

Project 1

Group Members:

1. Yash Goel, UFID - 51939756
2. Srikruth Reddy Puram, UFID - 70678514

Outline:

We have implemented a bitcoin mining simulation in Erlang using the Actor Model. We used SHA256 algorithm to hash and mine bitcoins with the desired number of leading zeros. We have also implemented the Remote Configuration using client and server machines.

Usage

- cd the project folder
- Start erl shell and compile both master and miner using `c(master)` and `c(miner)`.
- Run `master.erl` (Write `erl -name master@[your_ip] -setcookie [any_cookie_name]`).
- Run `miner.erl` (Write `erl -name miner@[your_ip] -setcookie [any_cookie_name]`).
- Ignore the warning and follow the inputs generated by code to start mining.

Implementation Details

- To run the program locally, run the `master.erl` by following the above directions. Then you will be prompted with "Number of 0s to mine:" and "Number of miners to spawn:", fill the desired values and start mining.
- To run the program on multiple machines start `master.erl` on one machine and pass 0 in "Number of miners to spawn:", then start `miner.erl` in other machines by following the usage guidelines you will get a prompt "Enter masters IP address with which you want to connect:", enter the host's IP here to connect and start mining.

System 1: master.erl

The `master.erl` is started prior to the `miner.erl` with the number of leading zeros (K) and the number of nodes on each system (Miners). The server spawns Miners (actors) to mine coins and then waits to receive messages either from the spawned actors that a coin is found, which the server will print, or from a client that wishes to participate in the mining. Upon receiving a message from a client, the server spawns other miners to continuously mine for coins. Any number of clients may connect. These actors on the client behave the same as actors on the server and will send a message to the server when a coin is found. Each child actor is designed to continue mining until the server finds a total of 100 coins.

System 2: miner.erl

Client takes in the server node name as the argument and a connection is established with the server after which the server spawns actors on the client to mine for coins.

Assignment Details

1. Work Unit:

Every child actor is tasked with generating a random string, computing the hash, and mining for bitcoins. Each actor runs until the minimum leading zero condition is satisfied and the generated hash is less than the target value. Upon finding 100 coins, all the actors are killed. We determined that each actor should take on the complete responsibility of generating the string, hashing it, and checking if it's a valid coin. Many miners send the string to each actor for hashing. Like wise, once a hash was found and sent to the server, the check for valid coin was moved to the child actor as the server spent a large number of time verifying each hash generated by these large number of actors. Thus, the child actor now takes all the responsibility and the server only tells the child actor whether to continue mining or not.

In our program we give the user the option to enter the number of workers to spawn with an upper threshold of max 4 digit numerical(20,000). We specifically chose this work unit because:-

- This will avoid the possibility of repeated generation of the same string across the workers and limit it to the first n number of miners required by the user.
- Since different workers get different workloads this approach can be horizontally scalable

2. Work Unit Metrics:

We have defined the number of processes to run as = No. of Cores * 4. This ensures that all the cores are used efficiently to mine bitcoins in a faster manner.

3. Result for 4 leading zeros on 4 miners spawned by server

```
PS C:\Users\yash\Desktop\UF\DOSE\New\src> erl -name master@10.20.170.40 -setcookie project.
=INFO REPORT=== 23-Sep-2022::23:15:39.463000 ===
inet_parse:"c:/WINDOWS/System32/drivers/etc/hosts":28: erroneous line, SKIPPED

=INFO REPORT=== 23-Sep-2022::23:15:39.463000 ===
inet_parse:"c:/WINDOWS/System32/drivers/etc/hosts":28: erroneous line, SKIPPED

Eshell V13.0.4 (abort with ^G)
(master@10.20.170.40)1> master:start().
Number of 0s to mine: 4.
Number of miners to spawn: 4.[]
```

Fig.1 Starting the server to mine bitcoins with 4 trailing zeros by spawning 4 miners.

```
23 coins found, minted: "y.goel;X0hLF0gVvaw=" with hash: "000047d7ecaebala39a7472ffa1149a10b9233a343ace1cf29848488e7e73c8" from miner <0.90.0>
24 coins found, minted: "y.goel;BgPFwN3SEz0=" with hash: "000068a68de6e8c7d36a3cc29e852ac84f60ec9fa18da8841704ed377f5a58a1" from miner <0.87.0>
25 coins found, minted: "y.goel;v9td0J3Gluo=" with hash: "00009f29e10af7261b8acabf884b7b61553b97d11e3562612aff1127032bda59" from miner <0.90.0>
26 coins found, minted: "y.goel;LDU4Xugbw3U=" with hash: "000005251cf84a980339b2d2764cb49b9c08f271634c4d60ff2a427c87234ee6" from miner <0.87.0>
27 coins found, minted: "y.goel;1Sc6o4hH0I4=" with hash: "0000019ad2a26535d815fd8df77c1d7a6678bc6057e48e6b91c931c3a482f8b3" from miner <0.87.0>
28 coins found, minted: "y.goel;mKCO5YKYzc4=" with hash: "00006b009d101d7b968c29e8907fdb73f7eedafa3407fdaabcb880ef2dcf4c5e" from miner <0.87.0>
29 coins found, minted: "y.goel;0d+g4CHLD0g=" with hash: "0000074a4cb94f9ee45c54b24992496b3e54650fb76b83d5d89efd84907a1db8" from miner <0.89.0>
30 coins found, minted: "y.goel;AtRbhrrhJLdw=" with hash: "0000d19872f94d743fc94688754323734b981d0f5620070dd660dc78cb10951" from miner <0.88.0>
31 coins found, minted: "y.goel;M9KHPhHu9Kw=" with hash: "0000f536c807301a9c3f7e23210cb4e3e0eefae88d76dc4656d3390b8f0aae4f" from miner <0.89.0>
32 coins found, minted: "y.goel;4zRXgroNQhk=" with hash: "00002f40c65cc4b14078d0c6ed06ba519a522ecb7e0ae18b70231eaa8c8ffcd8d" from miner <0.90.0>
33 coins found, minted: "y.goel;PIsa7IllcoQ=" with hash: "0000c2083090e3e65ff50b9278384bfe4bc43adec28fef8fd634935031013ee2" from miner <0.87.0>
```

Fig.2 Miners start mining.

```
99 coins found, minted: "y.goel;6dvj31/DbLc=" with hash: "00002f6f459cb6db42308a1cfcec45e0c43ebd532c7a96d28d7e1f0820fb6444" from miner <0.97.0>
Total clock time: 39942.041
Total CPU time 299593
CPU time/ Run Time 7.500693317099144
** exception exit: killed
```

Fig.3 CPU utilisation metrics.

CPU time/ Run Time: 7.500693317099144

4. Result for 5 leading zeros on miners spawned by both server and external client using IP address

```
PS C:\Users\yash\Desktop\UF\DOSP\New\src> erl -name master@10.20.170.40 -setcookie project.
=INFO REPORT=== 23-Sep-2022::23:29:47.416000 ===
inet_parse:"c:/WINDOWS/System32/drivers/etc/hosts":28: erroneous line, SKIPPED

=INFO REPORT=== 23-Sep-2022::23:29:47.416000 ===
inet_parse:"c:/WINDOWS/System32/drivers/etc/hosts":28: erroneous line, SKIPPED

Eshell V13.0.4 (abort with ^G)
(master@10.20.170.40)1> master:start().
Number of 0s to mine: 5.
Number of miners to spawn: 2.
```

Fig.4 Starting the server to mine bitcoins with 5 trailing zeros by spawning 2 miners on server and rest will be connected externally from different machine.

```
Terminal: Local +
ashish@Ashishs-MacBook-Pro sample % erl -name miner@10.20.170.65 -setcookie project
Erlang/OTP 25 [erts-13.0.4] [source] [64-bit] [smp:10:10] [ds:10:10:10] [async-threads:1] [jit] [trace]

Eshell V13.0.4 (abort with ^G)
(miner@10.20.170.65)1> miner:start().
~n Enter masters IP address with which you want to connect: "10.20.170.40".

Sending connection request to Master 'master@10.20.170.40'<0.88.0>

Received input from server to mine, starting mining(miner@10.20.170.65)2> miner:start().
~n Enter masters IP address with which you want to connect: "10.20.170.40".

Sending connection request to Master 'master@10.20.170.40'<0.96.0>

Received input from server to mine, starting mining(miner@10.20.170.65)3>
```

Fig.5 Starting miner on different machine.

```
21 coins found, minted: "y.goe!;BHSeZNGvM1U=" with hash: "00000e18a9c1e9f518ab092c777f03d08d74a4f4dc3a6372cf5adb21ad2222" from miner <0.99.0>
22 coins found, minted: "y.goe!;Gn0HAXIpuw=" with hash: "0000018cd65be920699e0c45e1dc6376c6b76e0314c54dfdc5665d4be324a183" from miner <0.100.0>
23 coins found, minted: "y.goe!;9pbfXxgH=" with hash: "0000083ccdd6d4847db0ab612c1c8447b194657b56e1dc3237185ea563c44" from miner <0.99.0>
24 coins found, minted: "y.goe!;Xw/kmEYbLE=" with hash: "00000eb10282117bc30dbdd47cca6f08229787b815be5f8e6a25cb76c50e708b" from miner <0.99.0>
25 coins found, minted: "y.goe!;PCDuMSl3cId=" with hash: "00000d3adbd5029f457227f6e22b728a61b8abec7b8d8e8f28ad72ee4bfd8" from miner <0.100.0>
26 coins found, minted: "y.goe!;h16A25nxdS=" with hash: "0000035ebcf9cdf8724baa98a763b381a8d42743202170ecf95c5db159e9d5b" from miner <0.100.0>

Incoming Connection Request
Received connection from: <14200.88.0>

27 coins found, minted: "y.goe!;5M8LRugDn/c=" with hash: "0000071b929d8145ee05c8ec7e1abaf6fb9fa6ae45f555c3f5411b760a5e1968" from miner <0.99.0>
28 coins found, minted: "y.goe!;8YwZJ1DMRFY=" with hash: "0000099a212bc3209547f9e1806b83e183f57d461ae5b28c0dc184cb04cae03" from miner <0.99.0>
29 coins found, minted: "y.goe!;NnyIwxJ8jYI=" with hash: "00000fdae9a94dd4d4e0c22b21bc1426763198b758d7f65a47d4b7a54b3563a" from miner <0.99.0>
30 coins found, minted: "y.goe!;8gcvr1mk4S=" with hash: "00000c45ad6f7145355a1cded3083301836dc1b205ee085bac3f0850e0972c" from miner <14200.88.0>
31 coins found, minted: "y.goe!;CnW4+78dZgzs=" with hash: "00000513581cf73c2b23da38708372b06d88cb7298105967cba5043f239d5" from miner <0.100.0>
32 coins found, minted: "y.goe!;otX5Zkrzk18=" with hash: "0000035a29f0ae9a9602e53c4877195215fe58add8bdec59d93278e4d6dfc89d" from miner <14200.88.0>
33 coins found, minted: "y.goe!;VeT/bNQG8nwe=" with hash: "000003255f7a3ce0477afc1070fc1413779ae1dc4b1e124533e96148fd12d04f" from miner <0.99.0>
34 coins found, minted: "y.goe!;pdEj08auJ2Q=" with hash: "000004d1e3532e05be98fbf87864f184246c34e8b3d2889d713a19d6fe5f58" from miner <14200.88.0>
35 coins found, minted: "y.goe!;w0rpMA0uGA=" with hash: "000008f7dc57128626c104464c037791390a99c29c965cf3d2cc8b0b7baa" from miner <14200.88.0>
36 coins found, minted: "y.goe!;0BFovvJsw8C=" with hash: "0000017c9e4147f5168152daa3d3a4a8a03b77827ef95fc3954d2a9f3b8699ae" from miner <0.99.0>
37 coins found, minted: "y.goe!;jM6Xu4wxzG4=" with hash: "000007d1100aa3a992387d68a4cf7749f3608628b7ee01ff5f21f42e3717ae3" from miner <14200.88.0>
38 coins found, minted: "y.goe!;ZKONckna5Mo=" with hash: "00000f013754fc58bb4deef17a558eb0ffc3e8c8839dbb11d61665f8be81841f" from miner <14200.88.0>
```

Fig.6 Server receives request from miner.

```
6 coins found, minted: "y.goe!;lriysV80e10=" with hash: "0000037e962ccc57f7d4e0d90c7150279ae106865295c21dbae2f0296cb3e52c" from miner <14200.88.0>

Incoming Connection Request
Received connection from: <14233.92.0>

7 coins found, minted: "y.goe!;s4WoGI0cv7M=" with hash: "0000d26c5e9c9be62245371c72364e7d5669cb98f14ca022f1bc669a080b2c4c" from miner <14233.92.0>
8 coins found, minted: "y.goe!;YKzcZfdn0uM=" with hash: "0000c867b5ef890e98df27d56e861e0e512ad2ccfa5a3ea00e3196f182772e73" from miner <14233.92.0>
9 coins found, minted: "y.goe!;tW09g3EMR8=" with hash: "0000bf53182b87295d954911f5069e486868dc02a7e9582e60c326818f1560b" from miner <14233.92.0>
10 coins found, minted: "y.goe!;0y00LZDJI=" with hash: "00004b0e905e90383c2d3b7a5f6c3b5466142e0311573000ae6079546c" from miner <14233.92.0>
11 coins found, minted: "y.goe!;YKCPZVHVZI=" with hash: "0000634e9180492818534a4762608cf025a0711fca9d9110f2289a086793c37" from miner <14233.92.0>
12 coins found, minted: "y.goe!;0btNlgMtPK8=" with hash: "0000091f4075e175b1a569385c9d3ac354aba22af9c8305c6b64df247ced" from miner <14233.92.0>
13 coins found, minted: "y.goe!;R2WjGDP8iC=" with hash: "0000f0d66d8d0a46bc9d16cb3c08e91b1dd8b685db9a5fd5db2170fa56ff5" from miner <14233.92.0>
14 coins found, minted: "y.goe!;R3id3FRN8A=" with hash: "00005922f65d6d65903603e39e8cc2e79121b7f6cb872ec3fc75f8c14cac1b5" from miner <14233.92.0>
15 coins found, minted: "y.goe!;ubrfM9cWVA=" with hash: "0000e477d3793ae5df170ef1d81efaf66df0ea70a240402a4fc7f0cc16a92" from miner <14233.92.0>
16 coins found, minted: "y.goe!;lgwVUPHyPg=" with hash: "0000ba22ad37b53bb8f21b723cbb4c74c9a78257769980b9786c88fa48cb9" from miner <14233.92.0>
17 coins found, minted: "y.goe!;FvVFL6LCbk=" with hash: "0000ec24722c1476d93874c944393f3df00e2d8c68b34b54644703de01c97b" from miner <14233.92.0>
18 coins found, minted: "y.goe!;x86wQZy+TDU=" with hash: "0000aa44c7258fb7080a6dbf735f0ab17e7e3198bddd4d1d67723d454a9bc7564" from miner <14233.92.0>
19 coins found, minted: "y.goe!;Y8ylwQhU4=" with hash: "0000094ec156e25ba813a5fc2154f91cae50848e286540420546f4a07be0cc" from miner <14233.92.0>
20 coins found, minted: "y.goe!;A0w8C0uYvS=" with hash: "0000e477d3793ae5df170ef1d81efaf66df0ea70a240402a4fc7f0cc16a92" from miner <14233.92.0>
21 coins found, minted: "y.goe!;754uSEOPxs=" with hash: "000068c00a79a72e74ee09d7da902db40aee1b8024245e14cdab502799b3237" from miner <14233.92.0>
22 coins found, minted: "y.goe!;8evpGRnS0u=" with hash: "0000d4c3eacaa5cc785afcead408ebc59714ce9b6e03b24c872b3513d00bfcf1" from miner <14233.92.0>
23 coins found, minted: "y.goe!;mb3+Rbsd0=" with hash: "0000f6cb3c420fb86fa893f85f6fc2743854ef910b85de9975583e8091735a" from miner <14233.92.0>
```

Fig.7 Starting 3 miners from different machine to connect to server.

- <0.99.0> and <0.100.0> are miners hosted by server on machine 1.
- <14200.88.0> is miner hosted by machine 2.
- <14233.92.0> is miner hosted by machine 3.
- -Total clock time: 468174.336

- -Total CPU time: 861953
- -CPU time/ Run Time: 1.841094083380085
-

5. Largest coin found (i.e., the coin with the highest number of leading 0's)

We found the largest coin to have seven zeros. The program was run for few hours to find 8 zeros, but no coins were found and the program was stopped.

```
2> master:start().
Number of 0s to mine: 7.
Number of miners to spawn: 16.
0 coins found, minted: "y.goel;0SiLEaxcR0A=" with hash: "00000004583c4687381e59137363e1e9b6e5561829b6d43a820444af04b2c635" from miner <0.87.0>
[]
```

Fig.8 Largest coin found with highest leading zeros

6. Largest number of working machines

We used Intel i7-8550U CPU (8 MB cache, 4 cores). We were able to run the script on four nodes but the same could be scaled to run on many more. We were able to connect three different machines to mine on 1 server.