Danny Diekroeger @dannydiekroeger

10 Jul 20 • 26 tweets • dannydiekroeger/status/1281614121947914240

An Introduction to #Bitcoin Mining and the Blockchain

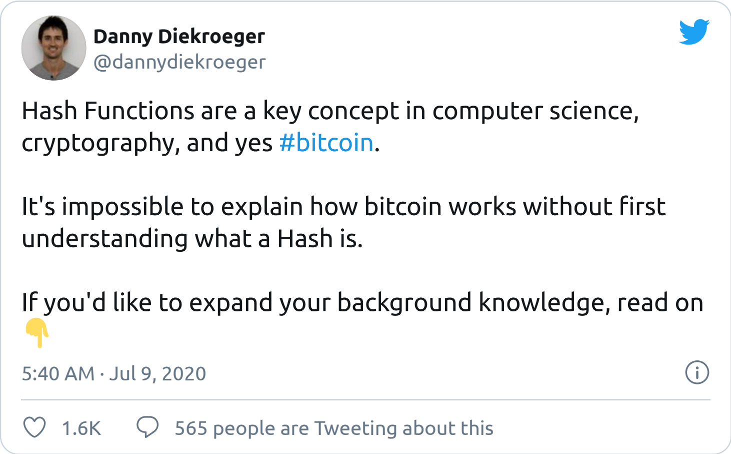
How does it all work? A thread for beginners

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

Before we start, it’s important you have some understanding of what a Hash is.

A Hash is like a data fingerprint that’s calculated using some fancy math

(If this is new, I suggest reading my previous beginner-friendly thread first)



Danny Diekroeger
@dannydiekroeger

Hash Functions are a key concept in computer science, cryptography, and yes #bitcoin.

It's impossible to explain how bitcoin works without first understanding what a Hash is.

If you'd like to expand your background knowledge, read on 👇

5:40 AM · Jul 9, 2020

1.6K 565 people are Tweeting about this

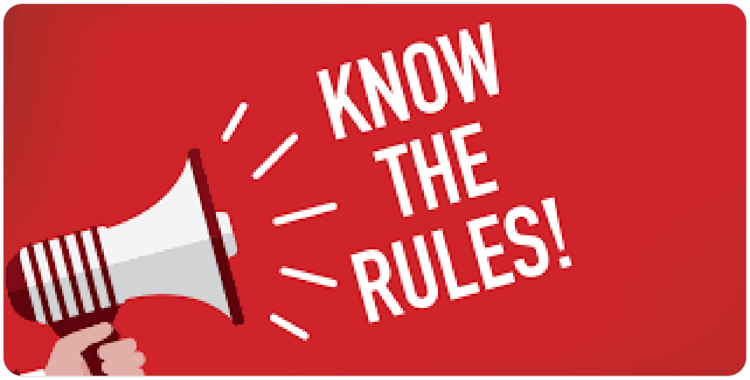
You can play around with Hashes using this helpful website (and I'll be using it for our demonstrations here):

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

Let's play!

Imagine you and I are miners in a simplified bitcoin network.

We can make some money if we mine new blocks, but we have to play according to rules, otherwise the other users in the network will reject our blocks.



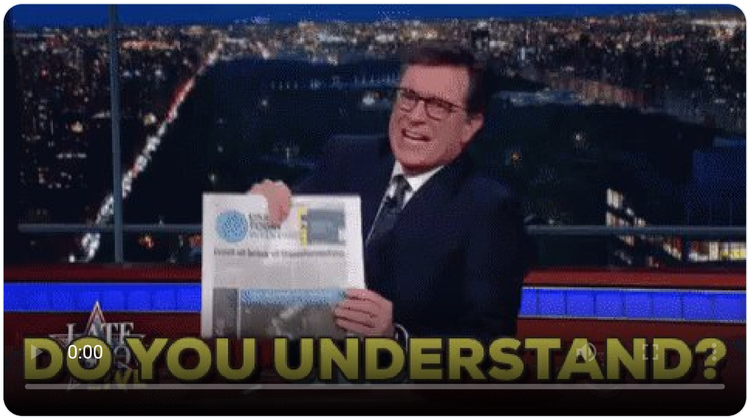
Rules:

- Max of 2 transactions per block

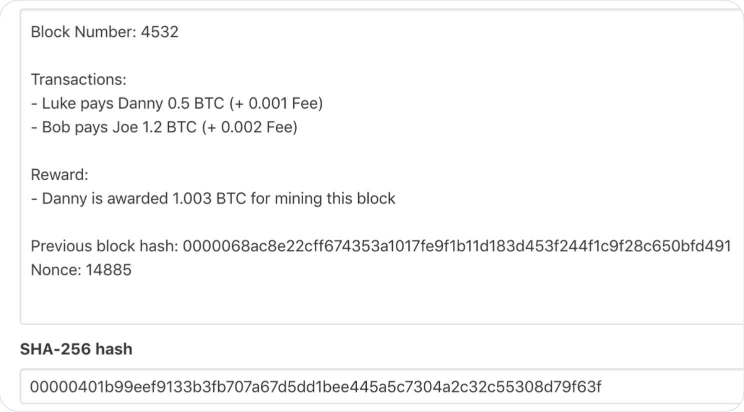
- Whoever mines the block can claim a reward of 1 bitcoin plus the fees of the transactions in that block

- The SHA-256 Hash of the block's contents must start with "00000"

- Each block must include the Hash of the previous block.



That's a lot to remember, so it might be easier if we just take a look at the most recent block, which I mined myself.



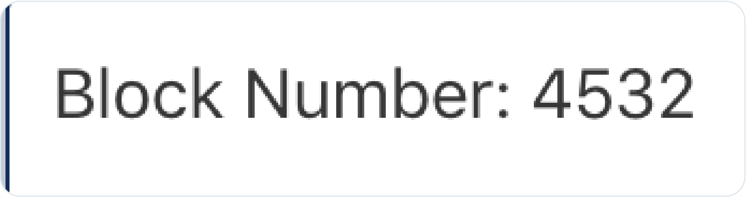
```
Block Number: 4532

Transactions:
- Luke pays Danny 0.5 BTC (+ 0.001 Fee)
- Bob pays Joe 1.2 BTC (+ 0.002 Fee)

Reward:
- Danny is awarded 1.003 BTC for mining this block

Previous block hash: 0000068ac8e22cff674353a1017fe9f1b11d183d453f244f1c9f28c650bfd491
Nonce: 14885
```

SHA-256 hash

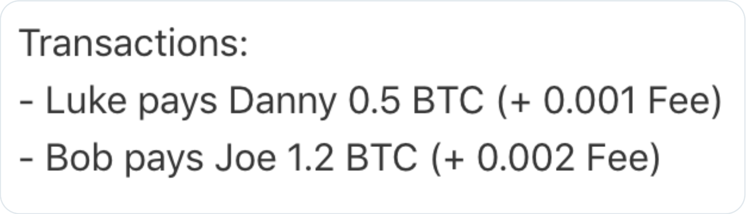
```
00000401b99eef9133b3fb707a67d5dd1bee445a5c7304a2c32c55308d79f63f
```

A few things to note:

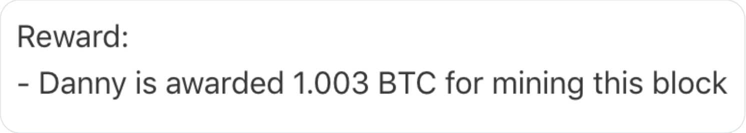
- The Block Number 4532 means its the 4532nd block in the entire history of the network


Block Number: 4532

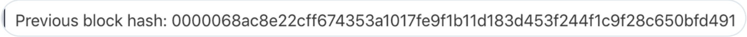
- There are two transactions in the block, each paying a small fee


Transactions:
- Luke pays Danny 0.5 BTC (+ 0.001 Fee)
- Bob pays Joe 1.2 BTC (+ 0.002 Fee)

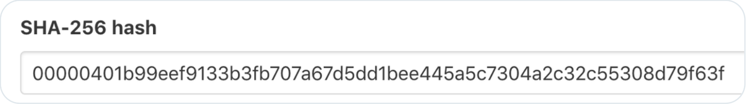
- I mined the block, so I got the reward - 1 newly created BTC, plus the 0.003 in fees.


Reward:
- Danny is awarded 1.003 BTC for mining this block

- It links the previous block's hash (which starts with five 0's)


Previous block hash: 0000068ac8e22cff674353a1017fe9f1b11d183d453f244f1c9f28c650bfd491

- And finally at the bottom, you can see the hash of this block also starts with five 0's - so it's valid!

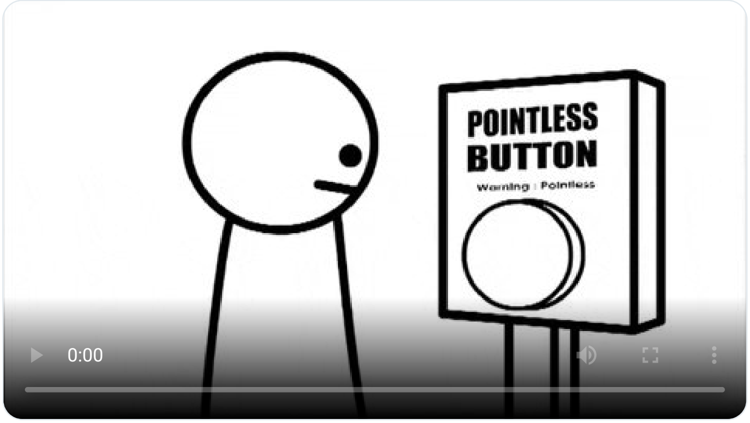

SHA-256 hash

00000401b99eef9133b3fb707a67d5dd1bee445a5c7304a2c32c55308d79f63f

But there's one more field, the "Nonce" - what's this?

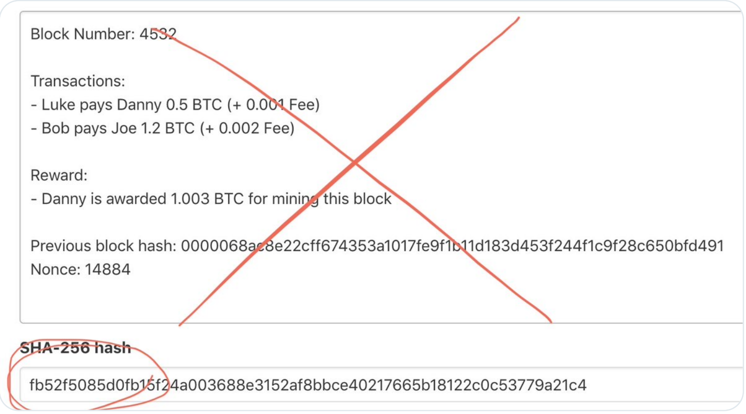
The Nonce is actually a meaningless field (you can put any number there).

It's sole purpose is to give you some data to tinker with until your block hashes to something valid.



Take a look what happens if we keep everything the same, but change the Nonce by 1 (we change it from 14885 to 14884)

The SHA-256 hash at the bottom is completely different. It no longer starts with five 0's, so the block is not valid!



Block Number: 4532

Transactions:
- Luke pays Danny 0.5 BTC (+ 0.001 Fee)
- Bob pays Joe 1.2 BTC (+ 0.002 Fee)

Reward:
- Danny is awarded 1.003 BTC for mining this block

Previous block hash: 0000068ac8e22cff674353a1017fe9f1b11d183d453f244f1c9f28c650bfd491
Nonce: 14884

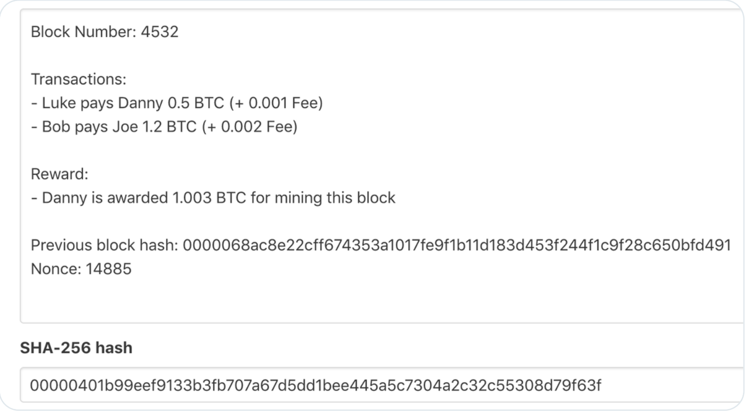
SHA-256 hash

fb52f5085d0fb15f24a003688e3152af8bbce40217665b18122c0c53779a21c4

The above, invalid block was one of the many guess-and-check attempts that my software made before finding a valid block.

The Nonce I finally found was 14885, and it works to make the block hash to start with 00000.

Hence the final valid block is:



Block Number: 4532

Transactions:
- Luke pays Danny 0.5 BTC (+ 0.001 Fee)
- Bob pays Joe 1.2 BTC (+ 0.002 Fee)

Reward:
- Danny is awarded 1.003 BTC for mining this block

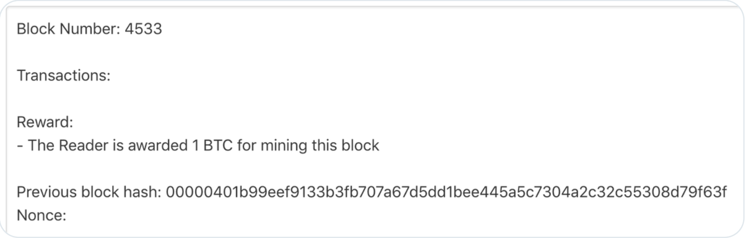
Previous block hash: 0000068ac8e22cff674353a1017fe9f1b11d183d453f244f1c9f28c650bfd491
Nonce: 14885

SHA-256 hash

00000401b99eef9133b3fb707a67d5dd1bee445a5c7304a2c32c55308d79f63f

Alright now I'm going to help YOU mine the next block.

Let's start by putting together the basics.



Block Number: 4533

Transactions:

Reward:
- The Reader is awarded 1 BTC for mining this block

Previous block hash: 00000401b99eef9133b3fb707a67d5dd1bee445a5c7304a2c32c55308d79f63f
Nonce:

Notice:

- We added 1 to the Block Number, so we're at 4533 now

- You, the Reader, claim a reward of 1 BTC

- We include the previous block's hash

But this block isn't complete yet.

While it *is* legal to have 0 transactions in the block, you might as well include as many as you can so that you can claim some additional fees.

So let's find some transactions to add.

Pending transactions get broadcast to you from other participants in the network.

Let's pretend that there are 3 valid pending transactions to choose from:

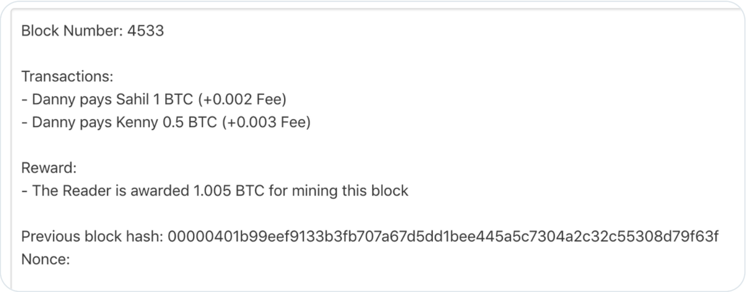
- Danny pays Sahil 1 BTC (+0.002 Fee)
- Sahil pays Sam 2 BTC (+0.001 Fee)
- Danny pays Kenny 0.5 BTC (+0.003 Fee)

Remember, the max transactions you can include in a block is 2... so which 2 will you choose?

Easy, pick the ones with the highest fees, so you can make the most money!

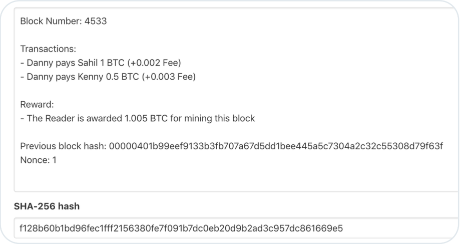
Let's add them to your block:

Notice how your reward is now 1.005 instead of just 1.



```
Block Number: 4533

Transactions:
- Danny pays Sahil 1 BTC (+0.002 Fee)
- Danny pays Kenny 0.5 BTC (+0.003 Fee)

Reward:
- The Reader is awarded 1.005 BTC for mining this block

Previous block hash: 00000401b99eef9133b3fb707a67d5dd1bee445a5c7304a2c32c55308d79f63f
Nonce:
```

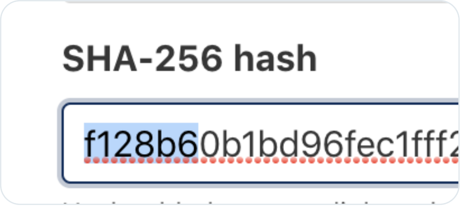
Ok now that you have your block ready to go, there's one final problem.... the hash does not start with 00000!



```
Block Number: 4533

Transactions:
- Danny pays Sahil 1 BTC (+0.002 Fee)
- Danny pays Kenny 0.5 BTC (+0.003 Fee)

Reward:
- The Reader is awarded 1.005 BTC for mining this block

Previous block hash: 00000401b99eef9133b3fb707a67d5dd1bee445a5c7304a2c32c55308d79f63f
Nonce: 1
```

SHA-256 hash

```
f128b60b1bd96fec1fff2156380fe7f091b7dc0eb20d9b2ad3c957dc861669e5
```



SHA-256 hash

```
f128b60b1bd96fec1fff2
```

What to do?

Well, remember the hash game from my previous thread?

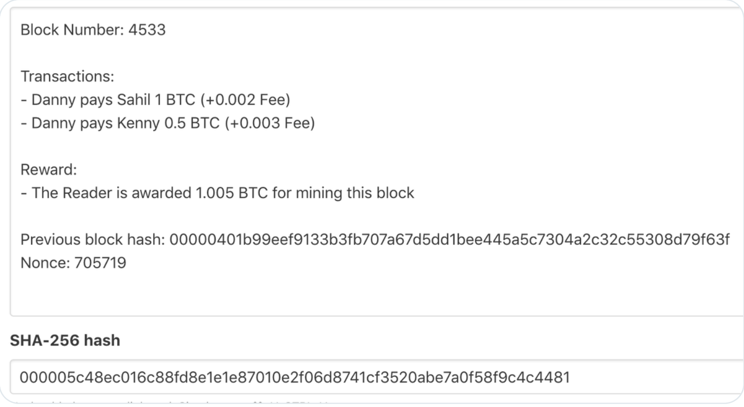
You need to start changing that Nonce and checking hashes until you find a valid one!

(Or better yet, let your friend's software do it for you!)

Luckily I have a script that does this.

After running my script for about a second, and trying 705719 different Nonces, look what I found for you.

It's a valid block!



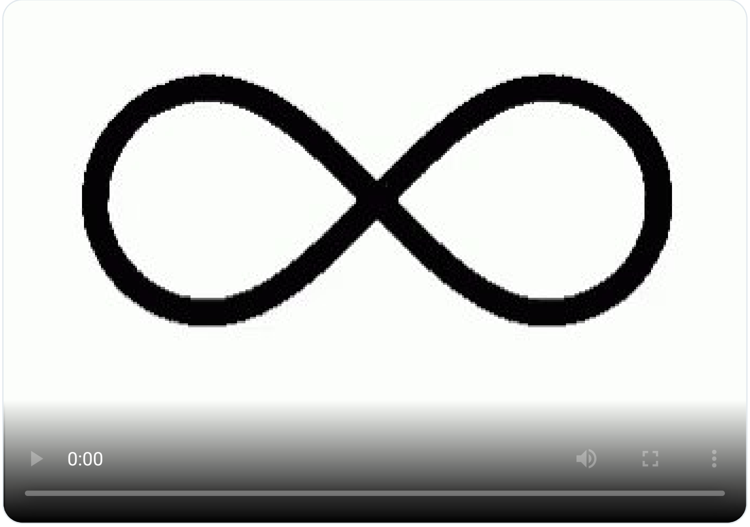
```
Block Number: 4533

Transactions:
- Danny pays Sahil 1 BTC (+0.002 Fee)
- Danny pays Kenny 0.5 BTC (+0.003 Fee)

Reward:
- The Reader is awarded 1.005 BTC for mining this block

Previous block hash: 00000401b99eef9133b3fb707a67d5dd1bee445a5c7304a2c32c55308d79f63f
Nonce: 705719
```

SHA-256 hash

```
000005c48ec016c88fd8e1e1e87010e2f06d8741cf3520abe7a0f58f9c4c4481
```

Go ahead and submit this to our fake bitcoin network, and everyone will agree that it is indeed valid, and your block will be added to the blockchain.

This block will be part of the blockchain forever!



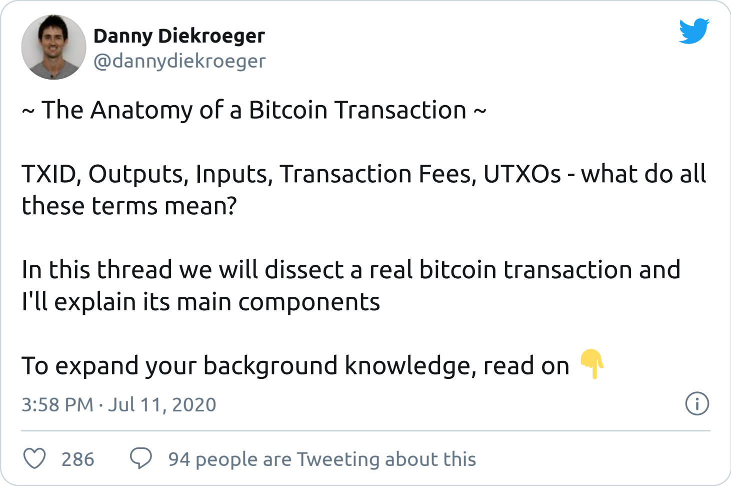
Oh and you got a reward of 1.005 Bitcoin, congrats!

Anyway, that's a simplified version of bitcoin mining. Hope it was helpful!

Comment or Follow + DM if you have any questions!

Also let me know what else you'd like to learn about in the next educational thread

New Thread just posted now - The Anatomy of a Bitcoin Transaction. Check it out!



Danny Diekroeger
@dannydiekroeger

~ The Anatomy of a Bitcoin Transaction ~

TXID, Outputs, Inputs, Transaction Fees, UTXOs - what do all these terms mean?

In this thread we will dissect a real bitcoin transaction and I'll explain its main components

To expand your background knowledge, read on 👇

3:58 PM · Jul 11, 2020

♡ 286 94 people are Tweeting about this