Blockchain and Cryptocurrencies Coursework

pbqk24

March 21, 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

The requested information for Proof of Stake is as follows:

Index	Information	Value
6	ECDSA public key (hex)	4f045a6cfacb3e67e7c5d4ddfb9f1acfe7d6ddda c29869734cce5218cdab24e2d2cc72601138d6f 324464df7691f819cd14e8b3752d9c463e5162a ad37393ca0
7	Signature of "Hello world" (hex)	eae12ab8fdbeb5635ac45edbfceb999907a5b090 42eeddbd9a07a744f656b3ac7e00124086256e5 caf86539e68186742d593e5e8b537b9f6d7ee055 57c2ef68a
8	Signature used in calculating hit (hex)	aa2974089248c51977f63350c3aad2757b935d68 a236dd777621c3ed879657d2c5e1f01d22ad16b b2d37f1c2567d1daeccd4e3f1a45201f53291e2e ba9e9bea3
9	Hit value (hex)	a135a0781dd3c0f6
10	Time (s) that you could forge a new block	394

Table 2: Mining Puzzles Information

The equations used for calculating the hit value are as follows:

$$hit_{full} = hash(sign(S_g)) \tag{4}$$

Where the hit value is the first 8 bytes of hit_{full}, and S_g is the generation signature for the previous block:

$$S_g = 9737957703d4eb54efdff91e15343266123c5f15aaf033292c9903015af817f1$$

$$sign(S_g) = aa2974089248c51977f63350c3aad2757b935d68a236dd777621c3ed879657d2c5e1f01d22ad16bb2d37f1c25$$

$$hash(sign(S_g))[:8] = a135a0781dd3c0f6$$

The time in seconds when you would be able to forge a new block was calculated using the following equations:

$$T = T_b * B_e \tag{5}$$

$$t_{forge} = \frac{hit}{T} \tag{6}$$

Where T is the target value (independent of time passed), T_b is the base target value, B_e is your effective balance, and t_{forge} is the time when you can forge a new block (rounded up, in seconds):

$$T = 1229782938247303 * 24 = 29514790517935272$$

$$t_{forge} = \frac{11616367251628998902}{29514790517935272} = 394$$

2 Interacting with bicoin-testnet

Index	Information	Value
1	User ID	pbqk24
2	blockchain.com links	This is included in Table 4 below
3	Transaction explanations	This is included in Table 4 below
4	bitcoin-testnet address	mvcM9NV5hesnSUNpZGZ9Pyt3PK8xDFmCTp
5	100 Satoshi Tx ID chain.so hyperlink	bfb4090faca08fe0f1ca46883cef1bf7e7860a4df6637acb7962741db0206f29 https://chain.so/tx/BTCTEST/bfb4090faca08fe0f1ca46883cef1bf7e7860a4df6637acb7962741db0206f29
6	Proof of Burn Tx ID chain.so hyperlink	611186bc95e29fc70127fce35bd9c8a7f86c46f00aecd9df4765731d27f64d31 https://chain.so/tx/BTCTEST/611186bc95e29fc70127fce35bd9c8a7f86c46f00aecd9df4765731d27f64d31
7	Hex used as script Explanation of hex script	6a067062716b323 This script is equivalent to 'OP_RETURN 06 7062716b323'. This causes the transaction to always be marked invalid, as OP_RETURN always outputs *fail*. The '06' signals that the next 6 bytes are to be pushed onto the stack, and '7062716b323' is the result of converting 'pbqk24', my USER ID, from ASCII to hex.

Table 3: Bitcoin-Testnet Information

Tx	Aspect	Explanation
1	blockchain.com link	
	General explanation	
	Input script	
	Output scripts	
	Inferences from structure	
2	blockchain.com link	
	General explanation	
	Input script	
	Output scripts	
	Inferences from structure	
3	blockchain.com link	
	General explanation	
	Input script	
	Output scripts	
	Inferences from structure	

Table 4: Bitcoin-Testnet Transactions Details