Schema seed - v1.0



Autore:

Section Sect		2^10 A	2^9 B	2^8	2^7 D	2^6 E	2^5 F	G	2^3 H	2^2	2^1	2^0 K				N°	RISULTATO	DELLA	SOMMA	PAROLA		
The control of the	_			256	128		32			4	2	1	_	_	_		Risultato	della so	omma	Parola		
1 1	Es:			1		1	1	1		0	0	1	256+64-	+32+16+1	= 369	N°					M E	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1																						
2 100 151 700 178 154 50 15 8 4 2 1 3 3 3 3 3 3 3 3 3	1	1024	512	256	128	64	32	16	8	4	2	1				1	Risultato	della so	omma	Parola		
Second Parallel	ı	1024	512	256	128	64	32	16	8	4	2	1					Risultato	della so	omma	Parola		
3	2	1024	E12	256	120	6.1	22	16	0			1					Disultato	dolla so		Darola		
1024 312 256 128 64 32 15 8 4 2 1	3	1024	512	250	120	04	52	10	0	4						3	RISUITATO	della sc	DITITIO	Parola		
1034 312 256 128 64 32 16 8 4 2 1	4	1024	512	256	128	64	32	16	8	4	2	1				4	Risultato	della so	omma	Parola	,	
Control Cont	4	1024	512	256	128	64	32	16	8	4	2	1				4	Risultato	della so	omma	Parola	,	
6	5	4004	[420											5						
Total St2 256 228 64 52 16 8 4 2 1	6	1024	512	256	128	64	32	16	8	4						6	RISUITATO	della so	omma	Parola		
1024 512 256 128 64 32 16 8 4 2 1 9 9 1 1 1 1 1 1 1		1024	512	256	128	64	32	16	8	4	2	1					Risultato	della so	omma	Parola	,	
9 Rivilato della somma Parola 10 1024 512 256 128 64 32 16 8 4 2 1 11 1025 512 256 128 64 32 16 8 4 2 1 11 1026 512 256 128 64 32 16 8 4 2 1 12 12 12 12 12 12		1024	512	256	128	64	32	16	8	4	2	1					Risultato	della so	omma	Parola		
9 1024 512 256 28 64 32 16 8 4 2 1 1024 512 256 28 64 32 16 8 4 2 1 112	8															8						
10 1024 512 256 128 64 32 16 8 4 2 1 1 1 1 1 1 1 1 1	9	1024	512	256	128	64	32	16	8	4	2	1				9	Risultato	della so	omma	Parola		
11		1024	512	256	128	64	32	16	8	4	2	1					Risultato	della so	omma	Parola		
11	10	1024	512	256	128	64	32	16	8	4	2	1				10	Risultato	della so	omma	Parola		
12	11															11					,	
13	12	1024	512	256	128	64	32	16	8	4	2	1	12	Checksum 128	- 4bits	12	Risultato	della so	omma	Parola		
1024 512 256 128 64 32 16 8 4 2 1 15	1 2	1024	512	256	128	64	32	16	8	4	2	1	12				Risultato	della so	omma	Parola	,	
14	13	1024	512	256	128	64	32	16	8	4	2	1				13	Risultato	della so	mma	Parola		
15	14															14						
16	1 5	1024	512	256	128	64	32	16	8	4	2	1		Checksum 160	- 5bits	15	Risultato	della so	omma	Parola	,	
17	1)	1024	512	256	128	64	32	16	8	4	2	1	13[Risultato	della so	omma	Parola		
17	16	1024	512	256	128	64	32	16	8		2	1				16	Risultato	della so	mma	Parola		
18	17															17				, 3, 0, 4		
19	10	1024	512	256	128	64	32	16	8	4	2	1	10	Checksum 192	- 6bits	10	Risultato	della so	omma	Parola		
20 Risultato della somma Parola 20 Risultato della somma Parola 21 Risultato della somma Parola	10	1024	512	256	128	64	32	16	8	4	2	1	10[10	Risultato	della so	omma	Parola		
20	19	1024	512	256	128	64	32	16	2	Δ	2	1				19	Risultato	della so	mma	Parola		
21 21 21 Risultato della somma Parola	20	1021			120											20	Tribatea Co			1 01010		
1024 512 256 128 64 32 16 8 4 2 1 Risultato della somma Parola	71	1024	512	256	128	64	32	16	8	4	2	1	21	Checksum 224	- 7bits	21	Risultato	della so	omma	Parola	•	
	Z I	1024	512	256	128	64	32	16	8	4	2	1	Z I [Z I [Risultato	della so	omma	Parola		
22	22	1024	E12	256	120	6.1	27	16	0	Л		1				22	Distribute	della sa	mm a	Darola		
23 Risultato della somma Parola 23 25 25 128 64 32 16 8 4 2 1	23	1024	JIZ	230	140	04	34	10	0	+		1				23	Nisuitato	della SC		FaIUld		
1024 512 256 128 64 32 16 8 4 2 1 Checksum 256 - 8bits Risultato della somma Parola	7 /	1024	512	256	128	64	32	16	8	4	2	1	24	Checksum 256	- 8bits	24	Risultato	della so	omma	Parola	,	

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