

Blockchain Summative

Bradley Mackey

for 22nd March 2019

Please be aware some of the hashes character wrap in strange ways—do not miss the odd wrapped character on the next line.

Task 1 - Mining Puzzles

1. *User ID*: wbbz74
2. *Block hash target*: 000003e7fc18000
000
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
 $D = 1 \implies 103.41 \times \frac{1}{0.001} = 103,410$ seconds
 $\implies \frac{103410}{60} = 1,723.5$ minutes
 $\implies \frac{1723.5}{60} = 28.72$ hours.

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

$$\begin{aligned} D &= 7454968648263 \implies 103.41 \times \frac{7454968648263}{0.001} = 7.70918 \times 10^{14} \text{ seconds} \\ &\implies \frac{7.70918 \times 10^{14}}{60 \times 60 \times 24} = 8.92266 \times 10^9 \text{ days} \\ &\implies \frac{8.92266 \times 10^9}{365.25} = 24,428,927.04 \text{ years} \\ &\implies \frac{24428927.04}{1000} = 24,428.9 \text{ millenia.} \end{aligned}$$

6. *ECDSA Public Key*: 14afbb92502c9294f19be099ac3fe51f8ea1c943e36a06c43b096864d887145b55e87f1a01b1b9275bcc9d528a2829a774ec6de06dfaed72933ced851105f3ba
7. *Hello World Signature*: acd855318df6ebb70e4c956caad1c7df1a3395c2ead557e6ec304ced9038037aa83e79ab1bb80ca3b912ea2806c67cc387301f1530e730834bb3213cf55b70d6

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) = 60 (Nxt block time is 1 min)
 New Target = $E \times T_B \times t$ = 684ebf8cccccc24519a66e
 Previous generation signature (G) = 9737957703d4eb54efdff91e15343266123c5f15aaf033292c9903015af817f1
 Signed G = $SK(G)$ = aa084cddc3d64a4425af1c1b6e4c41c0b9dd60176e41b7134bc3eb87de25f9411f83eddd7031f7048a47c5d0bfc4fdf268d6c7fd4eb41f72e65933ba8c453008
 Hashed = $SHA256(SK(G))$ = de9734e60820253cc47281d56b3e9c20d749c34f353e497000e8238eaa45cd55
Hit Value = de9734e60820253c
10. *Time to forge new block*

Task 2 - bitcoin-testnet

1. User ID: wbbz74
2. (a) trans 1 lnk
 (b) trans 2 lnk
 (c) trans 3 lnk
3. (a) trans 1
 (b) trans 2
 (c) trans 3
4. *Bitcoin Testnet Address*: mjLjznCbyKuGJ5xuz7Wo1Es3qXHoxoDXgo
5. ***100 Satoshi Transaction***
TX ID: 74b5486e061ac680cde0f132b0dec6c5010d2dee8da3a2856d680fcf5bf41c37
Link: <https://chain.so/tx/BCTEST/74b5486e061ac680cde0f132b0dec6c5010d2dee8da3a2856d680fcf5bf41c37>
6. ***Student ID Proof-of-Burn Transaction***
TX ID: bd1c2552fc0effda71e4e09137d8106aa6c67239dfba1e760040d1c78b66e0ac
Link: <https://chain.so/tx/BCTEST/bd1c2552fc0effda71e4e09137d8106aa6c67239dfba1e760040d1c78b66e0ac>

7. *Student ID Proof-of-Burn Script*

Script Hex: 6a067762627a3734

We can add data to the blockchain by immediately invalidating the script, allowing the remainder of the script to be interpreted as pure data. The first byte, 6a, is the `OP_RETURN` word. This invalidates the script, so the remainder of the script is not treated as a transaction. The next byte, 06, is the number of bytes that we will push onto the stack next—“wbbz74” is 6 characters long (6 bytes when ASCII encoded), so this is just 6. The remainder of the script, 7762627a3734, is the ASCII encoded “wbbz74”, which will be interpreted on the blockchain as pure data.

Task 3 - A Wise Investment?

400-500 WORDS ABOUT WHICH IS THE MOST WISE INVESTMENT? Easy stuff.