Making a BIP-39 key

BIP-39 is a globally recognised, standard way of representing your bitcoin keys as a series of simple words, commonly referred to as: "mnemonic phrase", "seed words", "mnemonic sentence" or "12 or 24 word backup".

We will perform and record coin flips, use the Hex lookup table below to produce a series of 3 digit hex codes, and then use the Mnemonic Words Lookup Book to produce our mnemonic phrase.

This key can be kept private, entered into a secure signing device, or entered into one of many popular digital bitcoin wallets depending on how you wish to use your key.

If you ever believe that your key has been compromised, be sure to transfer the bitcoin it protects to the protection of a new key. You can use this worksheet as many times as you need.

We will be creating a 12 word key. If you wish to create a 24 word key instead, you will need to create 24 rows, the last row will require only 3 flips and the companion device will the last two hex characters for your last word.

Hex lookup table

O O O O	0
O O O X	1
O O X O	2
O O X X	3
O X O O	4
O X O X	5
O X X O	6
O X X X	7

X O O O	8
X O O X	9
X O X O	A
X O X X	B
X X O O	C
X X O X	D
X X X O	E
X X X X	F

Every series of four coin flip results represents a single hex character.

Three hex characters represents a single hex code which can in turn represents a single word.

The last word of our mnemonic phrase relies on few coin flips, but also requires some additional computer generated data which we use the companion device to generate for us in a secure manner.

The additional data is known as a mathematical "checksum" that protects the integrity of the whole phrase. It acts like a digital tamper evident sticker if you mistype or accidentally re-order your words when entering this key into a Bitcoin wallet.

Instructions: Making a BIP-39 key

1. Draw or trace this worksheet onto a blank disposable piece of paper.

2. Flip a coin 128 times, recording heads as an O, and tails as an X each time in the "Coin flips" section below. *(11 flips per row, 7 flips on the last row, every row starts with an O for a total of 12 results per row)*

3. Use the "Hex lookup table" to fill the "Hex" section. *(The last row will have only 2 hex characters at this point)*

4. Enter the hex codes into your companion device in order to reveal the missing hex character on the last row.

5. Use the Mnemonic Words Lookup Booklet to map your hex codes and complete the "Words" section.

example:

0 X 0 X	X X X 0	0 X X 0	5 E 6	rubber

Coin flips			Hex	Words
0				
0				
0				
0				
0				
0				
0				
0				
0				
0				
0				
0				

Making an ephemeral key

An ephemeral key is one that was created, used, and then discarded with no recorded copy anywhere. Of course, a key that cannot be recalled later is pretty useless; we can combine multiple recorded keys to produce an ephemeral key that we can always reproduce.

A key that cannot be found recorded anywhere cannot be stolen and without additional information, a thief won't know how to reproduce it, nor which keys they need to reproduce it.

More details, as well as its use cases can be found in the bitcoin starter kit.

XOR map

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0 8	08	19	2A	3B	4C	5D	6E	7F	80	91	A2	B3	C4	D5	E6	F7
1 9	19	08	3B	2A	5D	4C	7F	6E	91	80	B3	A2	D5	C4	F7	E6
2 A	2A	3B	08	19	6E	7F	4C	5D	A2	B3	80	91	E6	F7	C4	D5
3 B	3B	2A	19	08	7F	6E	5D	4C	B3	A2	91	80	F7	E6	D5	C4
4 C	4C	5D	6E	7F	08	19	2A	3B	C4	D5	E6	F7	80	91	A2	B3
5 D	5D	4C	7F	6E	19	08	3B	2A	D5	C4	F7	E6	91	80	B3	A2
6 E	6E	7F	4C	5D	2A	3B	08	19	E6	F7	C4	D5	A2	B3	80	91
7 F	7F	6E	5D	4C	3B	2A	19	08	F7	E6	D5	C4	B3	A2	91	80

To use this map: look for your first character along the top to find the appropriate column. Then, find your second character along the left side of the table.

If your second character was underlined on the left column (0 - 7), cross reference and choose the underlined answer and if not, choose the other character as your answer.

e.g. **9** + **A** → B3 → 3 / **7** + **4** → 3B → 3

Hex character converter

8	9	A	B	C	D	E	F
0	1	2	3	4	5	6	7

Hex codes **must** start with a number from 0 - 7.

After combining two keys, the new code may need to be adjusted. Use this chart to replace the first character of any codes beginning with an invalid character.

e.g. EEF → 6EF / 0A3 → 0A3

Instructions: Making an ephemeral key

1. Draw or trace this worksheet onto a blank disposable piece of paper.

2. Write your first key's hex codes across the first row. *(exclude the last hex character)*

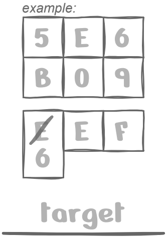
3. Write your second key's hex codes across the second row. *(exclude the last hex character)*

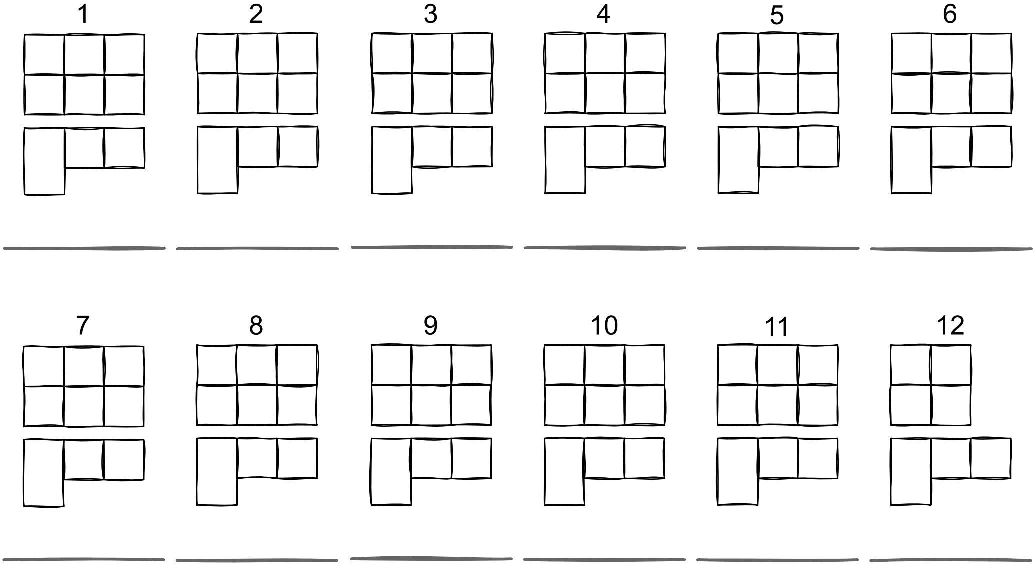
4. Use the "XOR map" to create a new set of hex codes.

5. Cross out and adjust the first character of any hex code that does not start with a number from 0 - 7. *(use the "Hex character converter")*

6. Enter the new hex codes into your companion device in order to reveal the missing hex character of the last block.

7. Use the mnemonic words booklet to map your hex codes to reveal the words for your ephemeral key.





Planning OPSEC

There is no such thing as perfect security, but it is both constructive and stress relieving to take some time and focus on your OPSEC (operational security).

OPSEC was first defined by the military during the Vietnam war and was defined as: “The ability to keep knowledge of our strengths and weaknesses away from hostile forces.”

Ultimately, we should be the only ones who know how we have created and are protecting our keys.

Creating a mobile wallet

- Key is ´hot´ - can be compromised
- Maximum amount I trust the wallet to hold: £100
- Software is open source on Github.com
- Recommended by a friend who is thinks a lot about technical security.
- I connected my phone to free public wifi

Creating a physical backup

- Likely disasters: flooding (yes), fire (yes), tornado (no)
- laminated paper: not fire resistant
- engrave steel plate: expensive?
- paper in safe: I´d need to buy a safe, not waterproof