Ian Brown

Collaborators: None

CSCI3390

3/19/21

Project 1

1.

spark-submit --class "project_1.main" --master "local[*]" target/scala-2.12/project_1_2.12-1.0.jar this_is_a_bitcoin_block_of_27534600 2 1000

string: this_is_a_bitcoin_block_of_27534600

k = 2, trials = 1000

Time Elapsed: 5s

Count: 2

xS: 2065767110this_is_a_bitcoin_block_of_27534600

Hash: 0021c507629666826a6f3df134bfcdb42abe8040804ecb14370d4cdc5dffddd6

k = 3, trials = 3000

Time Elapsed: 5s

Count: 1

xS: 1539512191this_is_a_bitcoin_block_of_27534600

Hash: 000263e0818f87091a4b282574c6abb54c5b1b57d4491385ae1d4e337ab48f4c

k = 4, trials = 30000

Time Elapsed: 5s

Count: 2

xS: (1382379825this_is_a_bitcoin_block_of_27534600

Hash: 0000079a18d4647f734ebc0921a5f40f92ffd1b789fa1e4cedec2a2fc12e4c06)

k = 5, trials = 500000

Time Elapsed: 7s

Count: 1

xS: 1157596949this_is_a_bitcoin_block_of_27534600

Hash: 0000068f11a5018702c628b36d55d66a574d2d661df324bc85de99fe4b850dab

k = 6, trials = 750000

Time Elapsed: 9s

Count: 1

xS: 14197595949this_is_a_bitcoin_block_of_27534600

Hash: 000000ea002548e615e045c0cb2969679cb32b91a521e41c59658b40ba977bd7

2.

First attempt: 100,000 trials with same cluster from setup → did not find after 16s

Second attempt: 200,000 trials with same cluster from setup → did not find after 11s

Third attempt: 200,000 trials with new cluster utilizing 3 Worker nodes rather than 2 and located in us-east1 region → did not find after 20s

Fourth attempt: 700,000 trials with new cluster utilizing 3 Worker nodes rather than 2 and located in us-east1 region → did not find after 12s

Fifth attempt: 1,900,000 trials same cluster from setup → did not find after 17s

Sixth attempt: 9,000,000 trials new cluster with 4 worker nodes → did not find after 43s

Seventh attempt: 9,000,000 trials new cluster with 4 worker nodes → did not find after 48s

Eighth attempt: 100,000,000 trials with cluster with 4 worker nodes → did not find after 357s

Ninth attempt: 1,000,000 trials with cluster with 4 worker nodes with a gpu added for computation → found in 207 seconds, count = 1 : 000000020b2c0c828c95817279eae9a36c0cc9c0aa2ed75e84a11615a122f04aa

- Easiest solution to solving this was to compute using a GPU added to the node. Additional memory and CPU speeds seemed to have little effect which I guess makes sense because PoW tends to work better in GPU heavy environments. At difficulty number 7, the number off trials becomes exponentially higher.

Note: Having a lot of trouble setting up clusters that deviate too much from the default, any time I do anything other than add one small change I get a quota error. I believe this is a

billing issue although in my account it shows that my education billing coupon was applied and I can see the balance.

3.

Change:

```
val nonce = sc.range(0, trials).mapPartitionsWithIndex((indx, iter) => {
  val list = (0 to trials).by(1).toList
  val m_iter = list.iterator
  iter.map(x => m_iter.next)
})
```

```
==================================
found. count:4
(76this_is_a_bitcoin_block_of_12345678,0005f39b49cda29235f7af3c23d0f1c0da688996c5bd73277fc046743fc15d4a)
Time elapsed:6s
==================================
```

While the program still works, I think randomly selecting the nonce would yield faster returns on average if one is to consider the random selections a dumbed down, naïve version of binary search. Likewise, as competition increases, you'd similarly want to heighten your odds and avoid bias at play with linear nonce iterations. Since ASIC miners are so fast and most likely start from 0 and increment the nonce value, they will have tried all possible lower bound values in no time at all, so it's much more worthwhile to make these random attempts.