

por @lunaticoin

12/10/2020

Este documento es una **pauta para ayudarte a crear tu propia semilla bitcoin** con tan solo esta hoja de papel, un bolígrafo y una moneda. Para calcular la última palabra necesitarás algún tipo de hardware también: SpecterDIY, o ordenador offline. La finalidad de este método es conseguir una semilla con una buena entropía sin tener que confiar en ningún generador de entropía de software y hardware wallets.

Puedes leer sobre cómo rellenar esta ficha y conseguir tu semilla con buena entropía leyendo el procedimiento de la segunda hoja. También puedes ampliar contexto con el artículo relacionado que publiqué en Estudio Bitcoin bit.ly/semilla-monedas

	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											
bit 128	1024	512	256	128	64	32	16	8	4	2	1
Fila 13											
	1024	512	256	128	64	32	16	8	4	2	1
Fila 14											
	1024	512	256	128	64	32	16	8	4	2	1
Fila 15											
bit 160	1024	512	256	128	64	32	16	8	4	2	1
Fila 16											
	1024	512	256	128	64	32	16	8	4	2	1
Fila 17											
	1024	512	256	128	64	32	16	8	4	2	1
Fila 18											
bit 192	1024	512	256	128	64	32	16	8	4	2	1
Fila 19											
	1024	512	256	128	64	32	16	8	4	2	1
Fila 20											
	1024	512	256	128	64	32	16	8	4	2	1
Fila 21											
bit 224	1024	512	256	128	64	32	16	8	4	2	1
Fila 22											
	1024	512	256	128	64	32	16	8	4	2	1
Fila 23											
	1024	512	256	128	64	32	16	8	4	2	1
Fila 24											
bit 256	1024	512	256	128	64	32	16	8	4	2	1

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	

PROCEDIMIENTO:

1. Asocia un valor '0' a una cara de la moneda y un valor '1' a la otra.
2. Lanza la moneda y anota el resultado obtenido (0 o 1) en la casilla '**Fila1-A**'. Vuelve a lanzarla consecutivamente hasta completar la **Fila 1** (de A a J).
3. Sigue lanzando la moneda para completar ahora la **Fila 2** (de A a J) y sigue haciéndolo hasta conseguir la entropía deseada (128, 160, 192, 224 o 256 bits para 12,15,18,21 o 24 palabras)
4. Cuando hayas conseguido rellenar la entropía deseada, tacha con una raya los números de color gris de debajo de cada casilla donde haya un 0. No hagas nada donde haya un 1.
5. En la línea de cálculo, ve anotando los valores correspondientes que hayan quedado sin tachar. Apóyate en la chuleta de cálculos rápidos para ir sumando números grandes con mayor velocidad.
6. Suma los valores y anota el resultado en la casilla '**Suma**'
7. **No** calcules la última palabra de la entropía seleccionada. Fila 12 para 128b, fila 15 para 160b, fila 18 para 192b, fila 21 para 224b y fila 24 para 256b.
8. Consigue una lista impresa de las palabras del BIP39
 - a. <https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt>
 - b. https://seedpicker.net/guide/SeedPicker_Lookup_Table.pdf
9. Si tu lista de palabras empieza por el número **0**, abandon
 - a. Busca los valores resultantes de la casilla '**Suma**' en la lista y anota la palabra en la **línea 'Palabra'**
10. Si tu lista de palabras empieza por el número **1**, abandon
 - a. Súmale 1 al resultado de la casilla 'Suma' y anota el resultado en la casilla '**¿+1?**'
 - b. Busca los valores resultantes de la casilla '**¿+1?**' en la lista y anota la palabra en la **línea 'Palabra'**
11. Para calcular la última palabra que en el punto 7 no calculaste:
 - a. Método seguro para entropías de 128, 192 y 256 bits:
 - i. Enciende tu [SpecterDIY](#) con versión superior a 1.4.0
 - ii. Haz click en 'Enter recovery phrase'
 - iii. Introduce tus 11,17 o 23 palabras
 - iv. añade una palabra 12, 18 o 24 aleatoria que te sugiera la Specter
 - v. Haz click en el botón 'fix' que te aparecerá. Acto seguido SpecterDIY te modificará esa última palabra inventada por la correcta para tu semilla.
 - vi. Anóta tu última palabra en esta pauta.
 - b. Para otros métodos ir a artículo de EstudioBitcoin.
12. Felicidades, acabas de calcular tu mismo tu propia semilla, con buena entropía y 100% offline, sin confiar en ningún generador de números aleatorios.
13. Ahora te toca almacenarla con seguridad. Te sugiero que la guardes en metal siguiendo la guía de [Blockmit](#).

Si esta **Semilla Moneda** te ha ayudado a entender un poco mejor a Bitcoin te agradecería que lo compartieras por twitter, linkedin o la red social que utilices.

Si te ha **encantado** te animo a que consideres dejarme una propina en <https://tallyco.in/lunaticoin/>