KEYSA AND D++

ROLL YOUR OWN 24 WORD BITCOIN SEED PHRASE OFFLINE

WHY ROLL YOUR OWN SEED?

Strong Entropy: It safeguards against weak entropy that could potentially be exploited in the future.

Trust Minimized: It ensures robust entropy, eliminating the need to trust the RNG (Random Number Generator).

Enhanced Security: Generating your seed offline reduces reliance on hardware or software wallets that could be compromised.

Control: You maintain complete ownership of your private keys, eliminating any risk of a third-party having knowledge of your key.

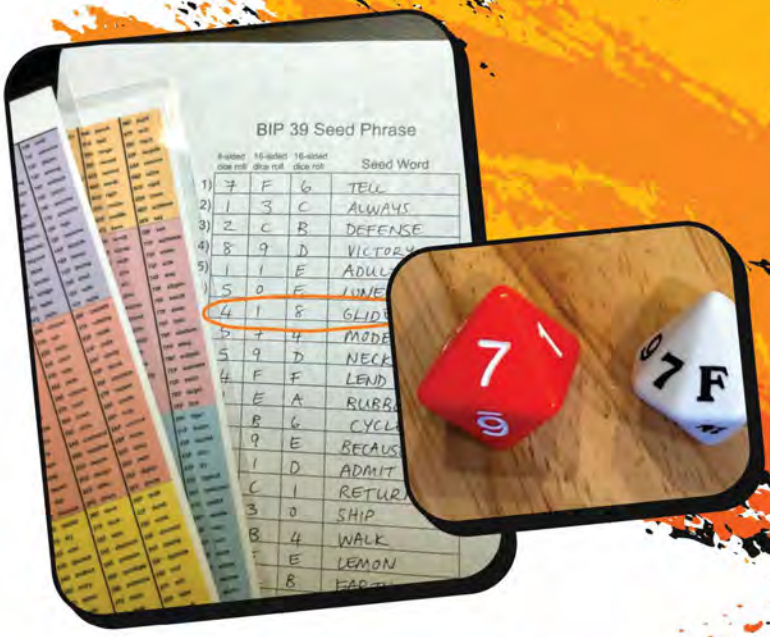
Privacy: No digital footprint is created.

Educational Value: It deepens your understanding of Bitcoin's cryptography.

MATERIALS NEEDED

VISIT: ENTROPY.PAGE/DICE

Dice: x1 Octal (8-sided) die, x2 Hex (16-sided) dice
BIP39 Worksheet **(Printed out from QR link on page 49)**
BIP39 Word List **(Printed out from QR link on page 49)**
Signing Device: Cold Card, Seed Signer, Jade or Passport (Needed to calculate the checksum/24th word offline)
Pen
Cup to roll the dice in
Hard, flat surface, in a room free of all electronics



IMPORTANT NOTES

Read through this whole guide before you start.

I highly recommend doing a complete practice run, carefully following all the instructions.

When you are ready to do it 'for real', be sure to **follow all the instructions on the following page** to ensure maximum security.

PREPARATION

Make sure you're in a room without any **electronics (aside from the signing device) and draw the shades** so no one can see in.

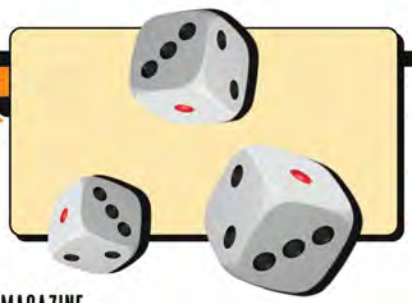
Switch on the lights if needed.

Since you are doing the proof-of-work to roll your own seed, **you want to maximize security and privacy** while doing so.

Let anyone else in the house know that **you need to be undisturbed** for an hour, ideally locking the door to prevent anyone accidentally coming in with a phone on.

Ensure you have a **hard surface for rolling the dice**—an empty box with a flat bottom can be helpful.

Check that you **have all the materials ready and with you** in the room.



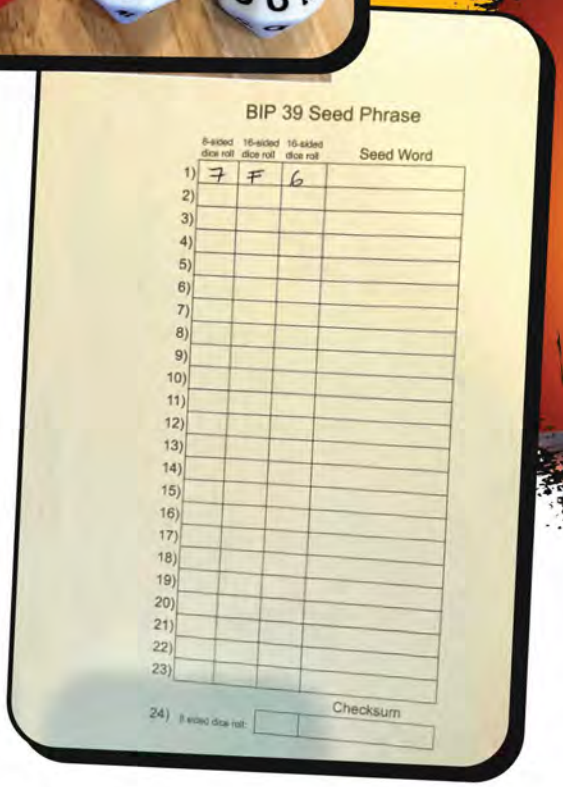
Use a cup to shake the three dice.

Throw them down on the table or in the box.

Carefully place them 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 shown on the dice in the boxes on Line 1 of the BIP 39 Seed Phrase Worksheet.

Make sure your writing is **legible!**

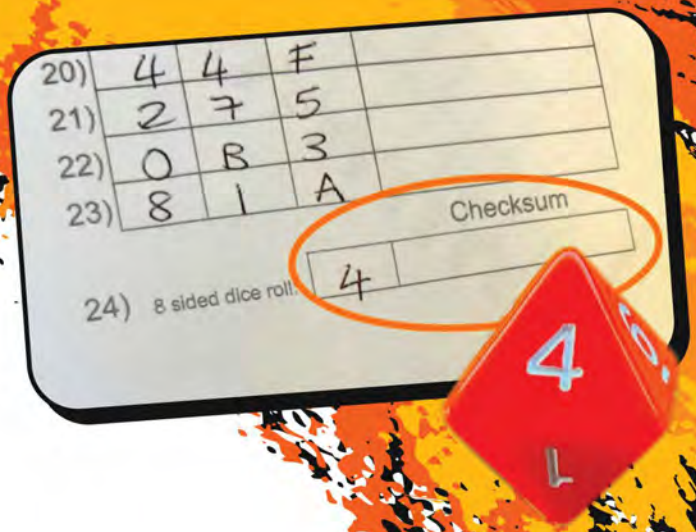
Continue the process until you get to the 24th word (the checksum).

Roll only the octal die one time, and enter the number in the box on the left.

Take a look at the **BIP 39 Dictionary.**

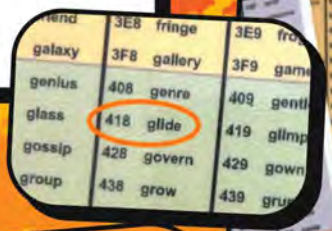
Note how **each section is a different color,** depending on the first number.

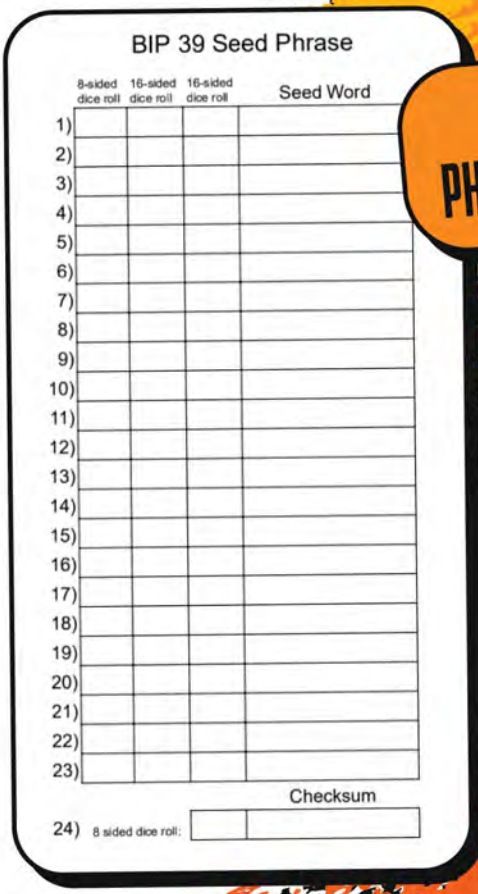
This will make it easier to find your words.



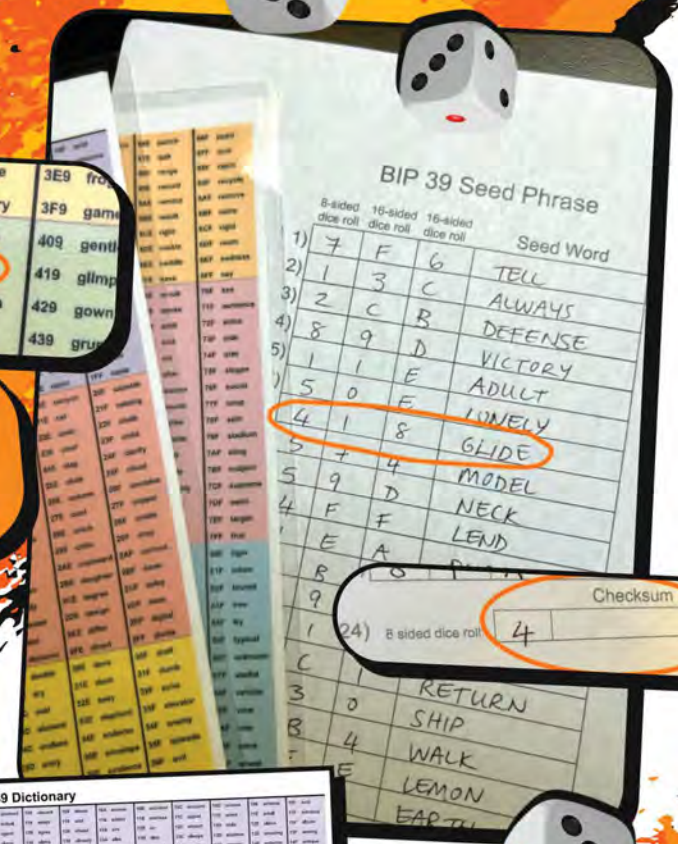
Using the word list, **write the 23 words corresponding to each dice roll** on the BIP 39 Seed Phrase Worksheet.

Leave the 24th word blank for now.





BIP 39 SEED PHRASE WORKSHEET



GET YOUR OWN WORKSHEET

GET YOUR OWN DICTIONARY

CALCULATE THE 24TH WORD CHECKSUM

Instructions follow for **calculating the final word** of your Seed Phrase using each of the following signing devices:

FOUNDATION PASSPORT

BLOCKSTREAM JADE

COLD CARD

SEED SIGNER

NOTE

There will be some differences in the process on each device.

Set up your Cold Card with a secure pin code.

Select > **Import Existing**

Select > **24 Words**

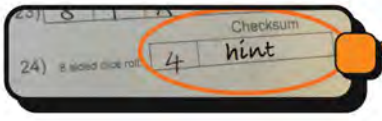
Enter the 23 words from the worksheet.

COLD CARD

After entering 23 words, 8 options will be shown for the 24th word.

Write down the one **corresponding to the number you rolled for line 24**

For this example, 'hint' was the fourth word.



Add this last word to your Worksheet on Line 24.

COLD CARD

Once you have selected the 24th word, you will want to **view your seed words** to confirm you entered them correctly.

Select:

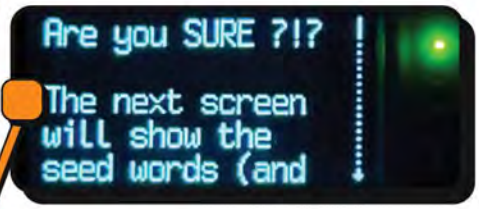
> **Advanced/Tools**

> **Danger Zone**

> **Seed Functions**

> **View Seed Words**

> **Accept** and check your words are correct



SEED SIGNER

Power on your Seed Signer.

Select > Tools

Select > Calc 12th/24th word

Select > 24 words

SEED SIGNER

Enter your 23 words

Once these are entered, the **Build Final Word** screen will appear.

Select a method to calculate the checksum.

For this tutorial, we'll use **'Coin flip entropy'.**

Flip a coin 3 times and enter the results.

SEED SIGNER

When the final word is calculated, **write it on Line 24 of your Worksheet.**

Click **Next** > **Load Seed.**

Note down the Fingerprint and click **Done.**

Since Seed Signer is stateless, **it will forget your seed when powered off.**

When you re-enter your seed in the future, you can confirm it is correct by **checking the fingerprint matches.**

SEED SIGNER

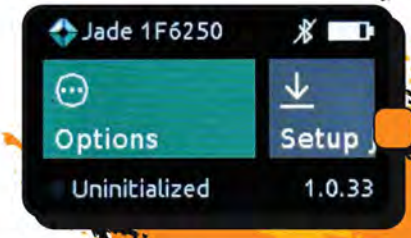
Time to confirm you entered your seed word correctly.

Select > **Backup Seed**

Select > **View Seed Words**

Select > **I Understand**

Go through and check the words against your Worksheet.



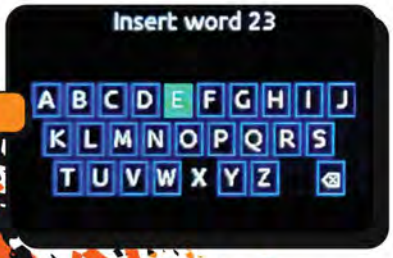
BLOCKSTREAM JADE

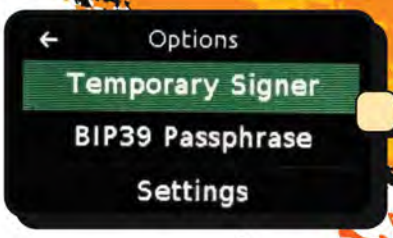
Power on your Jade.

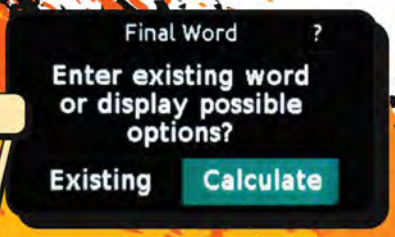
Select > **Options**

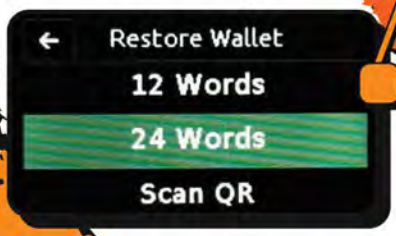
Select > **Temporary Signer**

Select > **24 words**









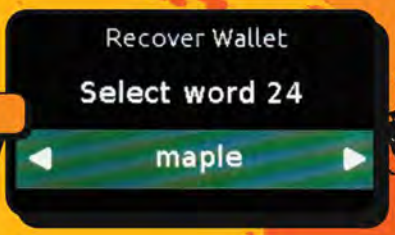
BLOCKSTREAM JADE

Enter the 23 words from your Worksheet.

Select > **Calculate** for the Final 24th Word

Scroll L/R to select the word that matches the number you entered on Line 24.

Note: Any of the 8 words offered will work as the checksum (24th word).



BLOCKSTREAM JADE

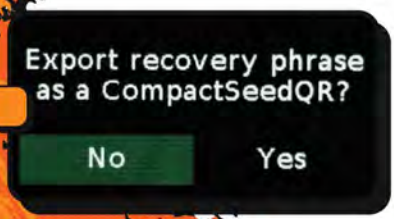
Select > **No** for Export.

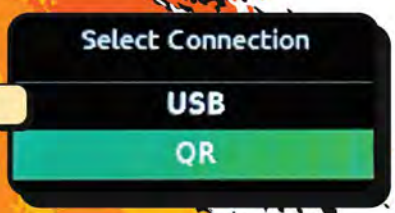
Select > **QR** for Connection to return to the **Home Screen**.

Note down the **Master Fingerprint** shown in the bottom right corner.

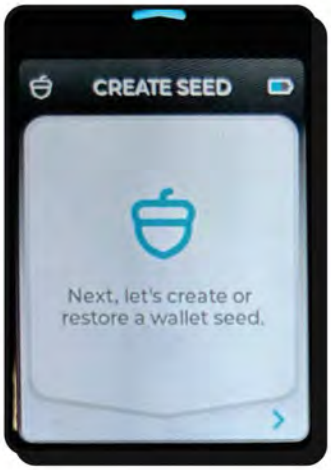
Power off the device. Power it on and **repeat the whole process.**

Check the master fingerprint matches the one you wrote down, to verify your seed phrase.





FOUNDATION PASSPORT



Power on your device

Select > **Import Seed**

Select > **Save Seed or Temporary Seed ***

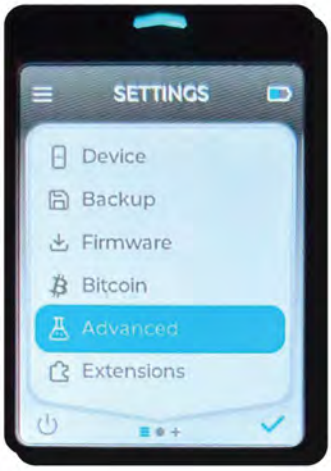
Select > **24 words**

Enter the 23 words from your Worksheet

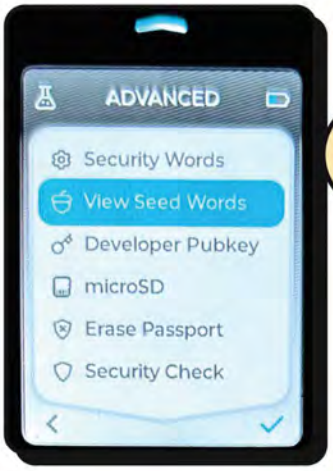
Select > **Generate Final Word**

Select > **Import and Save Seed**

Backup to MicroSD



Settings > **Advanced**



Select > **View Seed Words & verify they are correct**

AND THAT'S IT!

CONGRATULATIONS

YOU JUST ROLLED YOUR OWN SEED PHRASE OFFLINE!

* Select **Temporary Seed** if you already have a seed in your Passport & just want to calculate a checksum for a new seed.

IMMEDIATE NEXT STEPS

Make a copy so you have **two backups**.

Put clear packing tape over each one.

SECURELY HIDE EACH COPY **SEPARATELY**!

FINALLY

Buy 2 metal plates and stamp your seed in them for ultimate durability & protection from the elements. **Hide separately and securely!**

READ

REMEMBER

In bitcoin, possession is 10/10ths of the law! **Whoever has your Seed Phrase has access to your bitcoin! Secure it very very well!**
As always > Don't Trust, **Verify** > DYOR **D**o **Y**our **O**wn **R**esearch

FURTHER RESOURCES

BY GREG WALKER

BY D++

BY IAN COLEMAN

BY JAMESON LOPP

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

A bitcoin Private Key contains **256 bits** of entropy.

Each word in a Seed Phrase is **11 bits.**

An **octal die offers 3 bits of entropy,** since 8 is 2 to the power of 3, as in 2x2x2=8

A **hex die 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 bits + **4 bits** + **4 bits** = **11 bits of entropy** = One Seed Word.