Roll Your Own Bitcoin Seed Phrase

with @D_plus__plus

Slides by Keysa @SimplestBTCBook

MATERIALS NEEDED

Visit: entropy.page/dice

- Dice: x1 Octal (8-sided) di
  x2 Hex (16-sided) dice
- Printouts: BIP39 Worksheet
  BIP39 Word List
- Signing Device: Cold Card, Seed Signer or Jade
  (needed to calculate the checksum/last word offline)
- Pen
- Cup to roll the dice in
- Hard, flat surface, in a room free of all electronics.

IMPORTANT NOTE:

- I highly recommend doing a complete practice run, carefully following the instructions in this slide deck.
- Then when you are ready to do it ‘for real’, be sure to follow all the instructions on the following slide, to confirm you have the best security possible.
- If you think you will need to follow the instructions in this slide deck again, best practice would be to print or write them out, as you do not want any electronics of any kind in the room where you roll your seed phrase.
- The process is quite simple however, and you will probably not need the instructions the second time around.

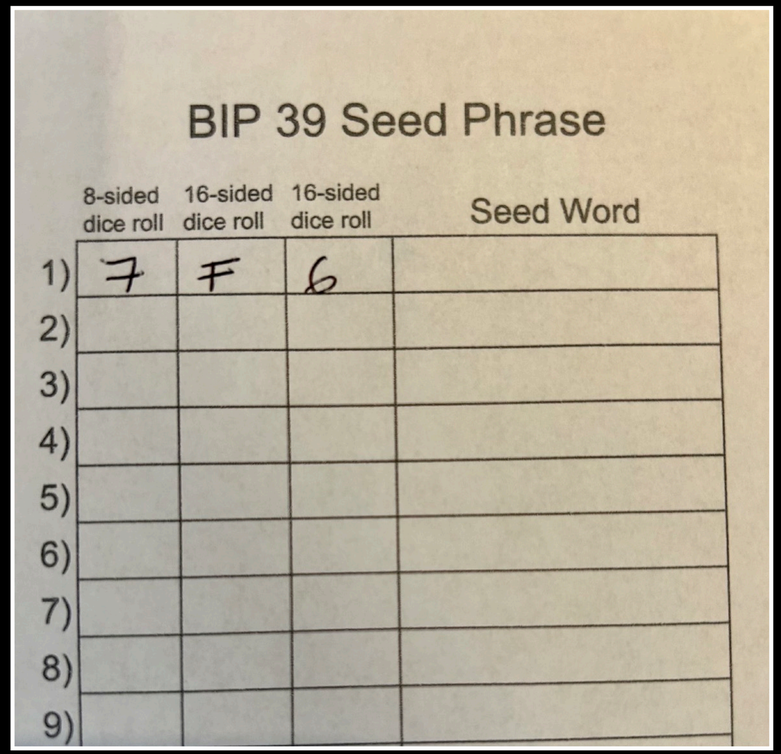
PREPARATION FOR ROLLING YOUR OWN SEED

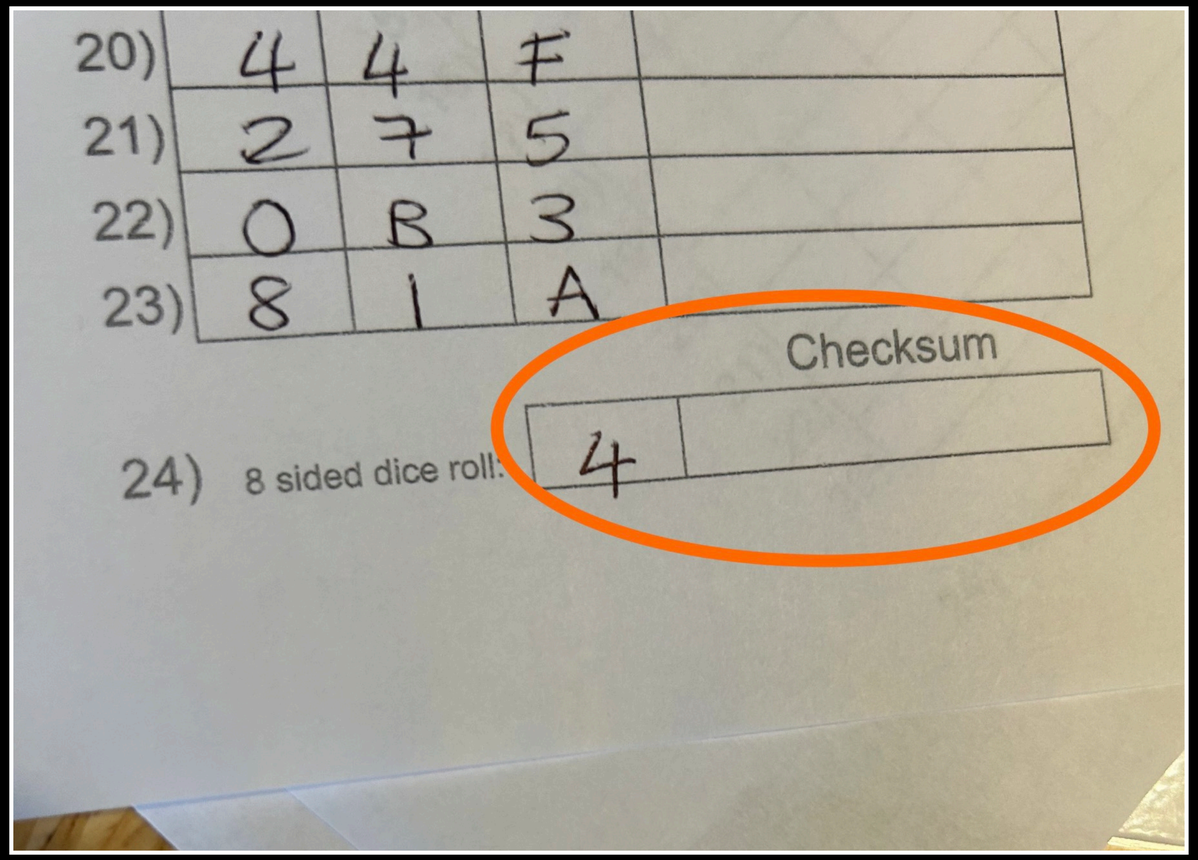
- Be sure to be in a room with no other electronics, and the shades drawn so no one can see in.
- Switch on the lights if needed.
- Let anyone else in the house know that you need to be undisturbed for an hour, ideally locking the door so no one accidentally comes in with a phone on.
- Since you are going to the trouble to roll your own seed, you want to be sure to be as secure and private as possible while doing so.
- Make sure you have a hard surface to roll the dice on. Using an empty box with a flat bottom can be helpful.
- Check that you have all the materials listed on the previous page ready and with you in the room.
- Ok great, let’s begin!

- Using a cup to shake the three dice, throw them down on the table or in the box.

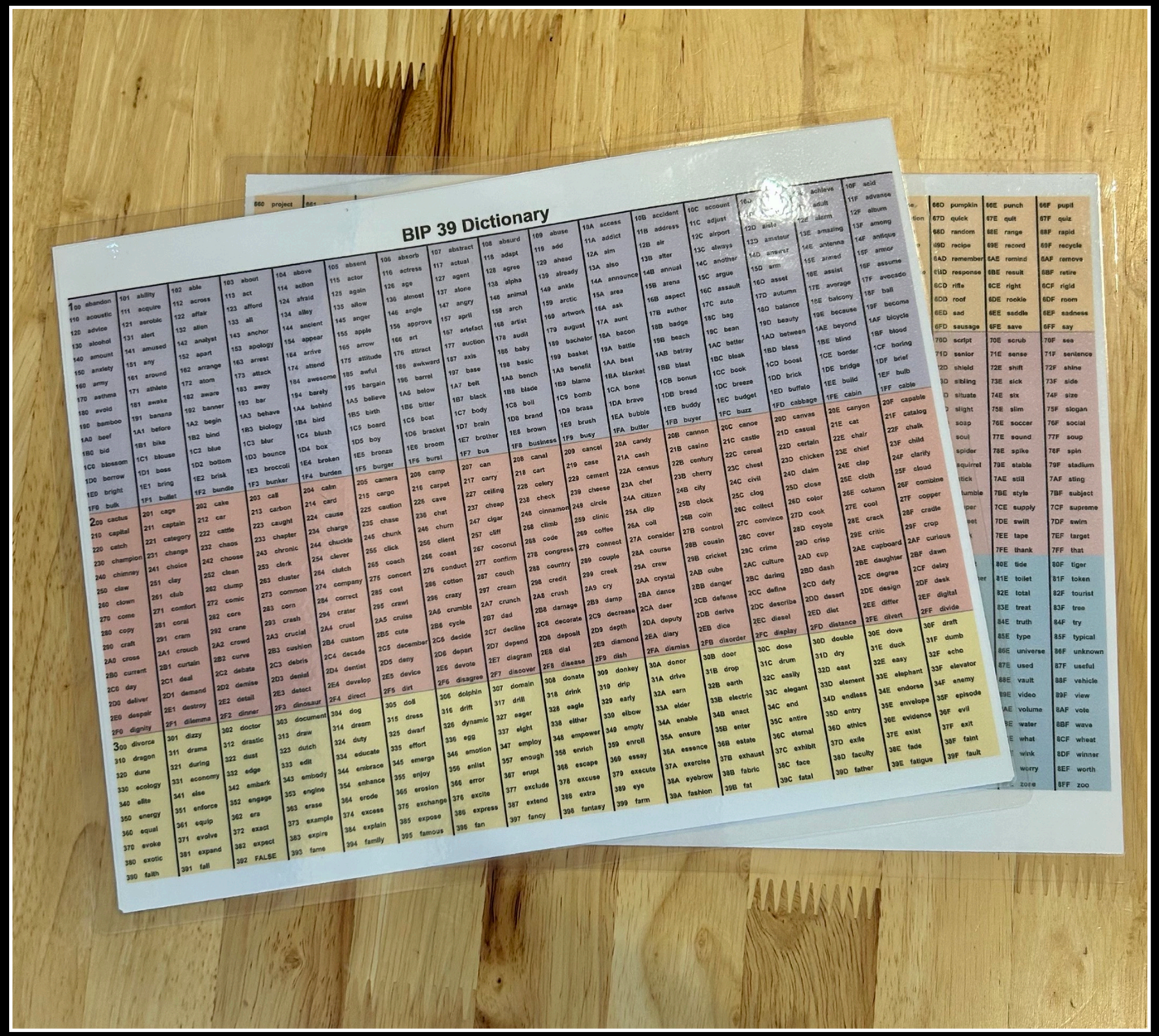
- Carefully place the three dice in a row, with the octal one on the left side.
- The order of the next two doesn’t matter.
- Don’t worry if they roll to a different number as you place them.

- Write the numbers and letters showing on the dice in the boxes on Line 1.
- Make sure your writing is legible!

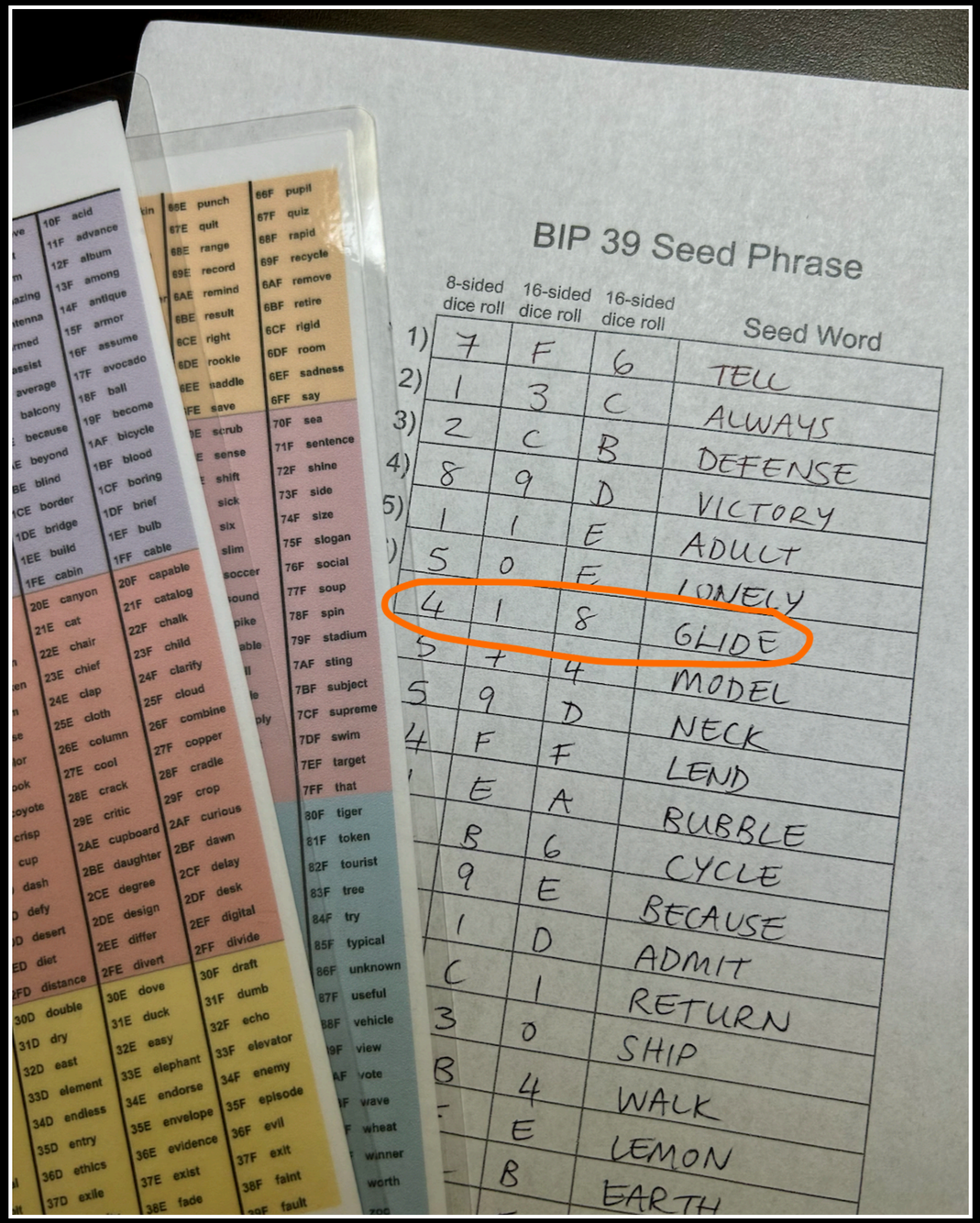


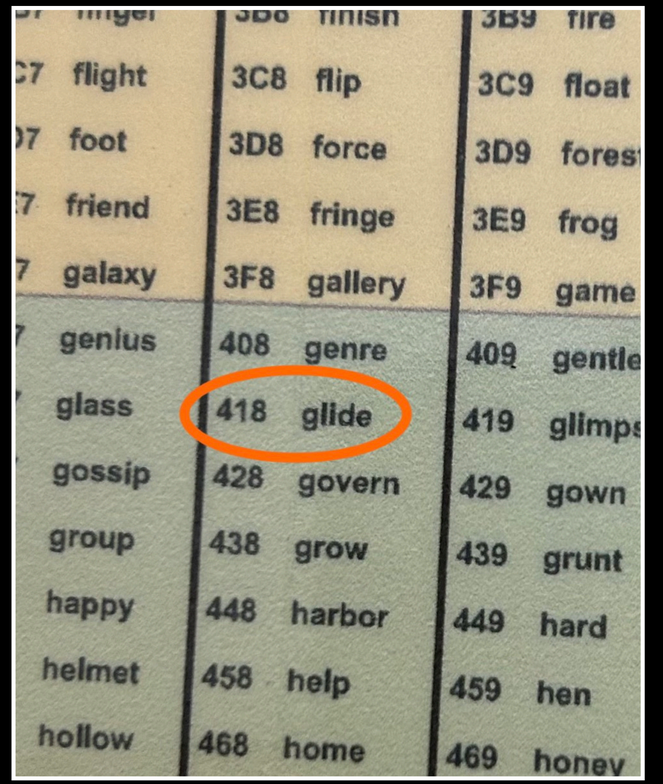


- Continue the process until you get to the 24th word.
- For this one, just roll the octal dice one time, and enter the number in the box on the left.
- Note: If you use a seed signer to calculate the 24th word, no need to roll this last one.



- Take a look at the BIP 39 Word List Dictionary.
- Note how each section is a different color, depending on the first number.
- This will make it easier to find your words.





- Using the list, write the word corresponding to each dice roll on the BIP 39 Seed Phrase worksheet.

HOW TO GET THE CHECKSUM -> 24TH WORD

Instructions follow for how to calculate the 24th word in your seed phrase, using each of the following signing devices:

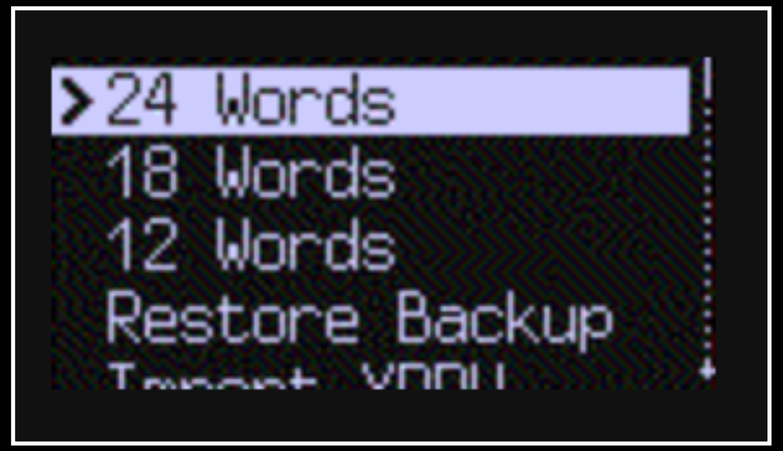
- Cold Card
- Seed Signer
- Jade

COLD CARD:

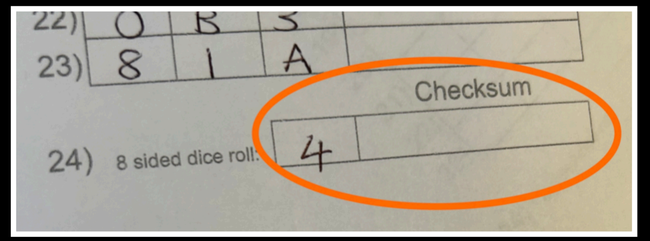
- Log into your Cold Card using your pin code.
- Click on ‘Import Existing’

COLD CARD cont.

- Click on ’24 Words’
- Input the 23 words you rolled.



- 8 options will then be shown for the 24th word.
- Select the option number of the dice you rolled for the 24th word, in this case #4.



SEED SIGNER:

Click on:

> Seed tools

> Calculate last word

> Select ’24 words’

SEED SIGNER cont.

> Enter your 23 words

> Once these are entered, the 24th word checksum will be displayed

> Write it down on your worksheet on line 24

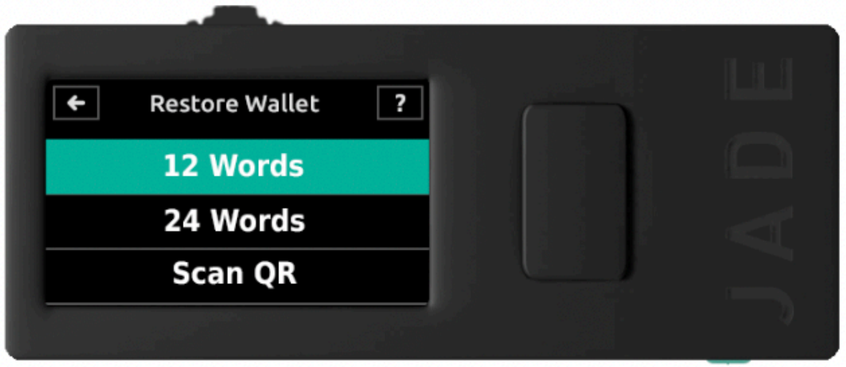
> Click the toggle to the right to view the full seed phrase and check to confirm you entered it correctly.

JADE:

Calculate Final Word

1. Turn on Jade and choose one of the following paths:

- **Setup Jade, Advanced Setup, Restore Wallet, 12/24 Words**
- **Options, Temporary Signer, 12/24 Words**

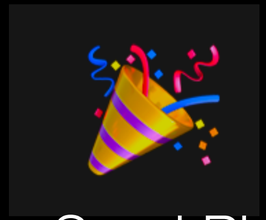


JADE cont.

2. Enter the first 11 or 23 words of your user-generated recovery phrase, then select **Calculate** when prompted. The keyboard for the final word will restrict your entry only to valid options.

Tip: The keyboard for the final word entry will automatically start on a random letter. After choosing 1-2 letters, Jade will display the remaining list of options and will also begin its selection on a random word. Simply click through the calculation section if you would like Jade to randomly select a final word for you.

And that's it!

CONGRATULATIONS 

You just rolled your own Seed Phrase!

Next Steps:

- MAKE A COPY
- PUT CLEAR PACKING TAPE OVER YOUR NEW SEED
- SECURELY HIDE EACH COPY SEPARATELY!

*** Finally, get a metal plate and stamp your seed in it, for ultimate durability & protection from the elements.

REMEMBER:

In bitcoin, possession is 10/10ths of the law!

Whoever has your seed phrase has access to your bitcoin!

WHY DOES ONE OCTAL & TWO HEX DICE CREATE A SEED WORD?

- A Master Private bitcoin key (xprv) contains 256 bits of entropy.
- 256 bits/24 words=10.66
- Rounded up, this amounts to 11 bits of entropy for each word in a 24-word Seep Phrase.
- An octal di offers 3 bits of entropy, since 8 is 2 to the power of 3, as in 2x2x2=8
- A hex di offer 4 bits of entropy, since 16 is 2 to the power of 4, as in 2x2x2x2=16.
- So one octal + two hex dice throws is 3+4+4, which equals 11 bits of entropy = one seed word.