

Würfle deine eigene Seed-Phrase.

Eine Kurzfassung, wie man Würfelergebnisse in eine BIP-39-Seed-Phrase mit 12 oder 24 Wörtern umwandelt.

Du kannst diese gedruckte Anleitung für eine echte Seed-Phrase verwenden. Wenn du während des Prozesses auf Schwierigkeiten stößt, gehe gerne zurück zur Online-Anleitung und mache einen Trockendurchlauf mit einer Dummy-Phrase. Halte Würfe, Bits und Seed-Wörter deiner echten Seed-Phrase von Geräten mit einer Netzwerkverbindung fern.

Vorbereiten

Würfel

Gut verarbeitete sechsseitige Würfel. Vermeide Deko-, Spaß-, beschädigte oder sichtbar ungleichmäßige Würfel.

Würfel-Setup

Eine Box mit Deckel, in der sich alle Würfel frei bewegen können, oder ein größerer Würfelbecher mit harter Unterlage.

Ausdrucke

Ein BitsToWords-Arbeitsblatt und die durchsuchbare englische BIP-39-Wortliste.

Stift

Um jedes Bit/Wort auf Papier aufzuschreiben. Tippe diese nie in ein internet-verbundenes Gerät.

Offline-Gerät für Prüfsumme

Eine Hardware-Wallet oder ein dauerhaft offline bleibender Laptop, der die Prüfsumme vervollständigt.

Nicht-öffentlicher Raum

Keine Kameras, Telefone, Smart Glasses, Beobachter oder Aufzeichnungsgeräte.

1

Wähle eine Kodierung aus

Oren's variable-length mapping - empfohlen

- 1 → 00
- 2 → 01
- 3 → 10
- 4 → 11
- 5 → 0
- 6 → 1

Rechne mit etwa 77 Würfeln für 12 Wörter oder 154 für 24 Wörter.

Binäre Quantisierung

- 1, 2 oder 3 → 0
- 4, 5 oder 6 → 1

Du wirst genau 128 Würfe für 12 Wörter oder 256 für 24 Wörter machen.

2

Wähle die Länge der Phrase

Wähle frei zwischen 12 und 24 Wörtern.

Drucke das passende BitsToWord Arbeitsblatt und notiere eine **willkürliche Bezeichnung**, damit du die Sicherung später wiederer kennst.

3

Würfeln und notieren

Box mit Deckel: Lege alle Würfel in die Box, schließe den Deckel und schüttele mindestens zehnmal kräftig. Kippe die Würfel dann vorsichtig zu einer Seite und lies von links nach rechts; eine zweite Reihe liest du von vorne nach hinten. Ordne Würfel nicht von Hand.

Becher und Unterlage: Schüttele kräftig, wirf mit genug Platz und Energie und lies die Würfel mit einer vor dem ersten Wurf gewählten räumlichen Regel.

Wandle jedes Ergebnis mit deiner Kodierung um und schreibe die Bits in die nächsten leeren Kästchen. Wenn ein Würfel schief liegt oder nicht eindeutig lesbar ist, verwirf den **ganzen Satz** und würfle ihn erneut.

Wiederhole diese Schritte bis du den dicken Trenner im letzten Wort erreichst. Lasse bei 12 Wörtern die letzten 4 Kästchen leer, bei 24 Wörtern die letzten 8. Verwirf Bits, falls sie diese Grenze überschreiten würden, und ignoriere danach alle übrigen Würfel des Wurfs.

4

Bits in Wörter umwandeln

Nutze für jede vollständige 11-Bit-Gruppe die ausgedruckte BIP-39-Wortliste um das zugehörige Wort zu bestimmen:

- Bits 1-3 (P) bestimmen die **Seite**;
- Bits 4-6 (C) bestimmen die **Spalte**;
- Bits 7-8 (R) bestimmen den **Block**;
- Bits 9-11 (R) bestimmen die **Zeile im Block** und damit das Wort.

Schreibe das Wort unter seine 11 Bits. Durchsuche die Wortliste nicht digital, auch nicht nach teilen eines Wortes.

5

Letztes Wort vervollständigen

Die Prüfsummen-Bits des letzten Wortes sind durch die bereits notierten Bits mathematisch festgelegt. Sie verringern die von den Würfeln erzeugte Zufallsstärke nicht.

- Bei 12 Wörtern lassen deine sieben gewürfelten Bits des letzten Wortes **16** mögliche Wörter.
- Bei 24 Wörtern lassen deine drei gewürfelten Bits des letzten Wortes **256** mögliche Wörter.

Gib die vorherigen Wörter als bestehende Seed-Phrase in dein Hardware-Wallet/deinen Offline Rechner ein. Lass dir ein letztes Wort vorschlagen und prüfe dann, dass es eines der zulässigen Wörter ist.

Verwahre deine Seed-Phrase privat, offline und sicher.