Blockchain and Cryptocurrencies Coursework

pbqk24

March 15, 2019

1 Mining Puzzles

1.1 Proof of Work

The requested information for Proof of Work is as follows:

Index	Information	Value
1	User ID	pbqk24
2	Block hash target calculated (hex)	000003e7fc180000000000000000000000000000000000000000000000000000
3	Nonce value (int)	2171906
4	Number of (double) hashes performed	2171907 (one per nonce tried, starting at 0)
5	Estimate for mining time for difficulty = 1 Estimate for mining time for difficulty = 7454968648263	58629 seconds $4.37 * 10^{17}$ seconds

Table 1: Mining Puzzles: Information Requested

The equations used for calculating the mining time estimates t are as follows:

$$target = \frac{target_{initial}}{difficulty} \tag{1}$$

$$h_q = \frac{h_{space}}{target} \tag{2}$$

$$t = h_q * t_h \tag{3}$$

Where h_q is the estimated number of hashes required to be performed to find a valid hash, $target$ is the target value, t_h is the estimated time per hash calculated by timing how long it takes to perform a large number of hashes (e.g. 10^9) and finding the average. t_h was computed as $1.365 * 10^{-5}$ and used for both calculations.

For difficulty of 1:

$$target = \frac{00000000FFFF0000000000000000000000000000000000000000000000000000}{1}$$

$$h_q = \frac{2^{256}}{00000000FFFF0000000000000000000000000000000000000000000000000000} = 4295032833$$

$$t = 4295032833 * 1.365 * 10^{-5} = 58629$$

For difficulty of 7454968648263:

$$target = \frac{00000000FFFF0000000000000000000000000000000000000000000000000000}{7454968648263} = 3.62 * 10^{54}$$

$$h_q = \frac{2^{256}}{3.62 * 10^{54}} = 3.2 * 10^{22}$$

$$t = 3.2 * 10^{22} * 1.365 * 10^{-5} = 4.37 * 10^{17}$$

1.2 Proof of Stake