

# PYTHON MINI PROJECT



**Project By:**

Manav Anandani

# Title : Demo Bitcoin Miner

## PROBLEM STATEMENT

Working demo of bitcoin mining technology using SHA256 library for cryptographic security.

## THEORY

Bitcoin is a ledger. A ledger is a set of transactions with your account balance. This set of transactions are stored in different blocks. These blocks are very similar to linked lists. These blockchains usually of 1MB hold the information of one transaction.

To secure these blocks we use cryptography. In cryptography we have SHA256(x) given an input string it will generate a hash which is 256 bit long and it is almost impossible to guess. It can be decoded only on the basis of trial and error. We use hashlib library to produce SHA of any string where as already discussed SHA256 is a hash function. In blockchain the block is not only transaction it has more things to it i.e. Block No, Previous hash you make all the information a string and supply it to SHA256 function and that will produce a hash and according to protocol first few digits of this hash must be zero. The number digits to be made zero changes time to time. The difficulty level increases as the number of zero digits increases. To make the first few digits zero we use Nonce i.e. number once. We use a for loop to guess the Nonce. If we guessed the Nonce right then our block is verified and this Nonce guessing is Bitcoin mining and to mine Bitcoin the miners get a reward. This mining is very time consuming.

## DATASET

No dataset was required for this project.

## PROGRAM

```
from hashlib import sha256
MAX_NONCE = 1000000000000

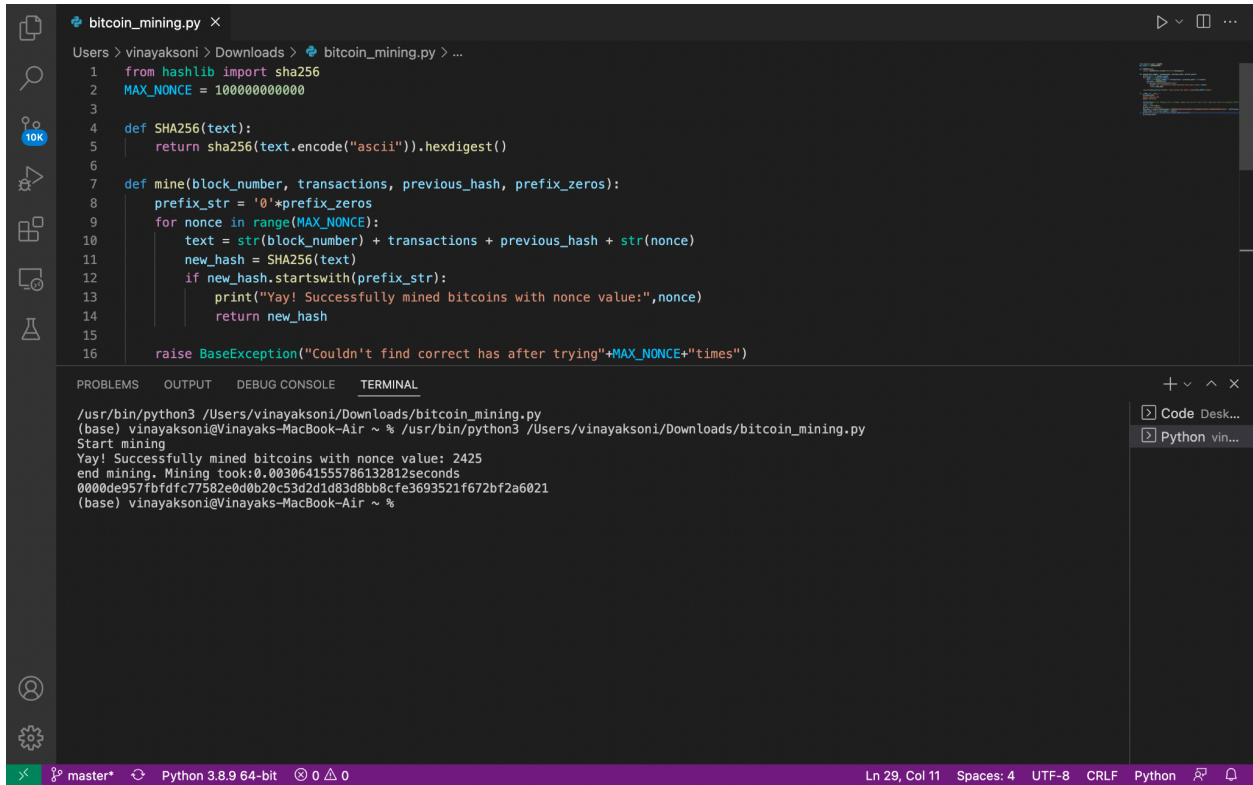
def SHA256(text):
    return sha256(text.encode("ascii")).hexdigest()

def mine(block_number, transactions, previous_hash, prefix_zeros):
    prefix_str = '0'*prefix_zeros
    for nonce in range(MAX_NONCE):
        text = str(block_number) + transactions + previous_hash +
str(nonce)
        new_hash = SHA256(text)
        if new_hash.startswith(prefix_str):
            print(f"Yay! Successfully mined bitcoins with nonce
value:{nonce}")
            return new_hash

        raise BaseException(f"Couldn't find correct has after trying
{MAX_NONCE} times")

if __name__=='__main__':
    transactions=''
    Dhaval->Bhavin->20,
    Mando->Cara->45
    '''
    difficulty=4 # try changing this to higher number and you will see it
will take more time for mining as difficulty increases
    import time
    start = time.time()
    print("start mining")
    new_hash =
mine(5,transactions,'0000000xa036944e29568d0cff17edbe038f81208fecf9a66be9a
2b8321c6ec7', difficulty)
    total_time = str((time.time() - start))
    print(f"end mining. Mining took: {total_time} seconds")
    print(new_hash)
```

## OUTPUT



The image shows a Visual Studio Code editor window with a file named `bitcoin_mining.py` open. The script defines a `SHA256` function and a `mine` function. The `mine` function iterates through nonces from 0 to `MAX_NONCE` (1000000000000) to find a valid hash. The terminal output shows the script being executed, the mining process starting, and a successful result being printed.

```
bitcoin_mining.py X
Users > vinayaksoni > Downloads > bitcoin_mining.py > ...
1 from hashlib import sha256
2 MAX_NONCE = 1000000000000
3
4 def SHA256(text):
5     return sha256(text.encode("ascii")).hexdigest()
6
7 def mine(block_number, transactions, previous_hash, prefix_zeros):
8     prefix_str = '0'*prefix_zeros
9     for nonce in range(MAX_NONCE):
10        text = str(block_number) + transactions + previous_hash + str(nonce)
11        new_hash = SHA256(text)
12        if new_hash.startswith(prefix_str):
13            print("Yay! Successfully mined bitcoins with nonce value:",nonce)
14            return new_hash
15
16        raise BaseException("Couldn't find correct has after trying"+MAX_NONCE+"times")
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

```
/usr/bin/python3 /Users/vinayaksoni/Downloads/bitcoin_mining.py
(base) vinayaksoni@Vinayaks-MacBook-Air ~ % /usr/bin/python3 /Users/vinayaksoni/Downloads/bitcoin_mining.py
Start mining
Yay! Successfully mined bitcoins with nonce value: 2425
end mining. Mining took:0.0030641555786132812seconds
0000de957fbdfc77582e0d0b20c53d2d1d83d8bb8cfe3693521f672bf2a6021
(base) vinayaksoni@Vinayaks-MacBook-Air ~ %
```

Ln 29, Col 11 Spaces: 4 UTF-8 CRLF Python