Blockchain and Future Society
Homework Set 2

2021/3/24
Instructor: Heung-No Lee
Due date: 2021/3/31

Problem 1 Check the GIST LV Testnet Explorer, locate the most up to date block, write down its block height, the time-stamp, and the hash value.

Problem 2 Make sure you have downloaded the blockchain programming package as well as the Anaconda/Python/C++.

2.1 Reference is Preparation of Blockchain Progamming.pdf. Please find it in our class web-page.

2.2 Complete the installation of BIT-ECC (BIT-ECC Installation and Testing_11032021.pdf). Run BIT-ECC in your local computer. Follow the instruction and set up the virtual environment, run and test the BIT-ECC [Bitcoin Error Correction Code PoW Blockchain] on your local machine.

2.3 Show the results of Test Private Network part, such as
- 2.3.1 Execute BIT-ECC/Run BIT-ECC server
- 2.3.2 Get Block count
- 2.3.3 Generate an account/Generate public address
- 2.3.4 Generate 10 new blocks
- 2.3.5 Check blockchain information
- 2.3.6 Send transaction
- 2.3.7 Create raw transaction
- 2.3.8 Sign raw transaction
- 2.3.9 Send raw transaction
- 2.3.10 Verification of the issued transaction in a block

2.4 Complete the installation of Anaconda/Python/C++
- 2.4.1 Submit your first Python program which returns a simple message of “Hello World GIST Folks.”

Problem 3 Use Satoshi’s paper and my lecture note #1 for these answers. Two or three line answers for each shall be enough.
- 3.1 What is the definition of bitcoin?
- 3.2 What is the double spending problem? How is it resolved in bitcoin network?
- 3.3 What is the timestamp server?
- 3.4 Write down your reasoning why blockchain provides data immutability.
- 3.5 Is the data stored in blockchain really immutable?
- 3.6 What is the kind of attack the bitcoin paper says is possible?

3.7 Write down the sequence of events to mine a block?
3.8 List the field types that needs to be recorded inside the blockheader?
3.9 What is the byte size of the private and that of the public key used in Bitcoin?
3.10 What is the meaning of signatures in Satoshi's paper?
3.11 Bob wants to send Alice a bitcoin. What are the three basic things that must be done to complete this transaction?
3.12 Why do we need proof-of-work in bitcoin network?
3.13 What is the benefit of eliminating the third party according to Satoshi?
3.14 Who is doing the proof-of-work in bitcoin network?
3.15 What is a hash cycle?

Problem 4 Define what a money is. Provide your source.

4.1 Define what currency is. Provide your source.
4.2 What is the current market price of a bitcoin? Is it expensive or cheap? Justify your answer.
4.3 Bitcoin intends to get rid of the bank and uses P2P network instead. What are the possible benefits of using P2P network, instead of a bank? What are the possible drawbacks? Justify your answer.
4.4 Does the fiat money such as KRW and USD have any intrinsic value? Why do you think they have a market value? Who or what decides their values?