COP5615 Bitcoin Mining Project

Team Members

- Rishabh Srivastav : UFID 7659-9488
- Ashish Sunny Abraham : UFID 6388-7782

Outline of the project

Using Erlang's Actor Model, we've created a simulation of bitcoin mining. To mine bitcoins with the required exact number of leading zeros, we employed the SHA256 algorithm. In addition, we've put in place IP address-based remote configuration between client and server devices.

Commands to run the program

- To run Server(server.erl) instance: ‘*erl -name server@{ipAddress} -setcookie {cookieName}*’
    - e.g.: ‘*erl -name server@10.20.170.60 -setcookie project’*
    - Compile server.erl using c(server). This compiles the server side implementation of the code.
    - Compile client.erl using c(client). This compiles the client side implementation of the code for distributed modeling.
    - Once you have entered the erl shell, to start the server: ‘*server:start().*’
        - Next ‘*Enter number of 0s to mine for bitcoin :* ’
        - Next ‘*Enter number of coins to mine :* ’
        - Next ‘*Enter number of workers to spawn :* ’
    - Server can mine coins without any active client nodes

- **Distributed Implementation of the Project:**
  Start the server using the above steps, then create client nodes.
  To create Client(client.erl) node: ‘*erl -name {clientName}@{ipAddress} -setcookie {cookieName}*’
    - e.g.: ‘*erl -name client@10.20.170.60 -setcookie project’*
    - To test the distributed implementation, enter 0 in Number of workers to spawn on the server side since we don’t want the server to mine coins by itself and want the client to mine.
    - Once you have entered the erl shell, to start the client: ‘*client:start(“{ip_address_of_server}”).*’
        - e.g.: *client:start(“10.20.170.60”).*

Implementation Details

File structure:

- **Server.erl**
  The server.erl is started with the number of leading zeros (Z_count), number of coins to mine (Max_Coins_Count) and the number of workers on each system (Miner_count). The server spawns workers (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. 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. The workers are designed to continue mining until the server finds the total number of coins given by the user.

- **Client.erl**
  Client takes in the server IP address as the argument and a connection is established with the server after which actors on the client side begin mining for coins.

Program Workflow:

- The server will take input from the user regarding the number of zeroes to classify a coin as a bitcoin, number of coins that the user wants to mine and the number of worker nodes that the user wants to spawn.

- The server spawns workers/actors depending on the input given by the user using the spawn_many() function. The workers spawned on the server begin to mine bitcoins.

- If a worker process shuts down, the work assigned to it will be delegated by the server to some other remote worker active at that time.

- The server will start generating random strings that will append to "rishabhsrivastav;" and the workers will start mining the bitcoins using start_mining() function. If the worker finds a bitcoin, it sends a message to the server informing it found one and the server then prints the bitcoin.

- The distributed implementation can be executed by creating client nodes using steps mentioned above. Enter the number of workers to spawn as 0 as now we'll set up individual client nodes by following steps mentioned above. Once a node is created and you're inside the shell, type ***client:start("<ipAddress>").*** and the client then informs the server that the connection has been established and starts to mine coins.

Work Unit:

Every actor is tasked with generating a random string, computing the hash, and mining for bitcoins. Each actor runs until the leading zero condition is satisfied and the generated hash is verified. Upon finding the number of coins given by the user, 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. Thus, the actor now takes all the responsibility and the server only tells the 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 5 digit numerical(10,000)*. We specifically chose this work unit because

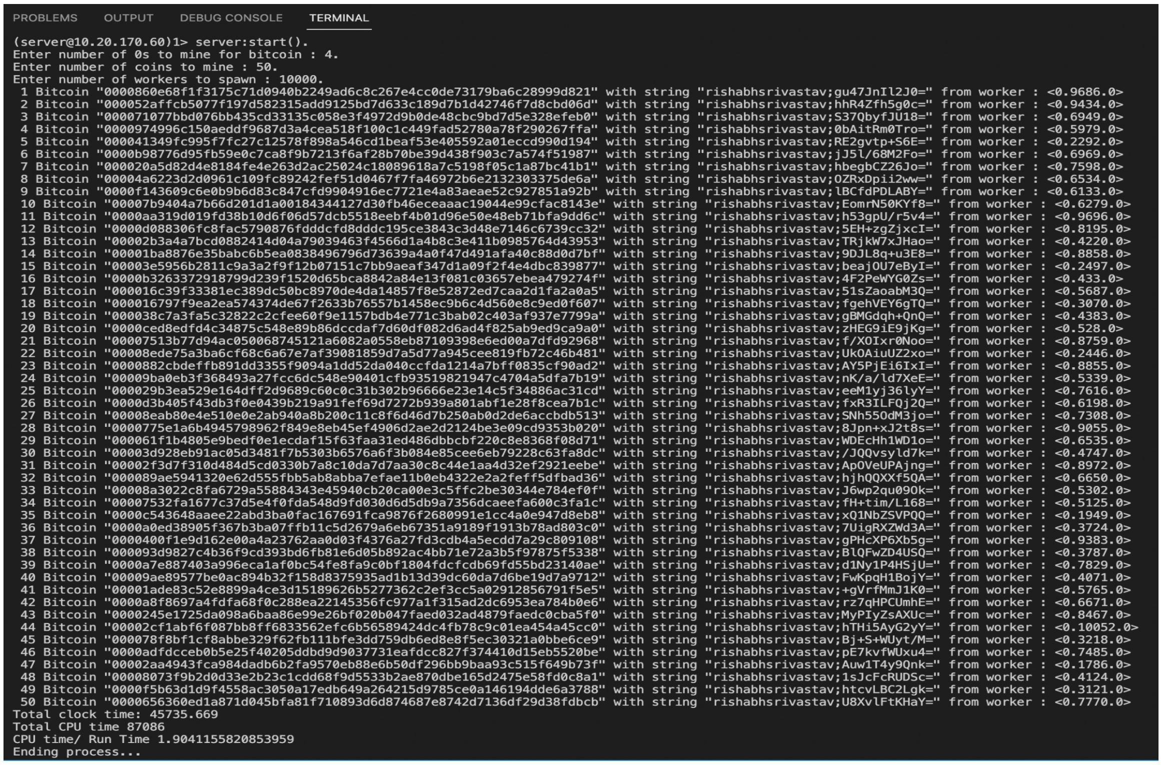
I. This will avoid the possibility of repeated generation of the same string across the workers and limit it to the first n number of miners required by the user.

II. This approach is scalable as different workers get different amounts of workload.

We have defined the ideal 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.

The result of running the program for input 4

We ran our program for *4 leading zeroes*, trying to find *50 bitcoins* and spawned *10,000 actors* receiving the following metrics :



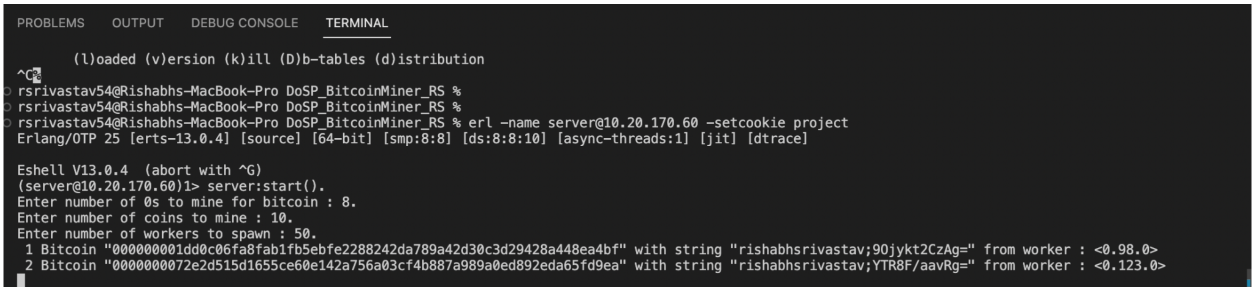
```
(server@10.20.170.60)1> server:start().
Enter number of 0s to mine for bitcoin : 4.
Enter number of coins to mine : 50.
Enter number of workers to spawn : 10000.
 1 Bitcoin "0000860e68f1f3175c71d0940b2249ad6c8c267e4cc0de73179ba6c28999d821" with string "rishabhsrivastav;gu47JnIl2J0=" from worker : <0.9686.0>
 2 Bitcoin "000052affcb5077f197d582315add9125bd7d633c189d7b1d42746f7d8cbd06d" with string "rishabhsrivastav;hhR4Zfh5g0c=" from worker : <0.9434.0>
 3 Bitcoin "000071077bbd076bb435cd33135c058e3f4972d9b0de48cbc9bd7d5e328efeb0" with string "rishabhsrivastav;S37QbyfJU18=" from worker : <0.6949.0>
 4 Bitcoin "0000974996c150aeddf9687d3a4cea518f100c1c449fad52780a78f290267ffa" with string "rishabhsrivastav;0bAitRm0Tro=" from worker : <0.5979.0>
 5 Bitcoin "000041349fc995f7fc27c12578f898a546cd1beaf53e405592a01eccd990d194" with string "rishabhsrivastav;RE2gvtp+S6E=" from worker : <0.2292.0>
 6 Bitcoin "0000b98776d95fb59e0c7ca8f9b7213f6af28b70be39d438f903c7a574f51987" with string "rishabhsrivastav;jJ5l/68M2Fo=" from worker : <0.6969.0>
 7 Bitcoin "000020a5d82d4e8184fe4e263d2ac25024c18089618a7c5198f05c1a87bc41b1" with string "rishabhsrivastav;hbegbCZ26Jo=" from worker : <0.7598.0>
 8 Bitcoin "00004a6223d2d0961c109fc89242fef51d0467f7fa46972b6e2132303375de6a" with string "rishabhsrivastav;OZRxDpii2ww=" from worker : <0.6534.0>
 9 Bitcoin "0000f143609c6e0b9b6d83c847cfd9904916ec7721e4a83aeae52c927851a92b" with string "rishabhsrivastav;lBCfdPDLABY=" from worker : <0.6133.0>
 10 Bitcoin "00007b9404a7b66d201d1a00184344127d30fb46eceaaac19044e99cfac8143e" with string "rishabhsrivastav;EomrN50KYf8=" from worker : <0.6279.0>
 11 Bitcoin "0000aa319d019fd38b10d6f06d57dcb5518eebf4b01d96e50e48eb71bfa9dd6c" with string "rishabhsrivastav;h53gpU/r5v4=" from worker : <0.9696.0>
 12 Bitcoin "0000d088306fc8fac5790876fdddcfd8dddc195ce3843c3d48e7146c6739cc32" with string "rishabhsrivastav;5EH+zgZjxcI=" from worker : <0.8195.0>
 13 Bitcoin "00002b3a4a7bcd0882414d04a79039463f4566d1a4b8c3e411b0985764d43953" with string "rishabhsrivastav;TRjkW7xJHao=" from worker : <0.4220.0>
 14 Bitcoin "00001ba8876e35babc6b5ea0838496796d73639a4a0f47d491afa40c88d0d7bf" with string "rishabhsrivastav;9DJL8q+u3E8=" from worker : <0.8858.0>
 15 Bitcoin "00003e5956b2811c9a3a2f9f12b07151c7bb9aeaf347d1a09f2f4e4dbc839877" with string "rishabhsrivastav;beajOU7eByI=" from worker : <0.2497.0>
 16 Bitcoin "0000b3263372918799d239f1520d65bca8842a84e13f081c03657ebea479274f" with string "rishabhsrivastav;4F2PeWYG0Zs=" from worker : <0.433.0>
 17 Bitcoin "000016c39f33381ec389dc50bc8970de4da14857f8e52872ed7caa2d1fa2a0a5" with string "rishabhsrivastav;51sZaoabM3Q=" from worker : <0.5687.0>
 18 Bitcoin "000016797f9ea2ea574374de67f2633b76557b1458ec9b6c4d560e8c9ed0f607" with string "rishabhsrivastav;fgehVEY6gTQ=" from worker : <0.3070.0>
 19 Bitcoin "000038c7a3fa5c32822c2cfee60f9e1157bdb4e771c3bab02c403af937e7799a" with string "rishabhsrivastav;gBMGdqh+QnQ=" from worker : <0.4383.0>
 20 Bitcoin "0000ced8edfd4c34875c548e89b86dccdaf7d60df082d6ad4f825ab9ed9ca9a0" with string "rishabhsrivastav;zHEG9iE9jKg=" from worker : <0.528.0>
 21 Bitcoin "00007513b77d94ac050068745121a6082a0558eb87109398e6ed00a7dfd92968" with string "rishabhsrivastav;f/XOIxr0Noo=" from worker : <0.8759.0>
 22 Bitcoin "00008ede75a3ba6cf68c6a67e7af39081859d7a5d77a945cee819fb72c46b481" with string "rishabhsrivastav;UkOAiuUZ2xo=" from worker : <0.2446.0>
 23 Bitcoin "0000882cbdeffb891dd3355f9094a1dd52da040ccfda1214a7bff0835cf90ad2" with string "rishabhsrivastav;AY5PjEi6IxI=" from worker : <0.8855.0>
 24 Bitcoin "00009ba0eb3f368493a27fcc6dc548e90401cfb93519821947c4704a5dfa7b19" with string "rishabhsrivastav;nK/a/ld7XeE=" from worker : <0.5339.0>
 25 Bitcoin "000029b3ea529e164dff2d9689c60c0c31b302b96666e23e14c5f34886ac31cd" with string "rishabhsrivastav;eeM1yj36lyY=" from worker : <0.7616.0>
 26 Bitcoin "0000d3b405f43db3f0e0439b219a91fef69d7272b939a801abf1e28f8cea7b1c" with string "rishabhsrivastav;fxR3ILFQj2Q=" from worker : <0.6198.0>
 27 Bitcoin "00008eab80e4e510e0e2ab940a8b200c11c8f6d46d7b250ab0d2de6accbdb513" with string "rishabhsrivastav;SNh55OdM3jo=" from worker : <0.7308.0>
 28 Bitcoin "0000775e1a6b4945798962f849e8eb45ef4906d2ae2d2124be3e09cd9353b020" with string "rishabhsrivastav;8Jpn+xJ2t8s=" from worker : <0.9055.0>
 29 Bitcoin "000061f1b4805e9bedf0e1ecdaf15f63faa31ed486dbbcbf220c8e8368f08d71" with string "rishabhsrivastav;WDEcHh1WD1o=" from worker : <0.6535.0>
 30 Bitcoin "00003d928eb91ac05d3481f7b5303b6576a6f3b084e85cee6eb79228c63fa8dc" with string "rishabhsrivastav;/JQQvsyld7k=" from worker : <0.4747.0>
 31 Bitcoin "00002f3d7f310d484d5cd0330b7a8c10da7d7aa30c8c44e1aa4d32ef2921eebe" with string "rishabhsrivastav;ApOVeUPAjng=" from worker : <0.8972.0>
 32 Bitcoin "000089ae5941320e62d555fbb5ab8abba7efae11b0eb4322e2a2feff5dfbad36" with string "rishabhsrivastav;hjhQQXXf5QA=" from worker : <0.6650.0>
 33 Bitcoin "00008a3022c8fa6729a55884343e45940cb20ca00e3c5ffc2be30344e784ef0f" with string "rishabhsrivastav;J6wp2qu09Ok=" from worker : <0.5302.0>
 34 Bitcoin "00007532fa1677c37d5e4f0fda548d9fd030d6d5db9a7356dcaeefa600c3fa1c" with string "rishabhsrivastav;fH+tim/L168=" from worker : <0.5125.0>
 35 Bitcoin "0000c543648aaee22abd3ba0fac167691fca9876f2680991e1cc4a0e947d8eb8" with string "rishabhsrivastav;xQ1NbZSVPQQ=" from worker : <0.1949.0>
 36 Bitcoin "0000a0ed38905f367b3ba07ffb11c5d2679a6eb67351a9189f1913b78ad803c0" with string "rishabhsrivastav;7UigRXZWd3A=" from worker : <0.3724.0>
 37 Bitcoin "0000400f1e9d162e00a4a23762aa0d03f4376a27fd3cdb4a5ecdd7a29c809108" with string "rishabhsrivastav;gPHcXP6Xb5g=" from worker : <0.9383.0>
 38 Bitcoin "000093d9827c4b36f9cd393bd6fb81e6d05b892ac4bb71e72a3b5f97875f5338" with string "rishabhsrivastav;BlQFwZD4USQ=" from worker : <0.3787.0>
 39 Bitcoin "0000a7e887403a996eca1af0bc54fe8fa9c0bf1804fdcfcdb69fd55bd23140ae" with string "rishabhsrivastav;d1Ny1P4HSjU=" from worker : <0.7829.0>
 40 Bitcoin "00009ae89577be0ac894b32f158d8375935ad1b13d39dc60da7d6be19d7a9712" with string "rishabhsrivastav;FwKpqH1BojY=" from worker : <0.4071.0>
 41 Bitcoin "00001ade83c52e8899a4ce3d15189626b5277362c2ef3cc5a02912856791f5e5" with string "rishabhsrivastav;+gVrfMmJ1K0=" from worker : <0.5765.0>
 42 Bitcoin "0000a8f8697a4fdfa68f0c288ea22145356fc977a1f315ad2dc6953ea784b0e6" with string "rishabhsrivastav;rz7qHPCUmhE=" from worker : <0.6671.0>
 43 Bitcoin "0000245e1725da098a6baa86e99e26bf020b047faed032ad4879faedc0cba5f0" with string "rishabhsrivastav;MyPIyZsAXUc=" from worker : <0.8467.0>
 44 Bitcoin "00002cf1abf6f087bb8ff6833562efc6b56589424dc4fb78c9c01ea454a45cc0" with string "rishabhsrivastav;hTHi5AyG2yY=" from worker : <0.10052.0>
 45 Bitcoin "000078f8bf1cf8abbe329f62fb111bfe3dd759db6ed8e8f5ec30321a0bbe6ce9" with string "rishabhsrivastav;Bj+S+WUyt/M=" from worker : <0.3218.0>
 46 Bitcoin "0000adfdcceb0b5e25f40205ddbd9d9037731eafdcc827f374410d15eb5520be" with string "rishabhsrivastav;pE7kvfWUxu4=" from worker : <0.7485.0>
 47 Bitcoin "00002aa4943fca984dadb6b2fa9570eb88e6b50df296bb9baa93c515f649b73f" with string "rishabhsrivastav;Auw1T4y9Qnk=" from worker : <0.1786.0>
 48 Bitcoin "00008073f9b2d0d33e2b23c1cdd68f9d5533b2ae870dbe165d2475e58fd0c8a1" with string "rishabhsrivastav;1sJcFcRUDSc=" from worker : <0.4124.0>
 49 Bitcoin "0000f5b63d1d9f4558ac3050a17edb649a264215d9785ce0a146194dde6a3788" with string "rishabhsrivastav;htcvLBC2Lgk=" from worker : <0.3121.0>
 50 Bitcoin "0000656360ed1a871d045bfa81f710893d6d874687e8742d7136df29d38fdbcb" with string "rishabhsrivastav;U8XvlFtKHaY=" from worker : <0.7770.0>
Total clock time: 45735.669
Total CPU time 87086
CPU time/ Run Time 1.9041155820853959
Ending process...
```

The ratio of CPU time to REAL time for the program

Total clock time: 97475.792 ms
Total CPU time: 185577 ms
CPU Utilization: CPU time/ Run Time 1.9038265418761613

The coin with the most 0s mined by our program.

We mined coins with *8 leading zeroes* resulting in *2 coins* within *~5 hours*. We executed this on a Macbook Pro with M1 pro chip with configurations: 10-core CPU and 14-core GPU.



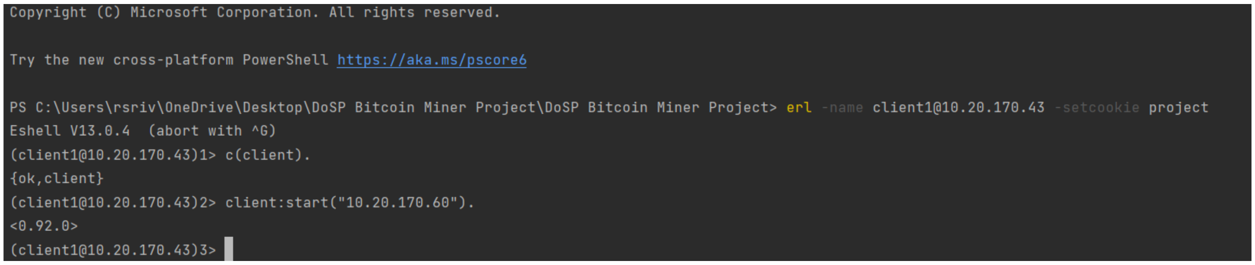
```
      (l)oaded (v)ersion (k)ill (D)b-tables (d)istribution
^C%
rsrivastav54@Rishabhs-MacBook-Pro DoSP_BitcoinMiner_RS %
rsrivastav54@Rishabhs-MacBook-Pro DoSP_BitcoinMiner_RS %
rsrivastav54@Rishabhs-MacBook-Pro DoSP_BitcoinMiner_RS % erl -name server@10.20.170.60 -setcookie project
Erlang/OTP 25 [erts-13.0.4] [source] [64-bit] [smp:8:8] [ds:8:8:10] [async-threads:1] [jit] [dtrace]

Eshell V13.0.4  (abort with ^G)
(server@10.20.170.60)1> server:start().
Enter number of 0s to mine for bitcoin : 8.
Enter number of coins to mine : 10.
Enter number of workers to spawn : 50.
 1 Bitcoin "000000001dd0c06fa8fab1fb5ebfe2288242da789a42d30c3d29428a448ea4bf" with string "rishabhsrivastav;9Ojykt2CzAg=" from worker : <0.98.0>
 2 Bitcoin "0000000072e2d515d1655ce60e142a756a03cf4b887a989a0ed892eda65fd9ea" with string "rishabhsrivastav;YTR8F/aavRg=" from worker : <0.123.0>
```

The largest number of working machines we were able to run our code with.

We were able to run our code on *3 different systems* and they all were able to mine bitcoins simultaneously. This can also be scaled up to multiple different machines.
The client id of the 3 machines are:

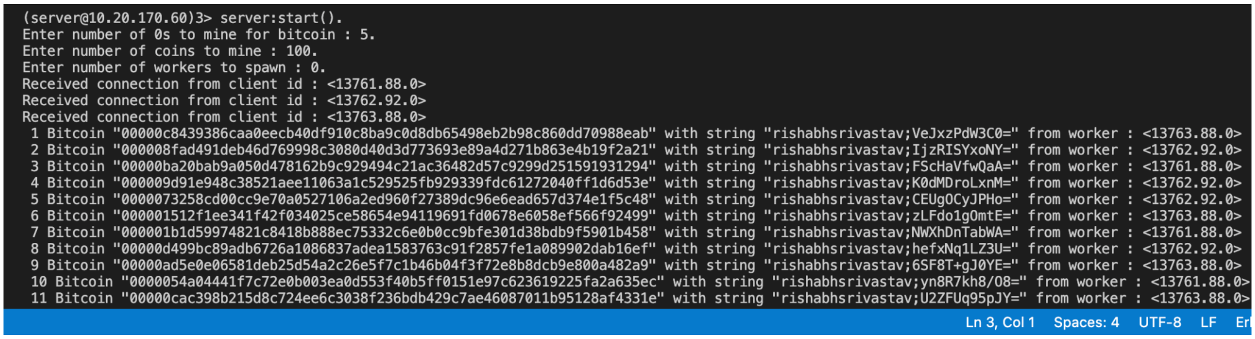
1. **<13761.88.0>**
2. **<13762.92.0>**
3. **<13763.88.0>**



```
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\rsriv\OneDrive\Desktop\DoSP Bitcoin Miner Project\DoSP Bitcoin Miner Project> erl -name client1@10.20.170.43 -setcookie project
Eshell V13.0.4  (abort with ^G)
(client1@10.20.170.43)1> c(client).
{ok,client}
(client1@10.20.170.43)2> client:start("10.20.170.60").
<0.92.0>
(client1@10.20.170.43)3>
```



```
(server@10.20.170.60)3> server:start().
Enter number of 0s to mine for bitcoin : 5.
Enter number of coins to mine : 100.
Enter number of workers to spawn : 0.
Received connection from client id : <13761.88.0>
Received connection from client id : <13762.92.0>
Received connection from client id : <13763.88.0>
 1 Bitcoin "00000c8439386caa0eecb40df910c8ba9c0d8db65498eb2b98c860dd70988eab" with string "rishabhsrivastav;VeJxzPdW3C0=" from worker : <13763.88.0>
 2 Bitcoin "000008fad491deb46d769998c3080d40d3d773693e89a4d271b863e4b19f2a21" with string "rishabhsrivastav;IjzRISYxoNY=" from worker : <13762.92.0>
 3 Bitcoin "00000ba20bab9a050d478162b9c929494c21ac36482d57c9299d251591931294" with string "rishabhsrivastav;FScHaVfwQaA=" from worker : <13761.88.0>
 4 Bitcoin "000009d91e948c38521aee11063a1c529525fb929339fdc61272040ff1d6d53e" with string "rishabhsrivastav;K0dMDroLxnM=" from worker : <13762.92.0>
 5 Bitcoin "0000073258cd00cc9e70a0527106a2ed960f27389dc96e6ead657d374e1f5c48" with string "rishabhsrivastav;CEUgOCyJPHo=" from worker : <13762.92.0>
 6 Bitcoin "000001512f1ee341f42f034025ce58654e94119691fd0678e6058ef566f92499" with string "rishabhsrivastav;zLFdo1gOmtE=" from worker : <13763.88.0>
 7 Bitcoin "000001b1d59974821c8418b888ec75332c6e0b0cc9bfe301d38bdb9f5901b458" with string "rishabhsrivastav;NWXhDnTabWA=" from worker : <13761.88.0>
 8 Bitcoin "00000d499bc89adb6726a1086837adea1583763c91f2857fe1a089902dab16ef" with string "rishabhsrivastav;hefxNq1LZ3U=" from worker : <13762.92.0>
 9 Bitcoin "00000ad5e0e06581deb25d54a2c26e5f7c1b46b04f3f72e8b8dcb9e800a482a9" with string "rishabhsrivastav;6SF8T+gJ0YE=" from worker : <13763.88.0>
 10 Bitcoin "0000054a04441f7c72e0b003ea0d553f40b5ff0151e97c623619225fa2a635ec" with string "rishabhsrivastav;yn8R7kh8/O8=" from worker : <13761.88.0>
 11 Bitcoin "00000cac398b215d8c724ee6c3038f236bdb429c7ae46087011b95128af4331e" with string "rishabhsrivastav;U2ZFUq95pJY=" from worker : <13763.88.0>
```