

GUIDA PRATICA

DISPOSITIVO OFFLINE · ULTIMA PAROLA BIP39 E PASSPHRASE DICEWARE

1 COSA FA E COSA NON FA

MODALITÀ 1

CHECKSUM

Gli dai le prime **11** parole del seed (o le prime **23**) e lui calcola l'ultima valida.

MODALITÀ 2

PASSPHRASE

Tu tiri i dadi, lui li traduce in parole della lista Diceware. Il caso lo porti tu.

QUELLO CHE NON FA

Niente WiFi né Bluetooth: non è una scelta del programma, è il chip che non li ha. **Non salva niente e non calcola chiavi private:** non può risalire al tuo portafoglio.

2 ACCENDILO E CONTROLLA L'IMPRONTA

Collegalo con un cavo micro-USB a un **caricatore da telefono**, non al computer: molte power bank potrebbero non funzionare perché il dispositivo assorbe pochissimo. Per una maggiore sicurezza puoi aggiungere un **Data Blocker USB**. Non c'è niente da installare, parte da solo. Ma se non ti fidi, puoi scaricare il firmware da github.com/Finalstepbitcoin/prisma e installarlo in autonomia.

ALL'ACCENSIONE DEVE MOSTRARE STABLE CHAIR PROBLEM

Sono l'impronta di tutto quello che il dispositivo esegue. Se ne mostra tre diverse, dentro c'è qualcosa di diverso: **fermati** e riscrivi il firmware. Protegge solo da un guasto accidentale, **non da una manomissione voluta**: un firmware manomesso potrebbe mostrarle comunque giuste. Verifica vera al punto 6.

Confrontale con quelle pubblicate su Nostr da questa chiave: `npub17ugguepv89nvdrrd72j7j25ymuts6w3d3lnsg6f0xgm2ah8zskhq3v5ulj`

3 I COMANDI

joystick	si muove fra lettere, voci di menu ed elenchi	B	cancella; a casella vuota torna indietro
A	conferma, sceglie	X e Y	i valori 1 e 0 quando si inseriscono i bit

Nei tiri di dado: **su = 1** **destra = 2** **giù = 3** **sinistra = 4** **centro = 5** **X = 6** – lo schema è disegnato sullo schermo.

4 MODALITÀ CHECKSUM: L'ULTIMA PAROLA DEL SEED

Un errore nell'inserimento delle parole darebbe un checksum **corretto, ma su parole sbagliate**. Il dispositivo ti mostrerà le parole che hai inserito. Controllale prima di proseguire. Una volta terminato, **non fotografare lo schermo** per salvare la parola.

- Menu → Checksum.** Scegli se il tuo seed è da **12** o da **24** parole.
- Inserisci le prime 11 parole** (o 23). Per ogni parola compare la griglia delle **sole lettere ancora possibili**: il joystick si muove, A conferma. Quando restano cinque parole o meno te le mostra e scegli quella giusta.
B cancella una lettera; a casella vuota, torna alla parola precedente.
- Aspetta il calcolo.** Con 11 parole ci mette circa 3 secondi e mezzo, con 23 circa 6: la barra arancione mostra a che punto è.
- Scegli come completare.** Il dispositivo propone tre strade:
Bit rimasti – quella giusta: inserisci i **7 bit** che ti avanzano dai dadi (3 se il seed è da 24), **nell'ordine in cui li hai generati**. X vale 1, Y vale 0.
Scegli tu – se non ti avanzano bit di entropia puoi sceglierne una a caso (**NON consigliato**): scorri l'elenco, X filtra per iniziale.
Tutti zeri – butta via i bit che avanzano. Solo se sai perché lo stai facendo.
- Copia la parola** che compare grande, in verde, e **rileggila** confrontandola con lo schermo.
- Stacca il cavo.** L'ultima schermata è un vicolo cieco voluto: nessun tasto porta da nessuna parte. È l'unico modo di azzerare davvero la memoria di lavoro.

5 MODALITÀ PASSPHRASE: I DADI E LA LISTA DICEWARE

- 1 Menu → Passphrase.** Scegli la lista: **Inglese** (Reinhold) o **Italiano** (Gamberini). Sono 7.776 voci ciascuna e **non sono la traduzione l'una dell'altra**: sono due liste indipendenti.
- 2 Tira cinque dadi** per ogni parola e registra i valori col joystick. Cinque dadi fanno $6 \times 6 \times 6 \times 6 \times 6 = 7.776$ combinazioni: una per ogni voce, nessuno scarto.
Se un lancio non ti piace, **tienilo lo stesso**. Ritirarlo rimette la tua testa nel processo e distrugge la casualità.
- 3 Guarda i bit che stai accumulando.** Dopo ogni parola: **A** per farne un'altra, **Y** per fermarti. Sotto le **6 parole** il dispositivo ti avvisa ogni volta; il massimo è **20** (258,5 bit), in due schermate da dieci.
- 4 Se compare "copiala esatta!"** la voce contiene simboli o cifre – per esempio **a, @, i 've, 12**. Sono legittime e vanno copiate **esattamente così**.
- 5 Copia tutte e due le schermate finali** – prima l'elenco numerato, poi la passphrase per intero – **sullo stesso foglio**. Poi stacca il cavo.
Con più di 10 parole l'elenco numerato sta su due schermate, con una freccia per passare alla seconda: copiale entrambe.

UNA PASSPHRASE NON HA CHECKSUM

Se la trascrivi male **non ricevi nessun errore**: entri semplicemente in un altro portafoglio, vuoto. Il seed BIP39 da questo ti protegge, la passphrase no.

COME SCRIVERE LA PASSPHRASE

rune a @ issue cat orin è la stringa da digitare, **spazi compresi**. Senza spazio, due parole potrebbero confondersi. Se vuoi scrivere la passphrase senza gli spazi, assicurati di conservare l'elenco delle parole.

COME SALVARE LA PASSPHRASE

Viene mostrato sia l'elenco delle singole parole, sia la stringa intera, per una **doppia conferma**. Salvali entrambi. Annota anche come scriverai la passphrase (con/senza spazi). **Non fotografare mai lo schermo**.

6 COME VERIFICARE IL FIRMWARE

- LIVELLO 1 Le tre parole all'accensione.** Immediato, ma è il programma che parla di sé: rileva un guasto accidentale, **non** una manomissione voluta.
- LIVELLO 2 Riscrivilo tu.** È il percorso più sicuro: invece di controllare quello che c'è dentro, lo sostituisci con quello che scarichi tu. Inquadra il codice QR o vai su **github.com/Finalstepbitcoin/prisma** e segui le istruzioni.
- LIVELLO 3 Leggilo e confrontalo.** Sempre da BOOTSEL, un programma di verifica rilegge la memoria a dispositivo spento: risponde il **bootloader di fabbrica**, non il firmware. È l'unica verifica che il firmware non può falsificare.



CODICE GITHUB

7 AVVERTENZE

SPEGNERE = STACCARE IL CAVO

Il tasto **RESET** riavvia il processore ma **non azzerà** la memoria di lavoro. L'unico spegnimento vero è togliere la corrente.

UNA MODALITÀ PER SESSIONE

Usa checksum e passphrase in **due sessioni separate**, staccando il cavo in mezzo: così il dispositivo non ha mai in memoria tutte e due le metà del tuo segreto.

TRASCRIVI IL RISULTATO

Trascrivi il segreto (ultima parola o passphrase). Attenzione al foglio su cui scrivi perché contiene il tuo segreto in chiaro: conservalo o distruggilo dopo aver copiato i segreti su un supporto metallico.

Progetto libero e ispezionabile. Dizionario BIP39 dal repository ufficiale dei BIP · lista Diceware inglese di Arnold Reinhold (CC BY 4.0) · lista Diceware italiana di Tarin Gamberini (GPL-3.0-or-later) · motore dei calcoli derivato da **embit** (MIT), la stessa libreria usata da SeedSigner e Krux. Il codice del progetto è MIT; il firmware assemblato, contenendo la lista italiana, esce sotto GPL-3.0. **Questo progetto non è stato sottoposto ad audit professionali**: i calcoli sono verificati contro i vettori ufficiali BIP39, il resto è codice scritto con cura ma non revisionato da terzi. Trattalo di conseguenza.



FINAL STEP BITCOIN

[YOUTUBE.COM/@FINAL STEP BITCOIN](https://www.youtube.com/@finalstepbitcoin)

[WWW.FINALSTEPBITCOIN.COM](https://www.finalstepbitcoin.com)

Trovi anche una **video guida** sul mio canale YouTube

