

# **Digital BitBox**

## User Guide

**Desktop App v2.2.2**

**Mar. 2018**

## Table of Contents

1. Introduction .....	3
2. What's inside the package? .....	3
3. Inserting the micro SD card.....	3
4. Download and install the desktop app .....	4
5. Setting up your BitBox .....	5
5.1 Best practice for wallet name .....	5
5.2 Entering a password.....	5
6. Changing your password .....	6
7. Desktop app tabs .....	6
7.1 History tab.....	6
7.2 Receive tab.....	7
7.3 Send Tab.....	8
8. Create and switching between wallets.....	10
9. Creating a hidden wallet .....	10
10. Options tab .....	11
11. Multisig tab.....	12
12. Second Factor Authentication .....	13
13. Restoring a wallet from backup .....	13
14. Using an Ether wallet.....	15
15. Sending ERC20 tokens .....	17
16. Using an Ethereum Classic Wallet .....	18
17. Upgrading the BitBox firmware.....	19
18. FAQs .....	20
19. Additional help.....	22
20. Revision History .....	22

## 1. Introduction

Thank you for purchasing the Digital BitBox (“BitBox”). Designed and produced in Switzerland, your BitBox hardware wallet gives you the highest level of security for your cryptocurrencies in a compact, discrete and robust design. The BitBox is the most secure way to manage your cryptocurrencies because your private keys that unlock access to your coins and transaction history **are not accessible via the internet or external devices**: they **NEVER** leave the BitBox (“cold storage”, the equivalent of an electronic vault). This is not the case with software wallets or cryptocurrency exchanges where the exchange **and not you** are in control of your private keys.

The BitBox supports Bitcoin, Ether (ETH, ETC and ERC20 tokens via [myetherwallet.com](http://myetherwallet.com)) and Litecoin (via [electrum-ltc.org](http://electrum-ltc.org)). More coins are continuously added, check the [Shift website](#) for the latest firmware and information about coin support. Note that the first part of this guide describes the BitBox used as a Bitcoin wallet. For Ethereum (ETH), Ethereum Classic (ETC) and ERC20 tokens, first setup a wallet using the BitBox desktop app. Then refer to the “Using an Ether Wallet” section of this guide.

Initializing your BitBox automatically creates a backup of the wallet on the micro SD card. Be sure to remember the password! Without it, your funds are permanently lost. Once initialized, the micro SD card should then be stored separately in a secure location away from the BitBox. Should you lose or damage your BitBox, your wallet can be recovered, including access to all funds and transactions, from the micro SD backup card in combination with the password. Note that if your micro SD backup card is stolen, it does not contain sufficient information for an attacker to recover your wallet or access your funds. This is a **major differentiator** from other hardware wallets which require you to write down a passphrase when setting up the device – this passphrase can be stolen, photographed or copied giving an attacker full access to your funds.

You can view a tutorial video [here](#).

A third party video tutorial can be viewed [here](#) and [here](#).

## 2. What’s inside the package?

The package delivered to you from Shift Cryptosecurity contains two electronic components:

- The BitBox hardware cryptocurrency wallet with USB-A, Micro SD interfaces and built-in touch-sensitive LED.
- Micro SD backup card

## 3. Inserting the micro SD card

The first step is to insert the micro SD card into the BitBox. The devices should be orientated according to this picture:



Figure 1: BitBox with backup Micro SD card inserted

When properly inserted, the text on the Micro SD card will be facing towards you, with the USB pads / beveled side of the BitBox also facing up and towards you. The plug fits into any standard USB-A socket. The LED will flash if the BitBox was inserted in the correct orientation.

#### 4. Download and install the desktop app

Download, install and run the desktop app from this location [digitalbitbox.com/start](https://digitalbitbox.com/start)

STEP 1: DOWNLOAD, INSTALL AND RUN THE LATEST DESKTOP APP



Figure 2: Supported operating systems

For the desktop app, Windows, Mac and Linux platforms are supported. The software version number is indicated in the download button. For second-factor authentication of crypto-currency transactions via smartphone, Android and iOS are supported.

Advanced tip: the sha256sum hash is also provided for verification purposes.

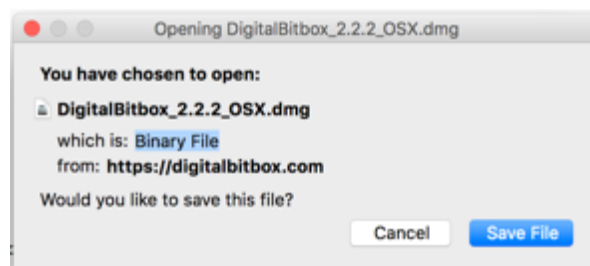
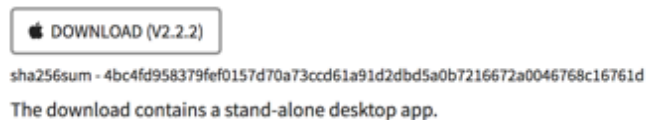


Figure 3: Desktop App Download Dialogue (for Mac)

Save the file and run it (example for Mac shown above). Once installed, start the desktop app by clicking on the icon.



Figure 4: Desktop App Icon

## 5. Setting up your BitBox

The first step is to give your BitBox wallet a name. For example, you could use your first name and call it “Daves Wallet”. Note that only alphanumeric characters are allowed; (Dave’s wallet is not valid because of the apostrophe).

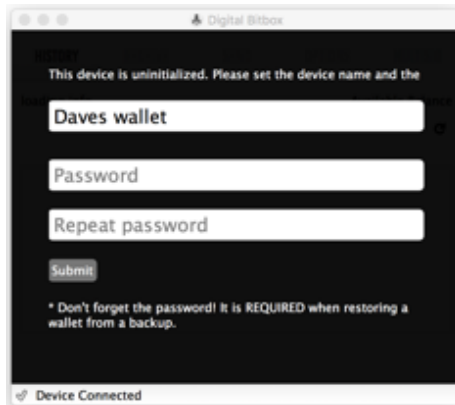


Figure 5: Creating your first wallet (example)

### 5.1 Best practice for wallet name

Your BitBox wallet name is arbitrary and is not used when creating your private key. Because you can create multiple wallets, simply use names which are most convenient, such as “Daves wallet” if your name is Dave, or “Daves business wallet” for a wallet you want to use only for conducting business transactions, etc.

### 5.2 Entering a password

The password you enter is extremely important. It will be cryptographically combined with the seed in order to generate the private keys that store your cryptocurrencies and access your transaction history in the public blockchain. **If you forget your password, you lose everything.** The following recommendation will protect you from typical threats. Please do your own due diligence when selecting a password, especially if you have access to large amounts of cryptocurrency.

Your password should be a combination of complexity and simplicity such that it cannot be guessed, but is easy to remember. A best practice is to use 4 or more random unrelated words. Blank spaces are accepted. For security, try to make the password at least 16 characters long. The password is case-sensitive. For additional security, add numbers and/or punctuation. Do not use familiar words such as family or pet names, or a password you already use for other purposes etc.

gnome asterix! zebra 2sday  
*(example only, please do not use this password!)*

For extreme security, use a random code as your password which you can generate from the random code generator in the desktop app (Options > Get Random Number), or use an open source external password generator application such as [Keepass](#). The disadvantage in this case is that you cannot easily remember the password, and will have to store it separately which introduces a risk.

Note that after 15 incorrect password attempts the BitBox will reset, deleting all stored information. This makes it impossible for anyone to brute force attack your BitBox. Don't worry, your coins and transaction history can be accessed again by recovering from the backup on the micro SD card.

**Do not forget your password as there is no way to recover it.**

## 6. Changing your password

Although you have the option to change your password later (via Options → Change password), this is **not recommended** because in the case you need to restore the wallet from backup, **you MUST remember the original password** you used when first setting up the BitBox. If you think your password has been compromised, it is best practice to create a new wallet (with micro SD card inserted) instead and transfer all funds from the compromised wallet to the new wallet, then delete the compromised wallet.

## 7. Desktop app tabs

There are 5 tabs within the desktop app that give you access to all features of the BitBox.

### 7.1 History tab

This tab displays all incoming and outgoing transactions made to/from your wallet. The arrow pointing to the left ( ← ) means outgoing payments; Bitcoin that you have sent to someone else (or more precisely, to a Bitcoin address). The arrow pointing to the right ( → ) indicates incoming payments; Bitcoin that someone else has sent to you. The transaction amount is shown in the first column, your remaining Bitcoin balance shown under "Available Balance".

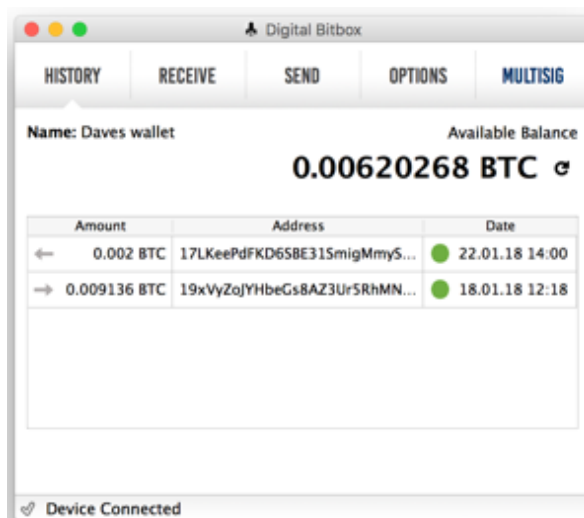


Figure 6 History Tab

For outgoing transactions, the alphanumeric string shown in the Address column is the address your BitBox used to send the Bitcoin from. If you want to keep records of your transactions, you should maintain a record of your "sent-to" addresses together with the persons who you sent Bitcoin to and the purpose for the payment. The same applies to incoming transactions.

For incoming transactions, the address field shows which address received the Bitcoin. For every incoming Bitcoin transaction a different address is used by default, following industry best practices. This makes transactions more private.

Your transaction history and Bitcoin balance are not stored on the BitBox; they are read from the public blockchain using the keys stored on your BitBox.

Advanced tip: double clicking on the address displays the complete information for each transaction within a Block Explorer pop-up window.

The smallest unit of Bitcoin is 0.00000001 Bitcoin, or  $10^{-8}$  Bitcoin (known as “the Satoshi” in honor of the creator of Bitcoin), and is the precision used to denote your balance. Typical Bitcoin transactions are in the range of Millibitcoins.

## 7.2 Receive tab

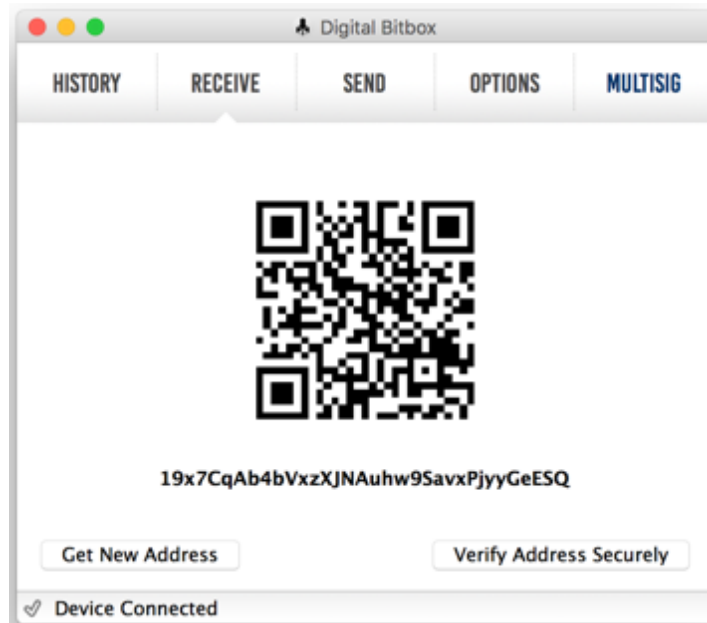


Figure 7 Receive Tab

The purpose of the receive tab is to generate a unique address that is associated with your wallet. Other people may use this address to send you Bitcoin. The address is displayed in two formats, (1) a QR code that can be scanned and (2) a string of text that can be copy-pasted into other Bitcoin applications. The BitBox will automatically generate a new address after a given address receives coins. This is best-practice for optimum privacy – each transaction is then associated with a unique address. Note that there is no security issue if you use the same address multiple times. If you prefer, you may click on “Get New Address” to generate the next new one. The number of possible receive addresses is virtually inexhaustible. All transactions which include receive address information are securely recorded on the Bitcoin network and accessible via your BitBox. Note that your BitBox does not have to be plugged in to receive Bitcoin.

Advanced tip: by clicking on “Verify Address Securely”, you can verify the displayed address automatically with a paired BitBox mobile smart verification app.

### 7.3 Send Tab

The purpose of the Send tab is to allow you to send Bitcoin to someone else. You can only send an amount that does not exceed the Available Balance, taking into account the transaction fee. To send Bitcoin, paste in the Bitcoin address of your intended recipient. You may have received this address via email, text, flash drive, etc. It will be uniquely associated with your intended recipient's wallet. Copy and paste the address into the "To Address" field. Visually check the address against the original to make sure it is correct. Alternatively, use the QR reader option (icon to the right of the "To Address" field) to read in the recipient's address using the computer's webcam. Note that your BitBox must be plugged in to send Bitcoin.

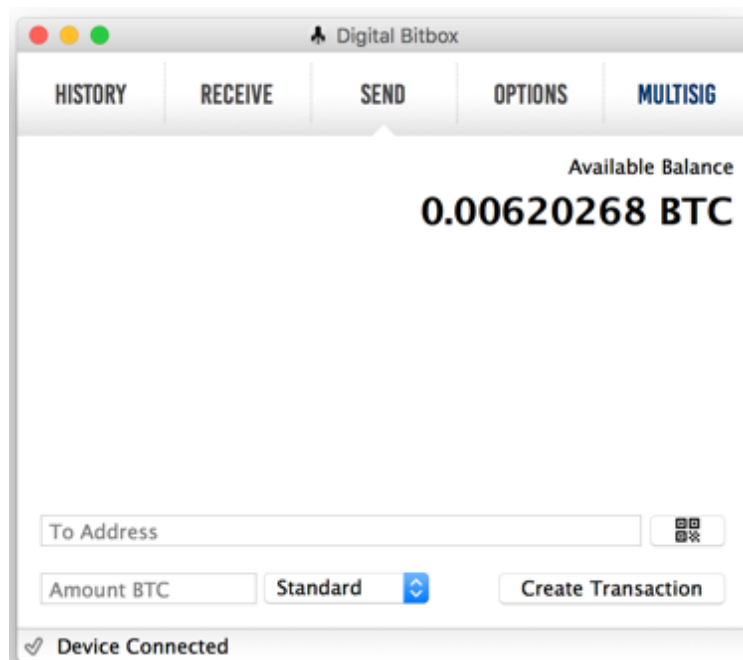


Figure 8 Send Tab

Next, enter in the amount of Bitcoin you want to send. Then select your desired "delivery speed"; Priority, Standard, Economy or Budget. This will determine the fee applied to the transaction. Note that your recipient receives the entered amount of Bitcoin and fees are deducted *in addition* from your Bitcoin balance.

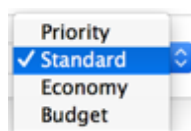


Figure 9 Delivery Speed Pulldown Menu

In general, the higher the level, the faster the transaction is executed. You can preview the fee added to your transaction amount by choosing one of the options (ex. "Standard"), then pressing "Create Transaction". Here you can preview the transaction, including the transaction fee before authorizing the transaction. You may abort the transaction by briefly pressing the LED, or simply waiting for the transaction to timeout and abort. Note that fees are not applied based on amount of Bitcoin associated with the transaction, but rather the amount of data associated with the transaction (i.e. the



number of receive addresses that are used to fulfil the send amount). Thus, a transaction involving a large amount of Bitcoin vs. a small amount of Bitcoin could have the same fee.

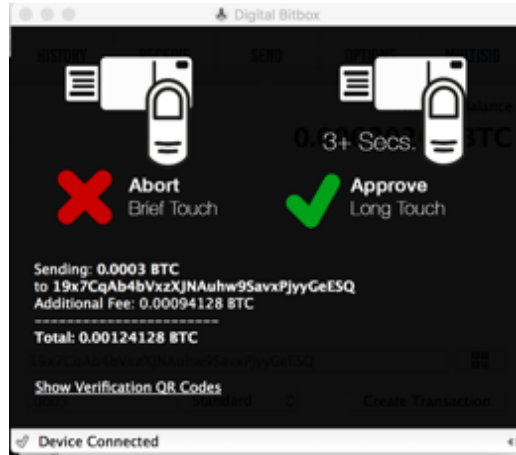


Figure 10: Preview in a send transaction

To confirm and broadcast a payment, touch the LED for 3+ seconds until your transaction is confirmed. Once a transaction has been broadcast to the network, it is OK to remove your BitBox and close the app. You may monitor the status of the transaction in the History tab. An empty red circle indicates it is in progress but not yet confirmed, a partially filled green circle indicates that it has been confirmed by the network, and a full green circle indicates it has completed with a full 6 confirmations. In general, the higher the fee, the faster the transaction will be confirmed.

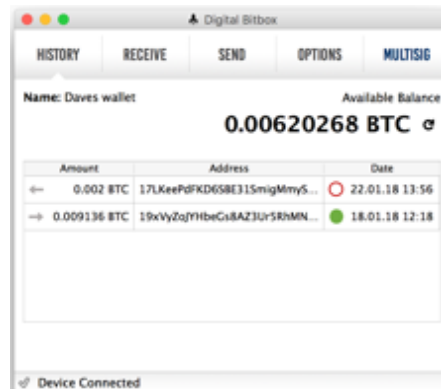


Figure 11: Payment is not yet confirmed

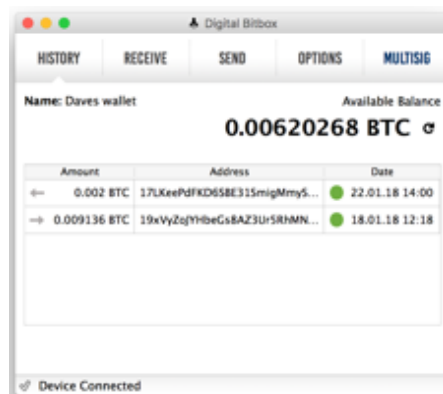


Figure 12: Payment confirmed

## 8. Create and switching between wallets

You can create multiple wallets, each of which is backed up on the micro SD card (make sure it's plugged in when creating wallets). Each wallet is defined by a wallet name and password combination and is backed up by a single unique "seed" stored in a PDF file on the micro SD card.

Only one wallet at a time, however, can be loaded onto your BitBox, with the exception of the „Hidden“ wallet whose sole purpose is to provide „plausible deniability“ described later in this guide.

To create a new wallet while logged into the BitBox go to:

### Options → Create New Wallet

You will be prompted for a new wallet name, for example "Daves second wallet". The new wallet is now created and becomes the active wallet on the BitBox (you can restore the previous wallet from the micro SD card). The new wallet will have the same password as the wallet you were previously in.

You can switch between wallets by restoring the wallet you want to use (with the micro SD card inserted) via

### Options → Manage Backups → Restore

Then select the backup PDF file of the wallet you want to restore, and enter in the original password used when creating the wallet. The restored wallet then replaces the previously active wallet on your BitBox.

## 9. Creating a hidden wallet

For "plausible deniability" purposes, you can create a "hidden wallet" on your BitBox. This is done via

### Options --> Expert Settings --> Hidden Wallet Password

Entering a password here (should be different than for your main wallet) creates a new wallet that looks like your primary wallet (same name), but allows you to store a different

Bitcoin balance. Consider adding a small amount of coins in order to add plausibility.

The scenario is this: if you are forced by someone to log into your BitBox and transfer your funds to another account, you can log into your Hidden Wallet and not your primary wallet.

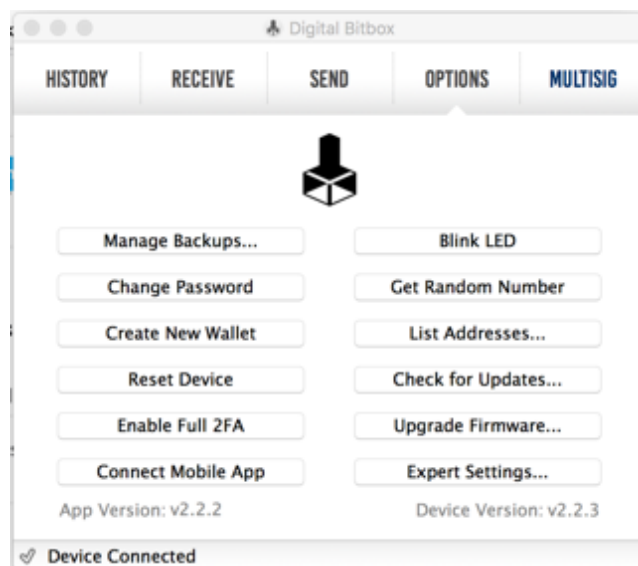
Note that if you restore a wallet from the micro SD backup card, you will need to re-activate the hidden wallet log-in by re-entering the password at:

**Options --> Expert settings --> Hidden Wallet Password.**

Second Factor Authentication (2FA) is activated by default for the hidden wallet; you will need your smartphone to authorize all transactions. This requires that your smartphone has been paired with your BitBox in advance. This also provides a convenient excuse if you do not have your smartphone with you: without it it is impossible to perform any transactions with the hidden wallet.

## 10. Options tab

The options tab gives you options to several features:



- **Manage Backups...**  
Allows you to view, restore, or delete wallet backups (**use delete conservatively and with extreme caution!**). If you want to create a second wallet backup on an additional micro SD card, you can insert a new card into the BitBox and select "Add". This will create a backup of the current wallet loaded on the BitBox. The same backup works for Bitcoin (including the hidden wallet), Ether, and any future coins added with a firmware upgrade. Creating a second backup is recommended in case you lose or damage your first backup.
- **Change Password**  
**This is not recommended** as it can lead to confusion: if you suspect your password has been compromised, we recommend creating a new wallet with a new password and transfer your funds to the new wallet.
- **Create New Wallet**  
This allows you to create a new wallet. Once completed, it immediately becomes the

active wallet on your BitBox and is backed-up on the micro SD card. The micro SD card must be inserted when you create a new wallet. It will use the current password, but generate a new seed. A better option which we recommend is to use the “Reset Device” option instead (see below) and create a new wallet from the reset state. Don't worry, your other wallet(s) is still restorable from the micro SD backup card.

- **Reset Device**  
This option restores your BitBox to its factory settings: all hardware wallet data on the BitBox is deleted. The U2F data remains and can be reset in the “Expert Settings”. Your backed-up wallet(s) can be restored from the micro SD card. Note that resetting your BitBox **does not** delete the backup files on the micro SD card.
- **Enable Full 2FA**  
Use your smartphone as a secure remote second authorization button. This option enables two factor authentication: all transactions are securely transmitted to your smartphone for authorization. Note that you must first pair your smartphone with your BitBox via “Connect Mobile App” before selecting this option.
- **Connect Mobile App**  
This option initiates the process that securely pairs your Android or iOS smartphone with your BitBox. Use your smartphone to securely view transaction information or verify receiving addresses.
- **Blink LED**  
This is a simple feature that confirms that your BitBox is successfully communicating with the desktop app.
- **Get Random Number**  
This is a random code generator which can be used to generate strong passwords.
- **List Addresses...**  
This function allows you to view all the transaction addresses that your BitBox could use over the course of its lifetime. These transaction addresses are unique to your BitBox - no one else will have them.
- **Check for Updates...**  
This informs you whether your BitBox has the latest firmware or not.
- **Upgrade Firmware...**  
This allows you to install new firmware. First download it from the Shift website, and select it from the location you stored it at. Only firmware signed by us can be run on your BitBox. Altered or malicious firmware cannot run.
- **Expert Settings...**  
Additional functionality allowing you to conduct your transactions via a proxy server for increased security, create a hidden wallet, etc.

## 11. Multisig tab

The multisig tab provides for multi-signatory capability for the BitBox; use the BitBox as one member of a multi-signature Copay wallet. In order to authorize transactions, multiple persons will need to provide a valid password. Multisig is currently done in conjunction with the copay app ([copay.io](https://copay.io)).

Simply initialize the wallet in the free and open source Copay app and enter the invitation code. No registration is required. Install it on your phone and select the multisig wallet option. Once you have generated the invitation code, you can enter it into the wallet by clicking “Join Multisig”. The multi-signature wallet co-exists independent of your personal wallet(s).

## 12. Second Factor Authentication

Second Factor Authentication (2FA) can be activated to provide a second level of security: transactions also need to be confirmed via your smartphone. This allows you to check the amount, fee and recipient of each transaction through a secure channel to the device.

**First, download and install the mobile app** on your smartphone from [digitalbitbox.com/start](https://digitalbitbox.com/start) (Apple iOS and Android are supported). For iOS, select the download from iTunes option. Double click on the BitBox icon to start the app.

Do **NOT** press “Enable Full 2FA” before pairing your device with your smartphone via:

### Options --> Connect Mobile App

You will be prompted to pair your smartphone with your BitBox. First, a QR code will appear. Point the camera at the QR code and it will automatically be scanned. The pairing process now begins. You will be prompted to enter in the number of times the LED on the BitBox blinks. You may do this as many or as few times as you like, but it is recommended to do it at least 5 times for high security. You may end the pairing process anytime after the first blinked code by tapping on the BitBox LED between code blinks. Your smartphone will confirm if the pairing is successful; you successfully entered the number of times the LED blinked. If you made a mistake, you will be prompted to repeat the process. Now you may enable 2FA:

### Go to: Options --> Enable Full 2FA

Note that when you enable 2FA, creating new backups and mobile app pairing are disabled. Additionally, Ether can be received but cannot be sent while 2FA is enabled.

To disable 2FA, the device needs to be reset, and your wallet must be restored from backup. All your transactions will now require authentication and confirmation from your smartphone. For example, when sending Bitcoin, complete details of the transaction are displayed i.e. amount and send address, as well as fee, and other transaction data. Pressing “Accept” continues the transaction signing process.

## 13. Restoring a wallet from backup

If you have lost, damaged or reset your wallet, you can restore it by following these instructions.

- 1) **You have lost or damaged your wallet:** in this case you should order a new BitBox and restore your wallet onto the new BitBox using the instructions below. Note that due to the comprehensive security features of the BitBox, it is virtually impossible for anyone to access your wallet should they find the lost BitBox.

Note: You could also restore your wallet to a software wallet (see instructions on [digitalbitbox.com/backup](https://digitalbitbox.com/backup)). In this way you can be sure your wallet(s) are always recoverable, independent of the BitBox.

- 2) **You have reset your wallet** (via Options-->Reset Device). In this case you can restore your wallet using the instructions below.

**Instructions for restoring a new or reset BitBox:** Insert the micro SD backup card. Create a “dummy” wallet (a temporary wallet so that you can access the desktop app). For the password, enter the password of the wallet you want to recover (**important!**).

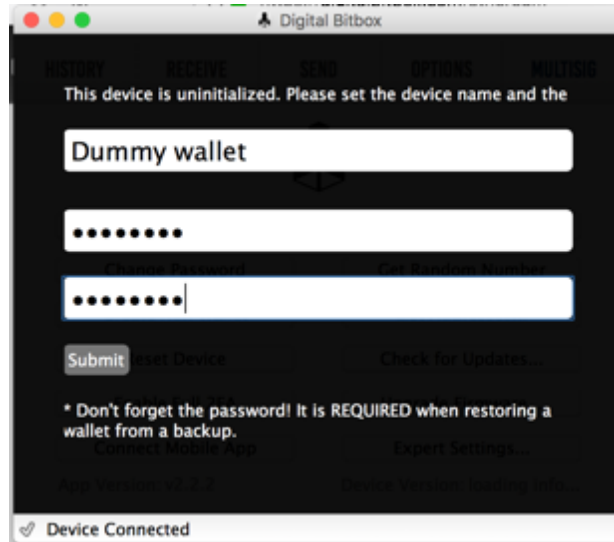


Figure 13: First step in restoring your wallet - create a dummy wallet

Once logged in to your “Dummy Wallet”, go to **“Options --> Manage backups...”**. From the available backups (PDFs), select the wallet you want to restore, for example:

Daves\_wallet-2018-01-11-16-10-01.pdf

You will be prompted to enter the password used when first creating the wallet you want restored. Be sure to enter it correctly: an incorrect password will generate a wallet different from your original wallet (Tip: this is an additional plausible deniability feature in the case someone forces you to recover your wallet from backup).

Click on “Restore”. You will be prompted to touch the LED for 3+ seconds to confirm. This will restore the wallet you created on 11 January 2018 named “Daves wallet”. Note you can only load one wallet at a time on your BitBox (including the associated “Hidden Wallet”).

Your wallet is now restored.

## 14. Using an Ether wallet

Once you have created a wallet, you can also receive and send Ether and ERC20 tokens via MyEtherWallet ([myetherwallet.com](https://myetherwallet.com)). Sending and receiving Ether and ERC20 tokens is done via [myetherwallet.com](https://myetherwallet.com). A private key stored on your BitBox gives you access in the same way as it gives you access to your Bitcoin wallet. The private key stays securely inside the BitBox and never enters MyEtherWallet. Phishing sites can NOT access the BitBox because the MyEtherWallet URL is hardcoded in the BitBox firmware. As a fallback option, a local copy of MyEtherWallet is provided at [digitalbitbox.com/mew](https://digitalbitbox.com/mew). The backup on your micro SD card is used to recover both your Bitcoin and Ethereum wallets.

Detailed instructions for setting up and using an Ether Wallet are here: [digitalbitbox.com/ethereum](https://digitalbitbox.com/ethereum)

To avoid having to install plugins, use either Chrome or Opera. Firefox or Safari only work if a browser extension for Universal 2<sup>nd</sup> Factor (U2F) devices is installed.

First plug your configured BitBox into your USB port and navigate to [myetherwallet.com](https://myetherwallet.com). Click on “Send Ether & Tokens” from the header menu and select Digital BitBox.

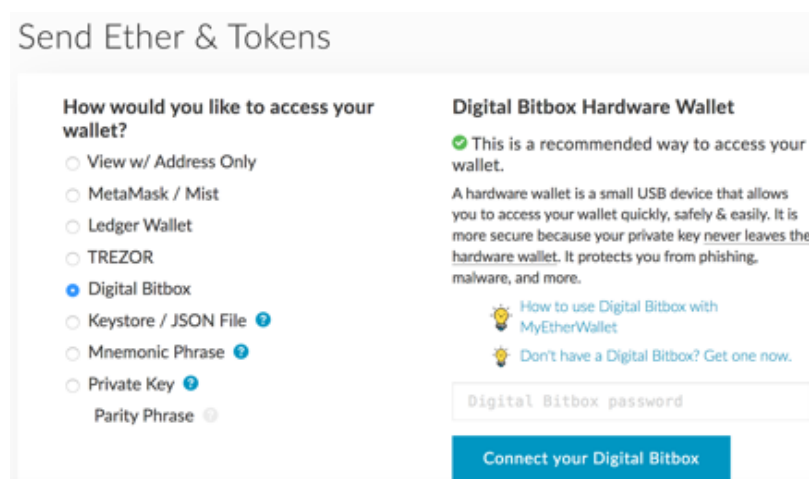


Figure 14: Select Digital BitBox

Enter your wallet password into the “Digital BitBox password” field and press “Connect your Digital BitBox”. The following screen appears.

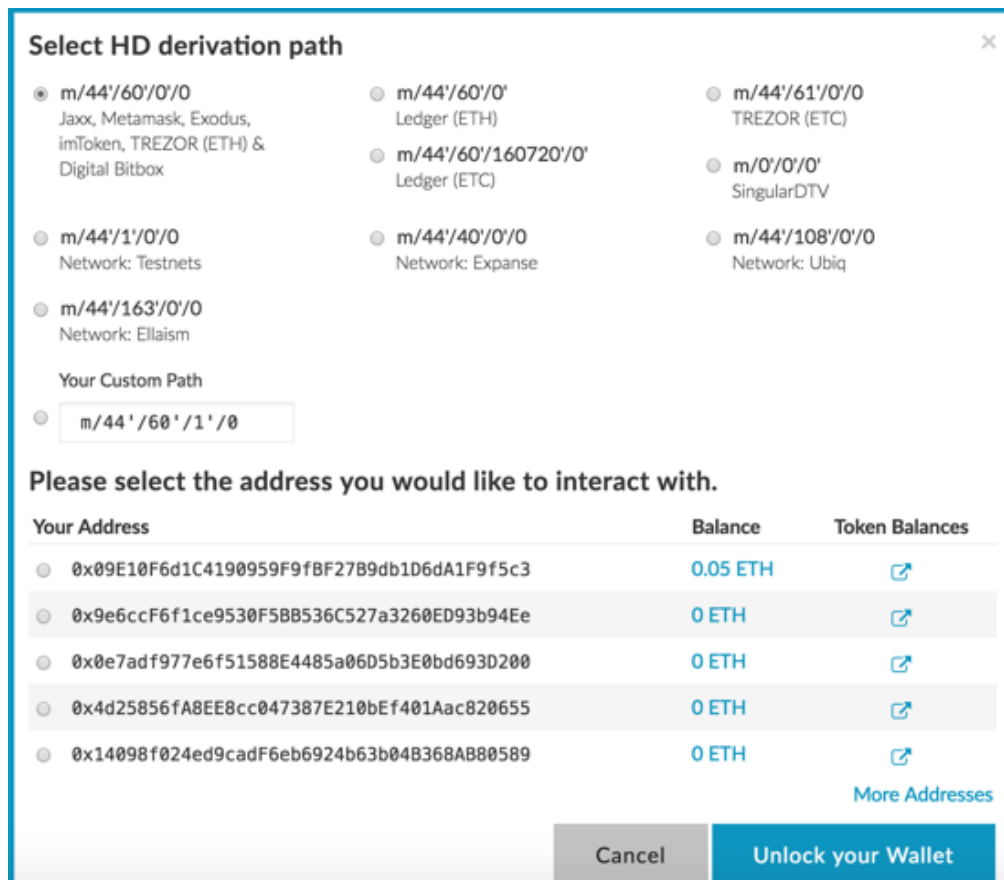


Figure 15: Initializing your Ether Wallet

Select HD derivation path: select the default setting, the first option where you see “Digital BitBox” beneath.

Please select the address you would like to interact with: select any one of the addresses. This will be your Ether wallet: the address where you will send and receive Ether. Unlike Bitcoin, the same address is always used. You may choose a different address later to create a second unique Ether wallet, completely independent of the first wallet. The addresses displayed will always be the same whenever you log in with the same BitBox wallet. Then press “Unlock your wallet”.

Note: for simplicity, if you only plan to use one Ether wallet, choose the first address on the list each time. This will ensure that you always access the same wallet, and the correct address location is easy to remember.



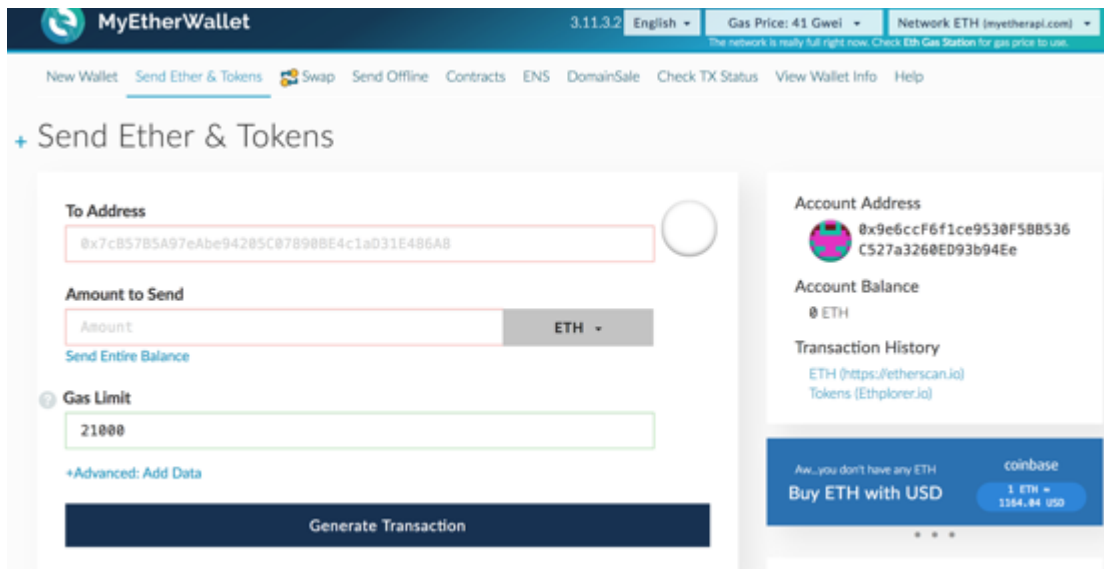


Figure 16: Your Etherwallet on myetherwallet.com; accessed using the BitBox

To send Ether, enter a send address of the person you want to send Ether to and follow the instructions. A transaction will be generated and signed but not yet sent to the network. Scroll down and press the button “Generate Transaction” to send the transaction.

Note: If 'Full Two-Factor Authentication (Full 2FA)' is enabled using the desktop app, Ether can be received but CANNOT be sent. This is also the situation for hidden wallets, where full 2FA is always enabled by default.

To view your transaction history:

Click on “**Transaction History**” → **ETH** to view your complete Ethereum transaction history.  
Click on “**Transaction History**” → **Tokens** to view your ERC20 tokens transaction history.

**ATTENTION:** Do NOT generate a new wallet on MyEtherWallet by pressing “New Wallet”. This will NOT create a wallet on your Digital BitBox, and coins sent there will NOT be accessible via your BitBox.

## 15. Sending ERC20 tokens

The process for sending ERC20 tokens is the same as for sending Ether. In this case, while you are logged into your Ether wallet, scroll down to the box on the right side of the window and click “Show All Tokens”. A pulldown menu will appear where you may choose the ERC20 Token you would like to send.

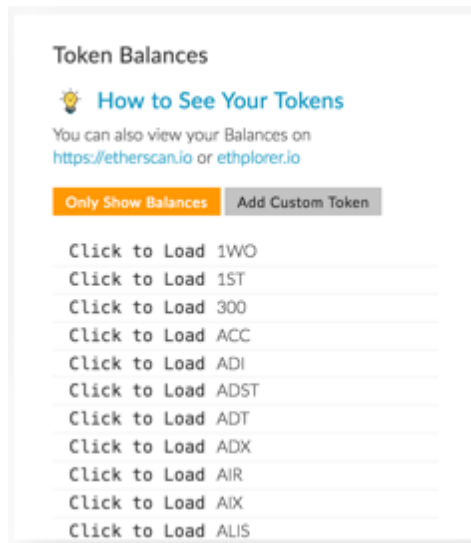


Figure 17 Selecting an ERC20 token for sending

You will see your selected ERC20 token in the “Amount to Send” box in the “Send Ether & Tokens” screen, but only if you actually have that particular token in your balance. Sending is the same as for sending Ether.

## 16. Using an Ethereum Classic Wallet

To send and receive Ethereum Classic, via the pulldown menu in the upper right, select “ETC”.

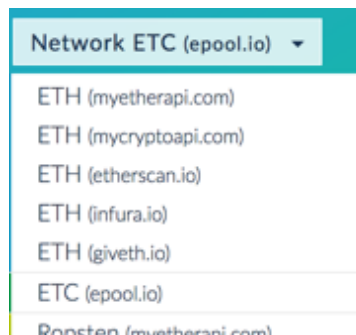


Figure 18: selecting an Ethereum Classic Wallet

The rest of the process is identical as for Ether Wallet described previously.

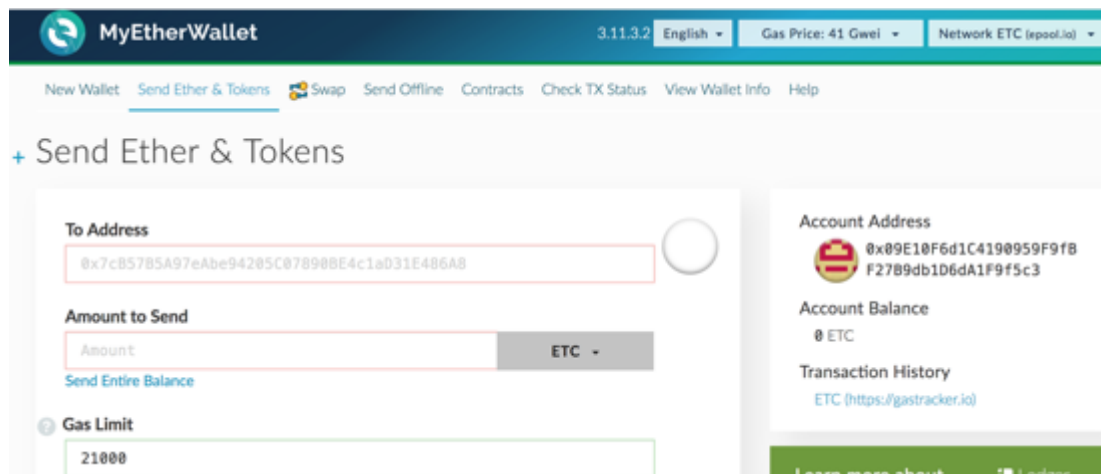


Figure 19: Accessing your Ethereum Classic Wallet

## 17. Upgrading the BitBox firmware

Upload firmware to your Digital BitBox using the **Options** menu item **Upgrade Firmware**, available in the desktop app. If you have problems after upgrading the firmware, check that you are also using the latest [desktop app](#). When upgrading on Linux operating systems, be sure you are using desktop app version 2.2.2 or later.

To upgrade, log into your BitBox and select:

**Options → Check for Updates:** this will indicate if your firmware is the latest or not. If not, first download the latest firmware, store it on your computer, then click on:

**Options → Upgrade Firmware**

Navigate to the downloaded firmware and double-click.

Downloads contain firmware signed using our company keys. The signatures are checked inside the Digital BitBox bootloader at every plug in. Invalid or modified firmware cannot run.

[Source code](#) is available on GitHub. If you wish, you can verify that the Digital BitBox is running the same code by building the firmware on your own and uploading it.

## 18. FAQs

- 1) **Are my coins and transaction history stored on my BitBox?**  
No. Your coins and transaction history are stored on the network, not the BitBox. Your BitBox securely stores the private key(s) that is required to access your funds. However, if you lose your BitBox and backup micro SD card and have no other backup, you lose access to all your funds.
- 2) **Are all my transactions stored forever?**  
Yes. The Bitcoin network stores all transactions indefinitely on thousands of distributed computers all over the world. This distributed ledger is called the Blockchain and is virtually impossible to alter or hack.
- 3) **Why should I keep my BitBox separate from the backup micro SD card?**  
If you lose your BitBox and micro SD card, you lose access to all your funds forever (assuming you have no other backups). Keep the micro SD card somewhere safe. If you have a lot of funds, create multiple backups on multiple micro SD cards and store them in separate secure locations. Pay attention to avoid environmental hazards such as fire, high humidity and flooding. With just the BitBox, or with just the micro SD card you can access your wallet as long as you also remember your password.
- 4) **I lost my micro SD card. If someone finds it, can they find out my password or my private key(s) from it?**  
No. The backup micro SD card only stores your seed. Without knowing your password your private keys (i.e. the wallet) cannot be derived, and hence your wallet cannot be accessed.
- 5) **Can I replace my micro SD card if I lose it?**  
Yes. The micro SD card is a standard off-the-shelf micro SD Card. Only a small fraction of the card is used, so the one with the smallest amount of memory is sufficient. To create a new backup of the wallet loaded on the BitBox, insert a micro SD card into the BitBox, then go to **Options > Manage Backups...** and press "Add".
- 6) **Can I have more than one copy of my micro SD card storing the same backup information?**  
Yes. Just insert a different micro SD card into the BitBox, go to **Options > Manage Backups...** and press "Add". Note that your password is NOT stored on the card. We recommend storing the password separately in a secure location.
- 7) **I prefer to use paper to store my backup, how can I do that?**  
The backup is saved as a PDF file. The micro SD card can be inserted into a trusted printer or computer for printing. Be aware that malware on a computer could view the backup, and the memory in a public printer that was used to print the file could be viewed by later users or administrators. Keep the paper copy somewhere safe. Do not use thermal printers because the ink will disappear quickly.
- 8) **Can I recover my wallet without a BitBox?**  
Yes, based on your seed ("wallet backup") and password, you can create recovery keys which can be used to load your wallet in a software wallet, see: [digitalbitbox.com/backup](https://digitalbitbox.com/backup). Instructions for loading the wallet onto a BitBox are

included. It is highly recommended, however, to restore your wallet to another BitBox so that you do not expose your private keys to an external computer or the internet.

- 9) **I can't find my BitBox. Is there a risk that someone who finds it will be able to access my cryptocurrency funds?**  
No. Assuming you have selected a reasonable password, someone who doesn't know the password cannot access your wallet. After 15 failed password attempts, the BitBox will reset and erase all stored information. It is good policy to transfer any funds you had in wallets associated with the lost BitBox to a new wallet(s).
- 10) **I lost/damaged my BitBox. How can I restore my wallet?**  
The safest method is to order a new BitBox and restore your wallet(s) via the micro SD backup card. Insert the micro SD card, create a temporary "dummy" wallet giving it the same password associated with the wallet you want to restore, then go to "**Options → Manage Backups...**". Each backup there (.pdfs) corresponds to one of your wallets. Select the wallet you want to restore and click "Restore" and enter the password that was used when first creating that wallet. Your BitBox wallet is now identical to the one you lost.
- 11) **Can I have more than one identical copy of my BitBox having the same access to my funds?**  
Yes. The backup on the micro SD card can be loaded onto multiple BitBoxes. You can do this for convenience without compromising on security – you could have one copy at work, a copy for home, a copy that you carry with you, a copy for family members, etc.
- 12) **I am concerned that the memory of the BitBox and micro SD backup card has a finite lifetime (10 – 50 years). How can I be sure I will always have access to my crypto-currencies?**  
No electronic media lasts forever. Best practice is to create multiple copies of your backup micro SD card and store them in geographically separate and secure locations. Periodically verify that the backups still work and replace any that fail. For large amounts of crypto-currencies, store several backup cards in addition to paper or engraved-metal/stone backup (including passwords, but in a separate location). You can also print out and securely store backups of the contents of the micro SD card, just make sure the computer and printer are secure and not connected to the internet, nor publically shared.
- 13) **Can I store ERC20 tokens on a BitBox wallet?**  
Yes, you can store ERC20 tokens on a BitBox wallet using MyEtherWallet integration.
- 14) **Will you be adding more coins?**  
Yes. The BitBox software is continuously improving and we will add more coins. Litecoin has been recently been added. Be sure to check our website and stay up to date with the latest software.
- 15) **How can I recover Ether without a BitBox ?**  
If you inspect our backup tool on [digitalbitbox.com/backup](https://digitalbitbox.com/backup) you will find a section for Ethereum private keys. Typically, Ethereum uses a single private key. If you do not know which key to use, it is likely the first key listed. These keys can be imported one by one to MyEtherWallet by going to

[www.myetherwallet.com/#send-transaction](http://www.myetherwallet.com/#send-transaction) and then selecting Private Key from the bullet list.

**16) What's the safest way to secure large amounts of coins with my BitBox?**

Choosing to access large amounts of cryptocurrencies is best done with a hardware wallet such as the BitBox. In this way your private keys cannot be stolen or hacked via the internet or compromised software running on your computer. Importantly, be sure to store your backup micro SD card and passwords separately in safe locations. There are several levels of security you could choose:

- Entry-level: make backups of your wallet(s) on your micro SD card. Remember your password(s) and/or write them down and store each in a separate secure location.
- Next-level (recommended): make two or more copies of your micro SD card backup and two or more copies of your password(s) and store them all in separate secure locations. You could also make multiple identical copies of your BitBox, each with identical access to your wallet(s).
- Enabling Full 2FA (Options tab) prevents thieves who stole both your BitBox and password from accessing your funds; they would also need to have access to your phone.
- For very large amounts of cryptocurrencies: in addition to the backup SD cards, print out the backup PDFs from your micro SD card on paper, or engraved in stone or metal and store in a safety-deposit box in a reputable bank in a financially and politically stable country. Store your password(s) in the same way in a different safety deposit box at a different bank. Make sure no one involved in the process has had access to both backup PDF(s) and password(s).

**17) Do I need to eject the BitBox before taking it out of the USB socket?**

No. You can simply remove the BitBox from the USB slot once you have finished using it.

## 19. Additional help

If you have questions not addressed in this guide, visit [support.digitalbitbox.com/](http://support.digitalbitbox.com/) to submit a support ticket.

## 20. Revision History

Version	Date	Author	Description
1.0	13.02.2018	<a href="mailto:cf@shiftcrypto.ch">cf@shiftcrypto.ch</a>	Initial version
1.1	19.03.2018	<a href="mailto:cf@shiftcrypto.ch">cf@shiftcrypto.ch</a>	Litecoin support added