**INFONET Blockchain Demonstration**

Kiwon Yang, Changyun Lee, Seungbum Kang

Advisor Prof. Heung-No Lee

Sept. 15th 2018



****

**INFONET Blockchain Demonstration**

Kiwon Yang, Changyun Lee, Seungbum Kang

Advisor Prof. Heung-No Lee

Sept. 15th 2018

The aim of this demo is show that our blockchain consensus mechanism is working properly. A suite of codes implementing the consensus mechanism is written in python and Flask language.

Currently the consensus mechanism includes the following items:

1. **The block and its header,**

That is, a block includes Index (the block number), Nonce, Data (shown as ‘Data’ in PPT), Previous hash, and Present hash.

1. **Proof-of-Work (PoW) based on SHA256 hash function,**
2. **Change of difficulty level by increasing or decreasing the number of zeros in hashes,**
3. **The longest chain consensus rule, and**

That is, whenever each node starts to mine a block, it looks for the longest valid chain. Each node communicates with all its neighbor miner nodes, determines which one has the longest chain. If the longest chain from the neighbor is longer than its own local chain and its hash sequence is validated, and it replaces its local chain with the longest validated chain.

1. **Inclusion of broadcasted transactions in to blocks.**

That is, those transactions broadcasted to the mining network are captured by a minor node and included in the blockchain.

To this end, we use six computers. Each one has its own IP address.

This demonstrates the operation of a small mining network with six computers in total.

Five computers do the role of independently working miner computers and one computer is set to generate transactions only.

The IP address of miner computers are

* Node 1 (IP: 172.26.16.41): a mining node
* Node 2 (IP: 172.26.16.66): a mining node
* Node 3 (IP: 172.26.16.43): a mining node
* Node 4 (IP: 172.26.16.42): a mining node
* Node 5 (IP: 172.26.16.32): a mining node

**The node generating the transactions is**

* **Node 6 (IP: 203.237.54.101): a transaction making node**

**The port number used is 5000 for all of these nodes.**

**Script for the Working Demo on Screen**

We ran the experimental set up and captured it into a video file.

This video file is replayed in this console.

First we open up Anaconda console at Node 1 (IP: 172.26.16.41).

Then go to the directory where the blockchain core file is located.

We start info\_blockchain by issuing the command:

>python info\_blockchian1.py

Then, the computer is running the blockchain core as we can see from the console.

Node 1 is now a blockchain server in this small network.

There are other nodes which were started as well at the same time.

This is not shown in this console.

Because this one is the console at Node 1.

First, into Node 1, other nodes are registered as its neighbors.

Node 1 (IP: 172.26.16.41) starts mining!

As soon as it starts mining, it first aims to gather all the chains from its neighbors.

Node 1 requests to obtain chains from its neighbors,

that of Node 4 (IP: 172.26.16.42),

that of Node 3 (IP: 172.26.16.43), and

that of Node 5 (IP: 172.26.16.32).

Node 1 announces its mining success to neighbors.

Other nodes stops mining their current block, accept this chain and start mining again to extend this adopted chain.

Node 4 is announcing the third block mining success.

Other nodes adopting it follows.

Again, Node 4 mines the next block, the 4th block.

The 5th block is mined by the Node 3.

Node 6 generates a transaction.

It is included in the 6th block which is mined by Node 2.

On each block, the first transaction is the mining reward of 50 coins, paid to miner’s address.

This continues…

7th Block minded by Node 4.

8th Block minded by Node 4

9th Block minded by Node 5

…

On the average, it takes about 4.7 seconds to mine single block at this difficulty level of five leading zeros.

This is hexadecimal zeros.

Thus, one more leading zero means that it takes 16 times longer than before.

Let us calculate the expected time to mine a block.

16 times 4.7 seconds per block is 75 seconds per block.

Thus, it will now take more than a single minute on the average to mine a single block.

…

We let it continues to 30th block.

On the 31st block, the difficulty level was changed to 6 leading zeros.

We will notice this at the frame at time 02:16.

As we have calculated already it will take about 75 second to mine a single block on the average.

Now stop waiting for the next block to be mined at this difficulty level.

On 03:32, the difficulty level is changed to 4 leading hexa zeros.

Thus, on the average, it will take about 0.6 second per block.

About 100 blocks mined for 1 minute, we will see.

One 04:36, the difficulty level is changed back to 5 leading hex zeros.

This continues till the end.

END