BitBox02
Würfle deinen eigenen Seed

1 Einleitung

Dieses Dokument bietet dir eine einfache Schritt-für-Schritt-Anleitung, wie du deinen eigenen zufälligen Seed zur Verwendung mit Bitcoin-Wallets erwürfeln kannst.

Es enthält eine Tabelle mit allen 2048 Wörtern der BIP39-Wortliste, übersichtlich in einer Matrix angeordnet zum einfachen Nachschlagen. Mit der BitBox02 Hardware-Wallet kannst du so deinen eigenen geheimen Seed generieren, ohne dich darauf verlassen zu müssen, dass die Wallet dies für dich tut.

Warum sollte ich das tun?

Zunächst einmal: Du brauchst das nicht zu tun. Die BitBox02 nutzt fünf verschiedene Quellen von Entropie, um maximale Zufälligkeit zu erzeugen: sowohl aus der Herstellung, deinem Gerätepasswort, deinem Rechner, dem Mikrocontroller und dem Secure Chip. Jede Quelle kann nur Zufälligkeit hinzufügen, nicht reduzieren. Da die Firmware vollständig quelloffen und reproduzierbar kompiliert ist, kann jeder überprüfen, wie das funktioniert.

Aber eine Hardware-Wallet sollte ein Werkzeug für persönliche Souveränität sein. Das ist der Grund, warum das Erstellen deines eigenen Seeds eine starke Erfahrung sein kann. Und wenn man es gründlich macht, kann man einen wirklich zufälligen Seed erhalten, der leicht verifiziert werden kann, ohne dass man dem Innenleben der BitBox02 in Bezug auf die Erzeugung von Zufälligkeit vertrauen muss.

Wie funktioniert das?

Moderne Wallets basieren auf einem einzigen geheimen Seed, von dem alle privaten Schlüssel und Adressen abgeleitet werden. Dieser Seed ist einfach eine grosse Zahl. Aber um sicher zu sein, muss er wirklich zufällig sein, sonst wird die Gesamtsicherheit reduziert.

Der Seed wird normalerweise in 24 englischen Wörtern kodiert, weil diese einfacher aufzuschreiben sind, ohne dabei Fehler zu machen. Aber einfach nur zufällige Wörter auszuwählen ist nicht so einfach wie es klingt: Menschen sind wirklich schlecht darin, zufällige Muster zu erstellen. Deshalb ist würfeln eine zuverlässige Methode, am besten mit richtig guten Casino-Würfeln.

Du kannst würfeln, um die ersten 23 Wörter zu bestimmen. Aber die grosse Herausforderung ist es, dass du nicht einfach irgendein Wort als dein 24te Wort verwenden kannst. Dieses letzte Wort ist zum Teil eine Prüfsumme über alle anderen Wörter und es ist fast unmöglich, dieses manuell zu berechnen.

Mit der BitBox02 Hardware-Wallet ist das aber kein Problem: du kannst die ersten 23 Wörter eingeben und das Gerät zeigt dir dann alle gültigen Optionen für das 24te Wort an. Wähle eins aus und das war's. Diese 24 Wiederherstellungswörter funktionieren mit jeder BIP39-kompatiblen Wallet, und können einfach durch den Import in eine andere Hardware-Wallet verifiziert werden.

BitBox02
Würfle deinen eigenen Seed

2 Vorbereitungen

Um deinen eigenen Seed zu würfeln benötigst du folgendes:

- Ausdruck dieser Anleitung mit faltbarer Backup-Karte
- Ausdruck der BitBox02 Diceware Wörtertabelle
- fünf Würfel in Casinoqualität
  (ein einzelner Würfel funktioniert auch)
- reguläre Münze (oder verwende ebenfalls einen Würfel)
- BitBox02 Hardware-Wallet

Stelle sicher, dass du ungestört bist. Schalte elektronische Geräte aus und lege dein Mobiltelefon weg. Sprich die Zahlen oder Recovery-Wörter nicht laut aus. Markiere nichts auf den Nachschlagetabellen. Und schreibe deine Wiederherstellungswörter nur auf die Backup-Karte, sie dürfen niemals mit einem elektronisches Gerät ausser der BitBox02 in Kontakt kommen.

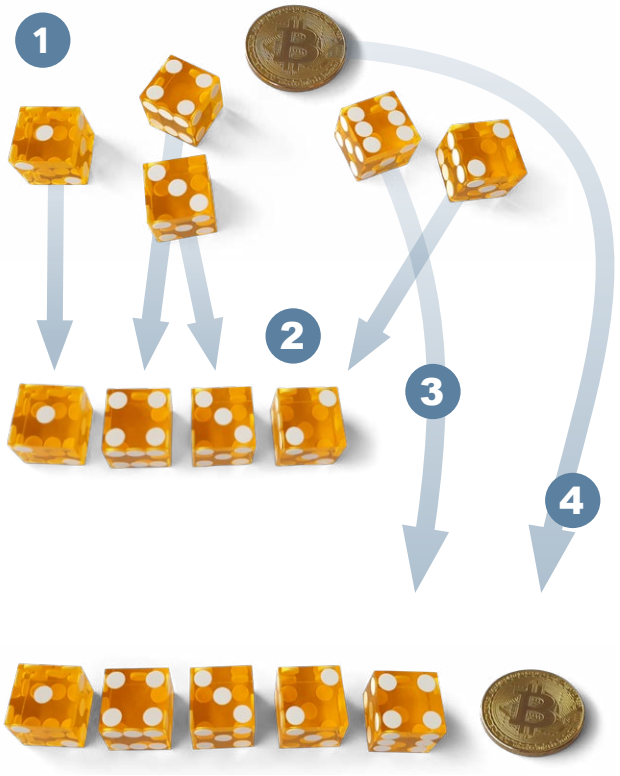
Zum Schluss: mach es dir gemütlich und lege etwas gute Musik auf.

3 Wie würfeln für maximale Zufälligkeit?

Es ist wichtig, sich zuerst für eine bestimmte Methode zu entscheiden und diese dann durchzuziehen, anstatt während dem Prozess scheinbar zufällige Entscheidungen zu treffen.

Wir finden, dass der folgende Ansatz am besten funktioniert:

1. Wirf alle fünf Würfel und die Münze zusammen.
2. Arrangiere alle Würfel, die eine Zahl von 1 bis 4 zeigen, in einer ordentlichen Reihe, wähle sie von links nach rechts (und im Zweifelsfall von oben nach unten).
3. Wirf alle Würfel, welche eine 5 oder 6 zeigen, erneut, bis sie eine Zahl von 1 bis 4 zeigen und reihe sie auf.
4. Lege die Münze neben die Würfel.



Nicht genug Würfel oder keine Münze? Wenn du keine fünf Würfel hast, kannst du einen einzelnen Würfel werfen, um die 5 Zahlen zwischen 1 und 4 nacheinander zu erhalten. Notiere sie einfach auf Papier (und verbrenne dieses danach).

Wenn du keine Münze benutzen willst, kannst du auch einen Würfel werfen: die Zahlen 1 bis 3 sind “Kopf” (“heads”) und die Zahlen 4 bis 6 sind “Zahl” (“tails”).

BitBox02
Würfle deinen eigenen Seed

4 Würfle deine ersten 23 Wörter

Wirf fünf Würfel und wirf die Münze wie oben beschrieben, dann wähle das nächste Wiederherstellungswort aus der BitBox02 Diceware Wörtertabelle wie folgt aus:

- Der erste Würfel gibt dir die Seitenzahl der Wörtertabelle.
- Die Würfel 1 bis 4 zeigen dir die richtige Zeile.
- Würfel 5 und der Münzwurf ergeben die richtige Spalte.

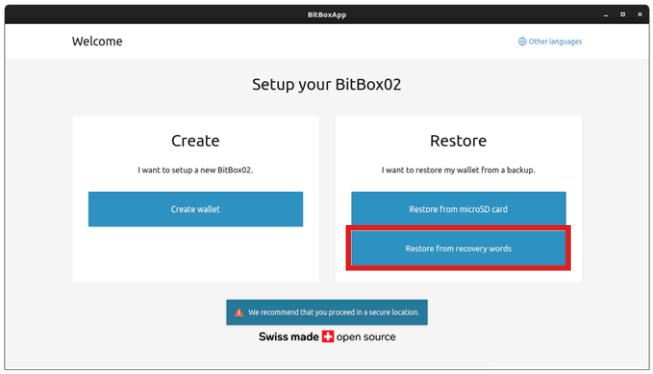
Schreibe das Lösungswort auf die Backup-Karte.

Wiederhole dies für die ersten 23 Wörter, aber noch nicht für das 24te Wort.

5 Finalisiere deine Wallet auf der BitBox02

Mit den 23 Wiederherstellungswörtern kannst du eine neue Wallet mit deiner BitBox02 erstellen. Wenn die BitBox02 bereits eingerichtet ist, stelle sicher, dass du ein gültiges Backup der aktuellen Wallet hast und setze das Gerät zurück.

- Wähle im Einrichtungsassistenten “Von Recovery-Wörtern wiederherstellen”
- Wähle auf der BitBox02 bei “How many recovery words?” die Option “24”
- Gib deine 23 Wiederherstellungswörter auf der BitBox02 ein (und nirgendwo sonst)
- Sobald du die 23 Wiederherstellungswörter eingegeben hast, zeigt die BitBox02 acht gültige Optionen für das letzte Wort an
- Wähle eines dieser Wörter nach dem Zufallsprinzip und notiere es als 24tes Wort auf der Backup-Karte
- Wähle es auf der BitBox02 aus und bestätige es auf dem Gerät
- Die BitBox02 wird die Meldung “Recovery words valid” anzeigen. Du kannst nun dein Gerätepasswort setzen



Die BitBox02 ist nun vollständig eingerichtet und wird alle Schlüssel und Adressen basierend auf deinem selbst erstellten Seed berechnen.

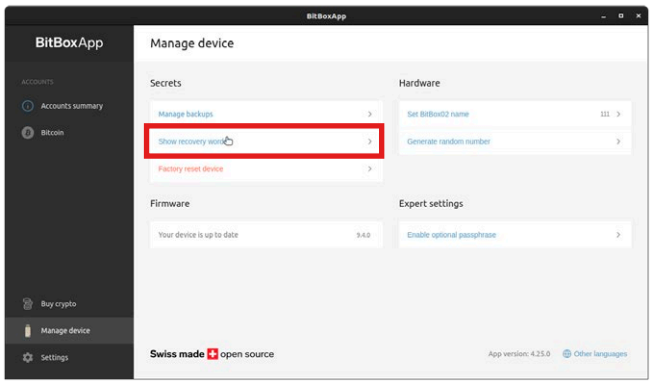
BitBox02
Würfle deinen eigenen Seed

6 Prüfe dein Wallet-Backup

Momentan ist deine Backup-Karte die einzige Sicherung, die du von deiner neuen Wallet hast. Um sicher zu gehen, dass diese zu 100% korrekt ist, musst du sie validieren.

- Wähle in der BitBoxApp “Gerät verwalten” > “Recovery-Wörter anzeigen”
- Bestätige die Sicherheitswarnungen in der BitBoxApp
- Gib dein Gerätepasswort auf der BitBox02 ein
- Deine 24 Wiederherstellungwörter werden nun auf der BitBox02 angezeigt. Du kannst sie alle schnell durchlaufen (tippe einfach mehrmals auf “>”)
- Die BitBox02 fordert dich nun für jedes Wort auf, die richtige Option zu wählen

Wenn alles ohne Warnung klappt, ist dein Backup korrekt.



7 Redundanz fürs Backup

Du kannst nun auch ein Backup auf der microSD-Karte erstellen.

Wenn diese Wallet viel Geld oder gar deine Lebensersparnisse enthält, solltest du darüber nachdenken, das Backup mit zusätzlicher Redundanz und Ausfallsicherheit zu sichern. Vielleicht kann sich unser bewährtes Backup-Zubehör wie die alterungsbeständige Backup-Karte, unsere Apokalypse-sicheres Steelwallet oder die manipulationssicheren Sicherheitstaschen als nützlich erweisen?