Schema seed - v1.0

Autore:

	2^10	2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0		RISULTATO DELLA SOMMA	PAROLA
	A	B	C	D	E	F	G	H	I	J	K	N°		

	1024	512	256	128	64	32	16	8	4	2	1		Risultato della somma	Parola
Es:	0	0	1	0	1	1	1	0	0	0	1	**256+64+32+16+1 = 369**	N° * 3 6 9	**C O M E**

	1024	512	256	128	64	32	16	8	4	2	1		Risultato della somma	Parola
1														
2														
3														
4														
5														
6														
7														
8														
9														
10														
11														
12												Checksum 128 - 4bits		
13														
14														
15												Checksum 160 - 5bits		
16														
17														
18												Checksum 192 - 6bits		
19														
20														
21												Checksum 224 - 7bits		
22														
23														
24												Checksum 256 - 8bits		

Questo documento è una linea guida per aiutarvi a creare il vostro SEED bitcoin con questo foglio di carta, una penna e una moneta. Per calcolare l'ultima parola è necessario anche dell'hardware: ColdCard o un computer offline. Lo scopo di questo metodo è quello di ottenere un seed con una buona entropia senza dover ricorrere a generatori di entropia da portafogli software e hardware.
Per sapere come compilare questo modulo e ottenere il vostro seed con una buona entropia, potete leggere la procedura riportata nel secondo foglio

PROCEDURA:

1. Associare il valore "0" a una faccia della moneta e il valore "1" all'altra.

2. Lanciare la moneta e registrare il risultato (0 o 1) nella casella "Riga 1-A". Continua a lanciare la moneta nuovamente fino a completare la fila 1 (da A a J).

3. Continuare a lanciare la moneta per completare la riga 2 (da A a J) e continuare a farlo finché non si ottiene l'entropia desiderata (128, 160, 192, 224 o 256 bit per 12,15,18,21 o 24 parole).

4. Dopo aver inserito l'entropia desiderata, tracciate un segno su tutti gli 0 in modo da eliminarli dal conteggio (potete anche non tracciare alcun segno purché vi ricordate di non considerare gli zeri). Solo i numeri 1 saranno validi per il calcolo.

5. Sulla riga del calcolo " RISULTATO DELLA SOMMA", scrivere il risultato della somma di tutti i valori 1 trovati nella stessa riga.

6. Non calcolare l'ultima parola dell'entropia selezionata. Riga 12 per 128b, riga 15 per 160b, riga 18 per 192b, riga 21 per 224b e riga 24 per 256b.

7. Ottenere un elenco stampato delle parole BIP39.

a. https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt | accesso con QR

8. Se il vostro elenco di parole inizia con il numero "0" > ABANDON, Trovate i valori risultanti dalla casella "Somma" nell'elenco e scrivete il valore parola nella riga "Parola

9. Se l'elenco delle parole inizia con il numero "1" > ABANDON, Aggiungere 1 al risultato nella casella "somma" e registrare il risultato aggiornato nella casella "parola". (NB: conviene controllare il tipo di elenco prima di scrivere il risultato della somma dei numeri per non dover rifare il calcolo)

10. Per calcolare l'ultima parola non calcolata ai punti precedenti potete sfruttare un tool come https://seedpicker.net/calculator/last-word.html OFFLINE o far suggerire al vostri hardware la parola corretta che sarà valida come checksum.

11. Congratulazioni, avete appena calcolato da soli il vostro seed, con una buona entropia e 100% offline, senza affidarsi ad alcun generatore di numeri casuali.

12. Ora tocca a voi conservarlo in modo sicuro. Vi suggerisco di conservarlo in un contenitore di metallo seguendo la guida di Blockmit o continuare nella lettura di questa guida.

Se questo Documento vi ha aiutato a capire un po' meglio il Bitcoin, vi sarei grato se voleste condividerlo su twitter, linkedin o qualsiasi altro social network che utilizziate.

Se vi è piaciuto, vi invito a lasciarmi un suggerimento e ad effettuare una donazione.

Autore **Lista bip39** **Seedpicker**