00:00 Introduction00:19 Theory09:21 Coding



This is a ledger with transactions that are happening. We need to store the transactions in blocks using a linked list structure with blocks of a specific size like 1MB blocks.



Bitcoin blocks use cryptography to ensure security that the blocks have not been tampered with

Using SHA256 function, we give a function and get a 256bit hash value back. This SHA values are almost impossible to guess or hack.

```
SHA256("ABC")

b5d4045c3f466fa91fe2cc6abe79232a1a57cdf104f7a26e716e0a1e2789df78

from hashlib import sha256

text = "ABC"

print(sha256(text.encode('ascii')).hexdigest())
```

You can write the 3 lines of python code to get the SHA256 value for the block

SHA256 is a cryptographic hash function

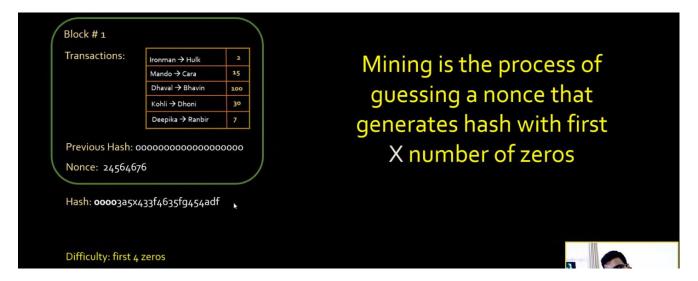


The protocol requires that certain starting values of the SHA256 hash value should be zero, this is the level of difficulty because we have to introduce a guess value called a Nonce to fulfil the difficulty using a for-loop.



Hash: b5d4o45c3f46354345as234

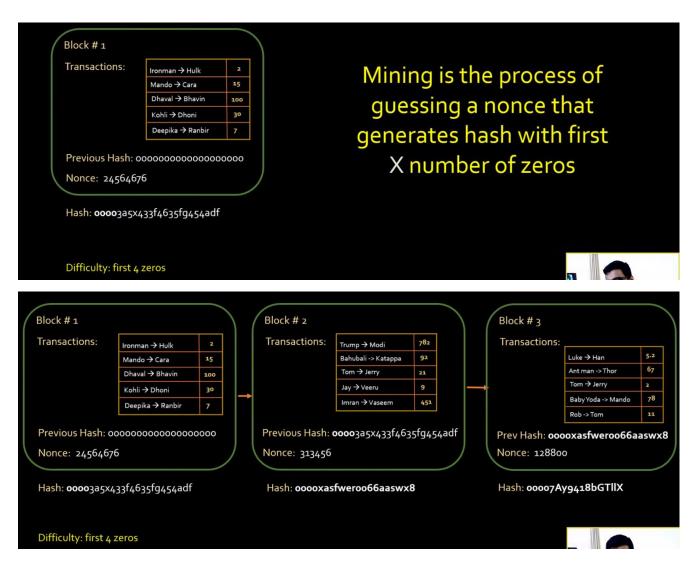
Difficulty: first 4 zeros



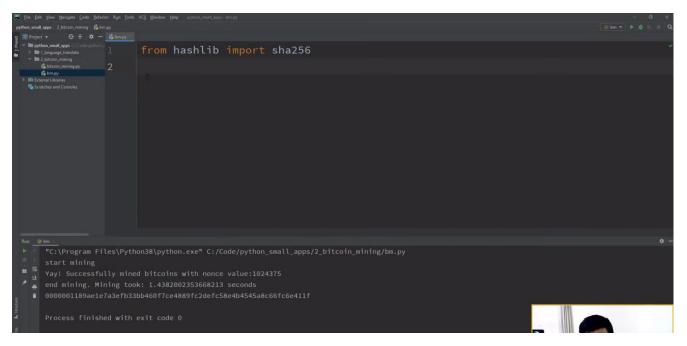
The process of guessing a correct nonce value to have the expected hash value with the required leading zeros is called Bitcoin mining.

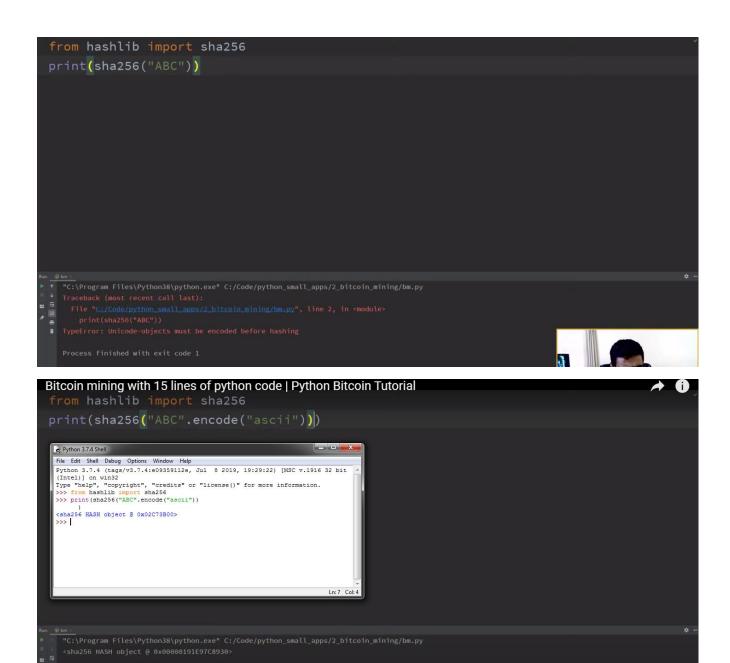


Miners get a reward for doing bitcoin mining, the reward gets halved every 4 years. The reward is currently 6.25BTC today. Bitcoin is about guessing the correct nonce value and getting a reward. Currently, miners get 6.25 BTC per valid block mined. But this reward changes roughly every four years, or after every 210,000 blocks are mined and gets reduced by half each time. ... After the first halving, the reward was reduced to 25 BTC, then to 12.5 BTC and finally to 6.25 BTC.



In the end, the blockchain looks like the above where every block will have a reference to the previous blocks' hash value. The blocks become a chain as they are added.





This will give you the sha256 object that you can get the actual hash out of



This **sha256("ABC".encode("ascii")).hexdigest())** command will give you the hash value as a 64-bit hexadecimal value which is actually 256-bit value.

```
from hashlib import sha256

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

if __name__=='__main__':|
    print(SHA256("ABC"))

print(SHA256("ABC"))

** "c:\Program Files\Python38\python.exe" c:/Code/python_small_apps/z_bitcoin_mining/bm.py
    bid4845c3f466fa91fe2cc6abe79232ala57cdf184f7a26e716e9ale2789df78

** Process finished with exit code 8
```

We can create a function to pass in our text value as above.

```
from hashlib import sha256

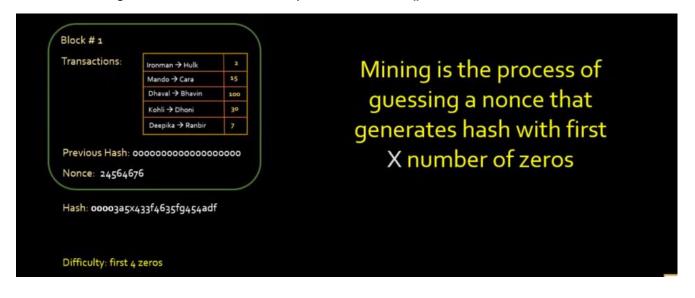
def SHA256(text):
    return sha256(text.encode("ascii")).hexdigest()

def mine():
    pass

if __name__=='__main__':
    transactions='''
    Dhaval->Bhavin->20,
    Mando->Cara->45
    '''
    new_hash = mine(transactions)

print(new_hash)
```

For bitcoin mining, we need transactions to be passed to our mine() function as above



The hash value to be calculated needs all the values above plus our guessed nonce value, we are trying to get a nonce that gives a hash value that has 20 starting zeros on the hash value

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

def mine(block_number, transactions, previous_hash, prefix_zeros):
    pass

if __name__=='__main__':
    transactions='''
    Dhaval->Bhavin->20,
    Mando->Cara->45
    '''
    difficulty=4
    new_hash = mine(5,transactions,'0000000xa036944e29568d0cff17edbe038f81208fecf9a66tectors)
    print(new_hash)
```

```
ions,'00000000xa036944e29568d0cff17edbe038f81208fecf9a66be9a2b8321c6ec7', difficulty
```

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

def mine(block_number, transactions, previous_hash, prefix_zeros):
    nonce=1
    text = str(block_number) + transactions + previous_hash + str(nonce)
    new_hash = SHA256(text)
    return new_hash

if __name__=='__main__':
    transactions='''
    Dhaval->Bhavin->20,
    Mando->Cara->45
    '''
    difficulty=4
    new_hash = mine(5,transactions,'00000000xa036944e29568d0cff17edb)
```

```
return sha256(text.encode("ascii")).hexdigest()

def mine(block_number, transactions, previous_hash, prefix_zeros):
    nonce=1
    text = str(block_number) + transactions + previous_hash + str(nonce)
    new_hash = SHA256(text)
    return new_hash

if __name__=='__main__':
    transactions='''
    Dhaval->Bhavin->20,
    Mando->Cara->45

    ***
    ***
    ***
    ***
    ***
    ***
    ***
    ***
    ***
    ***
    ***
    ***
    ***
    ***
    ***
    ***
    ***
    ***
    ***
    ***
    ***
    ***
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    *
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    **
    *
    **
    *
    **
    *
    *
    *
    *
    *
    *
    *
    *
    *
    *
    *
    *
    *
    *
    *
    *
    *
    *
    *
    *
    *
    *
    *
    *
    *
    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *

    *
```

Our first 4 digits of the hash are not zero for a guessed nonce value of 1. We need to try a different nonce guess

```
from hashlib import sha256
MAX_NONCE = 100000000000
def SHA256(text):
    return sha256(text.encode("ascii")).hexdigest()
def mine(block_number, transactions, previous_hash, prefix_zeros):
    for nonce in range(MAX_NONCE):
    nonce=3
    text = str(block_number) + transactions + previous_hash + str(nonce)
    new_hash = SHA256(text)
    return new_hash
def SHA256(text):
    return sha256(text.encode("ascii")).hexdigest()
def mine(block_number, transactions, previous_hash, prefix_zeros):
    for nonce in range(MAX_NONCE):
        text = str(block_number) + transactions + previous_hash + str(nonce)
        new_hash = SHA256(text)
    return new_hash
if __name__=='__main__':
    transactions='''
    difficulty=4
    new_hash = mine(5,transactions,'0000000xa036944e29568d0cff17edb
    print(new_hash)
```

```
def SHA256(text):
     return sha256(text.encode("ascii")).hexdigest()
def mine(block Python 3.8.5 Shell
     for nonce Python 3.8.5 (tags/v3.8.5:580fbb0, Jul 20 2020, 15:57:54) [MSC v.1924 64 bit (AM
                   D64)] on win32
                                                                                        str(nonce)
          text = Type "help", "copyright", "credits" or "license()" for more information.
                   >>> s='234ljskfasljfdlslfds243'
          new_ha>>> s.startswith('234')
                   True
                   >>> s.startswith('2sfd34')
     return new False
                   >>> s.startswith('0000')
                  False
if __name__== '4
                  >>> '0000'
     transactic
                   >>> '0'*4
     Dhaval->Bh
     Mando->Car >>>
     difficulty
     new_hash =
```

```
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
    '''
```

```
return new_hash
    raise BaseException(f"Couldn't find correct has after trying {MAX_NONCE} times")
if __name__=='__main__':
    transactions='''
    difficulty=4
    new_hash = mine(5,transactions,'00000000xa036944e29568d0cff17edbe038f81208fecf9a66
    print(new_hash)
            return new_hash
    raise BaseException(f|"Couldn't find correct has after trying {MAX_NONCE} times")
if __name__=='__main__':
    transactions='''
    difficulty=4
    new_hash = mine(5,transactions, '00000000xa036944e29568d0cff17edbe038f81208fecf9a66
```

It ran the for loop 2425 times before getting the nonce value for a hash starting with 4 zeros

```
if __name__ == '__main__':
    transactions='''
    Dhaval -> Bhavin -> 20,
    Mando -> Cara -> 45
    '''
    difficulty=6
    new_hash = mine(5,transactions,'00000000xa036944e29568d0cff17edbe038f81208fecf9a66b
    print(new_hash)

print(new_hash)

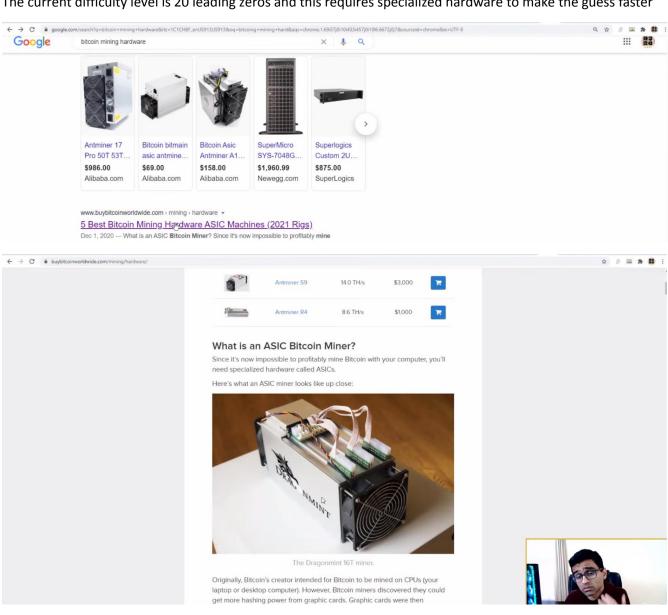
** "C:\Program Files\Python38\python.exe" C:\Code\python_small_apps/2_bitcoin_mining/bm.py
    'Yay! Successfully mined bitcoins with nonce value:8894382
    ** 99090021c251a735b47c72aec01a1803db7660f1fb6ccd2a7e8fb416645f90f6
    ** Process finished with exit code 0
```

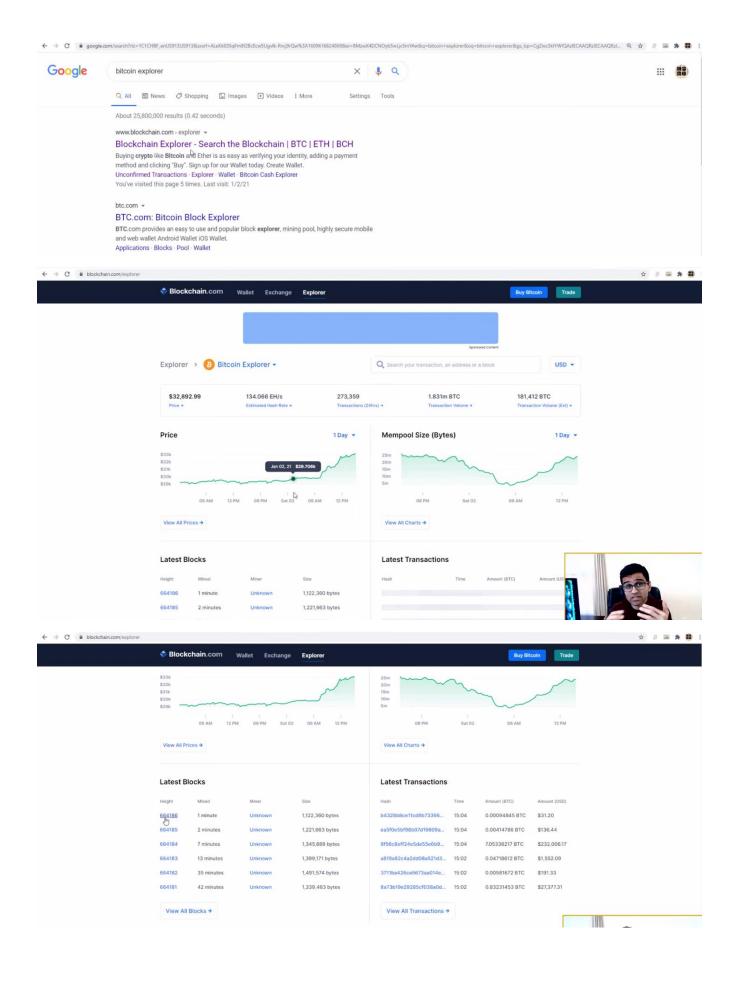
It ran the for loop 8894392 times before getting the nonce value for a hash starting with 6 zeros

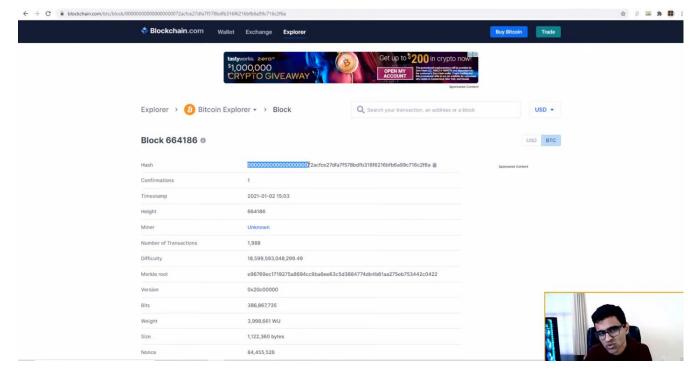
```
raise BaseException(f"Couldn't find correct has after trying {MAX_NONCE} times")
if __name__=='__main__':
   transactions='''
    difficulty=6
    import time
    start = time.time()
    new_hash = mine(5,transactions,'00000000xa036944e29568d0cff17edbe038f81208fecf9a66
    total_time = str((time.time() - start))
    print(f"end mining. Mining took: {total_time} seconds")
    print(new_hash)
    difficulty=6
    start = time.time()
    new_hash = mine(5,transactions,'00000000xa036944e29568d0cff17edbe038f81208fecf9a66t
    total_time = str((time.time() - start))
    print(f"end mining. Mining took: {total_time} seconds")
    print(new_hash)
```

```
difficulty=20
import time
start = time.time()
new_hash = mine(5,transactions,'00000000xa036944e29568d0cff17edbe038f81208fecf9a66b
total_time = str((time.time() - start))
print(f"end mining. Mining took: {total_time} seconds")
print(new_hash)
```

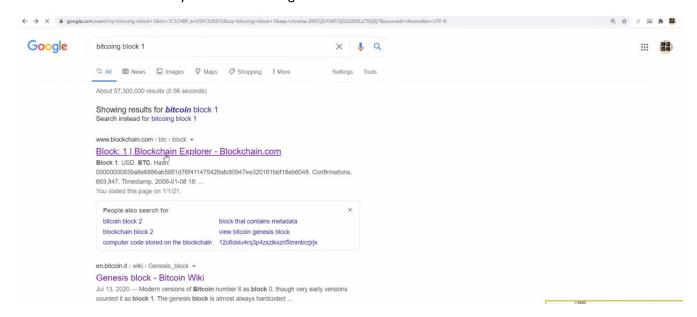
The current difficulty level is 20 leading zeros and this requires specialized hardware to make the guess faster

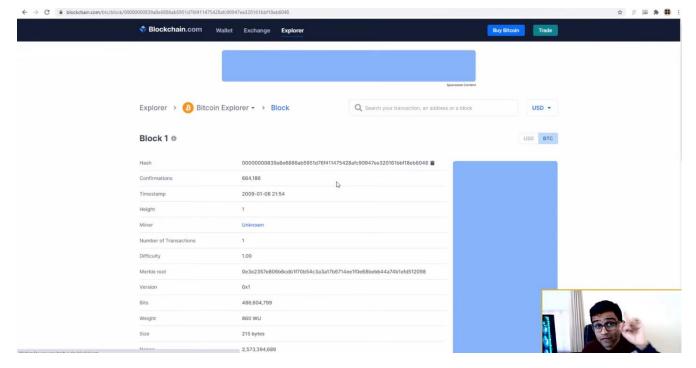




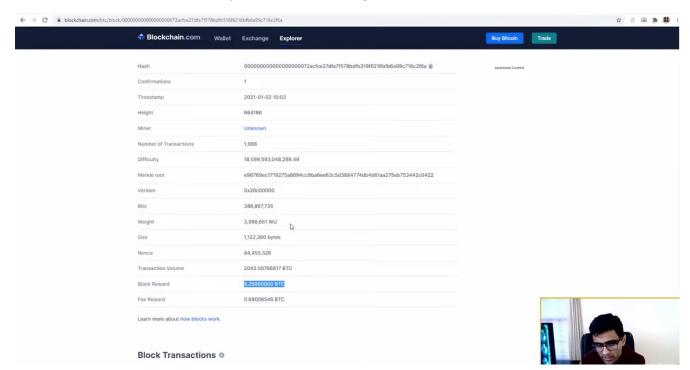


The current bitcoin difficulty level is 20 leading zeros





This is the first block even created by Satoshi with 8 leading zeros



```
from hashlib import sha256
MAX_NONCE = 100000000000

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 {Main transactions = ''' transactions = ''' transactions = '''
```

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

if __name__=='__main__':
    transactions='''
    Dhaval->Bhavin->20,

    Mando->Cara->45
    '''

    difficulty=20
    import time
    start = time.time()
    print("start mining")
    new_hash = mine(5,transactions,'0000000xa036944e29568d0cff17edbe038f81208fecf9a66t
    total_time = str((time.time() - start))
    print(f"end mining. Mining took: {total_time} seconds")
    print(new_hash)
```

The real difficulty is who might guess the correct nonce value faster.

