

[Open in app](#)[Get started](#)

Published in ShiftCrypto



Stadicus

[Follow](#)

Jul 9, 2020 · 8 min read · [Listen](#)

# Use the BitBox02 with Electrum wallet

## BitBox02 ❤️ Electrum: part 1

This is the start of our Electrum article series. In this post we explain how to use the Electrum wallet together with your [BitBox02](#) hardware wallet. It is written for advanced users, so we go a bit more into details.



**Part 1: Use the BitBox02 with Electrum wallet**

Part 2: Advanced Electrum features

Part 3: BitBox02 multisignature wallet

Part 4: Multi-vendor multisig with BitBox02 and Electrum (coming soon)

## Electrum



[Open in app](#)[Get started](#)

*Note: Electrum wallet is a third-party application. We don't have control over the development and distribution of the software and can't provide any guarantees.*

## **Install**

To get the latest release of Electrum, download and install it from the official website <https://www.electrum.org>. Double-check the domain name to avoid installing malware. If you want to be sure that you got an official release, follow the instructions to verify the GPG signatures.

## **Choose your server wisely**

When first starting Electrum, you need to choose the server to connect to. You can either select “Auto connect” and use a random server, or manually select a server. Before going further, let's quickly examine what Electrum servers are.

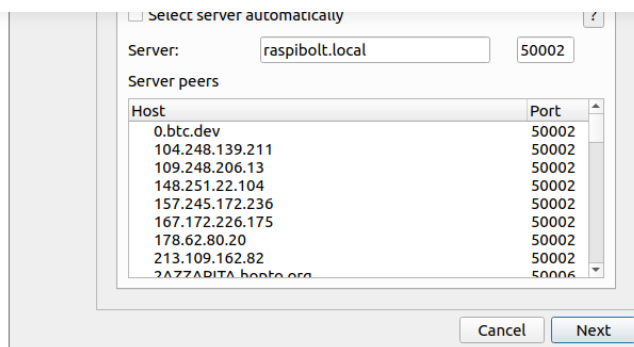
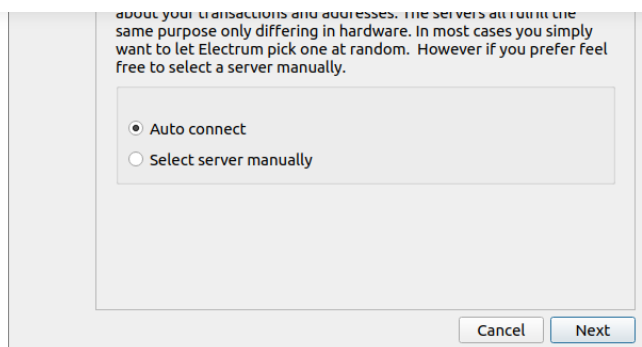
Electrum does not communicate with the Bitcoin network directly. Instead, it relies on Electrum servers that are indexing the Bitcoin blockchain and provide all relevant information — like transaction details, address balances or fee estimates — to the Electrum wallet.

You need to trust the server you use to a certain extent. It learns about your total Bitcoin holdings and past transactions, and can cluster all your various Bitcoin addresses. It is safe to assume that blockchain analytics companies run Electrum servers to gather information about Bitcoin transactions and address clusters.

This is why we strongly recommend to only use Electrum connected to a server you know and trust. The best way to achieve this is to run your own server, either locally with [Electrum Personal Server](#) if you already run Bitcoin Core on your computer, as a DIY solution like the [RaspiBolt](#) on a Raspberry Pi, or using a commercially available Bitcoin node.

If you choose manual server selection, provide your connection data on the next screen.



[Open in app](#)[Get started](#)

## Electrum & your BitBox02

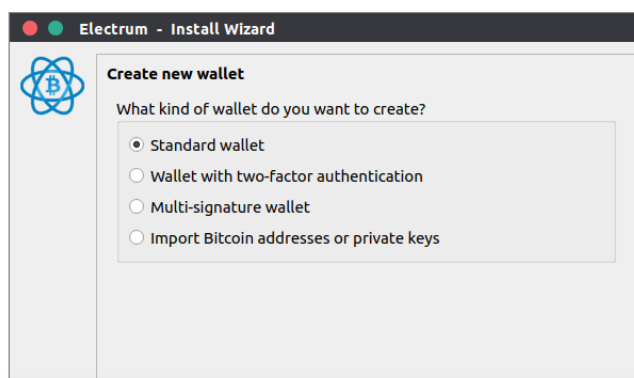
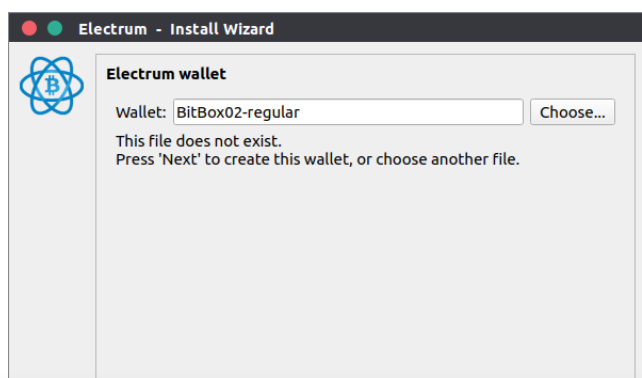
Storing private keys on a regular computer is not very secure. This is why it makes sense to use Electrum in combination with a hardware wallet. In this setup, all private keys are managed by the BitBox02, they never touch any networked device and all your receiving addresses and outgoing transactions can be confirmed on the trusted screen of your BitBox02.

The BitBox02 needs to be set up with the BitBoxApp first. Follow the instruction on <https://shiftercrypto.ch/download> to do that.

### Connect your BitBox02 to Electrum

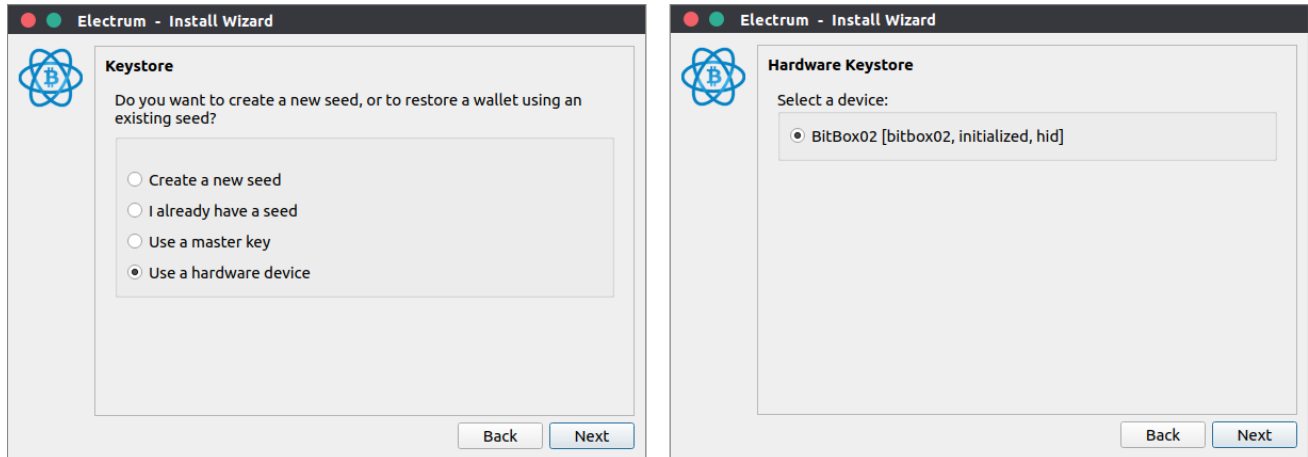
Plug in your BitBox02 and tap the side to choose screen orientation. It now displays “*See the BitBoxApp*”.

Electrum stores information about wallets in individual files. To create a new wallet, select “*File > New/Restore*” in Electrum, enter a descriptive filename and click “*Next*”. On the next screen, choose the wallet type to set up. Select “*Standard wallet*” and click “*Next*”.



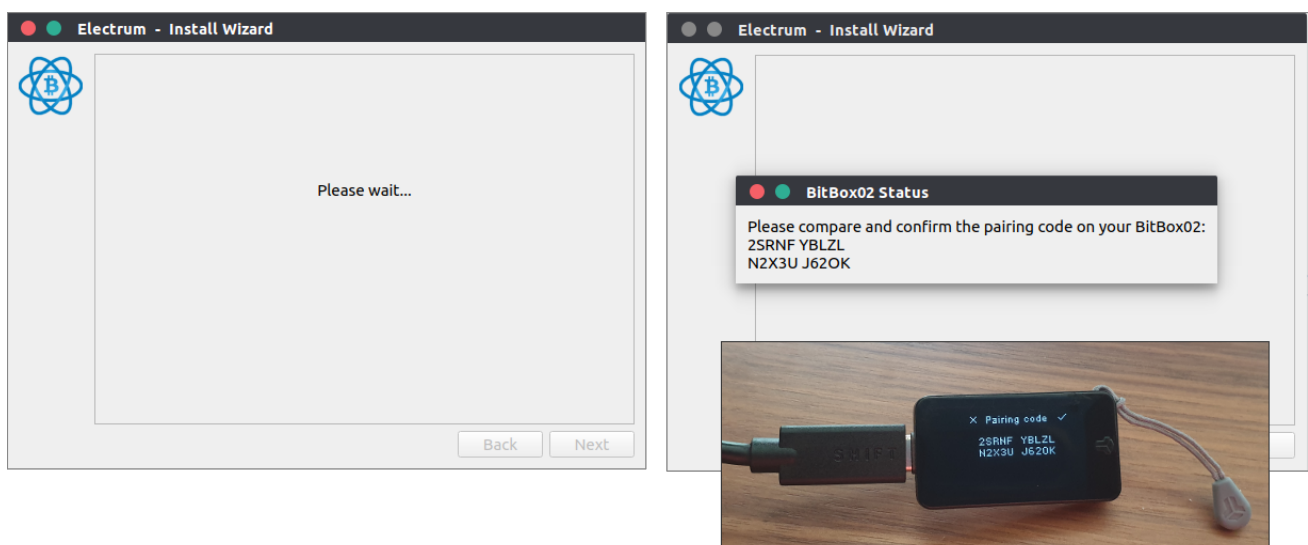
[Open in app](#)[Get started](#)

then click “Next”. Once Electrum detects the BitBox02, it lists it as a Hardware Keystore, which you can confirm by clicking “Next”.



If you run into trouble at this point, it’s probably because the BitBox02 is not connected or blocked by a different application. Make sure the BitBoxApp is not running as well.

Electrum now waits for you to unlock your BitBox02 by entering the device password. Next, if you use the BitBox02 for the first time with Electrum, you’re asked to confirm a pairing code. This enables the secure encryption of all future communication between Electrum and the BitBox02.




If the pairing codes match, confirm on the BitBox02, and then click “Next” in



[Open in app](#)[Get started](#)

complex screen during the whole wallet creation process.

**Electrum - Install Wizard**



**Script type and Derivation path**

Choose the type of addresses in your wallet.

☐ legacy (p2pkh)

☐ p2sh-segwit (p2wpkh-p2sh)

☒ native segwit (p2wpkh)

You can override the suggested derivation path. If you are not sure what this is, leave this field unchanged.

[Back](#) [Next](#)

First, choose what type of Bitcoin addresses you want to use:

- **Legacy: not supported**

Legacy Bitcoin addresses starting with 1 are not supported by the BitBox02.

- **p2sh-segwit: backwards-compatible Segwit**

Corresponds to the regular “Bitcoin” account in the BitBoxApp and uses wrapped Segwit addresses (starting with “3”) for backwards compatibility. Helps save on fees, supported by most services. Specified in [BIP 49](#).

- **Native segwit: most efficient Segwit (“bech32”)**

Also called “bech32”, this is the most lean and efficient Segwit implementation with the lowest fees. Addresses start with “bc1”. It’s the future, but not all services support that address format just yet, so older wallets potentially cannot send you bitcoin to this wallet. You can send bitcoin to any address type without



[Open in app](#)[Get started](#)

possible to use your BitBox02 to create additional wallets of a different type later.

See the [Bitcoin Wiki](#) for additional information.

### Wallet derivation path

A derivation path makes it possible to have an organized structure with many different wallet types, accounts and individual addresses all derived from a single secret. The main advantage is that a backup only needs to include the single secret, not every individual account and address. An account corresponds to an independent wallet and can help to keep funds clearly separated.

All wallet types follow a universal derivation path syntax. In Electrum you can define it as follows:

```
m / purpose' / coin_type' / account'
```

These parameters have the following meanings:

- `purpose` : corresponds to the wallet type selected above and corresponds to the respective BIP number
- `coin_type` : defines the currency (e.g. `0` for Bitcoin, `1` for Testnet)
- `account` : number of individual accounts, starting at `0`

The only parameter you may want to change is the `account` number. This way, you can create an unlimited number of wallets, but make sure to use consecutive numbering. Otherwise, they might never be found again. For example, you could use:

- `m/84'/0'/0'` : first account, corresponds to the BitBoxApp “Bitcoin bech32” account (but we don’t recommend using the same account in Electrum and the BitBoxApp)

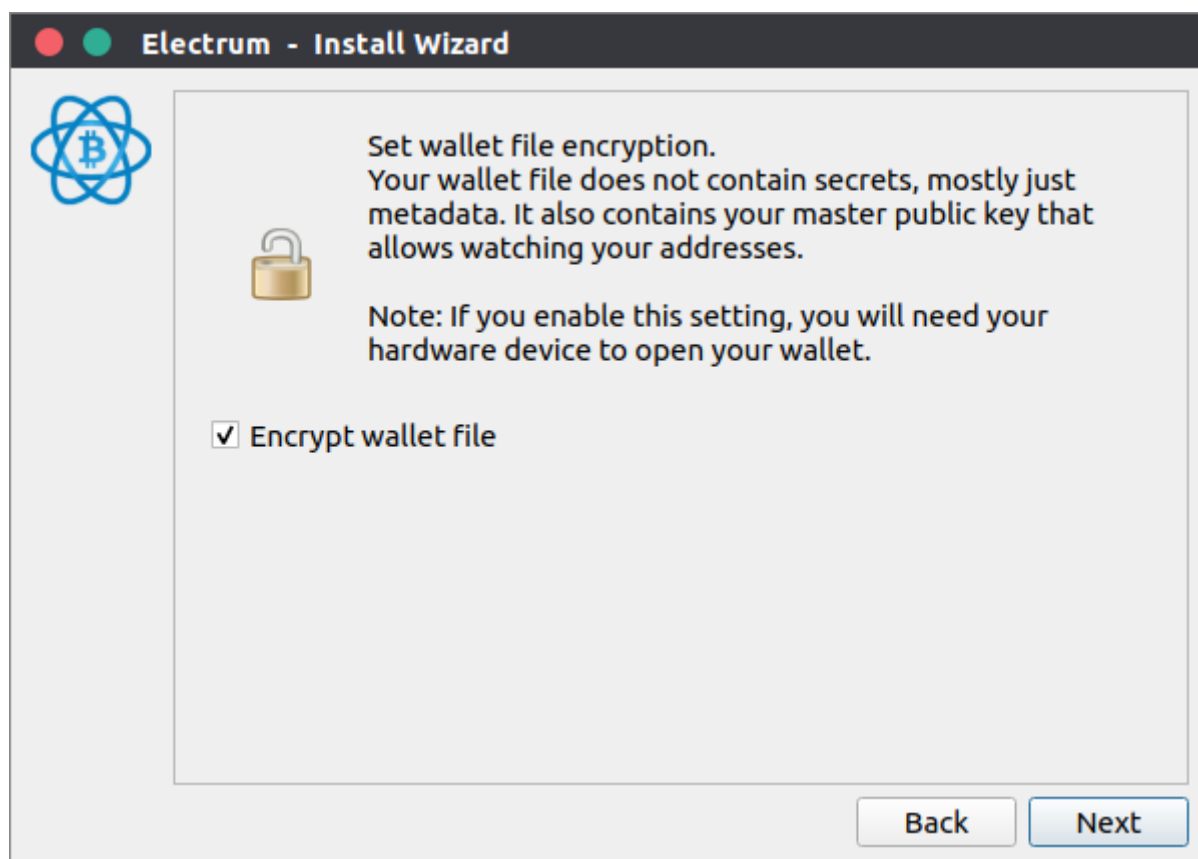


[Open in app](#)[Get started](#)

With wallet type and derivation path set, click “Next”.

### Wallet file encryption

This is the last screen for creating a new Electrum wallet. You’re asked if you want to encrypt the wallet information stored on your computer with your BitBox02.



Electrum does not store secret information, as your private keys never leave the BitBox02. Nonetheless, the public keys and transaction data is private information and you might want to secure that.

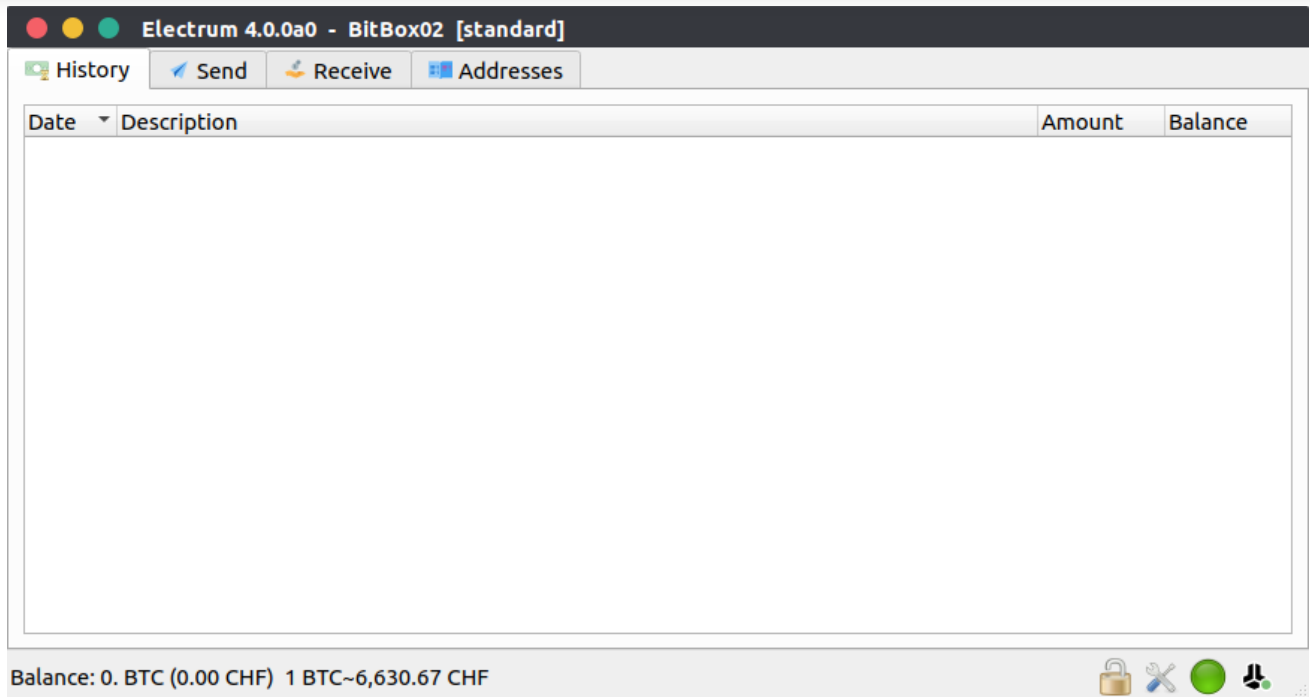
- **Encrypt wallet file**

You need to connect and unlock the BitBox02 every time you open the Electrum wallet, even if you only want to check a past transaction. Good for privacy, can be a bit cumbersome.

- **Don't encrypt wallet file**

You are able to open the Electrum wallet and check your balance and all past

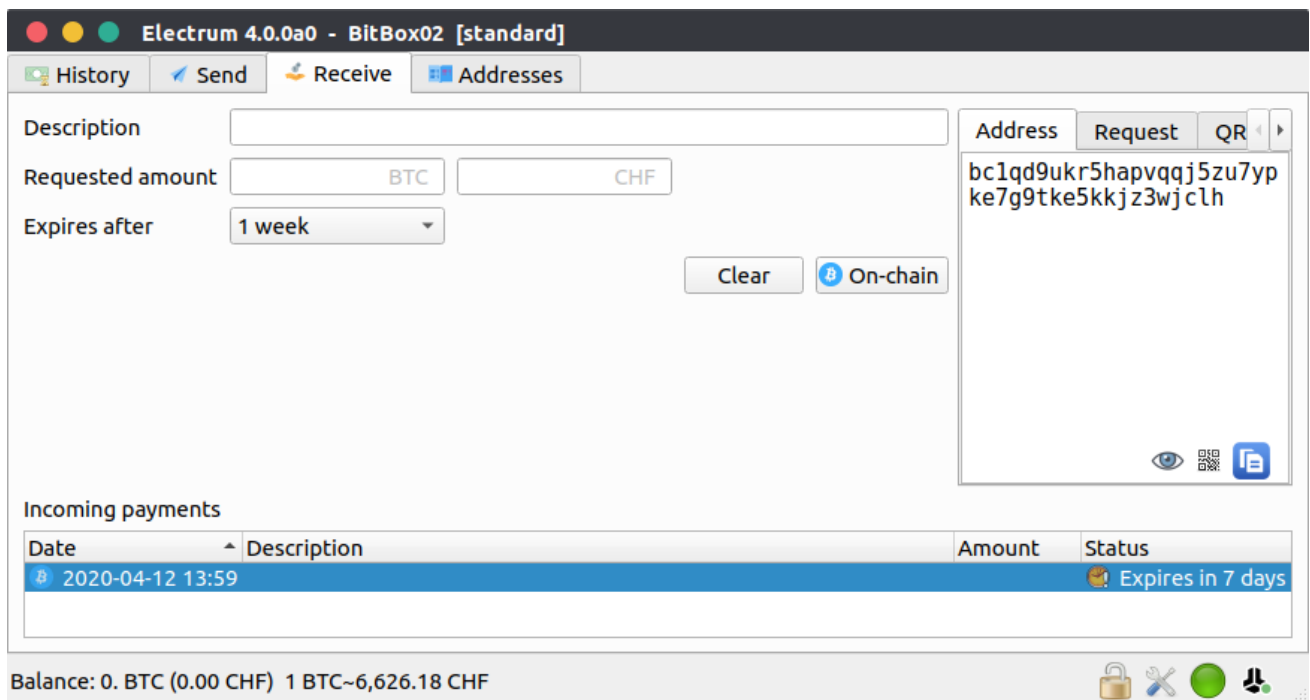


[Open in app](#)[Get started](#)

Congratulations, your new Electrum wallet is now ready to use!

## Receive bitcoin

Now that your Electrum BitBox02 wallet is configured, you're all set up to receive bitcoin. Go to the “*Receive*” tab.






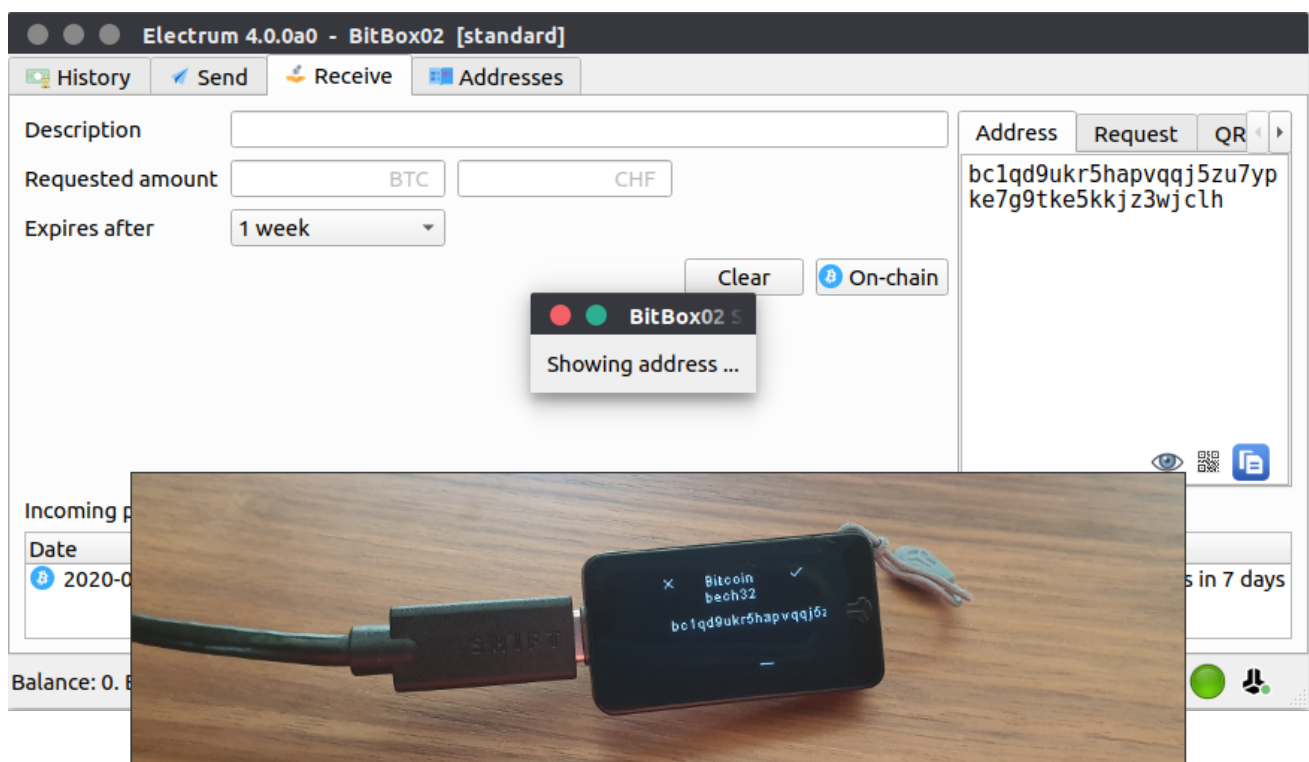
[Open in app](#)[Get started](#)

## Optional features

- set a Description
- enter the requested amount
- set an expiration date
- Click on “On-chain” to create a new Payment Request

You now have a bitcoin: link or a QR code to share with your counterparty that both include the description, amount and expiration date. Of course, you can still use the bare Bitcoin address without all the metadata.

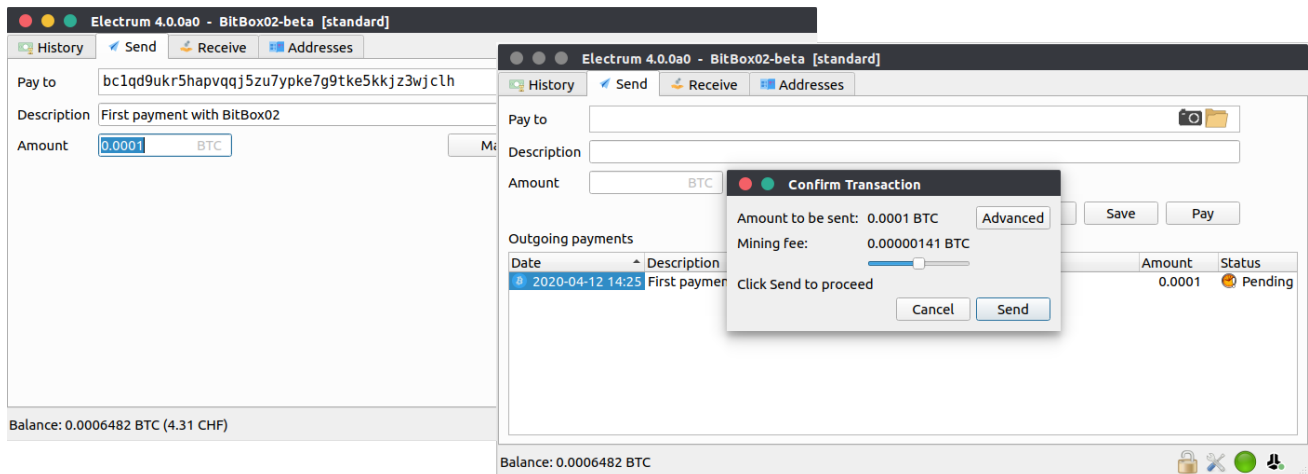
Now it is very important to verify this Bitcoin address on your BitBox02. A computer virus could easily change the receiving address to an address that belongs to an attacker. Check the address on your hardware wallet by clicking on the little eye icon  at the bottom right corner to make sure that the address actually belongs to you .



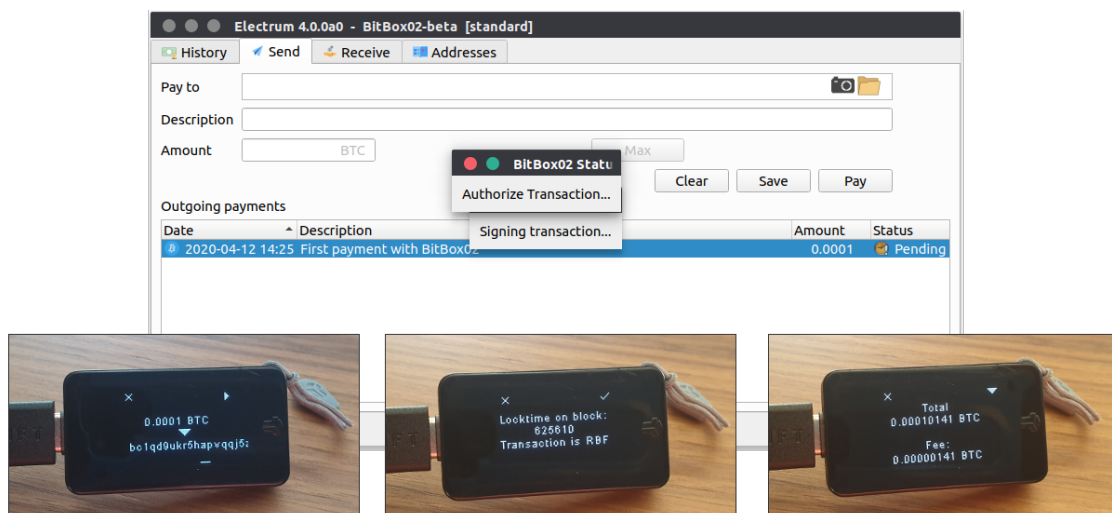
## Send bitcoin

To send some bitcoin, go to the “Send” tab. Enter the receiving address, the amount



[Open in app](#)[Get started](#)

Electrum does not know your private keys. If you now click on “Send”, Electrum creates an unsigned Bitcoin transaction and hands it over to the BitBox02. There, all relevant details are shown on the secure screen and you can verify the recipient’s address, the amount and fee to either approve or decline the transaction.



If you approve, the BitBox02 signs the transaction and hands it back to Electrum, which broadcasts it to the network. In that process, your private keys never leave the BitBox02.

## Next: advanced features

This concludes part 1 of our **BitBox02** ❤️ **Electrum** series. The next blog post covers more advanced Electrum features like pay-to-manv, coin control and replace-by-fee.



[Open in app](#)[Get started](#)

## BitBox02 Bitcoin-only edition

The BitBox02 is available in a Bitcoin-only edition, with radically focused firmware. Less code means less attack surface which further improves your security when only storing Bitcoin.



If you want to use your BitBox02 with Electrum, make sure you have the latest firmware installed. Download it at [shiftcrypto.ch/download](https://shiftcrypto.ch/download).

If you don't own a BitBox02 yet, [get one in our shop!](#)

Shift Crypto is a privately held company based in Zurich, Switzerland. Our international team of specialists across engineering, cryptosecurity and Bitcoin core development build the BitBox products and provide consulting services. The BitBox02, a second generation hardware wallet, equips individuals to easily store, protect, and transact cryptocurrencies. Its companion, the BitBoxApp, provides an all-in-one solution to securely manage your digital assets with ease.

