

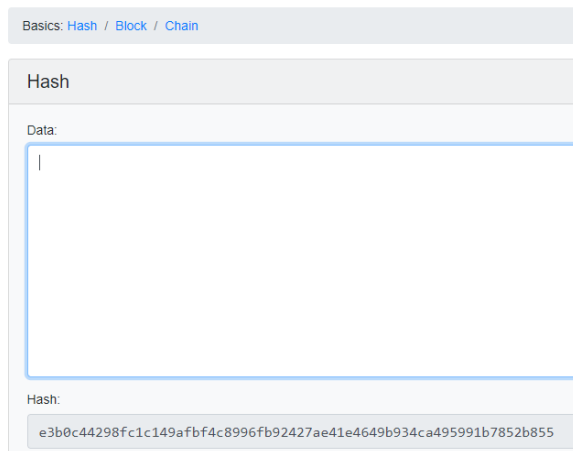
## Module 2 - Assignment Questions

*\* Adjust the response space according to what you need.*

*\* For answers that include data, please, include a screenshot with the appropriate size for its exact display.*

1. How many characters are there in the “hash” field if the data field is empty? In addition to giving the answer, please include a screenshot.

There are 256 bits (64 hexadecimal char)



Basics: [Hash](#) / [Block](#) / [Chain](#)

Hash

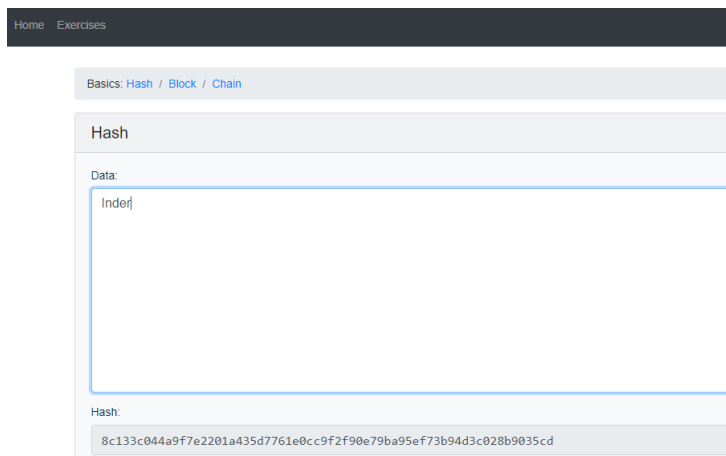
Data:

Hash:

e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855

2. Enter something into the “data” field. Has the *length* of the “hash” field changed? In addition to giving the answer, please include a screenshot.

No. Size is fixed independent of the data contents



Home Exercises

Basics: [Hash](#) / [Block](#) / [Chain](#)

Hash

Data:

Index

Hash:

8c133c044a9f7e2201a435d7761e0cc9f2f90e79ba95ef73b94d3c028b9035cd

3. Enter a name (e.g., “Abel Sanchez”) into the “data” field. What is the value of the *hash*? In addition to giving the answer, please include a screenshot.

Here is the hash:

52b6e946d570e9ea28840f0a209f132c4946d44906239bbbce73db09c63ba078

Basics: [Hash](#) / [Block](#) / [Chain](#)

### Hash

Data:

Abel Sanchez

Hash:

52b6e946d570e9ea28840f0a209f132c4946d44906239bbbce73db09c63ba078

4. Now add an arbitrary character 0 at the end of the name (e.g., “Abel Sanchez0”). What is the value of the *hash* now? In addition to giving the answer, please include a screenshot.

Here it is: cf370446365152f194dab710b6ad8e7636b5c49978b63950b9122005b66e1e74

Basics: [Hash](#) / [Block](#) / [Chain](#)

### Hash

Data:

Abel Sanchez0

Hash:

cf370446365152f194dab710b6ad8e7636b5c49978b63950b9122005b66e1e74

5. Now try it with your name and check the hash that you get. Now delete your name from the “data” field. Re- enter it. Is the value of the *hash* the same as previously?

With my name : Inderpreet Grang, the hash is :

b64a32ac877f45d1d2d9f1bc603077cc5768255eeeb6c89fd85e485758080d41

Yes it is same after I re-enter it

6. From the following list of *hashes*, mark which ones are lower than the target difficulty:

- a. 2413fb3709b05939f04cf2e92f7d0897fc2596f9ad0b8a9ea855c7bfebaae892
- b. 6bbb0da1891646e58eb3e6a63af3a6fc3c8eb5a0d44824cba581d2e14a0450cf
- c. 3b405a612a147405d4f1ea3e7a55135900ce30d63d3bc0c5cd7d28d3b7bd80a2
- d. 038e57600deb326f3101c6e394502c51e552e5243ea81384ec36e89ffddae68d
- e. 746eb24fc73762d085b6b3e0172c1a04d1120b7cc1984f3e04b8dbb574788da4
- f. 0bb1e98f35f647ebee6286ea4bcc243ddefc2773ee2a371a5a1b2a9793b08894
- g. e96af55ff47640d56d25f91ef0868d7490f66da26b495c791db71b80955c0d9e

Please see hashes highlighted

7. If you increase the *nonce* between 0 and 63, how many *hashes* will fall, on average, below the target difficulty?

There are 16 values and 1 in 16 can be below target difficulty. So out of 64 values, on average we can have  $64/16=4$  nonce values that fall below target difficulty

8. Indicate the *nonce* values that will fall below the target difficulty. In addition to giving the answer, please include a screenshot.

For Inderpreet Grang as data, nonce of 6,26, 28, 38, 39, 46, 55 was lower

### Blockchain Basics: Standalone Block

Block:

1

Nonce:

6

Data:

Inderpreet Grang

Hash:

0ad6d407a6e757fd758668f8b1036745c0a743c29a4f0efe7897ddf2f96783c0

Nonce 26:

Block:

1

Nonce:

26

Data:

Inderpreet Grang

Hash:

048dcf57d88a04c9979670356ecd33a028aa6c44f9df30109ff5f6dd284d1c4f

Block:

1

Nonce:

28

Data:

Inderpreet Grang

Hash:

00ce2fbe76edc0baeed000159d374ef89d2cfe18c7a41e2b3f3504ed9e3adf67

Block:

1

Nonce:

38

Data:

Inderpreet Grang

Hash:

0b67fd434e76bca4f9f8db9f5fe9d06f02c36a2775d7679be85b405f501f6bc5

Blockchain Basics: Standardized Block

Block:

1

Nonce:

39

Data:

Inderpreet Grang

Hash:

02211109e50dd5aafb6ba9f7e6bdd467d4ea3e5da0037032d94fe823dbcb15a4

Block:

1

Nonce:

46

Data:

Inderpreet Grang

Hash:

0096d5ee850b094a288f016e85b12d7354efa0461cf0760e50efe1994040e056

Block:

1

Nonce:

55

Data:

Inderpreet Grang

Hash:

07bd0f3dd2640ff5ea90a3490d7e94ef2237fb2f255aee51aa52ab65b8d170af

9. If a worker is allowed to test *nonce* values for an entire day, how many times will they find, on average, a new suitable *nonce*?

Assuming 64 per minute, on average we will have  $60 \times 24 \times 4$  suitable nonce values. = 5760. For above data (“Inderpreet Grang”), we may see that 5760 suitable nonces per day

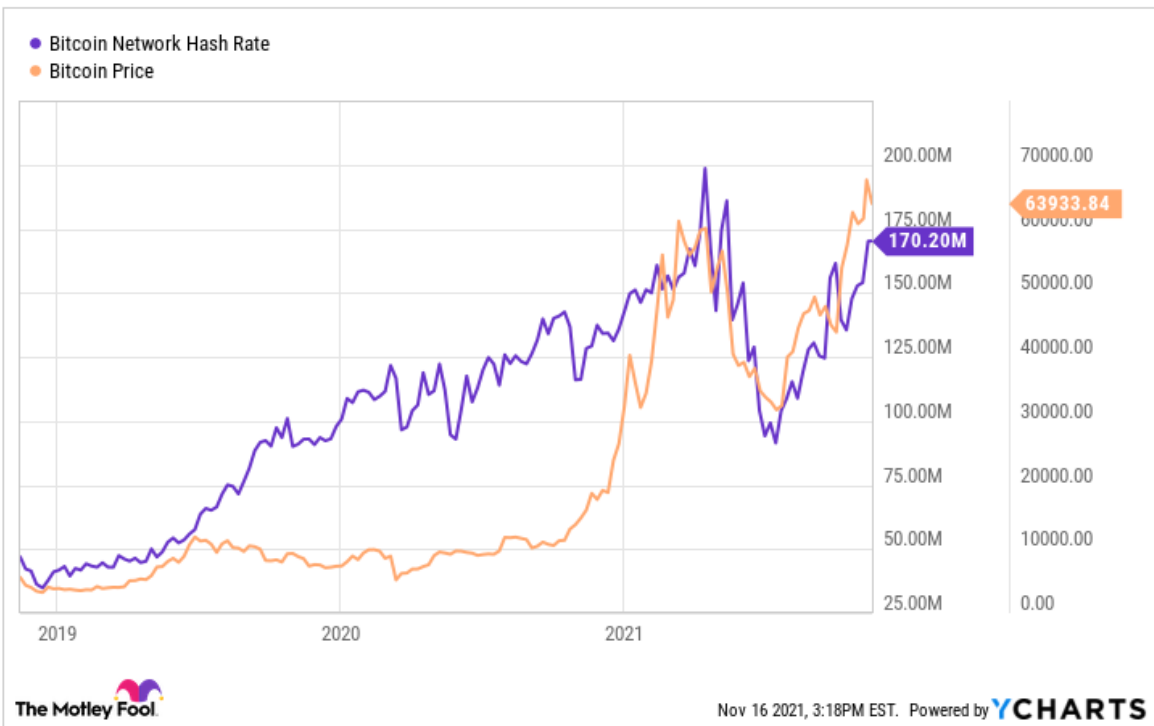
10. If the worker works at the same speed (64 hashes per minute), how many times will they find a new suitable *nonce*?

If the new suitable nonce has two leading zeros, it will take  $(1/16)^2$  or one nonce every 256 hashes.

11. Do *hash* rates in high-end *mining rigs* increase steadily or are they regulated from a maximum value? Include links and/or references and a copy of graphics to show evidence on your point of view. Avoid copying text directly from external documents or web pages.

Hash rates for Proof of Work (PoW) increase with price of underlying crypto currency. This is true for coins like Bitcoin. To limit the number of new bitcoins being added to block chain, the algorithm is

supposed to increase the difficulty level (more number of leading zeros) so that number of bitcoins being added remain constant. This is caused lot of hue and cry among the environmentalists to push the miners to use renewable energy sources. Here is an example of hash rate vs bit coin price (courtesy of YCharts)



12. Is the participation in *mining pools* increasing or decreasing? Include links and/or references and a copy of graphics to show evidence on your point of view. Avoid copying text directly from external documents or web pages.

Participation in mining pools is increasing as seen various hash rates over time for popular hashing sites. In 2010 the first bitcoin mining pool SlushPool is created. In terms of individual miners, the cpu power and energy efficiency is dropping. Compared to individual miners, all miners in the pool receive awards in proportion to their mining power. Pool takes a fee in the process. Cloud mining is any important concept and it getting some traction.



Please refer to <https://genesisblockhk.com/the-history-and-future-of-bitcoin-mining/#Mining-Pool>

Here are miningpool stats: <https://miningpoolstats.stream/>

Here are stats on Ethereum which recently switched to Proof of stake (PoS)

<https://miningpoolstats.stream/ethereum>

13. Using what you have learned, make a prediction on whether the overall participation in Bitcoin mining will be democratized and increased by more people joining mining pools, or if the participation will be controlled by just a couple of organizations with the most powerful *mining rigs*. Include links and/or references and a copy of graphics to show evidence on your point of view. Avoid copying text directly from external documents or web pages.

As the CPU technology continue to defy the moores law, many individuals Will have more and more faster CPUs and GPUs that can be used for mining. With the mining pools, those miners can speed up the coin mining even more. So we see a shift in mining to mining pool concept and these miners may move into cloud computing as well. Longer term, as the price of crypto coins like bitcoin and Ethereum increase, the cloud companies like Amazon and Microsft may start to get engaged in building mining pools.

14. Explain the concept of the “network *hash* rate” and how it differs from a computer *hash* rate.

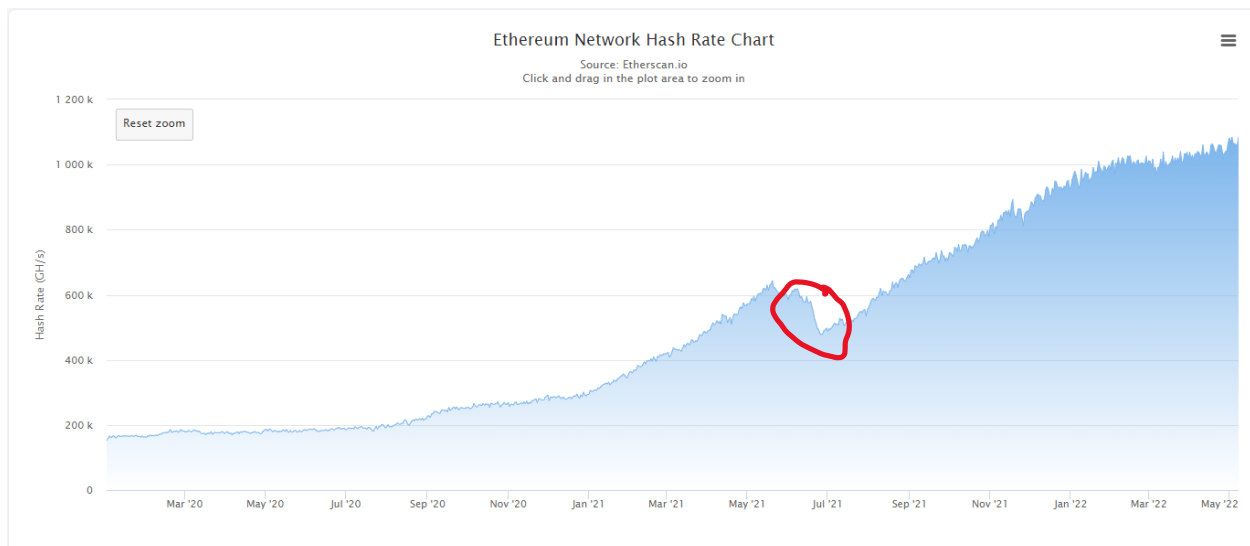
Individual hash rate is simply the hash rate a single entity (computer or server) produces and network hash rate is the combined hash rate of all miners on the network that are int hes ame

15. What does this decrease in the network *hash* rate mean for the Ethereum network? Can you explain why the network *hash* rate has decreased so significantly? Include links and/or references and a copy of graphics to show evidence on your point of view. Avoid copying text directly from external documents or web pages.

Here is Ethereum price since 1/1/2020 : <https://etherscan.io/chart/etherprice>

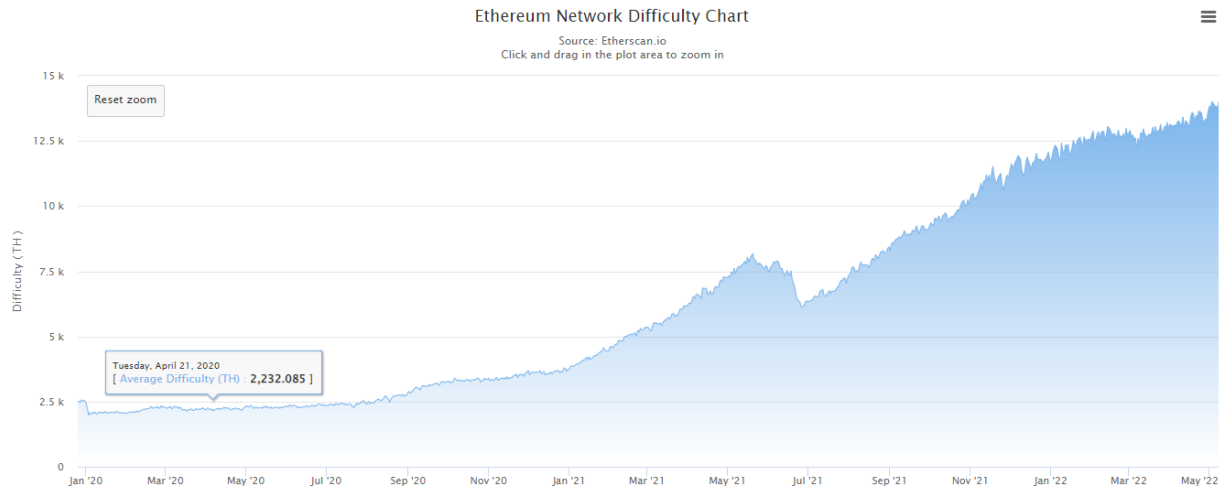


Here is network hash rate:

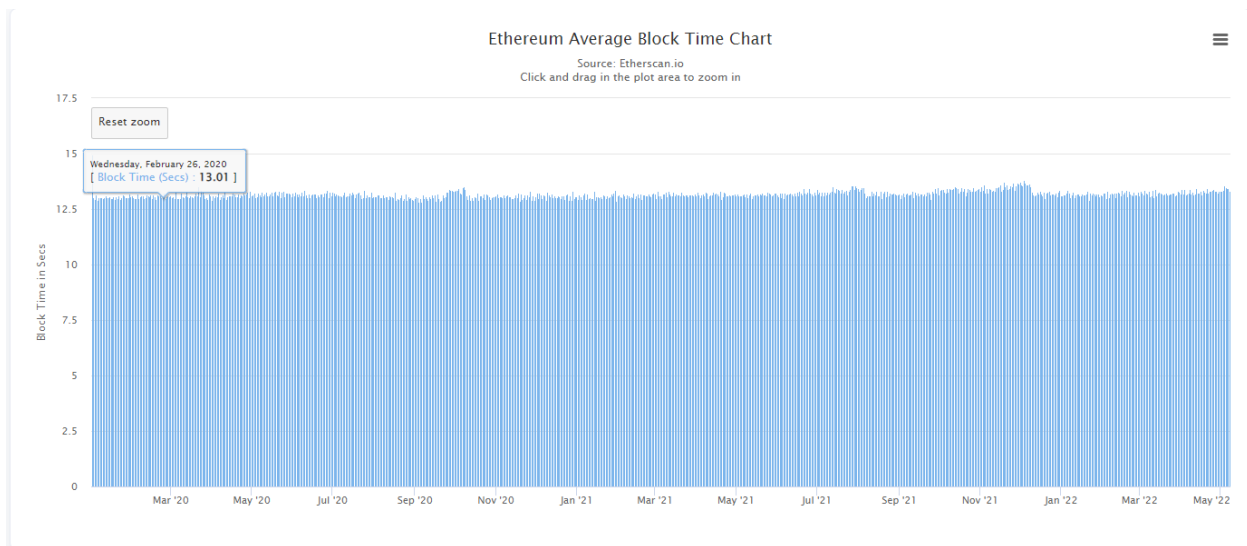


Based on the red circle, it seems the price of Ethereum dropped and caused the network hash rate to drop.

Note that difficulty level also dropped as hash rate dropped so the transaction time for each coin was almost unchanged. Also recently, the hash rate has gone up and so has the difficulty level

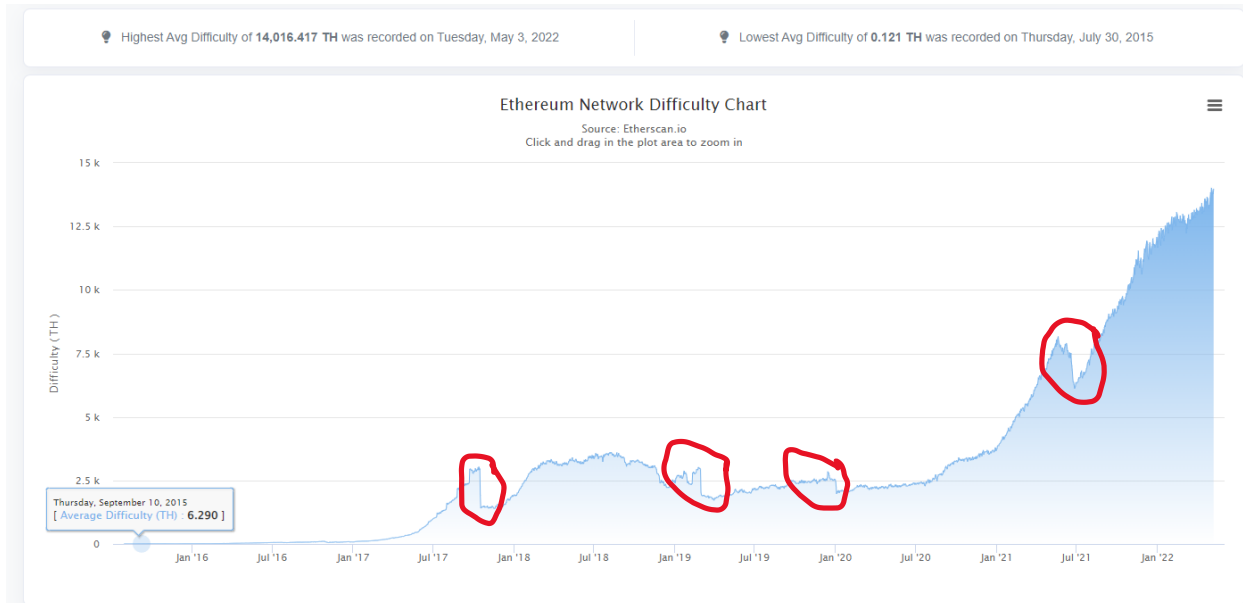


The constant time to generate a Ethereum block is reflected in this chart:



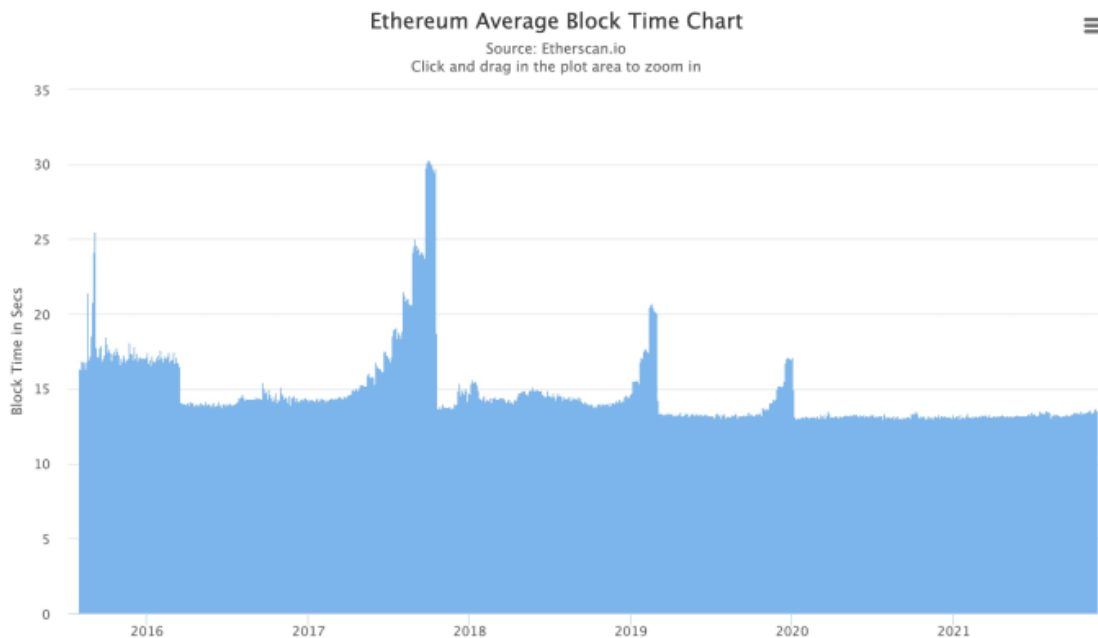
16. When looking at the difficulty table, what important characteristics do you detect? Based on your knowledge on the history of the blockchain Ethereum, what are those characteristics? Include links and/or references and a copy of graphics to show evidence on your point of view. Avoid copying text directly from external documents or web pages.

Here is difficulty level of Ethereum: <https://etherscan.io/chart/difficulty>



There are 4 places in history of Ethereum where the difficulty level dropped. These difficulty levels increase to force miners to switch to proof of stake (Ethereum 2.0) instead of proof of work (used by BitCoin and Ethereum 1.0).

It is also reflected in average block time chart:



Ethereum picks the block time to be between 10 to 19 seconds because that is as fast as possible, but is at the same time substantially longer than network latency. A 2013 paper by Decker and Wattenhofer in Zurich measures bitcoin network latency, and determines that 12.6 seconds is the time it takes for a new block to propagate to 95% of nodes; however, the paper also points out that the bulk of the propagation time is proportional to block size. BTW, Bitcoin tries to maintain its block time to be around 10 minutes with its difficulty algorithm. The very first reference of having 10 minutes as the bitcoin block time comes from the original research paper, which introduced bitcoin in 2008, by Satoshi Nakamoto.