# Basic Bitcoin Tech: Bitcoin Mining

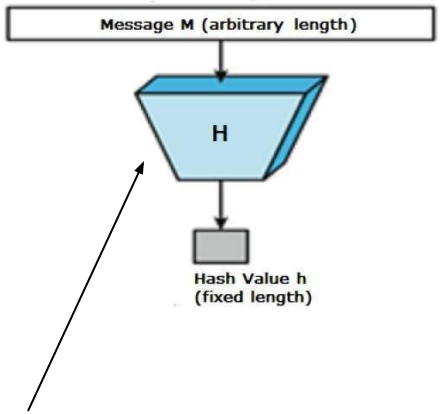
Host - Simplest Bitcoin Book w/ Portland.HODL

# - Overview -

**Topics**

- What is a hash?
- What does it mean to mine bitcoins?
  - Creation of a Block
  - Difficulty Number
  - Block Subsidy
  - Fees
- Mining Hardware
- Energy Usage

# What is a hash?

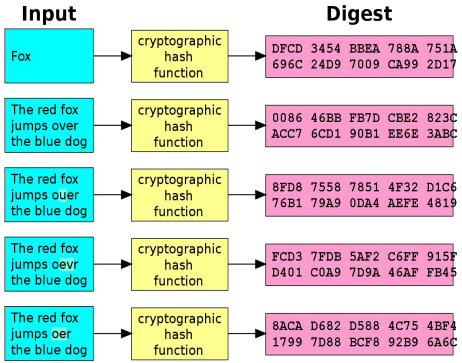



Hashing Function

## Definition

- “A hash function is any function that can be used to map data of arbitrary size to fixed-size values.”
- **Simply put a hash function takes in any amount of data and spits out a fixed length result.**
- Example the word “satoshi” when hashed with SHA-256 returns
“da2876b3eb31edb4436fa4650673fc6f01f90de2f1793c4ec332b2387b09726f”

# Notes about hashing




- Unless noted these slides are referring to SHA-256 hashing.
- Hashing the same data always returns the same hash.
- Changing even a single bit causes the output to change dramatically.
- A hashing operation takes **time and energy** to compute.
- Bitcoin miners hash the block header (80 bytes)
- There isn't a good way to determine with any level of precision what a hash function will return. The output has a number of combos greater than the number of atoms in the universe.

# What does it mean to mine bitcoin?

Bitcoin mining means to hash block data such that the headers hash is lower than the difficulty value. Doing so lets the miner add data to the timechain.

**Reasons for mining are ...**

- **Block Reward** : The number of bitcoins rewarded for finding the correct block header hash. (6.25BTC right now until 2024)
- **Fees :** The miner also collects all of the fees from transactions included in the block they mined.
- **Network Security :** The more hashes consumed to mine a bitcoin block, the more hashes that are needed to successfully attack the network.



# The Lottery example.

Miners change one thing about the block header they are trying to mine. Then they hash the change they made.

After the hash is complete the miner checks if the hash is lower than the difficulty number. If it is they mine the next block (**WIN**). This process happens trillions of times a second per machine.

This is similar to a person pulling lottery tickets from a machine where you can't pick the numbers and you only win if the number you draw is lower than the threshold to win the prize. Slot machines are also similar.

The more hashes per second you have the higher the chance of 'winning' and mining the next block.

Network Hashrate


*Blocks mined on satoshis computer came in at the same rate as the 1,000,000+ mining machines do today.*

# The difficulty number?

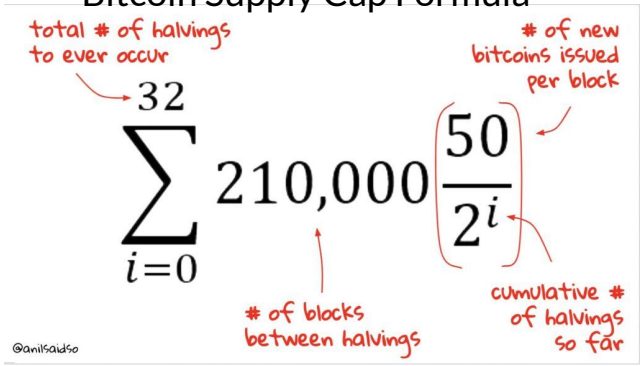
A miner must adjust the nonce, and other data in the blockheader so that when hashed the resultant hash is a lower value than the difficulty value.

**The difficulty number gets adjusted every 2016 blocks.** If blocks were being mined on average faster than ten minutes during the laster 2016 blocks the difficulty number goes down. This means more hashes will be necessary to find a block since the odds become lower of ‘guessing’ the right header hash. The opposite is true if blocks take longer than 10 mins on average.

**This is the feedback mechanism on the Bitcoin network to ensure blocks come in at a constant rate.** Put simply it’s like a car that under all circumstances must maintain a certain speed. If the car starts speeding up, the brakes are hit (downward adjustment %). If the car slows down the gas pedal is pressed to speed it up (upward adjustment %)

# Block Subsidy and the Bitcoin Supply Cap

Bitcoin Supply Cap Formula




- Each block has a block subsidy. These are new bitcoin minted and awarded to the miner who found the block hash.
- Every 210,000 blocks (~4 years) the block subsidy is cut in half. This happens a total of 32 times (Epochs)until 2140.
- During the first epoch  each block minted 50BTC, then at block 210,000 the next block minted 25BTC, and so on.
- All bitcoins in existence go back to a block subsidy
- The block subsidy schedule is the supply cap itself.

# Bitcoin Mining Hardware and History

GPU MINING RIG

My old S9 in 2017

**All mining hardware is still connected to a node!**

- 2009 - 2011: CPU mining using Bitcoin Core.
- 2011 - 2013: GPUs (Graphics Cards Mining Bitcoin)
- 2012 - 2014: FPGA Mining (never widespread)
- 2012 - Today: ASIC Mining

# Mining Energy Usage

**ENERGY IS THE GLUE THAT SECURES THE TIMECHAIN.**

- To hash takes energy, and finding the correct hash takes time. Since there are no shortcuts to speed up the process energy is used over time.
- Each block that is mined is appended  or ‘glued’ to the last block mined.
- The strength of this ‘glue’ is equal to the energy used to mine the block. If blocks were not mined with a lot of energy it would make it easy for an attacker to pull blocks off the timechain and replace them with their own.
- Energy is what protects bitcoins ledger of history and ensures it’s immutability.

# Thanks For Listening.

1. Questions or Comments? Please ask to come on stage.
2. Anything incorrect please comment on the slide in question.