Project 1

Group Members:

1. Vaishnavi Chilakamarthi, UFID: 99936597, vchilakamarthi@ufl.edu

2. Vanshika Mehrotra, UFID: 77239277 , vmehrotra@ufl.edu

Description:

The goal of this project is to use Erlang and the actor model to build a good solution to the bitcoin mining problem that runs well on multi-core machines. Concurrency in Erlang is fundamental to its success. Rather than providing threads that share memory, each Erlang process executes in its own memory space and owns its own heap and stack. Processes can't interfere with each other inadvertently, as is all too easy in threading models, leading to deadlocks and other horrors The ACTOR model will work as distributed system to find a hashed value (basically a string) that will have a smaller or equal value to the target hash and will contain some leading zeros that will be given by the user. The target hash algorithm we are using is SHA-256. We will also implement a basic client-server model to distribute work to multiple machines.

Execution steps:

1. cd the project1 folder

2. Start erl shell and compile both miningserver and miningclient using 'c(miningserver).' and 'c(miningclient).'

3. Run miningserver.erl with k as an argument where k is the no of leading zeros and N as the number of trials

4. Run miningclient.erl to start the connection between, the client will start mining and will provide the final string to the server which will be printed.

5. Ignore the warning and follow the inputs generated by code to start mining.

Implementation Details

System 1: miningserver.erl

The Server on startup takes the number of leading zeros from the user as K and N as the number of trials and starts mining until clients are available.

When a client node is available for mining, the Server receives a connect request, processes it and sends the K value required for the client to start mining.

The Server consists of the logic to accept client requests, and print the coins mined by the clients as well as itself.

System 2: miningclient.erl

When a client node is created, it first needs to send a connection request to the server using the name of the node on which the server is running.

Once the connection is established, the client receives the number of zeros to mine, and spawns the Worker units on its own machine and generates as many bitcoins as possible.

Wherever a bitcoin is mined, the data is sent to the Server and the server prints it.

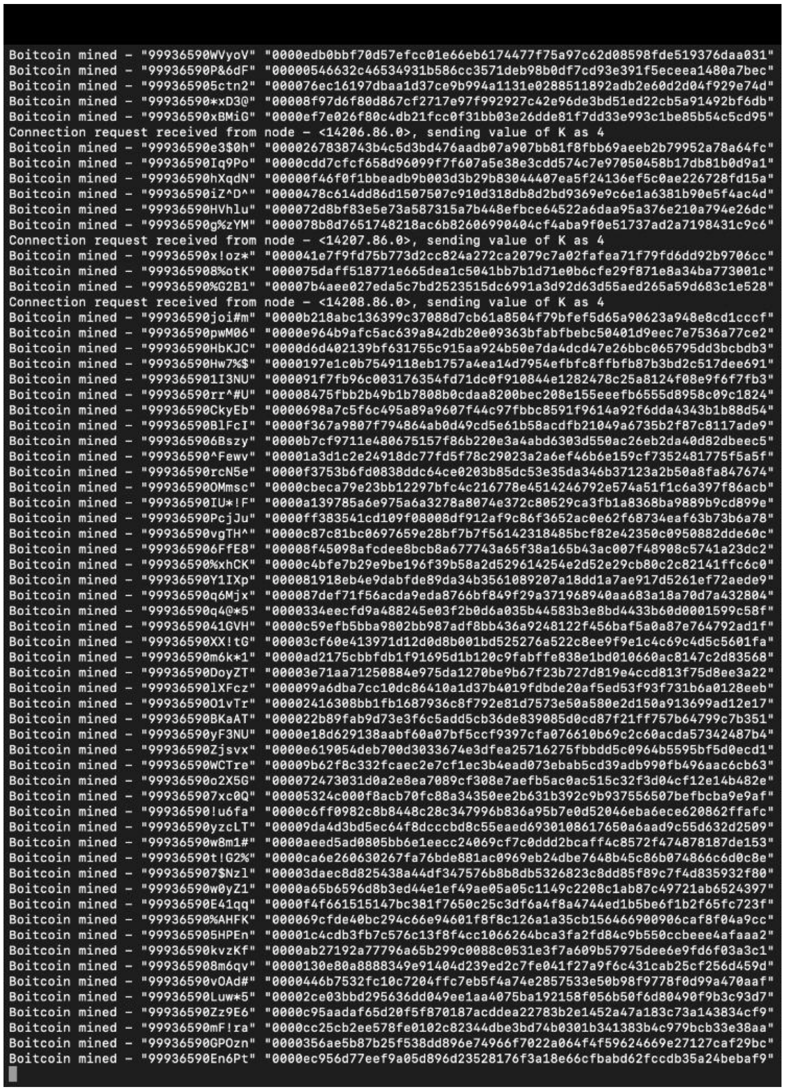
In our project, we are using the get_random_string function to generate random strings based on the length of the string to be generated and the allowed characters for the random string, which is further hashed with SHA256. This generates a fixed length string of 32 digits. The total number of permutations for an alphanumeric string of 32 characters is (32)^36. This approach makes sures that no two worker nodes mine using the same string.

1. Work Unit:

The application follows a Client-Server architecture.

The work unit for the project refers to the number of calls the process will make to the method which does the work of generating random strings of length N, calculating the hash of each string and checking if the leading zeros are correct as per the requirement. We have executed the program in a 10th Gen Intel Quad-Core i5 system.

2. Result for 4 leading zeros



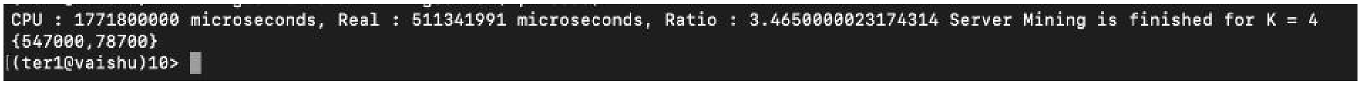
```
Boitcoin mined - "99936590WVyoV" "0000edb0bbf70d57efcc01e66eb6174477f75a97c62d08598fde519376daa031"
Boitcoin mined - "99936590P&6dF" "00000546632c46534931b586cc3571deb98b0df7cd93e391f5eceea1480a7bec"
Boitcoin mined - "999365905ctn2" "000076ec16197dbaa1d37ce9b994a1131e0288511892adb2e60d2d04f929e74d"
Boitcoin mined - "99936590*xD3@" "00008f97d6f80d867cf2717e97f992927c42e96de3bd51ed22cb5a91492bf6db"
Boitcoin mined - "99936590xBMiG" "0000ef7e026f80c4db21fcc0f31bb03e26dde81f7dd33e993c1be85b54c5cd95"
Connection request received from node - <14206.86.0>, sending value of K as 4
Boitcoin mined - "99936590e3$0h" "0000267838743b4c5d3bd476aadb07a907bb81f8fbb69aeeb2b79952a78a64fc"
Boitcoin mined - "99936590Iq9Po" "0000cdd7cfcf658d96099f7f607a5e38e3cdd574c7e97050458b17db81b0d9a1"
Boitcoin mined - "99936590hXqdN" "00000f46f0f1bbeadb9b003d3b29b83044407ea5f24136ef5c0ae226728fd15a"
Boitcoin mined - "99936590iZ^D^" "0000478c614dd86d1507507c910d318db8d2bd9369e9c6e1a6381b90e5f4ac4d"
Boitcoin mined - "99936590HVhlu" "000072d8bf83e5e73a587315a7b448efbce64522a6daa95a376e210a794e26dc"
Boitcoin mined - "99936590g%zYM" "000078b8d7651748218ac6b82606990404cf4aba9f0e51737ad2a7198431c9c6"
Connection request received from node - <14207.86.0>, sending value of K as 4
Boitcoin mined - "99936590x!oz*" "000041e7f9fd75b773d2cc824a272ca2079c7a02fafea71f79fd6dd92b9706cc"
Boitcoin mined - "999365908%otK" "000075daff518771e665dea1c5041bb7b1d71e0b6cfe29f871e8a34ba773001c"
Boitcoin mined - "99936590%G2B1" "00007b4aee027eda5c7bd2523515dc6991a3d92d63d55aed265a59d683c1e528"
Connection request received from node - <14208.86.0>, sending value of K as 4
Boitcoin mined - "99936590joi#m" "0000b218abc136399c37088d7cb61a8504f79bfef5d65a90623a948e8cd1cccf"
Boitcoin mined - "99936590pwM06" "0000e964b9afc5ac639a842db20e09363bfabfbebc50401d9eec7e7536a77ce2"
Boitcoin mined - "99936590HbKJC" "0000d6d402139bf631755c915aa924b50e7da4dcd47e26bbc065795dd3bcbdb3"
Boitcoin mined - "99936590Hw7%$" "0000197e1c0b7549118eb1757a4ea14d7954efbfc8ffbfb87b3bd2c517dee691"
Boitcoin mined - "999365901I3NU" "000091f7fb96c003176354fd71dc0f910844e1282478c25a8124f08e9f6f7fb3"
Boitcoin mined - "99936590rr^#U" "00008475fbb2b49b1b7808b0cdaa8200bec208e155eeefb6555d8958c09c1824"
Boitcoin mined - "99936590CkyEb" "0000698a7c5f6c495a89a9607f44c97fbbc8591f9614a92f6dda4343b1b88d54"
Boitcoin mined - "99936590BlFcI" "0000f367a9807f794864ab0d49cd5e61b58acdfb21049a6735b2f87c8117ade9"
Boitcoin mined - "999365906Bszy" "0000b7cf9711e480675157f86b220e3a4abd6303d550ac26eb2da40d82dbeec5"
Boitcoin mined - "99936590^Fewv" "00001a3d1c2e24918dc77fd5f78c29023a2a6ef46b6e159cf7352481775f5a5f"
Boitcoin mined - "99936590rcN5e" "0000f3753b6fd0838ddc64ce0203b85dc53e35da346b37123a2b50a8fa847674"
Boitcoin mined - "99936590OMmsc" "0000cbeca79e23bb12297bfc4c216778e4514246792e574a51f1c6a397f86acb"
Boitcoin mined - "99936590IU*!F" "0000a139785a6e975a6a3278a8074e372c80529ca3fb1a8368ba9889b9cd899e"
Boitcoin mined - "99936590PcjJu" "0000ff383541cd109f08008df912af9c86f3652ac0e62f68734eaf63b73b6a78"
Boitcoin mined - "99936590vgTH^" "0000c87c81bc0697659e28bf7b7f56142318485bcf82e42350c0950882dde60c"
Boitcoin mined - "999365906FfE8" "00008f45098afcdee8bcb8a677743a65f38a165b43ac007f48908c5741a23dc2"
Boitcoin mined - "99936590%xhCK" "0000c4bfe7b29e9be196f39b58a2d529614254e2d52e29cb80c2c82141ffc6c0"
Boitcoin mined - "99936590Y1IXp" "000081918eb4e9dabfde89da34b3561089207a18dd1a7ae917d5261ef72aede9"
Boitcoin mined - "99936590q6Mjx" "000087def71f56acda9eda8766bf849f29a371968940aa683a18a70d7a432804"
Boitcoin mined - "99936590q4@*5" "0000334eecfd9a488245e03f2b0d6a035b44583b3e8bd4433b60d0001599c58f"
Boitcoin mined - "9993659041GVH" "0000c59efb5bba9802bb987adf8bb436a9248122f456baf5a0a87e764792ad1f"
Boitcoin mined - "99936590XX!tG" "00003cf60e413971d12d0d8b001bd525276a522c8ee9f9e1c4c69c4d5c5601fa"
Boitcoin mined - "99936590m6k*1" "0000ad2175cbbfdb1f91695d1b120c9fabffe838e1bd010660ac8147c2d83568"
Boitcoin mined - "99936590DoyZT" "00003e71aa71250884e975da1270be9b67f23b727d819e4ccd813f75d8ee3a22"
Boitcoin mined - "99936590lXFcz" "000099a6dba7cc10dc86410a1d37b4019fdbde20af5ed53f93f731b6a0128eeb"
Boitcoin mined - "99936590O1vTr" "00002416308bb1fb1687936c8f792e81d7573e50a580e2d150a913699ad12e17"
Boitcoin mined - "99936590BKaAT" "000022b89fab9d73e3f6c5add5cb36de839085d0cd87f21ff757b64799c7b351"
Boitcoin mined - "99936590yF3NU" "0000e18d629138aabf60a07bf5ccf9397cfa076610b69c2c60acda57342487b4"
Boitcoin mined - "99936590Zjsvx" "0000e619054deb700d3033674e3dfea25716275fbbdd5c0964b5595bf5d0ecd1"
Boitcoin mined - "99936590WCTre" "00009b62f8c332fcaec2e7cf1ec3b4ead073ebab5cd39adb990fb496aac6cb63"
Boitcoin mined - "99936590o2X5G" "000072473031d0a2e8ea7089cf308e7aefb5ac0ac515c32f3d04cf12e14b482e"
Boitcoin mined - "999365907xc0Q" "00005324c000f8acb70fc88a34350ee2b631b392c9b937556507befbcba9e9af"
Boitcoin mined - "99936590!u6fa" "0000c6ff0982c8b8448c28c347996b836a95b7e0d52046eba6ece620862ffafc"
Boitcoin mined - "99936590yzcLT" "00009da4d3bd5ec64f8dcccbd8c55eaed6930108617650a6aad9c55d632d2509"
Boitcoin mined - "99936590w8m1#" "0000aeed5ad0805bb6e1eecc24069cf7c0ddd2bcaff4c8572f474878187de153"
Boitcoin mined - "99936590t!G2%" "0000ca6e260630267fa76bde881ac0969eb24dbe7648b45c86b074866c6d0c8e"
Boitcoin mined - "999365907$Nzl" "00003daec8d825438a44df347576b8b8db5326823c8dd85f89c7f4d835932f80"
Boitcoin mined - "99936590w0yZ1" "0000a65b6596d8b3ed44e1ef49ae05a05c1149c2208c1ab87c49721ab6524397"
Boitcoin mined - "99936590E41qq" "0000f4f661515147bc381f7650c25c3df6a4f8a4744ed1b5be6f1b2f65fc723f"
Boitcoin mined - "99936590%AHFK" "000069cfde40bc294c66e94601f8f8c126a1a35cb15646690090 6caf8f04a9cc"
Boitcoin mined - "999365905HPEn" "00001c4cdb3fb7c576c13f8f4cc1066264bca3fa2fd84c9b550ccbeee4afaaa2"
Boitcoin mined - "99936590kvzKf" "0000ab27192a77796a65b299c0088c0531e3f7a609b57975dee6e9fd6f03a3c1"
Boitcoin mined - "999365908m6qv" "0000130e80a8888349e91404d239ed2c7fe041f27a9f6c431cab25cf256d459d"
Boitcoin mined - "99936590vOAd#" "0000446b7532fc10c7204ffc7eb5f4a74e2857533e50b98f9778f0d99a470aaf"
Boitcoin mined - "99936590Luw*5" "00002ce03bbd295636dd049ee1aa4075ba192158f056b50f6d80490f9b3c93d7"
Boitcoin mined - "99936590Zz9E6" "0000c95aadaf65d20f5f870187acddea22783b2e1452a47a183c73a143834cf9"
Boitcoin mined - "99936590mF!ra" "0000cc25cb2ee578fe0102c82344dbe3bd74b0301b341383b4c979bcb33e38aa"
Boitcoin mined - "99936590GPOzn" "0000356ae5b87b25f538dd896e74966f7022a064f4f59624669e27127caf29bc"
Boitcoin mined - "99936590En6Pt" "0000ec956d77eef9a05d896d23528176f3a18e66cfbabd62fccdb35a24bebaf9"
▮
```

Fig.1 Output for mining the coins with 4 leading zeros

3. Ratio of CPU time to Real Time

The ratio of the cpu and real time is calculated to prove the parallel usage of the cores present in the machine and it illustrates the number of cores which are effectively used in computation.

Ratio= 3.46

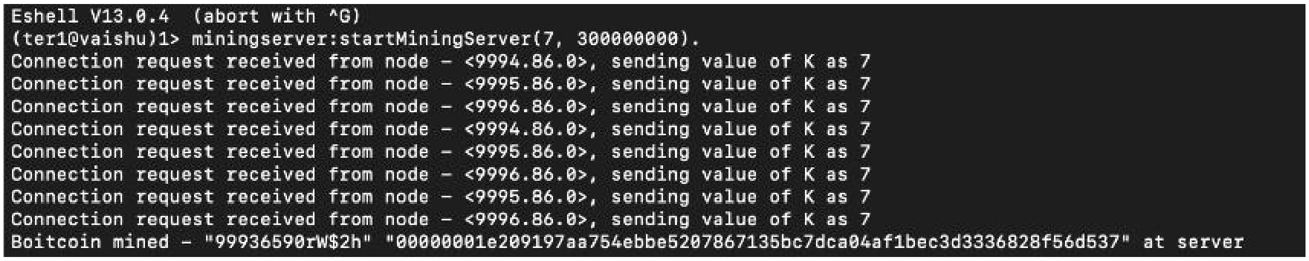


```
CPU : 1771800000 microseconds, Real : 511341991 microseconds, Ratio : 3.4650000023174314 Server Mining is finished for K = 4
{547000,78700}
[(ter1@vaishu)10> ▮
```

Fig.2 Output for the computation of ratio of the CPU time to the Real time

4. Largest coin found with highest leading zeros

We found the largest coin to have seven zeros.



```
Eshell V13.0.4  (abort with ^G)
(ter1@vaishu)1> miningserver:startMiningServer(7, 300000000).
Connection request received from node - <9994.86.0>, sending value of K as 7
Connection request received from node - <9995.86.0>, sending value of K as 7
Connection request received from node - <9996.86.0>, sending value of K as 7
Connection request received from node - <9994.86.0>, sending value of K as 7
Connection request received from node - <9995.86.0>, sending value of K as 7
Connection request received from node - <9996.86.0>, sending value of K as 7
Connection request received from node - <9995.86.0>, sending value of K as 7
Connection request received from node - <9996.86.0>, sending value of K as 7
Boitcoin mined - "99936590rW$2h" "00000001e209197aa754ebbe5207867135bc7dca04af1bec3d3336828f56d537" at server
```

Fig.3 Output for the coin found with 7 leading zeros

5. Largest number of working machines on which the code was run

The size of the work unit refers to the number of subproblems that a worker gets in a single request from the boss. The code was simultaneously run on 6 nodes with one functioning as server and the other 5 as workers.