Blockchain Summative

Bradley Mackey

for 22nd March 2019

Task 1 - Mining Puzzles

- 1. User ID: wbbz74
- 3. Valid nonce: 3856645
- 4. Number of double hashes: 3856645

Time taken: 103.41s

5. Time to mine at initial difficulty of 1

Difficulty (D) 0.001 takes 103.41s

$$D = 1 \implies 103.41 \times \frac{1}{0.001} = 103,410 \text{ seconds}$$

$$\implies \frac{103410}{60} = 1,723.5 \text{ minutes}$$

$$\implies \frac{1723.5}{60} = 28.72 \text{ hours.}$$

Time to mine at peak 2018 difficulty of 7, 454, 968, 648, 263

$$D = 7454968648263 \implies 103.41 \times \frac{7454968648263}{0.001} = 7.70918 \times 10^{14} \text{ seconds}$$

$$\implies \frac{103410}{60 \times 60 \times 24} = 8.92266 \times 10^9 \text{ days}$$

$$\implies \frac{8922665600.88}{365.25} = 24,428,927.04 \text{ years}$$

$$\implies \frac{24428927.04}{1000} = 24,428.9 \text{ millenia.}$$

- $6. \ ECDSA\ Public\ Key:\ 14afbb92502c9294f19be099ac3fe51f8ea1c943e36a06c43b096864d8871\\ 45b55e87f1a01b1b9275bcc9d528a2829a774ec6de06dfaed72933ced851105f3ba$
- $7. \ \textit{Hello World Signature}: \ acd 855318df 6ebb 70e4c 956c aad 1c7df 1a 3395c 2ead 557e 6ec 304ced 9038037aa 83e79ab 1bb 80c a3b 912ea 2806c 67cc 387301f 1530e730834bb 3213cf 55b70d 6$
- 8. $Signing\ Key\ (SK)$: f3fdb06bc3e08e4d97849c7a599d78d5991a629cd446ecef25f8ec7a80adc657

9. Hit Value:

Effective balance (E) = 74

Base target $(T_B) = 1229782938247303$ (from prev. block)

Time since last block (t) = 1385656125

New Target = $E \times T_B \times t = 684$ ebf8ccccc24519a66e

Previous generation signature (G) = 9737957703d4eb54efdff91e15343266123c5f15aaf033 292c9903015af817f1

 $\label{eq:Signed} \text{Signed} \ G = \text{SK}(G) = \text{aa}084\text{cddc}3\text{d}64\text{a}4425\text{af}1\text{c}1\text{b}6\text{e}4\text{c}41\text{c}0\text{b}9\text{d}60176\text{e}41\text{b}7134\text{b}c3\text{e}b87\text{d}e\\ 25f9411f83\text{e}ddd7031f7048\text{a}47c5\text{d}0\text{b}f\text{c}4\text{f}df268\text{d}6\text{c}7\text{f}d4\text{e}b41f72\text{e}65933\text{b}a8\text{c}453008\\$

 $\operatorname{Hashed} = \operatorname{SHA256}(\operatorname{SK}(G)) = \operatorname{de9734e60820253cc47281d56b3e9c20d749c34f353e497000e8238eaa45cd55}$

Hit Value = de9734e60820253c

Task 2 - bitcoin-testnet

1. User ID: wbbz74

Task 3 - A Wise Investment?

400-500 WORDS ABOUT WHICH IS THE MOST WISE INVESTMENT? dfkjsdf df sdfk sdfkj sdfkj