Cryptocurrency Emissions

By Alise Braick & Ben Eckley

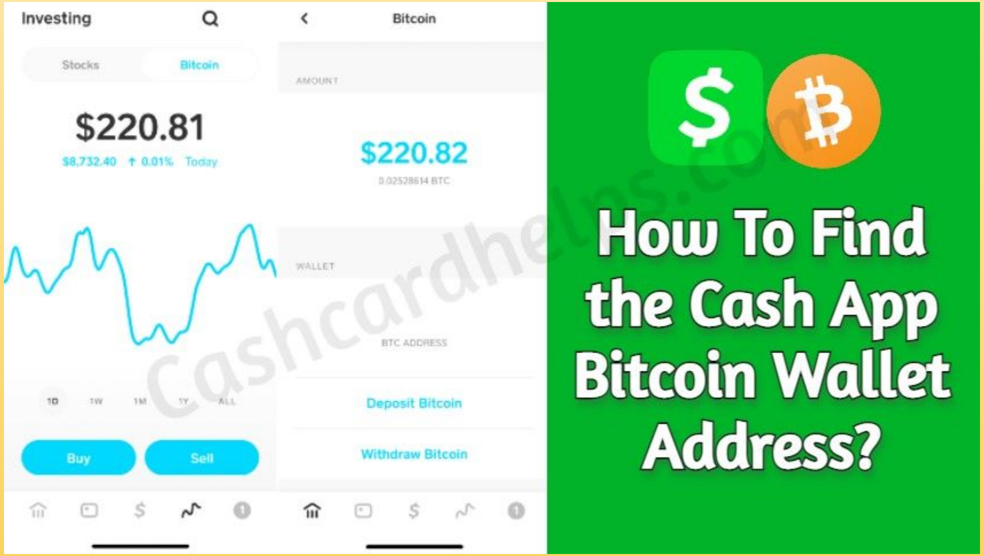
What is Cryptocurrency?

Cryptocurrency is a form of virtual currency that enables secure online payment without the use of third-party intermediaries.

Bitcoin is the world’s oldest and best-known cryptocurrency.

How Do Bitcoin Payments Work?

You transfer Bitcoins from your digital wallet to someone else’s using an app or website and the person’s unique Bitcoin address. The digital wallet is obtained when you buy the currency from a crypto exchange or by using a “Cold Wallet” for offline storage.



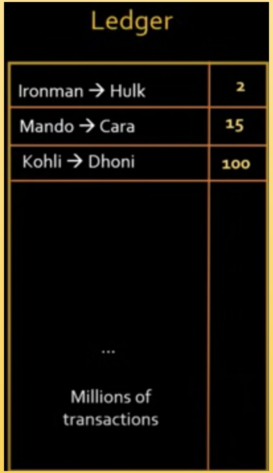
How Are Bitcoin Payments Processed?

Payments are processed and verified **by a network of ordinary people with computers** running special mining software.

These volunteers are called **Bitcoin miners.** They use high-end computer hardware to crack increasingly complex, mathematical verification problems generated by Bitcoin’s source code

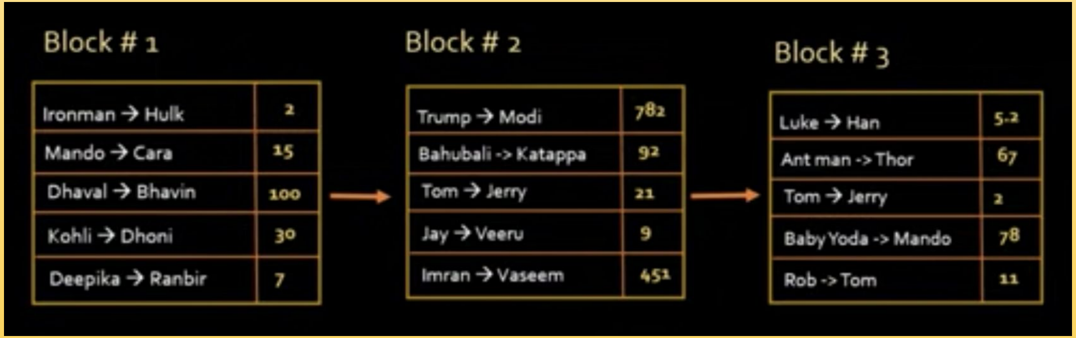
Once a payment is verified, the miner adds a record of the transaction to a shared online ledger. The record includes the sender and recipients' Bitcoin addresses and the amount transferred.

Transactions are grouped into 'blocks' which have a limited amount of space. When a block is 'full', a new, empty block is created.



Ledger

Ironman → Hulk	2
Mando → Cara	15
Kohli → Dhoni	100
... Millions of transactions	



Block # 1

Ironman → Hulk	2
Mando → Cara	15
Dhaval → Bhavin	100
Kohli → Dhoni	30
Deepika → Ranbir	7

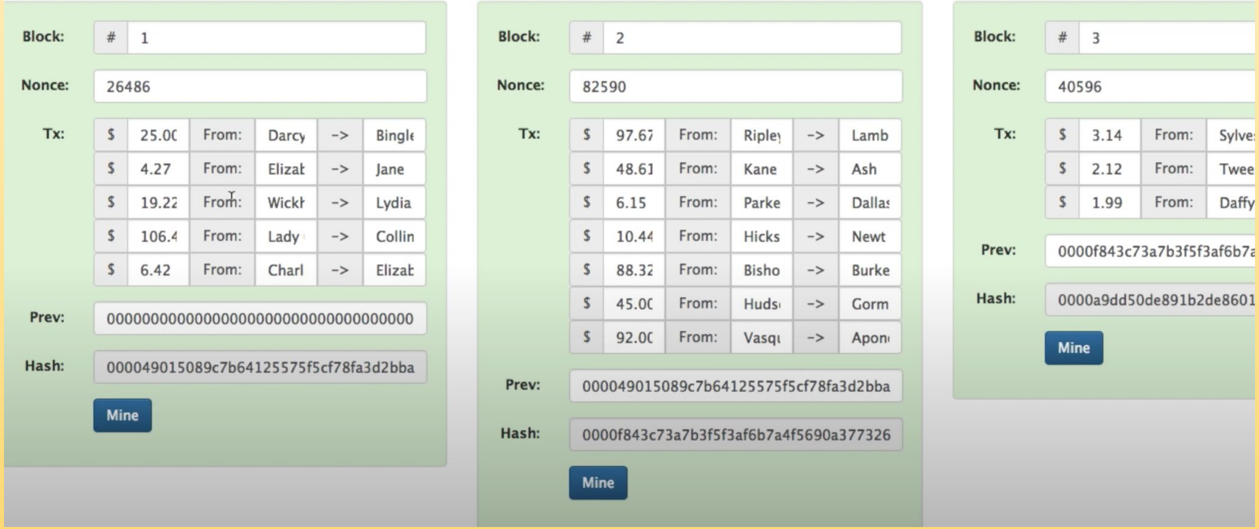
Block # 2

Trump → Modi	782
Bahubali -> Katappa	92
Tom → Jerry	21
Jay → Veeru	9
Imran → Vaseem	451

Block # 3

Luke → Han	5.2
Ant man -> Thor	67
Tom → Jerry	2
Baby Yoda -> Mando	78
Rob -> Tom	11

Each **new block links** back to the previous block containing information about older transactions. The blocks form a chain that links back all the way to the very first Bitcoin transaction.



Block: # 1

Nonce: 26486

Tx:

$	25.0	From:	Darcy	->	Bingle
$	4.27	From:	Elizab	->	Jane
$	19.22	From:	Wickh	->	Lydia
$	106.4	From:	Lady	->	Collin
$	6.42	From:	Charl	->	Elizab

Prev: 0000000000000000000000000000000000

Hash: 000049015089c7b64125575f5cf78fa3d2bba

Block: # 2

Nonce: 82590

Tx:

$	97.67	From:	Ripley	->	Lamb
$	48.61	From:	Kane	->	Ash
$	6.15	From:	Parke	->	Dallas
$	10.44	From:	Hicks	->	Newt
$	88.32	From:	Bisho	->	Burke
$	45.0	From:	Huds	->	Gorm
$	92.0	From:	Vasqu	->	Apon

Prev: 000049015089c7b64125575f5cf78fa3d2bba

Hash: 0000f843c73a7b3f5f3af6b7a4f5690a377326

Block: # 3

Nonce: 40596

Tx:

$	3.14	From:	Sylve
$	2.12	From:	Twee
$	1.99	From:	Daffy

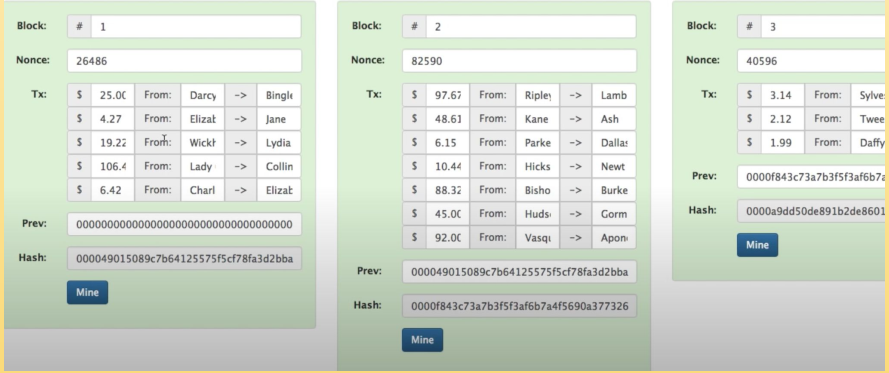
Prev: 0000f843c73a7b3f5f3af6b7a

Hash: 0000a9dd50de891b2de8601

Records stored in the blockchain are immutable

So the automated process of creating valid blocks that add transaction records to Bitcoin public ledger (Block Chain) is called Bitcoin Mining.

Blockchain Demo



Block: # 1
Nonce: 26486
Tx:
$ 25.0(From: Darcy -> Bingl
$ 4.27 From: Elizat -> Jane
$ 19.22 From: Wickl -> Lydia
$ 106.4 From: Lady -> Collin
$ 6.42 From: Charl -> Elizat
Prev: 0000000000000000000000000000000000
Hash: 000049015089c7b64125575f5cf78fa3d2bba

Block: # 2
Nonce: 82590
Tx:
$ 97.67 From: Riple -> Lamb
$ 48.61 From: Kane -> Ash
$ 6.15 From: Parke -> Dallas
$ 10.44 From: Hicks -> Newt
$ 88.32 From: Bisho -> Burke
$ 45.0(From: Huds -> Gorm
$ 92.0(From: Vasqu -> Apon
Prev: 000049015089c7b64125575f5cf78fa3d2bba
Hash: 0000f843c73a7b3f5f3af6b7a4f5690a377326

Block: # 3
Nonce: 40596
Tx:
$ 3.14 From: Sylve
$ 2.12 From: Twee
$ 1.99 From: Daffy
Prev: 0000f843c73a7b3f5f3af6b7a
Hash: 0000a9dd50de891b2de8601

Why Mine Bitcoin?

Bitcoin uses a consensus mechanism known as proof-of-work, in which miners compete to solve cryptographic puzzles in order to be the first to complete a block, i**n exchange for a reward of Bitcoin.**

In the early days of Bitcoin, miners could use home computers to mint new coins that were worth a few dollars. As the market grew over time, the puzzles the miners had to solve to earn new coins grew more and more complex, requiring increased computing power and, by extension, energy.

What’s All the Fuss Over Bitcoin ?
Is Bitcoin Mining Bad for the Environment?

Bitcoin mining is a power intensive process. Miners are opening warehouses filled with computers than run around the clock

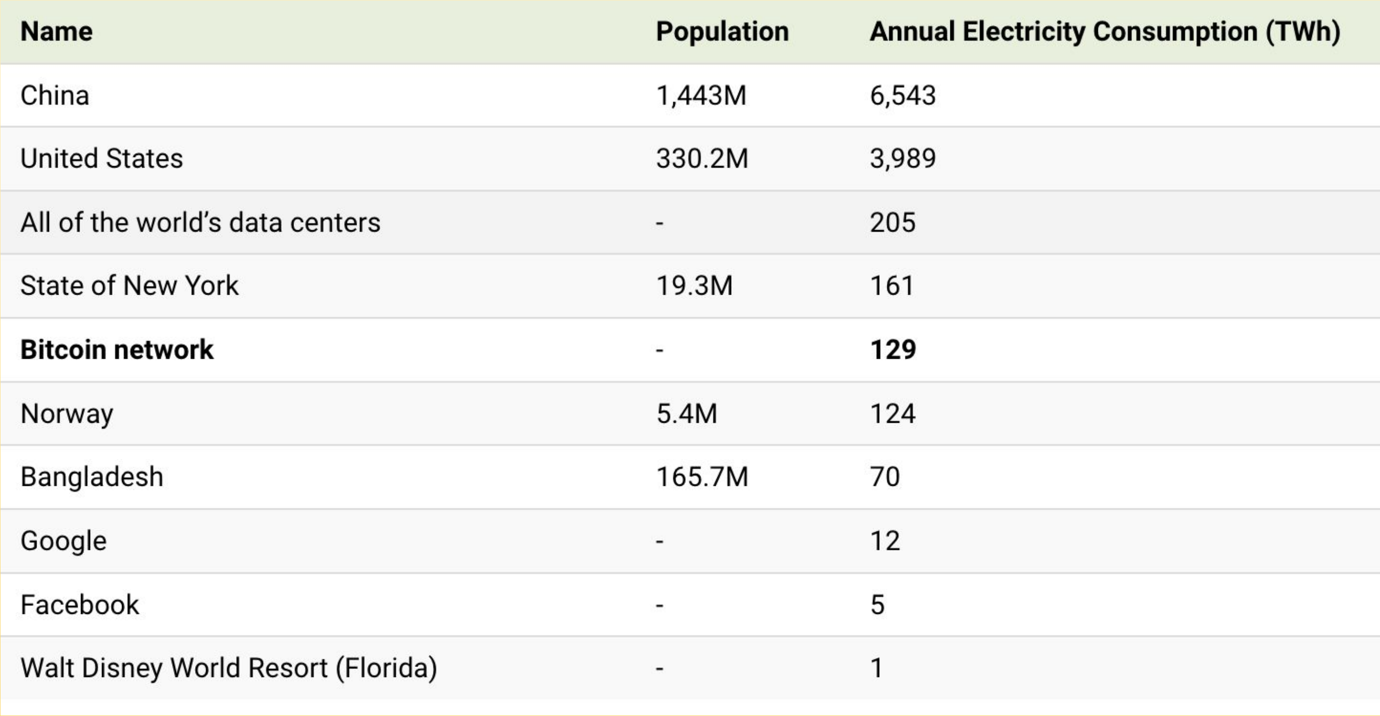
Bitcoin consumes an estimate 150 terawat-hours of electricity annually-— more than the entire country of Argentina, population 45 million.

Producing that energy emits some 65 megatons of carbon dioxide into the atmosphere annually — comparable to the emissions of Greece

Crypto impacts global air pollution and climate change.

Putting Bitcoin’s Power Consumption Into Perspective

***Note**: A terawatt hour (TWh) is a measure of electricity that represents 1 trillion watts sustained for one hour.*

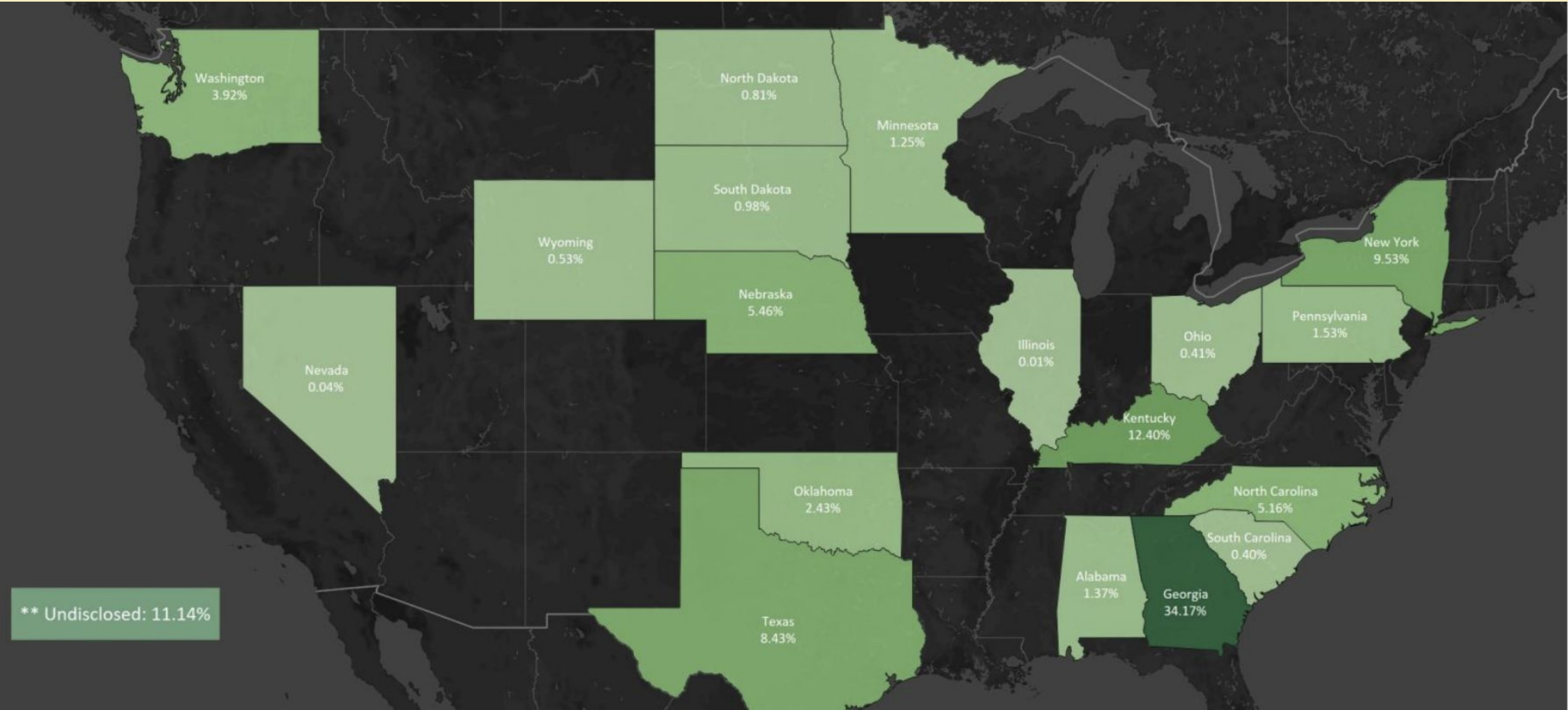


Name	Population	Annual Electricity Consumption (TWh)
China	1,443M	6,543
United States	330.2M	3,989
All of the world’s data centers	-	205
State of New York	19.3M	161
Bitcoin network	-	**129**
Norway	5.4M	124
Bangladesh	165.7M	70
Google	-	12
Facebook	-	5
Walt Disney World Resort (Florida)	-	1

“When it comes to Bitcoin’s energy use, it’s currently something of a ‘wildcatter’ market. The Texas grid operator estimates that crypto miners may increase energy demand by up to 6 gigawatts by mid-2023, roughly the equivalent of adding another Houston to the grid.”

Today, the lion’s share of Bitcoin mining takes place in the United States, where 35% of Bitcoin hashrate (the number of hashes produced each second. — the total computational power used to mine and process transactions — is now located.

Map of the percentage of Foundry USA’s Bitcoin hashrate by U.S. state, March, 2022.



Some companies in the U.S. are now bringing retired power plants back online in order to cash in on crypto.

Greenidge Generation, a natural gas-powered Bitcoin mining plant in the picturesque Finger Lakes region of upstate New York.The plant not only pollutes the air, but also harms the Seneca Lake ecosystem by discharging up to 134 million gallons of hot water a day into New York’s deepest glacial lake.

Ethical justification

- A - Bitcoin Maximalists
- B - Use less resources then all money markets used today
- C - Payments are P2P needing no extra resources
- D - Causing energy companies to devote more research into using wasted energy (e.g. Using methane gas escaping from oil wells for Bitcoin mining

bitcoin
Maximalism

- Belief that Bitcoin will eventually take the place of gold and the US dollar as the standard for global trade.
- According to the Crypto Fact Sheet released by the White House in 2021, the mining of all cryptocurrencies created between 25 and 40 Mt CO_2/y. The global gold mining alone creates around 100 Mt Co_2/y.

Uses less resources than current banking

“It’s the same situation as gold and gold mining. The marginal cost of gold mining tends to stay near the price of gold. Gold mining is a waste, but that waste is far less than the utility of having gold available as a medium of exchange. I think the case will be the same for Bitcoin. The utility of the exchanges made possible by Bitcoin will far exceed the cost of electricity used. Therefore, not having Bitcoin would be the net waste.”

- Satoshi Nakamoto

Cap on Mining

- All 21,000,000 Bitcoins will be mined by 2140.

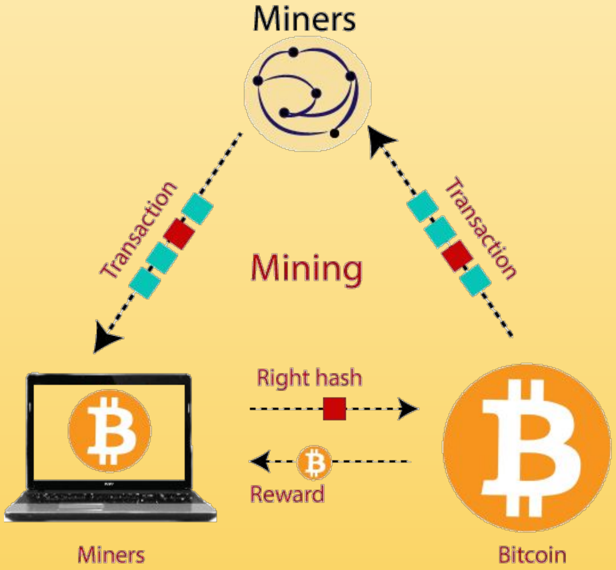
  -Using this, miners can calculate supply vs. cost benefit for mining.

Future Solutions: Renewable energy & P.O.W.

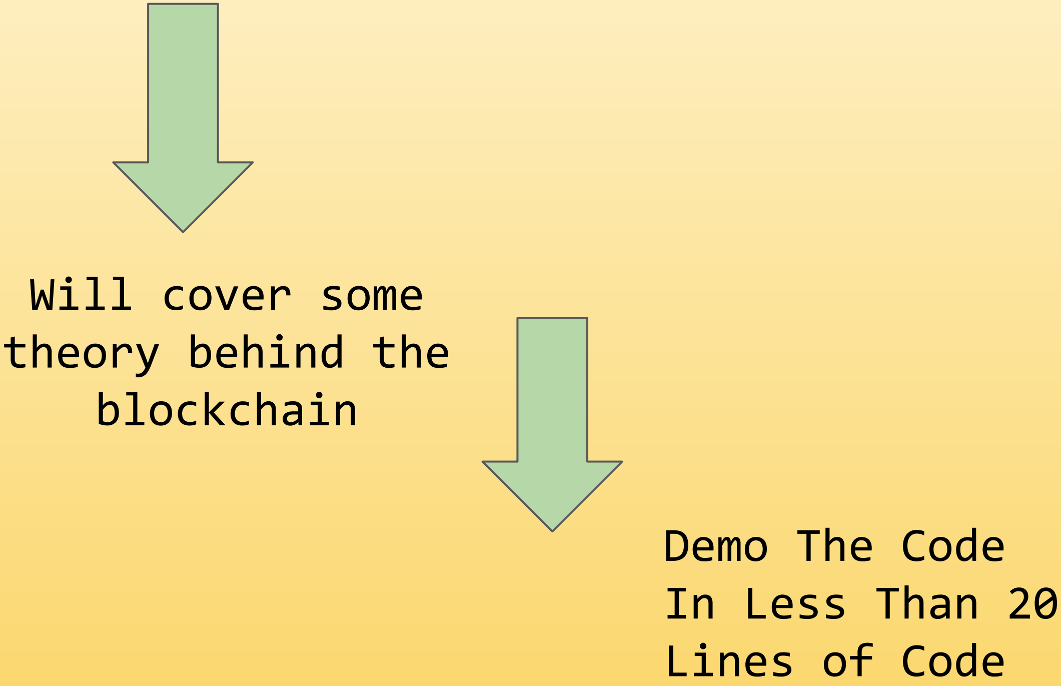
List and explanation of 3 POW cryptocurrencies:

- Cardano
- Ripple
- Nano

The Theory behind Bitcoin Mining and Blockchain



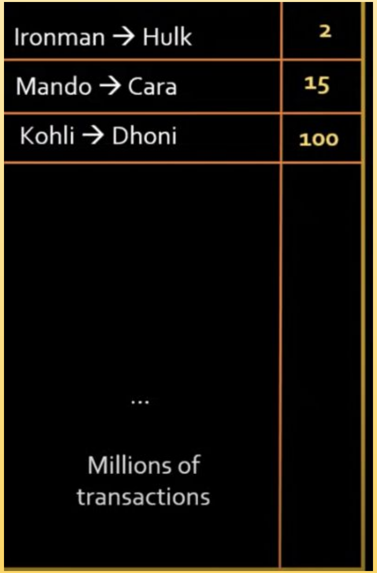
How Does Bitcoin Mining Work in Python?



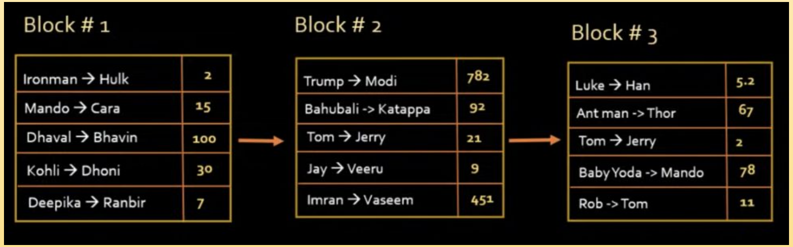
Will cover some theory behind the blockchain

Demo The Code In Less Than 20 Lines of Code

Bitcoin is a ledger: a set of transactions → stored in blocks that are linked together→linklist: one node and the address to the second node)



Ironman → Hulk	2
Mando → Cara	15
Kohli → Dhoni	100
... Millions of transactions	



Block # 1

Ironman → Hulk	2
Mando → Cara	15
Dhaval → Bhavin	100
Kohli → Dhoni	30
Deepika → Ranbir	7

Block # 2

Trump → Modi	782
Bahubali -> Katappa	92
Tom → Jerry	21
Jay → Veeru	9
Imran → Vaseem	451

Block # 3

Luke → Han	5.2
Ant man -> Thor	67
Tom → Jerry	2
Baby Yoda -> Mando	78
Rob -> Tom	11

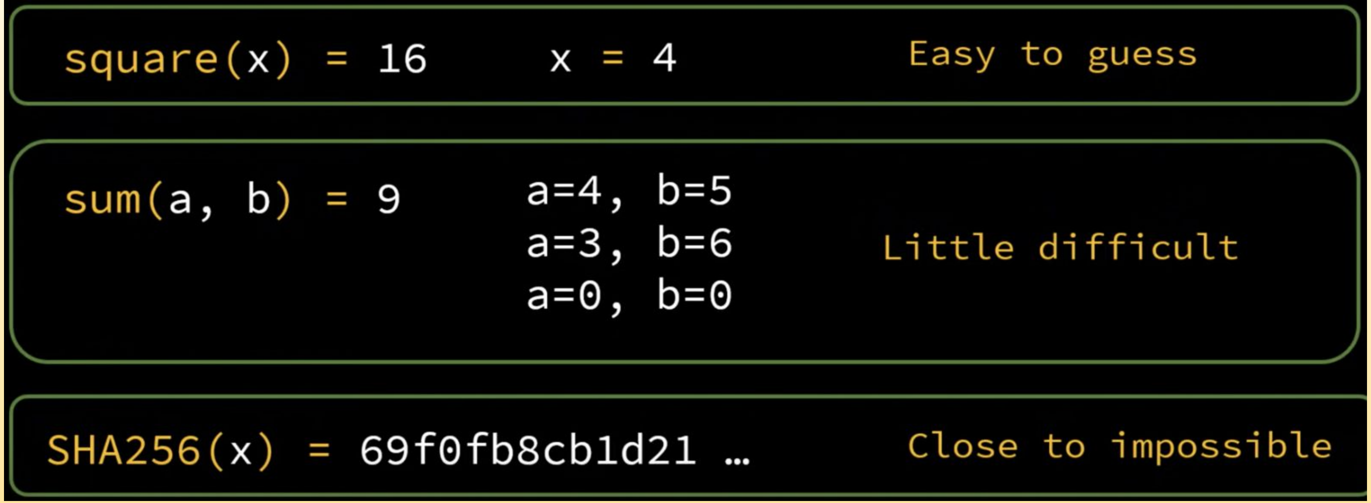
Each block = 1 megabyte

What is the Protocol to verify Transactions?

1. Bitcoin uses a Cryptographic Hash Algorithm Secure (SHA256)

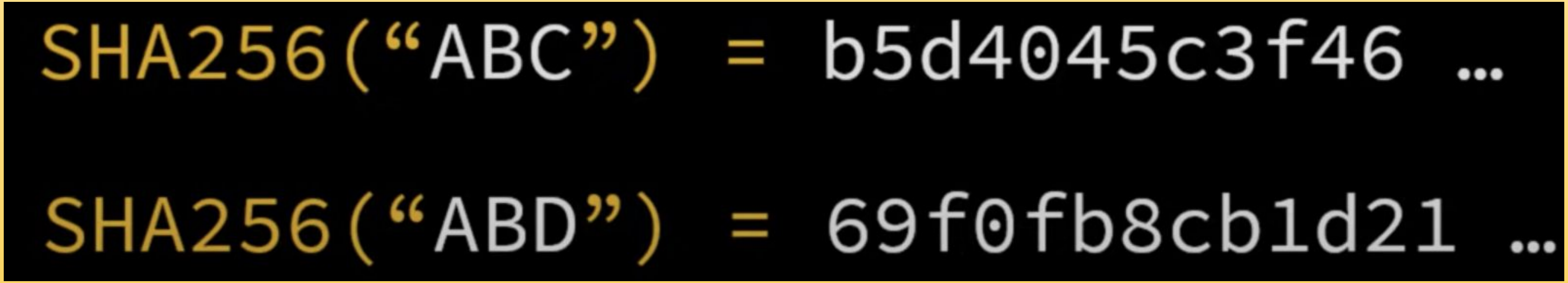
2. SHA256 is a cryptographic Secure hash Function: it takes an input of any length and it returns a hash of 64 characters long in hexadecimal(base 16: 0-9 and A-B-C-D-E-F)

3. 256 the number of bits it takes up in memory 256/4 bits (1 character) = 64 characters

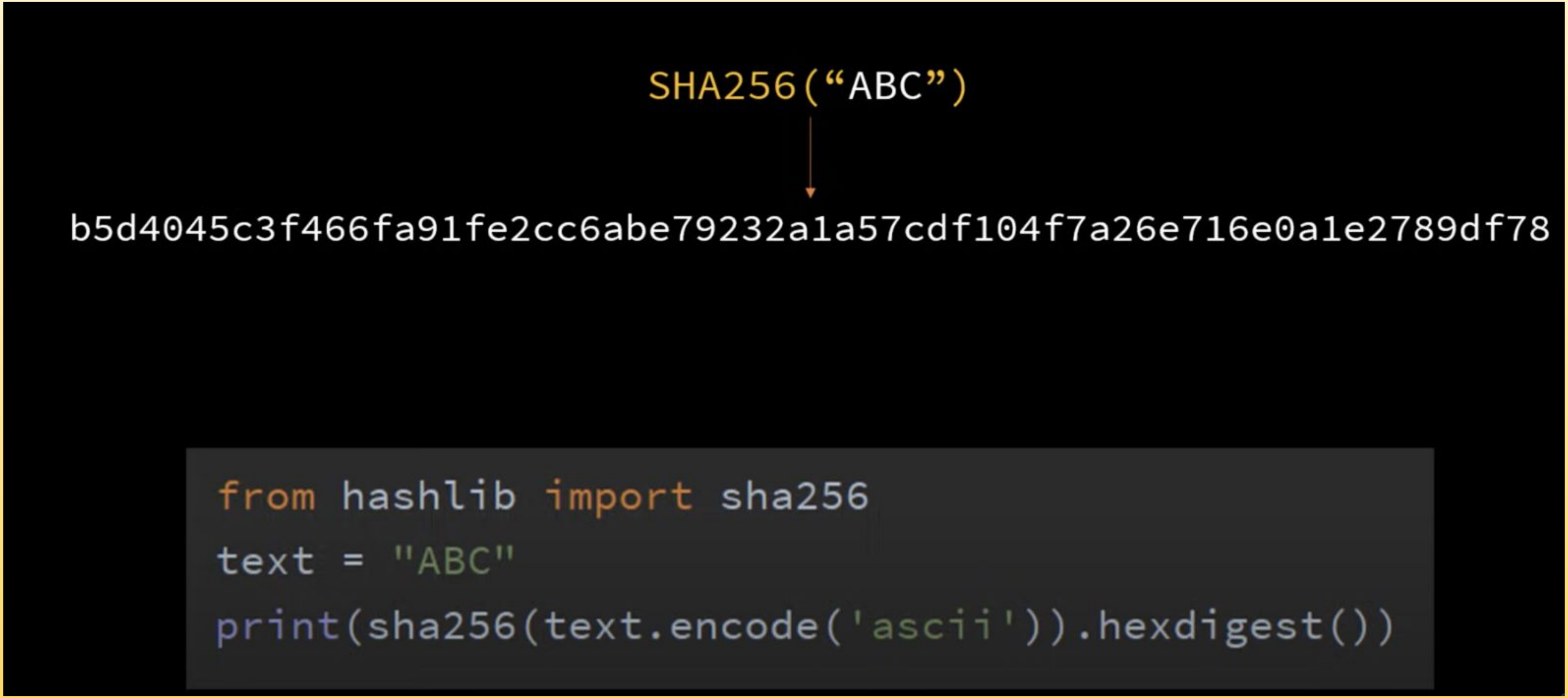


```
square(x) = 16       x = 4                Easy to guess

sum(a, b) = 9        a=4, b=5
                     a=3, b=6             Little difficult
                     a=0, b=0

SHA256(x) = 69f0fb8cb1d21 …               Close to impossible
```

SHA256(x) = 69f0fb8cb1d21 … Close to impossible



```
SHA256(“ABC”) = b5d4045c3f46 …

SHA256(“ABD”) = 69f0fb8cb1d21 …
```

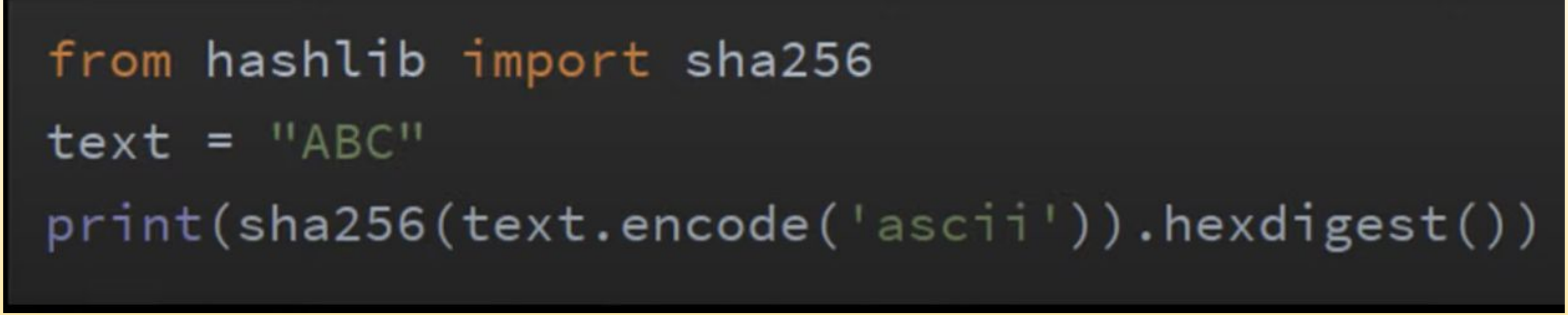


SHA256(“ABC”)

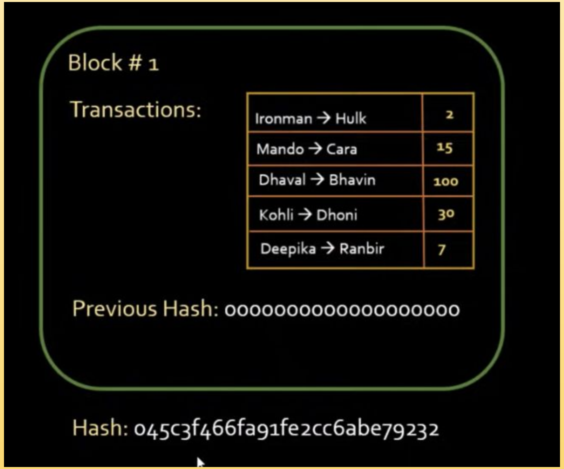
↓

b5d4045c3f466fa91fe2cc6abe79232a1a57cdf104f7a26e716e0a1e2789df78

```python
from hashlib import sha256
text = "ABC"
print(sha256(text.encode('ascii')).hexdigest())
```



```
from hashlib import sha256
text = "ABC"
print(sha256(text.encode('ascii')).hexdigest())
```



Block # 1

Transactions:

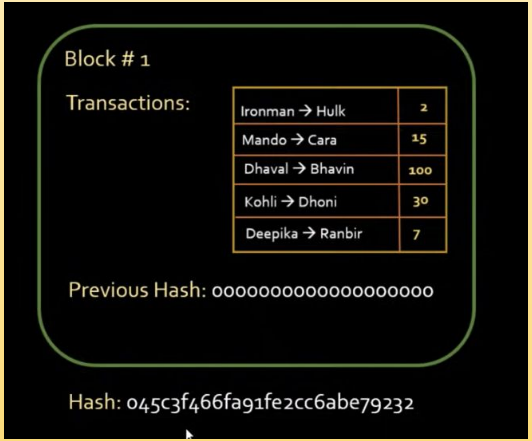
Ironman → Hulk	2
Mando → Cara	15
Dhaval → Bhavin	100
Kohli → Dhoni	30
Deepika → Ranbir	7

Previous Hash: 0000000000000000000

Hash: 045c3f466fa91fe2cc6abe79232

Convert the whole block into a string and supply that string to sha256 function to produce the 64 hexadecimal hash

Mining Difficulty: The mining difficulty of the bitcoin network is altered by adding or reducing the zeros at the front of the target hash order to maintaining a 10-minute duration for finding new blocks.



Block # 1

Transactions:

Ironman → Hulk	2
Mando → Cara	15
Dhaval → Bhavin	100
Kohli → Dhoni	30
Deepika → Ranbir	7

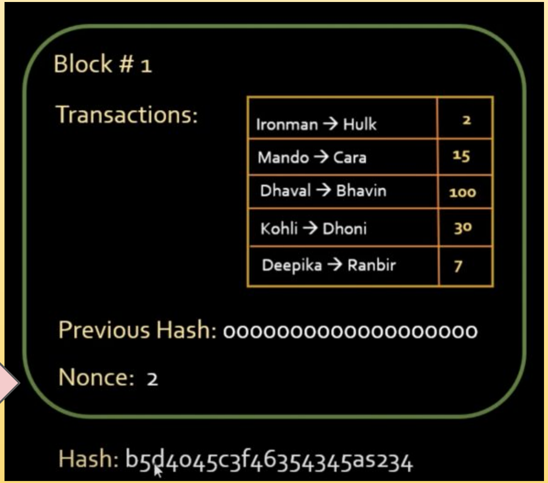
Previous Hash: 0000000000000000000

Hash: 045c3f466fa91fe2cc6abe79232

Ranges from 4 leading zeros to currently 30 leading zeros

Nonce

Number Only Once



Block # 1

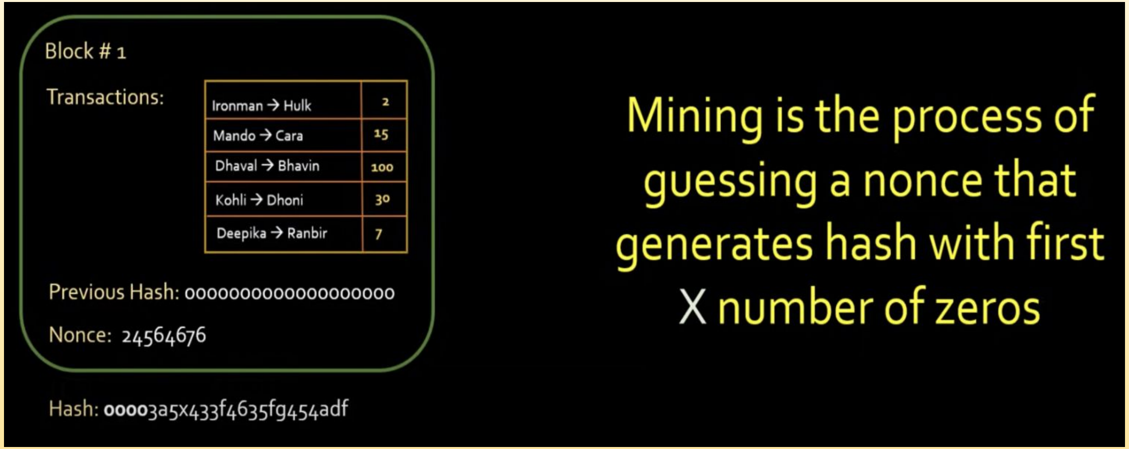
Transactions:

Ironman → Hulk	2
Mando → Cara	15
Dhaval → Bhavin	100
Kohli → Dhoni	30
Deepika → Ranbir	7

Previous Hash: 0000000000000000000

Nonce: 2

Hash: b5d4045c3f46354345as234



Block # 1

Transactions:

Ironman → Hulk	2
Mando → Cara	15
Dhaval → Bhavin	100
Kohli → Dhoni	30
Deepika → Ranbir	7

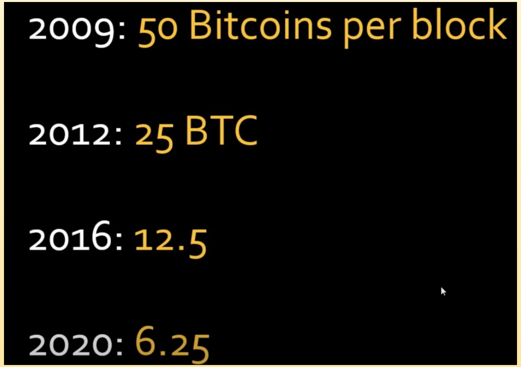
Previous Hash: 0000000000000000000

Nonce: 24564676

Hash: 00003a5x433f4635fg454adf

Mining is the process of guessing a nonce that generates hash with first X number of zeros

REWARD!



2009: 50 Bitcoins per block

2012: 25 BTC

2016: 12.5

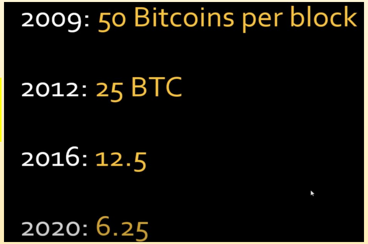
2020: 6.25

$$$$$$$$$$$$$$

NO ALGORITHM WORK! It is a Simple for loop (million ->trillion times) to try different Nonce to figure out a hash that starts with 4 zeros

This Block is Verified/Confirmed!

REWARD!



2009: 50 Bitcoins per block

2012: 25 BTC

2016: 12.5

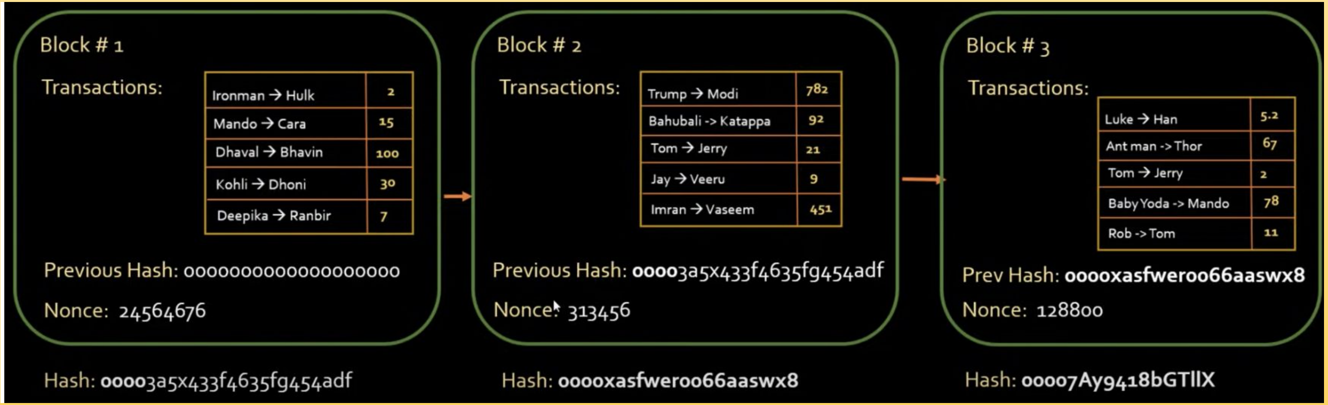
2020: 6.25

$$$$$$$$$$$$$$

There are about 1 million miners competing for the reward. The first person who makes the correct guess will be the winner !!!

It takes a lot of computational power and electricity

It is a Simple for loop (run million ->trillion times)



Block # 1

Transactions:

Ironman → Hulk	2
Mando → Cara	15
Dhaval → Bhavin	100
Kohli → Dhoni	30
Deepika → Ranbir	7

Previous Hash: 0000000000000000000

Nonce: 24564676

Hash: 00003a5x433f4635fg454adf

Block # 2

Transactions:

Trump → Modi	782
Bahubali -> Katappa	92
Tom → Jerry	21
Jay → Veeru	9
Imran → Vaseem	451

Previous Hash: 00003a5x433f4635fg454adf

Nonce: 313456

Hash: 0000xasfwer0066aaswx8

Block # 3

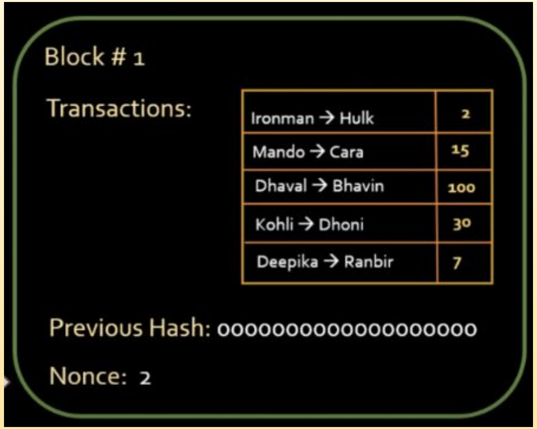
Transactions:

Luke → Han	5.2
Ant man -> Thor	67
Tom → Jerry	2
Baby Yoda -> Mando	78
Rob -> Tom	11

Prev Hash: 0000xasfwer0066aaswx8

Nonce: 128800

Hash: 00007Ay9418bGTIlX



Block # 1

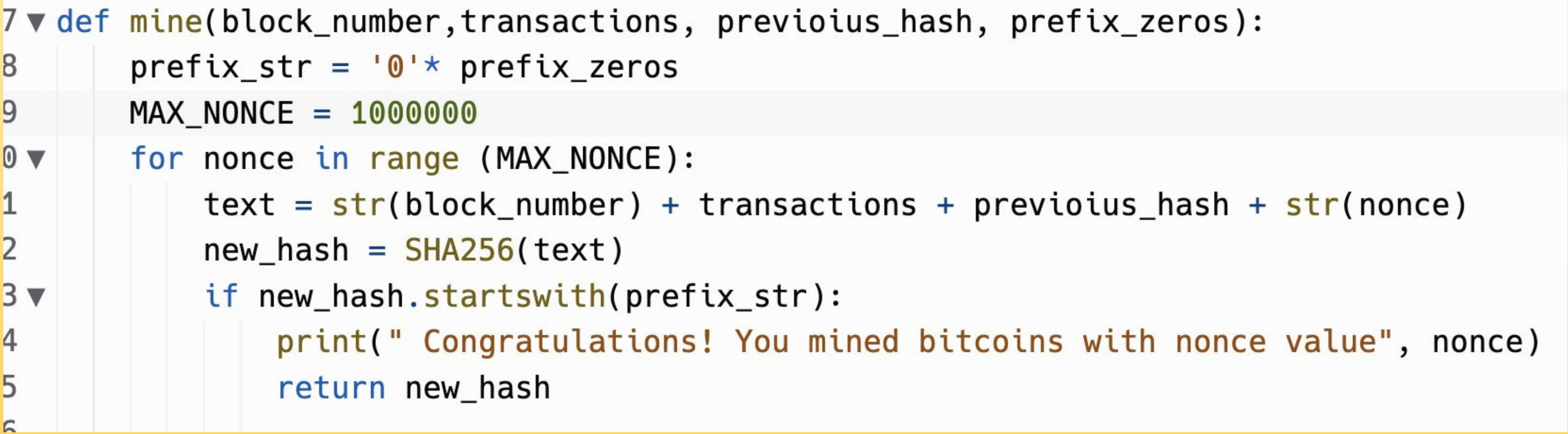
Transactions:

Ironman → Hulk	2
Mando → Cara	15
Dhaval → Bhavin	100
Kohli → Dhoni	30
Deepika → Ranbir	7

Previous Hash: 0000000000000000000

Nonce: 2

CODE DEMO Python



```python
def mine(block_number,transactions, previoius_hash, prefix_zeros):
    prefix_str = '0'* prefix_zeros
    MAX_NONCE = 1000000
    for nonce in range (MAX_NONCE):
        text = str(block_number) + transactions + previoius_hash + str(nonce)
        new_hash = SHA256(text)
        if new_hash.startswith(prefix_str):
            print(" Congratulations! You mined bitcoins with nonce value", nonce)
            return new_hash
```