Hardware wallet: tutto quello che avreste voluto sapere ma non avete mai osato chiedere

Valerio Vaccaro

Satoshi Spritz Bergamo

4 Aprile 2025

Chi Sono

- Sviluppatore Bitcoin ed Esperto Hardware
- Contribuisco a Progetti Open Source Bitcoin
- https://github.com/valerio-vaccaro/
- Appassionato di Sicurezza Hardware
- Ingegnere presso Blockstream

? Meme

⚠ Non le tue chiavi, non i tuoi bitcoin!

Cos'è un Hardware Wallet?

- Dispositivi fisici per utilizzare le chiavi private senza esporle al mio telefono/computer
- Introducono un livello di sicurezza e controllo aggiuntivo
- Proteggono da malware e attacchi remoti
- Combina sicurezza e usabilità (anche per persone meno esperte)

Cosa fa un Hardware Wallet?

- Firma Transazioni
- Generazione di chiavi pubbliche ed indirizzi
- Supporto alla generazione della mnemonica (con entropia esterna)

Cosa NON fa un Hardware Wallet?

- Generazione di transazioni
- Calcolo saldo, storico transazioni, ...
- Backup e memorizzazione delle chiavi private
- Generazione sicura della mnemonica (ho detto SICURA!)

Comprendere l'Entropia

- Entropia = Misura della casualità/imprevedibilità
- Utilizzata per generare:
  - Mnemonica (BIP39)
  - Nonce
  - Randomicità output, randomicità gui, ...
- Cruciale per la sicurezza: entropia debole = chiavi deboli o entropia predicibile = chiavi predicibili

Fonti di Entropia

Fonti Hardware

- Generatori di Numeri Casuali (TRNG)
- Sensori di temperatura
- Rumore elettronico
- Rumore radio
- Jitter di clock

Fonti Utente

- Movimenti nella gui
- Tempi di arrivo messaggi
- Intervalli pressione tasti
- Camera

Ma come facciamo a sapere se l'entropia è abbastanza casuale?

Dall'Entropia alla Mnemonica a 24 parole

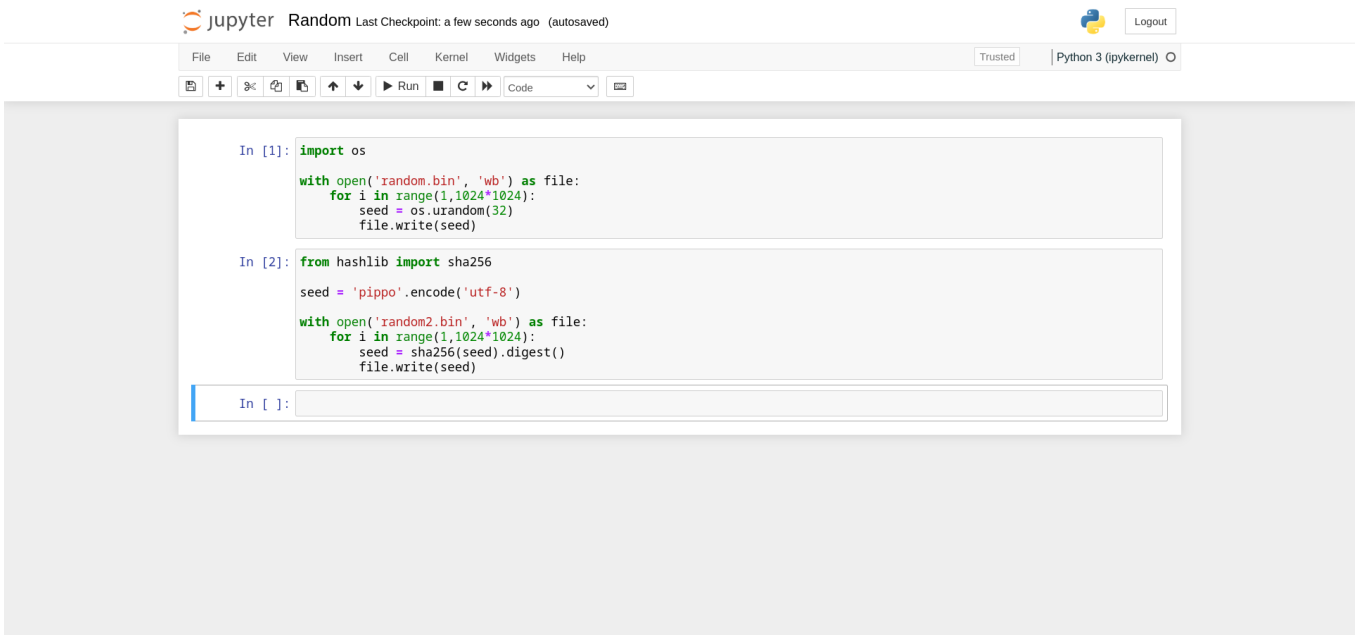
- Generazione di 256 bit di entropia
- Esempio:
  `0c1e24e5917779d297e14d45f14e1a1a...`
- Aggiunta checksum (primi 8 bit dello SHA256)
- Divisione in 24 gruppi da 11 bit
- Mappatura di ogni gruppo a parola da lista 2048
- Risultato: frase seed di 24 parole
  `abandon math mimic master...`

Ma come facciamo a sapere se l'entropia è abbastanza casuale?

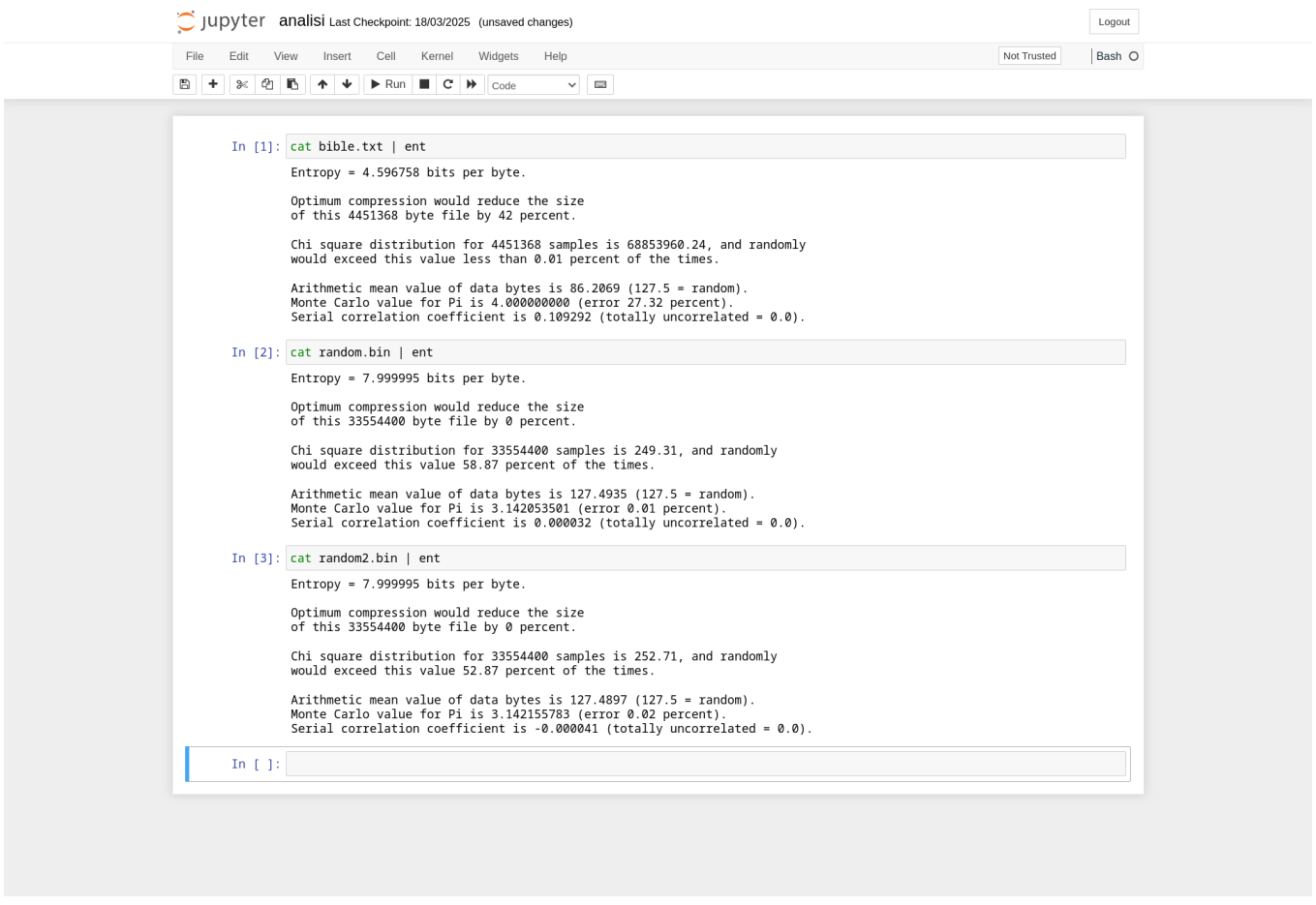
Qualità dell'Entropia

- Problemi Comuni:
  - Generatori di numeri casuali deboli
  - Pattern prevedibili
  - Entropia iniziale insufficiente
  - Miscelazione entropia inadeguata
  - Entropia non uniforme
  - Perdita di entropia
  - Generatori black-box

Test della Qualità dell'Entropia



Test della Qualità dell'Entropia



Secure Elements

Alcuni HW hanno un secure element, altri no. Di cosa si tratta?

- Chip hardware dedicati alla sicurezza
- Protezione contro manomissioni fisiche
- Archiviazione sicura delle chiavi
- Operazioni crittografiche in ambiente isolato
- Protezione contro attacchi side-channel

Ma...

- Chip close source
- Backdoor possibili
- Entropia non controllabile
- Costo

Hardware Wallet & Secure Element

Gli HW con possono avere (dal piu insicuro al piu sicuro):

- 0 secure element
- 1 secure element
- Piu di 1 secure element
- Secure element software e open source

E poi ci sono i device che non memorizzano nulla ...

Hardware Wallet Open Source

- Perché Open Source è Importante:
  - Codice verificabile da chiunque
  - Scoperta più rapida delle vulnerabilità
  - Contributi della community
  - Nessuna backdoor nascosta
- Rischi Closed Source:
  - Pratiche di sicurezza sconosciute
  - Funzionalità nascoste
  - Vendor lock-in
  - Attacchi alla supply chain

Ma il solo open source non è sufficiente.

Build Riproducibili

Vantaggi

- Sicurezza supply chain
- Verifica build
- Validazione community
- Rilevamento malware

Processo

- Checkout codice sorgente
- Compilazione deterministica
- Verifica hash
- Validazione firme

Ma è necessario molto lavoro per avere un build riproducibile.

Verifica del tuo Hardware Wallet

Il processo di verifica del tuo HW è molto importante.

- Build da Sorgente:
  - Clone repository
  - Setup ambiente build
  - Seguire istruzioni build
  - Confronto checksum
- Verifica Firmware:
  - Download firmware firmato
  - Controllo chiavi di firma
  - Verifica firme
  - Aggiornamento sicuro

Sicurezza Supply Chain

- Vettori di Attacco:
  - Manomissione hardware
  - Modifica firmware
  - Interferenza packaging
  - Attacchi alla distribuzione
- Protezioni:
  - Packaging anti-manomissione
  - Firmware firmato
  - Verifica autenticità
  - Processo di boot sicuro

Attenzione alle soluzioni DIY!

Tipologie di connessione

- Seriale
- Bluetooth
- Qrcode
- Memorie di massa

Tuttavia il mezzo di connessione non va mai considerato come sicuro.

Migliori Pratiche Open Source

- Prima dell'Acquisto:
  - Verifica disponibilità codice sorgente
  - Controlla feedback della community
  - Verifica storico di sicurezza
  - Leggi la documentazione
- Dopo l'Acquisto:
  - Verifica autenticità
  - Compila/verifica firmware
  - Controlla firme
  - Mantieni aggiornato

Hardware Wallet Popolari

Trezor One

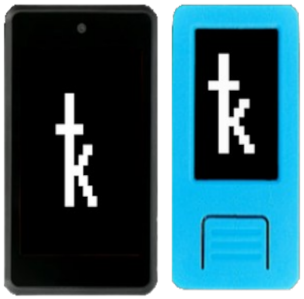
ColdCard

Ledger Nano S Plus

BitBox02

Hardware Wallet Popolari

Portal



Krux

SeedSigner

Specter DIY

Hardware Wallet Jade

- Sviluppato da Blockstream
- Hardware e software open source
  - Secure element software
- Seriale e Bluetooth
- Supporto nativo Liquid Network
- Interazione con QR code
- Funziona con wallet come Blockstream Green, Sparrow, Electrum e altri.

Blockstream Jade

Blind Pin Server

Sistema di sicurezza alternativo all'elemento sicuro tradizionale.

- Il segreto per decifrare il seed è su di server remoto ("blind oracle").
- Il server conosce solo un hash del PIN combinato con un nonce, senza accesso a chiavi private o indirizzi.
- L'utente inserisce il PIN corretto; il wallet richiede al blind oracle la parte mancante del segreto tramite canale crittografato (scambio chiavi ECDH).
- Il seed viene sbloccato per autorizzare transazioni.
- Dopo tre PIN errati, dispositivo e server cancellano i dati sensibili, rendendo il wallet inutilizzabile senza seed di recupero.
- Utenti avanzati possono configurare un proprio blind oracle, riducendo la dipendenza da Blockstream.

Blind Pin Server

Vantaggi:

- Architettura trasparente e open-source.
- Evita costi e limitazioni dei secure elements proprietari.
- Protezione robusta contro attacchi fisici o estrazione delle chiavi.
- Possibilità di configurare un proprio blind oracle.

Punti Chiave

- Gli hardware wallet sono essenziali soprattutto per i meno esperti
- Un'entropia adeguata è cruciale per la sicurezza
- Le soluzioni open source garantiscono trasparenza
- Diverse soluzioni per diverse esigenze
  - Qualcuno preferisce fare senza, non è un problema ma sono richieste conoscenze maggiori

True Random Mnemonic Generator (TRMG)

Dado D8

Dado D16

- Dadi Necessari:
  - 1× D8 (Primo dado)
  - 2× D16 (Secondo & Terzo dado)
- Processo:
  - Lancia tutti i 3 dadi 12/24 volte
  - Consulta tabella TRMG
- Indice = (Primo-1)$\times 2^8 + (Secondo - 1)2^4 + (Terzo - 1)$

Esempio TRMG

Words table

First	Second	Third	Index	Word	Index in binary	Group 12	Group 24
1	1	1	0	abandon	00000000000	0000000	000
1	1	2	1	ability	00000000001	0000000	000
1	1	3	2	able	00000000010	0000000	000
1	1	4	3	about	00000000011	0000000	000
1	1	5	4	above	00000000100	0000000	000
1	1	6	5	absent	00000000101	0000000	000
1	1	7	6	absorb	00000000110	0000000	000

Tabella di Consultazione TRMG

Lancio di Esempio

- Primo (D8) = 1
- Secondo (D16) = 1
- Terzo (D16) = 1
- → Indice = 0
- Parola = "abandon"

Panoramica Processo TRMG

Per 12/24 parole:

- Lancia i dadi
- Consulta la tabella
- Calcola l'indice
- Seleziona la parola

Fix dell'ultima parola. Usa un hardware wallet per calcolare o testare tutte le possibili ultime parole che sono ottenibili:

- 12 parole: Controlla Pil gruppo formato dal primo & secondo dado

  24 parole: Controlla il gruppo formato dal solo lancio del primo dado

Migliori Pratiche TRMG

- Considerazioni Importanti:
  - Usa dadi di alta qualità, equa
  - Lancia su superficie pulita, piana
  - Assicurati privacy durante generazione
  - Distruggi qualsiasi record cartaceo
- Passaggi di Verifica:
  - Registra parole attentamente
  - Raddoppia controlla ogni parola
  - Testa piccola quantità prima
  - Crea backup sicuri

Backup su Metallo - SAFU Ninja

SAFU Ninja Plate

Vantaggi del Backup su Metallo:

- Resistente al fuoco
- Resistente all'acqua
- Durata nel tempo
- Resistente agli urti

Processo SAFU Ninja:

- Punzonatura lettere su metallo
- Nessuna pre-marcatura delle parole
- Design anti-tamper
- Kit completo di strumenti

Progetto Satoshi Spritz

- Federazione di gruppi locali di Bitcoiner
- Eventi gratuiti e privacy oriented
- BITCOIN ONLY
- Satoshi Spritz Connect online settimanale
- Orientato all'apprendimento della self-sovereign

satoshispritz.it

Officine Bitcoin

- Comunità Italiana di Bitcoiners, totalmente gratuita
- BITCOIN ONLY
- Focus su educazione e sviluppo di progetti
- Progetti:
  - Sviluppo nodi Bitcoin
  - Uso di Hardware Wallet
  - Filosofia open source
  - Installazione di Debian
    - ... e molto altro

officinebitcoin.it

? Domande?

👍 Grazie per l'attenzione!

✉ Contatti: https://t.me/valeriovaccaro