CMSC 398F
Week #3
Blockchain Structure

Announcements

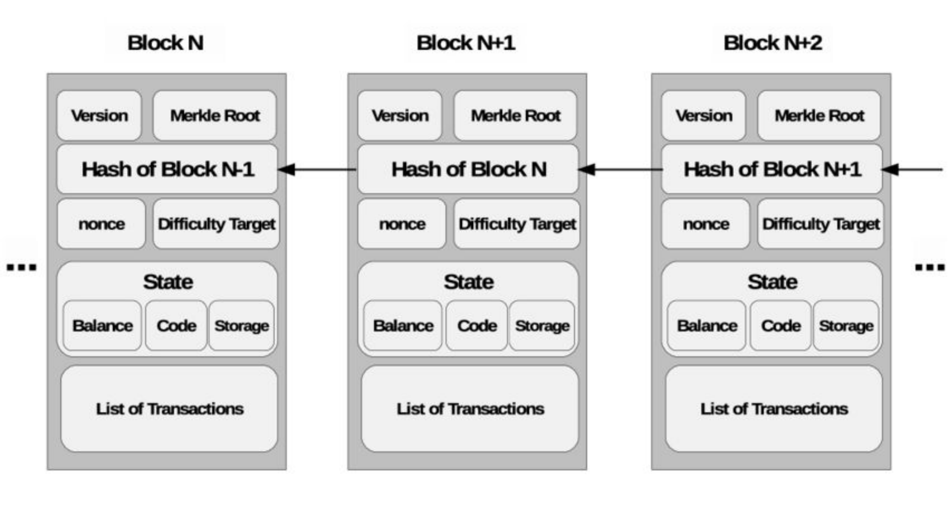
- Quiz 1 scores are out
- Quiz 2 was due this morning
- Quiz 3 has been released
- Project #1 will be released next week
- Join the class Piazza!
  - piazza.com/umd/fall2022/cmsc398f

Review Quiz 2 Answers

- Quiz answers are available through Canvas

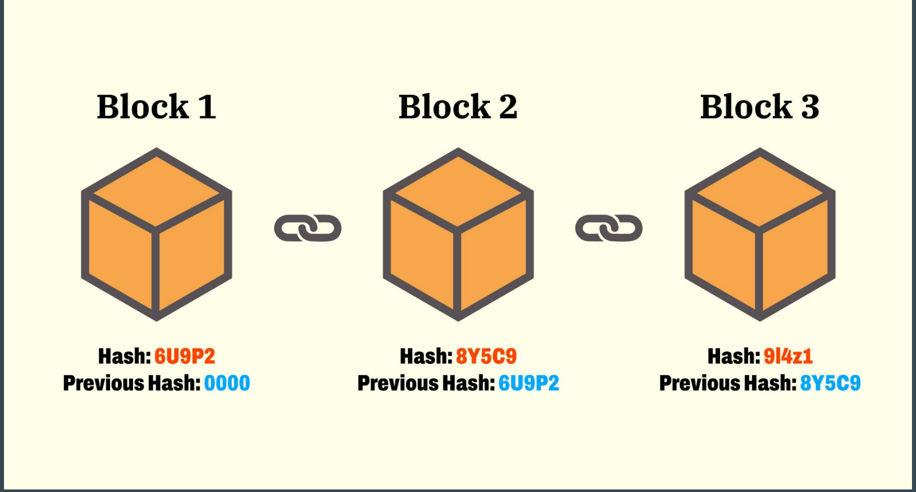
Blockchain Structure Review: Components of a Block

- Block Header:
  - Previous Block Hash
  - Root hash of Merkle tree
  - Nonce
  - Other Metadata: Timestamp, the goal of the current difficulty
- Block Body
  - List of Transactions



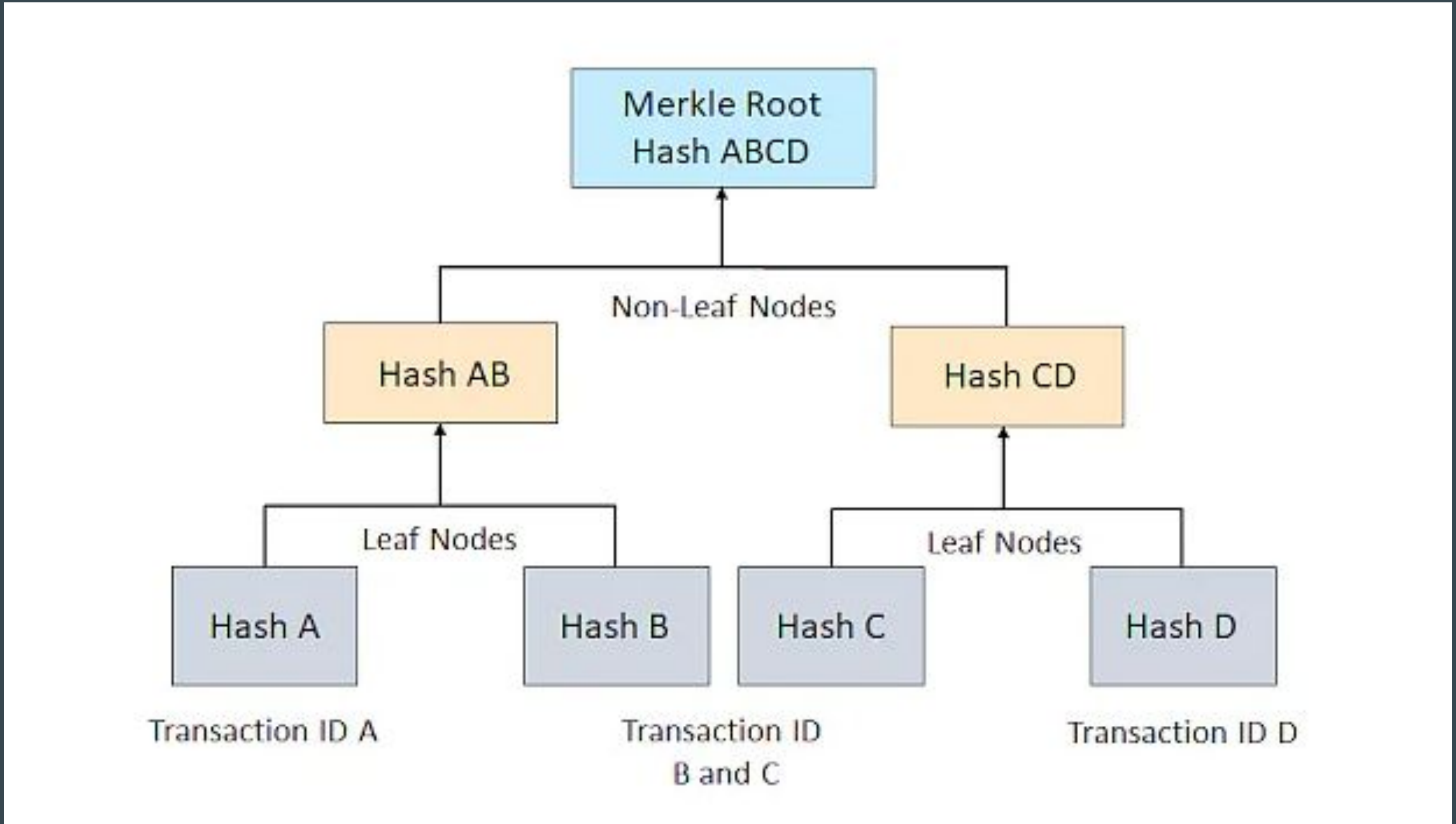
Components of a Block: Previous Block Hash

- The block header contains the hash to the previous block
  - This is the "chain" in blockchain
- Without this component, there would be no connection and chronology between each block.



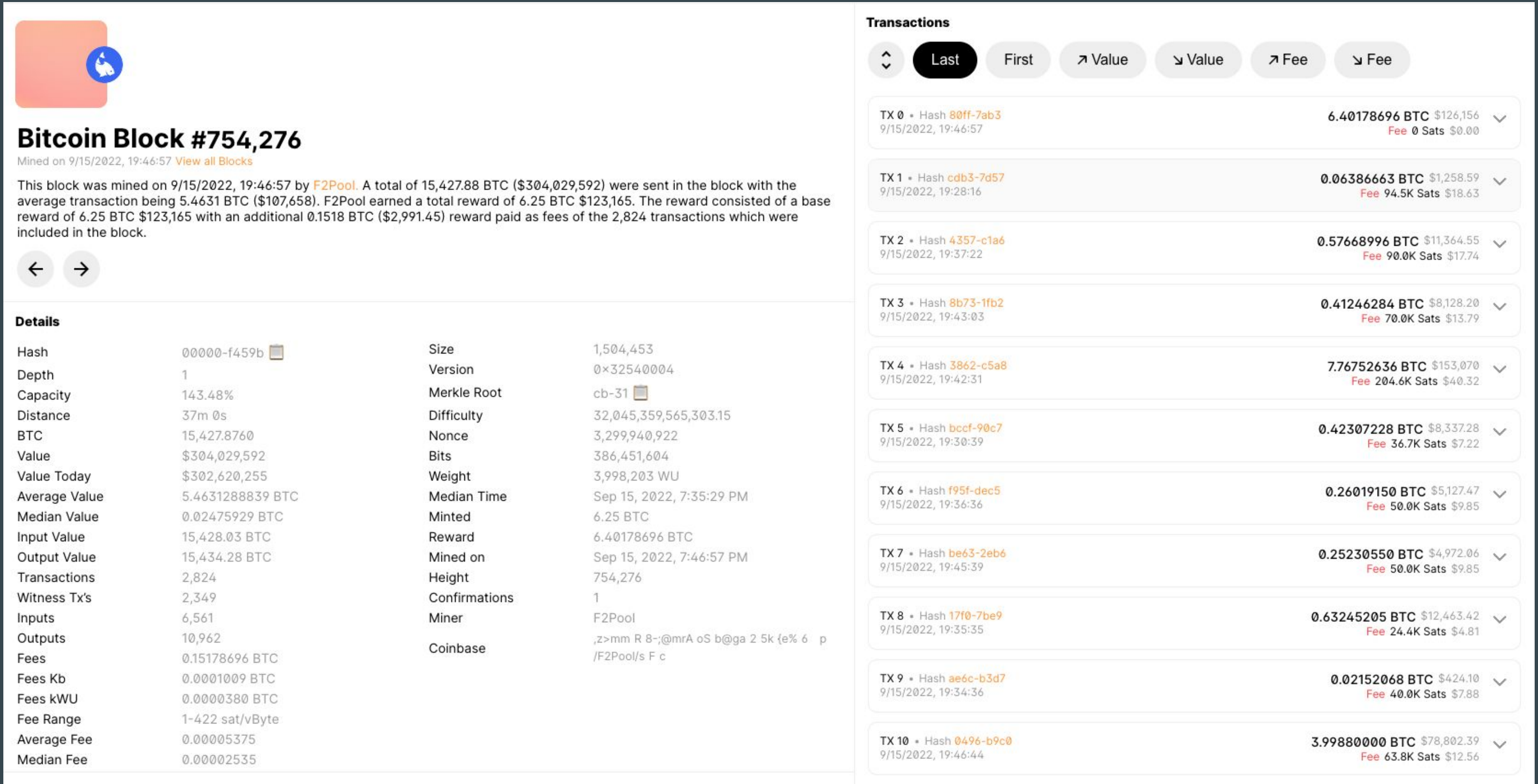
Components of a Block: List of Transactions

- Transactions are stored in the block with a so-called Merkle Tree
    - hash-based binary tree of transactions
- To develop this, transaction data is initially hashed. This hash then gets repeatedly hashed with other transactions hashes until a singular hash value remains
    - This value is called the "root hash"
- The root hash represents the information of all its "leaves" (individual transactions) and "branches" (hashes of the leaves)


Merkle Root
Hash ABCD
Non-Leaf Nodes
Hash AB
Hash CD
Leaf Nodes
Leaf Nodes
Hash A
Hash B
Hash C
Hash D
Transaction ID A
Transaction ID
B and C
Transaction ID D

Components of a Block: Nonce

- 32-bit integer that is included in the block
- The nonce will hash together with the previous block hash and merkle root hash to create the hash for the entire block
- A block hash is valid if it is less than a certain target, which usually means starting with a certain number of 0-bits (i.e., the hash must look like 0x000000023FB23..., not 0x12FD23A123...)
    - Small exceptions to this
- If the block has the correct hash, we call that nonce the "winning" nonce



Bitcoin Block #754,276

Mined on 9/15/2022, 19:46:57 View all Blocks

This block was mined on 9/15/2022, 19:46:57 by F2Pool. A total of 15,427.88 BTC ($304,029,592) were sent in the block with the average transaction being 5.4631 BTC ($107,658). F2Pool earned a total reward of 6.25 BTC $123,165. The reward consisted of a base reward of 6.25 BTC $123,165 with an additional 0.1518 BTC ($2,991.45) reward paid as fees of the 2,824 transactions which were included in the block.

← →

Details

Hash	00000-f459b
Depth	1
Capacity	143.48%
Distance	37m 0s
BTC	15,427.8760
Value	$304,029,592
Value Today	$302,620,255
Average Value	5.4631288839 BTC
Median Value	0.02475929 BTC
Input Value	15,428.03 BTC
Output Value	15,434.28 BTC
Transactions	2,824
Witness Tx's	2,349
Inputs	6,561
Outputs	10,962
Fees	0.15178696 BTC
Fees Kb	0.0001009 BTC
Fees kWU	0.0000380 BTC
Fee Range	1-422 sat/vByte
Average Fee	0.00005375
Median Fee	0.00002535

Size	1,504,453
Version	0×32540004
Merkle Root	cb-31
Difficulty	32,045,359,565,303.15
Nonce	3,299,940,922
Bits	386,451,604
Weight	3,998,203 WU
Median Time	Sep 15, 2022, 7:35:29 PM
Minted	6.25 BTC
Reward	6.40178696 BTC
Mined on	Sep 15, 2022, 7:46:57 PM
Height	754,276
Confirmations	1
Miner	F2Pool
Coinbase	,z>mm R 8-;@mrA oS b@ga 2 5k {e% 6 p /F2Pool/s F c

Transactions

TX 0 • Hash 80ff-7ab3
9/15/2022, 19:46:57
6.40178696 BTC $126,156
Fee 0 Sats $0.00

TX 1 • Hash cdb3-7d57
9/15/2022, 19:28:16
0.06386663 BTC $1,258.59
Fee 94.5K Sats $18.63

TX 2 • Hash 4357-c1a6
9/15/2022, 19:37:22
0.57668996 BTC $11,364.55
Fee 90.0K Sats $17.74

TX 3 • Hash 8b73-1fb2
9/15/2022, 19:43:03
0.41246284 BTC $8,128.20
Fee 70.0K Sats $13.79

TX 4 • Hash 3862-c5a8
9/15/2022, 19:42:31
7.76752636 BTC $153,070
Fee 204.6K Sats $40.32

TX 5 • Hash bccf-90c7
9/15/2022, 19:30:39
0.42307228 BTC $8,337.28
Fee 36.7K Sats $7.22

TX 6 • Hash f95f-dec5
9/15/2022, 19:36:36
0.26019150 BTC $5,127.47
Fee 50.0K Sats $9.85

TX 7 • Hash be63-2eb6
9/15/2022, 19:45:39
0.25230550 BTC $4,972.06
Fee 50.0K Sats $9.85

TX 8 • Hash 17f0-7be9
9/15/2022, 19:35:35
0.63245205 BTC $12,463.42
Fee 24.4K Sats $4.81

TX 9 • Hash ae6c-b3d7
9/15/2022, 19:34:36
0.02152068 BTC $424.10
Fee 40.0K Sats $7.88

TX 10 • Hash 0496-b9c0
9/15/2022, 19:46:44
3.99880000 BTC $78,802.39
Fee 63.8K Sats $12.56

"Bitcoin mining is the process by which new bitcoins are entered into circulation. It is also the way the network confirms new transactions and is a critical component of the blockchain ledger's maintenance and development."

Mining

- When a Bitcoin transaction occurs, it is grouped together in a mathematically protected “block” with other transactions that have happened in the same time frame.
- These blocks cannot be added to the Blockchain until they are verified by miners.
- Miners are computers on the Bitcoin network, who use their computational power validate blocks

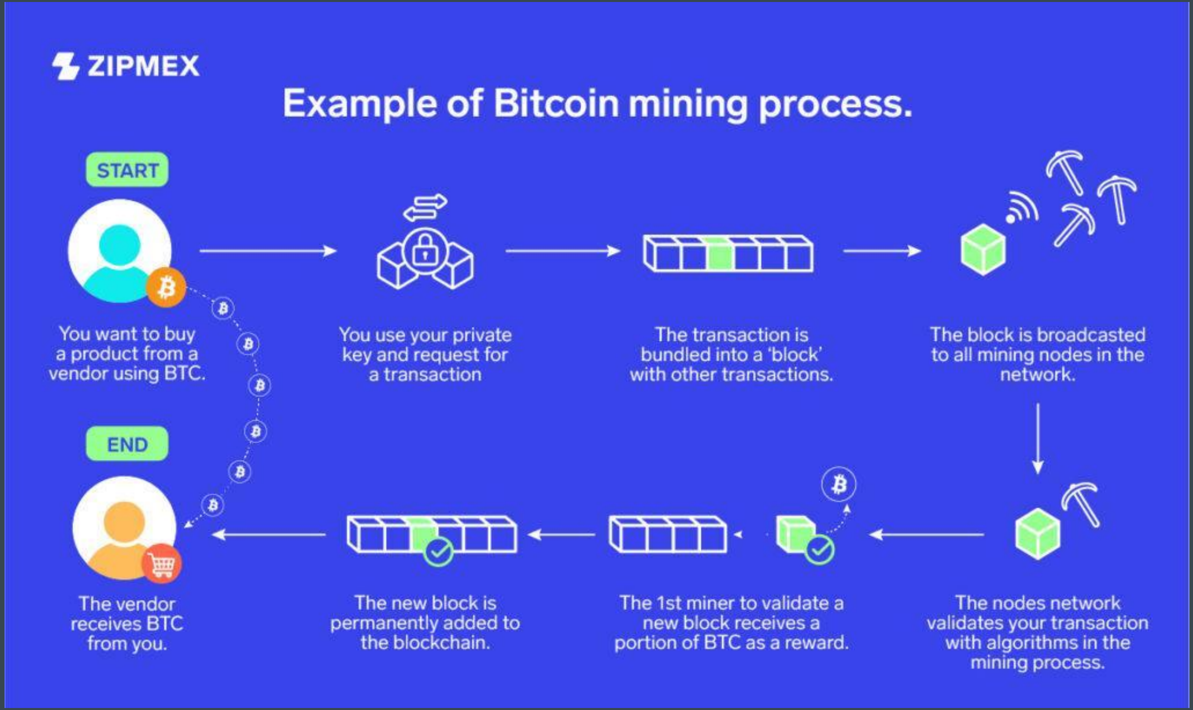
Mining

- Say we have a block of transactions that needs to be verified. How is this actually done?
- Recall that the Nonce is a variable value added to each block.
- The math problem stipulates that the first miner to produce a hash with a certain amount of leading 0s will be the winner of that block and be able to add it to the network.
- Miners continuously change the Nonce until SHA256 hash function results in a hash with a certain amount of leading 0s

Example

- Say that Om sends Soham 10 BTC
    - It gets added to a block, along with other transactions, which is hashed by the BTC network into "9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08"
- The crypto network says: find the Nonce that when appended to the block, produces a hash with 10 or less leading 0s.
- Computers on the network work hard to find this hash. Once it is found, the block is validated and gets added to the network
- If the Nonce cannot be found, the block cannot be validated
- Once the correct hash is found, the transaction and the hash are permanently stored in the blockchain, and if anyone tries to change the information in the block, the hashes will mismatch.

Mining: Bringing it all together



ZIPMEX

Example of Bitcoin mining process.

START

You want to buy a product from a vendor using BTC.

You use your private key and request for a transaction

The transaction is bundled into a 'block' with other transactions.

The block is broadcasted to all mining nodes in the network.

The nodes network validates your transaction with algorithms in the mining process.

The 1st miner to validate a new block receives a portion of BTC as a reward.

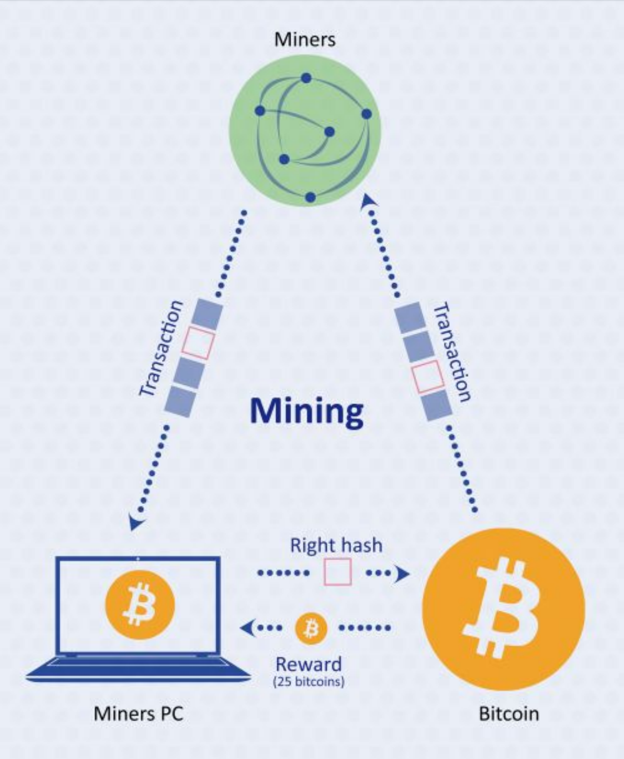
The new block is permanently added to the blockchain.

END

The vendor receives BTC from you.

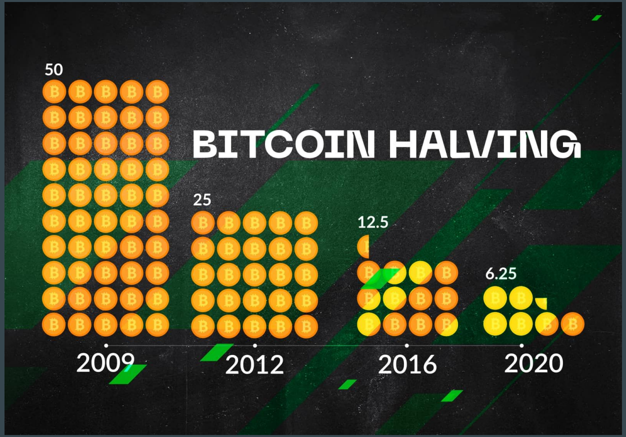
Coinbase Transactions

- A coinbase transaction is the first transaction in a block. It is a unique type of bitcoin transaction that can be created by a miner.
- When BTC first came out, the reward for mining one block was 50 BTC.
- Currently, the mining award is sitting at 6.25 BTC.
- It is expected that by 2026, the mining reward will be 0.0061 BTC for each BTC.
- Why does this happen? Halving.



Bitcoin Halving

- One of the most pivotal events on Bitcoin's blockchain is the halving, when the supply of new bitcoins is cut in half.
- Currently, miners are rewarded 6.25 BTC
  - In 2024, this will fall to 3.125 BTC
- Each halving reduces the rate of inflation, thereby creating upwards pressure on the Bitcoin price.
- Occurs around every 4 years
- The total number of BTC in circulation will be capped at 21 million.
- As of June 2022, there are 19.07 BTC in circulation



Why coinbase transactions?

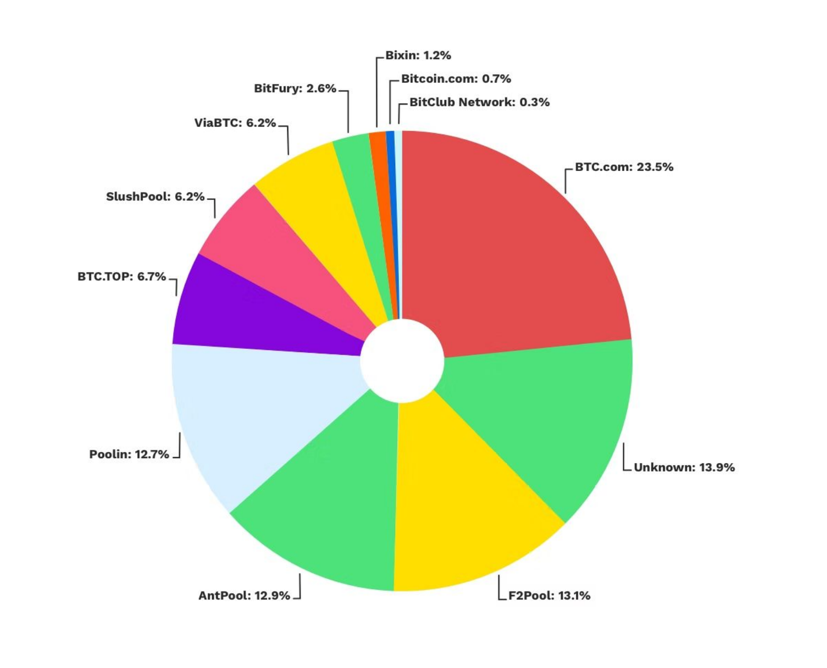
- The purpose of a coinbase transaction is to provide miners with an incentive so that they keep supporting the network. If miners are not mining, then no new transactions will be added to the blockchain.
- Supply and Demand:
  - Help increase the supply of BTC in circulation
  - Cover up for lost BTC
  - Coinbase transaction sets a limit for the number of BTC (21 Million)

Difficulty in Bitcoin

- More and more people mine because they want to win the reward
- As more people mine, and add their computational resources to the network, the Nonce will be found faster and faster
- The Bitcoin protocol has an explicit **goal** to add a block once every 10 minutes.
- Setting difficulty is accomplished by establishing a "target" for the hash: the lower the target, the smaller the set of valid hashes, and the harder it is to generate one. In practice, this means a hash that starts with a very long string of zeros.
- Every 2016 blocks, Bitcoin measures how long it took to solve the last 2016 blocks and adjusts the difficulty (leading 0s)
- Other cryptocurrency networks also define a target rate for blocks to be added, and adjust the difficulty accordingly

Mining pools

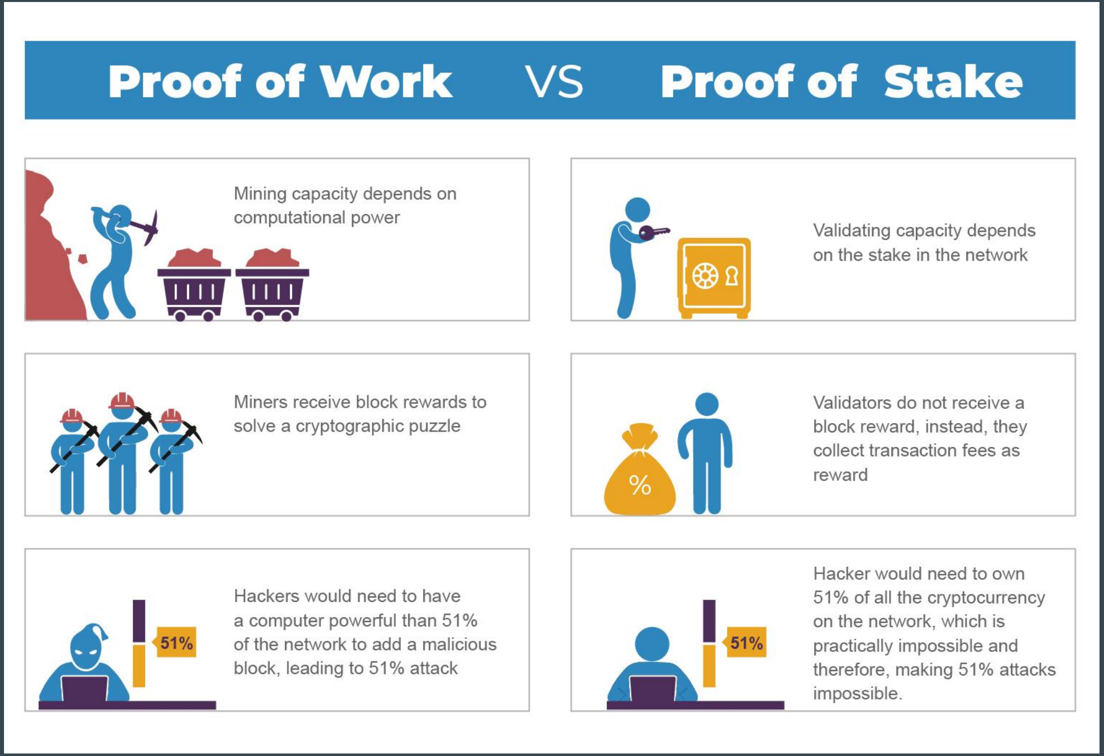
- A mining pool is the pooling of resources by miners, who share their processing power over a network, to split the reward equally.
- Block reward is usually distributed among miners based on the amount of hashing power they provide to the collective pool
- Why?
- In addition to creating new coins, pools simultaneously work to keep bitcoin’s network functioning
- Mining is only profitable if you make more in bitcoin than you spend on electricity per month



Proof-Of-Work

- Proof of work describes the process that allows the bitcoin network to remain robust by making the process of mining, or recording transactions, difficult.
- This entire process of mining and validating blocks, so that new blocks can be appended is known as proof-of-work.

ETH Merge



Proof of Work VS Proof of Stake

Mining capacity depends on computational power

Validating capacity depends on the stake in the network

Miners receive block rewards to solve a cryptographic puzzle

Validators do not receive a block reward, instead, they collect transaction fees as reward

Hackers would need to have a computer powerful than 51% of the network to add a malicious block, leading to 51% attack

Hacker would need to own 51% of all the cryptocurrency on the network, which is practically impossible and therefore, making 51% attacks impossible.