**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)

Graphical user interface, text, application, email

Description automatically generated

1. 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 if fixed independent of the data contentsGraphical user interface, text, application, email

Description automatically generated

1. 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

Graphical user interface, text, application, email

Description automatically generated

1. 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

Graphical user interface, text, application, email

Description automatically generated

1. 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

1. 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

1. 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

1. 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

Graphical user interface

Description automatically generated

Nonce 26:

Graphical user interface, application

Description automatically generated

Graphical user interface

Description automatically generated

Graphical user interface

Description automatically generated with medium confidence

Graphical user interface

Description automatically generated with medium confidence

Graphical user interface, application

Description automatically generated

A picture containing table

Description automatically generated

1. 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\*24\*4 suitable nonce values. = 5760. For above data (“Inderpreet Grang”), we may see that 5760 suitable nonces per day

1. 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.

1. 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)

Chart, line chart

Description automatically generated

1. 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 tgerms of individual miners, the cpu power and energy efficiency is dropping. Compared to individual miners, all miners in the pool receive awards in proporation 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

1. 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.

1. 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

1. 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

Graphical user interface, chart, scatter chart

Description automatically generated

Here is network hash rate:

Chart

Description automatically generated

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 hast rate has gone up and so has the difficulty level

Chart, line chart

Description automatically generated

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

Chart

Description automatically generated

1. 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

A screenshot of a computer

Description automatically generated with medium confidence

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:

Chart, histogram

Description automatically generated

Ethereum picks the block time 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.

Optional

1. 40059

Abel Sanchez sends 1 SanchezCoin to

Inderpreet Grang

[Other transactions]

1. a. 283237, b. 21960 c. 10887 d. 15351

With 2 coins, the hash value is 000081c47e074847c47779b0d8e2b5c90d1cb0299bca33c32b1dccc50771ccb5

And Dr Sanchez has hash value of

0000c4275c2f63dee50f755cc284056782b00abd1cb22a24ad23946d6b00ff83

So he wont believe the message is correct

https://www.thesslstore.com/blog/sha-1-collision-created/