THE BITCOIN HALVING

part 1: a technical explainer

by amiti

what is a halving?

new bitcoin are created when a new block is mined

this is the only way new bitcoin come into existence

this is called the block subsidy

the number of new bitcoins per block was written into the code since the 1st release of bitcoin

the subsidy started at 50₿ per block

every 210,000 blocks the subsidy cuts in 1 / 2

the halving is the block where that happens

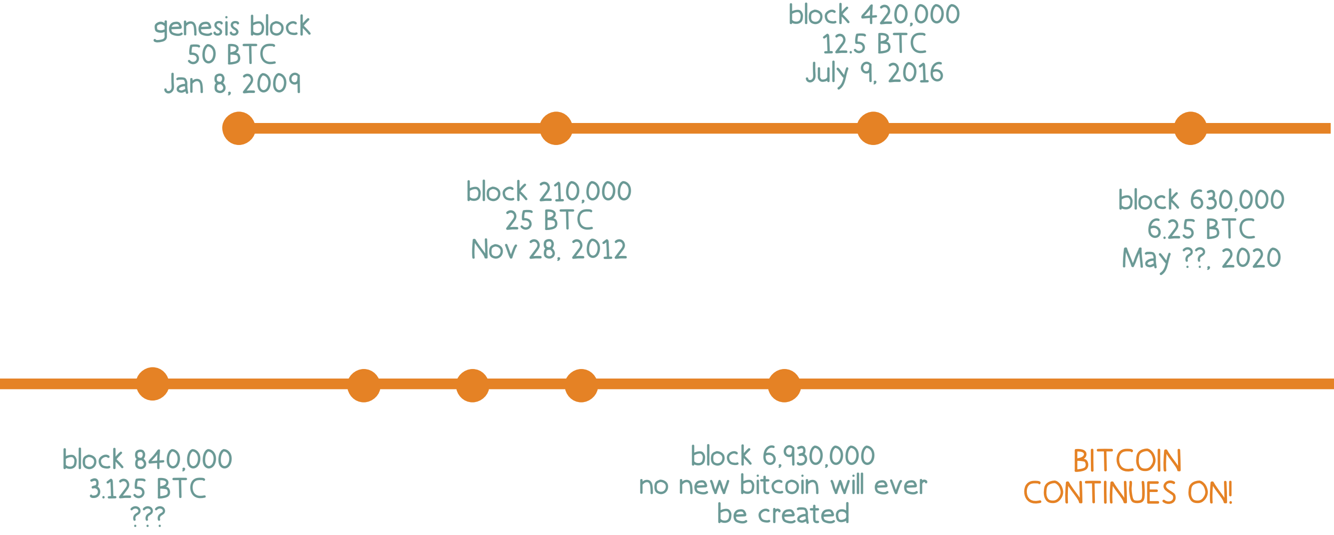
when halving?

the Bitcoin halving is scheduled by block height, not calendar date

at block 630,000 the subsidy will change from

12.5 ฿ → 6.25 ฿

this block is anticipated to be mined on May 11



genesis block
50 BTC
Jan 8, 2009

block 210,000
25 BTC
Nov 28, 2012

block 420,000
12.5 BTC
July 9, 2016

block 630,000
6.25 BTC
May ??, 2020

block 840,000
3.125 BTC
???

block 6,930,000
no new bitcoin will ever be created

BITCOIN CONTINUES ON!

Bitcoin v0.1

the emission schedule & max supply cap have been a fundamental part of Bitcoin from the start.

21 million BTC

Satoshi released Bitcoin by announcing it to the cryptography mailing list.

check out this excerpt:

> Total circulation will be 21,000,000 coins. It'll be distributed to network nodes when they make blocks, with the amount cut in half every 4 years.
>
> first 4 years: 10,500,000 coins
> next 4 years: 5,250,000 coins
> next 4 years: 2,625,000 coins
> next 4 years: 1,312,500 coins
> etc...
>
> When that runs out, the system can support transaction fees if needed. It's based on open market competition, and there will probably always be nodes willing to process transactions for free.
>
> Satoshi Nakamoto

LOL!

but wait...

a digital monetary system with a finite supply is a brilliant idea

unfortunately, the implementation had a bug

```
int64_t nSubsidy = 50 * COIN;
   // Subsidy is cut in half every 210,000 blocks
   // which will occur approximately every 4 years.
   nSubsidy >>= (nHeight / 210000);
```

the block subsidy would eventually wrap back around to 50 and cause an infinite supply

In 2014, BIP 42 fixed the bug

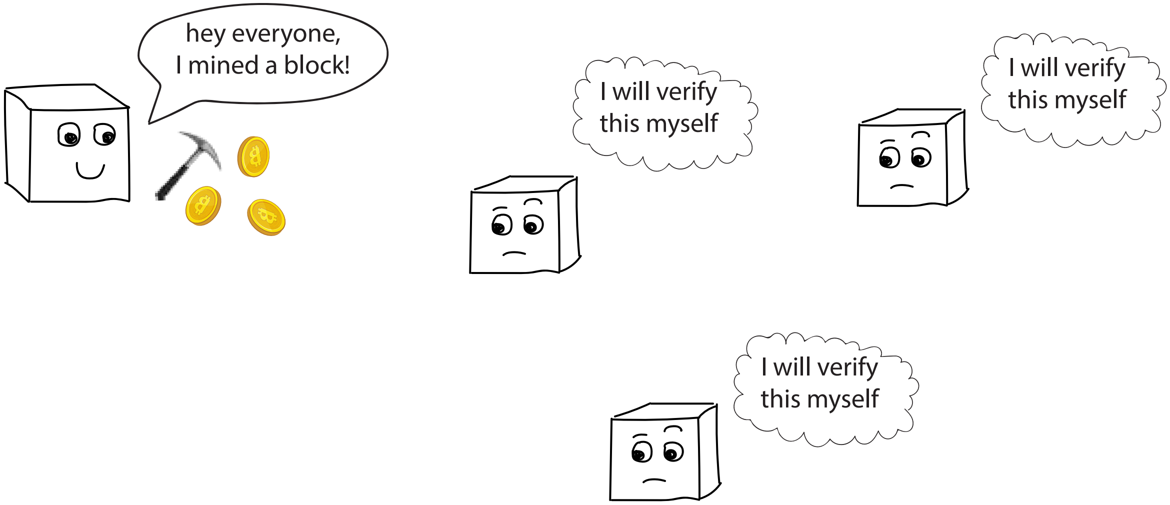
what enforces the limit?

YOU DO !

a coinbase transaction is special. it is the only type of transaction that is allowed to create new bitcoin.

every time a full node receives a new block, it validates

1. there is only one coinbase txn
2. the amount of coinbase is <= max subsidy


hey everyone,
I mined a block!
I will verify this myself
I will verify this myself
I will verify this myself

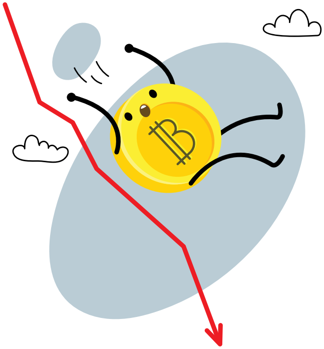
are you suuuure?

in july 2019, there was a block mined that tried to create more bitcoin than the allocated subsidy

it was rejected from the network

at height 584,802 :

```
ERROR: ConnectBlock(): coinbase pays too much
    (actual=1326546691 vs limit=1250000000)
```



thank you for reading!

if you're interested in getting an email when I release new comics, please sign up at:

https://tinyletter.com/amiti

bitcoin artwork by aniwhite

http://www.shutterstock.com/g/aniwhite?rid=908080

learn more!
satoshi announces bitcoin: https://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html
bip 42: https://github.com/bitcoin/bips/blob/master/bip-0042.mediawiki
BitMEX Research reports invalid block: https://twitter.com/BitMEXResearch/status/1148989508588883970

COMING SOON

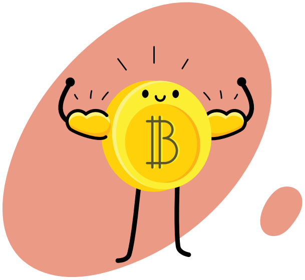
THE BITCOIN HALVING

part 2: see for yourself!

you can observe block subsidies by using bitcoin-cli to query your node

part 2 will walk through some exercises

if you don't have access to a full-node, you can use a block explorer to access this information



by amiti