Cryptocurrency Emissions

By Alise Braick & Ben Eckley

What is Cryptocurrency?

Cryptocurrency is a form of virtual currency that enable 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

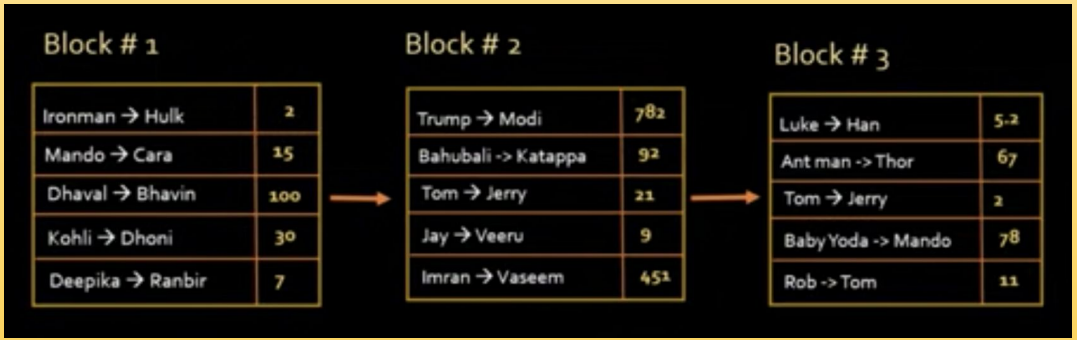
How Do Bitcoin Payment Process?

Payments are processed and verified **by a network of ordinary people with computers r**unning specialist software.

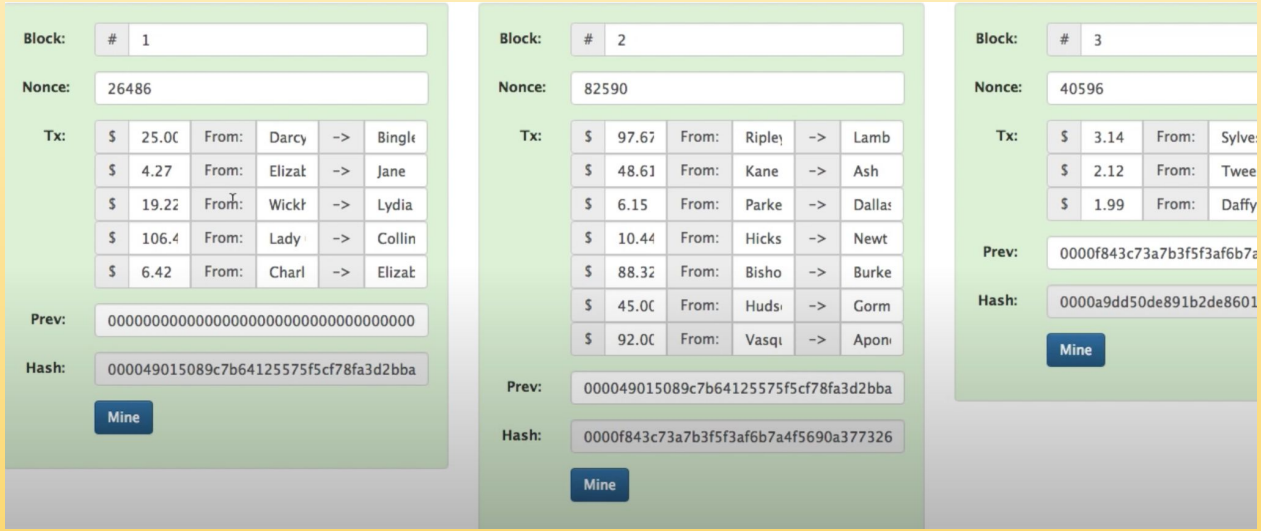
These volunteers are called **Bitcoin miners.** They use high-end computer hardware to crack increasingly complex, mathematical verification problems generated by Bitcoin’s source code

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.



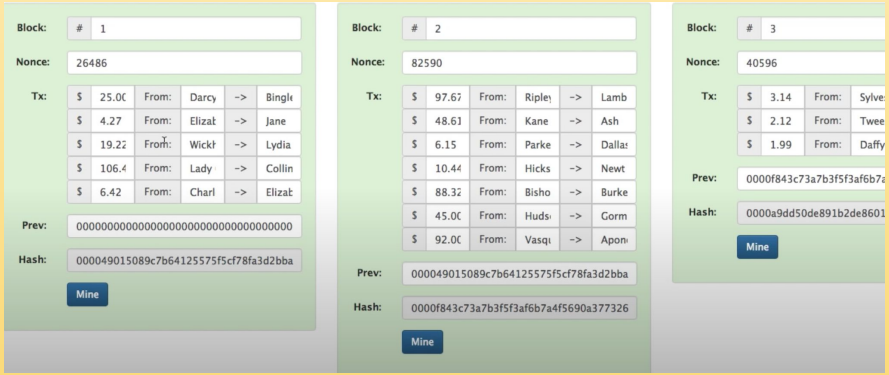
Each **new block links** back to the previous block containing information about older transactions. The blocks form a chain that links back all the way to the very first Bitcoin transaction.



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]



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, **in 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

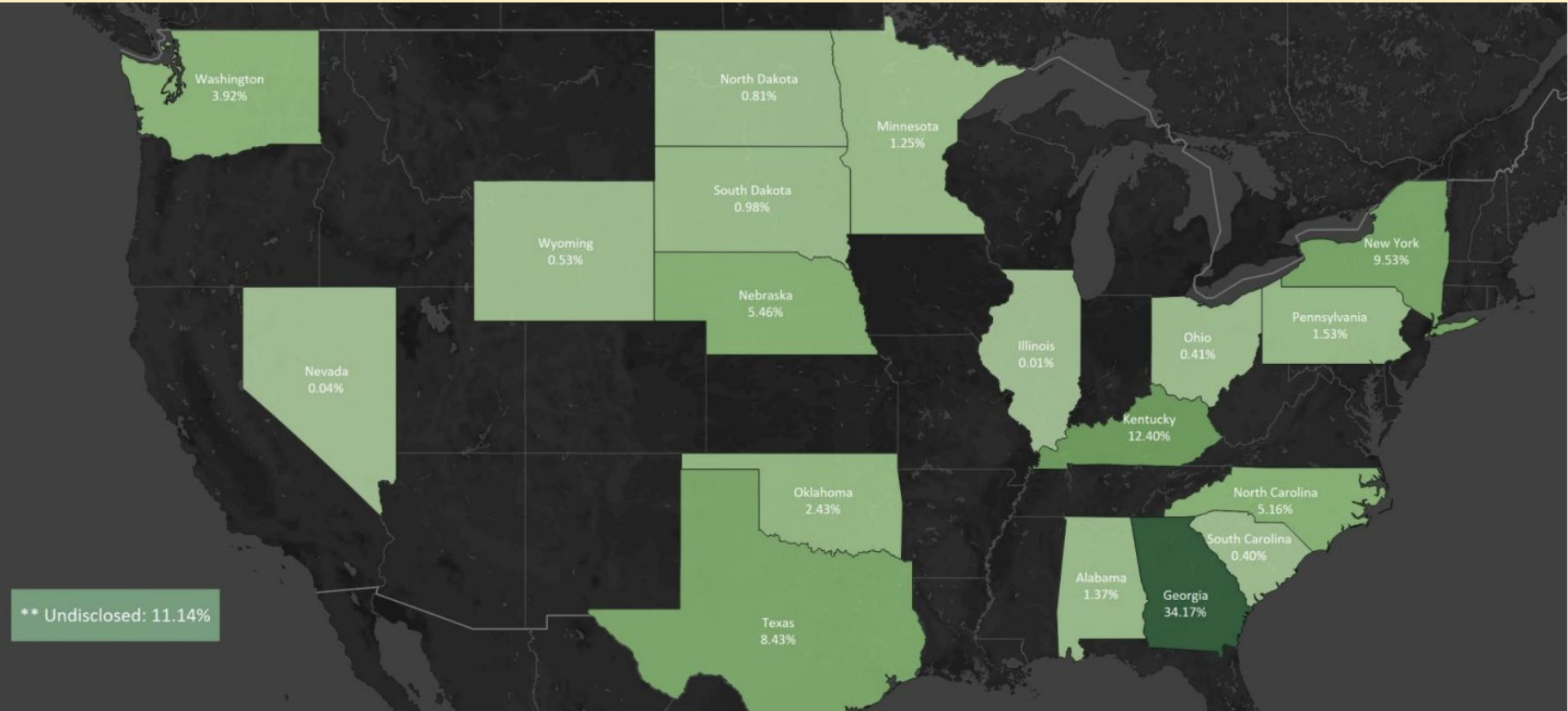
***Note**: A terawatt hour (TWh) is a measure of electricity that represents 1 trillion watts sustained for one hour.*

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.

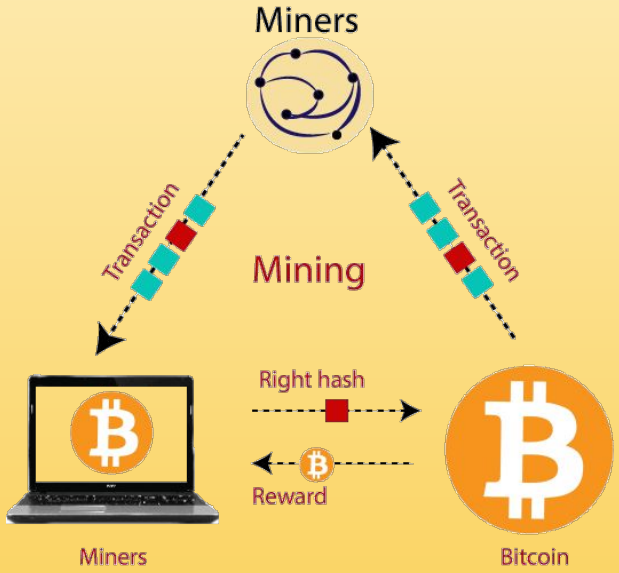
Greenidge Generation, a natural gas-powered Bitcoin mining plant in the picturesque Finger Lakes region of upstate New York.The plant not only pollutes the air, but also harms the Seneca Lake ecosystem by discharging up to 134 million gallons of hot water a day into New York’s deepest glacial lake.

WE NEED TO ADDRESS THAT (Ben)

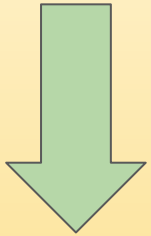
1. Ethical justification
    - A - articulates arguments on multiple sides.

FUTURE Solution ???? Renewable energy

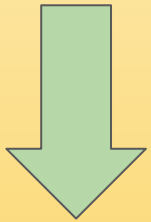
The Theory behind Bitcoin Mining and Blockchain



How Does Bitcoin Mining Work in Python?



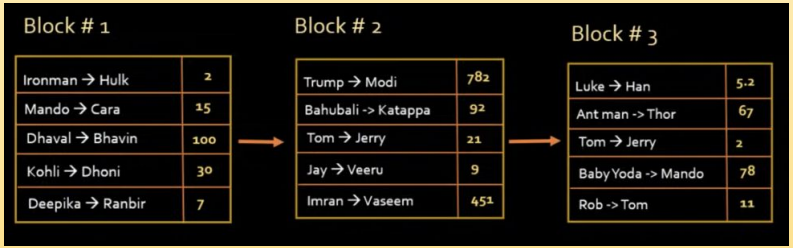
Will cover some theory behind the blockchain



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	



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
a=0, b=0
Little difficult

SHA256(x) = 69f0fb8cb1d21 … Close to impossible

SHA256(x) = 69f0fb8cb1d21 … Close to impossible

SHA256("ABC") = b5d4045c3f46 …

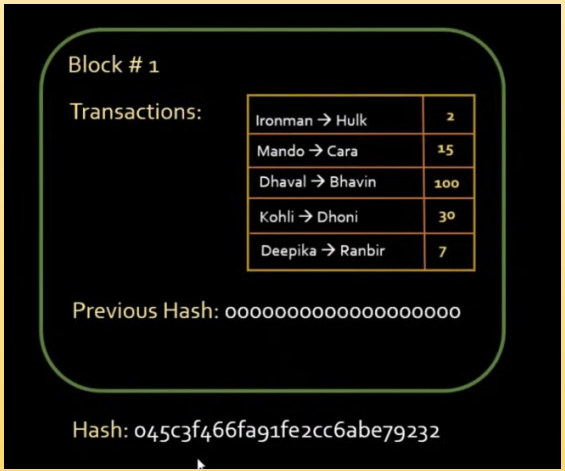
SHA256("ABD") = 69f0fb8cb1d21 …

SHA256(“ABC”)

b5d4045c3f466fa91fe2cc6abe79232a1a57cdf104f7a26e716e0a1e2789df78

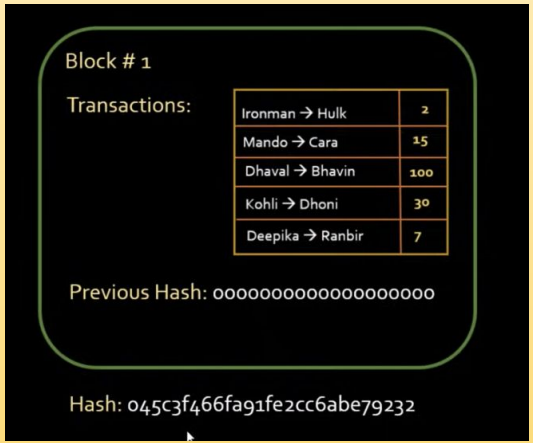
```
from hashlib import sha256
text = "ABC"
print(sha256(text.encode('ascii')).hexdigest())
```

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



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

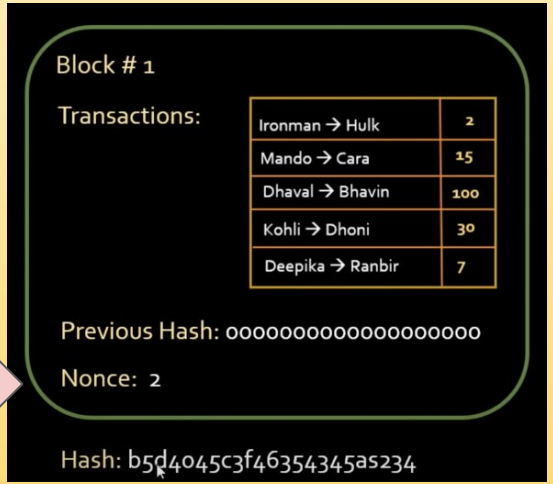
Mining Difficulty: The mining difficulty of the bitcoin network is altered by adding or reducing the zeros at the front of the target hash order to maintaining a 10-minute duration for finding new blocks.



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: 24564676

Hash: 0000**3a5x433f4635fg454adf**

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

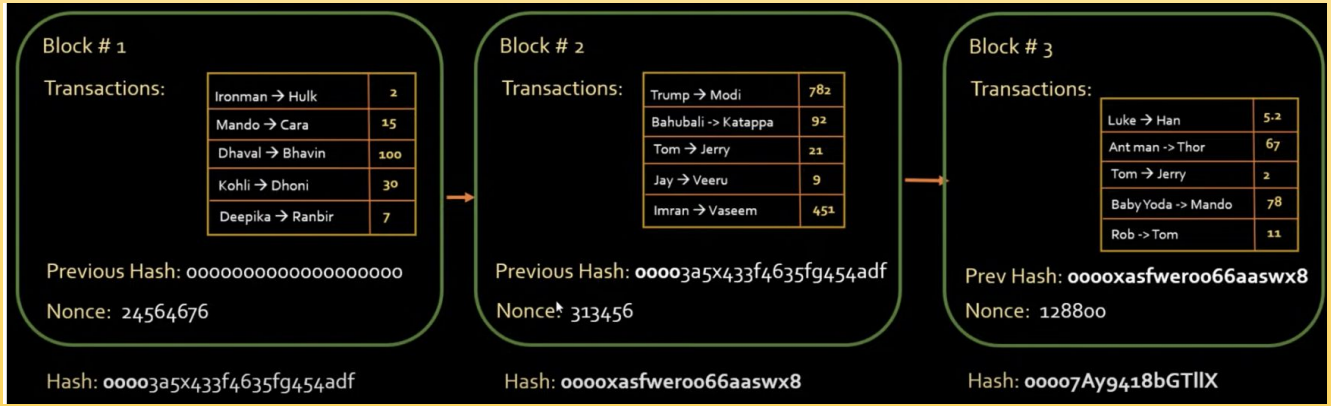
2020: 6.25

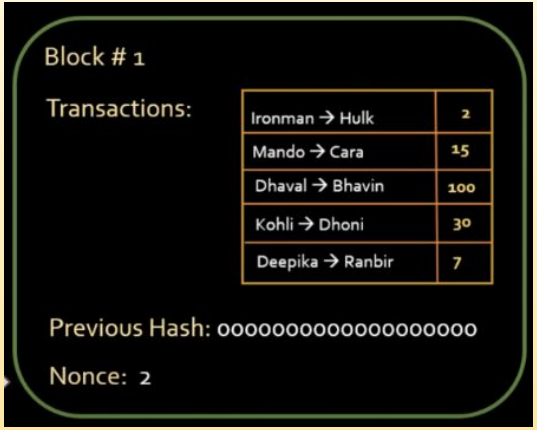
$$$$$$$$$$$$$

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)





CODE DEMO 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
```