

Forum:[Hack Forums](#)

Thread: [How to Create a Seed with Dice](#)

Omniscient - August 3, 2026, 10:55 am

Creating a BIP39 Seed Phrase With a 16-Sided Die

Quote:Important: This procedure is intended for generating a standard BIP39 seed phrase entirely offline. Never enter your rolls, entropy, or finished seed phrase into a website, online computer, chatbot, password manager, cloud storage account, or electronic message.

What You Need

A reasonably balanced 16-sided die, commonly called a d16

A pen or pencil

Paper that will remain private

A permanently offline computer

Python 3 installed on that offline computer

The official BIP39 English word list saved as Code english.txt

The official BIP39 word list must contain exactly 2,048 words, beginning with Code abandon and ending with Code zoo.

Choose Your Seed Length

12 words: Roll the d16 exactly 32 times. This produces 128 bits of entropy.

24 words: Roll the d16 exactly 64 times. This produces 256 bits of entropy.

A 24-word phrase provides more entropy, but both lengths are standard BIP39 phrases.

Step 1: Assign Each Die Face a Hexadecimal Digit

Use the following mapping consistently:

Code Die Roll Hex Digit

1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	A
11	B
12	C
13	D
14	E
15	F
16	0

Each roll produces one hexadecimal digit. Every hexadecimal digit represents exactly four bits.

Do not change the mapping after beginning.

Step 2: Roll the Die

Roll the die on a flat surface where it can tumble freely.

Record every result in order. Do not reroll a result merely because it repeats. Repeated results are normal.

For easier transcription, place a space after every eight rolls.

A fictional 32-roll example might look like this:

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

Remove the spaces to create one hexadecimal entropy value:

```
Code 4B702F91C38A66D51E49B20F7A3D8C56  
Do not use the example above as your seed entropy.
```

Your actual entropy must come from your own private rolls.

Step 3: Confirm the Length

For a 12-word phrase, your entropy must contain exactly:

```
Code 32 hexadecimal characters  
For a 24-word phrase, your entropy must contain exactly:
```

```
Code 64 hexadecimal characters  
Count the characters carefully before continuing.
```

Step 4: Prepare the Offline Converter

On the permanently offline computer, place these two files in the same directory:
Code english.txt — the official 2,048-word BIP39 English word list
Code dice_to_bip39.py — the script shown below

Save the following as Code dice_to_bip39.py:

```
Code #!/usr/bin/env python3
```

```
import hashlib  
import sys  
from pathlib import Path
```

```
ALLOWED_ENTROPY_BITS = {128, 160, 192, 224, 256}
```

```
def load_wordlist(path: str = "english.txt") -> list[str]:  
    wordlist_path = Path(path)
```

```
...
```

```

if not wordlist_path.is_file():
    raise FileNotFoundError(
        f"Cannot find {wordlist_path}. Place the official BIP39 "
        "English word list in the same directory."
    )

words = [
    line.strip()
    for line in wordlist_path.read_text(encoding="utf-8").splitlines()
    if line.strip()
]

if len(words) != 2048:
    raise ValueError(
        f"The word list contains {len(words)} words instead of 2048."
    )

if words[0] != "abandon" or words[-1] != "zoo":
    raise ValueError(
        "The word list does not appear to be the official "
        "BIP39 English word list."
    )

return words
'''

def entropy_to_mnemonic(entropy_hex: str, words: list[str]) -> str:
    entropy_hex = entropy_hex.strip().replace(" ", "").lower()

    '''
    if any(character not in "0123456789abcdef" for character in entropy_hex):
        raise ValueError(
            "Entropy may contain only hexadecimal characters 0-9 and A-F."
        )

    entropy_bits_length = len(entropy_hex) * 4

    if entropy_bits_length not in ALLOWED_ENTROPY_BITS:
        raise ValueError(
            "Invalid entropy length. Use 32 hexadecimal characters for "
            "a 12-word phrase or 64 characters for a 24-word phrase."
        )

    entropy_bytes = bytes.fromhex(entropy_hex)

    entropy_bits = "".join(
        f'{byte:08b}' for byte in entropy_bytes
    )

    checksum_length = entropy_bits_length // 32
    digest = hashlib.sha256(entropy_bytes).digest()
    digest_bits = "".join(f'{byte:08b}' for byte in digest)
    checksum_bits = digest_bits[:checksum_length]

```

```

combined_bits = entropy_bits + checksum_bits

indexes = [
    int(combined_bits[position:position + 11], 2)
    for position in range(0, len(combined_bits), 11)
]

return " ".join(words[index] for index in indexes)
'''

def main() -> None:
try:
wordlist = load_wordlist()

'''
    print("BIP39 Dice Entropy Converter")
    print("-----")
    print("Enter 32 hex characters for 12 words.")
    print("Enter 64 hex characters for 24 words.")
    print()

    entropy_hex = input("Entropy: ")
    mnemonic = entropy_to_mnemonic(entropy_hex, wordlist)

    print()
    print("BIP39 mnemonic:")
    print(mnemonic)
    print()
    print("Word count:", len(mnemonic.split()))

except (ValueError, FileNotFoundError) as error:
    print(f"Error: {error}", file=sys.stderr)
    sys.exit(1)
'''

if __name__ == "__main__":
    main()

```

This script uses Python's built-in SHA-256 implementation. It does not require an internet connection or third-party Python packages.

Step 5: Disconnect the Computer

Before entering your entropy:
 Disconnect Ethernet.
 Disable Wi-Fi and Bluetooth.
 Remove unnecessary USB devices.
 Confirm that no remote-access or screen-recording software is running.
 Cover or disconnect cameras that could observe your paper or screen.

For meaningful amounts of cryptocurrency, use a computer that will remain permanently offline or use a temporary live operating system that never connects to a network.

Step 6: Run the Converter

Open a terminal in the directory containing both files and run:

Code `python3 dice_to_bip39.py`

When prompted, enter your hexadecimal entropy without spaces.

For example:

Code Entropy: YOUR_PRIVATE_HEX_ENTROPY

The script will:

Convert the hexadecimal value into binary entropy.

Calculate its SHA-256 hash.

Append the required BIP39 checksum bits.

Divide the result into 11-bit values.

Use those values as indexes into the official BIP39 word list.

Display the resulting 12-word or 24-word phrase.

Step 7: Record the Phrase

Write down each word clearly and number the words in order:

Code 1.

2.

3.

4.

5.

6.

7.

8.

9.

10.

11.

12.

For a 24-word phrase, continue through word 24.

Spelling and order are critical. A correctly spelled word in the wrong position creates a different wallet.

Step 8: Verify the Phrase

Before transferring significant funds:

Import the phrase into a compatible wallet while still offline.

Record the first receiving address.

Erase or reset the wallet.

Restore it again using the written phrase.

Confirm that the same receiving address appears.

Send only a small test amount initially.

Test the complete recovery process again before depositing a significant amount.

Do not assume a phrase is safe merely because a wallet accepts it. Confirm that the wallet specifically supports standard BIP39 phrases.

Step 9: Secure or Destroy the Roll Record

The hexadecimal roll record contains the same underlying entropy as the seed phrase. Anyone who obtains either one can recreate the wallet.

After confirming the backup:

Destroy the roll worksheet securely, or

Protect it to the same standard as the finished seed phrase.

Do not keep the roll record and seed phrase together as though they were independent backups. They represent the same secret.

Optional BIP39 Passphrase

A BIP39 passphrase is sometimes called a "25th word," although it can contain multiple characters or words.

Every possible passphrase creates a valid but different wallet. A mistyped or forgotten passphrase cannot be recovered from the seed words.

Use one only when you fully understand:

How it changes the derived wallet

How it will be backed up

How your beneficiaries will recover it

How you will test restoration

Never store the seed phrase and its passphrase in the same location.

Security Warnings

Never use an online BIP39 converter.

Never photograph or scan the seed phrase.

Never paste it into a website or chatbot.

Never save it in email, cloud storage, or online notes.

Never print it using a network-connected printer.

Never allow another person to roll, record, or convert it for you.

Never use example entropy or example seed phrases.

Never use decorative, damaged, or visibly unbalanced dice.

Never disclose even part of the phrase as a "verification."

Quote:Final reminder: Creating the phrase securely is only one part of wallet security. You must also verify the wallet software, protect the backup from theft and destruction, test recovery, and keep the signing environment secure.

Omniscient - August 3, 2026, 10:56 am

D16 dice available at local game stores or Amazon.

<https://www.amazon.com/Polyhedral-Dungeons-Dragons-Colored-Assortment/dp/B0C45ZQ7VD/>