CHAOS IS SECURITY

Workshop di Entropia & Jade Giveaway

Satoshi Spritz Cagliari

15 dicembre 2025

Atto I: La Filosofia dell'Entropia

Il Paradosso della Fiducia

"Perché generare le parole a mano se il mio hardware wallet lo fa in 1 secondo?"

- Se usi un software, ti stai fidando del programmatore.
- Se usi un hardware, ti stai fidando del chip (RNG).
- **Se usi i dadi, ti fidi solo della gravità.**

PRNG vs TRNG

PRNG (Computer)

Pseudo-Random Number Generator

I computer sono macchine deterministiche. Non sanno "inventare". Usano algoritmi che *sembrano* casuali.

Rischio: Se l'algoritmo è bacato, la chiave è prevedibile.

TRNG (Fisica)

True Random Number Generator

Il mondo fisico è caos puro.

Lancio di dadi, rumore atmosferico, decadimento radioattivo.

Vantaggio: Imprevedibile per chiunque.

Atto II: Generazione Mnemonica

Il Nostro Obiettivo

Generare le prime **11 parole** (su 12) usando l'entropia fisica.

Vedremo 3 protocolli operativi per estrarre numeri tra 1 e 2048.

Metodo 1: Dadi D6 (Protocollo Binario)

Strumenti: 11 Dadi comuni (D6) lanciati insieme.

Passo 1: Conversione Bit

Ogni dado è un bit.

- **Pari** (2,4,6) $\rightarrow$ **0**
- **Dispari** (1,3,5) $\rightarrow$ **1**

Passo 2: La Somma

Ogni posizione ha un valore (Potenze di 2).
Sommiamo i valori dove è uscito **1**.

Esempio Calcolo D6

Lancio 11 dadi. Mettiamoli in fila e calcoliamo:

Potenza	**1024**	**512**	**256**	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
Lancio	D	P	P	D	P	P	D	P	P	D	D
Bit	**1**	0	0	**1**	0	0	**1**	0	0	**1**	**1**
Valore	1024	-	-	128	-	-	16	-	-	2	1

$$\textit{Somma} = 1024 + 128 + 16 + 2 + 1 = \mathbf{1171}$$

$$\mathbf{1171} + 1 = \text{Parola } \#1172 \text{ nella lista} \rightarrow \textit{"Mystery"}$$

(Nota: La lista BIP39 parte da 1, il calcolo da 0, quindi aggiungiamo +1)

Metodo 2: Urna (Targhette 3D)

Strumenti: Barattolo con 1024 targhette a doppia faccia.
(Totale 2048 parole stampate)

1. **Mischiare** vigorosamente.
2. **Estrarre** una targhetta.
3. **Leggere** la parola (Faccia A o B? Lanciare moneta o scegliere a priori).
4. **CRUCIALE: Rimettere la targhetta dentro!**

Attenzione

Se non rimetti la targhetta dentro, alteri la probabilità delle estrazioni successive (Entropia viziata).

Metodo 3: Precisione RPG (TRGM)

Strumenti: 1 Dado D8 + 2 Dadi D16.

Metodo sviluppato da *Officine Bitcoin*.

(TRGM = True Random Mnemonic Generator)

La Logica

Il dizionario ha 2048 parole.

$$2048 = 8 \times 16 \times 16$$

Ogni combinazione di dadi punta a una coordinata esatta.

Esempio Calcolo TRGM

Formula: $[(D8 - 1) \times 256] + [(D16_A - 1) \times 16] + (D16_B - 1) + 1$

Il Lancio (Esempio "Bacon"):

- D8 (Settore): Esce **1**
- D16 A (Riga): Esce **9**
- D16 B (Colonna): Esce **11**

Il Calcolo:

$$(0 \times 256) = 0$$

$$+(8 \times 16) = 128$$

$$+(10) = 10$$

$$0 + 128 + 10 + 1 = \mathbf{139}$$

Parola #139 nella lista BIP39 $\rightarrow$ **"Bacon"**

Atto III: II Checksum & Jade

Come calcoliamo l'ultima parola?

Abbiamo 11 parole (caos). Ci serve la 12a per "chiudere" il wallet.
La 12a parola contiene il **Checksum** (algoritmo SHA-256).

Abbiamo 3 strade per calcolarlo:

1. Hardcore (A Mano)

Carta, penna e calcoli binari su SHA-256.

Difficoltà: Estrema
Tempo: Ore
Rischio: Errore umano certo.

2. Software (Tails)

Computer con OS Linux Tails (senza rete).

Difficoltà: Alta
Tempo: 15 min
Rischio: Malware o errori di setup.

3. Hardware (Jade)

Il device agisce da calcolatrice isolata.

Difficoltà: Bassa
Tempo: 30 sec
Rischio: Molto basso (Air-gapped).

Il Dilemma: 12 o 24 Parole?

La lunghezza del seed cambia la sicurezza (Entropia) ma anche la dimensione del controllo finale (Checksum).

12 Parole (Standard)

Entropia: 128 bit

(Sicurezza oltre ogni scala umana)

Opzioni ultima parola:

Il checksum è leggero (4 bit).

128 Parole Valide

(su 2048)

24 Parole (Paranoid)

Entropia: 256 bit

(Sicurezza militare / Futuro)

Opzioni ultima parola:

Il checksum è severo (8 bit).

Solo 8 Parole Valide

(su 2048)

Più parole hai, più il checksum diventa selettivo e la lista finale si accorcia.

12 vs 24: Sicurezza o Comodità?

Il Mito della "Maggiore Sicurezza"

Lato crittografia, **12 parole bastano**.
Indovinare 2^{128} combinazioni è impossibile quanto indovinarne 2^{256}.
Allora perché usare 24 parole?

Vantaggi 12 Parole (UX)

- ✓ Veloci da scrivere e verificare.
- ✓ Meno spazio su acciaio/carta.
- ✗ **Non divisibili:** Se dividi il seed (6+6) e ne trovano metà, le altre 6 si trovano con un PC potente.

Vantaggi 24 Parole (OpSec)

- ✗ Lunghe e noiose da gestire.
- ✓ **Divisibili:** Se dividi il seed (12+12) in due case diverse e ne trovano metà...
  ...mancherebbero ancora 12 parole (che sono inviolabili)!

Nerd Bonus: Cosa succede "sotto il cofano"?

Molti pensano che 12 parole generino una chiave più "corta".

Lo Standard Bitcoin (secp256k1)

La matematica di Bitcoin usa la curva ellittica **secp256k1**.

Questa richiede che la chiave privata sia **sempre** un numero di 256 bit.

Input: 12 Parole

Entropia: 128 bit

↓ (PBKDF2)

↓ **Chiave Finale: 256 bit**

La chiave è lunga uguale, ma ha **128 bit di forza reale**.

Input: 24 Parole

Entropia: 256 bit

↓ (PBKDF2)

↓ **Chiave Finale: 256 bit**

La chiave è lunga uguale e ha **256 bit di forza reale**.

In entrambi i casi, il "contenitore" finale è identico (256 bit).

Il Ruolo del Jade: "Calcolatrice Blindata"

Come trasformiamo 11 parole casuali in un Wallet sicuro?

1. Input (Noi)

Inseriamo le **11 parole** generate coi dadi.

(Entropia Incompleta)

→

2. Filtro (Jade)

Il chip calcola il checksum su tutte le 2048 opzioni.

(Matematica)

→

3. Selezione

Ci mostra la **lista** delle parole valide. **Ne scegliamo una.**

(Wallet Creato!)

VANTAGGIO: Il Jade impedisce l'errore umano, garantendo un wallet matematicamente valido.

Anatomia della 12a Parola

Perché il Jade ci mostra una lista di parole e non una sola?

Il Segreto della Parola 12

La 12a parola non è puro Checksum. È un **Ibrido**.

ENTROPIA (7 bit)	CHECKSUM (4 bit)
Decisa da noi (Scelta Finale)	*Calcolata dal Jade*

- Noi forniamo 11 parole $\rightarrow$ Mancano 7 bit di entropia.
- Il Jade prova tutte le combinazioni ($2^7 = 128$ parole).
- Solo quelle col checksum corretto (4 bit) vengono mostrate.
- **A noi spetta la scelta finale tra le opzioni valide.**

L'Ultima Scelta: Caso 12 Parole

Situazione: Checksum piccolo (4 bit).
Lista Jade: 128 Parole (2^7 opzioni valide).

Metodo A (Dadi RPG)

Usa **D8** (Blocco) + **D16** (Riga).

Formula: $[(D8 - 1) \times 16] + D16$

Un solo lancio definisce il numero tra 1 e 128.

Metodo B (Universale)

Servono **7 bit** ($2^7 = 128$).

- Lancia **7 Monete** (o Dadi D6).
- Converti Binario $\rightarrow$ Decimale.
- Aggiungi $+1$ per trovare la riga.

L'Ultima Scelta: Caso 24 Parole

Situazione: Checksum grande (8 bit).
Lista Jade: Solo **8 Parole** (2^3 opzioni valide).

Metodo A (Dado D8)

Hai esattamente 8 opzioni.

- Lancia un solo **Dado D8**.
- Il numero che esce è la parola da scegliere.

Metodo B (Universale)

Servono **3 bit** ($2^3 = 8$).

- Lancia **3 Monete** (T=1, C=0).
- Esempio: $101_2 = 5$.
- Seleziona la 6a parola ($5 + 1$).

Con 24 parole il cerchio si stringe moltissimo!

Le Regole d'Oro della Sicurezza

Prima di lasciarvi al contest, ricordate:

DA FARE ✓

- Usare sempre **dadi fisici**.
- Scrivere il seed su **carta** o **acciaio**.
- Fare **multipli backup** in luoghi diversi.
- Verificare il checksum col Jade (Offline).

DA EVITARE ✗

- **MAI** fare foto alle parole.
- **MAI** scriverle sul PC/Note/Cloud.
- **MAI** inserirle in un sito web.
- Non fidarsi di software non verificati.

Atto IV: II Contest

Il Patto d'Onore

Il Jade non è un regalo. È una responsabilità.

L'Obbligo del Vincitore

Chi vince stasera si impegna a:

- Studiare il dispositivo a casa.
- Tornare al prossimo Satoshi Spritz.
- **Fare una demo pratica** o raccontare le proprie impressioni d'uso (recensione).

Se non accetti questa condizione, per favore non partecipare al quiz.

Win a Jade

Le Regole del Gioco:

- Premi **Answer This Quiz** e digita il **Game PIN**.
- 10 domande totali.
- Ogni domanda avrà un timer di **30 secondi**.
- Vince chi risponde correttamente al maggior numero di domande (in caso di pareggio vince il più veloce).

Scansiona per partecipare
https://quiz.satoshispritz.it/quiz/442d2e51

Rimaniamo in Contatto

SATOSHI SPRITZ

Grazie a tutti per la partecipazione!

SS Cagliari

Sito Web

SS Connect

Officine Bitcoin