PROOF OF WORK
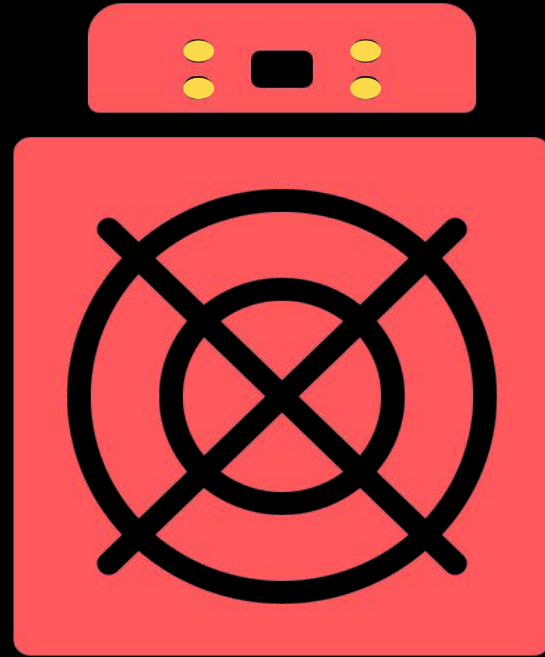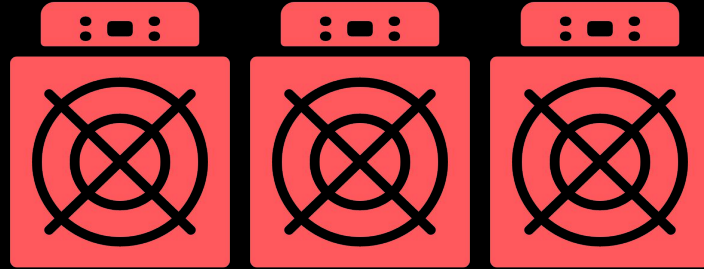
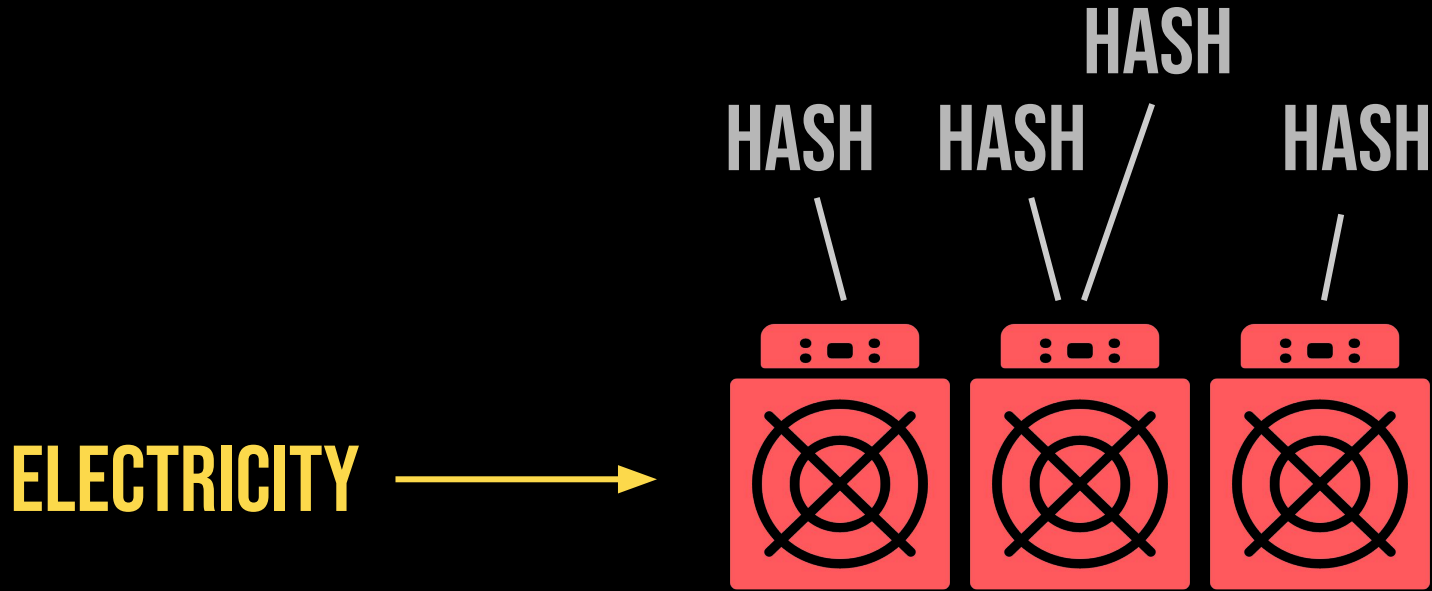# BASICS

ELECTRICITY →

Miners consume electricity from an electrical grid or generated directly from an energy source onsite.

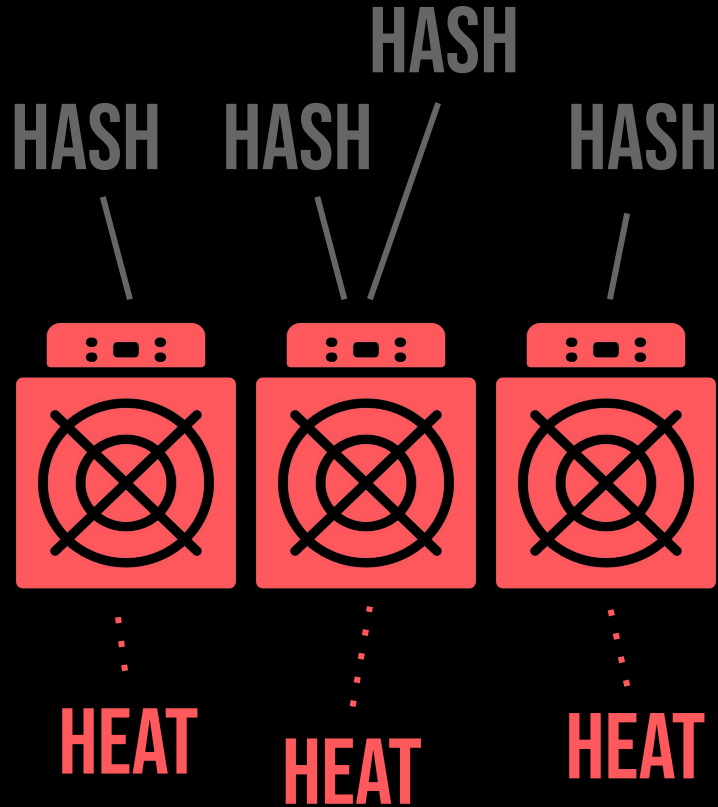HASH HASH HASH HASH HASH

ELECTRICITY

@ANILSAIDSO

While 'miner' is a helpful descriptor, these machines are actually engaged in the process of 'hashing' data with the goal of achieving a certain output.

HASHING *(verb)*

Using an algorithm to convert a piece of data into a unique fixed-length string output.

| STAY HUMBLE, STACK SATS | → | *HASH* | → | 66A91DE5... |

HASH

HASH HASH HASH

ELECTRICITY

HEAT HEAT HEAT

@ANILSAIDSO

Miners produce heat as a byproduct of producing hashes.

THERMODYNAMICS *1st Law*

Energy cannot be created nor destroyed in isolated systems. It can only be transformed.

Miners expend computational power (converting electricity into hashes) and dissipating heat as the byproduct.

HASH

/

26A03CAD6CEF052E
5772286E18D7986D
E1B3D2D9F959C56D
FCE04CA7B469449E

ELECTRICITY →

@ANILSAIDSO

Miners are engaged in the search for a random number
(known as a 'nonce') that produces a hash output meeting
the current difficulty level (# of leading zeros).

NONCE *(noun)*

A random number that is generated to produce an output meeting certain specifications (i.e., leading zeros) when combined with existing data.

| DATA | + | NONCE | HASH | → | NEW OUTPUT |

HASH

/

OOOOOOOOOOOOOOOO
OOO77D7E94EA7787
80E2D6138D4E38EB
091932E6C6CA4004

WINNER!

ELECTRICITY →

@ANILSAIDSO

The winner has the right to claim tx fees & mint themselves new bitcoin. This is done by proposing a new block to the network and including a self-paying 'coinbase' tx.

WHAT DO MINERS COMPETE FOR?

0   *21M*

19.2M | **1.8M**

@ANILSAIDSO

TRANSACTION FEES
from circulating supply

REMAINING BITCOIN
issued w/ new blocks

BLOCK SUBSIDY *(noun)*

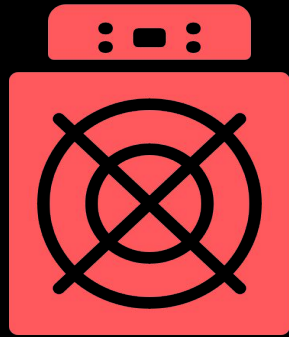*A predetermined amount of bitcoin a successful miner is permitted to mint with each block.*
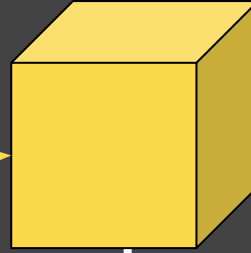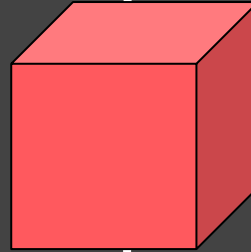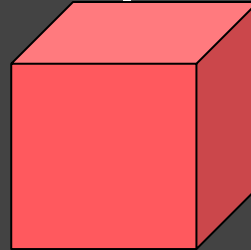
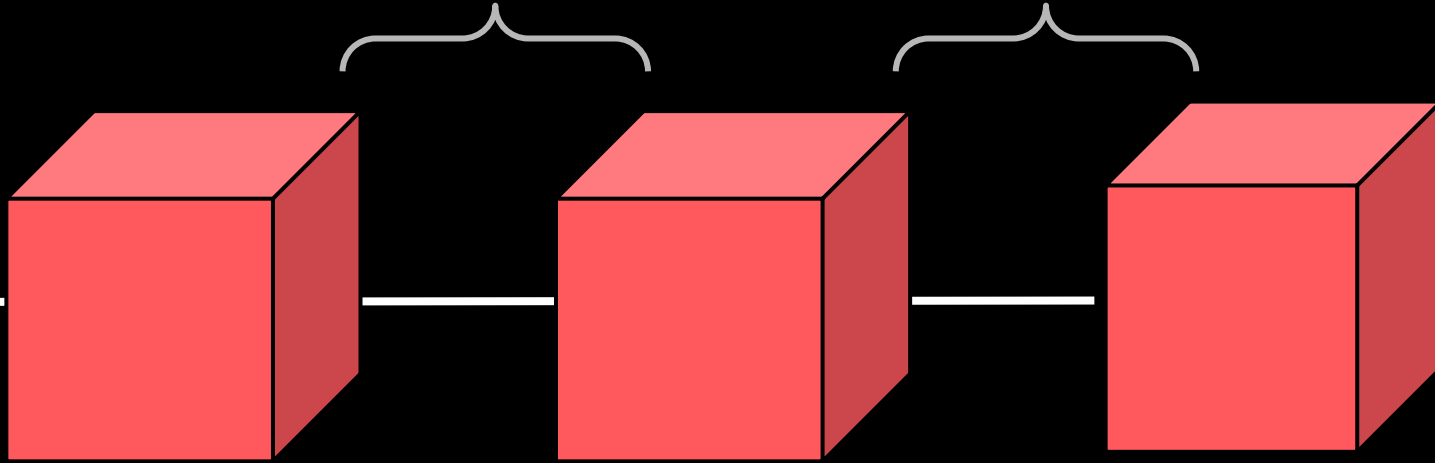| 50BTC | 25BTC | 12.5BTC | 6.25BTC | 3.125BTC | ❯ |

CHAIN TIP

PROPOSED BLOCK

CONFIRMED BLOCK

A proposed block is broadcast to the network and propagates if valid, forming the new tip of the chain.

@ANILSAIDSO

10 MIN INTERVALS
(ON AVG.)

@ANILSAIDSO

Block production is programmed to occur at a regular interval. If block times stray too far from the targeted 10 minute interval, the level of difficulty adjusts upwards or downwards.

DIFFICULTY *(noun)*

A measure of how likely a new block will be found given certain parameters.

00000000000000000077D7E94EA778780E2D6138D4E38EB091932E6C6CA4004

"Bitcoin is robust historical immutability by thermodynamic law.

We only need one proof-of-work immutable ledger."

—ANDREAS ANTONOPOULOS

Now available:

Anil

@anilsaidso