Nodejs
200行的迷你區塊鏈

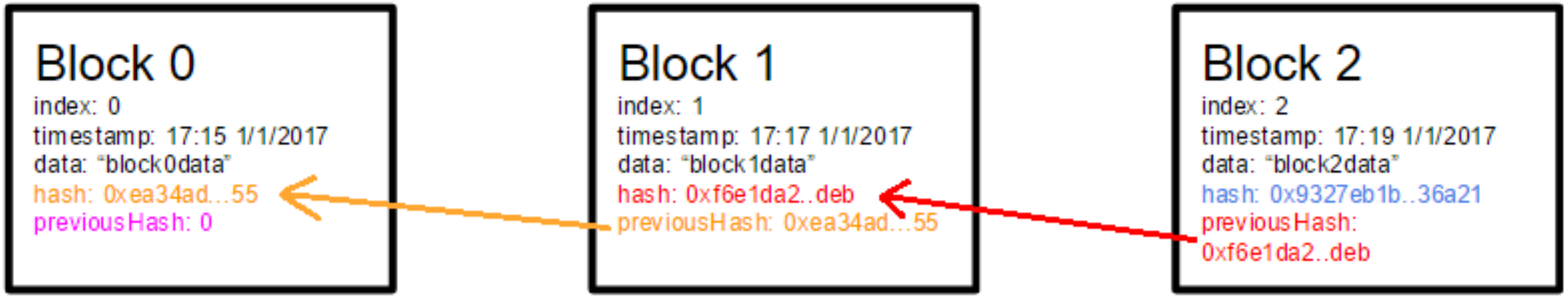
盧瑞山 教授

觀念講解

一個區塊鏈系統包含什麼？

- p2p網路
- 共識系統
- 區塊定義與結構
- 區塊鏈的構成
- 交易

僅200行程式碼的最小的區塊鏈系統

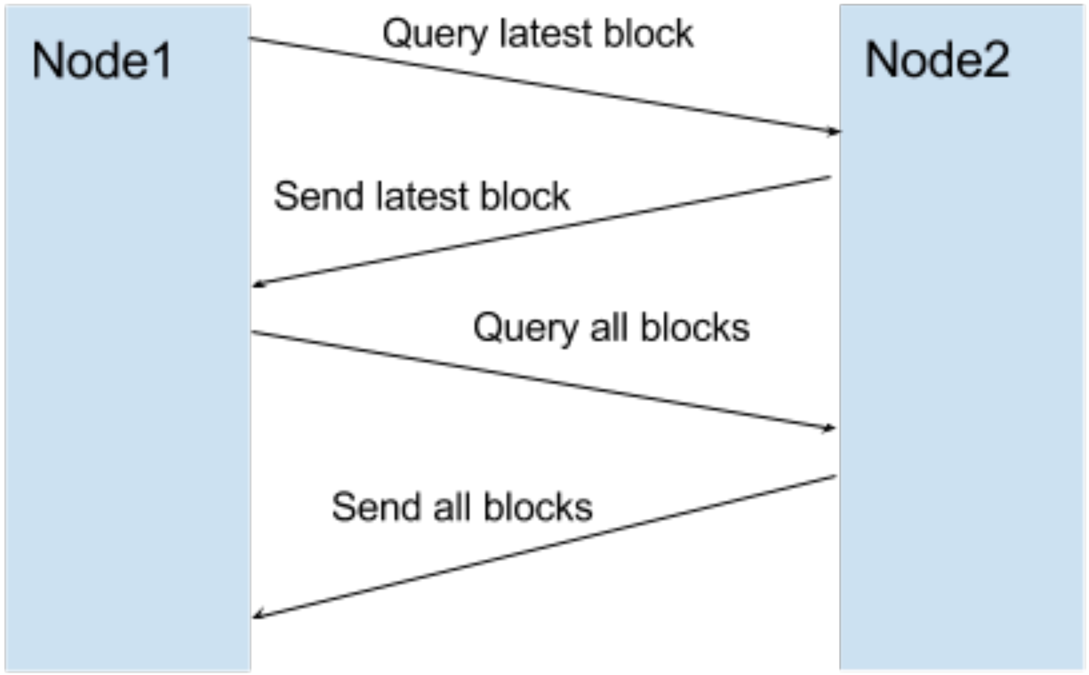


Block 0
index: 0
timestamp: 17:15 1/1/2017
data: “block0data”
hash: 0xea34ad…55
previousHash: 0

Block 1
index: 1
timestamp: 17:17 1/1/2017
data: “block1data”
hash: 0xf6e1da2..deb
previousHash: 0xea34ad…55

Block 2
index: 2
timestamp: 17:19 1/1/2017
data: “block2data”
hash: 0x9327eb1b..36a21
previousHash:
0xf6e1da2..deb

Node1 connects and syncs with Node2



Node1

Node2

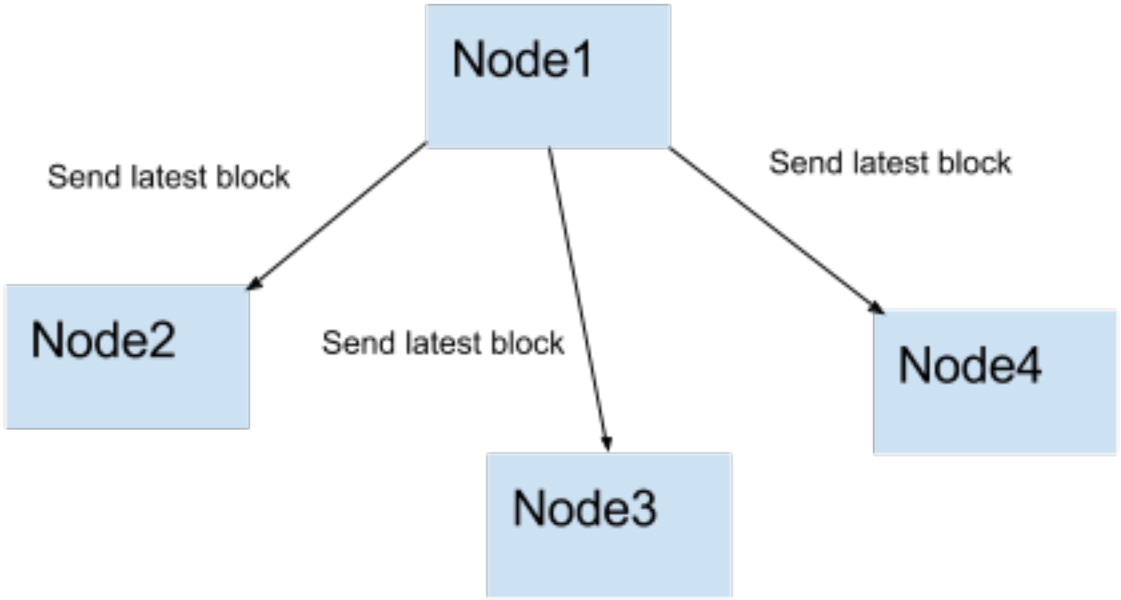
Query latest block

Send latest block

Query all blocks

Send all blocks

Node1 generates a block and broadcasts it



Node1

Send latest block

Send latest block

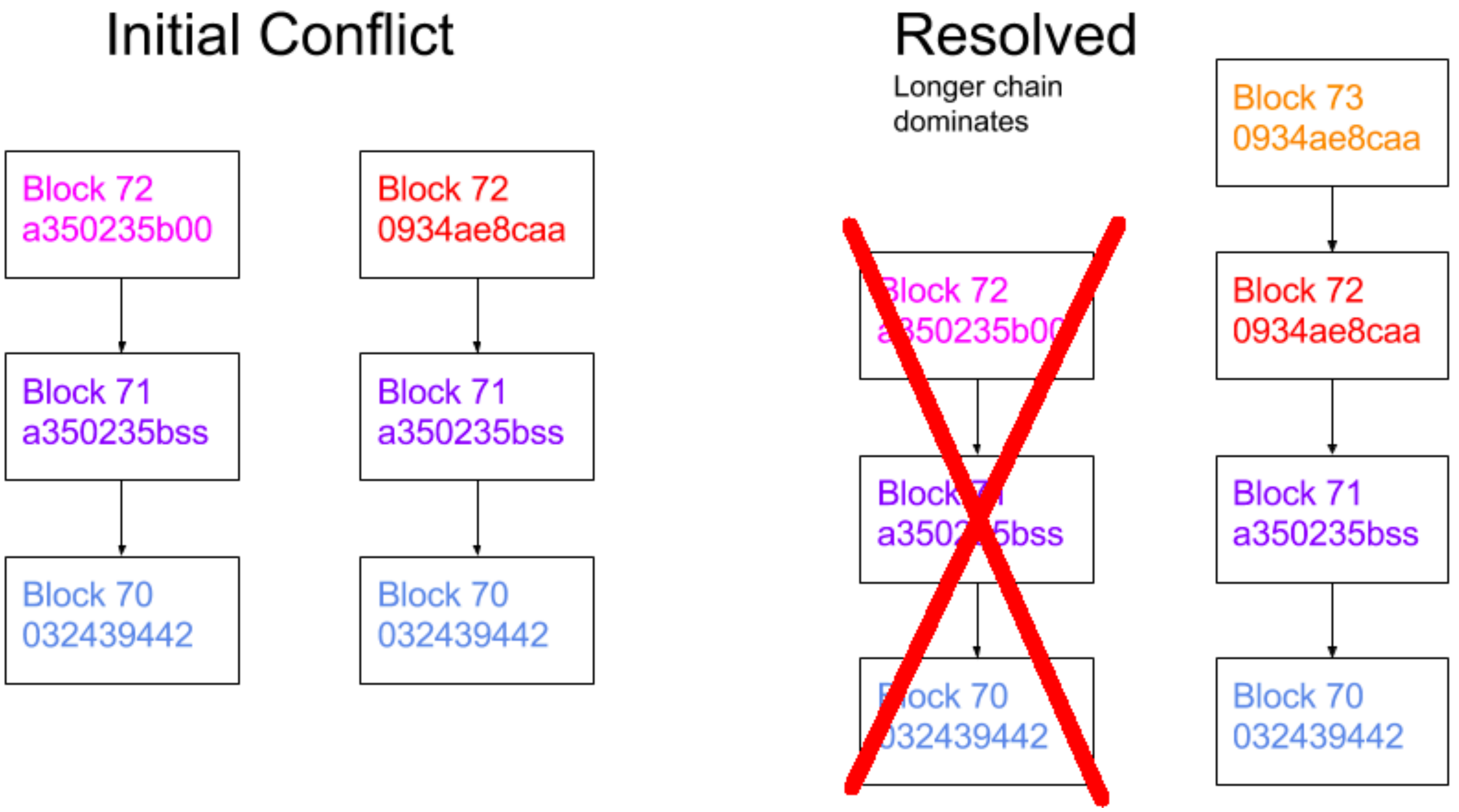
Send latest block

Node2

Node3

Node4

Choosing the longest chain



Initial Conflict

Block 72
a350235b00

Block 71
a350235bss

Block 70
032439442

Block 72
0934ae8caa

Block 71
a350235bss

Block 70
032439442

Resolved

Longer chain dominates

Block 72
a350235b00

Block 71
a350235bss

Block 70
032439442

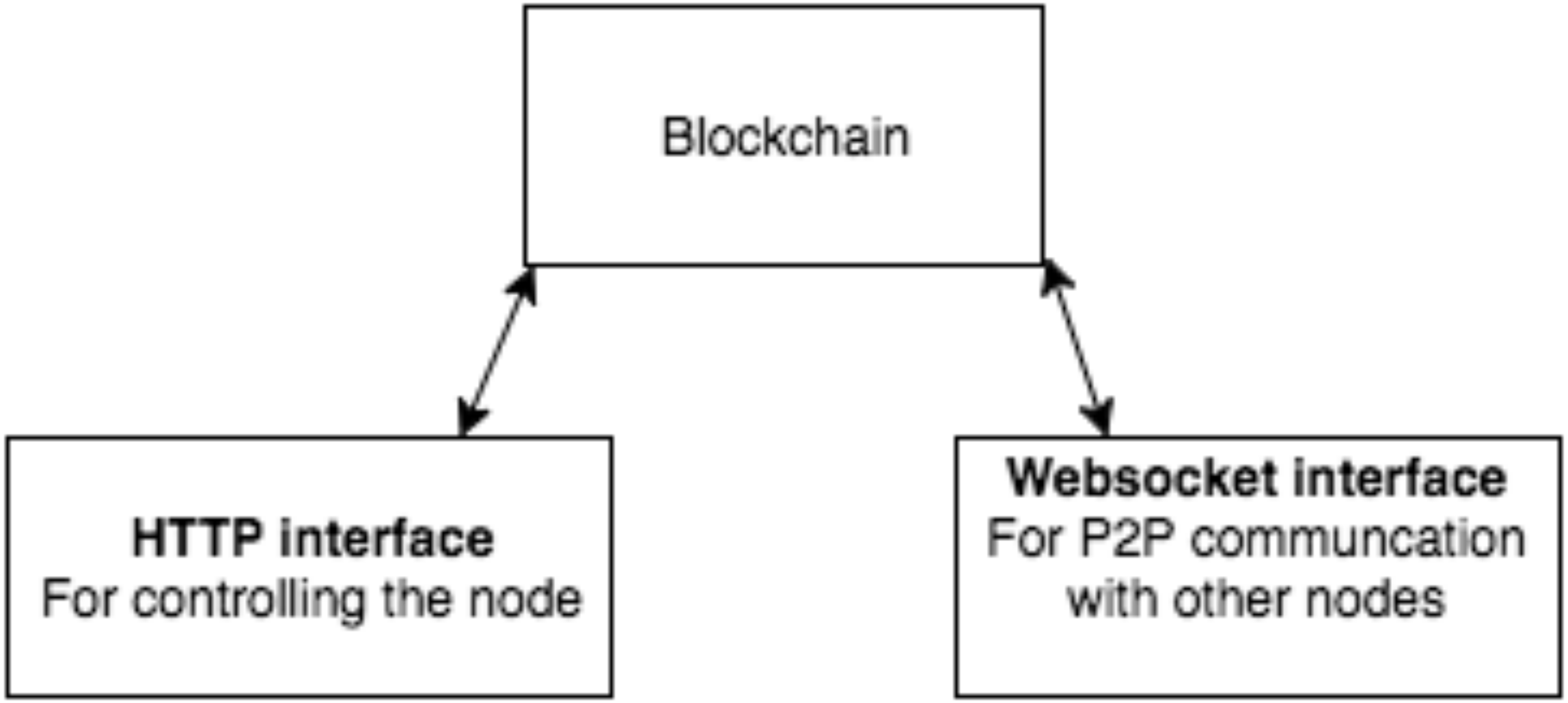
Block 73
0934ae8caa

Block 72
0934ae8caa

Block 71
a350235bss

Block 70
032439442

Architecture



Blockchain

HTTP interface
For controlling the node

Websocket interface
For P2P communcation
with other nodes

200行程式碼的迷你區塊鏈

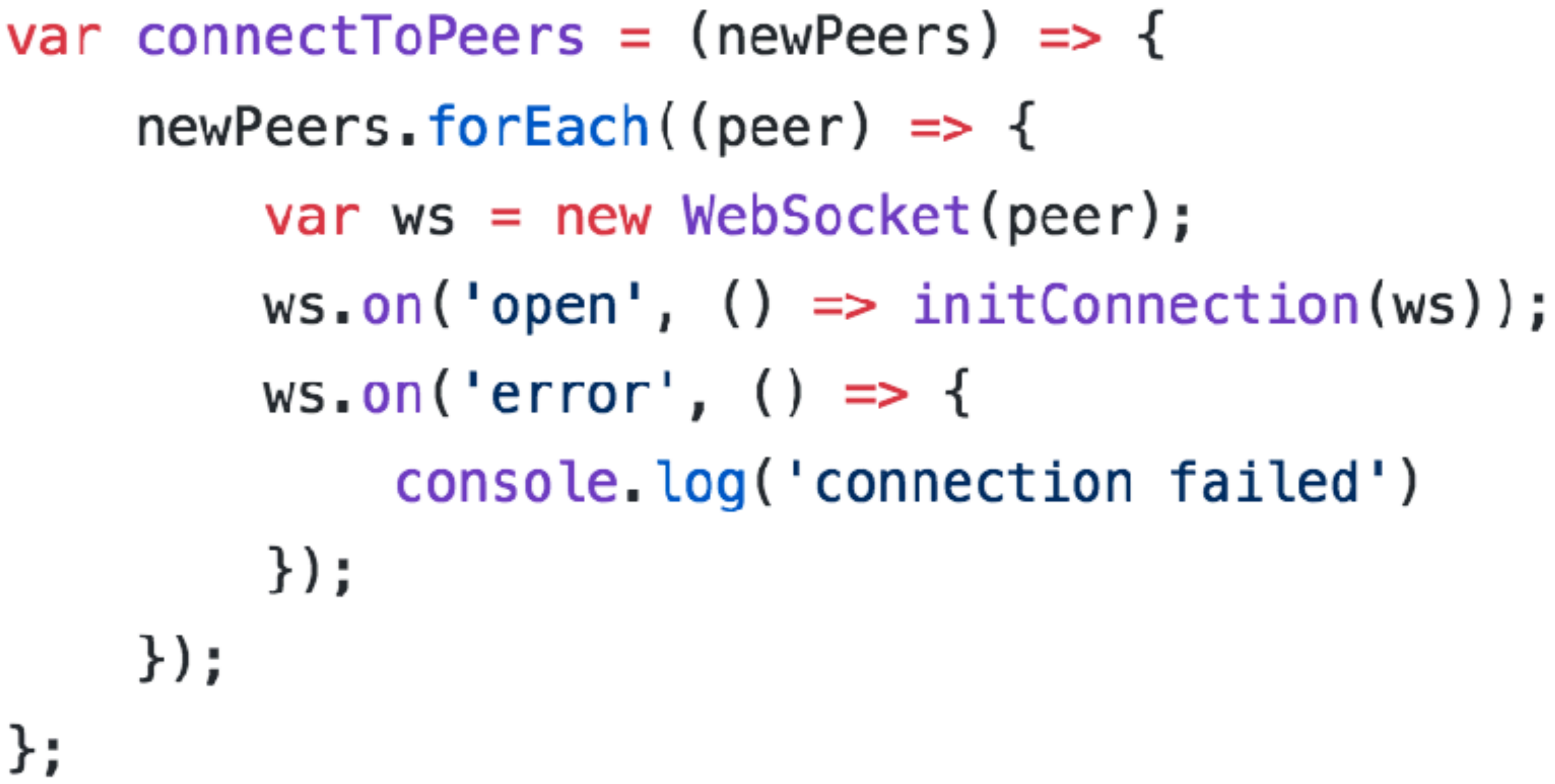
- 每一個節點都是 websocket server
- 每一個節點都是 websocket client

程式初始化

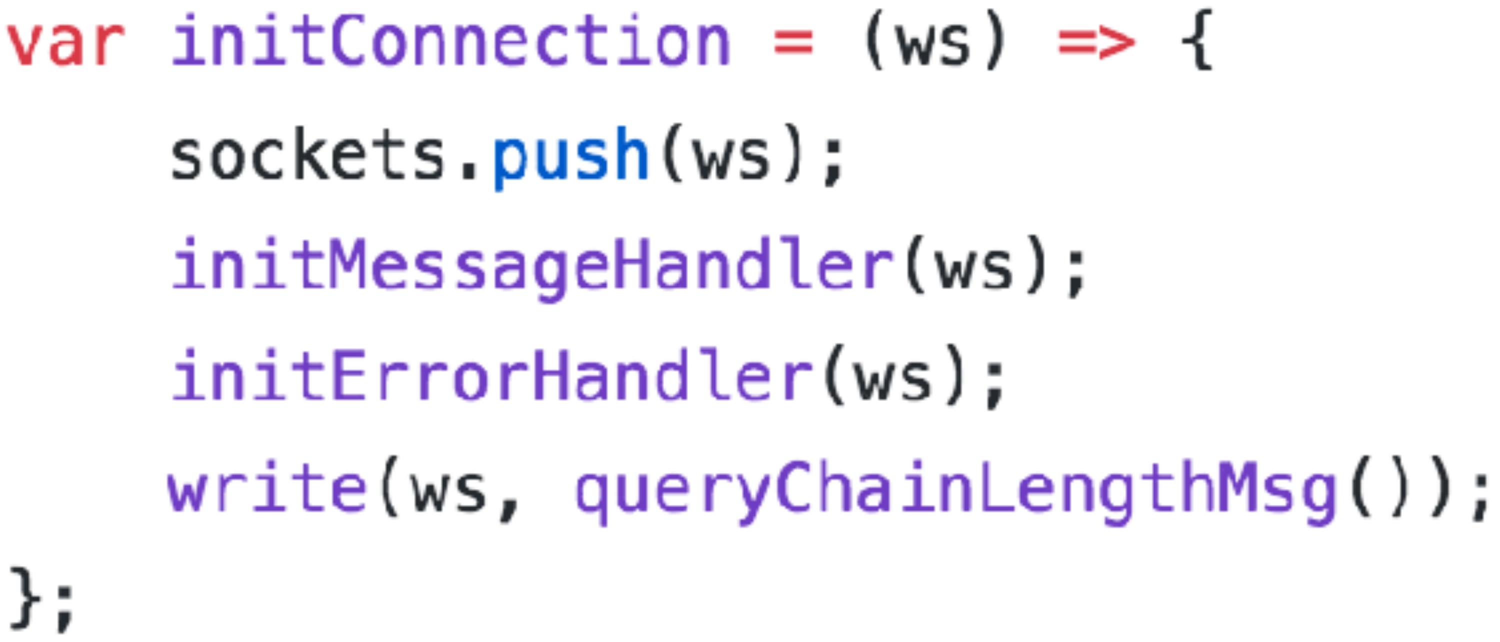
主程式 main.js

- connectToPeers(initialPeers);
- initHttpServer();
- initP2PServer();

connectToPeers(initialPeers);

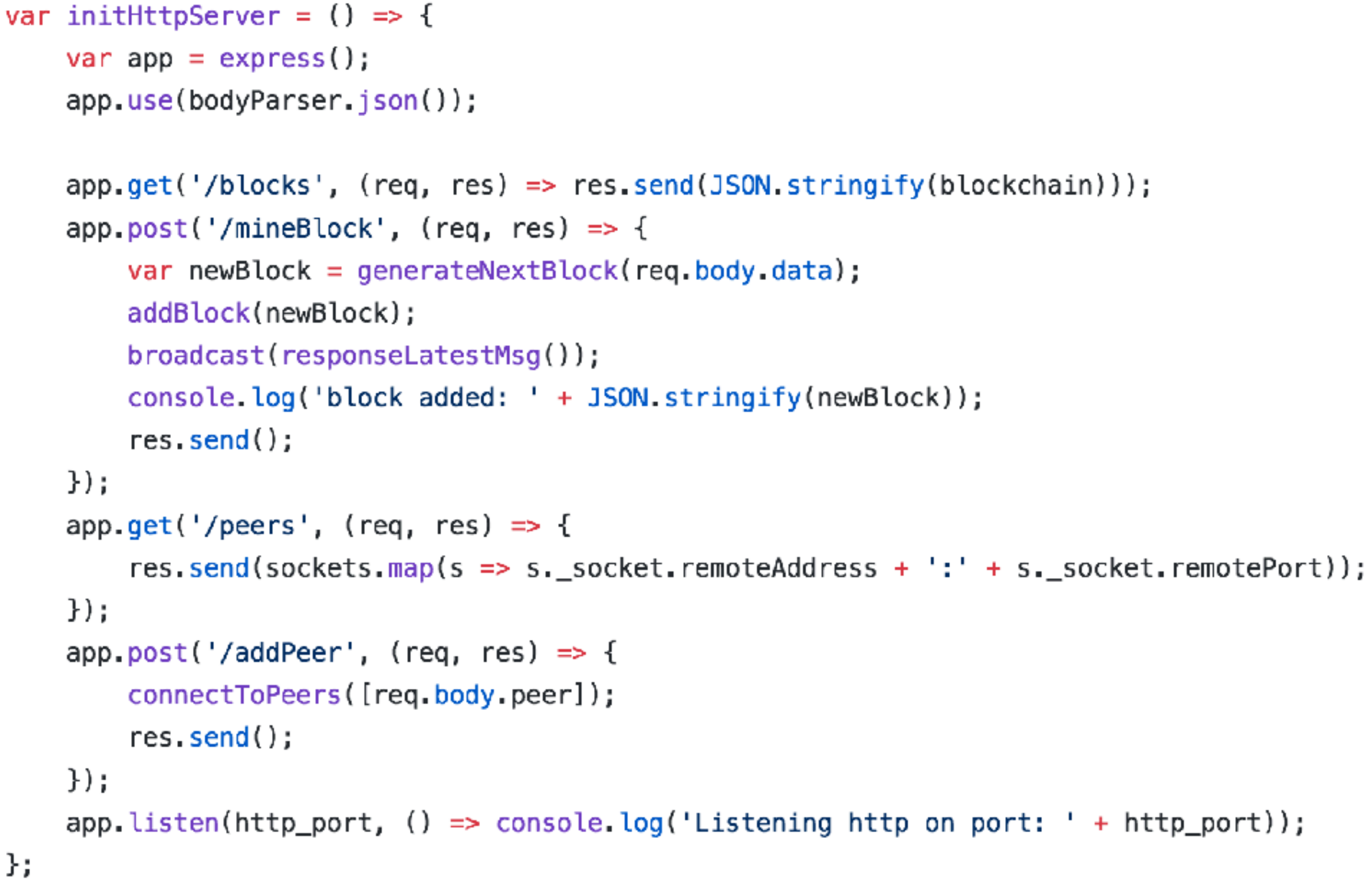


```
var connectToPeers = (newPeers) => {
    newPeers.forEach((peer) => {
        var ws = new WebSocket(peer);
        ws.on('open', () => initConnection(ws));
        ws.on('error', () => {
            console.log('connection failed')
        });
    });
};
```



```
var initConnection = (ws) => {
    sockets.push(ws);
    initMessageHandler(ws);
    initErrorHandler(ws);
    write(ws, queryChainLengthMsg());
};
```

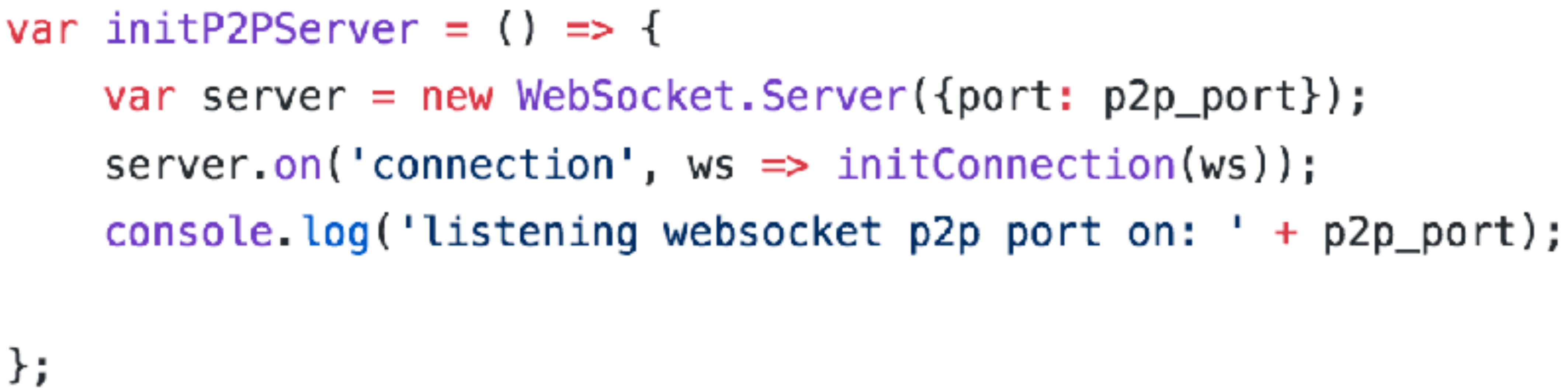
initHttpServer();



```
var initHttpServer = () => {
    var app = express();
    app.use(bodyParser.json());

    app.get('/blocks', (req, res) => res.send(JSON.stringify(blockchain)));
    app.post('/mineBlock', (req, res) => {
        var newBlock = generateNextBlock(req.body.data);
        addBlock(newBlock);
        broadcast(responseLatestMsg());
        console.log('block added: ' + JSON.stringify(newBlock));
        res.send();
    });
    app.get('/peers', (req, res) => {
        res.send(sockets.map(s => s._socket.remoteAddress + ':' + s._socket.remotePort));
    });
    app.post('/addPeer', (req, res) => {
        connectToPeers([req.body.peer]);
        res.send();
    });
    app.listen(http_port, () => console.log('Listening http on port: ' + http_port));
};
```

initP2PServer();



```
var initP2PServer = () => {
    var server = new WebSocket.Server({port: p2p_port});
    server.on('connection', ws => initConnection(ws));
    console.log('listening websocket p2p port on: ' + p2p_port);

};
```

Linux上的Node.js安裝

-Linux系統(以Ubuntu為例) 通常無法裝到最新版，可採自行編譯Nodejs的方式安裝到最新版

1.使用app-get 來安裝，若是CentOS則用yum install

- $ sudo apt-get install nodejs
- $ sudo apt-get install npm

更新Node.js的版本

- in Mac OS

```
brew upgrade node
```

- in linux

```
sudo npm cache clean -f

sudo npm install -g n

sudo n stable

sudo n latest

sudo ln -sf /usr/local/n/versions/node/8.1.2/bin/node /usr/bin/node
```

自行編譯Nodejs

- sudo apt-get install gcc g++
- sudo apt-get install make
- wget https://nodejs.org/dist/v8.1.2/node-v8.1.2.tar.gz
- 或git clone https://github.com/nodejs/node
- tar xvf node-v8.1.2.tar.gz
- cd node-v8.1.2
- ./configure
- make or make -j4
- sudo make install

自行編譯Nodejs

- sudo apt-get install build-essential libtool autotools-dev automake pkg-config libssl-dev libevent-dev bsdmainutils
- wget https://nodejs.org/dist/v8.1.2/node-v8.1.2.tar.gz
- 或git clone https://github.com/nodejs/node
- tar xvf node-v8.1.2.tar.gz
- cd node-v8.1.2
- ./configure
- make or make -j4
- sudo make install

Nodejs 開發編輯器

- Visual Studio Code (VS Code)
- sublime
- Bracket

安裝NaiveChain

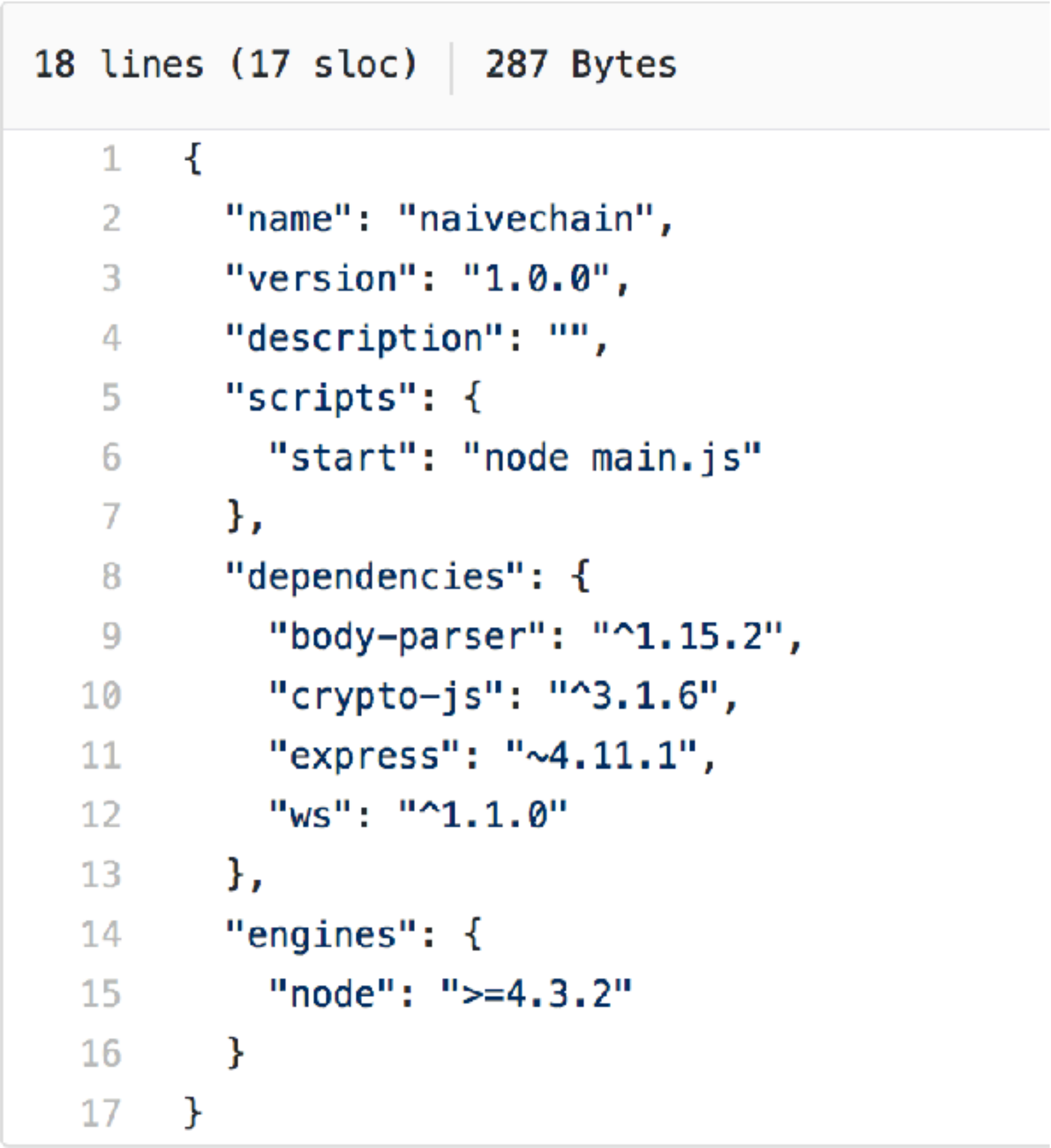
- chmod +x docker_install.sh
- sudo apt-get install docker-compose
- git clone https://github.com/rslu2000/naivechain
- cd naivechain
- npm install

或從docker安裝啟動也可以

- chmod +x docker_install.sh
- sudo apt-get install docker-compose

```
$  git clone https://github.com/rslu2000/naivechain
$ cd naivechain
$ docker-compose up
```

package.json



18 lines (17 sloc) | 287 Bytes

```json
{
  "name": "naivechain",
  "version": "1.0.0",
  "description": "",
  "scripts": {
    "start": "node main.js"
  },
  "dependencies": {
    "body-parser": "^1.15.2",
    "crypto-js": "^3.1.6",
    "express": "~4.11.1",
    "ws": "^1.1.0"
  },
  "engines": {
    "node": ">=4.3.2"
  }
}
```

運行NaiveChain

- HTTP_PORT=3001 P2P_PORT=6001 npm start **(運行第一個節點)**

- HTTP_PORT=3002 P2P_PORT=6002 PEERS=ws://localhost:6001 npm start **(運行第二個節點, 同時去把第一個節點給連起來)**

- HTTP_PORT=3003 P2P_PORT=6003 PEERS=ws://localhost:6001 npm start **(運行第三個節點, 同時去把第一個節點給連起來)**

- HTTP_PORT=3004 P2P_PORT=6004 PEERS=ws://localhost:6001 npm start **(運行第二個節點, 同時去把第一個節點給連起來)**

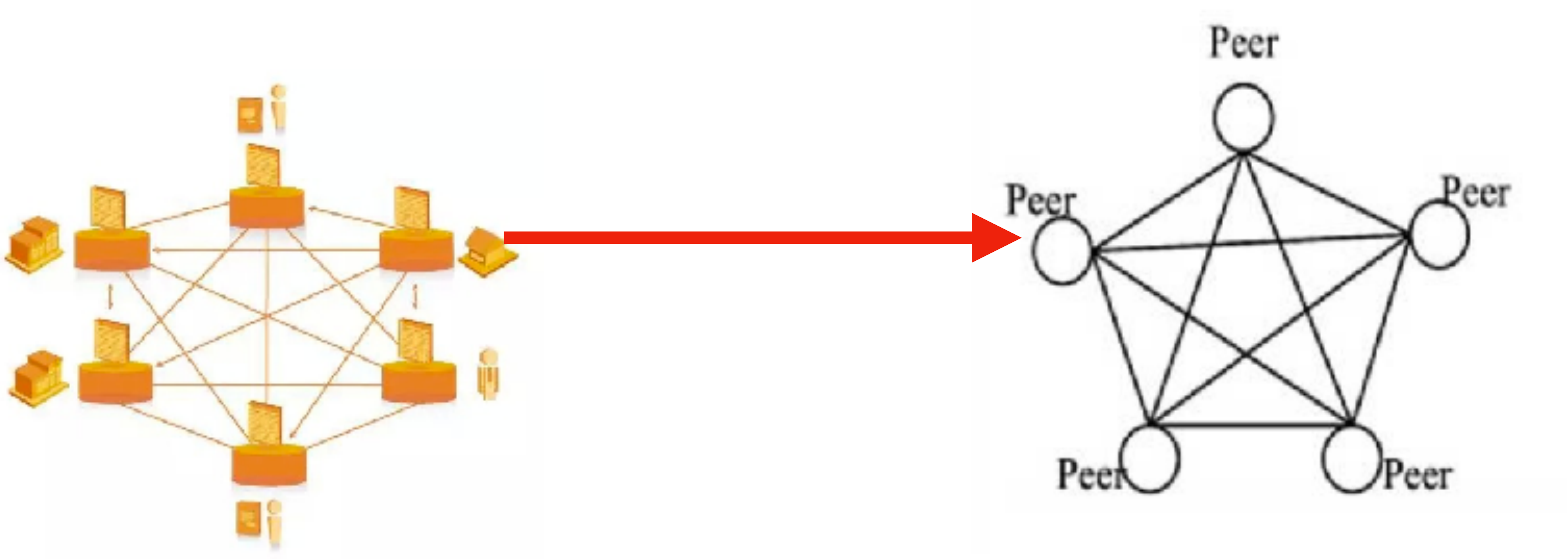
- curl -H "Content-type:application/json" --data '{"data" : "Some data to the first block"}' http://localhost:3001/mineBlock

請鄰座同學一起加入節點成為區塊鏈成員

- HTTP_PORT=3002 P2P_PORT=6002 PEERS=ws://**同學的ip**:**6001** npm start **(運行自己的節點, 同時去把某同學的節點給連起來)**

兩條區塊鏈結成聯盟
將對方加入節點

-
  ```
  curl -H "Content-type:application/json" --data '{"peer" : "ws://35.194.228.1:6001"}' http://localhost:3002/addPeer
  ```

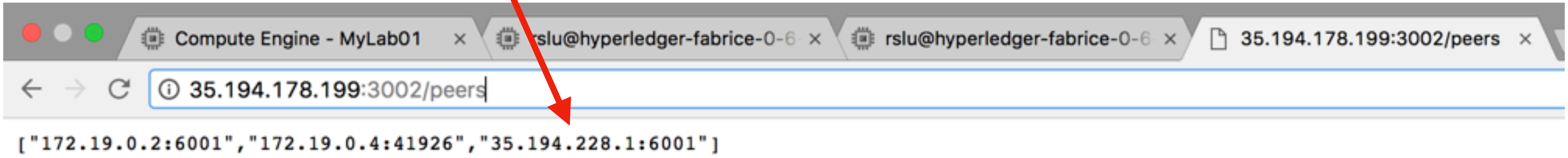


區塊高度為5

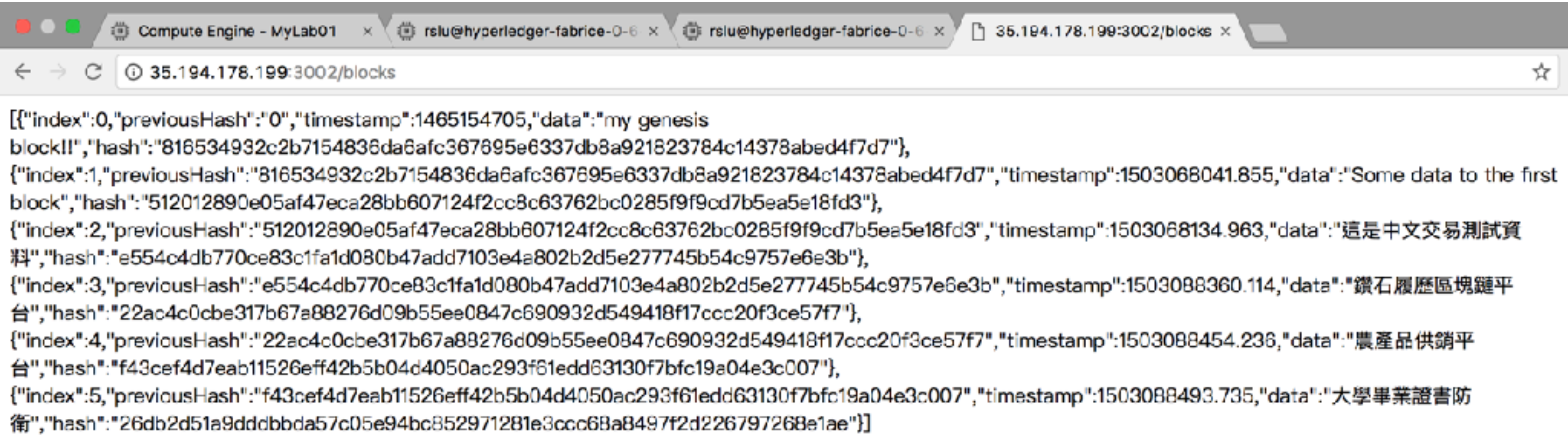
區塊高度為3

- curl -H "Content-type:application/json" --data '{"peer" : "ws://35.194.228.1:6001"}' http://localhost:3002/addPeer

測試結果

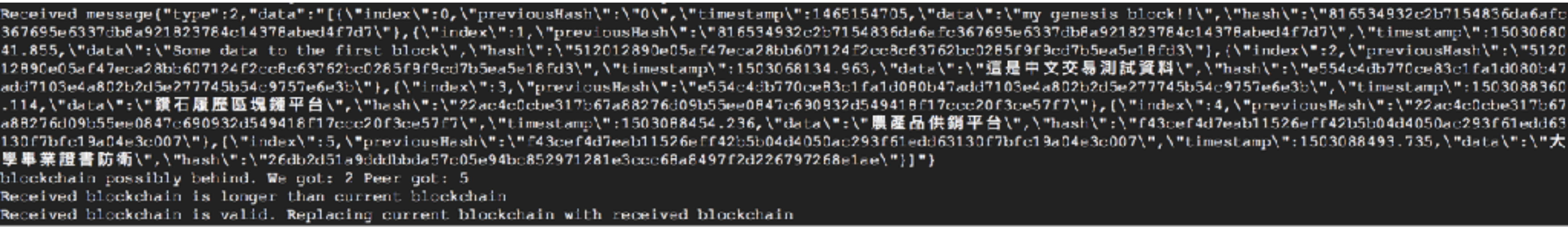

Compute Engine - MyLab01
rslu@hyperledger-fabrice-0-6
rslu@hyperledger-fabrice-0-6
35.194.178.199:3002/peers
35.194.178.199:3002/peers

```
["172.19.0.2:6001","172.19.0.4:41926","35.194.228.1:6001"]
```


Compute Engine - MyLab01
rslu@hyperledger-fabrice-0-6
rslu@hyperledger-fabrice-0-6
35.194.178.199:3002/blocks
35.194.178.199:3002/blocks

```
[{"index":0,"previousHash":"0","timestamp":1465154705,"data":"my genesis
block!!","hash":"816534932c2b7154836da6afc367695e6337db8a921823784c14378abed4f7d7"},
{"index":1,"previousHash":"816534932c2b7154836da6afc367695e6337db8a921823784c14378abed4f7d7","timestamp":1503068041.855,"data":"Some data to the first
block","hash":"512012890e05af47eca28bb607124f2cc8c63762bc0285f9f9cd7b5ea5e18fd3"},
{"index":2,"previousHash":"512012890e05af47eca28bb607124f2cc8c63762bc0285f9f9cd7b5ea5e18fd3","timestamp":1503068134.963,"data":"這是中文交易測試資
料","hash":"e554c4db770ce83c1fa1d080b47add7103e4a802b2d5e277745b54c9757e6e3b"},
{"index":3,"previousHash":"e554c4db770ce83c1fa1d080b47add7103e4a802b2d5e277745b54c9757e6e3b","timestamp":1503088360.114,"data":"鑽石履歷區塊鏈平
台","hash":"22ac4c0cbe317b67a88276d09b55ee0847c690932d549418f17ccc20f3ce57f7"},
{"index":4,"previousHash":"22ac4c0cbe317b67a88276d09b55ee0847c690932d549418f17ccc20f3ce57f7","timestamp":1503088454.236,"data":"農產品供銷平
台","hash":"f43cef4d7eab11526eff42b5b04d4050ac293f61edd63130f7bfc19a04e3c007"},
{"index":5,"previousHash":"f43cef4d7eab11526eff42b5b04d4050ac293f61edd63130f7bfc19a04e3c007","timestamp":1503088493.735,"data":"大學畢業證書防
衛","hash":"26db2d51a9dddbbda57c05e94bc852971281e3ccc68a8497f2d226797268e1ae"}]
```

原本比較短鏈的那個區塊鏈上的節點會發生什麼事？



```
Received message{"type":2,"data":"[{\"index\":0,\"previousHash\":\"0\",\"timestamp\":1465154705,\"data\":\"my genesis block!!\",\"hash\":\"816534932c2b7154836da6afc
367695e6337db8a921823784c14378abed4f7d7\"},{\"index\":1,\"previousHash\":\"816534932c2b7154836da6afc367695e6337db8a921823784c14378abed4f7d7\",\"timestamp\":15030680
41.855,\"data\":\"Some data to the first block\",\"hash\":\"512012890e05af47eca28bb607124f2cc8c63762bc0285f9f9cd7b5ea5e18fd3\"},{\"index\":2,\"previousHash\":\"5120
12890e05af47eca28bb607124f2cc8c63762bc0285f9f9cd7b5ea5e18fd3\",\"timestamp\":1503068134.963,\"data\":\"這是中文交易測試資料\",\"hash\":\"e554c4db770ce83c1fa1d080b47
add7103e4a802b2d5e277745b54c9757e6e3b\"},{\"index\":3,\"previousHash\":\"e554c4db770ce83c1fa1d080b47add7103e4a802b2d5e277745b54c9757e6e3b\",\"timestamp\":1503088360
.114,\"data\":\"鑽石履歷區塊鏈平台\",\"hash\":\"22ac4c0cbe317b67a88276d09b55ee0847c690932d549418f17ccc20f3ce57f7\"},{\"index\":4,\"previousHash\":\"22ac4c0cbe317b67
a88276d09b55ee0847c690932d549418f17ccc20f3ce57f7\",\"timestamp\":1503088454.236,\"data\":\"農產品供銷平台\",\"hash\":\"f43cef4d7eab11526eff42b5b04d4050ac293f61edd63
130f7bfc19a04e3c007\"},{\"index\":5,\"previousHash\":\"f43cef4d7eab11526eff42b5b04d4050ac293f61edd63130f7bfc19a04e3c007\",\"timestamp\":1503088493.735,\"data\":\"大
學畢業證書防衛\",\"hash\":\"26db2d51a9dddbbda57c05e94bc852971281e3ccc68a6497f2d226797268e1ae\"}]"}
blockchain possibly behind. We got: 2 Peer got: 5
Received blockchain is longer than current blockchain
Received blockchain is valid. Replacing current blockchain with received blockchain
```