第7回 exercise

submit

https://docs.google.com/forms/d/e/1FAIpQLScAFLD5lGNhiFIZt8SvUJIFA-nVy2GKcMZLho0kx0_ZAFSYHQ/viewform

①testnetとregtestの二つのモードの違いを述べよ

- answer:

  いずれもテスト用の環境だが、TestnetがMainnet同様に他ユーザと共用のネットワークであるのに対して、Regtestは、blockchainネットワークそのものの構築から、プライベートなクローズド環境でテストできる、自動テスト用環境を構築できることが異なる。 また、Testnetについては、coinに価値が生じたら、再起動される。

detail from course memo:

- Testnet

  -> coinに価値が生じたら、再起動

- Regtest
  - miningが最も簡単で、そもそもルールがない
  - 自動テストを容易にするもの
  - 自動的にプライベートブロックチェーンを新規に作成するところからテスト実行されるために利用

②Coreのウォレットにあるビットコインを手動で取引作成して、署名して、配信したい場合に使用するRPCコールを順番に述べよ

1. createrawtransaction
2. signrawtransaction
3. sendrawtransaction

③現行バージョンの初期値で「relayfee」はいくらになっているか述べよ (ヒント：ノードの情報を教えてくれるRPCはどれ)

- answer

```
0.00001000
```

http://chainquery.com/でgetnetworkinfoコマンドを実行

(FYI) result of getnetworkinfo

- solution：getnetworkinfoコマンドを使用、relayfee以外にも以下確認可能
    - Bitcoin Coreのバージョン ”version”:
    - 取引、トランザクションをこのノードが中継するときに支払う料金設定 ”relayfee”:
    - ノードの接続数 ”connections”:
    - 自ノードのアドレス ”localaddresses”:

④自分のCoreにあるアドレスで「Blockchain Daigakko」を署名してその結果(アドレスも含めて)を述べよ

- example answer
    - address

```
muTeGjvKaEA26wJfQX9wzKyEs54sYGTFpH
```

    - message signed

```
HzFlPM5+Ek/KGl0RH1VHwCqACUewtFKCKvd0NZN/mJetCwIkfpZncjwmVdNvdQtjyVEiuqyFGFft
/wAkn6Z7LT4=
```

- solution

1. bitcoin core インストール

- Windows: bitcoin-0.16.1-win32-setup.exe
- reference：https://bitcoin.org/en/developer-examples#testing-applications

2. daemon 起動

- bitcoin.conf (rpcuser, rpcpassword are depend on individual environment/user)

```
testnet = 3
txindex = 1

server = 1

rpcuser=nobutanaka
rpcpassword=Password123
rpcport = 18332
```

windows の場合、%AppData%¥Roaming¥Bitcoin¥bitcoin.conf に保存

Linux の場合は ~/.bitcoin/bitcoin.conf

$ bitcoind -testnet -daemon

- windows 10で実行時は以下エラーとなるためdaemonオプション指定なしに

  ```
  Error: -daemon is not supported on this operating system
  ```

```
> bitcoind -testnet
```

3. コマンド実行

   Windowsの場合には、別のコマンドプロンプトを起動して以下を実行

```
> bitcoin-cli -testnet getnewaddress "nobutanaka" legacy
muTeGjvKaEA26wJfQX9wzKyEs54sYGTFpH
```

Note:

- label(account) is accepptable "" instead of above
- **legacy option is mandetory** to convert (default) segwit addresses because signmessage doesn't work with segwit addresses as of Bitcoin Core version 0.16~0.14

```
> bitcoin-cli -testnet signmessage muTeGjvKaEA26wJfQX9wzKyEs54sYGTFpH \
> 'Blockchain Daigakko'
```