bitcoin

A Peer-to-Peer Electronic Cash System

In

elixir

Project Description:

This project includes the implementation of web interface for the simulation of bitcoin protocol with features such as mining, wallets, blockchain, P2P Network, payment processing and bitcoin transaction from a sender to a receiver. For mining, a low threshold value (less than 5) for zero bits in block's hash has been set for faster mining. The program takes 100 number of participants in the bitcoin peer to peer network and number of transactions that have to be taken place among the participants in the network as the inputs from the user. The output will the transaction summaries which include sender, receiver wallet details along with the numbers of bitcoins transferred from the sender to receiver in the form of graphs in the browser.

Instructions:

Steps to compile and run the project:

- Extract the project folder from the project zip folder
- Open terminal, move to extracted project directory by executing **"cd project5"**
- Execute **"mix deps.get"** to load the dependencies.
- Execute **"mix phx.server"** to initiate the server. Copy the link: http://localhost:4000 and paste in the browser to run the project.

Bitcoin Features that have been implemented:

Wallets: Each participant in the bitcoin network will have a wallet associated with them. The wallets include public keys to send and receive bitcoins, corresponding private keys to spend those bitcoins and the number of bitcoins. Following are the operations taken care by the wallets:

- Initialize transaction: Whenever a sender sends certain number of bitcoins, sender's wallet will initiate the transaction and transfers the transaction data which consists of number of bitcoins to be transferred and the receiver's public key to the bitcoin network where the process of bitcoin mining will be taken place for generation of new blocks in the blockchain.
- Signing: Wallets also sign the transactions and broadcast the signed transactions over the peer to peer bitcoin network.
- Payment processing: Wallets will also implement payment processing feature of bitcoin protocol which will be explained later.

“wallet.ex” file in the “lib” folder of the project is associated with the wallets feature of bitcoin protocol.

Blockchain: The block chain provides Bitcoin’s public ledger, an ordered and timestamped record of transactions. It contains the new blocks that have been added by the bitcoin miners whenever a new transaction occurs. Each block in the blockchain consists of the following fields:

- Transaction data: This field contains the information about number of bitcoins to be transferred to the receiver and the receiver’s public key.
- Previous hash: Contains hash of the previous block in the blockchain.
- Hash: Contains hash of the present block in the blockchain
- Signed message: Contains the signature which depicts the sender’s ownership of the transaction
- Timestamp: Stores the date and time at which a new block has been created and added to the block.
- Sender’s public key: Contains the sender’s public key.

“block.ex” file in the “lib” folder of the project is associated with blockchain feature of bitcoin protocol.

Mining: Mining adds new blocks to the blockchain, making transaction history hard to verify. It is a process in which a miner attempts to generate a new block on his own by taking transaction data, previous hash and a nonce. The proof-of-work involves scanning for a value that when hashed using sha256, the hash begins with a certain number of zero bits. We have implemented the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits.

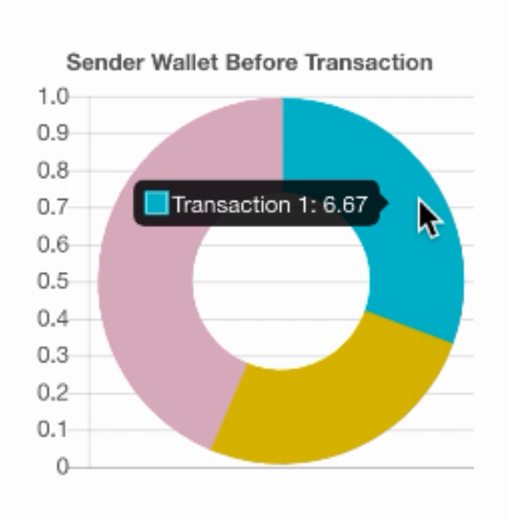
“Mining.ex” file in the “lib” folder of the project is associated with mining feature of bitcoin protocol.

Transaction: As mentioned, every participant in the bitcoin network is associated with a wallet from where a transaction gets initialized and ends until the receiver’s wallet gets updated with the bitcoins that have been transferred. We have taken a random sender and receiver from the list of participants provided as an input to implement transaction feature of bitcoin protocol.

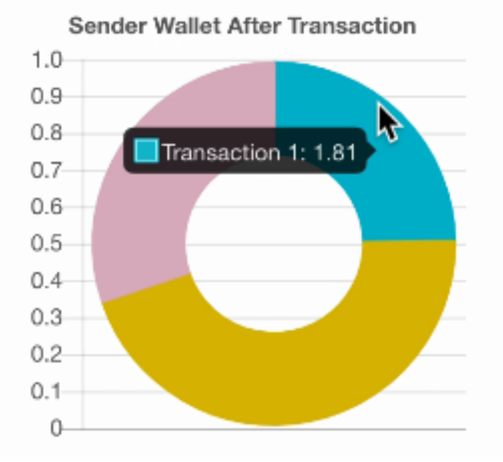
Payment Processing: Whenever a bitcoin transaction is made, all the wallets (participants) present in the bitcoin network will scan the updated block chain to check whether the payment which is being done is intended for them. When a wallet’s (participant’s) public key matches with receiver’s public key in the block and if the transaction is successful, it updates the existing bitcoins in it. This feature of bitcoin protocol is known as payment processing.

P2P Network: Whenever a new block has been added to the blockchain, all the peers in the P2P network of bitcoin protocol will verify the ownership of the new block with the help of sender's public key before making payment processing. If any of the peer declares the new block as fraud, that new block will be removed from the blockchain and payment processing will be revoked so that the transaction would be unsuccessful.

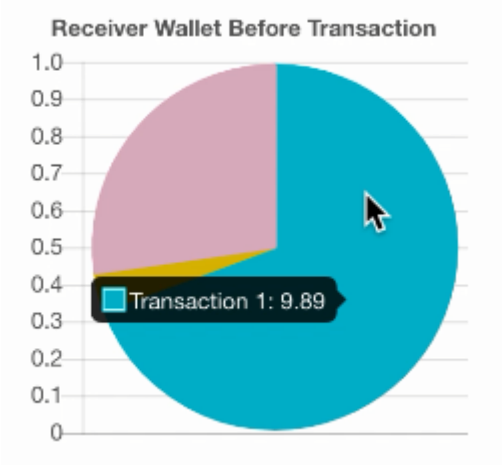
Results (graphs in the browser):



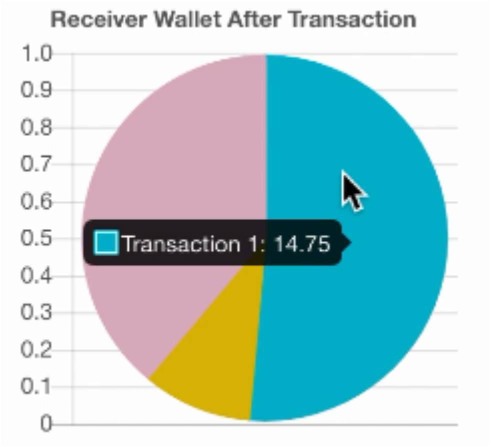
This graph gives the information about bitcoins in the sender wallet before the bitcoin transaction. For example, we conclude from the above the graph that sender wallet has 6.67 BTC before the transaction-1 occurred.



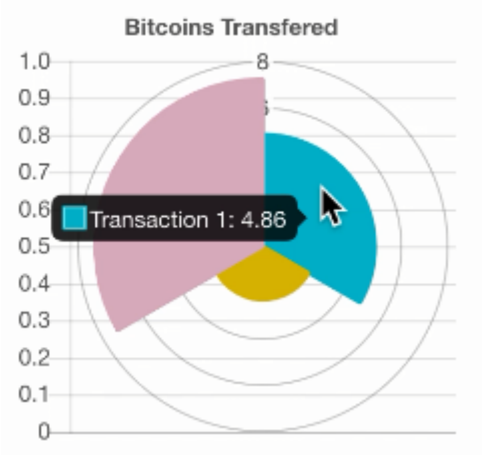
This graph gives the information about bitcoins in the sender wallet after the bitcoin transaction. For example, we conclude from the above the graph that sender wallet has 1.81 BTC before the transaction-1 occurred.



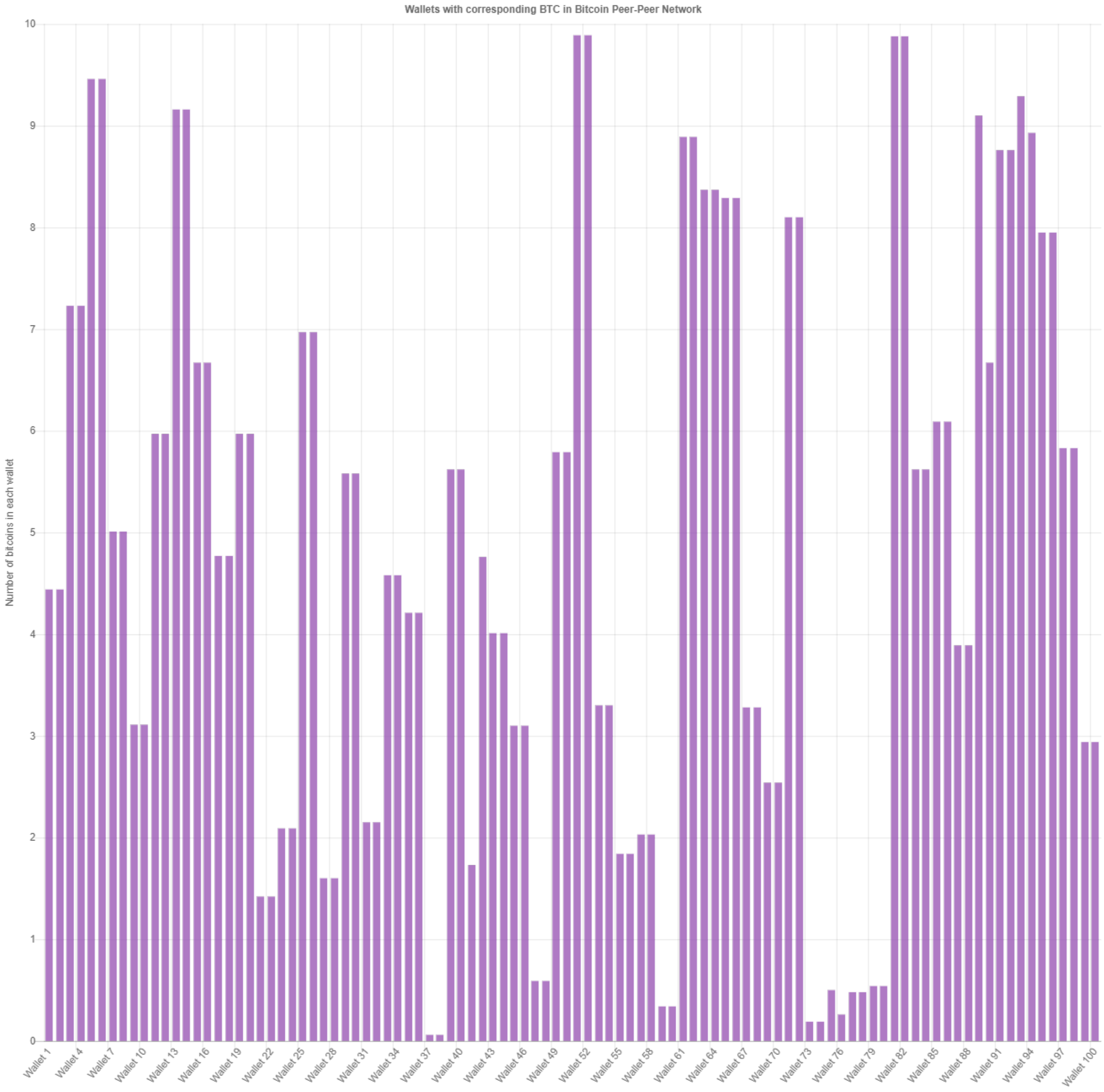
This graph gives the information about bitcoins in the receiver wallet before the bitcoin transaction. For example, we conclude from the above the graph that sender wallet has 9.89 BTC before the transaction-1 occurred.



This graph gives the information about bitcoins in the receiver wallet after the bitcoin transaction. For example, we conclude from the above the graph that sender wallet has 14.75 BTC before the transaction-1 occurred.



This graph gives the information about number of bitcoins that have been successfully transferred from a sender to receiver in a particular transaction. For example, in transaction-1, 4.86 BTC have been transferred successfully.



This graph gives the information about bitcoins in each wallet after all the transactions have been successfully completed.

Conclusion:

Web interface for the bitcoin peer-peer network protocol has been successfully implemented and tested.