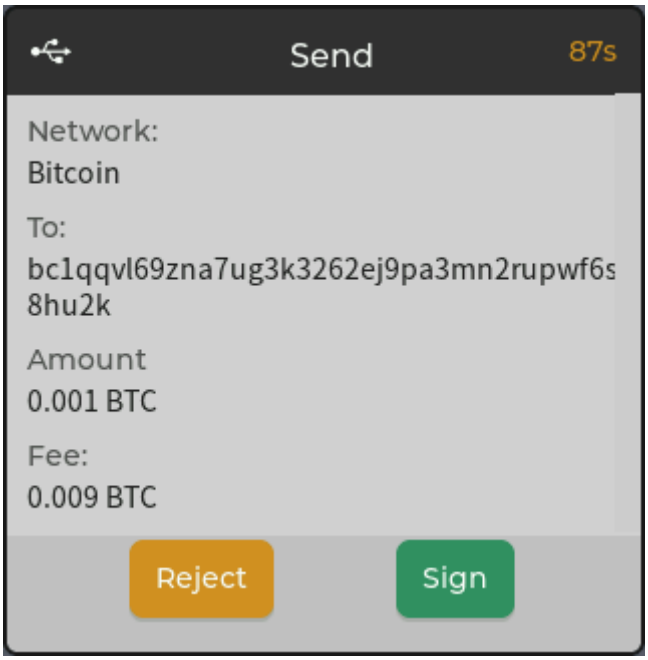
When you sign a transaction on Openloop, the items shown on the confirmation screen differ by asset type. This section covers each currency and token in detail.

Timeout: the confirmation screen shows a countdown (starting at 90 seconds) in the top right. If you do nothing for 90 seconds, the request is automatically rejected and an error is returned to your companion wallet. In that case, start the signature again from the wallet.

Addresses are shown in full: Openloop never abbreviates destination addresses or hashes. Check the whole value — not just the start and end, but the middle too.

6.7.1 Bitcoin (BTC)

What is shown:



Bitcoin signing confirmation

What each item means:

Item	Description	What to check
Destination	The recipient's Bitcoin address	Is it the right address?
Amount	How much BTC is being sent	Is it the amount you intended?
Fee	Payment to miners (fee rate × transaction size)	Typically 0.00001–0.0001 BTC

Types of Bitcoin address:

Prefix	Type	Description
`1...`	Legacy (P2PKH)	The oldest format. Higher fees
`3...`	SegWit (P2SH)	A compatibility-focused format
`bc1q...`	Native SegWit (P2WPKH)	Openloop's standard format. Lower fees
`tb1q...`	Testnet SegWit	Testnet addresses
`bc1p...`	Taproot (P2TR)	⚠ Address display only. **Signing is not supported**

⚠ **Note**: Openloop generates `bc1q...` (Native SegWit) addresses.

⚠ **Taproot cannot be signed**: if you create a Taproot (`m/86'`) account in your companion wallet, Openloop shows “Cannot sign: Taproot (P2TR) is not supported” on the confirmation screen and disables the “Sign” button. In Sparrow Wallet and similar, choose Native SegWit (P2WPKH), Nested SegWit, or Legacy instead.

Two safety warnings on the confirmation screen:

Warning	Meaning	What to do
(unverified) in red on an output, plus “Unverified destination. Please check the address.”	Openloop could not confirm that the change address belongs to you. This may be an attack that redirects your change to a fake address	Always cross-check the change address in your companion wallet
“Too many outputs to display them all”	There are more than 16 outputs, so the 17th onward cannot be shown	Verify all outputs in your companion wallet before signing

6.7.2 Ethereum (ETH)

What is shown:

Ethereum signing confirmation

What each item means:

Item	Description	What to check
Destination	The recipient's Ethereum address (starting 0x)	A 42-character address. Compare it end to end
Amount	How much ETH is being sent	Up to 18 decimal places can be shown
Fee	The transaction fee (gas)	Varies with network congestion
Network	The EVM chain name	Check it is the network you intended
Nonce	The transaction sequence number	Orders transfers from the same account
Transaction hash	The keccak256 hash of the data being signed (all 64 digits shown)	You can compare it with the hash Safe and others display

ℹ If the fee exceeds 0.01 ETH, an orange warning appears: "Gas fee is high!"

Why checking the chain ID matters:

Network	Chain ID	Note
Ethereum Mainnet	1	Production. Mistakes cost real assets
Arbitrum One	42161	L2. Cheap fees
Optimism	10	L2. Cheap fees
Base	8453	L2. Run by Coinbase
Sepolia Testnet	11155111	For testing. No value

⚠ **Warning**: sending to a network with a different chain ID can lose your assets.

ℹ **Networks that are not built in**: for networks outside the 215 built-in ones, the screen shows something like "Chain ID 12345" instead of a name, and the currency symbol for the amount and fee becomes "ETH?". Signing is still possible, so check the network information in your companion wallet before you sign.

6.7.3 ERC-20 tokens

What is shown:

ERC-20 token signing confirmation

What each item means:

Item	Description	What to check
Destination	The recipient's address	The same 0x address as for ETH
Amount	How many tokens are being sent	Watch the decimal places for each token
Fee	Gas (paid in ETH)	You need ETH, not the token
Network	Which chain the token is on	The same token name on a different chain is a different token
Nonce	The transaction sequence number	Orders transfers from the same account

Item	Description	What to check
Token	The token symbol	USDT, USDC, DAI, JPYC, and so on
Contract	The token's smart contract address	Always check it is not a scam token
Transaction hash	The keccak256 hash of the data being signed (all 64 digits shown)	You can compare it with the hash Safe and others display

Official contract addresses for major tokens (Ethereum Mainnet):

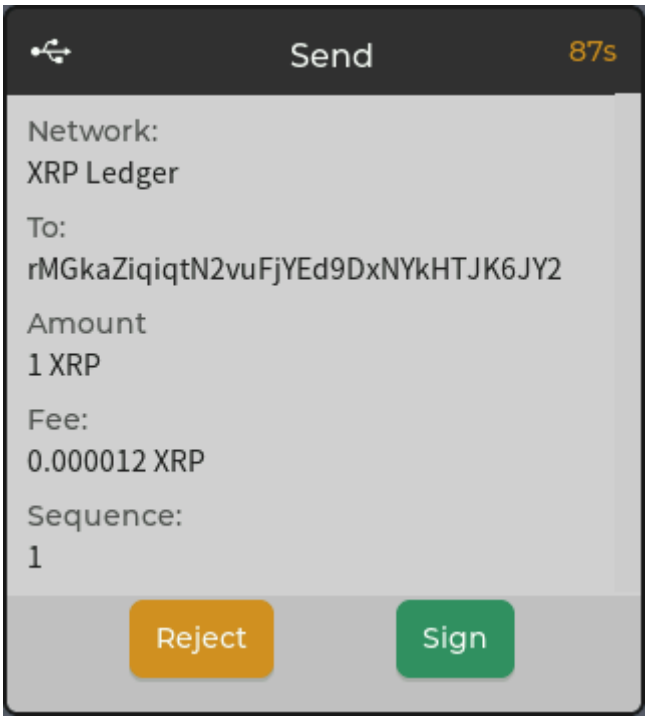
Token	Contract address
USDT	`0xdAC17F958D2ee523a2206206994597C13D831ec7`
USDC	`0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48`
DAI	`0x6B175474E89094C44Da98b954EedeAC495271d0F`
WETH	`0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2`

⚠ **Important**: "fake tokens" with different contract addresses exist. Always confirm the official address on the project's website, CoinGecko, or a similar source.

ℹ **Tokens that are not built in**: for tokens outside the 2,599 built-in ones, the screen shows "ERC-20 Token" or "Unknown ERC-20" instead of a name, together with an orange warning, "Unknown token - verify contract!" Signing is still possible, so compare the contract address (shown in full) with your companion wallet before you sign.

6.7.4 XRP (Ripple)

What is shown:



XRP signing confirmation

What each item means:

Item	Description	What to check
Network	Shows `XRP Ledger`	—
Destination	The recipient's XRP address (starting r, shown in full)	Classic Address format
Amount	How much XRP is being sent	In drops: 1 XRP = 1,000,000 drops
Fee	The transaction fee	Typically 10–12 drops (about 0.00001 XRP)
Destination tag	The identifier used when sending to an exchange (shown only when set)	Check it matches the number the exchange gave you
Sequence	The account sequence number	—
Last ledger sequence	The ledger number at which the transaction expires (shown only when set)	—

Characteristics of XRP addresses:

Format	Description	Support
Classic Address (`r...`)	The standard format	

Format	Description	Support
		✓ Supported
X-Address (`X...`)	Embeds the destination tag	✗ Not supported

About destination tags:

When sending XRP to an exchange, a **destination tag** is often required.

- **When a destination tag is required**: the exchange's XRP address is shared among many users, and the tag identifies you
- **When it is not required**: sending to a personal wallet (an address that is yours alone)

⚠ **Warning**: getting the destination tag wrong when sending to an exchange can cost you your assets.

About the XRP curve setting:

XRP supports two elliptic curves:

Curve	Characteristics	Recommendation
Ed25519	The newer format, the default for software wallets	✓ Recommended
secp256k1	The traditional format, Ledger's default	For compatibility

⚠ **Important**: when using XRP Toolkit, go to "Wallet" → "Connect Wallet" → select XRP → set "Curve" to **Ed25519**. Leaving it on "Auto" can make signing fail. See "4.1 The Connect Wallet screen" for details.

6.7.5 Solana (SOL)

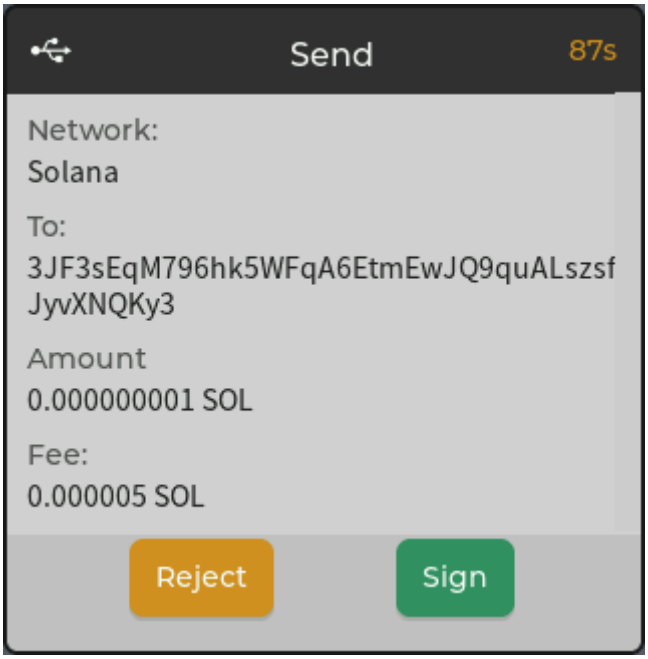
What the confirmation screen shows:

Item	Description
Network	Shows `Solana`
Destination	The destination Solana address (shown in full)
Amount	How much SOL is being sent
Fee	Number of signatures × 5,000 lamports

Solana supports both transaction signing and off-chain message signing. The display falls into three patterns.

Pattern	Display
Simple transfer	As in the table above (network / destination / amount / fee)
Blind signing	A two-line orange warning: “Unknown program” and “Verify in dApp.” Over USB/BLE, destination, amount, and fee all become “See dApp”
Message signing	Message / hash (all 64 digits shown) / length

⚠ **The blind-signing warning**: when you see “Unknown program,” Openloop could not interpret the contents of the transaction. **The “Sign” button remains enabled**, so make absolutely sure you know what you are signing by checking in the dApp. If it looks unfamiliar, choose “Reject.”



Solana signing confirmation

6.7.6 TRON (TRX)

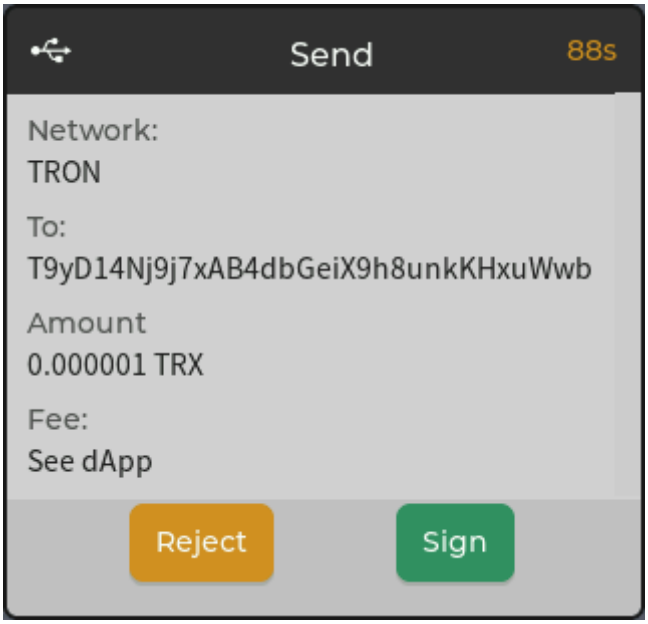
What the confirmation screen shows:

Item	Description
Network	Shows `TRON`
Destination	The destination TRON address (Base58Check, shown in full)

Item	Description
Amount	How much TRX is being sent
Fee	**Always shows "See dApp"** (the device cannot calculate TRON fees)

TRON transactions are encoded in protobuf format.

⚠ **The blind-signing warning**: the only TRON transaction Openloop can read is a plain TRX transfer. A TRC-20 token transfer (USDT-TRC20 and the like) is a smart-contract call, which the device cannot interpret: destination, amount and fee all become "See dApp" and a two-line orange warning appears — "Unknown contract" and "Verify in dApp." **The "Sign" button remains enabled**, so make absolutely sure you know what you are signing by checking in the dApp. If it looks unfamiliar, choose "Reject."



TRON signing confirmation

6.7.7 Other EVM chains

Supported EVM chains:

Openloop supports **215 EVM chains (129 mainnets + 86 testnets)**:

Chain	Chain ID	Native currency	Characteristics
Ethereum	1	ETH	The main chain
Arbitrum One	42161	ETH	L2, low fees
Optimism	10	ETH	L2, low fees

Chain	Chain ID	Native currency	Characteristics
Base	8453	ETH	Coinbase L2
Polygon	137	POL	Sidechain
BNB Chain	56	BNB	Binance chain
Avalanche C-Chain	43114	AVAX	Fast chain
Berachain	80094	BERA	Emerging chain
Blast	81457	ETH	L2, high yield
Others	-	-	All 215 chains supported

Points to watch when confirming a signature:

1. Check the native currency
   - Fees (gas) are paid in that chain's native currency
   - For example: POL on Polygon, BNB on BNB Chain
2. Not the same as bridging
   - Openloop only handles transfers within a single chain
   - Moving between chains (bridging) requires a separate bridge service
3. Address format
   - Every EVM chain uses the same `0x...` address format
   - The same private key produces the same address

6.7.8 Signing screens other than transfers

Openloop handles several kinds of signing request beyond simple transfers. **The title at the top of the screen tells you which one it is.**

Title	Meaning	Main items shown
Send	An ordinary transfer	Destination / amount / fee
ERC-20 Transfer	A token transfer	Plus token / contract
Contract Call	A smart contract invocation	Contract / method / arguments
Off-chain Signature	EIP-712 typed data signing	Type / domain / contract / domain hash / message hash / digest (each shown in full, 64 digits)
Message Signature	personal_sign / BIP-322 / Solana off-chain	Message / hash / length

⚠ “Approve” and “Set Approval For All” deserve special care

If the “Contract Call” screen shows **“Method: Approve”** together with **“Amount: Unlimited,”** you are granting that contract **the right to withdraw an unlimited amount of your tokens.**

“Method: Set Approval For All” with **“Allow: All NFTs”** likewise grants the right to move every one of your NFTs.

Never sign these except on a DEX or marketplace you trust. This is one of the classic ways assets are drained.

If it shows **“Revoke (0)”** instead, that is a revocation of permission and is safe.

Openloop also decodes and displays other methods such as delegated transfer, NFT transfer, multi-send, and batch send.

⚠ The “Unverified contract” warning (red)

This appears in red for an EIP-7702 authority delegation when the delegate is not on the known list. If it looks unfamiliar, choose “Reject.”

6.7.9 Signing security checklist

Before you sign a transaction, always check the following:

✓ Mandatory checks:

#	Item	How
1	Destination address	The screen shows every digit. Compare the whole address, including the middle, not just the start and end
2	Amount	Confirm it matches exactly what you intended
3	Network / chain ID	Confirm it is the right network (mainnet vs. testnet)
4	Fee	Check the fee is not abnormally high
5	Token contract	For ERC-20, confirm it is the official address

⚠ Do not sign when:

- You do not recognize the address
- The amount is not what you intended

- The fee is abnormally high (ten times normal or more)
- You did not expect a token transfer request
- The chain ID is an unexpected network

Safe transaction habits:

1. Test small: send a small amount to a new address first
2. Use an address book: register frequently used addresses in your wallet software
3. Double-check: for large transfers, confirm with the recipient through another channel
4. Do not rush: take your time even if someone is pressing you

---

7. Choosing and Configuring the Connection Method

7.1 Comparing the connection methods

Openloop supports three connection methods. Use whichever suits the task.

Method	Security	Convenience	Devices	Recommended for
Air Gap (QR code)	★★★★★	★★★★	PC / phone (camera required)	Large holdings, maximum security
USB	★★★★	★★★★★	PC (USB-C)	Everyday use, fast operation
BLE (Bluetooth)	★★★★	★★★★★	Phones and tablets	Mobile use, while out

> **All three methods have been verified to a practical standard.** Choose freely according to your needs.

7.2 Air Gap (QR code) in detail

Advantages

The highest security

- Zero electronic or radio communication
- Physical data isolation (air gap)

- No risk of malware infection
- Privacy protection (no IP address leakage)

No extra hardware

- No cable needed
- No Bluetooth needed
- All you need is a camera and a display

Future-proof

- More and more wallets support QR codes
- Supports the standard formats (BBQr, UR)

Disadvantages

More complex to operate

- You have to scan QR codes
- Multi-frame codes take time

A camera is essential

- Your PC or phone needs a camera

Recommended for

- ★ Anyone who puts security first
- Anyone managing large holdings
- Anyone whose PC has a camera
- Anyone who does not mind a little complexity

How to use it, in summary

1. Prepare wallet software: install Sparrow Wallet
2. Export the public key: Openloop → QR code → Sparrow
3. Build a transaction: Sparrow → PSBT QR code
4. Sign: Openloop → scan → review → sign
5. Broadcast: Openloop → signed QR code → Sparrow → send

7.3 USB in detail

Advantages

Fast and stable

- Quick data transfer

- Few communication errors
- You can use it while charging

Simple to operate

- Just plug in the cable
- No QR code scanning
- Works with MetaMask (for Ethereum)

Versatile

- Can also be used for firmware updates (OTA)

Disadvantages

Requires a physical connection

- You need a USB-C cable
- You must be near the PC

Security risk

- Exposed to malware on the PC
- You are using an internet-connected PC

Recommended for

- Anyone who wants fast operation
- Anyone managing assets from a PC
- Anyone who does not mind a cable
- Anyone who wants to use Ethereum in MetaMask

How to use it, in summary

1. Turn USB on: “Settings” → “USB” → ON
2. Choose a mode: “Native” or “Compatible”
3. Connect the PC: use a USB-C cable
4. Launch your wallet software: MetaMask, for example
5. The device is recognized: it appears as “Ledger Nano S”
6. Send: operate in the software, sign on Openloop

7.4 BLE (Bluetooth) in detail

Advantages

Wireless

- No cable
- Easy to carry
- Works with phones and tablets

Mobile

- Usable while you are out
- Works with MetaMask Mobile and others

Power-efficient

- Bluetooth Low Energy (BLE) means long battery life

Disadvantages

Pairing required

- One-time setup is needed
- Verifying the code takes a moment

Communication can be unstable

- Depends on radio conditions
- Disconnects if you move too far away

Security risk

- Wireless communication carries risk
- Man-in-the-middle attacks are possible (unlikely, but real)

Recommended for

- Anyone who wants to manage assets from a phone
- Anyone who wants to use it while out
- Anyone who prefers wireless
- Anyone whose transfers are mostly small

How to use it, in summary

1. Turn BLE on: “Settings” → “BLE” → ON
2. Start pairing: scroll down the “Settings” screen and tap “Start pairing”
3. Pair from your phone: connect over Bluetooth in MetaMask Mobile or similar

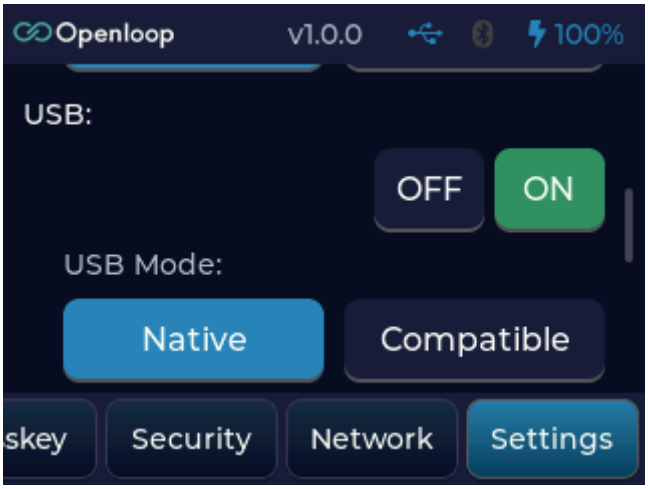
4. Verify the code: compare the six-digit code
5. Send: operate on the phone, sign on Openloop

7.5 Switching between connection methods

Each method can be **enabled and disabled independently**.

USB settings

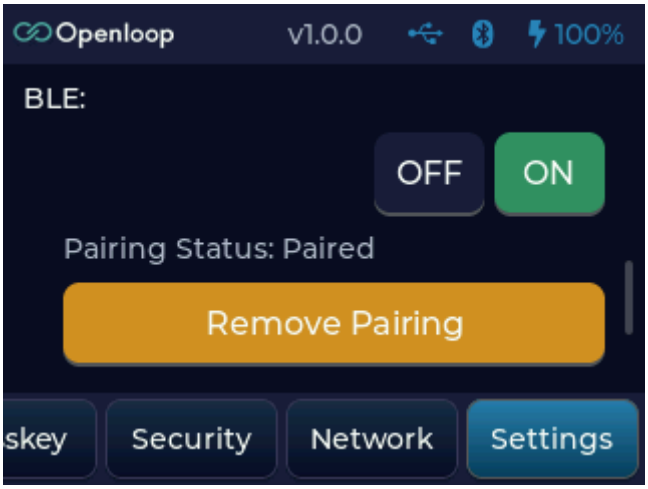
1. “Settings” → “USB”
2. Turn it on or off with the toggle
3. Choose a mode (Native / Compatible)



USB settings

BLE settings

1. “Settings” → “BLE”
2. Turn it on or off with the toggle
3. Applies immediately



Tip: disabling both USB and BLE gives you a complete air-gapped mode (QR codes only).

7.6 Power management

Openloop is designed to conserve power and maximize battery life.

Battery

- Capacity: 450 mAh lithium polymer (built-in, custom cell)
- Normal use: about 1 hour
- Sleeping: several hours on standby

Automatic sleep and power off

Event	Behaviour
60 seconds with no input	Sleep (backlight off)
Touch or USB connection	Wake from sleep
5 minutes asleep without USB	Automatic power off
Battery at 15% or below	Safe shutdown

Important: we recommend using the device above 30% battery (it powers off automatically at 15% or below).

Conditions that prevent sleep

The device will not sleep while:

- Connected over USB (communicating with a host): to keep the connection alive
- Connected over BLE: to keep communication with the phone alive
- Scanning a QR code: while reading a multi-frame QR

BLE idle disconnect timer

For security, a BLE connection is dropped automatically after a period with no traffic.

Condition	Time to disconnect
Normal mode	60 seconds with no traffic → automatic disconnect

Condition	Time to disconnect
While a signing confirmation is displayed	Timer paused (waiting for you to confirm)

- The timer resets with every message
- After a disconnect you need to reconnect
- This is a security feature that prevents unauthorized access to an idle BLE connection

ℹ **Tip**: for long sessions, use the device while charging over USB-C.

7.7 Recommended settings by security level

Maximum security (large holdings)

- ✓ Air Gap only
- ✗ USB disabled
- ✗ BLE disabled
- ℹ A fully air-gapped setup

Balanced (PC use)

- ✓ Air Gap + USB
- ✗ BLE disabled
- ℹ Mainly used from a PC

Balanced (smartphone use)

- ✓ Air Gap + BLE
- ✗ USB disabled
- ℹ Mainly used from a phone

Convenience first (small amounts, mobile)

- ✓ Air Gap + USB + BLE
- ℹ Everything enabled

⚠ **Warning**: if you manage large holdings, we strongly recommend Air Gap mode.

8. Security and Backup

8.1 Managing your PIN

What the PIN is for

- Purpose: to prevent unauthorized use of the device
- Length: 4–6 digits (6 recommended)
- Failure limit: **all data is erased automatically** after 10 consecutive failures (see 2.4)

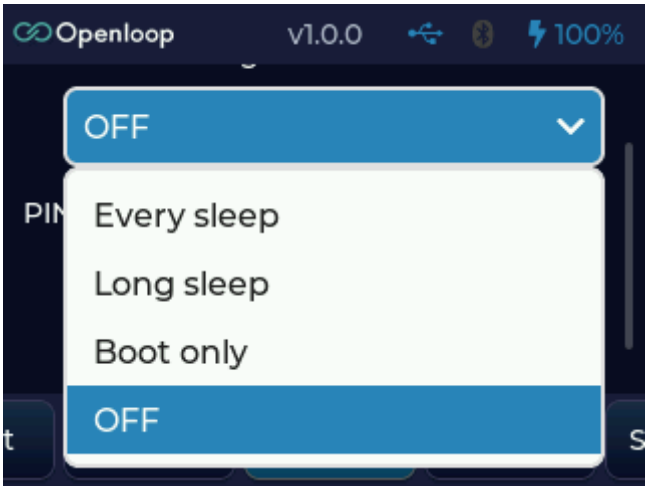
PIN lock timing

You can choose from four settings for when the PIN is required. Set it with the “PIN lock timing:” dropdown on the “Security” screen.

Setting	On waking from sleep	Recommended for
On sleep	PIN every time	Maximum security
On long sleep (default)	PIN only after a long sleep	Balanced
At boot only	No PIN	Convenience
Off	No PIN	Testing (not recommended)

Note: in addition to waking from sleep, every setting other than “Off” also requires a PIN:

- **At boot (power on)**: every time
- **When displaying the recovery phrase**: every time

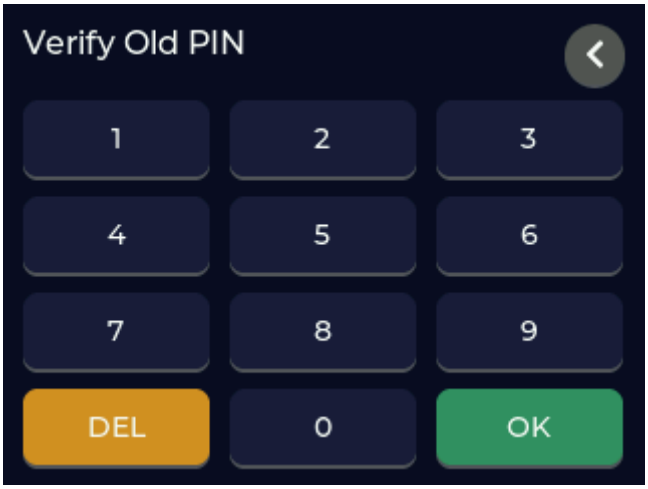


Security screen

Warning: with “Off,” anyone can operate the device. If you manage large holdings, we recommend “On sleep” or “On long sleep.”

Changing your PIN

1. “Security” screen → “Change PIN”
2. Enter the old PIN
3. Enter the new PIN
4. Enter it again to confirm
5. Done



Change PIN

If you forget your PIN

⚠ **Important**: if you forget your PIN, you can recover as follows.

1. Have your recovery phrase ready
   - The 12 or 24 words you wrote down when you created the wallet
2. Perform a factory reset
   - “Settings” → “Factory Reset”
   - ⚠ All data is erased
3. Restore your wallet
   - Restore from your recovery phrase
   - See “8.4 Restoring a wallet” for details

Automatic erase after 10 failures

⚠ Getting the PIN wrong 10 times in a row makes the device **automatically perform a factory reset**. It does not lock — **the data is erased**.

What is erased:

- Your wallet (recovery phrase), PIN, and all settings

- **FIDO2 passkeys** (you must register again at each service)
- **PIV keys and certificates** (you must regenerate them and reissue certificates)

How to recover:

1. Restore your wallet from your recovery phrase (crypto assets only)
2. Register your passkeys again at each service
3. Regenerate your PIV keys and reissue certificates

⚠ **Warning**: without your recovery phrase, your assets are lost forever. **Passkeys and PIV keys cannot be restored from a recovery phrase.**

8.2 Backing up your recovery phrase

Why the recovery phrase matters

⚠ **Most important**: those 12 or 24 words are **the only way** to protect your assets.

With your recovery phrase:

- You can recover even if you lose the device
- You can recover even if the device breaks
- You can migrate to a new device

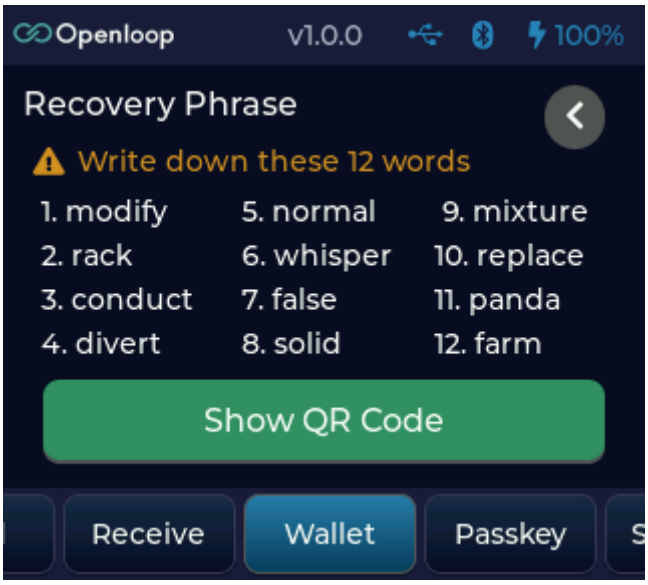
Without it:

- Losing the device = losing your assets
- A device failure = losing your assets
- Forgetting your PIN = losing your assets

Displaying the recovery phrase

⚠ **Warning**: make sure nobody is nearby before you do this.

1. “Wallet” screen → “Recovery Phrase”
2. Enter your PIN
   - For security verification
3. The recovery phrase appears
   - The 12 or 24 words are shown in order



Recovery phrase

Tip: check periodically that your written copy has not faded (once a year is a good rule).

Storing it safely

Recommended methods:

1. Written on paper (the basics)
   - The included record sheet, or durable paper
   - A waterproof, fire-resistant notebook also works
2. Stamped into metal (advanced)
   - Resistant to fire and flood
   - Use a metal backup product such as Cryptosteel or Billfodl
3. Several copies in different places
   - A safe at home
   - A bank safe deposit box
   - A trusted family member's home (a different location)

Methods to avoid:

- Photographing it with your phone and storing it in the cloud (the cloud can be hacked)
- Saving it on a computer (malware can steal it)
- Email or cloud storage
- Password managers (risky)
- Keeping only one copy in one place (fire and theft risk)

Tip: making several copies and storing them in different places reduces the risk from disasters.

8.3 Erasing a wallet

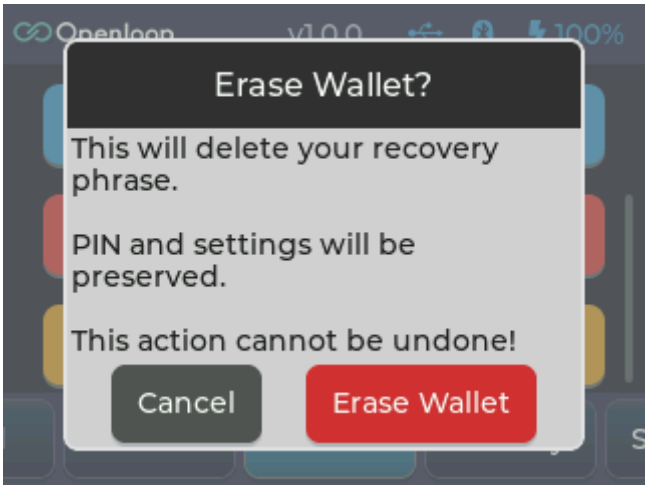
Dangerous operation: this completely deletes the wallet from the device.

Before you erase:

- My recovery phrase is backed up
- I have moved all my assets (or I plan to restore)

How to erase

1. "Wallet" screen → "Erase Wallet"
2. Review the first warning
   - "This will delete your recovery phrase. Your PIN and settings will be kept. This cannot be undone!"
   - Tap "Erase"
3. Review the second, final warning
   - "Are you sure? Only the recovery phrase will be deleted. Your PIN and settings will be kept."
   - Tap "Erase"
4. Done



Erase wallet warning

Warning: this **cannot be undone**. Without your recovery phrase, you lose your assets.

▲ **Important**: erasing a wallet **does not require your PIN** (unlike “Factory Reset”). If someone else can operate your unlocked device, they could perform this operation. We recommend setting “PIN lock timing:” on the “Security” screen to “On sleep.”

When you might need to erase:

- Before giving the device to someone else
- Before creating a new wallet
- To clear out a test wallet

8.4 Restoring a wallet

You can restore an existing wallet from its recovery phrase.

When you need to restore

- ★ You forgot your PIN (after a factory reset)
- You are moving to a new device
- You erased a wallet by mistake
- You reset the device

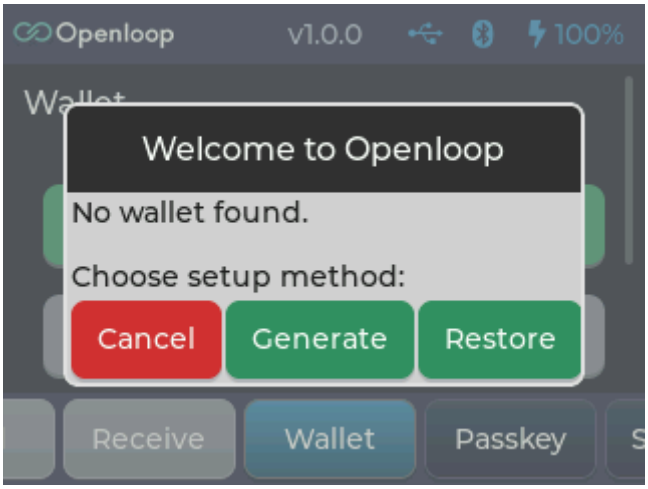
How to start a restore

Option 1: from the automatic dialog on first boot

- Starting the device with no wallet shows the “Welcome to Openloop” dialog automatically
- Tap “Restore”

Option 2: from the Wallet screen

- “Wallet” screen → tap the “Create Wallet” button
- Tap “Restore” in the “Welcome to Openloop” dialog that appears



Restore button

How to restore

Step 1: Choose a restore method

Tapping “Restore” brings up the **restore method dialog**.

The “Restore Wallet” dialog:

Restore method selection

Options:

Button	Description
Manual	Type the recovery phrase one word at a time (recommended)
QR	Scan a QR code of the recovery phrase
Cancel	Abandon the restore

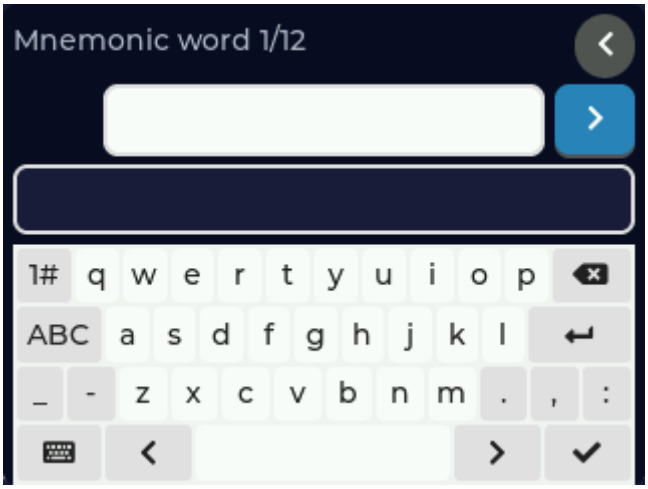
Recommended: choose **Manual**. Restoring from a QR code carries a security risk (the code could be photographed by someone else).

Step 2: Enter the recovery phrase

Manual entry:

1. Enter the first word
   - Start typing on the on-screen keyboard
   - Suggestions appear as you type (from the BIP39 word list)
2. Choose the correct word from the suggestions
3. Enter the remaining words the same way

4. Finish entering all the words (12 or 24)



Manual entry

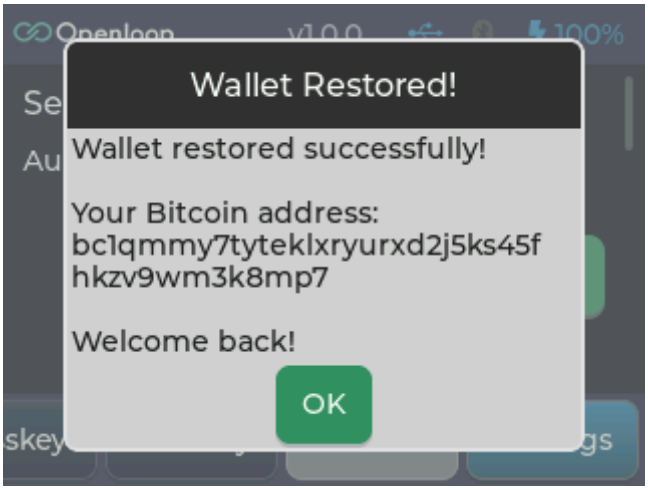
Tip: if a word does not appear in the suggestion list, it is probably misspelled. The BIP39 list contains exactly 2,048 words.

QR scanning:

1. The camera opens
2. Hold the recovery phrase QR code in view
3. It is read automatically

Step 3: Restore complete

- The message “Wallet restored” appears
- Returning to the home screen shows the restored addresses



Restore complete

How to verify: check that the addresses on the Receive screen match your previous wallet.

Troubleshooting a failed restore

If you see an “Invalid mnemonic” error:

- Cause 1: a spelling mistake
  - Fix: check the words again (against the BIP39 word list)
- Cause 2: the order is wrong
  - Fix: check the order in your notes
- Cause 3: the number of words is wrong
  - Fix: confirm whether it is 12 or 24 words

⚠ **Important**: if it still will not restore after several attempts, your notes may be wrong. Look for another backup.

---

9. Using It as a Security Key (FIDO2 / Passkeys)

Openloop also works as a FIDO2/CTAP2 security key. It supports passwordless sign-in to web services and two-factor authentication for PC security, over **USB** or **BLE (with the Openloop Connect mobile app)**.

> ⚠ **Certification status**: Openloop is not currently a **FIDO Certified Authenticator** (FIDO2 Certified) with the FIDO Alliance. The CTAP2/WebAuthn implementation follows the specification, but official FIDO Alliance certification and AAGUID registration (the FIDO Metadata Service) are something we may pursue in future.

9.1 What FIDO2 and passkeys are

FIDO2 (Fast IDentity Online 2) is a secure alternative to passwords. Using a private key stored in Openloop, you can sign in securely to web services and applications from both a PC and a smartphone.

Key characteristics:

- No password: resistant to phishing
- Device authentication: you cannot sign in without your Openloop
- Privacy protection: a different key is used for each service
- Multi-device: works on PCs (Windows / macOS / Linux) and smartphones (iOS / Android)

Supported algorithms:

- ES256 (ECDSA P-256)
- EdDSA (Ed25519)

Two connection paths:

Path	What you need	Where you use it
USB CTAPHID	Just the OS's built-in security key support (no app needed)	Browsers on a PC (Windows / macOS / Linux)
BLE (via Openloop Connect)	The Openloop Connect mobile app + BLE pairing	Browsers on iPhone / Android

⚠ **A note for iPhone users**: on iOS 17 and later you can connect over BLE through Openloop Connect's Credential Provider Extension. The iOS picker shows "**Openloop Connect**" — that is iOS fixing the name to the containing app — but **the actual communication is over BLE**, not USB.

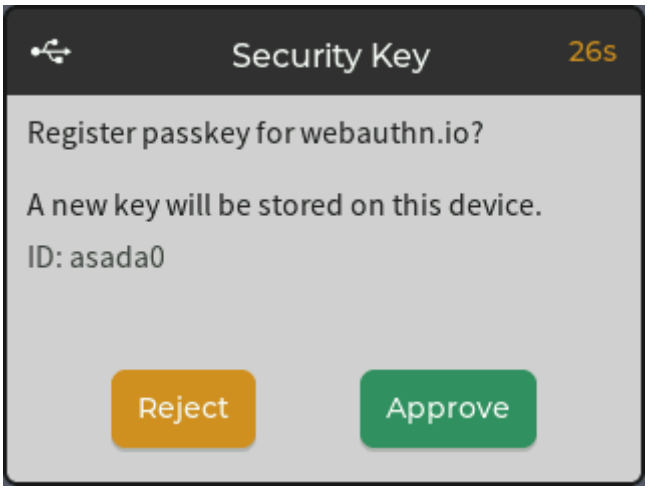
9.2 Registering a passkey

On a PC (USB):

1. Go to a FIDO2-capable service in your web browser
2. In the security settings, choose "Add a security key"
3. Connect Openloop over USB
4. The registration confirmation appears on the Openloop screen
5. Review it and tap the approve button
6. Registration complete

On a smartphone (BLE + Openloop Connect):

1. Install the Openloop Connect mobile app
2. Pair and select your Openloop device over BLE in the app
3. Enable Openloop Connect as a credential provider in your iOS or Android settings
4. Go to a FIDO2-capable service in your browser and choose the create-passkey option
5. Choose **"Openloop Connect"** in the OS picker
6. The registration confirmation appears on the Openloop screen
7. Tap the approve button → registration complete



Passkey registration confirmation

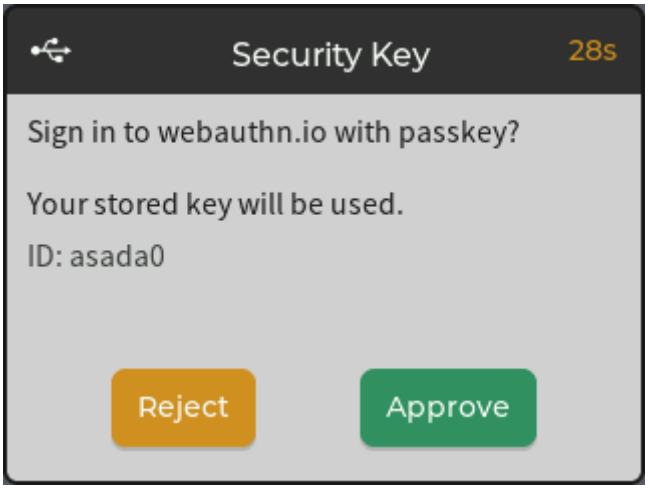
9.3 Signing in with a passkey

On a PC (USB):

1. Sign in to a FIDO2-capable service in a browser or app
2. Choose “Use a security key”
3. Connect Openloop over USB
4. The authentication confirmation appears on the Openloop screen
5. Tap the approve button → signed in

On a smartphone (BLE + Openloop Connect):

1. Go to the sign-in page of a FIDO2-capable service and choose passkey authentication
2. Choose **“Openloop Connect”** in the OS picker
3. Openloop wakes over BLE and shows the authentication confirmation
4. Tap the approve button → signed in



Passkey authentication confirmation

9.3.1 USB and BLE registration compatibility (generally fine; Google is the exception)

With most services, a single registration lets you use the passkey over either USB or BLE. With major services such as Microsoft, GitHub, Monex, JAL, and SBI VC Trade, one registration works on both transports.

However, **some services (Google being the prime example)** manage transports strictly per credential, so **a passkey registered over USB CTAPHID is not visible to Openloop Connect's BLE flow** (and vice versa). Only for such services do you need to **register the passkey twice with the same Openloop device — once over USB and once over BLE**. Openloop issues a different credential ID per transport even on the same hardware, so the server records two independent credentials.

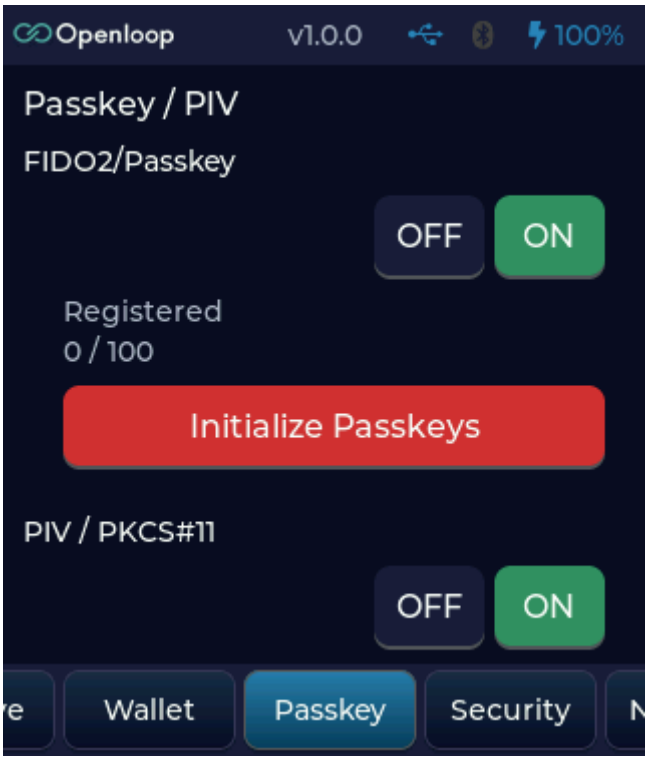
> ℹ️ In the device's "Passkey" list, a 🔌 (USB) or 📶 (Bluetooth) icon to the left of each credential tells you which path it was registered through.

9.4 Managing passkeys

You can manage your registered passkeys from the "Passkey" screen in the navigation bar.

The FIDO2/Passkey section:

- **ON/OFF**: enable or disable the passkey feature
- **Registered passkey list**: lists your passkeys by service
- **Delete individually**: use the trash icon next to each passkey
- **Reset passkeys**: completely deletes and regenerates every passkey and cryptographic key



Passkey management screen

⚠ **Warning**: running “Reset passkeys” makes every passkey unusable. You will have to register the security key again at each service.

⚠ **Important**: passkeys cannot be restored from a recovery phrase. Your wallet’s crypto assets can be, but passkeys **can never be recovered** after a reset or a factory reset. Registering again at each service is the only way back.

9.5 Examples of supported services and apps

Here are examples of services and applications where you can use Openloop as a security key.

Services confirmed to work:

Service	Use
Google / Gmail	Two-factor authentication and passwordless sign-in for Google accounts
Microsoft / Azure AD	Microsoft accounts, Microsoft 365
GitHub	Protecting repository access
Amazon	Two-factor authentication for Amazon accounts
Cloudflare	Protecting the dashboard

Service	Use
JAL (Japan Airlines)	Signing in to JAL Mileage Bank
Meta (Facebook / Instagram)	Meta account security
Nomura Securities	Signing in to online trading
SMBC Nikko Securities	Signing in to online trading
Monex Securities	Signing in to online trading
SBI VC Trade	Signing in to a crypto exchange

Tip: you can store up to 100 passkeys (resident keys).

Note: not every FIDO2-capable service accepts a physical security key. Some services and apps accept only the biometrics built into a phone (Face ID or a fingerprint) as a passkey and do not support external security keys. Check whether a “security key” option appears when you register.

---

10. Using It as a PKCS#11 Signer (PIV)

Openloop also works as a PIV (Personal Identity Verification) PKCS#11 signer. You can use it for SSH public key authentication, PDF signing, TLS client authentication, GPG signing, and more.

Note: to use the PIV features you need the **Openloop Connect** desktop application. The PKCS#11 library communicates with the Openloop device through Openloop Connect.

10.1 PIV at a glance

Four PIV slots:

Slot	Purpose	Description
9A	Authentication	SSH authentication, TLS client authentication
9C	Digital Signature	PDF signing, GPG signing, code signing
9D	Key Management	Key management
9E	Card Authentication	Card authentication

Supported algorithms:

- P-256 (ECDSA)
- Ed25519
- RSA-2048

10.2 Preparation

1. **Install Openloop Connect**: download the latest version from https://crypto.haudi.jp/openloop/connect/
2. **Connect Openloop over USB**
3. **Launch Openloop Connect**
4. **Turn PIV on**: switch it on in the PIV section of the “Passkey” screen in the navigation bar

10.3 Generating keys and creating certificates

Use a PKCS#11 tool (such as `pkcs11-tool`) to generate PIV keys and create certificates.

The PKCS#11 library is bundled with Openloop Connect, in the `pkcs11/` folder under the application’s installation path:

OS	Relative to the app
macOS	`<app>/Contents/Resources/pkcs11/libopenloop-pkcs11.dylib`
Windows	`<app>/resources/pkcs11/libopenloop-pkcs11.dll`
Linux	`<app>/resources/pkcs11/libopenloop-pkcs11.so`

The installation path `<app>` depends on how you installed the app:

Installation method	Location
macOS (DMG)	`/Applications/Openloop Connect.app`
Windows (official installer)	`C:\Program Files\Openloop Connect`
Windows (Microsoft Store)	In PowerShell: `(Get-AppxPackage 7CA75049.OpenloopConnect).InstallLocation`
Linux (deb)	`/opt/Openloop Connect`

The examples below set the full path for the macOS DMG build in a shell variable:

```
MODULE="/Applications/Openloop Connect.app/Contents/Resources/pkcs11/libopenloop-pkcs11.dylib"

# Generate a P-256 key in slot 9A
pkcs11-tool --module "$MODULE" --slot 0 --keypairgen --key-type EC:prime256v1 --id 9a

# Generate an RSA-2048 key in slot 9C
pkcs11-tool --module "$MODULE" --slot 1 --keypairgen --key-type rsa:2048 --id 9c
```

Step-by-step instructions: for details on SSH authentication, TLS client authentication, and using pkcs11-tool, see the Security Key Guide.

10.4 SSH authentication

You can use an Openloop PIV key for SSH public key authentication.

```
# Retrieve the public key
ssh-keygen -D "$MODULE"

# Connect over SSH (via PKCS#11)
ssh -I "$MODULE" user@hostname
```

10.5 PDF signing (Adobe Acrobat)

You can sign PDFs in Adobe Acrobat using an Openloop RSA-2048 key.

1. Acrobat preferences → “Signatures” → “Identities & Trusted Certificates” → “More”
2. “PKCS#11 Modules and Tokens” → “Attach Module”
3. Specify the path to the PKCS#11 library
4. Choose “Sign” in a PDF document and use your Openloop digital ID

Note: launch Openloop Connect before using Acrobat.

10.6 GPG signing

You can use an Openloop PIV key for GPG (GNU Privacy Guard) signing. Through gnupg-pkcs11-scd, you can sign Git commits and cryptographically sign files.

Note: gnupg-pkcs11-scd supports RSA keys only. EC keys (P-256 / Ed25519) cannot be used for GPG signing.

10.7 Managing PIV keys

Manage them in the PIV section of the “Passkey” screen in the navigation bar.

The PIV section:

- **ON/OFF**: enable or disable the PIV feature (USB connection required)
- **PIV PIN**: a separate PIN for PIV operations (see below)
- **Slot status**: shows the key type and whether a certificate is present for each slot
- **Reset PIV**: completely deletes every PIV key, certificate, and PIN

About the PIV PIN

The PIV PIN authenticates PIV signing over USB. It is **a separate PIN from your wallet PIN**.

Characteristics of the PIV PIN:

- 6–8 digits
- Locks after 8 failed attempts
- Managed separately from the wallet PIN

What the PIV PIN is for:

Once a PIV PIN is set, an application on your PC (SSH, Acrobat, and so on) can send the PIN over USB and sign without you approving on the Openloop screen (USB PIN authentication).

PIV PIN	Behaviour when signing
Not set	Tap the approve button on the Openloop screen for every signature
Set	Sending the PIN from the PC signs without any on-screen interaction (USB PIN authentication)

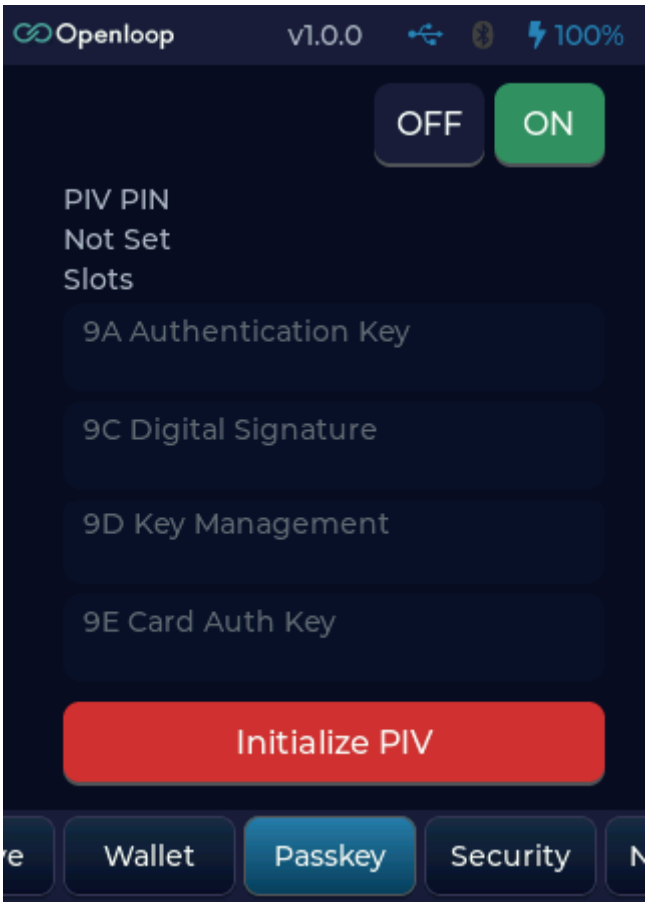
Tip: setting a PIV PIN is convenient when you sign frequently, as with SSH authentication or GPG signing. For important signatures such as PDF signing, it is safer to leave the PIV PIN unset and confirm on screen.

Setting the PIV PIN:

Set the PIV PIN from a PKCS#11 tool on your PC. A confirmation dialog appears on the Openloop screen — approve it.

Deleting the PIV PIN:

Tap the trash icon in the PIV section of the Passkey screen.



PIV management screen

⚠ **Warning**: running “Reset PIV” deletes every PIV key and certificate. You will have to set up SSH authentication and PDF signing again.

⚠ **Important**: PIV keys cannot be restored from a recovery phrase. After a reset or a factory reset they **can never be recovered**. You will have to regenerate the keys and reissue the certificates.

---

11. Screen Map

Here is how the Openloop screens are organized. You can reach the eight screens directly from the navigation bar, and swipe left and right to move between them.

```
Openloop navigation bar (scrolls horizontally)
│
├── Home ──────────────── Logo, connection mode, addresses for 5 currencies
│
├── Send ──────────────── Scan transaction QR → display signed QR
│
├── Receive ──────────┬── Choose a currency (7 options) → show address
│                     └── Show QR
│
├── Wallet
│   ├── Create Wallet ──── Generate / Restore
│   ├── Connect Wallet ─── BTC/ETH/XRP/SOL
│   ├── Erase Wallet
│   └── Recovery Phrase
│
├── Passkey
│   ├── FIDO2/Passkey ─── ON/OFF, count, passkey list (delete individually)
│   │                     Reset passkeys (deletes HMAC + seed + all entries)
│   │
│   └── PIV/PKCS#11 ────── ON/OFF, PIV PIN management
│                         Slot status (9A/9C/9D/9E: algorithm + certificate)
│                         Reset PIV (all slots + PIN)
│
├── Security
│   ├── PIN lock timing: — On sleep / On long sleep / At boot only / Off
│   ├── Set PIN (4-6 digits) / Change PIN
│   └── Delete PIN
│
├── Coin ──────────────── BTC/ETH/XRP/SOL/TRX
│   ├── Bitcoin ──────── Supported networks, Air Gap format (BBQr/UR), USB/BLE format
│   ├── Ethereum ─────── Supported networks, supported tokens, Air Gap format, USB/BLE format
│   ├── XRP ──────────── Supported networks, Air Gap format, USB/BLE format
│   ├── Solana ───────── Supported networks, Air Gap format, USB/BLE format
│   └── TRON ─────────── Supported networks, USB/BLE format
│
└── Settings
    ├── Sound ────────── Click sound ON/OFF, volume
    ├── Language ─────── Japanese / English
    ├── USB ──────────── ON/OFF, mode (Native / Compatible)
    ├── BLE ──────────── ON/OFF, pairing management
    ├── <span class="symbol warn">▲</span> Factory Reset
    └── About ────────── Version, copyright, open-source libraries
```

Related sections: initial setup → Ch. 2, screen operation → Ch. 3, connection methods → Ch. 7, security → Ch. 8, passkeys → Ch. 9, PIV → Ch. 10

12. Firmware Update (OTA)

12.1 What an OTA update is

Over-the-air (OTA) updates let you update the device firmware to the latest version.

Why update:

- New features
- Bug fixes
- Security patches
- Performance improvements

⚠ **Important**: Openloop has no internet connectivity. Firmware updates are performed over USB or BLE using **Openloop Connect** (the desktop or mobile app). You can download Openloop Connect from https://crypto.haudi.jp/openloop/connect/

12.2 How updating works

Openloop firmware updates are performed with Openloop Connect.

The mechanism:

1. Openloop Connect downloads the new firmware from the server
2. It sends the firmware data to Openloop over USB or BLE
3. Openloop verifies and installs the firmware

ℹ **Note**: the device on its own cannot check for or download updates. It must be connected to Openloop Connect.

When an update can be started

⚠ **Important**: a firmware update can only be started while the device is **awake and showing nothing on screen**. The update is rejected when:

- The device is **asleep** (screen off)
- A **PIN entry screen is showing** (waiting for unlock, changing the PIN, confirming a factory reset, and so on)
- A confirmation dialog or message is showing
- The QR scanner, mnemonic entry, or wallet creation/restore is in progress

This applies even if you have set the PIN lock to "Off." An update cannot be started while the device is asleep.

If the update is rejected, touch the device to wake it, unlock it if a PIN screen appears, close whatever is on screen, and start the update again.

Why this restriction exists: replacing the firmware is the most far-reaching operation the device can perform. If the update confirmation appeared on top of the lock screen, the update could be approved without the PIN ever being entered. Requiring an awake, idle device means the update is always approved by someone who can actually operate it.

12.3 Updating over USB

How to update

Step 1: Prepare

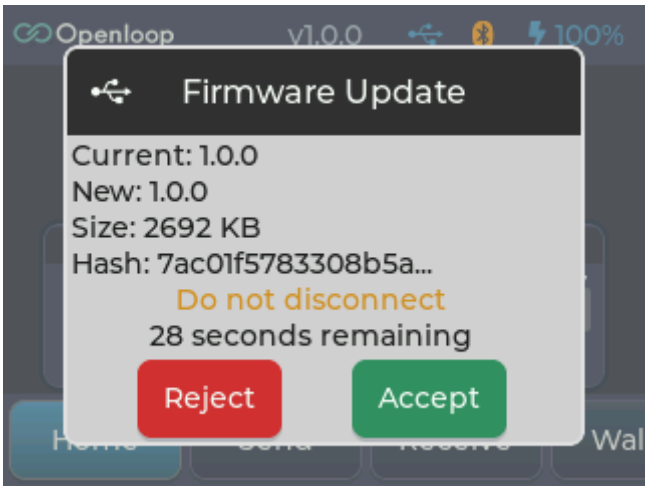
- Connect the USB-C cable (charging)
- Battery above 30%
- A stable power source
- Launch Openloop Connect
- **The device awake and showing nothing** (such as the home screen) — an update cannot be started while it is asleep or on a PIN entry screen

Step 2: Start the update

1. Run “Check for updates” in Openloop Connect
2. If a newer version exists, start the update
3. The “Firmware Update” confirmation dialog appears on Openloop

Item	Contents
Current	The current firmware version
New	The version to be installed
Size	The firmware size (KB)
Hash	The first 16 digits of the SHA-256 hash
N s remaining	A 30-second countdown

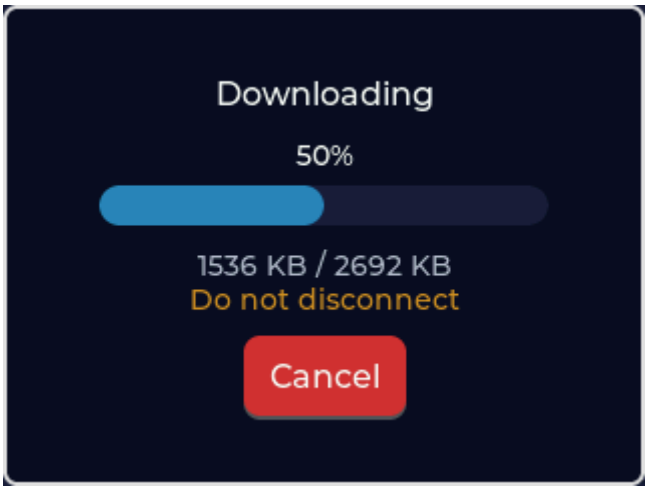
The dialog warns you not to disconnect. **If you do nothing for 30 seconds, it is rejected automatically.**



OTA notification

Step 3: Download and verification

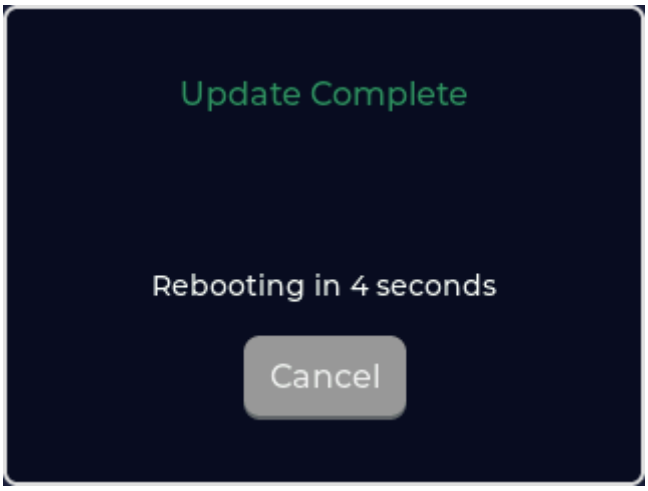
1. Choose “Approve” (right) rather than “Reject” (left)
2. The screen shows “Preparing…” then “Downloading,” with a progress bar and the percentage and KB updating
3. When the transfer finishes, it switches automatically to “Verifying” and checks the SHA-256 hash and the firmware signature



Download

Step 4: Installation and restart

1. After successful verification, “Update complete” appears
2. ⚠ **Never unplug the cable**
3. After a “Restarting in 5 seconds” countdown, the device restarts automatically



Installation

Step 5: Done

- After restarting, the new version is shown
- Check the version under “Settings” → “About”

Update complete: you can confirm the new version under “Settings” → “About”

12.4 Updating over BLE

You can also update over BLE (the steps are almost identical to USB).

How to update

1. **Touch the device to wake it** (an update cannot be started while it is asleep or on a PIN entry screen — see 12.2, “When an update can be started”)
2. Connect to your phone over BLE
3. Receive the update notification
4. Tap “Approve”
5. Download → verify → install
6. Restart

⚠ **Note**: keep your phone close to the device during a BLE update so the connection does not drop.

ℹ **Also**: while asleep on battery power the device does not advertise over BLE. If your phone cannot find it, wake the device first.

12.5 Cautions during an update

⚠ Do not

- ✗ Disconnect USB or BLE partway through
  - The firmware could be corrupted
- ✗ Press the power button
  - The update will be interrupted
- ✗ Update on a low battery
  - The device could lose power partway through

Do

- Use a stable power source (USB is recommended)
- Keep the battery above 30%
- Wait until the update finishes (2–3 minutes)
- Do not move the device

12.6 If an update fails

If an update fails, one of the following error messages appears:

Example errors:

- “Update failed” — an error occurred during the update
- “Hash verification failed” — the downloaded data is corrupted
- “Protocol error” — an error occurred during communication
- “Invalid firmware signature” — signature verification failed
- “Invalid OTA data” — the received data is malformed

You may also see this error **before** the update starts:

- “OTA rejected: UI busy” — the device is asleep, showing a PIN entry screen, or showing a dialog. Touch the device to wake it, clear whatever is on screen, and start the update again (see 12.2, “When an update can be started”)

What to do:

1. Restart the device
   - Power off, then on
2. If it still fails
   - Switch to USB
   - If you are on BLE, improve the radio conditions

⚠ **Important**: even if an update fails, your wallet data is unaffected (it is safe).

12.7 Checking the current version

Check the current version under “Settings” → “About.”

About screen

Tip: updating regularly keeps you on the latest features and security.

13. Troubleshooting

13.1 Frequently asked questions

Q1: I forgot my PIN

A: You can recover if you have your recovery phrase.

1. Perform a factory reset
   - “Settings” → “Factory Reset”
2. Restore the wallet
   - “Wallet” screen → “Create Wallet” → “Restore”
   - Enter your recovery phrase

⚠ **Warning**: without your recovery phrase, you lose your assets.

Q2: The screen is unresponsive or frozen

A: Restart as follows.

1. Power off with the power button
2. Press the power button again to start up

ℹ **Tip**: this resolves almost every problem.

Q3: The QR code will not scan

A: Check the following.

- Screen brightness: turn up your monitor’s brightness
- Distance: adjust the distance between Openloop and the monitor (15–30 cm recommended)
- Angle: change the angle to avoid reflections
- QR code size: enlarge it in Sparrow Wallet or similar

ℹ **Tip**: when a QR code has several frames, wait for it to cycle through automatically.

Q4: The USB or BLE connection keeps dropping

Over USB:

- Check that the cable is properly connected
- Try a different USB port
- Replace the cable (it may be faulty)

Over BLE:

- Move the device and your phone closer together
- Re-check your Bluetooth settings
- Remove the pairing and connect again

Q5: I lost my recovery phrase

A: Unfortunately, there is no way to recover it.

⚠️ **Worst case**: if the device breaks, your assets are lost forever.

What to do right now:

1. Display the recovery phrase again: “Wallet” screen → “Recovery Phrase”
2. Make several copies: paper plus a metal plate
3. Store them in different places

ℹ️ **The lesson**: your recovery phrase **is** your assets. Guard it carefully.

13.2 Error messages and what to do

“Wrong PIN!”

Cause: the PIN is incorrect.

What to do:

- Enter it again carefully
- After 10 failures the device erases all data (the number of remaining attempts is shown)

“No wallet”

Cause: no wallet has been created.

What to do:

1. Create one: “Wallet” screen → “Create Wallet” → “Generate”
2. Restore one: “Wallet” screen → “Create Wallet” → “Restore”

“Wallet Corrupted”

Cause: when this appears on a device that has no wallet yet (first power-on, or just after “Erase Wallet”), it is a **false alarm from a defect in v1.1.0 and earlier**, not a fault. **Fixed in v1.1.1** — from v1.1.1 on, the “Welcome to Openloop” dialog appears as it should.

What to do:

- The choices are the same as the “Welcome to Openloop” dialog. Just choose “Generate” or “Restore” (see 2.3)
- **Updating to v1.1.1 or later** stops it appearing (see chapter 12)

⚠ If it appears suddenly on a device with a wallet you were using, it may not be a false alarm (see 8.4).

“Pairing failed” (BLE)

Cause: Bluetooth pairing failed.

What to do:

1. Check the BLE setting: “Settings” → “BLE” → ON
2. Re-check the pairing code: do the six digits match?
3. Pair again: “Unpair” → “Start pairing”

“Update failed” (OTA)

Cause: the firmware update failed.

What to do:

1. Restart the device
2. Switch to USB (if you were on BLE)
3. Try the update again

Tip: your wallet data is unaffected (it is safe).

"Invalid mnemonic" (when restoring)

Cause: the recovery phrase is wrong.

What to do:

- Check the spelling against the BIP39 word list
- Check the order: first word, second word, and so on
- Check the count: 12 or 24 words

13.3 Factory Reset

What a factory reset does

It erases all data and returns the device to its initial state.

Warning: this **cannot be undone**.

Data that is deleted:

- The wallet (private keys, recovery phrase)
- The PIN
- Settings (language, sound, network, and so on)
- BLE pairing data
- FIDO2 passkeys (HMAC key, seed, all entries)
- PIV key pairs and certificates (all four slots)
- The PIV PIN

Data that is not deleted:

- The firmware version

▲ **About recovery**: your wallet's crypto assets can be restored from your recovery phrase.

However, **FIDO2 passkeys and PIV keys cannot be restored**. Passkeys must be registered again at each service, and PIV keys must be regenerated with new certificates issued.

How to perform a factory reset

Step 1: Confirm your backup

▲ **Essential**: check the following.

- My recovery phrase is backed up
- I have moved all my assets (or I plan to restore)

Step 2: Run the factory reset

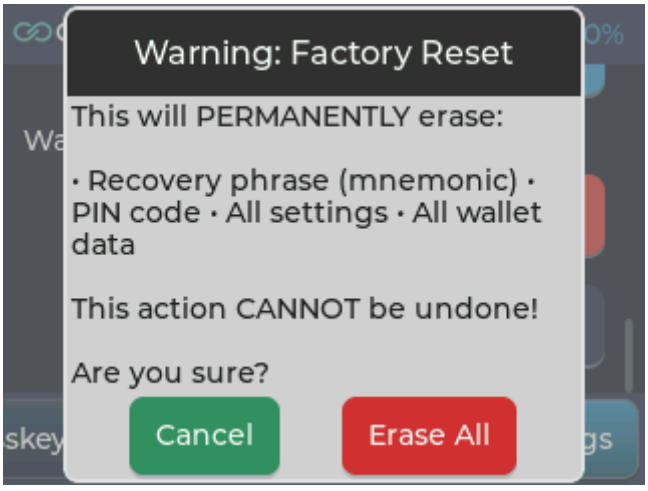
1. "Settings" → "Factory Reset"
2. Review the warning

```
<span class="symbol warn">▲</span> Warning: danger zone

The following will be completely erased:
- Recovery phrase (mnemonic)
- PIN
- All settings
- All wallet data

This cannot be undone!

[Erase All] [Cancel]
```



Factory reset confirmation

1. Tap "Erase All"
2. Enter your PIN (final confirmation)

3. The erase runs
   - “Please wait…” is displayed
   - It finishes in a few seconds

Step 3: Back to the initial state

- The device restarts
- It is in the same state as on first boot
- You need to create or restore a wallet

Done: the device has been returned to factory condition.

When you might need a factory reset

- ★ You forgot your PIN (and plan to restore from your recovery phrase)
- You are giving the device to someone else
- You want to clear out a test wallet
- You want to reset your settings

13.4 Recovery mode (recovery firmware)

What recovery mode is

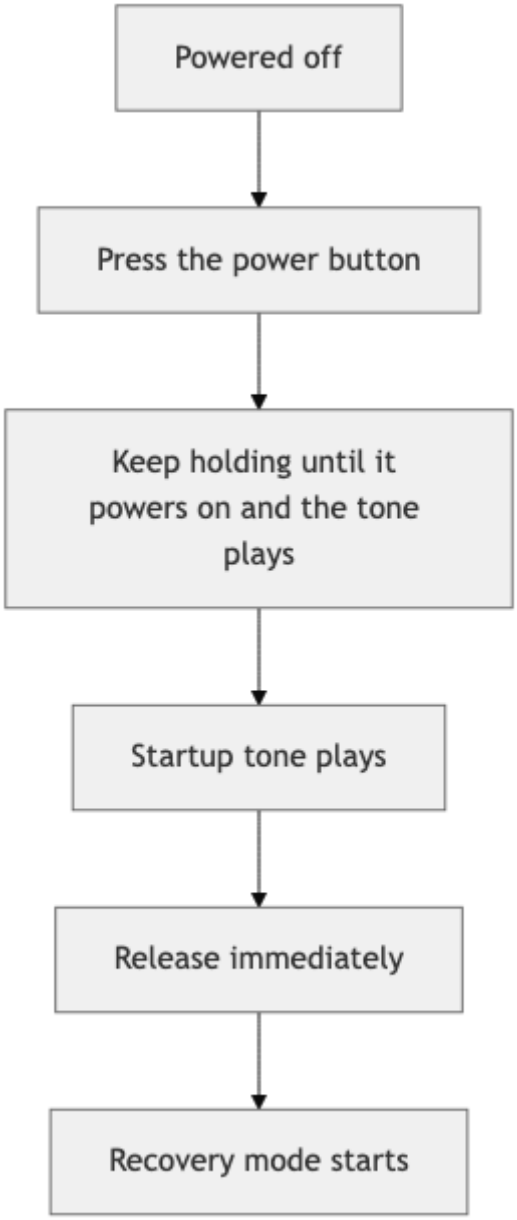
Recovery mode is an emergency feature that starts automatically or manually when the main firmware becomes corrupted and will not boot. Recovery firmware stored in a separate partition starts up, letting you reinstall the main firmware over USB or BLE.

Characteristics of recovery mode:

- A dedicated partition: stored in a “factory” partition separate from the main firmware
- Firmware update: you can reinstall the main firmware through Openloop Connect
- ★ **Wallet data is protected**: your wallet data is preserved even in recovery mode
- Settings: you can change the language, USB, BLE, and pairing settings

How to enter recovery mode

1. Power the device off
2. Hold the power button down until it powers on and the startup tone plays
3. Release the power button as soon as you hear the tone



⚠ **Important**: release within **3 seconds** of the tone. Too late and it boots normally.

ℹ **Tip**: the trick is to use the tone as your cue. Even if the volume is set to zero, the timing is judged internally in exactly the same way.

The recovery mode home screen

In recovery mode you see the following information and buttons:

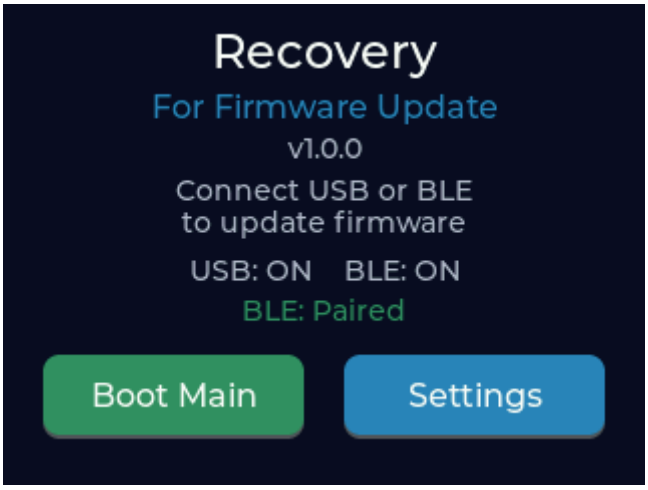
Information shown:

- The recovery firmware version
- USB connection status

- BLE connection status

Buttons:

- **Boot Main**: returns to the main firmware. Tap this if you entered recovery mode by accident (if the main firmware cannot be read, it shows “No FW” and the button is disabled)
- **Settings**: opens the settings screen for language, USB, BLE, and pairing



Recovery mode screen

⚠ **Note**: if the main firmware is corrupted, tapping “Boot Main” may return you to recovery mode. In that case you need to reinstall the firmware.

The recovery mode settings screen

You can change the following on the settings screen:

- **Language**: Japanese / English
- **USB**: ON / OFF
- **BLE**: ON / OFF
- **Pairing**: start pairing / unpair

ℹ **Tip**: even when the main firmware will not boot, you can turn USB or BLE on from the recovery mode settings screen and then connect and update with Openloop Connect.

Updating firmware in recovery mode

Supported transports:

- USB: over USB Type-C
- BLE: over Bluetooth Low Energy

How to update:

1. Boot into recovery mode
2. Turn USB or BLE on in the settings screen (if needed)
3. Launch Openloop Connect and connect the device
4. Openloop Connect shows the latest firmware — run the update
5. The device restarts automatically and boots the main firmware

⚠ **Note**: do not power the device off during a firmware update.

---

14. Supported Crypto Assets and Networks

14.1 Bitcoin (BTC)

Supported networks

Network	Short name	Purpose
Bitcoin Mainnet	BTC Main	Real transactions (production)
Bitcoin Testnet	BTC Test	Development and testing

Address formats (examples)

- Legacy (P2PKH): `1...` (BIP44)
- Nested SegWit (P2SH): `3...` (BIP49)
- Native SegWit (Bech32): `bc1q...` (BIP84)
- Taproot (P2TR): `bc1p...` (BIP86) ⚠ **Address display only. Signing is not supported**
- Testnet: `tb1q...` and so on

HD derivation path

- Standard path (example): `m/84'/0'/0'/0/0` (BIP84: Native SegWit)
- Depending on the script type you can also choose `m/49'` (Nested SegWit), `m/44'` (Legacy), or `m/48'` (multisig) — see 4.1

⚠ **Taproot (`m/86'`) cannot be signed.** If you create a Taproot account in your companion wallet, the signing confirmation screen shows “Cannot sign: Taproot (P2TR) is not supported” and the “Sign” button is disabled.

ℹ **Tip**: compatibility with Sparrow Wallet is excellent.

For details of the confirmation screen, see "6.7.1 Bitcoin (BTC)."

14.2 Ethereum (ETH)

Supported networks (215 chains: 129 mainnets + 86 testnets)

Openloop supports every EVM chain on which a CoinGecko Top 1000 token exists.

Support at a glance:

Category	Count
Mainnets	129
Testnets	86
Total	**215**

Broadly, this covers Ethereum and its layer 2s, alternative layer 1s (BNB Smart Chain, Avalanche, and so on), ZK rollups, and emerging chains. For the complete list of built-in network names, see "15.7 Built-in EVM networks."

Major networks:

Display name	Chain ID	Purpose
Ethereum Mainnet	1	Production
Ethereum Sepolia	11155111	Testing
Ethereum Holesky	17000	Testing
Arbitrum One	42161	Layer 2
Arbitrum Sepolia	421614	Testing
Optimism	10	Layer 2
Optimism Sepolia	11155420	Testing
Base	8453	Layer 2 (Coinbase)
Base Sepolia	84532	Testing
Polygon	137	Sidechain
Polygon Amoy	80002	Testing
zkSync Era	324	zkRollup
zkSync Sepolia	300	Testing
Linea	59144	zkRollup

Display name	Chain ID	Purpose
Linea Sepolia	59141	Testing
Scroll	534352	zkRollup
Scroll Sepolia	534351	Testing
Polygon zkEVM	1101	zkRollup
Polygon zkEVM Cardona	2442	Testing
BNB Smart Chain	56	EVM-compatible chain
BNB Testnet	97	Testing
Avalanche C-Chain	43114	EVM-compatible chain
Avalanche Fuji	43113	Testing
Fantom Opera	250	EVM-compatible chain
Fantom Testnet	4002	Testing
Gnosis Chain	100	Sidechain
Gnosis Chiado	10200	Testing
Cronos Mainnet	25	Crypto.com
Cronos Testnet	338	Testing
Mantle	5000	Layer 2
Mantle Sepolia	5003	Testing
Blast	81457	Layer 2
Blast Sepolia	168587773	Testing
Celo	42220	Mobile-first
Celo Alfajores	44787	Testing
Mode	34443	Layer 2
Mode Sepolia	919	Testing

Other supported networks (excerpt):

Category	Networks included
Layer 2	Manta Pacific, Metis, Boba, Immutable zkEVM, Taiko, Fraxtal
Alt L1	Aurora, Moonbeam, Moonriver, Kava, Canto, Evmos, Klaytn
DeFi-focused	

Category	Networks included
	PulseChain, Ronin, Core DAO, Oasis, Harmony, Conflux
Gaming/NFT	Immutable X, Loot, Ancient8, Beam
Enterprise	XDC Network, Rootstock, Telos, Wanchain
Emerging	Berachain Bartio (testnet), Morph, Merlin, BOB, Zora

Tip: for the list of built-in networks, see "15.7 Built-in EVM networks."

About networks that are not built in:

- EVM networks outside the list above can still **be signed for**
- The signing confirmation screen shows something like "Chain ID 12345" instead of a name, and the currency symbol for the amount and fee becomes "ETH?"
- Check the network information in your companion wallet before signing

Address format

- All: `0x...` (20 bytes of hex)

HD derivation path

- Standard path (example): `m/44'/60'/0'/0/0` (BIP44: Ethereum)

ERC-20 token support (2,599 tokens)

Coverage: the CoinGecko top 1000 tokens by market capitalization (2,599 entries including multi-chain deployments)

Supported tokens at a glance:

Category	Tokens (approx.)	Representative tokens
Stablecoins	180+	USDT, USDC, DAI, FRAX, TUSD, BUSD
DeFi protocols	450+	UNI, AAVE, COMP, MKR, CRV, SUSHI
Layer 2 tokens	200+	ARB, OP, POL, IMX, LRC
Meme tokens	150+	DOGE, SHIB, PEPE, FLOKI, BONK
Gaming/NFT	180+	AXS, SAND, MANA, ENJ, GALA, APE

Category	Tokens (approx.)	Representative tokens
Infrastructure	250+	LINK, GRT, FIL, RNDR, OCEAN
Wrapped tokens	120+	WETH, WBTC, stETH, rETH, cbETH
Other	1,057+	Various project tokens

Important characteristics:

- A shared address: ETH and ERC-20 tokens use the same address (`0x...`)
- Gas is required: fees for ERC-20 transfers are paid in ETH
- Network-dependent: the same token name on a different network is a different token (for example, mainnet USDT and Arbitrum USDT are different)
- Multi-chain: many tokens are deployed on several chains

Rough fees by network (as of 2025):

Network	Gas fee (USD)	Speed
Ethereum Mainnet	$1–$20+	15 seconds to a few minutes
Arbitrum One	$0.01–$0.5	Seconds
Base	$0.01–$0.3	Seconds
Polygon	$0.001–$0.1	Seconds

Major token examples:

Token	Contract address (mainnet)	Purpose
USDT	`0xdAC17F958D2ee523a2206206994597C13D831ec7`	Stablecoin
USDC	`0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48`	Stablecoin
DAI	`0x6B175474E89094C44Da98b954EedeAC495271d0F`	Decentralized stablecoin
LINK	`0x514910771AF9Ca656af840dff83E8264EcF986CA`	Oracle
UNI	`0x1f9840a85d5aF5bf1D1762F925BDADdC4201F984`	DEX governance
AAVE	`0x7Fc66500c84A76Ad7e9c93437bFc5Ac33E2DDaE9`	Lending protocol
ARB	`0x912CE59144191C1204E64559FE8253a0e49E6548`	Arbitrum L2 token

Token	Contract address (mainnet)	Purpose
OP	`0x4200000000000000000000000000000000000042`	Optimism L2 token
POL (ex-MATIC)	`0x455e53CBB86018Ac2B8092FdCd39d8444aFFC3F6`	Polygon token
JPYC	`0xE7C3D8C9a439feDe00D2600032D5dB0Be71C3c29`	Japanese yen stablecoin

Tip: for the list of built-in tokens, see "15.8 Built-in ERC-20 tokens."

About tokens that are not built in:

- ERC-20 tokens outside the list above can still **be signed for**
- The signing confirmation screen shows "ERC-20 Token" or "Unknown ERC-20" instead of a name, together with the warning "Unknown token - verify contract!"
- The contract address is displayed, so compare it with your companion wallet

Note: check the contract address before sending, and confirm it is not a scam token.

For details of the confirmation screen, see "6.7 The signing confirmation screen in detail."

Detailed instructions:

- Receiving: 5.6 Receiving ERC-20 tokens
- Sending: 6.6 Sending ERC-20 tokens

14.3 XRP (Ripple)

Supported networks

Network	Short name	Purpose
XRP Ledger Mainnet	XRP Main	Real transactions
XRP Testnet	XRP Test	Testing

Address format

- Classic Address: `r...`

Note: X-Address is not supported at present.

Destination tag support

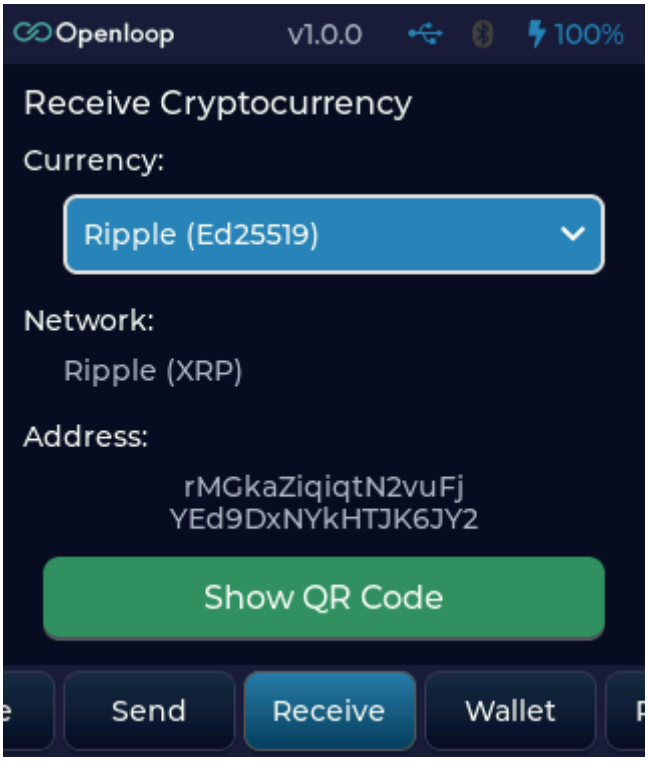
Supported: the destination tag required when sending to an exchange is displayed.

ℹ For details of the confirmation screen, see "6.7.4 XRP (Ripple)."

HD derivation path

- Standard path for Ed25519: `m/44'/144'/0'/0'/0'` (BIP44, all levels hardened)
- Standard path for secp256k1: `m/44'/144'/0'/0/0` (BIP44)

⚠ For XRP the derivation path changes with the curve you select. Set the curve on the "Connect Wallet" screen (see 4.1).



XRP receive screen

14.4 Solana (SOL)

Supported networks

Network	Purpose
Solana Mainnet	Real transactions

Address format

- A Base58-encoded 32-byte public key (for example `7xKXtg...`)

HD derivation path

- Receive screen default: `m/44'/501'/0'` (three levels)
- Used when signing: `m/44'/501'/0'/0'` (four levels)
- Both are SLIP-0010 (all levels hardened, Ed25519)

Supported signature types

- Transaction signing
- Off-chain message signing

Connection methods

Method	Support
Air Gap (UR)	✓
USB (APDU)	✓
BLE (APDU)	▲ The device supports it, but there is currently no Solana wallet app that connects over BLE

14.5 TRON (TRX)

Supported networks

Network	Purpose
TRON Mainnet	Real transactions

Address format

- Base58Check encoded, starting with `T` (for example `TJYs...`)

HD derivation path

- Standard path: `m/44'/195'/0'/0/0` (BIP44: TRON, secp256k1)

Connection methods

Method	Support
Air Gap (UR)	✗ Not supported
USB (APDU)	✓
BLE (APDU)	

Method	Support
	⚠ The device supports it, but there is currently no TRON wallet app that connects over BLE

⚠ **TRON does not support Air Gap (QR codes).** Use a USB connection for TRON.

---

15. Appendix

15.1 Glossary

Hardware wallet

A wallet that keeps private keys safely on a dedicated device. Because it is isolated from the internet, it is largely immune to malware.

Recovery phrase (mnemonic)

A list of 12 or 24 English words. The only way to restore a wallet. **Your most important asset.**

PSBT (Partially Signed Bitcoin Transaction)

An unsigned Bitcoin transaction. The standard format for signing with an air-gapped wallet.

Air Gap

A method that isolates a device completely from the internet, exchanging data through QR codes. The highest level of security.

HD key derivation (Hierarchical Deterministic Key Derivation)

The technique of generating many addresses hierarchically from a single seed (recovery phrase) — BIP32/BIP44/BIP84.

Mainnet

The production blockchain network where real crypto assets circulate.

Testnet

A blockchain network for development and testing, where you can practise with worthless coins.

BBQr

A format that splits large data across several QR codes for transmission. Optimized for Bitcoin PSBTs.

UR (Uniform Resources)

A general-purpose QR code format, expected to be adopted by many wallets.

BIP32

The standard for HD (hierarchical deterministic) wallets. It lets you generate many addresses from one seed by specifying a derivation path (for example m/84'/0'/0'/0/0).

BIP39

The standard for recovery phrases, whose words are drawn from a list of 2,048 English words.

BIP44 / BIP84

Standards for address derivation paths. BIP44 is used for the traditional format (P2PKH); BIP84 for Native SegWit (bc1…).

BLE (Bluetooth Low Energy)

The low-power Bluetooth standard, used to connect to phones.

OTA (Over-The-Air)

Firmware updating over a wireless connection.

ERC-20

The token standard on Ethereum (USDT, USDC, and so on).

FIDO2 / CTAP2

A secure authentication standard that replaces passwords, enabling passwordless sign-in to web services. CTAP2 (Client to Authenticator Protocol 2) is the protocol between the device and the browser.

Passkey

An authentication credential based on FIDO2. A unique key pair is generated for each service and stored safely on the device.

PIV (Personal Identity Verification)

The US government's smart card authentication standard, used for SSH authentication, PDF signing, TLS client authentication, and more.

PKCS#11

The standard interface to cryptographic tokens (smart cards, HSMs, and so on). Openloop uses it to reach the PIV features.

Openloop Connect

Openloop's companion application, available for desktop (Windows/Mac/Linux) and mobile (iOS/Android). For PIV/PKCS#11 it works with the PKCS#11 library over WebSocket.

Destination tag

An optional identifier used when sending XRP. Required when sending to an exchange.

15.2 Supported wallet software

For Bitcoin

Software	Transport	OS	Verified
Sparrow Wallet	QR code	Windows / Mac / Linux	✓ Verified
Other KeyStone-compatible apps	QR code	Various	✓ Many supported

For Ethereum / ERC-20

Software	Transport	OS	Verified
MetaMask (PC)	USB (WebHID)	Chrome / Brave / Edge	✓ Verified
MetaMask Mobile	BLE / QR code	iOS / Android	✓ Verified
Rabby	USB (WebHID)	Chrome / Brave / Edge	✓ Verified
Other Ledger-compatible apps	USB / BLE	Various	✓ Many supported
Other KeyStone-compatible apps	QR code	Various	✓ Many supported

For XRP

Software	Transport	OS	Verified
XRP Toolkit	USB	Web	✓ Verified
Other Ledger-compatible apps	USB / BLE	Various	✓ Many supported

For Solana

Software	Transport	OS	Verified
Other Ledger-compatible apps	USB	Various	✓ Many supported

For TRON

Software	Transport	OS	Verified
Other Ledger-compatible apps	USB	Various	✓ Many supported

> **About compatibility**: Openloop uses the Ledger-compatible protocol over USB and BLE, and the KeyStone-compatible protocol over QR codes. Ledger-compatible applications other than Ledger Live, and KeyStone-compatible applications, generally work.

15.3 Technical specifications (summary)

Hardware

- Processor: ESP32-S3 (dual-core Xtensa LX7, running at 160 MHz)
- Memory: 8 MB PSRAM, 16 MB flash
- Display: 320×240 pixel IPS LCD (touchscreen)
- Secure element: NXP SE050 (EAL 6+ certified)
- Connectivity: USB-C / Bluetooth 5.0 (BLE) (Wi-Fi hardware is present but the firmware never uses it)
- Camera: GC0308 (for scanning QR codes)
- Battery: 450 mAh lithium polymer (built-in)

Software

- Firmware: based on ESP-IDF 5.4
- UI: LVGL 9.x
- Cryptography: mbedTLS, SE050
- Standards: BIP32/BIP39/BIP44/BIP84, EIP-55, SLIP-0044
- FIDO2/CTAP2: ES256 (P-256), EdDSA (Ed25519), up to 100 resident keys
- PIV: P-256, Ed25519, RSA-2048, four slots (9A/9C/9D/9E)

15.4 Third-party libraries

Libraries used

Openloop uses well-established third-party libraries:

Library	Purpose	Licence
AES-GCM (Brian Gladman)	AES-GCM encryption	BSD
BBQr	The BBQr protocol	MIT
bc-ur	UR encoding/decoding	BSD-2-Clause-Patent
Blockstream Jade	OTA / wire protocol	MIT
ESP-BSP	Board support	Apache 2.0
ESP-IDF	Firmware framework	Apache 2.0
ESP32-Camera	Camera driver	Apache 2.0
esp32_deflate	Compression/decompression	MIT
esp_jpeg	JPEG decoding	Apache 2.0
esp_tinyusb	USB communication wrapper	Apache 2.0
FreeRTOS	Real-time OS	MIT
LVGL	UI framework	MIT
lwIP	TCP/IP stack	BSD-3-Clause
mbedTLS	TLS / cryptography	Apache 2.0
newlib	C standard library	BSD
NimBLE	BLE stack	Apache 2.0
Noto Sans CJK (Google)	Japanese font	SIL OFL 1.1
NXP SE050 Middleware	Secure element communication	BSD-3-Clause

Library	Purpose	Licence
quirc	QR code decoding	ISC
secp256k1	Elliptic curve cryptography	MIT
TinyCBOR	CBOR encoding/decoding	MIT
TinyUSB	USB device stack	MIT
Trezor Crypto	Cryptography and signing	MIT

You can see the details under “Settings” → “About.”

Licences

15.5 Tutorial: Sparrow Wallet (Bitcoin Air Gap)

This tutorial walks through pairing Sparrow Wallet with Openloop over Air Gap (QR codes) and sending Bitcoin.

What you need:

- An Openloop with a wallet created
- A PC with Sparrow Wallet installed
- An internet connection (for the PC only)

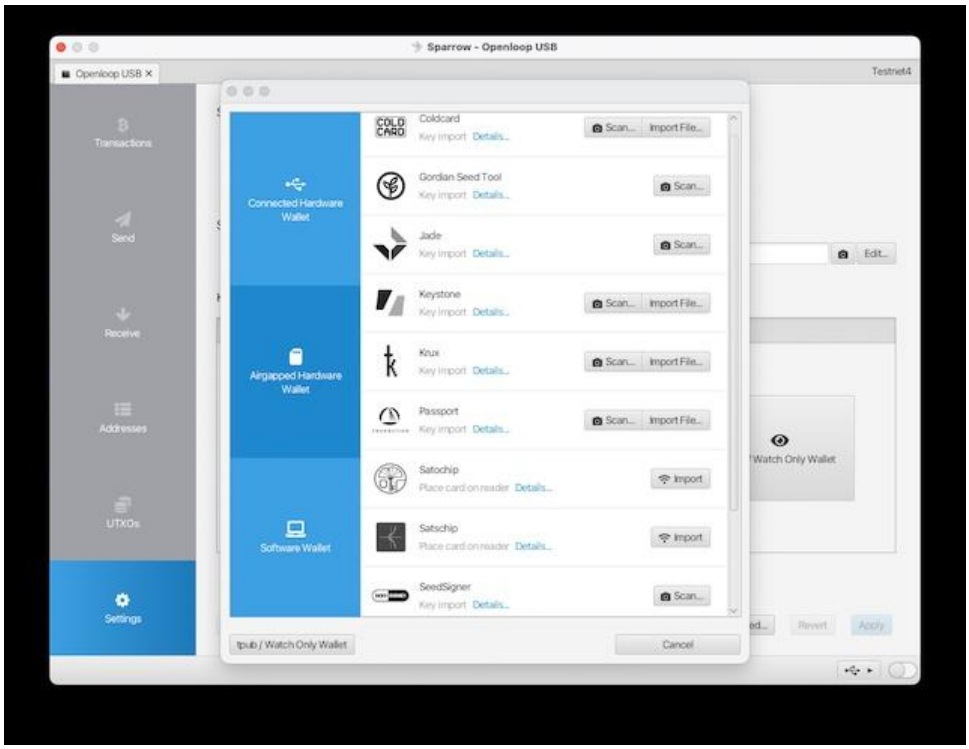
Step 1: Export the xpub from Openloop

1. On Openloop, tap “Wallet” → “Connect Wallet” → “Bitcoin”
2. The QR code appears

Wallet export QR

Step 2: Create the wallet in Sparrow Wallet

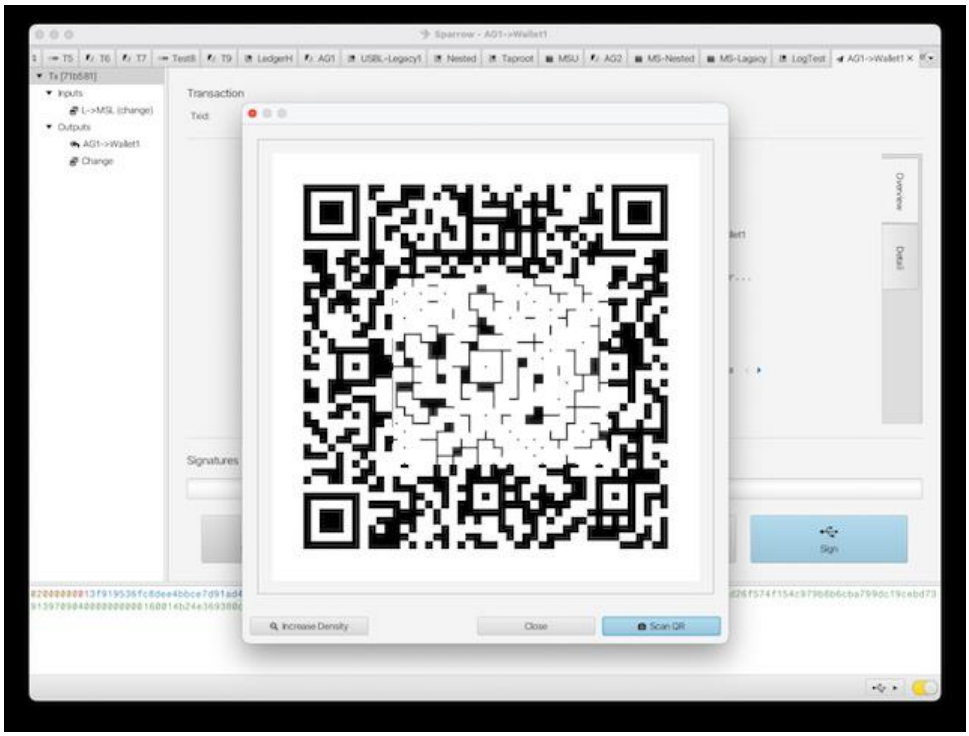
1. Launch Sparrow Wallet
2. “File” → “New Wallet” → enter a wallet name
3. Choose “Airgapped Hardware Wallet”
4. Click “Scan…” and scan the QR code on Openloop



1. Once the xpub is read, click “Apply” → “Save”

Step 3: Build the transaction

1. Select the “Send” tab in Sparrow Wallet
2. Enter the destination address and the amount
3. Click “Create Transaction”
4. Click “Finalize Transaction for Signing”
5. Click “Show QR” to display the PSBT QR code



Step 4: Sign the PSBT on Openloop

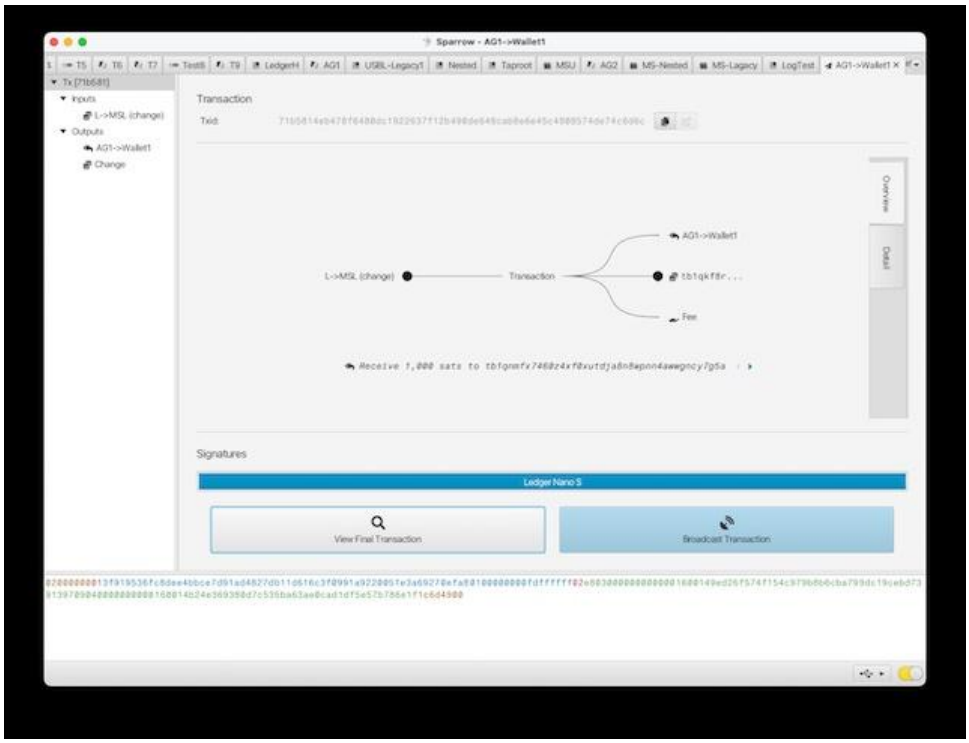
1. Tap “Send” on Openloop
2. Tap “Scan QR”
3. Scan the PSBT QR code shown in Sparrow
4. Review the transaction details
5. Tap “Sign” (right) to sign
6. The signed PSBT QR code appears

Step 5: Read the signed PSBT back into Sparrow

1. Click “Scan QR” in Sparrow Wallet
2. Scan the signed QR code on Openloop
3. The signature is verified

Step 6: Broadcast

1. Click “Broadcast Transaction”
2. The transaction is sent to the network
3. Check it on the “Transactions” tab



Done: the Bitcoin transfer is complete.

15.6 Tutorial: Safe (Ethereum USB)

This tutorial walks through pairing Safe (a multisig wallet) with Openloop over USB and sending Ethereum.

What you need:

- An Openloop with a wallet created and USB enabled
- A PC with Chrome, Brave, or Edge
- A USB-C cable
- An internet connection

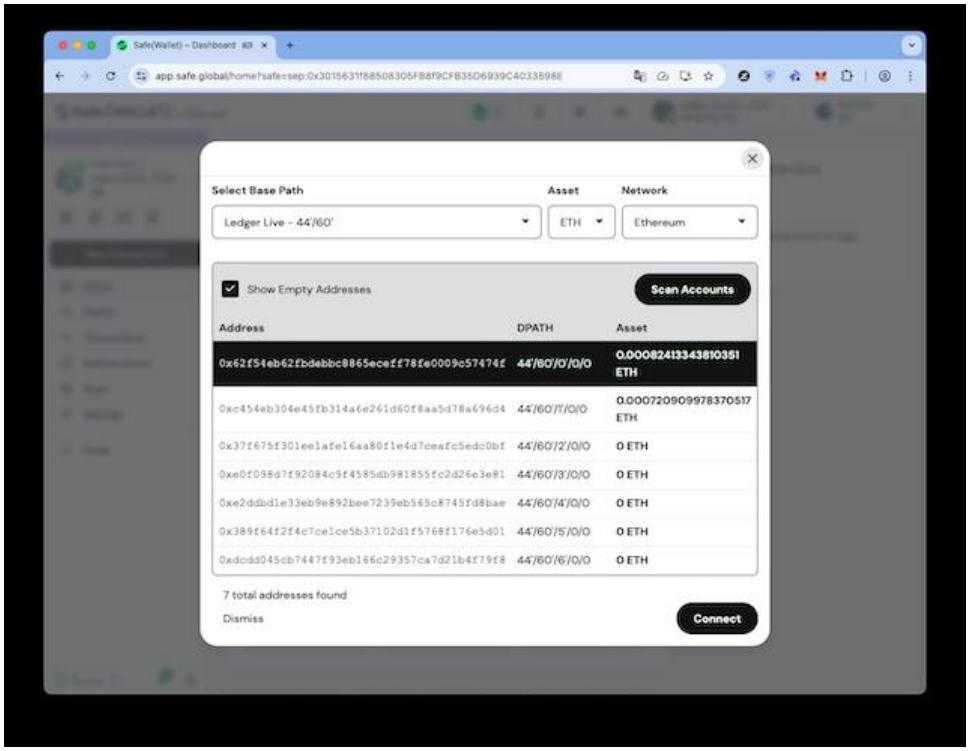
Step 1: Turn on USB on Openloop

1. On Openloop, tap “Settings” → “USB”
2. Set USB to “ON”
3. Connect to the PC with a USB-C cable

Step 2: Add the account in Safe

1. Go to app.safe.global
2. Click “Connect Wallet”
3. Choose “Ledger” (Openloop is Ledger-compatible)

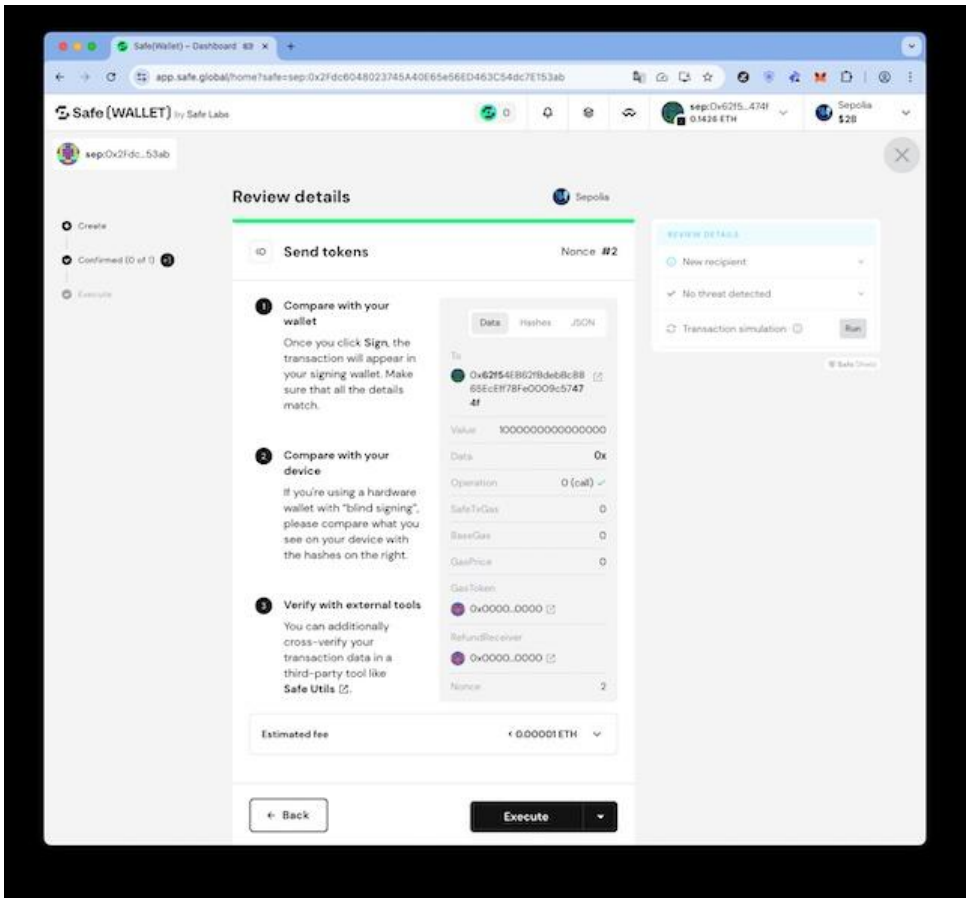
4. Choose the “Ledger Live” path



1. When the address confirmation appears on Openloop, tap “Approve”
2. The address is added as a Safe owner

Step 3: Build the transaction

1. Click “New Transaction” in Safe
2. Choose “Send tokens”
3. Enter the destination address and the amount
4. Click “Next” → “Execute”

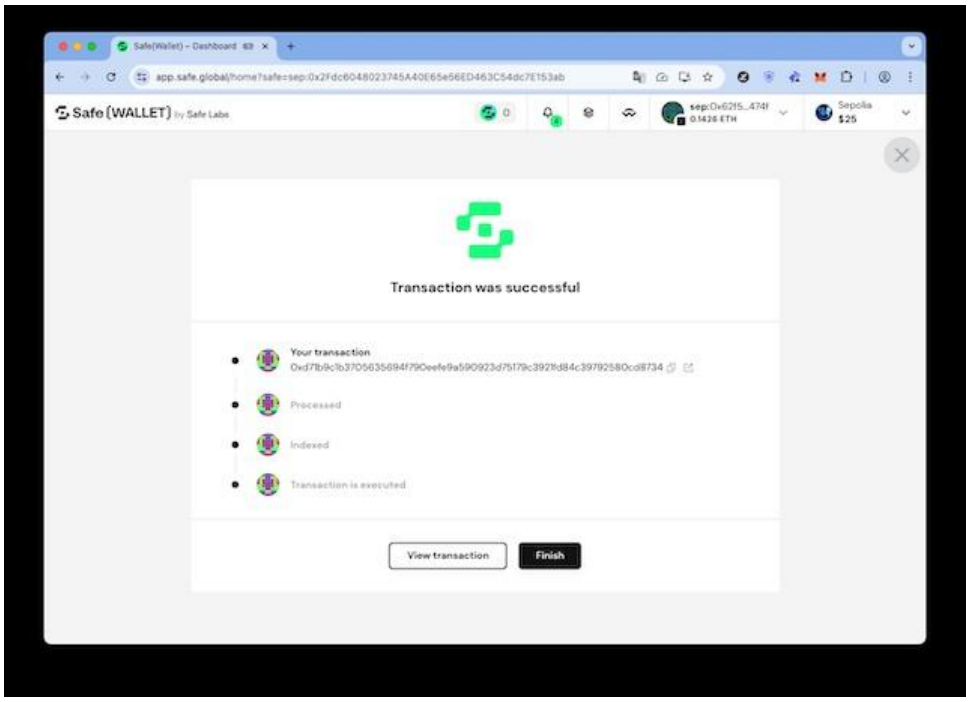


Step 4: Sign on Openloop

1. The transaction confirmation screen appears on Openloop
2. Check the destination, amount, and fee
3. Tap “Sign” (right) to sign

Step 5: Execute the transaction

1. Safe confirms the signature
2. Once enough signatures are collected, it broadcasts automatically
3. “Transaction was successful” appears



Done: the transfer from Safe is complete.

15.7 Built-in EVM networks

Openloop supports **every EVM network**. The list below covers the built-in networks (215 chains) whose names are displayed on the device screen.

Note: EVM networks not in this list can still be used. In that case the chain ID is displayed instead of a network name.

EVM mainnets (129 chains)

Chain ID	Network name	Native currency
1	Ethereum	ETH
10	Optimism	ETH
14	Flare Network	FLR
19	Songbird	SGB
20	Elastos	ELA
24	KardiaChain	KAI
25	Cronos	CRO
30	Rootstock RSK	RBTC

Chain ID	Network name	Native currency
40	Telos	TLOS
50	XDC Network	XDC
56	BNB Smart Chain	BNB
57	Syscoin NEVM	SYS
66	OKT Chain	OKT
82	Meter	MTR
88	Viction	VIC
100	Gnosis Chain	XDAI
106	Velas	VLX
122	Fuse	FUSE
128	Huobi ECO Chain	HT
130	Unichain	UNI
137	Polygon	POL
143	Monad	MON
146	Sonic	S
169	Manta Pacific	ETH
177	HashKey Chain	HSK
185	Mint	ETH
196	X Layer	OKB
199	BitTorrent	BTT
204	opBNB	BNB
232	Lens	GHO
239	TAC	TAC
250	Fantom	FTM
252	Fraxtal	frxETH
255	Kroma	ETH
288	Boba Network	ETH
295	Hedera	HBAR
324	zkSync Era	ETH
369	PulseChain	PLS

Chain ID	Network name	Native currency
388	Cronos zkEVM	zkCRO
416	SX Network	SX
480	World Chain	ETH
592	Astar	ASTR
747	Flow EVM	FLOW
766	QL1	QOM
964	Bittensor EVM	TAO
988	Stable	FREE
999	HyperEVM	HYPE
1030	Conflux eSpace	CFX
1088	Metis Andromeda	METIS
1101	Polygon zkEVM	ETH
1111	WEMIX	WEMIX
1116	Core	CORE
1135	Lisk	ETH
1284	Moonbeam	GLMR
1285	Moonriver	MOVR
1300	Glue	GLUE
1329	Sei	SEI
1514	Story	IP
1625	Gravity	G
1868	Soneium	ETH
1890	LightLink	ETH
1923	Swellchain	ETH
2001	Milkomeda C1	milkADA
2020	Ronin	RON
2040	Vanar	VANRY
2222	Kava	KAVA
2345	Goat	BTC
2741	Abstract	ETH

Chain ID	Network name	Native currency
2818	Morph	ETH
3338	Peaq	PEAQ
3637	Botanix	BTC
4162	SX Rollup	SX
4200	Merlin Chain	BTC
4689	IoTeX	IOTX
5000	Mantle	MNT
5031	Somnia	STT
5330	Superseed	ETH
5464	Saga	SAGA
5545	DuckChain	TON
6900	Nibiru	NIBI
7000	ZetaChain	ZETA
7560	Cyber	ETH
7700	Canto	CANTO
8217	Kaia	KAIA
8453	Base	ETH
8822	IOTA EVM	IOTA
9001	Evmos	EVMOS
9745	Plasma	FSN
10000	SmartBCH	BCH
11501	BEVM	BTC
13371	Immutable zkEVM	IMX
16661	0G	A0GI
22776	Map Protocol	MAPO
23294	Oasis Sapphire	ROSE
31612	Mezo	BTC
33139	ApeChain	APE
34443	Mode	ETH
39797	Energi	NRG

Chain ID	Network name	Native currency
41923	EDU Chain	EDU
42161	Arbitrum One	ETH
42170	Arbitrum Nova	ETH
42220	Celo	CELO
42793	Etherlink	XTZ
43111	Hemi	ETH
43114	Avalanche C-Chain	AVAX
48900	Zircuit	ETH
50104	Sophon	SOPH
55244	Superposition	ETH
57073	Ink	ETH
59144	Linea	ETH
68414	Henesys	HNS
80094	Berachain	BERA
81457	Blast	ETH
83872	Zedxion	ZEDX
98866	Plume	ETH
167000	Taiko	ETH
200901	Bitlayer	BTC
534352	Scroll	ETH
747474	Katana	ETH
1440000	XRPL EVM	XRP
7777777	Zora	ETH
21000000	Corn	BTCN
245022934	Neon EVM	NEON
666666666	Degen	DEGEN
888888888	Ancient8	ETH
1313161554	Aurora	ETH
1380012617	Rari Chain	ETH
1666600000	Harmony	ONE

Chain ID	Network name	Native currency
2046399126	SKALE Europa	sFUEL

EVM testnets (86 chains)

Chain ID	Network name	Native currency
16	Songbird Coston	CFLR
31	Rootstock Testnet	tRBTC
41	Telos Testnet	TLOS
51	XDC Apothem	TXDC
65	OKT Chain Testnet	OKT
71	Conflux eSpace Testnet	CFX
83	Meter Testnet	MTR
89	Viction Testnet	VIC
97	BNB Testnet	tBNB
114	Flare Coston2	C2FLR
123	Fuse Sparknet	SPARK
133	HashKey Testnet	HSK
195	X Layer Testnet	OKB
256	Huobi ECO Testnet	HT
282	Cronos zkEVM Testnet	zkTCRO
296	Hedera Testnet	HBAR
300	zkSync Sepolia	ETH
338	Cronos Testnet	TCRO
545	Flow EVM Testnet	FLOW
919	Mode Sepolia	ETH
943	PulseChain Testnet	tPLS
1001	Kaia Kairos	KAIA
1029	BitTorrent Donau	BTT
1075	IOTA EVM Testnet	IOTA
1112	WEMIX Testnet	tWEMIX
1115	Core Testnet	tCORE

Chain ID	Network name	Native currency
1287	Moonbase Alpha	DEV
1301	Unichain Sepolia	ETH
1513	Story Aeneid	IP
1687	Mint Sepolia	ETH
1891	LightLink Pegasus	ETH
1946	Soneium Minato	ETH
2021	Ronin Saigon	RON
2221	Kava Testnet	TKAVA
2358	Kroma Sepolia	ETH
2442	Polygon zkEVM Cardona	ETH
2522	Fraxtal Testnet	frxETH
2810	Morph Holesky	ETH
4002	Fantom Testnet	FTM
4202	Lisk Sepolia	ETH
4690	IoTeX Testnet	IOTX
4801	World Chain Sepolia	ETH
5003	Mantle Sepolia	MNT
5611	opBNB Testnet	tBNB
7001	ZetaChain Athens	aZETA
7701	Canto Testnet	CANTO
9000	Evmos Testnet	tEVMOS
10001	SmartBCH Testnet	BCHT
10200	Gnosis Chiado	XDAI
11124	Abstract Testnet	ETH
11155111	Ethereum Sepolia	ETH
11155420	Optimism Sepolia	ETH
11503	BEVM Testnet	BTC
13473	Immutable zkEVM Testnet	tIMX
13505	Gravity Sepolia	G
17000	Ethereum Holesky	ETH

Chain ID	Network name	Native currency
23295	Oasis Sapphire Testnet	TEST
28882	Boba Sepolia	ETH
33111	ApeChain Curtis	APE
37111	Lens Sepolia	GHO
43113	Avalanche Fuji	AVAX
44787	Celo Alfajores	CELO
48899	Zircuit Testnet	ETH
49797	Energi Testnet	tNRG
57054	Sonic Blaze	S
59141	Linea Sepolia	ETH
59902	Metis Sepolia	tMETIS
80002	Polygon Amoy	POL
80084	Berachain Bartio	BERA
84532	Base Sepolia	ETH
98864	Plume Testnet	ETH
128123	Etherlink Testnet	XTZ
167009	Taiko Hekla	ETH
168587773	Blast Sepolia	ETH
200810	Bitlayer Testnet	BTC
421614	Arbitrum Sepolia	ETH
534351	Scroll Sepolia	ETH
686868	Merlin Testnet	BTC
743111	Hemi Sepolia	ETH
763373	Ink Sepolia	ETH
999999999	Zora Sepolia	ETH
1440002	XRPL EVM Devnet	XRP
1666700000	Harmony Testnet	ONE
3441006	Manta Pacific Sepolia	ETH
245022926	Neon EVM Devnet	NEON
1313161555	Aurora Testnet	ETH

15.8 Built-in ERC-20 tokens

Openloop supports **every ERC-20 token**. The summary below covers the built-in tokens (2,599 entries) whose names and symbols are displayed on the device screen.

Note: ERC-20 tokens not in this list can still be used. In that case the contract address is displayed instead of a token name.

Token data source

- **Source**: the CoinGecko API (top 1000 by market capitalization)
- **Multi-chain deployments**: where the same token is deployed on several chains, each deployment is registered as its own entry
- **Decimals verified**: decimals were verified against Uniswap/1inch/CoinGecko for 99.6% of tokens

Tokens by category

Category	Tokens (approx.)	Representative tokens
Stablecoins	180+	USDT, USDC, DAI, FRAX, TUSD, BUSD, USDD, PYUSD
DeFi protocols	450+	UNI, AAVE, COMP, MKR, CRV, SUSHI, YFI, SNX
Layer 2 tokens	200+	ARB, OP, POL, IMX, LRC, METIS, BOBA
Meme tokens	150+	DOGE, SHIB, PEPE, FLOKI, BONK, WIF, BRETT
Gaming/NFT	180+	AXS, SAND, MANA, ENJ, GALA, APE, ILV, MAGIC
Infrastructure	250+	LINK, GRT, FIL, RNDR, OCEAN, ANKR, LPT
Wrapped tokens	120+	WETH, WBTC, stETH, rETH, cbETH, wstETH
Exchange tokens	80+	BNB, OKB, CRO, KCS, GT, HT
DAO/governance	100+	ENS, APE, LDO, RPL, CVX, AURA
Other	877+	Various project tokens

The per-category counts are rough approximations. Category is not stored in the token data, so the total does not match the number of registered entries (2,599).

Token deployments on major chains

Chain	Chain ID	Tokens
Ethereum	1	642
BNB Smart Chain	56	387
Base	8453	240
Arbitrum One	42161	181
Polygon	137	122
Avalanche C-Chain	43114	92
Optimism	10	80
Other 119 chains	-	855
Total	-	**2,599**

The token record

Each token entry contains the following:

Field	Description	Example
chain_id	The chain the token is deployed on	1 (Ethereum)
address	The contract address (20 bytes)	0xdAC17F958D2ee523a2206206994597C13D831ec7
symbol	The token symbol	USDT
decimals	The number of decimal places	6
name	The token name	Tether USD

Cautions

1. **Watch for duplicate symbols**: the same symbol on a different chain is a different contract
2. **Verify the official address**: always check the official contract address before sending
3. **Beware of scam tokens**: scam tokens imitating well-known ones exist
4. **Check the network**: always select the correct network when sending

Closing

Thank you for choosing the Openloop hardware wallet.

We hope this manual helps you manage your crypto assets safely and comfortably.

Three things to remember:

1. ★ **Guard your recovery phrase carefully**
2. Practise on testnet before using mainnet
3. When something is unclear, check the manual

Enjoy managing your crypto assets safely.

Haudi Crypto, Inc. — Openloop development team Version 1.1.1 | 2026-08-13
