FINAL STEP ₿ITCOIN

DA BINARIO A MNEMONICA BIP39

SCHEDA DI LAVORO · 11 BIT = 1 PAROLA

1 I QUATTRO PASSAGGI

PASSO 1

CREA ENTROPIA

Usa i dadi, le monete o le carte e crea 23 gruppi di 11 bit (0 o 1). Per la parola 24 avrai solo 3 bit (0 o 1).

PASSO 2

SCRIVI I BIT IN TABELLA

Scrivi gli 11 bit nella tabella. La colonna rappresenta il numero della parola.

PASSO 3

SOMMA DOVE C'È 1

Somma i valori delle sole colonne dove hai scritto un 1. Viene un numero fra 0 e 2047: scrivilo nella colonna *somma*.

PASSO 4

AGGIUNGI 1 E CERCA

Somma + 1 = numero della parola. Cercalo nella lista BIP39 numerata e scrivi la parola nell'ultima colonna.

ESEMPIO SVOLTO — GRUPPO 01011001011

VALORE	1024	512	256	128	64	32	16	8	4	2	1
BIT	**0**	**1**	**0**	**1**	**1**	**0**	**0**	**1**	**0**	**1**	**1**
DA SOMMARE	–	512	–	128	64	–	–	8	–	2	1

512 + 128 + 64 + 8 + 2 + 1 = **715** → 715 + 1 = parola n. **716** → **floor**

2 LA PROVA DEL NOVE

`00000000000` somma 0 → parola n. 1 → **abandon**	`11111111111` somma 2047 → parola n. 2048 → **zoo**	`10000000000` somma 1024 → parola n. **1025**

Se un gruppo ti dà una somma sopra 2047, hai contato dodici bit invece di undici: ricontrolla l'incolonnamento.

3 QUELLO CHE LA TABELLA NON PUÒ FARE

I CONTI SONO SU 264 BIT, NON 256

Una seed da 24 parole non nasce da 256 bit ma da **264**: 256 bit di entropia più 8 bit di **checksum**, che sono i primi 8 bit dello SHA-256 dell'entropia. 264 diviso 11 fa esattamente 24.

COME SI DISTRIBUISCONO I BIT

Le prime **23 parole** usano 253 bit (23 × 11), cioè quasi tutta la tua entropia: quelle le ricavi con questa tabella e nient'altro. La **parola 24** è fatta dagli ultimi **3 bit di entropia** più gli **8 bit di checksum**. Ecco perché la 24° parola non la scegli tu: su 2048 parole solo **8** sono valide.

IL CHECKSUM A MATITA NON SI CALCOLA

SHA-256 non è un'operazione che si fa a mano. Le prime 23 parole le ottieni con questa scheda; per l'ultima serve uno strumento che calcoli il checksum **offline**, senza mai toccare internet. Puoi usare un hardware wallet che abbia questa funzionalità (BitBox02, SeedSigner, Jade).

> ## REGOLE DI SICUREZZA
>
> Compila questa scheda **su carta**: mai in un file, mai in una chat, mai in un foglio di calcolo. L'entropia deve venire da una fonte fisica — dadi, monete — oppure da un dispositivo offline. Un computer connesso, o qualunque servizio online, vede quello che scrivi: se la seed passa da lì, quella seed non è più tua. Finito il lavoro, **distruggi la scheda**: tieni solo le 24 parole, sul supporto definitivo.

LA LISTA DELLE PAROLE

Serve la wordlist inglese ufficiale BIP39, numerata da 1 a 2048: è quella della specifica BIP-39, identica in tutti i portafogli. **2048 parole**, ognuna riconoscibile dalle prime quattro lettere. La puoi trovare sul mio sito web finalstepbitcoin.com/risorse

4 GRIGLIA DA COMPILARE — 24 PAROLE

Una riga per parola. Un bit per casella, somma i valori delle colonne con 1, aggiungi 1, cerca la parola.

PAROLA	1024	512	256	128	64	32	16	8	4	2	1	SOMMA	N.	PAROLA BIP39
1														
2														
3														
4														
5														
6														
7														
8														
9														
10														
11														
12														
13														
14														
15														
16														
17														
18														
19														
20														
21														
22														
23														
24														

Righe 12 e 24: **arancione carico** = i bit che scrivi tu, **arancione chiaro** = il checksum, che si calcola a parte. La 24 chiude una seed da 24 parole (3 + 8), la 12 solo se ti fermi a 12 parole (7 + 4). Vedi le note del punto 3.
