

Würfelvorlage

Bits zu Wörtern: so entsteht deine Seedphrase aus echtem Zufall.

Diese Vorlage ist nach dem Ausfüllen so wertvoll wie deine Seedphrase.

Sie enthält deinen kompletten Schlüssel in Binärform. Verwahre sie danach so sicher wie dein Backup oder vernichte sie vollständig. Ein Papierkorb ist keine Vernichtung.

In vier Schritten

1. Würfeln

Wirf alle Würfel auf einmal und schiebe sie zu einer Linie zusammen.
Sortiere sie nicht und schaue sie vorher nicht an. Immer dieselbe Abfolge.

2. In Bits übersetzen

Gehe die Linie von links nach rechts durch.
Würfel zeigt 1, 2 oder 3 -> trage eine 0 in das nächste freie Kästchen ein.
Würfel zeigt 4, 5 oder 6 -> trage eine 1 ein.

3. Wiederholen

Bis alle Kästchen gefüllt sind. Ausnahme: Die grau hinterlegten Kästchen
beim letzten Wort bleiben leer. Das ist die Prüfsumme.

4. Wörter nachschlagen

Erste drei Bits = Seite, nächste drei Bits = Spalte, letzte fünf Bits = Zeile.
Schlage in der ausgedruckten BIP39-Wortliste nach und trage das Wort ein.

Wie viele Würfe?

LÄNGE	BITS GESAMT	DAVON PRÜFSUMME	WÜRFE
12 Wörter	132	4	128
24 Wörter	264	8	256

Zwölf Wörter reichen völlig aus. 128 Bit Zufall sind mit keiner denkbaren Rechenleistung zu durchsuchen.
Das letzte Wort bestimmst du zum Schluss mit deiner Hardware-Wallet, weil die Prüfsumme berechnet werden muss.

Vorlage: 12 Wörter

128 Würfe. Die letzten vier Kästchen bleiben frei.

Bezeichnung:

Wähle etwas, das für Außenstehende nichts verrät.

	SEITE 3 BIT	SPALTE 3 BIT	ZEILE 5 BIT	WORT AUS DER LISTE
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				

Die grauen Kästchen bleiben leer.

Das sind 4 Bit Prüfsumme. Sie werden aus allen vorherigen Bits berechnet und lassen sich nicht würfeln.
Gib die ersten Wörter in deine Hardware-Wallet ein, sie schlägt dir die gültigen letzten Wörter vor.

Vorlage: 24 Wörter, Teil 1

Wörter 1 bis 12 von 24. Insgesamt 256 Würfe.

Bezeichnung:

Wähle etwas, das für Außenstehende nichts verrät.

	SEITE 3 BIT	SPALTE 3 BIT	ZEILE 5 BIT	WORT AUS DER LISTE
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				

Vorlage: 24 Wörter, Teil 2

Wörter 13 bis 24 von 24. Die letzten acht Kästchen bleiben frei.

Bezeichnung: Wähle etwas, das für Außenstehende nichts verrät.

	SEITE 3 BIT	SPALTE 3 BIT	ZEILE 5 BIT	WORT AUS DER LISTE
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				

Die grauen Kästchen bleiben leer.

Das sind 8 Bit Prüfsumme. Sie werden aus allen vorherigen Bits berechnet und lassen sich nicht würfeln.
Gib die ersten Wörter in deine Hardware-Wallet ein, sie schlägt dir die gültigen letzten Wörter vor.