한 번에 끝내는 블록체인, DApp 개발의 모든 것

Chapter 1

Blockchain 1.0 - Bitcoin

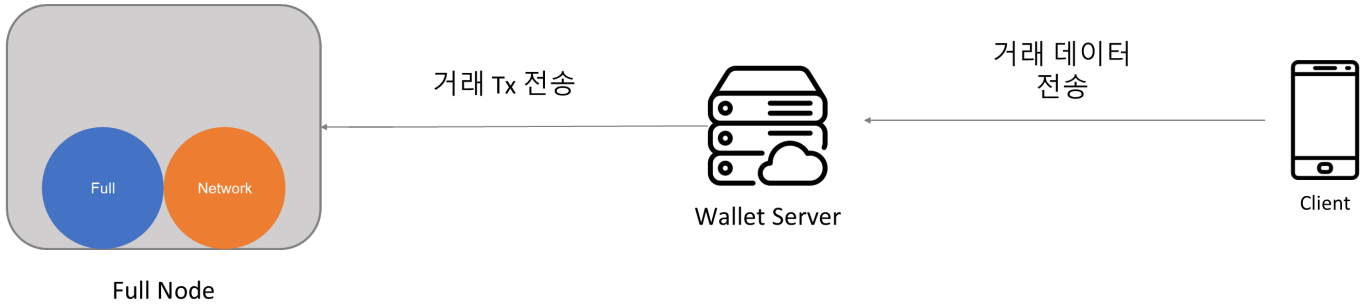
Chapter 1

Blockchain 1.0 - Bitcoin

Bitcoind 소개

Bitcoin Core(bitcoind)

- Satoshi Nakamoto가 개발한 Bitcoin 공식 클라이언트(노드) 소프트웨어
- SPV 노드의 대표적인 소프트웨어에는 Electrum이 있다.
- 현재 Bitcoin Full Node 를 Sync 하는데 걸리는 시간은 약 1주정도 이다.(성능에 따라 달라짐)
- Bitcoin Core를 통해서 네트워크에 참여할 수 있기 때문에 우리가 사용하는 대부분의 Wallet들이 접속해야 하는 노드가 존재한다.
- 현재 Bitcoin Full Node는 약 10만개 이상(접근 가능한 노드 수는 15,000개)
- Bitcoin-qt, bitcoin-daemon, bitcoin-cli 로 구성되어 있다.



Bitcoin Core(bitcoind) 설치 (Windows)

1) bitcoin.org/ko/download 페이지 접속

2) Windows 실행 파일(exe) 다운로드 후 실행

3) Bitcoin-Qt 를 통해 Wallet 생성

Bitcoin Core(bitcoind) 설치 (Ubuntu)

1) >> apt update

2) >> git clone https://github.com/bitcoin/bitcoin.git

3) >> cd bitcoin/ && ./autogen.sh

4) >> ./configure

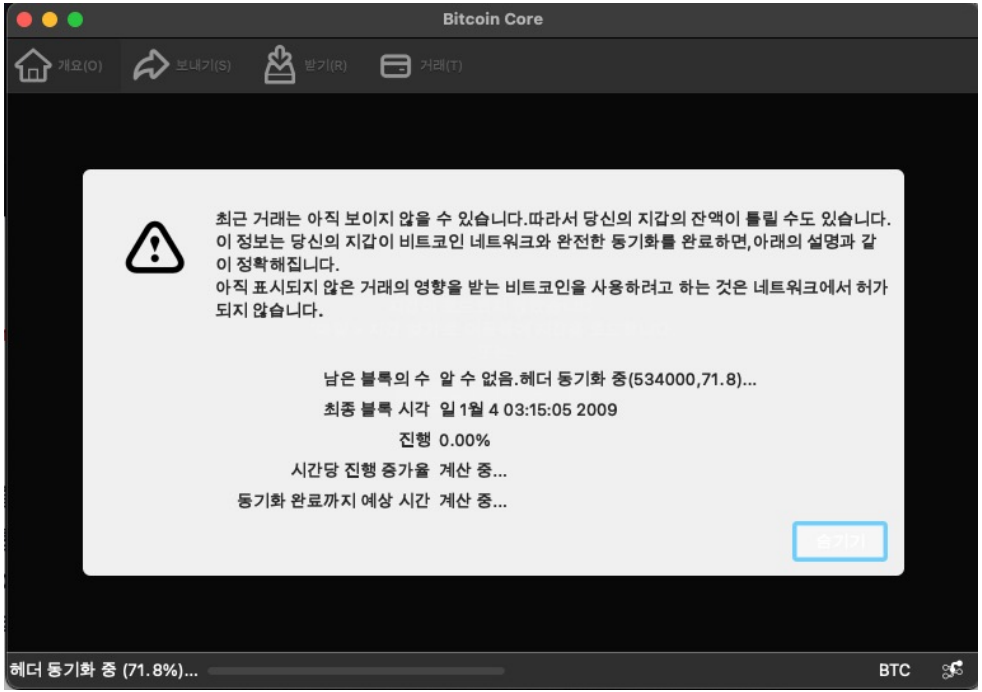
5) >> make

6) >> make install

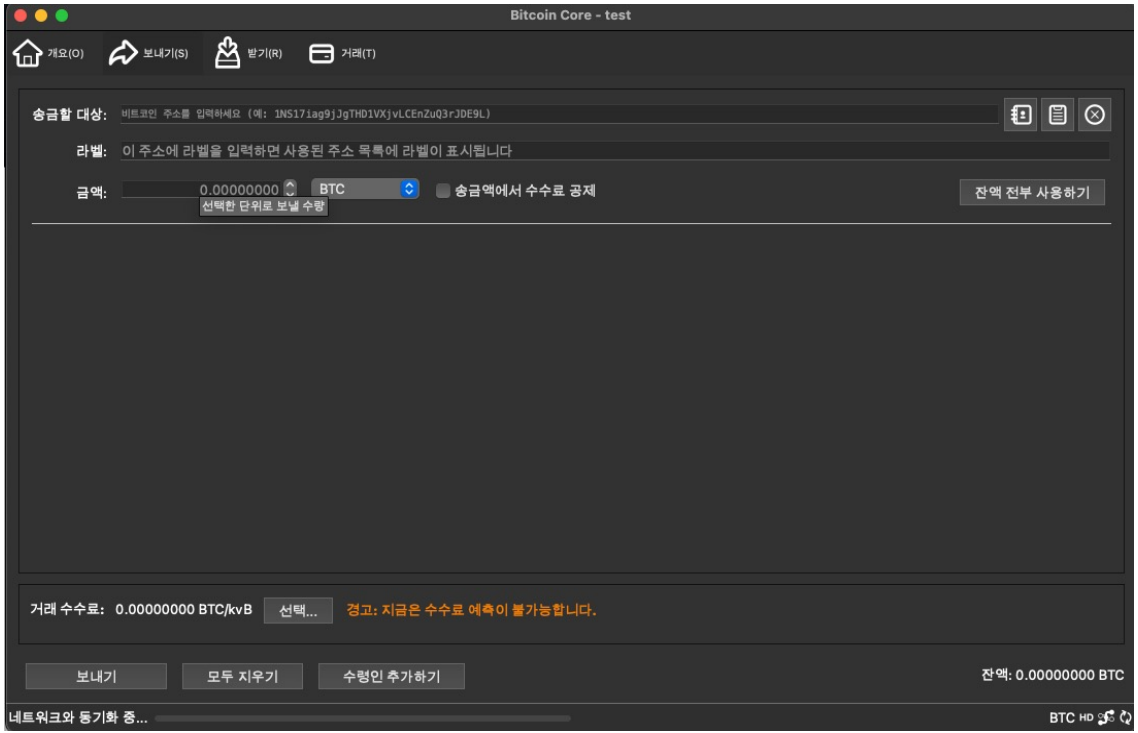
7) >> bitcoind --version

(https://github.com/bitcoin/bitcoin/blob/master/doc/build-unix.md)

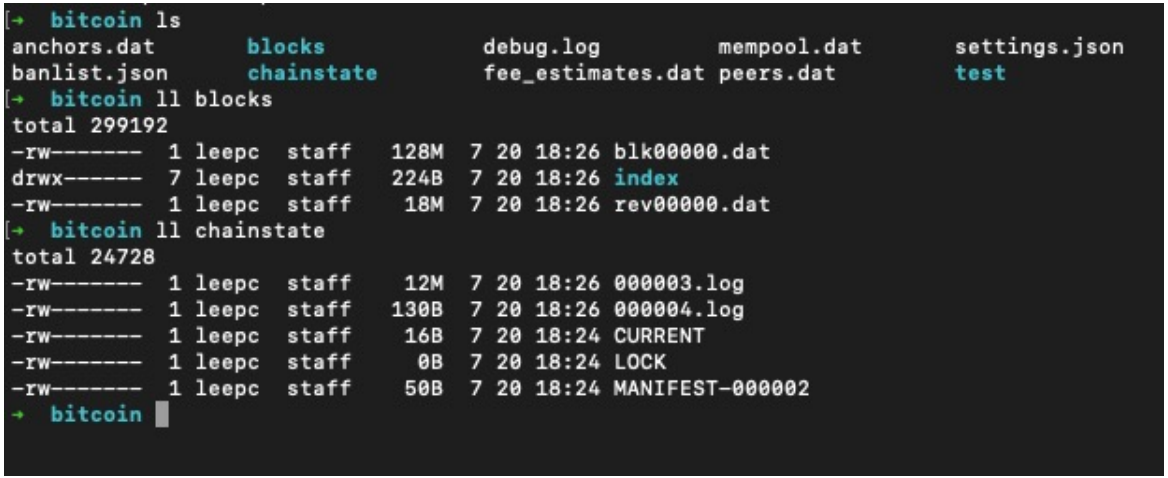
Bitcoin Core 실행화면



Bitcoin Core 실행화면



Bitcoin Core 실행화면



Bitcoin Core에서 BTC 전송

```
>> bitcoin-cli listunspent 1 99999999 '["mkrzDhhZtzQm8zgckSs4fMNrvtNJ66zaFe"]'
>> [{ "txid": "12b8e7ede4992f4d30f93idj3085746951d945e39f40becebd7c290af8c2e7ad", "vout": 1, "address":
"mkrzDhhZtzQm8zgckSs4fMNrvtNJ66zaFe", "account": "micz", "scriptPubKey":
"76a9143aa28e1740a6a5a2190975b6e7f1ad67aaec9a3988ac", "amount": 0.05000000, "confirmations": 94,
"spendable": true }, { "txid": "8443bc63b65d569ff9ekwm37sy3b67b9c7c6f8f386c3cdf372b260961b64ec9fc",
"vout": 1, "address": "mkrzDhhZtzQm8zgckSs4fMNrvtNJ66zaFe", "account": "micz", "scriptPubKey":
"76a9143aa28e1740a6a5a2190975b6e7f1ad67aaec9a3988ac", "amount": 0.01000000, "confirmations": 93,
"spendable": true }]
```

Bitcoin Core에서 BTC 전송

```
>> bitcoin-cli createrawtransaction '[{ "txid" :
"12b8e7ede4992f4d30f93idj3085746951d945e39f40becebd7c290af8c2e7ad", "vout" : 0 }]'
'{"mxh3H416KCRoBDiweSESew5YJyAk1nxLrN": 0.025, "mkrzDhhZtzQm8zgckSs4fMNrvtNJ66zaFe": 0.0245}’
>>
0100000001e34ac1e2baac09c366fce1c2245536bda8f7db0f6685862aecf53ebd69f9a89c0000000000ffffffff02a02526000
00000001976a914d90d36e98f62968d2bc9bbd68107564a156a9bcf88ac506225000000000001976a91407bdb518fa2e6089fd81
0235cf1100c9c13d1fd288ac00000000
```

Bitcoin Core에서 BTC 전송

```
>> bitcoin-cli signrawtransaction
0100000001e34ac1e2baac09c366fce1c2245536bda8f7db0f6685862aecf53ebd69f9a89c0000000000ffffffff02a02526000
00000001976a914d90d36e98f62968d2bc9bbd68107564a156a9bcf88ac506225000000000001976a91407bdb518fa2e6089fd81
0235cf1100c9c13d1fd288ac00000000
>> { "hex" :
"0100000001e34ac1e2baac09c366fce1c2245536bda8f7db0f6685862aecf53ebd69f9a89c000000006a47304402203e8a1652
2da80cef66bacfbc0c800c6d52c4a26d1d86a54e0a1b76d661f020c9022010397f00149f2a8fb2bc5bca52f2d7a7f87e3897a27
3ef54b277e4af52051a06012103c9700559f690c4a9182faa8bed88ad8a0c563777ac1d3f00fd44ea6c71dc5127ffffffff02a0
252600000000001976a914d90d36e98f62968d2bc9bbd68107564a156a9bcf88ac506225000000000001976a91407bdb518fa2e6
089fd810235cf1100c9c13d1fd288ac00000000", "complete" : true }
```

Bitcoin Core에서 BTC 전송

```
>> bitcoin-cli sendrawtransaction
0100000001e34ac1e2baac09c366fce1c2245536bda8f7db0f6685862aecf53ebd69f9a89c000000006a47304402203e8a16522
da80cef66bacfbc0c800c6d52c4a26d1d86a54e0a1b76d661f020c9022010397f00149f2a8fb2bc5bca52f2d7a7f87e3897a273
ef54b277e4af52051a06012103c9700559f690c4a9182faa8bed88ad8a0c563777ac1d3f00fd44ea6c71dc5127ffffffff02a02
526000000000001976a914d90d36e98f62968d2bc9bbd68107564a156a9bcf88ac506225000000000001976a91407bdb518fa2e60
89fd810235cf1100c9c13d1fd288ac00000000
```

RPC API Reference

Blockchain RPCs

- getbestblockhash
- getblock
- getblockchaininfo
- getblockcount
- getblockfilter
- getblockhash
- getblockheader
- getblockstats
- getchaintips
- getchaintxstats
- getdifficulty
- getmempoolancestors

Control RPCs

- getmemoryinfo
- getrpcinfo
- help
- logging
- stop
- uptime

Mining RPCs

- getblocktemplate
- getmininginfo
- getnetworkhashps
- prioritisetransaction
- submitblock
- submitheader

Network RPCs

- addnode
- clearbanned
- disconnectnode
- getaddednodeinfo
- getconnectioncount
- getnettotals
- getnetworkinfo
- getnodeaddresses
- getpeerinfo
- listbanned
- ping
- setban
- setnetworkactive

Rawtransactions RPCs

- analyzepsbt
- combinepsbt
- combinerawtransaction
- converttopsbt
- createpsbt
- createrawtransaction
- decodepsbt
- decoderawtransaction
- decodescript
- finalizepsbt
- fundrawtransaction
- getrawtransaction
- joinpsbts
- sendrawtransaction
- signrawtransactionwithkey
- testmempoolaccept
- utxoupdatepsbt

Generating RPCs

- generateblock
- generatetoaddress
- generatetodescriptor

Util RPCs

- createmultisig
- deriveaddresses
- estimatesmartfee
- getdescriptorinfo
- getindexinfo
- signmessagewithprivkey
- validateaddress
- verifymessage

출처) developer.bitcoin.org/reference/rpc/

Prune Mode

- Bitcoin 전체 Blockchain을 모두 보관하는게 부담되는 Full Node 사용자에게 제공되는 기능
- Bitcoind 에서 Prune-mode=on 을 하게 되면 최신 블록부터 특정 깊이의 Block 까지만 저장하도록 설정 가능
- 전체 BlockChain Sync & Validation 후에 적용
- 전체 Blockchain이 없어도 Mining 가능
- 특정 깊이 이전의 Block 정보 조회 불가능(getblock, getrawtransaction API)

  1) blk*.dat, rev*.dat, block index(leveldb) 삭제