Danny Diekroeger @dannydiekroeger

13 Jul 20 • 27 tweets • dannydiekroeger/status/1282544554650951680

~ Bitcoin's Difficulty Adjustment ~

How does the bitcoin network ensure that blocks continue to get mined once every 10 minutes on average?

In this thread I'll explain the Difficulty Adjustment, and why it might be the most genius part of bitcoin 👇

If you remember my thread on bitcoin mining, we discussed how the miners are trying to construct a block that hashes to something that starts with a bunch of 0's

Danny Diekroeger
@dannydiekroeger

Replying to @dannydiekroeger

Bitcoin Mining

Danny Diekroeger @dannydiekroeger

An Introduction to #Bitcoin Mining and the Blockchain

How does it all work? A thread for beginners

I'm going to take you through a little game, and together we're going to mine a simplified version of a bitcoin block. 👇

5:14 PM · Jul 11, 2020

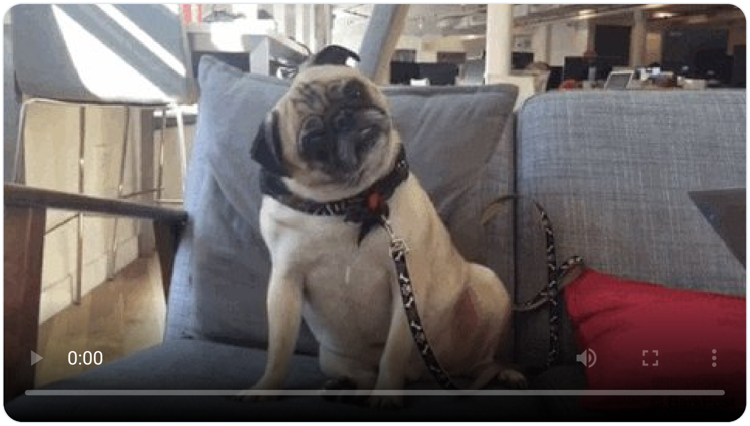
♡ 13 See Danny Diekroeger's other Tweets

So I have a question for you... which is harder...

1) Finding some data that hashes to something beginning with one zero ("0")

or

2) Finding some data that hashes to something beginning with 10 zeros ("0000000000")



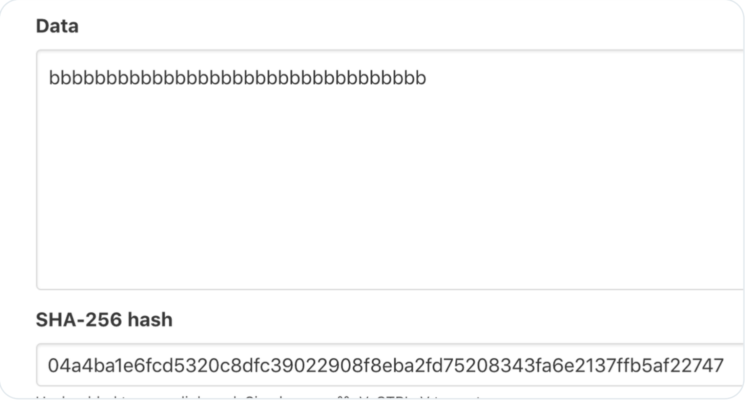
If you said number two, you're right!

Go ahead and try it yourself with this online hash calculator if you like.

https://xorbin.com/tools/sha256-hash-calculator

Look, in just about 30 seconds of clicking, I found a hash that starts with a 0.

Super easy, I just kept typing a bunch of b's and trying each one



Data

bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb

SHA-256 hash

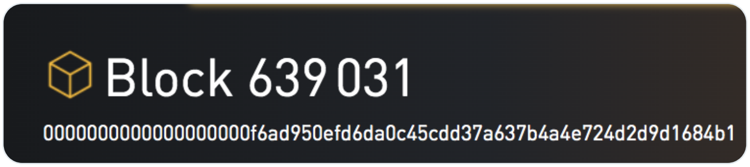
04a4ba1e6fcd5320c8dfc39022908f8eba2fd75208343fa6e2137ffb5af22747

But finding a hash that starts with 10 zeros is a whole new ballgame. It would take me forever trying to just click around on that website

I'd definitely need some custom hardware, and probably a whole factory of them

In fact, this is exactly what's going on in the bitcoin network right now.

Look at the hash of the most recent bitcoin block... it starts with 19 zeros!!



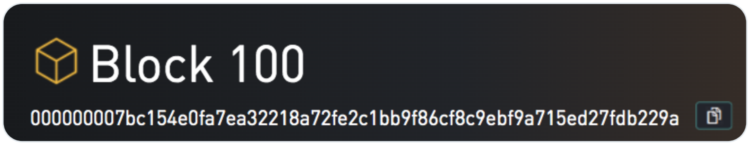
Block 639 031

0000000000000000000f6ad950efd6da0c45cdd37a637b4a4e724d2d9d1684b1

But mining a bitcoin block wasn't always this hard. Check out block 100, back in the good old days in 2009.

This block hash only starts with 8 zeros.

It was so much easier to mine blocks back then - people could mine them with just their simple desktop computers.



Block 100

000000007bc154e0fa7ea32218a72fe2c1bb9f86cf8c9ebf9a715ed27fdb229a

So what changed? And how did it change?

This is.... the Difficulty Adjustment!

The number of leading zeros required for a block's hash to be valid is designed to change over time.

In other words, the mining difficulty adjusts.

Imagine if the bitcoin network did not adjust the difficulty.

Imagine if the network had required just 8 leading zeros for all block hashes, forever...

What would happen?

Well, as the prices went up, more and more miners joined the network, there would be more total computer power trying to mine blocks...

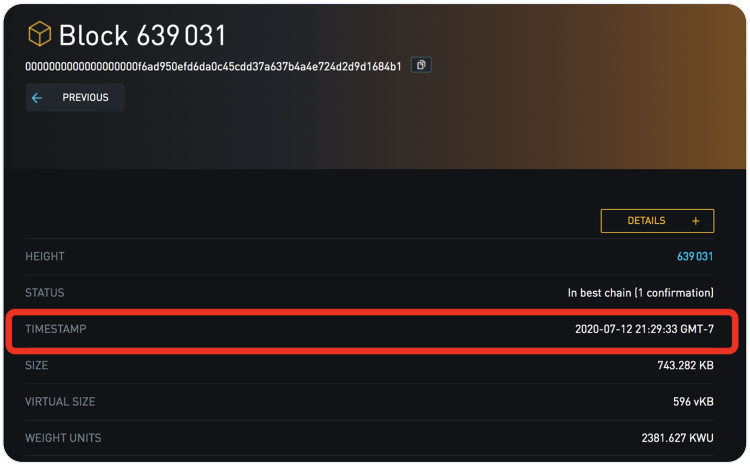
As a result, blocks would start getting mined very quickly. We might start getting a block once every minute, or even every second.

Alternatively, what if a bunch of miners went out of business or stopped trying? There might not be enough total computing power to find blocks quickly, and blocks might start taking really really long to find, grinding the network to a halt...

Luckily, Satoshi had a brilliant idea. Let the mining difficulty adjust based on network conditions, so that the average block time stays at 10 minutes.

Here's how it works:

Every block has a timestamp in its header, which states approximately at what time the block was mined.

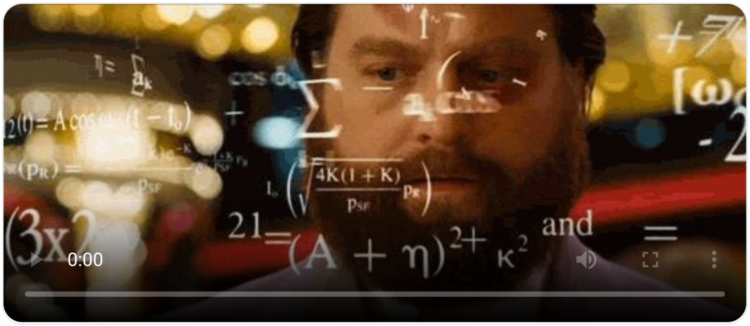


Block 639 031

0000000000000000000f6ad950efd6da0c45cdd37a637b4a4e724d2d9d1684b1

HEIGHT	639 031
STATUS	In best chain (1 confirmation)
TIMESTAMP	2020-07-12 21:29:33 GMT-7
SIZE	743.282 KB
VIRTUAL SIZE	596 vKB
WEIGHT UNITS	2381.627 KWU

And once every 2016 blocks (~2 weeks), each node in the network performs a calculation...



They look at the timestamp of the current block, and compare it to the timestamp of the block from 2015 blocks ago.

They then calculate the total time it took to mine all those blocks in that 2016 block window.

Call this time T

If every block took an average of 10 minutes to find, then this calculated time T should be exactly 2 weeks.

Why 2 weeks?

(10 minutes / block) * (2016 blocks) = 20160 minutes

20160 minutes = 336 Hours = 14 days = 2 weeks!

So here is the calculation that every node in the network performs:

If T is greater than 2 weeks, it means blocks were mined slower than expected, and the difficulty should decrease.

Instead of requiring 19 leading zeros for block hashes, they might bump it down to 18

If T is less than 2 weeks, it means blocks were mined faster than expected, and the difficulty should increase.

Instead of requiring 19 leading zeros, they might bump it up to 20.

Sometimes the time is close enough to 2 weeks, that no difficulty change is made at all.

But how do we ensure that all nodes arrive to the same conclusion on this calculation?

Well, they all are looking at the same blockchain, and they are all running the same software, so they are guaranteed to arrive at the same conclusion.

Pretty genius if you ask me..

So there you have it... that's how the difficulty adjustment works.

But why does it matter so much?

What's so important about making sure we have 10-minute block intervals?

In my opinion, the biggest implication of this is that it ensures the supply issuance of bitcoin stays at an expected rate.

Remember, each new block creates new bitcoins..

Faster or slower block times affect the rate of new bitcoins entering the market.

In every other asset class, when the price goes UP, more of it gets produced, and the supply begins to increase more quickly, which ultimately drives the price back DOWN.

@saifedean has explained this wonderfully in his book The Bitcoin Standard

https://www.amazon.com/Bitcoin-Standard-Decentralized-Alternative-Central/dp/1119473861

But #bitcoin fixes this.

We now have a monetary asset who's supply issuance is on a FIXED schedule, for all of eternity, no matter how hard people try to create more.

We've never seen a monetary commodity like this in history, and this is why Bitcoin is a massive breakthrough in monetary technology

Get you some and a spacesuit. We're going to the moon.

0:00

• • •