Semilla moneda - 12 palabras

v01 - 10/08/2026 - 100% a mano

por @lunaticoin

Nombre: _____

XFP: _____

Con 128 lanzamientos de moneda y esta hoja conseguirás las doce palabras de una frase mnemónica BIP-39. Aquí la moneda es quien decide la entropía, no tu hardware wallet. Lo único que no puedes calcular a mano es la última palabra que exige practicar un SHA-256. Calcula ahora las 11 primeras + los 7 bits A-G de la 12:

	2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**
Fila 1											
	1024	512	256	128	64	32	16	8	4	2	1
Fila 2											
	1024	512	256	128	64	32	16	8	4	2	1
Fila 3											
	1024	512	256	128	64	32	16	8	4	2	1
Fila 4											
	1024	512	256	128	64	32	16	8	4	2	1
Fila 5											
	1024	512	256	128	64	32	16	8	4	2	1
Fila 6											
	1024	512	256	128	64	32	16	8	4	2	1
Fila 7											
	1024	512	256	128	64	32	16	8	4	2	1
Fila 8											
	1024	512	256	128	64	32	16	8	4	2	1
Fila 9											
	1024	512	256	128	64	32	16	8	4	2	1
Fila 10											
	1024	512	256	128	64	32	16	8	4	2	1
Fila 11											
	1024	512	256	128	64	32	16	8	4	2	1
Fila 12								C	h	e	c	k	s	u	m
bit 128	1024	512	256	128	64	32	16				

Cálculos rápidos

1024 + 512 =	**1536**
1024 + 256 =	**1280**
1024 + 128 =	**1152**
1024 + 64 =	**1088**
512 + 256 =	**768**
512 + 128 =	**640**
512 + 64 =	**576**
512 + 32 =	**544**
256 + 128 =	**384**
256 + 64 =	**320**
256 + 32 =	**288**
256 + 16 =	**272**
128 + 64 =	**192**
128 + 32 =	**160**
128 + 16 =	**144**
128 + 8 =	**136**
64 + 32 =	**96**
64 + 16 =	**80**
64 + 8 =	**72**
32 + 16 =	**48**
32 + 8 =	**40**

Cálculos		Suma	¿+1?	Palabra
1	=			
2	=			
3	=			
4	=			
5	=			
6	=			
7	=			
8	=			
9	=			
10	=			
11	=			
Z1	=			sigue en la tabla de abajo

12 la definitiva, una vez encontrada

LA PALABRA 12 · LAS 16 CANDIDATAS

Has obtenido 11 palabras y un valor **Z** de los primeros 7 bits A-G de la palabra 12. Las columnas tapadas (H, I, J y K) son los pesos 8, 4, 2 y 1 que desconocemos. Sumen lo que sumen, el resultado estará entre 0 y 15. Así que hay 16 resultados candidatos que además son **16 palabras consecutivas del diccionario**: ponte en la línea Z1 de tu lista impresa y copia las 16 siguientes, en orden. Ahora verifica 1 a 1 en tu hardware wallet cuál es la palabra correcta:

	Z1 +	PALABRA CANDIDATA	HIJK
Z1	0		0000
Z2	1		0001
Z3	2		0010
Z4	3		0011
Z5	4		0100
Z6	5		0101
Z7	6		0110
Z8	7		0111

	Z1 +	PALABRA CANDIDATA	HIJK
Z9	8		1000
Z10	9		1001
Z11	10		1010
Z12	11		1011
Z13	12		1100
Z14	13		1101
Z15	14		1110
Z16	15		1111

Si tu lista está numerada desde 1, empieza a copiar en la casilla **¿+1?** en vez de en la Suma: el +1 se aplica una sola vez, a Z1. Exactamente una de las 16 tiene el checksum bueno. Pruébalas todas en tu hardware wallet. Tacha las que no sean y marca con un círculo la que sí. Rellena la palabra 12 de la rejilla de arriba cuando la encuentres.

INSTRUCCIONES - ANTES DE EMPEZAR

Hazlo solo, sin conexión y sin que nadie mire. Tapa todas las cámaras de la habitación, incluidas las del portátil y el móvil. Desenchufa los asistentes de voz o sácalos de la sala. No uses ninguna calculadora que esté conectada a algo: la chuleta de cálculos rápidos está para no necesitarla. Y haz un ensayo con una frase de usar y tirar antes de la buena, para equivocarte cuando todavía no hay dinero de por medio.

PROCEDIMIENTO

1. Elige qué cara de la moneda vale **0** y cuál vale **1**, y no lo cambies hasta el final.
2. Lanza la moneda y anota el resultado en la casilla **Fila 1-A**. Sigue lanzando y rellenando hacia la derecha hasta completar la fila: **once casillas, de la A a la K**.
3. Rellena así las once primeras filas enteras y, en la **fila 12**, solo de la **A a la G**. Son **128 lanzamientos** en total.
4. Con los lanzamientos hechos, tacha el número gris que hay debajo de cada casilla donde haya un **0**. Donde haya un 1 no hagas nada.
5. **Verifica la tirada.** Cuenta los tachones, que son tus ceros: deben salir **entre 50 y 78**. Le pasa al 99% de las tiradas honestas y es el umbral del estándar NIST. Si te sales de ahí, lo más probable es un error de conteo o de técnica: revisa y repite. No avances si quedaste fuera.
6. Fila por fila, anota en su línea de **Cálculo** los números grises que hayan quedado sin tachar y súmalos. Apóyate en la chuleta de **Cálculos rápidos**. Las filas 1 a 11 te dan las palabras 1 a 11; la fila 12 te da **Z1**, el pre-cálculo de la 12. Seguiremos con esto en el punto 8.
7. Ahora busca cada **Suma** de las filas 1 a 11 en una lista BIP-39 impresa **[0] [1]** y anota la palabra que corresponda. **Si tu lista está numerada desde el 1 en vez de desde 0**, súmale 1 a la suma, anota el resultado en la casilla **¿+1?** y busca el número resultante en la lista.
8. Haz lo mismo con **Z1**: súmale 1 si tu lista empieza en 1. Ponte en esa línea de la lista y copia a la tabla de candidatas las 16 palabras que vienen a partir de ahí, en el mismo orden. Son 16 líneas seguidas: no hay que calcular nada.
9. Averigua cuál es la buena con una hardware wallet, como se explica aquí debajo, y anótala como palabra 12 debajo de Z1, el pre-cálculo.
10. Comprueba la frase entera antes de meter dinero: carga las doce palabras y apunta la huella maestra y la primera dirección.
11. **Destruye esta hoja o guárdala en una bolsa de evidencias opaca y seriada como backup de tu frase.** Rellena es tu frase mnemónica a la vista, en binario, en decimal y en palabras. Guárdala bien o quémala. No le hagas una foto. No la teclees en un ordenador conectado a nada.

CÓMO ENCONTRAR LA PALABRA BUENA

Si tu aparato solo admite finales válidas (COLDCARD Mk4, Mk5 y Q, SeedSigner, Krux, BitBox02, Nova) no hay que probar nada. Unas te ofrecen la lista de las 128 finales que cuadran, y solo una está entre tus 16 candidatas. Otras autocompletan mientras escribes: empieza por la primera de tus 16 y, si la propuesta se sale de la horquilla, borra la última letra y prueba con la siguiente letra distinta de tu lista.

Si solo acepta o rechaza la frase entera (COLDCARD Mk3 y la mayoría de carteras software) teclea las once palabras más la primera candidata y mira si la acepta; si la rechaza, baja por la lista de Z1 a Z16. Como mucho 16 intentos, ocho de media.

POR QUÉ ESTA VERSIÓN

Cuando completas 11 palabras en tu hardware wallet, le das 121 bits y ésta se inventa los 7 que faltan para completar la última palabra. Aquí no pone ninguno: los 128 son tuyos. El aparato solo hace de árbitro y te dice cuál de las 16 candidatas cuadra con el checksum. Si su generador de aleatoriedad estuviera roto, que es lo que les pasó a las COLDCARD en julio de 2026, daría exactamente igual. Tu frase mnemónica de 12 palabras habrá salido de una moneda. No de un chip defectuoso.

La diferencia práctica es pequeña: aunque el aparato eligiera esos 7 bits de la peor manera posible, a un atacante le seguirían quedando 121 bits por delante, que es muchísimo más de lo que nadie va a recorrer nunca. Esta versión no es más segura pero es la que no le debe nada a nadie. Cuesta 7 lanzamientos más y, según el aparato, hasta 16 intentos. **YOUR** keys, your coins. TUS claves, tus monedas.

ANTES DE METER DINERO

Carga la frase en una hardware wallet sin conexión y copia aquí su fingerprint XFP y primera dirección de recepción. Borra la hardware wallet y verifica que eres capaz de volver a dar con la misma fingerprint y dirección:

Huella maestra (XFP) _____

Primera dirección de recepción _____

Y después destruye la hoja o guárdala bien en una bolsa de evidencia seriada y opaca. Paso 11.