Lanzamientos y cálculo

128 lanzamientos, uno por casilla, en orden: 1A → 1K, 2A → 2K… hasta 12G. Las casillas rayadas (12H–12K) son el checksum: no se lanzan. Debajo de cada casilla está su valor; tacha los valores de las casillas con 0 y suma los que quedan.

CONTIENE SECRETOS Esta hoja reconstruye tu semilla. Sin cámaras ni teléfonos cerca. Al terminar, quémala.

Cara vale _____ Reverso vale _____ Lista usada: ☐ numerada desde 0 ☐ desde 1 (suma +1 al índice)

Nº	A	B	C	D	E	F	G	H	I	J	K	A–C	D–G	H–K	Índice	Palabra
01	1A	1B	1C	1D	1E	1F	1G	1H	1I	1J	1K					
	1024	512	256	128	64	32	16	8	4	2	1					
02	2A	2B	2C	2D	2E	2F	2G	2H	2I	2J	2K					
	1024	512	256	128	64	32	16	8	4	2	1					
03	3A	3B	3C	3D	3E	3F	3G	3H	3I	3J	3K					
	1024	512	256	128	64	32	16	8	4	2	1					
04	4A	4B	4C	4D	4E	4F	4G	4H	4I	4J	4K					
	1024	512	256	128	64	32	16	8	4	2	1					
05	5A	5B	5C	5D	5E	5F	5G	5H	5I	5J	5K					
	1024	512	256	128	64	32	16	8	4	2	1					
06	6A	6B	6C	6D	6E	6F	6G	6H	6I	6J	6K					
	1024	512	256	128	64	32	16	8	4	2	1					
07	7A	7B	7C	7D	7E	7F	7G	7H	7I	7J	7K					
	1024	512	256	128	64	32	16	8	4	2	1					
08	8A	8B	8C	8D	8E	8F	8G	8H	8I	8J	8K					
	1024	512	256	128	64	32	16	8	4	2	1					
09	9A	9B	9C	9D	9E	9F	9G	9H	9I	9J	9K					
	1024	512	256	128	64	32	16	8	4	2	1					
10	10A	10B	10C	10D	10E	10F	10G	10H	10I	10J	10K					
	1024	512	256	128	64	32	16	8	4	2	1					
11	11A	11B	11C	11D	11E	11F	11G	11H	11I	11J	11K					
	1024	512	256	128	64	32	16	8	4	2	1					
12	12A	12B	12C	12D	12E	12F	12G	12H	12I	12J	12K				Z1	
	1024	512	256	128	64	32	16	cs	cs	cs	cs					NO ES LA PALABRA 12 → HOJA 2

Ceros contados _____ de 128

Cuenta los tachones. Debe dar entre **50 y 78** (el 99 % de las series honestas cae ahí). Si no, destruye esta hoja y empieza de nuevo.

Unos contados _____ ceros + unos = 128

Si la suma no da 128, omitiste o repetiste una casilla. Revisa fila por fila antes de seguir.

La palabra 12 y la verificación

Los 7 lanzamientos de la fila 12 dejan 16 palabras posibles. Solo una cumple el checksum, y la calcula una wallet. Después, comprueba que la frase restaura exactamente la misma wallet.

CONTIENE SECRETOS Junto con la hoja 1, esta hoja permite robar tus bitcoin. Quémala al terminar.

Las 16 candidatas

Z1 (índice de la fila 12) = _____ Bloque = Z1 ÷ 16 = _____

En la lista de Soberanía Satoshi, copia el bloque entero.

+	ÍNDICE	PALABRA	VÁLIDA
+0			☐
+1			☐
+2			☐
+3			☐
+4			☐
+5			☐
+6			☐
+7			☐

+	ÍNDICE	PALABRA	VÁLIDA
+8			☐
+9			☐
+10			☐
+11			☐
+12			☐
+13			☐
+14			☐
+15			☐

Palabra 12 elegida por la wallet _____

Verificación

WALLET O HERRAMIENTA USADA

FINGERPRINT (8 CARACTERES)

☐☐☐☐☐☐☐☐

PRIMERA DIRECCIÓN DE RECEPCIÓN (M/84'/0'/0'/0/0, EMPIEZA POR BC1Q)

☐ Borré la wallet de prueba, volví a introducir las 12 palabras y el fingerprint coincide.

☐ La primera dirección de recepción coincide carácter por carácter.

Antes de cerrar

☐ Copié las 12 palabras en la tarjeta de respaldo (o en metal) y las comparé de nuevo con la hoja 1.

☐ Borré la wallet de prueba o la dejé lista para cargar la semilla definitiva.

☐ Quemé las hojas 1 y 2 y cualquier borrador. La hoja 3 no tiene secretos.

Guía rápida y tablas de suma

Cada fila de 11 lanzamientos es un número binario entre 0 y 2047. En lugar de sumar 11 valores, divide la fila en tres grupos y busca cada grupo en su tabla.

SIN SECRETOS Esta hoja no contiene datos tuyos. Puedes conservarla para la próxima vez.

A–C · 1024 512 256

BITS	VALOR
000	0
001	256
010	512
011	768
100	1024
101	1280
110	1536
111	1792

D–G · 128 64 32 16

BITS	VALOR
0000	0
0001	16
0010	32
0011	48
0100	64
0101	80
0110	96
0111	112

BITS	VALOR
1000	128
1001	144
1010	160
1011	176
1100	192
1101	208
1110	224
1111	240

H–K · 8 4 2 1

BITS	VALOR
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7

BITS	VALOR
1000	8
1001	9
1010	10
1011	11
1100	12
1101	13
1110	14
1111	15

Ejemplo · fila 00110100111 → A–C 001 = 256 · D–G 1010 = 160 · H–K 0111 = 7 → índice 423 = «crunch» (lista desde 0) · línea 424 en english.txt

Fila 12: solo existen A–G. Z1 = (A–C) + (D–G); el número de bloque es Z1 ÷ 16 y coincide con los 7 bits leídos como número de 0 a 127. Las 16 candidatas son Z1, Z1+1… Z1+15.

El procedimiento en 9 pasos

01 Prepara el lugar
Sin cámaras, webcams ni teléfonos en la habitación. No digas los resultados en voz alta.

02 Asigna valores
Anota qué lado vale 1 y cuál 0. Mantén la regla hasta el final.

03 Lanza 128 veces
Agita la moneda entre las manos antes de cada tirada, lánzala alto y déjala caer sobre la mesa. Anota en orden.

04 Comprueba los ceros
Entre 50 y 78 ceros, y ceros + unos = 128. Si no, hoja nueva.

05 Suma cada fila
Con las tablas de esta hoja: (A–C) + (D–G) + (H–K) = índice. +1 solo si tu lista empieza en 1.

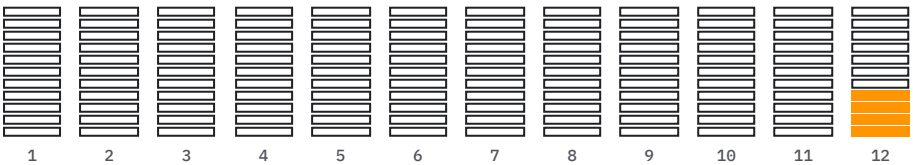
06 Busca las 11 palabras
Compara también los bits de la fila con los que trae la lista: si no coinciden, hay un error de suma.

07 Calcula la palabra 12
Z1 = (A–C) + (D–G) de la fila 12. Copia su bloque de 16 palabras y deja que la wallet elija la única válida.

08 Verifica
Anota el fingerprint y la primera dirección. Borra, restaura y comprueba que coinciden.

09 Respalda y destruye
Pasa las palabras a la tarjeta o al metal. Quema las hojas 1 y 2.

Por qué salen 12 palabras



128 bits de moneda + 4 bits de checksum = 132 bits = 12 palabras de 11 bits. El checksum son los 4 primeros bits del SHA-256 de tus 128 bits: no se puede calcular a mano con comodidad, por eso lo calcula la wallet.