Distributed Operation System

Report
Bitcoin Implementation in Elixir (Web UI in Phoenix)
Project 4.2

Submitted By:
Akshay Sehgal (UFID: 14167988)
Aswin Suresh Krishnan (UFID: 18901173)

Table of Contents

Introduction

This project report is in continuation to our initial project which was implemented to build a Bitcoin framework in Elixir. In this project we have tried to implement the UI part and made some changes to let users control the processes from the FE. This report will take you through the steps that would help you to understand the phoenix implementation in detail. At the end we have provided a You tube link for the demo and the summary of our design and architecture.

How to run

Initially you have to set up Phoenix and you can refer the online documentation for the same.

Once done just run the below command to set the server running.

- mix phx.server

Let the program run in the command line and initially it would set up a fix number of users and miners in the application and the following message will appear in your console: “All nodes have started.”.

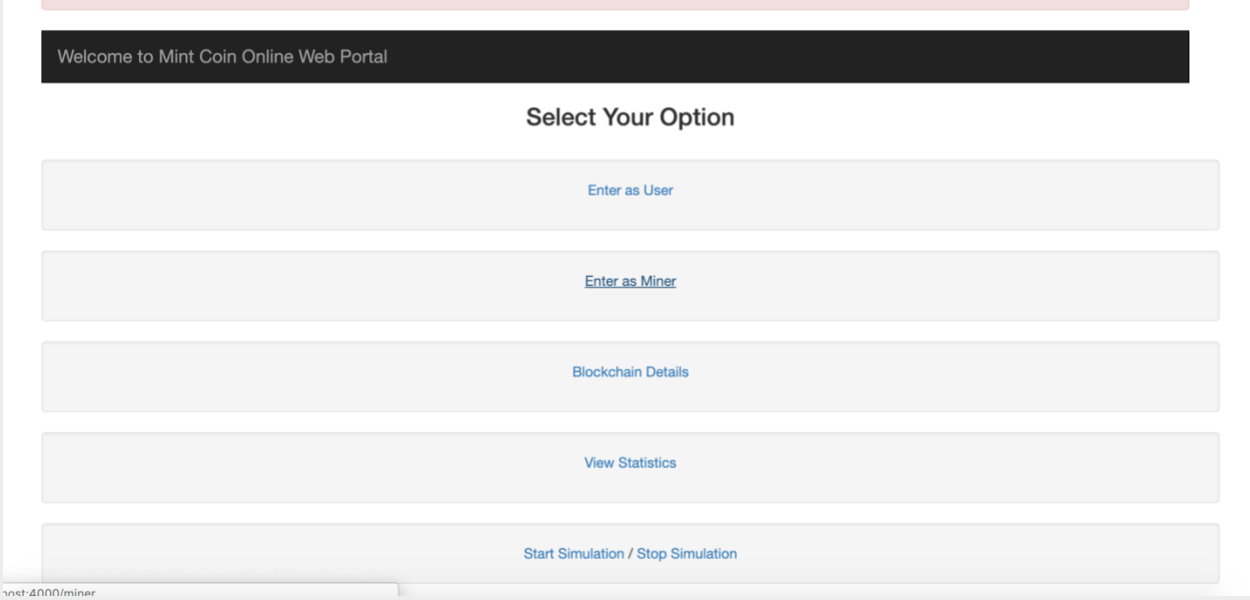
Once the above mentioned message appears, the application is up and running with the fixed number of nodes.

After this, Enter the following URL in your browser : http://localhost:4000

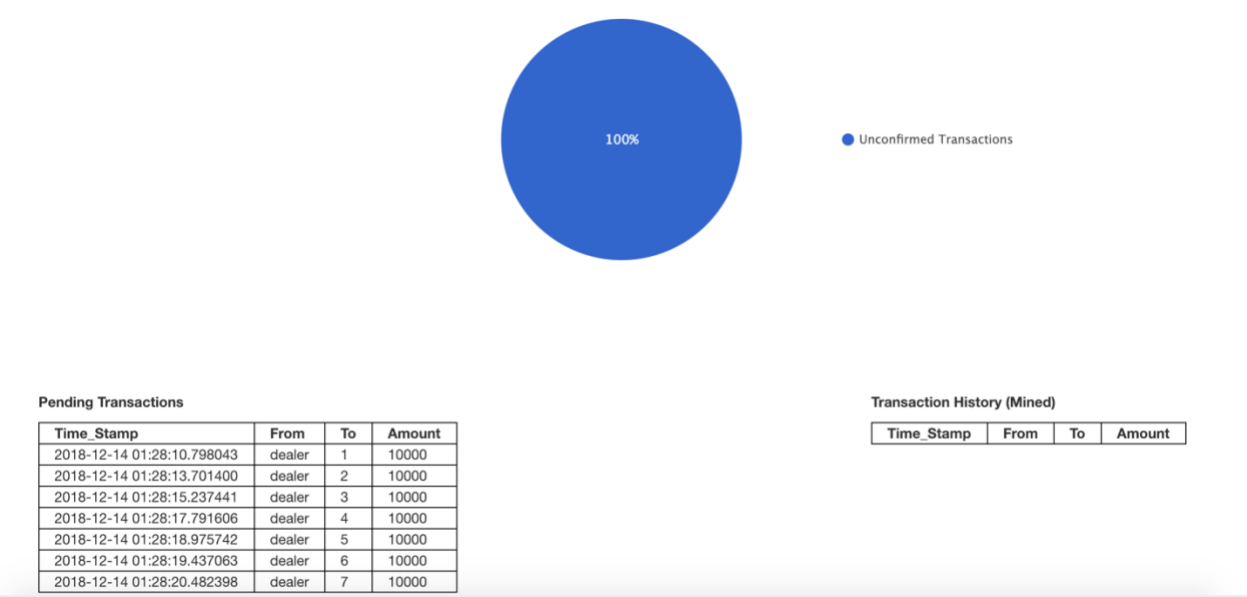
Landing Page

As the application starts, you will land on the following landing page.

First Half:



Scroll Down for the second Half:

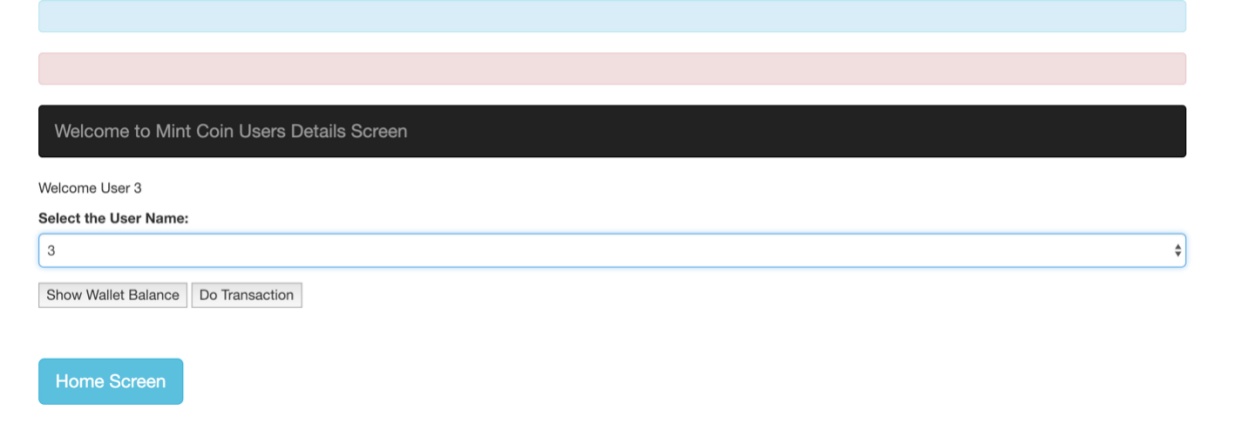


The first half of the screen lets you select among the following options:

- Login as the user
- Login as the miner
- See Blockchain Details
- View statistics
- Start and Stop Simulation

Enter as User

User Screen

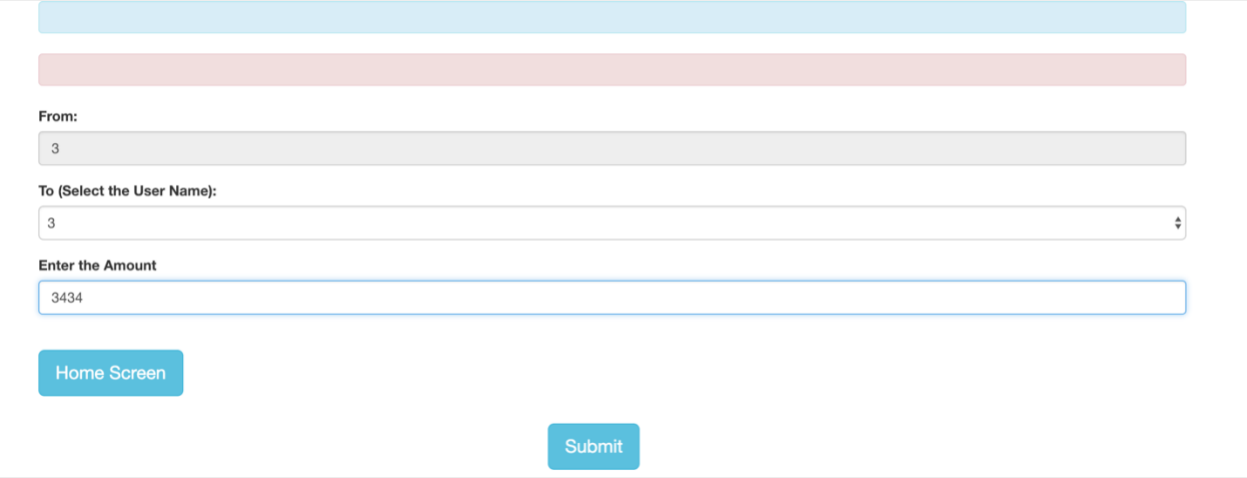


When you select the user it allows you to perform the following actions:

- See the Wallet Balance
- Do Transaction

The wallet balance screen displays the present balance of the user and is relatively simple to explain. I would devote my time and space to explain the do transaction process which is fairly interesting.

Do Transaction



The from fields is non-editable and the user selects the “TO” from the drop down. Once the user submits the transaction, it goes into the pool of pending transactions and can be seen in the second half of the “Landing Screen”.

Pending Transactions

Time_Stamp	From	To	Amount
2018-12-14 01:28:10.798043	dealer	1	10000
2018-12-14 01:28:13.701400	dealer	2	10000
2018-12-14 01:28:15.237441	dealer	3	10000
2018-12-14 01:28:17.791606	dealer	4	10000
2018-12-14 01:28:18.975742	dealer	5	10000
2018-12-14 01:28:19.437063	dealer	6	10000
2018-12-14 01:28:20.482398	dealer	7	10000
2018-12-14 01:41:42.777638	3	3	3434

Transaction History (Mined)

Time_Stamp	From	To	Amount

The transaction in the upper section of the table are the **genesis transactions**, in order to set up the system.

The recent transaction is displayed at **the bottom**. This all stands in pending transaction because the mining has not yet started.

In order to start the mining, the user has to login as the miner and start the mining process.

After the start of the mining process and refreshing the “Landing Screen”, which will be explained in the next section, the following results are obtained.

Pending Transactions

Time_Stamp	From	To	Amount

Transaction History (Mined)

Time_Stamp	From	To	Amount
2018-12-14 01:28:10.798043	dealer	1	10000
2018-12-14 01:28:13.701400	dealer	2	10000
2018-12-14 01:28:15.237441	dealer	3	10000
2018-12-14 01:28:17.791606	dealer	4	10000
2018-12-14 01:28:18.975742	dealer	5	10000
2018-12-14 01:28:19.437063	dealer	6	10000
2018-12-14 01:28:20.482398	dealer	7	10000
2018-12-14 01:41:42.777638	3	3	3434

Inference from the above Screenshot:
As you can see the transactions are a part of “**Mined transactions**”.

View Blockchain

This feature lets you see all the mined blocks in the application.

For the above example, we have only one block to display.

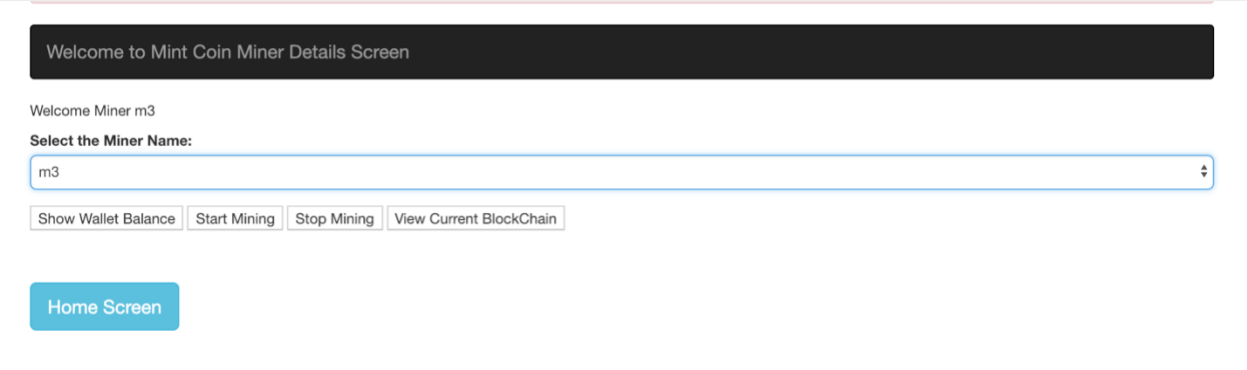
Blockchain

Index	Time_Stamp	Hash_Value	Previous_Block_Hash	Transactions	Nonce
1	2018-12-14 01:44:50.305813	00000000000000000	00000000000000000		
2	2018-12-14 01:44:52.977659	00003AD65F444367F2FB923C3492E89BED1F9523AD8F1F39E50A82967814BF96	00000000000000000	from / to / amount / Time_Stamp dealer / 1 / 10000 / 2018-12-14 01:28:10.798043 dealer / 2 / 10000 / 2018-12-14 01:28:13.701400 dealer / 3 / 10000 / 2018-12-14 01:28:15.237441 dealer / 4 / 10000 / 2018-12-14 01:28:17.791606 dealer / 5 / 10000 / 2018-12-14 01:28:18.975742 dealer / 6 / 10000 / 2018-12-14 01:28:19.437063 dealer / 7 / 10000 / 2018-12-14 01:28:20.482398 3 / 3 / 3434 / 2018-12-14 01:41:42.777638	33247

Inference from the above Screenshot:
The transactions are mined, and Block is added in the blockchain.

Enter as Miner

Miner Screen



Once you enter as the miner. You can perform the following actions:

- See Wallet Balance
- Start Mining
- Stop Mining
- View Current Blockchain

The options are a self-explanatory in terms of the what they do. You can view the video attached for better understanding.

View Statistics

This option displays a chart that shows the number of blocks mined in the given time frame.

Start/Stop Simulation

1. This is where the system performs at its full capability.
2. The above features and options let you know the system architecture and minimal functionality with respect to what they do.
3. The start simulation does the following things in the system and the results are attached with what they refer to:

Simulation has started. > Started more users to make 100 users. > Random users among 100 users will perform random transactions in interval of 30 seconds. > All the 6 miners have started mining.

The system can take some time to start the 100 users, it depends on the system.

Note: Please wait for the following message to appear in your console “All nodes have started.”.

4. Now when you refresh the “Landing Page”, you will find a whole lot of transactions in the mined transactions and the same can be observed in the “View Statistics” and “View Blockchain” functionalities.

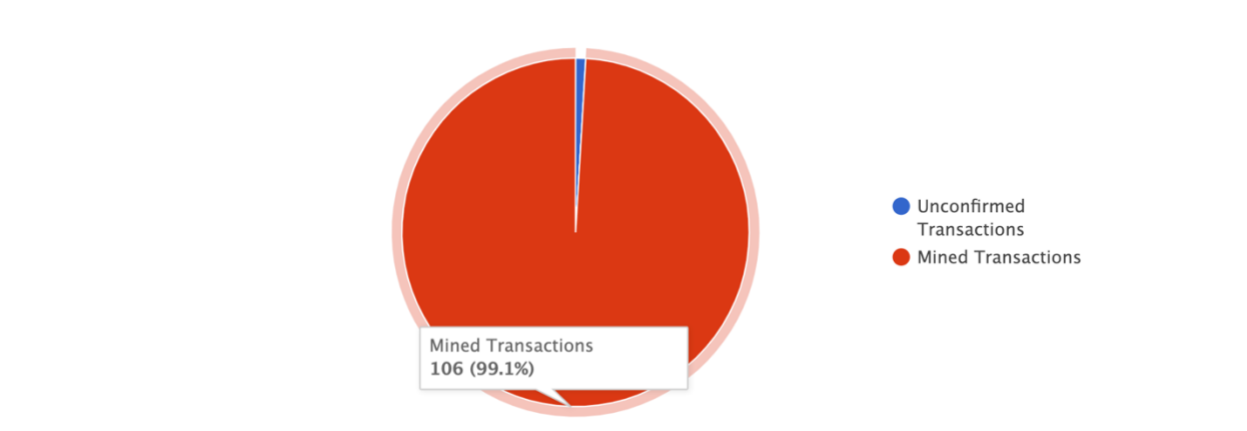
I have attached screenshots for your reference.

New Blockchain after the start of simulation.

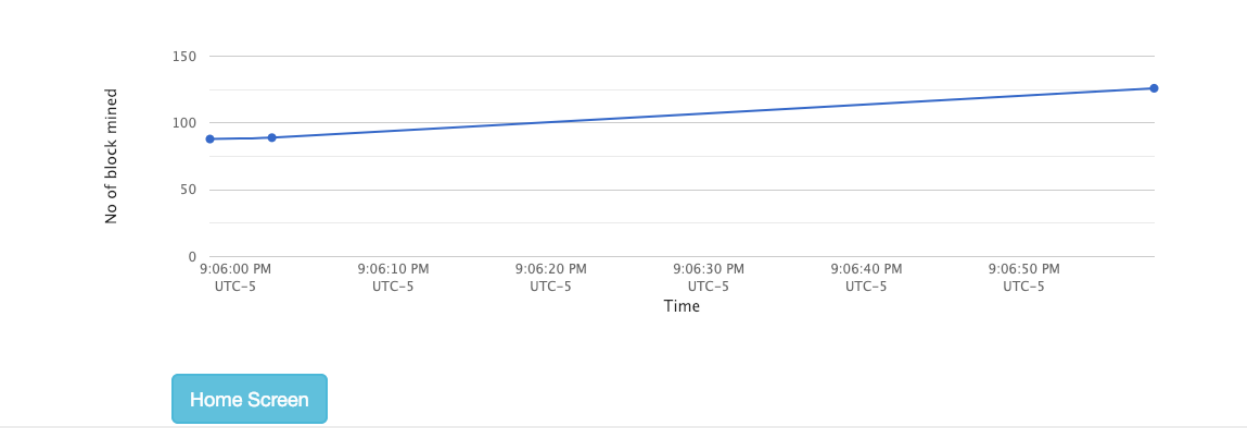
Blockchain

Index	Time_Stamp	Hash_Value	Previous_Block_Hash	Transactions	Nonce
1	2018-12-14 01:59:58.781495	00000000000000000	00000000000000000		
2	2018-12-14 02:00:00.011965	0007A9E87F5199610EFDA5E7D5D5E688541C2C05CF30354D0BFD2A1B79A791F3	00000000000000000	from: dealer, to: 1, amount: 10000, Time_Stamp: 2018-12-14 01:58:12.299453 from: dealer, to: 2, amount: 10000, Time_Stamp: 2018-12-14 01:58:13.878439 from: dealer, to: 3, amount: 10000, Time_Stamp: 2018-12-14 01:58:15.773281 from: dealer, to: 4, amount: 10000, Time_Stamp: 2018-12-14 01:58:17.273269 from: dealer, to: 5, amount: 10000, Time_Stamp: 2018-12-14 01:58:18.424286 from: dealer, to: 6, amount: 10000, Time_Stamp: 2018-12-14 01:58:19.133199 from: dealer, to: 7, amount: 10000, Time_Stamp: 2018-12-14 01:58:20.287713	24524
3	2018-12-14 02:02:21.702965	000B9D7770E9E3D9987418FBBECF722CFE32725142D4C5CE119E912B83591070	0007A9E87F5199610EFDA5E7D5D5E688541C2C05CF30354D0BFD2A1B79A791F3	from: dealer, to: 8, amount: 10000, Time_Stamp: 2018-12-14 02:02:21.488599	80534
4	2018-12-14 02:02:23.228009	00094CC91D04CCFE30EA8A04F62EA4B3A244F92507B04202B87D3603176BCC69	000B9D7770E9E3D9987418FBBECF722CFE32725142D4C5CE119E912B83591070	from: dealer, to: 9, amount: 10000, Time_Stamp: 2018-12-14 02:02:22.912822	105024
5	2018-12-14 02:02:25.275313	00025D04F8DD5AF12A417E698CF3ABA05E04F1B0532107F5E38651FBC7D25D49	00094CC91D04CCFE30EA8A04F62EA4B3A244F92507B04202B87D3603176BCC69	from: dealer, to: 10, amount: 10000, Time_Stamp: 2018-12-14 02:02:25.047511	73486
6	2018-12-14 02:02:26.694004	0006C0CB7B45D9475A1CE446FAE93C45C4ED39100B418E7E9FAF81CF54DFB3B0	00025D04F8DD5AF12A417E698CF3ABA05E04F1B0532107F5E38651FBC7D25D49	from: dealer, to: 11, amount: 10000, Time_Stamp: 2018-12-14 02:02:26.421136	104969
7	2018-12-14 02:02:30.320013	000B5C6FF8E4C263A53CAD64585868487 27FEE7892DEC6709BF79C3909464269	0006C0CB7B45D9475A1CE446FAE93C45C4ED39100B418E7E9FAF81CF54DFB3B0	from: dealer, to: 12, amount: 10000, Time_Stamp: 2018-12-14 02:02:30.268095	95366
8	2018-12-14 02:02:33.253428	0007D7AD54BEF6602F6082F65A344DA7C6A332356EB42BAD374A7535A23ED8C4	000B5C6FF8E4C263A53CAD64585868487 27FEE7892DEC6709BF79C3909464269	from: dealer, to: 13, amount: 10000, Time_Stamp: 2018-12-14 02:02:32.795813	65789
9	2018-12-14 02:02:34.677998	0000A27125760B0B9585604E3D8F9D0A0C4D11D3B008D80175B83A51C3A2266F	0007D7AD54BEF6602F6082F65A344DA7C6A332356EB42BAD374A7535A23ED8C4	from: dealer, to: 14, amount: 10000, Time_Stamp: 2018-12-14 02:02:34.429403	76421

Graph on the landing page, showing the Unconfirmed and Mined transactions:



The graph showing the number of blocks mined in the given span of time. This can be viewed from “View Statistics” option.



Bonus Implementation:

Apart from the simulation and the UI, we have implemented following functionality as the part of the bonus implementation.

1. The application provides the functionality for the user to log in as the Miners and start and stop the mining process for that particular miner at their own discretion.
2. The second functionality is to add transactions by the user apart from the one in the simulation. This is provided when you enter as the user and click on the “Do Transaction” button.

The functionality of the bonus implementation is explained in the above section and in the video link provided below:

Summary:

Program overview [for brief understanding]

We start the web application with a default of 7 miners and 7 users.

> 100 user simulation

There is an option to 'Run Simulation' which will add extra 100 users and perform transaction between the randomly selected users in interval of 30 seconds

When refreshing the home screen, we can see the amount of transactions that are mined and what are opening.

Project Description and further explanation:

The project aims to provide a User Interface for the users to perform transactions and for miners to participate in mining and earn reward as bitcoin.

The following options are provided in the User Interface -

1> Enter as User
- > View Wallet Balance
- > Perform Transaction
- > Enter target user and amount -> start transaction

2> Enter as Miner
- > View Wallet Balance
- > Start Mine
- > Stop Mine
- > View BlockChain

3> View the proportion of the mined transactions on the home screen pie chart

4> View the current status of the BlockChain on the 'View Blockchain' Screen

5> View the mining rate chart on the 'Statistics' screen

6> Unconfirmed and mined transactions are visible on the home screen on separate tables.

7> 'Run Simulation' will add 100 new users and start a simulation in which transactions occur between two randomly selected users at an interval of 30 seconds.

The users need to log in by selecting their name and perform a transaction to another user by selecting the recipient's name and amount.

The miners need to start mining in order for the unconfirmed transactions (which are stored in each miner's state) are mined to form a block and the mining algorithm comes into action (competition among miners begin) when multiple miners click on the 'Start mine' button.

Any miner can at any point stop their mining activity by clicking on the 'Stop mine' option on the miner's screen.

The above activities can be simulated by using 'Run Simulation' option on the home screen. Note: a 5 sec wait time is expected for 100 new users to be spawned by the Supervisor. However, the initiation begins as a background process and no halt is seen on the UI.

YouTube Video Link of Demo.

https://youtu.be/_A8oYoyxS_E