COP5615 - DOSP Project 1

Team Members:

1. Aadithya Kandeth - 69802791
2. Anol Kurian Vadakkeparampil - 56268544

Objective

This project intends to hash using SHA 256 and mine bitcoins based on the number of leading zeros that is passed as an input to the program.
It has been developed in erlang and uses the actor model. The client and server are run on 2 separate machines and multiple clients can be added in order to spawn more worker nodes.

bc_server.erl (System 1)

The server is run on system 1 and does the following:
start: Takes in the number of nodes to spawn and the required number of leading zeros to be found as input arguments.
receive: The receive function can accepts two types of messages. Messages received from the workers are printed to indicate that a coin has been found. Messages received from the client leads to further actors being spawned. These new actors are also used for mining. The process continues till 234 (arbitrary) coins are found.
spawn_nodes: Spawns nodes based on the input passed.
mine_coins: Finds the bitcoin based on the number of leading zeroes.
hash_computor: Generates the hash using SHA 256 on the randomly generated string.
random_string_generator: generates a random string that is prefixed by the team member names and the UFID.

bc_client.erl (System 2)

The client only contains one function. It takes in the server name as an argument to setup a connection with the server. The current node name is then passed as a message to the server after which actors are spawned on the client. These actors continue the job.

1. Worker process

Steps:

1. Generate a random string

2. Calculate the hash for that string
3. Keep running until the leading zero condition is satisfied.
4. If a message is received form the client, more actors are spawned.
5. Any coins found by the client nodes are printed on the server itself.
6. The actors are killed once a certain number of coins are found.
7. The relevant statistics are calculated once the program is terminated

OUTPUT

The following screenshots show the output for running the program across a single server and 2 clients running on different machines.

Starting Server:

```
Eshell V13.0.4  (abort with ^G)
(aadiserver@10.20.226.59)1> c(bc_server)
.
bc_server.erl:4:2: Warning: export_all flag enabled - all functions will be exported
%    4| -compile(export_all).
%     |  ^

{ok,bc_server}
(aadiserver@10.20.226.59)2> bc_server:start(5,5).
Number of Zeroes : 5 || String representation of zeroes "00000"
```

Client 1 Connecting:

```
Coins found: 1 :
BitCoin :  "aadithyakandeth;/z/UrOjhgeM=" and Generated Hash is "00000cf377b125b9a8073d7cd9cf60e307d66bf725a0da6d31c52c6e34693efb"
Found by <0.92.0>

Connection request by 'anolclient1@192.168.56.1' Spawning..

Coins found: 2 :
BitCoin :  "aadithyakandeth;E/gJKV+LiUQ=" and Generated Hash is "00000971543ee6398db692d3f42b8cd9ad6b2ee296fbbd7ed50c62496ab021c7"
Found by <13817.110.0>
```

Client 2 Connecting:

```
Coins found: 31 :
BitCoin :  "aadithyakandeth;eVlWSm7WBDk=" and Generated Hash is "00000ec5cf69bd9a3840a36dd3457b227b4d270a98d28789189b2695b35cade7"
Found by <0.93.0>

Connection request by 'anolclient@192.168.56.1' Spawning..

Coins found: 32 :
BitCoin :  "aadithyakandeth;NmL+KwRoDw8=" and Generated Hash is "00000828d7141ff6353201e7194b5623a11f30185342c6ce4b17ce5cc95cd898"
Found by <0.92.0>
```

Client Side:

```
{node,'anolclient1@192.168.56.1'}
(anolclient1@192.168.56.1)3> bc_client:start('aadiser
ver@10.20.226.59').
```

```
36-Fall2022-main> erl -name anolclient@192.168.56.1 -se
tcookie aadi
Eshell V13.0.4  (abort with ^G)
(anolclient@192.168.56.1)1> bc_client:start('aadiserver
@10.20.226.59').
{node,'anolclient@192.168.56.1'}
(anolclient@192.168.56.1)2>
```

Statistics:

```
Coins found: 234 :
BitCoin :  "aadithyakandeth;POb8hHbkWOM=" and Generated Hash is "00008a92ef4f68426c61f8e0a8038f034a119ffd6f2746d0f69c4ef5f0d9b08b"
Found by <13362.98.0>

Total clock time(Time/1000): 18029.465
Total CPU time: 88875
 CPU time/RunTime: 4.929430795644796
ok
(aadiserver@10.20.226.59)3>
```

Statistics with 2 clients and 1 server working:

Size of the work unit = 24

For input 4 (4 leading zeros):

Total Clock time = 18029.465

Total CPU time = 88875

CPU time/Run time ratio = 4.929430795644796

Largest coin found

The most number of leading zeroes found was 7. The program took around 10 minutes to find a coin with 7 leading zeroes.

7 zeroes:

```
(anolserver@10.20.226.59)1> bc_server:start(7,10000).
Number of Zeroes : 7 || String representation of zeroes "0000000"

Coins found: 1 :
BitCoin :  "anolkurivadakke;1BRSR9CetK0=" and Generated Hash is "00000008732b725faa93226a4e1808345ba4e460332cb05981a42a0d8fbc4d90"
Found by <0.6429.0>
```

Trying with 8 zeroes (No coins found after half an hour):

```
PS C:\Users\Aadi\Desktop\Final Project\COP5615-Bitcoin_Project> erl -name anolserver@10.20.226.59 -setcookie anol
Eshell V13.0.4  (abort with ^G)
(anolserver@10.20.226.59)1> bc_server:start(8,10000).
Number of Zeroes : 8 || String representation of zeroes "00000000"
```

Max number of Systems Used for Mining

For testing, five systems were used as different clients but the program would work with

more.