Project 4.2 Readme

COP5615: Distributed Operating System Principles

Teammates: Shashank Mayekar (UFID: 50059142), Tanya Pathak(UFID: 18373292)

Youtube video at:

https://youtu.be/AZLhvqB13xM

Working functionality:

4.2 specific

- Distributed protocol:
  - Network can handle 100+ nodes and as many miners
  - Distributed transaction pool for new broadcasted transactions at each node
  - 16 transactions execute (creating 16 blocks; # transactions can be increased)
- Implemented Phoenix application which runs the 4.1 code
- Created chart – Bitcoins transacted(http://localhost:4000/bitcoinBtc)
- Created chart – Hashes computed to mine (http://localhost:4000/bitcoinHash)
- Created chart – Transactions in block (http://localhost:4000/bitcoinTx)
- Created list –Transactions broadcasted (http://localhost:4000/bitcoinTxList)

4.1 specific

- Wallets (Every node is a wallet with a public-private key pair and a derivable public address.
- Genesis block mining
- Bitcoin Transactions (Starting from first miner)
- Coinbase transaction (Rewards)
- Node gets interrupted when someone else broadcasts a mined block of same height
- Unspent transaction outputs for each wallet (UTXO model)
- Change transaction as part of UTXO (in tx outputs)
- Computing balance of wallet from its UTXOs
- Multiple inputs and multiple outputs for transactions
- Digitally signing a transaction using private key
- Verifying a signed transaction using signer's public key

Steps to run the project:

The main bitcoin program initiates from within the Phoenix 'Application.ex'.

We pass 100 as the number of nodes, and 80 as number of miners among them to Btcmain GenServer.

Main components:

- node.ex corresponds to each node in the network.
- wallet.ex corresponds to the wallet of each node.
- proj42.ex is the main component program which creates nodes
- btcmain.ex invokes proj42.ex, executes transactions, and monitors the network

To compile the project, do:

- cd into project directory (bitcoin1)
- **`>> mix compile`**

`Open 4 pages on the browser:`

http://localhost:4000/bitcoinBtc
http://localhost:4000/bitcoinHash
http://localhost:4000/bitcoinTx
http://localhost:4000/bitcoinTxList

To run the Application:

`>> mix phx.server`

The program will begin running.

The 4 pages will keep updating (Need to refresh if they don't)

The program output is also visible in the cmd (information on blocks, transactions and balances of nodes involved in transactions).

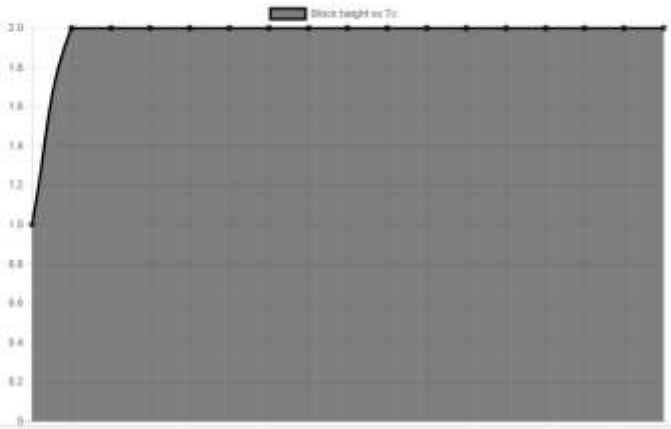
Around 16 blocks will be mined.

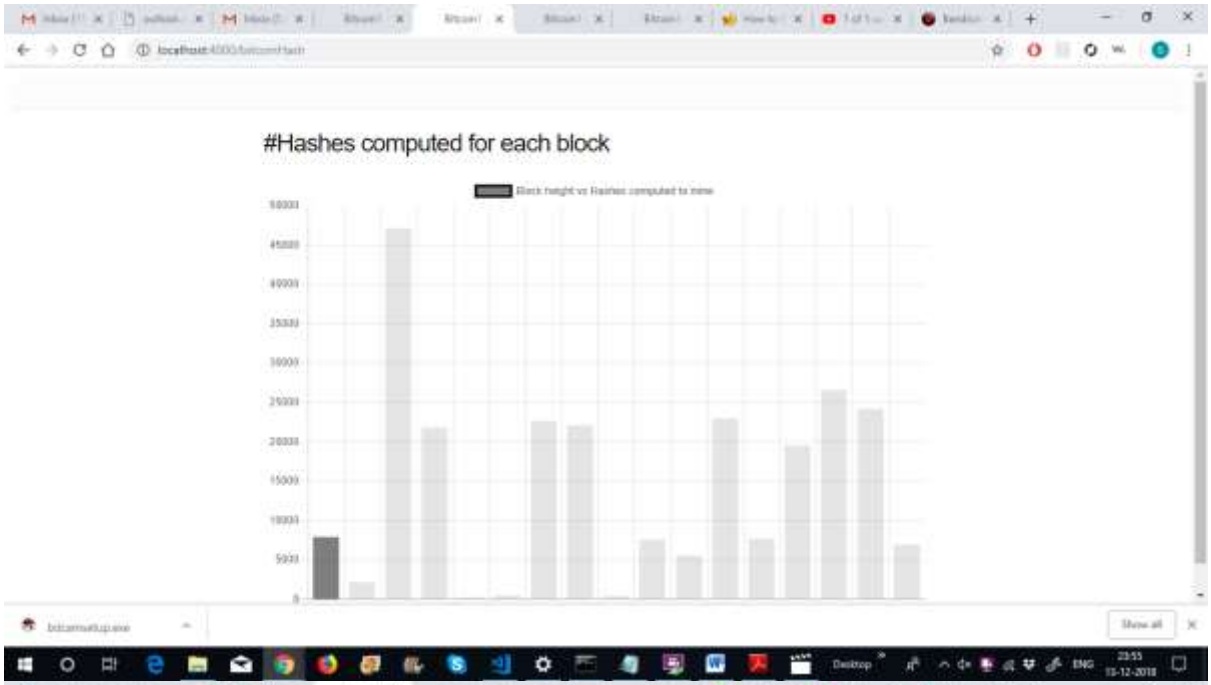
SCREENSHOTS INCLUDED ON NEXT PAGE

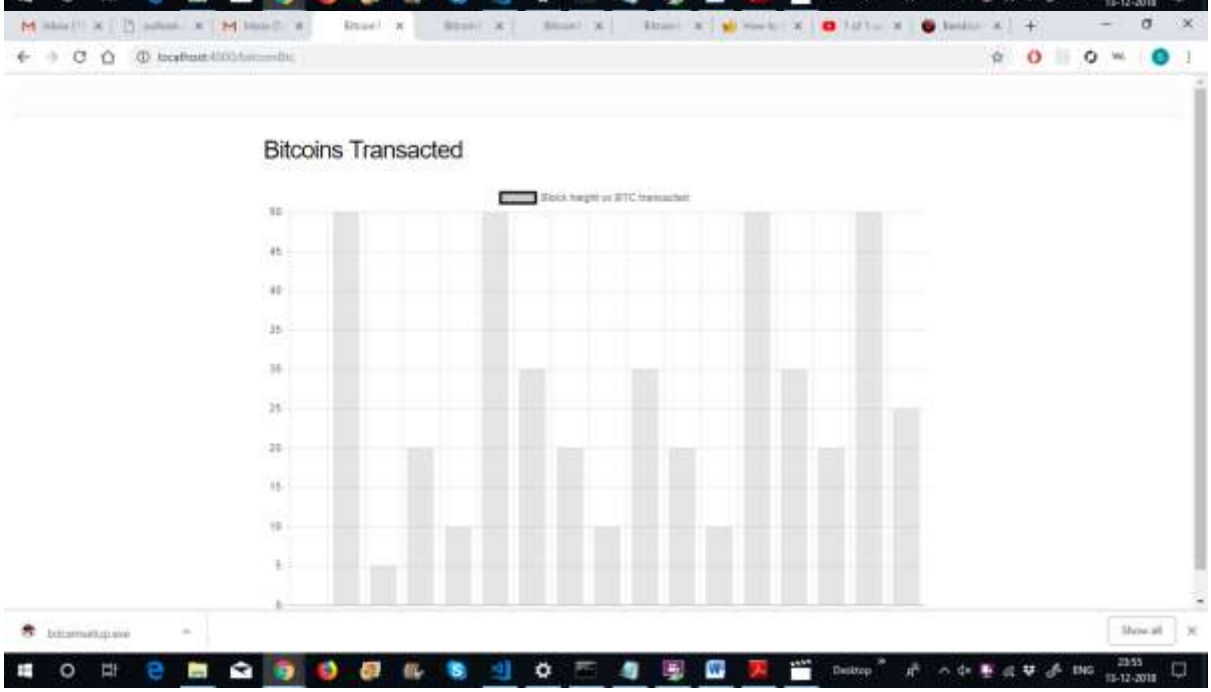
Transactions broadcasted

Tx -> DB2AE03D6F80DB152BCB74924518AA6A951BB9A3 sent 20 BTC to 5A6C65F756A48CCEB2AC6F51C590D95AFB51377D
Tx -> DB2AE03D6F80DB152BCB74924518AA6A951BB9A3 sent 5 BTC to F766A052848E6AFEDD00C4669CC9F8BA128FAFEB
Tx -> 5A6C65F756A48CCEB2AC6F51C590D95AFB51377D sent 10 BTC to 76AEA3F942B60FA37F5009BA458B9F5C80DDE3B5
Tx -> 76AEA3F942B60FA37F5009BA458B9F5C80DDE3B5 sent 8 BTC to DBA195723387331A0423A18F4F44777AC0945297
Tx -> DB2AE03D6F80DB152BCB74924518AA6A951BB9A3 sent 20 BTC to EE68993F12D6BE74810D1951745FEDDC73838629
Tx -> DB2AE03D6F80DB152BCB74924518AA6A951BB9A3 sent 5 BTC to CF2F8EDA1391A937929D61C9E8D676C6BB63E6FF
Tx -> EE68993F12D6BE74810D1951745FEDDC73838629 sent 10 BTC to 38F527FE2F465C8BDC06121934B3601B043237AE
Tx -> 38F527FE2F465C8BDC06121934B3601B043237AE sent 8 BTC to EF0C54616DF8BA81CE5EEF96856B5320A64C8F4B
Tx -> 5ABC1D94B0F5F13A3817CF67B7652B2E8C4E417F sent 20 BTC to DDB5B67F17CE62EEF43C73752672D01E0605B216

No. of transactions per block




#Hashes computed for each block


Bitcoins Transacted