Electrum

BitBox02: advanced Electrum tricks

BitBox02 ❤ Electrum: part 2

Stadicus
14 Jul 2020 • 7 min read

This is the second article of our Electrum series. In this post we explain how to use advanced Electrum features, best in combination with the BitBox02 hardware wallet. It is written for advanced users, so we go a bit more into details.

> *Part 1: Use BitBox02 with Electrum wallet*
>
> ***Part 2: Advanced Electrum features***

> *Part 3: BitBox02 multisignature wallet*

Electrum

The Electrum wallet is a powerful Bitcoin light client for Windows, Mac and Linux. It connects to an Electrum server of your choice and offers many advanced features. It can be used as a pure software wallet, with the private keys stored on your computer, but it also works very well with many leading hardware wallets.

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.

Why use Electrum with your BitBox02?

The Electrum wallet is the de-facto standard for a power-user Bitcoin wallet. It works with all possible setups, including hot and cold wallets, and hardware wallets from many manufacturers. The user interface is more functional than beautiful, but that's probably the price for such a rich feature-set.

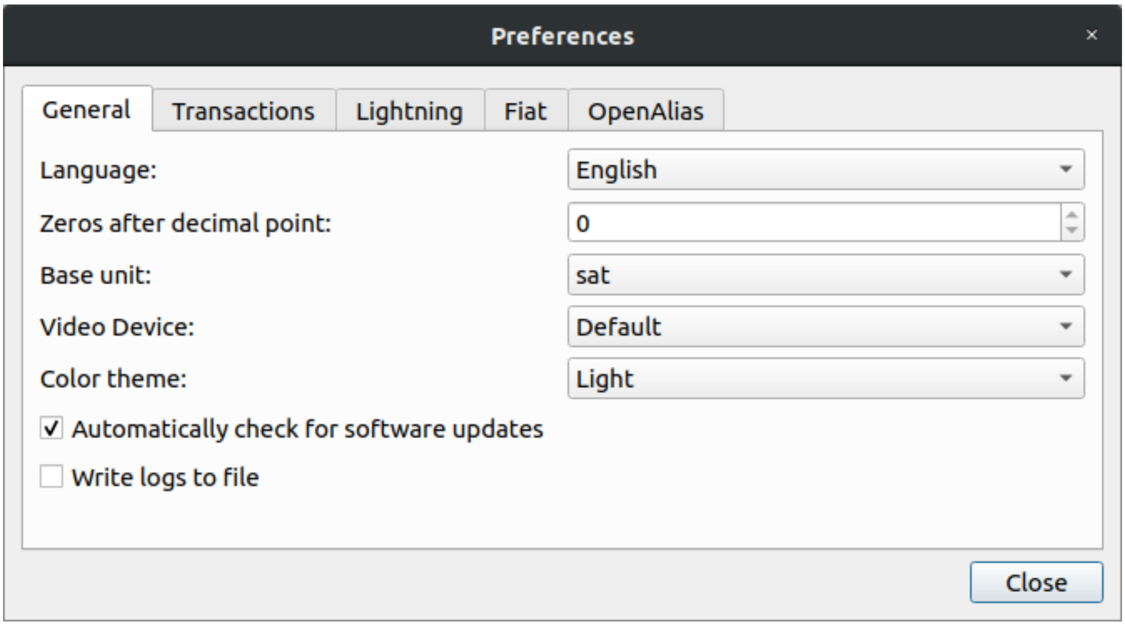
With the BitBoxApp, we strive to create a simple, minimalistic Bitcoin wallet for desktop and mobile platforms. While it provides advanced features like coin control or connectivity to your own Bitcoin full node, it will probably never cover all features of Electrum. This is why interoperability with Electrum is very important to us. If you need advanced features that are not offered by the BitBoxApp, the Electrum wallet is your friend.

In the first part of this series, we covered how to install Electrum and use it with our BitBox02 hardware wallet. It also explains how to simply send and receive Bitcoin.

Let’s dive into some advanced options.

Settings

Customize Electrum to your needs and get the most out of it by selecting the menu item “*Tools / Preferences*”.



Language: English

Zeros after decimal point: 0

Base unit: sat

Video Device: Default

Color theme: Light

☑ Automatically check for software updates

□ Write logs to file

Besides the obvious settings, the most used features include:

General tab

- Base unit: select your Bitcoin unit, e.g. `BTC` or `sat`
- Video device: allows to scan QR codes via webcam
- You can select “Dark Mode” ?

Transaction

- Use Replace-by-fee: enabled by default, see section below

Fiat

- Fiat currency: select your reference fiat currency
- Show history rates: shows the historic fiat value of past

transactions

Addresses

To get an overview over addresses controlled by your wallet, you can display a separate Addresses tab in the menu with "*View / Show Addresses*".

This separate tab shows your addresses, both used and unused, for receiving payments and change from your own transactions. Using the context menu you can show additional details for each address, or freeze individual addresses so that they are not spent when creating new Bitcoin transactions.

Pay to many

When using Bitcoin regularly, there are situations where you want to make several payments at the same time. This helps automate mass payments, save on fees and blockspace.

If you enable *"Tools / Pay to many"* in the menu, the *"Pay to"* field in the Send tab changes into a multi-line textbox. Now you're able to enter multiple receiving addresses and a corresponding value on separate lines, like this:

```
tb1q8tlfylnvwr4sd2k0xp7urkqxavrd0gv77lnq6w, 0.0004
tb1qk9222ky3pf0jgxh7p45zdnmacgk0gfw4hpf7zk, 0.0001
tb1q78xuwudps736p9zztry9jyfmr6lkmnd0m76at4, 0.0007
```

Using the file icon, you can also load a text file of the same content, even without activating the feature beforehand.

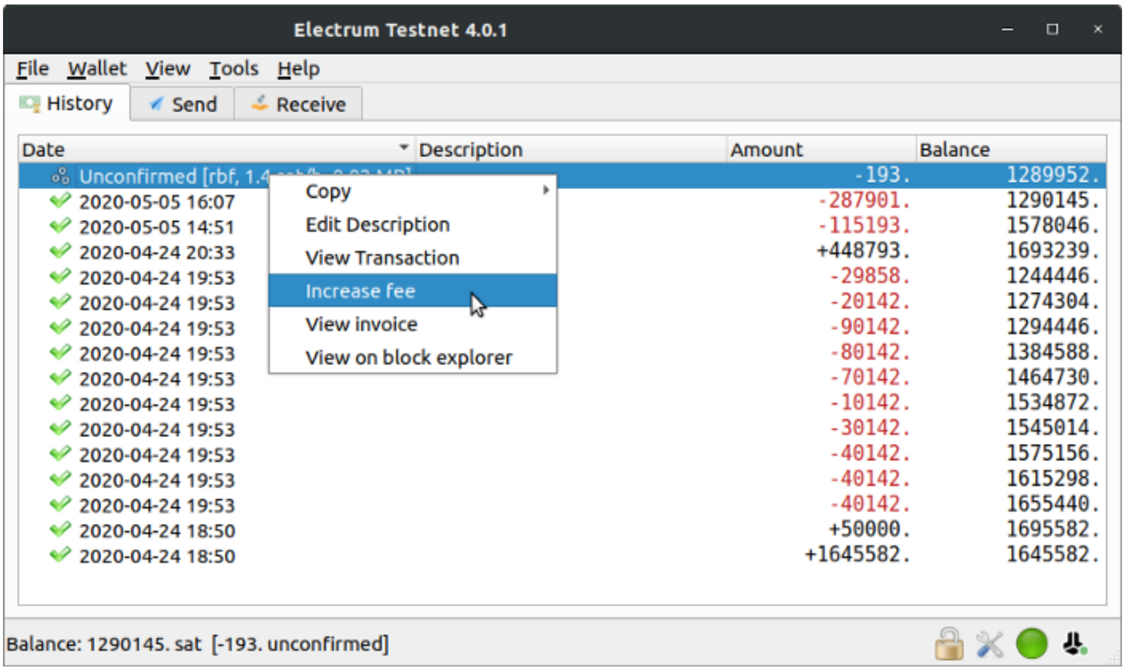
Replace-by-fee

Finding the right fee for a transaction can be tricky. Replace

Finding the right fee for a transaction can be tricky. Replace-by-fee (RBF) helps by explicitly marking transactions as replaceable, so you can start with a low fee and — for example if the mempool suddenly fills up — replace it later with a higher fee if necessary.

This setting is enabled by default and can be configured by selecting the menu item *“Tools / Preferences / Fees”*.

As long as they are unconfirmed, RBF transactions are listed with `[rbf, 1. sat/b]` in the History tab. Use the context menu (right mouse-click) to select *“Increase fee”*, update the fee and rebroadcast the transaction.



Date	Description	Amount	Balance
Unconfirmed [rbf, 1.4		-193.	1289952.
2020-05-05 16:07		-287901.	1290145.
2020-05-05 14:51		-115193.	1578046.
2020-04-24 20:33		+448793.	1693239.
2020-04-24 19:53		-29858.	1244446.
2020-04-24 19:53		-20142.	1274304.
2020-04-24 19:53		-90142.	1294446.
2020-04-24 19:53		-80142.	1384588.
2020-04-24 19:53		-70142.	1464730.
2020-04-24 19:53		-10142.	1534872.
2020-04-24 19:53		-30142.	1545014.
2020-04-24 19:53		-40142.	1575156.
2020-04-24 19:53		-40142.	1615298.
2020-04-24 19:53		-40142.	1655440.
2020-04-24 18:50		+50000.	1695582.
2020-04-24 18:50		+1645582.	1645582.

Balance: 1290145. sat [-193. unconfirmed]

Another interesting option is *“Batch RBF transaction”*, which can be enabled in *“Tools / Preferences”* as well. This feature automatically combines outgoing RBF transactions. If you create a new RBF transaction, while there is still at least one unconfirmed transaction present, Electrum is able to replace the latter with an updated batch transaction containing both. So even if you’re not planning on sending multiple transactions, you might still be able to batch them and save on fees and blockspace.

Coin control

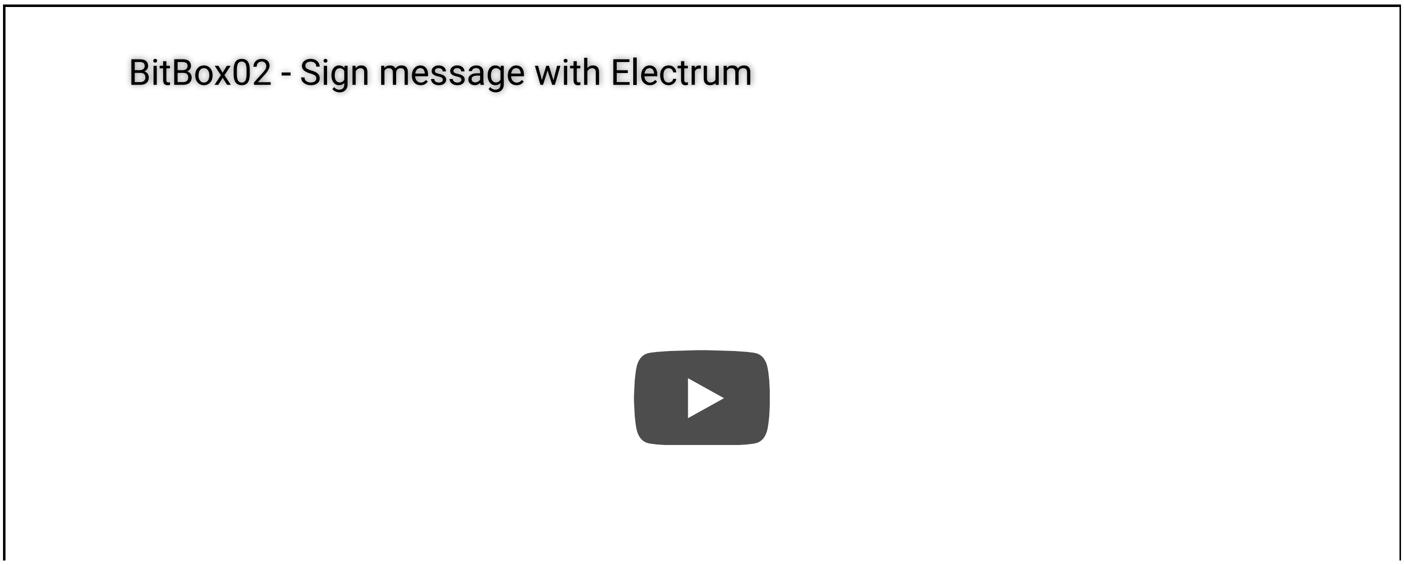
Performing some extra steps like CoinJoins to preserve your financial privacy? Or do you want to make sure not to mix coins (UTXO) of different sources when sending funds to a recipient? To gain such fine control, you need to manage the coins in your wallet.

With *“View / Show Coins”* you can display the *“Coins”* tab and see all coins that in sum make up your wallet balance. With the context menu, you can spend a coin directly, see additional information, or also freeze it so that it will no longer be considered for spending.

Sign messages

With Electrum, you can prove that you are in full control of a bitcoin address by signing an arbitrary text message with the private key of that specific address. This can be used for various reasons, one being for regulatory reasons.

For instance, the Swiss exchange Bity uses this to allow their customers to buy and withdraw up to 5000 Swiss Francs (~5000 USD) of cryptocurrencies without any KYC requirements.

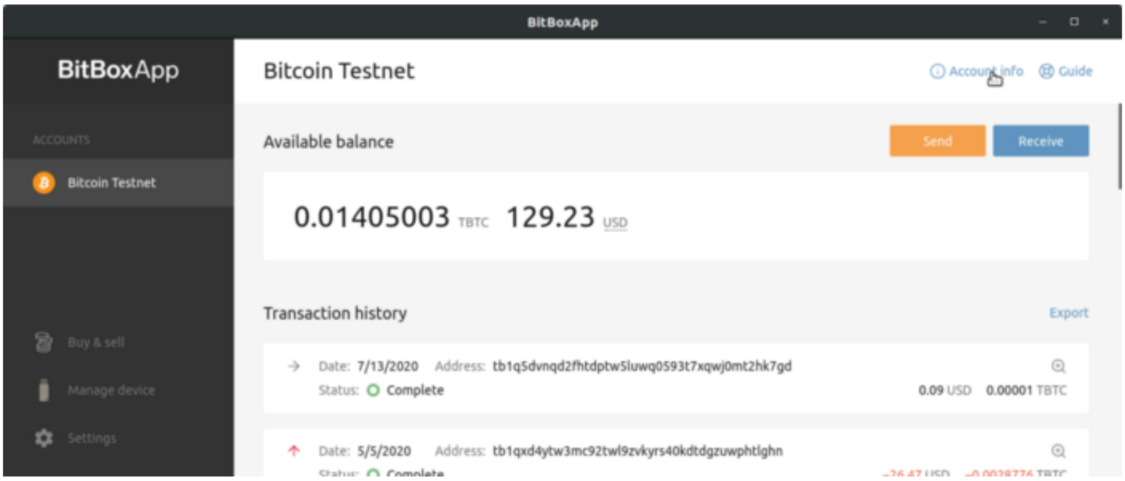


You find this feature in "Tools / Sign/verify message", and it's quite self-explanatory.

Watch-only wallets

You can use Electrum to watch a wallet without knowing the private key. For that you need the extended public key (xpub), which contains all necessary information to watch past and future transactions and create new addresses. It does not contain any private keys, so you cannot spend any of these funds.

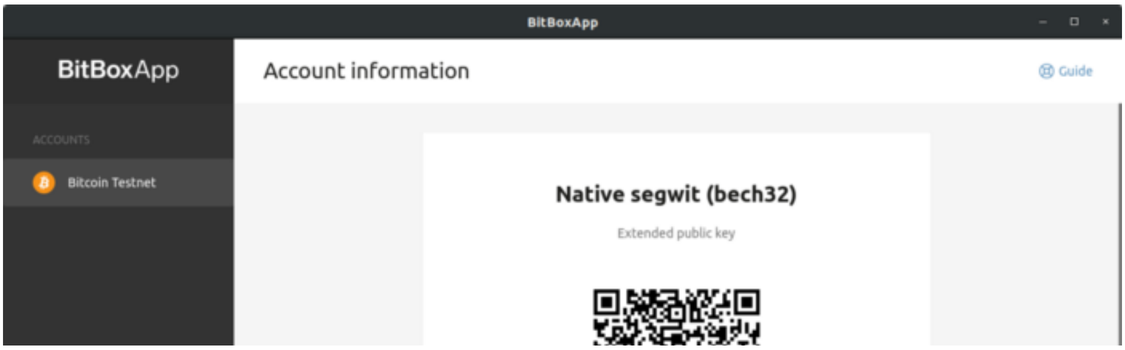
Most wallets allow you to export the xpub. In the BitBoxApp, for example, you can display the extended public key for every account by clicking on “Account info” at the top.

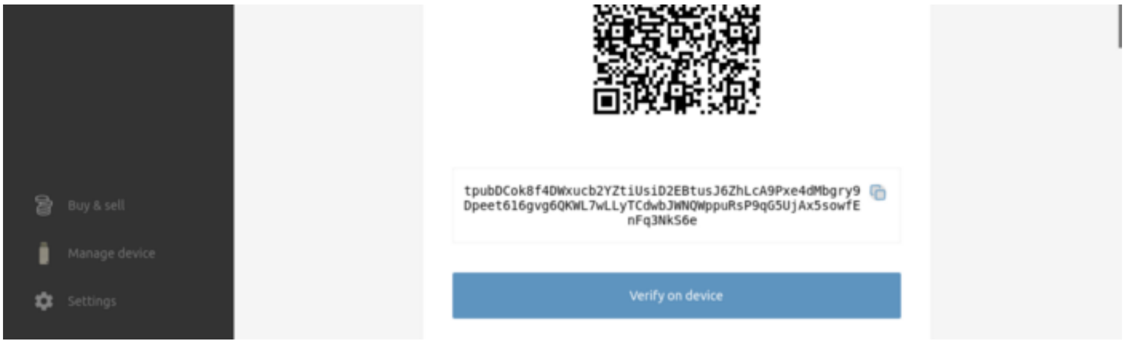


0.01405003 TBTC 129.23 USD

Date: 7/13/2020 Address: tb1q5dvnqd2fhtdptw5luwq0593t7xqwj0mt2hk7gd
Status: Complete 0.09 USD 0.00001 TBTC

Date: 5/5/2020 Address: tb1qxd4ytw3mc92twl9zvkyrs40kdtdgzuwphtlghn
Status: Complete -26.47 USD -0.0028776 TBTC





tpubDCok8f4DWxucb2YZtiUsiD2EBtusJ6ZhLcA9Pxe4dMbgry9Dpeet616gvg6QKWL7wLLyTCdwbJWNQWppuRsP9qG5UjAx5sowfEnFq3NkS6e

To create an Electrum watch-only wallet, create a new wallet with the menu item *“File / New/Restore”*, select *“Standard wallet”* and *“Use a master key”*. Paste your xpub into the text field (or load if from file or via QR code with your webcam) and choose whether to password-protect it for added privacy.

Now you have an (almost) regular Electrum wallet, it just says `[watching only]` in the title bar. This can be useful to create new receiving addresses, without having the private keys present. Just be aware that if you don’t verify your receiving address on the secure screen of a second device like the BitBox02, malware on your computer could potentially trick you into giving out addresses that don’t belong to you, but are under the control of an attacker. Never use this method for significant amounts.

Should you want to export your xpub from Electrum into another software wallet that supports watch-only wallets, you can easily do that by navigating into the menu item *“Wallet / Information”* and exporting your *“Master Public Key”* as text or as a QR code.

Sweep a Paper Wallet

Still have an old paper wallet lying around? Be careful when spending these funds: you need to create a transaction that spends the whole amount, otherwise it might be hard to recover your change.

Electrum lets you safely sweep a paper wallet with the menu item *“Wallet / Private keys / Sweep”*. Copy the private keys into the text box and Electrum will automatically create a transaction that sends all funds into your current wallet.

Please be aware that this is a “hot wallet” operation and the private keys of your paper wallet are exposed on your computer, even if for only a brief moment. Don’t use this method for large sums without additional precautions.

Tor

As outlined in part 1 of our series, you should be careful what Electrum server to choose. Whether you use a random server, or your own, Tor as an anonymity networking layer can help in both cases:

- Public Electrum server: Although the Electrum server learns about your Bitcoin holdings and past transactions, Tor helps hide your real IP address and geographical location.
- Your own Electrum server: Tor allows you to access your Electrum server without much network configuration. This is especially helpful if your node runs in a home network and is not reachable from the outside.

To use Electrum with Tor, install either the Tor Browser from the official website https://www.torproject.org. Follow the steps outlined in the download section.

In Electrum, click on the menu item *“Tools / Network”* (or click on the green LED button in the bottom right corner) and go to the *“Proxy”* tab. Select *“Use Tor proxy at port 9050”*. You can now either continue using a regular public server, or configure a Tor `.onion` address in the *“Server”* tab.

The previously green LED should now switch to blue to indicate that you’re connected over the Tor network.

Next: BitBox02 multisig with Electrum

This concludes part 2 of our BitBox02 ❤️ Electrum series. The next blog post covers how to use BitBox02 multi-signature in Electrum.

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.

If you don’t own a BitBox02 yet, get one in our shop!