BitBox02

Seed generation with dice

1 Introduction

This document provides you with easy step-by-step instructions on how to create your own random seed to use with Bitcoin wallets.

It contains a table with all 2048 words of the BIP39 wordlist, neatly arranged in a matrix and mapped for easy lookup. In combination with the **BitBox02** hardware wallet, this allows you to generate your own secret seed, without relying on the wallet to do it for you.

Why should I do this?

First of all: you don't need to do this. The BitBox02 uses five different sources of entropy to create high-quality randomness: from manufacturing, your device password, the host computer, the microcontroller and the secure chip.

Each source can only add randomness, not reduce it. And with the firmware fully open-source and reproducibly built, anyone can check how that works.

But a hardware wallet should be a tool for personal sovereignty. This is why creating your own seed can be an empowering experience. And if done well, you can get a truly random seed that can easily be verified, with zero trust put in the inner workings of the BitBox02 to create randomness.

How does that work?

Modern wallets are based on a single secret seed, from which all private keys and addresses are derived. This seed is just a huge number. But to be secure, it must be truly random, otherwise overall security is reduced.

The seed number is usually encoded into 24 English words, because these are easier to write down without introducing mistakes. But just picking random words is not as easy as it sounds, because humans are really bad at creating random patterns. This is why the best choice is to roll dice, preferably really good casino-grade ones.

You can roll your dice to determine the first 23 words. But the main challenge in this process is that you can't simply pick any word as your 24th word because it needs to be calculated using a hashing algorithm. This last word is in fact in part a checksum over all other words and it's nearly impossible to compute it manually.

But that's no problem with the BitBox02 hardware wallet: it enables you to enter the first 23 words and then the device shows you all valid 24th word options. Pick one and you're all set. That set of 24 recovery words works with every wallet that follows the BIP39 standard and can easily be verified by importing it into another hardware wallet.

BitBox02
Seed generation with dice

2 Preparations

To generate your own seed, you need the following:

- a printout of this document with directions and foldable backup card
- a printout of the BitBox02 Diceware lookup table
- five casino-grade dice (a single die works as well)
- regular coin (or use another die)
- BitBox02 hardware wallet

Make sure you are in a private environment. Turn off electronic devices, and put your mobile phone somewhere else. Don't say the numbers or recovery words out loud. Don't mark anything on the lookup tables. And write down your recovery words only on the backup card, they must never touch an electronic device except the BitBox02.

Finally: get comfortable and put on some good music.

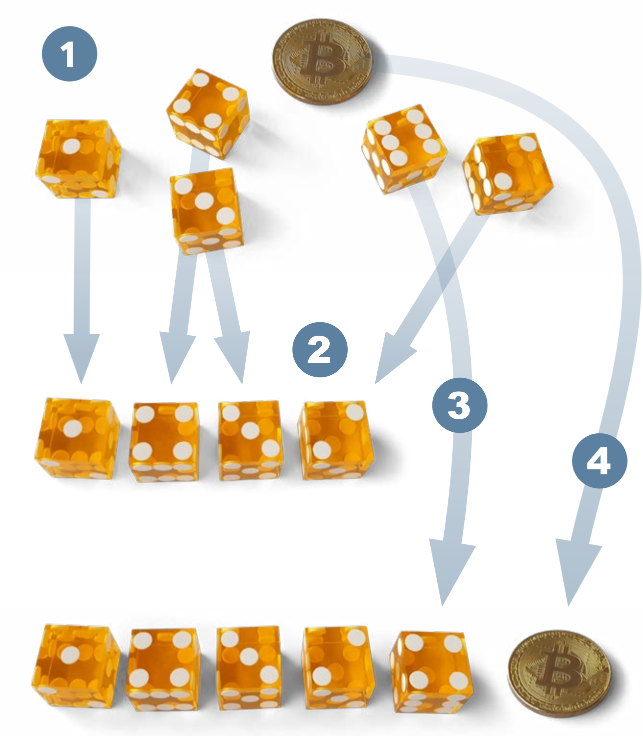
3 How to roll your dice to get good randomness

It's important to decide on a specific method first and follow it through, instead of making seemingly random decisions during the process.

We find that the following approach works best:

1. Roll all five dice and the coin together
2. Line all dice that show a number from 1 to 4 in a neat line, pick them from left to right (and top to bottom if in doubt)
3. Reroll all dice that show a 5 or 6 until they show a number from 1 to 4 and line them up as well.
4. Put the coin next to the dice as well.

Not enough dice or no coin? If you don't have five dice, you can roll a single die to get the 5 numbers between 1 and 4



BitBox02
Seed generation with dice

4 Pick your first 23 recovery words

Roll five dice and flip the coin as described above, then pick out the next recovery word from the BitBox02 Diceware lookup table document as follows:

- Die 1 gives you the page number of the lookup table
- Dice 1 to 4 give you the correct row
- Die 5 and the coin flip give you the correct column

Write down the recovery word on the backup card.

Repeat this for the first 23 words.

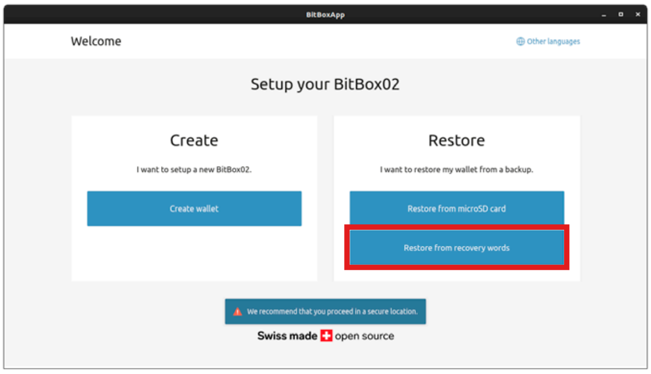
Don't choose the 24th word yet.

5 Finalize your wallet on the BitBox02

With all 23 recovery words, you can create a new wallet with your BitBox02. If the BitBox02 is already set up, make sure you have a valid backup of the current wallet and reset the device.

- In the setup wizard, choose "Restore from recovery words"
- On the BitBox02, select "24 words"
- Enter your 23 recovery words on the BitBox02 (and nowhere else)
- Once you've entered the 23 recovery words, the BitBox02 will display 8 valid options for the final checksum word
- Pick one of the final recovery words at random and write it down as the 24th word on the backup card
- The BitBox02 will show a "Recovery words valid" message. You can now set your device password.

The BitBox02 is now fully set up and will calculate all keys and addresses based on your very own seed.



Setup your BitBox02

Create

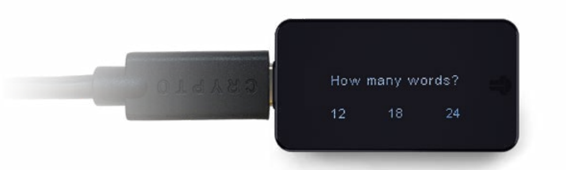
I want to setup a new BitBox02.

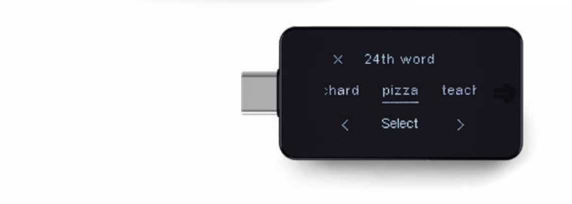
Restore

I want to restore my wallet from a backup.

We recommend that you proceed in a secure location.

Swiss made open source





BitBox02
Seed generation with dice

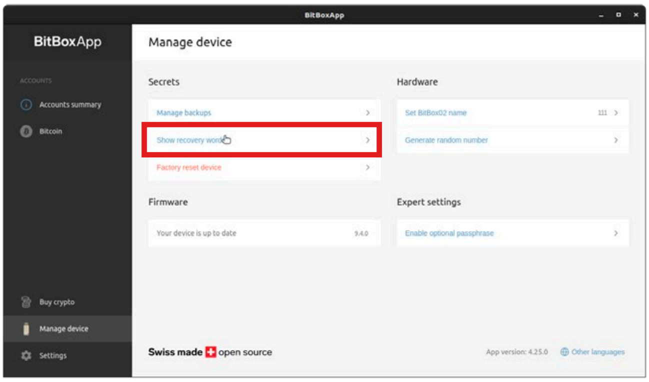
6 Validate your wallet backup

As of now, your backup card is the only backup you have of your new wallet.

To make sure it's 100% correct, you need to validate it.

- In the BitBoxApp, choose "Manage device" > "Show recovery words"
- Confirm the security precautions in the BitBoxApp
- Enter your device password on the BitBox02
- Your 24 words are now shown on the BitBox02. You can quickly race through all of them (just tap ">" repeatedly) and then tap "Continue"
- The BitBox02 now challenges you for each recovery word to pick the right option

If you get everything right, your backup is accurate.



7 Backup redundancy

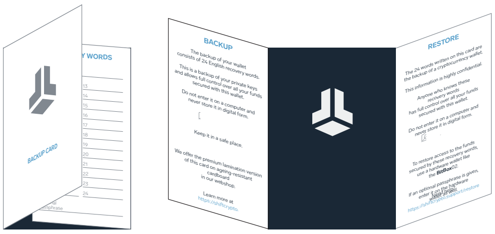
You can now also create a backup on the microSD card.

If this wallet will hold your life savings, think about securing the backup with additional redundancy and resilience. Maybe our proven backup accessories like the ageing-resistant Backup card, our Apocalypse-proof Steelwallet, or the tamper-evident security bags come in handy?

BitBox02 backup card

Cut and fold to create your wallet backup using recovery words.

Get the premium version with lamination, printed on aging-resistant cardboard in our webshop at https://bitbox.shop.



BACKUP CARD

BACKUP

The backup of your wallet consists of 24 English words.

This is a backup of your private keys and allows full control over all the funds secured with this wallet.

Do not enter it on a computer and never print, copy or store it in digital form.

Keep the backup card in a safe place.

We offer the premium version of this card, with lamination, printed on ageing-resistant cardboard in our webshop.

Learn more at
https://bitbox.swiss/backupcard

CONFIDENTIAL
keep this document safe

Backup name

Date

Notes

RECOVERY WORDS

Wallet name

01

02

03

04

05

06

07

08

09

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

Optional passphrase

RESTORE

The 24 words written on this card are the backup of a cryptocurrency wallet.

This information is highly confidential.

Anyone who knows these recovery words has full control over all the funds secured with this wallet.

Do not enter it on a computer and never print, copy or store it in digital form.

To restore access to the funds secured by these recovery words, use a hardware wallet like the **BitBox**02.

If an optional passphrase is given, enter it on the hardware wallet as well.

Need help?
https://bitbox.swiss/backupcard

Shift Crypto AG, Switzerland