Blockchain and Cryptocurrency

Assignment 5: Bitcoin Core

To help you understand what is happening in blockchain, let's use bitcoin that made the blockchain known to the world. To do this, you will install and run the Bitcoin core client.

Description of this assignment:

- This task consists of a series of steps, like a tutorial.
- You must submit a report containing the results obtained as you go through each step.

Minimum Requirements:

- Desktop or laptop hardware running recent versions of Windows, Mac OS X, or Linux.
  - ■ You can use your laptop or desktop running Windows, Mac OS X, Ubuntu or other linux.
- Accessible Hard disk at a minimum read/write speed of 100 MB/s.
  - ■ Do not worry if you do not have enough disk space, you can use the prune option to reduce the capacity.
- 2 gigabytes of memory (RAM).
- A broadband Internet connection with upload speeds of at least 400 kilobits (50 kilobytes) per second.

<Step. 1> Install Bitcoin core client.

Go to this URL, https://bitcoin.org/en/full-node, for information on installing the Bitcoin core. Follow the instructions in this URL.

※ If you don't have enough disk space for maintaining full node, please refer to "Reduce Storage" of Configuration Tuning.

You can reduce storage requirements by enabling pruning (deleting) of old blocks, using bitcoind prune option. (bitcoind –prune=N)

I'll assume that Bitcoind is running from here. (bitcoind –daemon)

※ However, you have to do this assignment using Testnet. For the Testnet, you can run Bitcoin Core with this option like "bitcoind -testnet -daemon". Do not forget setting RPC.

You must type "-testnet" option also every time you use "bitcoin-cli" in the following steps below. If you do not want to do that, create "bitcoin.conf" file in the directory "/home/username/.bitcoin/" and put "testnet=1".

<Step. 2> Check out the JSON-RPC APIs.

Search for available JSON-RPC commands. (Refer to "bitcoin-cli help")

Please include the result you obtained here in the report

<Step. 3> Set a password on the wallet / Unlock the password on the wallet.

[Before setting the password on the wallet]

Make sure there is no "unlocked_until" field in the output from "bitcoin-cli -testnet getwalletinfo".

[After setting the password on the wallet]

Make sure there is an "unlocked_until" field in the output from "bitcoin-cli –testnet getwalletinfo".

[After unlocking the password on the wallet]

In the output from "bitcoin-cli –testnet getwalletinfo", make sure that the time you specified is applied to the "unlocked_until" field.

<Step. 4> Generate an address / Get a Bitcoin / Check the balance.

Create an address to hold the Bitcoin and check the balance held by that address.

If you have never received a Bitcoin (BTC) or have never mined a block, the balance will be zero.

※ How to get a free Bitcoin.

There are several sites to get a free Bitcoin (BTC). The following URLs are sites giving a free BTC for you to test Bitcoin Client.

https://coinfaucet.eu/en/btc-testnet/

https://kuttler.eu/en/bitcoin/btc/faucet/

https://bitcoinfaucet.uo1.net/

<Step. 5> Check the reception of BTC Examine transaction contents/ Investigate more detailed transaction contents.

5-1) Verify the transaction related to BTC reception and then check the balance. You can get information such as txid, amount and recipient's address.

5-2) Examine the transaction, using txid found in 5-1.

5-3) The results of 5-2 are simple. Print out the actual details of the transaction.

<Step. 6> Create a transaction using UTXO / Sign the transaction / Send the transaction.

6-1) Determine the unspent and confirmed outputs to use as an input of a transaction.

6-2) Choose one of UTXOs gained from 6-1 and then create a transaction.

※ Keep in mind that the remaining BTC from UTXO is used as a fee for transmission. You should consume the balance of the UTXO except the proper amount of fees.

(You can find the proper amount of fees by checking transactions in mined blocks at the https://blockchain.info/ that is one of famous explorers for Bitcoin)

And you can also choose multiple addresses to transfer BTC.

6-3) Decode rawtransaction with hex string generated in 6-2. You can see that the 'scriptsig' field is empty.

6-4) Sign the transaction so that the 'scriptsig' field can be filled. As a result of signing, you will

obtain a new hex string.

※ Before you sign, you need to unlock your wallet in order to allow you to access a secret key in the wallet.

6-5) Check if 'scriptsig' field of the transaction is filled or not. If you have performed everything correctly, you will be able to see the filled 'scriptsig' field after decoding the hex string.

6-6) Send the transaction (raw transaction) which you got at 6-3 to the bitcoin network. If the transaction is completely transferred, txid (transaction id) will be printed out as an output.

6-7) Examine contents of the transaction using txid obtained from 6-5.

<Step. 7> Search for blocks

Try to search for blocks connected to the chain.

1) Height of block: 0
2) Height of block: 10000
3) The block including the transaction which is used in transferring your BTC.

Submit a report containing all results obtained from Steps 1 to 7.

<TA>
Chaehyeon Lee <chlee0211@postech.ac.kr>
Wonseok Choi <ws4583@postech.ac.kr>