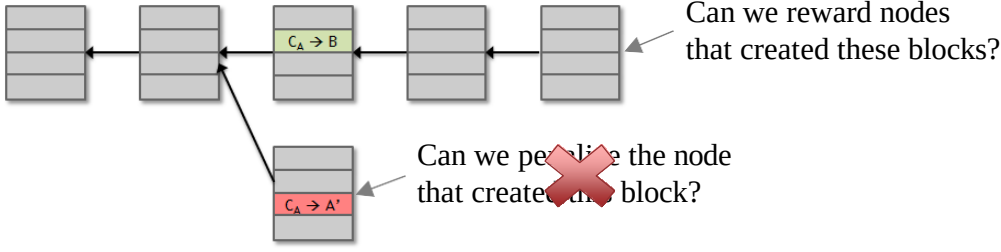
# Introduction to Cryptocurrency

## Proof of Work

# ASSUMPTION OF HONESTY IS PROBLEMATIC

- Can we give nodes incentives for behaving honestly?




- Everything so far is just a distributed consensus protocol.
- But now we utilize the fact that the currency has value.

# INCENTIVE 1: BLOCK REWARD

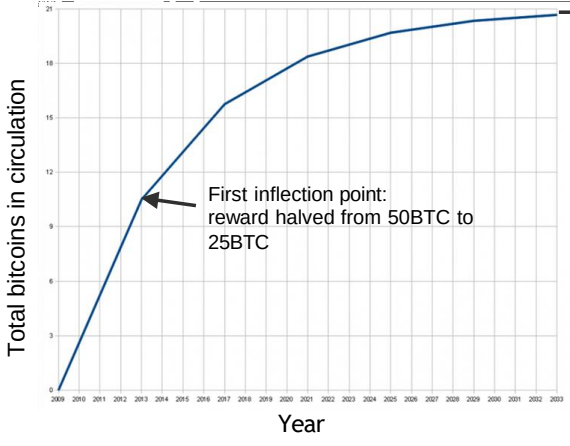
- Creator of block gets to
  - include special coin-creation transaction in the block
  - choose recipient address of this transaction

- Value is fixed: currently 6.25 BTC, halves every 4 years.

- Block creator gets to collect the reward only if the block ends up on long-term consensus branch!

- Note: This is the only way to create new Bitcoins!

# THERE'S A FINITE SUPPLY OF BITCOINS



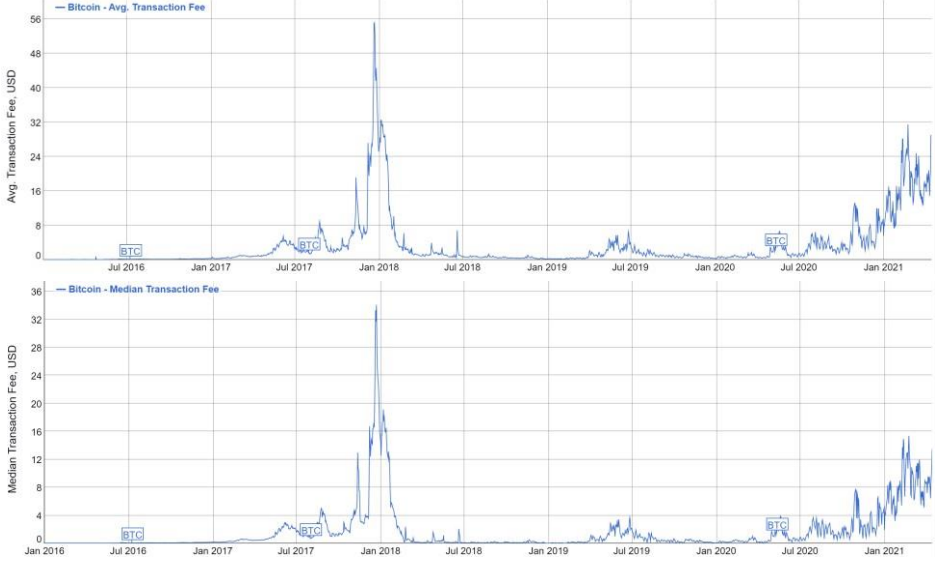

Total supply: 21 million

- Block reward is how new Bitcoins are created
- Runs out in 2140. No new Bitcoins unless rules change

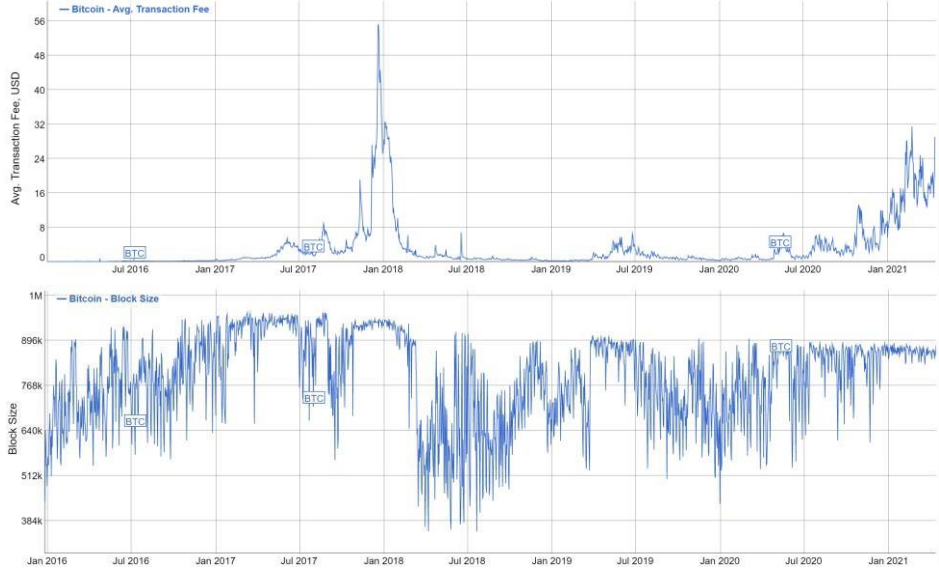
# INCENTIVE 2: TRANSACTION FEES

- Creator of transaction can choose to make output value less than input value.
- Remainder is a transaction fee and goes to block creator.
- Purely voluntary, like a tip.

# AVERAGE TRANSACTION FEE



# AVERAGE TRANSACTION FEE

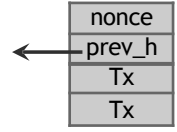


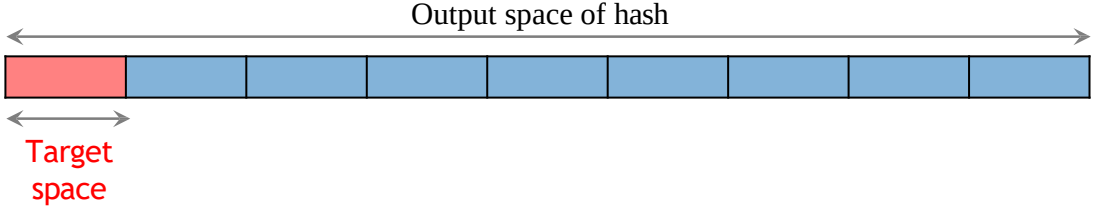
# RANDOM NODE: PROOF OF WORK

- To approximate selecting a random node:
  - select nodes in proportion to a resource
  - that no one can monopolize (we hope)
- In proportion to computing power: proof-of-work
- Equivalent view of proof-of-work
  - Select nodes in proportion to computing power
  - Let nodes compete for right to create block
  - Make it moderately hard to create new identities

# HASH PUZZLES

To create block, find nonce s.t.
H(nonce ‖ prev_hash ‖ merkle_root) < target




If hash function is secure:
only way to succeed is to try enough nonces until you get lucky

# PROPERTIES OF HASH PUZZLES

Property 1: Must be (moderately) difficult to compute

Property 2: The Cost must be “parameterizable”

Property 3: Must be trivial to verify

# 1. DIFFICULT TO COMPUTE

- It takes about $2^{32} \times$ Difficulty hashes to find a block.


- Only some nodes bother to compete: **Miners**

# 2. PARAMETRIZABLE COST

- Nodes automatically re-calculate the target every 2016 blocks (about every two weeks).
- Goal: average time between blocks = 10 minutes
- Adjust difficulty to meet 10-minute goal.
  - Current difficulty is around $2^{44} \rightarrow 2^{76}$ hash/block
  - Maximum difficulty is $2^{224}$

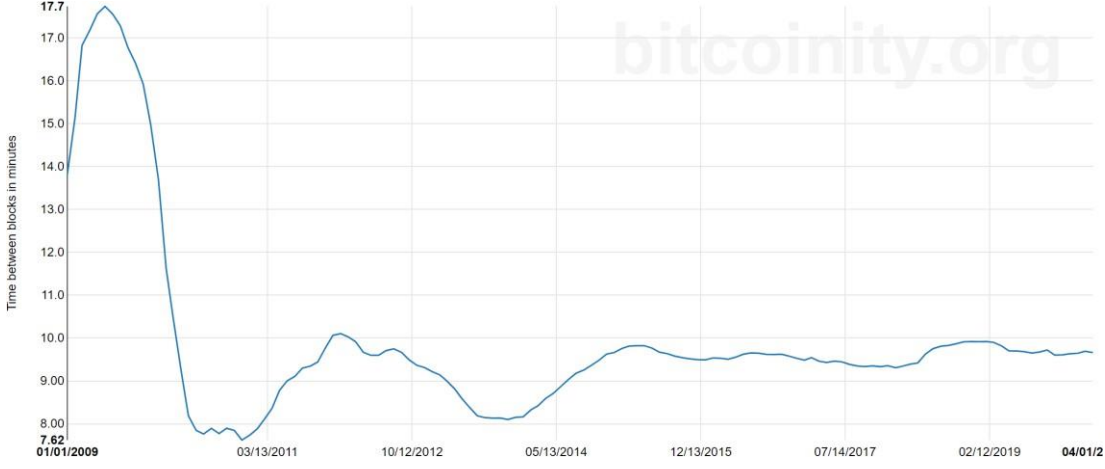
# SOLVING HASH PUZZLES IS PROBABILISTIC

Prob (Alice wins next block) =
fraction of global hash power she controls

For individual miner:

$$\text{mean time to find block} = \frac{10 \text{ minutes}}{\text{fraction of hash power}}$$

# AVERAGE TIME TO MINE A BLOCK



# 3. TRIVIAL TO VERIFY

- Nonce is published as part of block.
- Other miners simply verify that

$$H(\text{nonce} \parallel \text{prev\_hash} \parallel \text{merkle\_root}) < \text{target}$$

- This is an important property because, once again, it allows us to get rid of centralization.
  - We don't need any centralized authority verifying that miners are doing their job correctly.
  - Any node or any miner can instantly verify that a block found by another miner satisfies this proof-of-work property

# MINING ECONOMICS

| If mining reward (block reward + Tx fees) | > | mining cost (hardware + operational cost) | → | Profit |
|---|---|---|---|---|

- Operational Costs: electricity, cooling, …
- Complications:
  - fixed vs. variable costs
  - reward depends on global hash rate
  - cost in USD vs. reward in Bitcoins → Exchange rate varies fast
  - being an honest miner is not provably optimal!

- Actually analyzing whether it makes sense to mine is a complicated game theory problem.

# WHAT CAN A "51% ATTACKER" DO?

- **Key security assumption:** Attacks infeasible if majority of miners weighted by hash power follow the protocol.
- What would happen if consensus failed and there was in fact an attacker who controls 51 percent or more of the mining power?

  - Steal coins from existing address? ✗
  - Suppress some transactions?
    - From the block chain ✓
    - From the P2P network ✗
  - Change the block reward? ✗
  - Destroy confidence in Bitcoin? ✓✓

# BITCOIN GOLD 51% ATTACK

- Bitcoin Gold (BTG) is a hard fork of Bitcoin.


- The stated purpose of the hard fork is to change the proof of work algorithm so that ASICs which are used to mine Bitcoin cannot be used to mine the Bitcoin Gold blockchain in the hopes that enabling mining on commonly available graphics cards will democratize and decentralize the mining and distribution of the cryptocurrency.

- In May 2018, Bitcoin Gold was hit by a 51% hashing attack by an unknown actor. During the attack, 388,000 BTG (worth approximately US$18 million) was double-spent.

- Bitcoin Gold suffered from 51% attacks again in January 2020.

# OTHER 51% ATTACKS