한 번에 끝내는
블록체인 개발 A to Z

Chapter 1

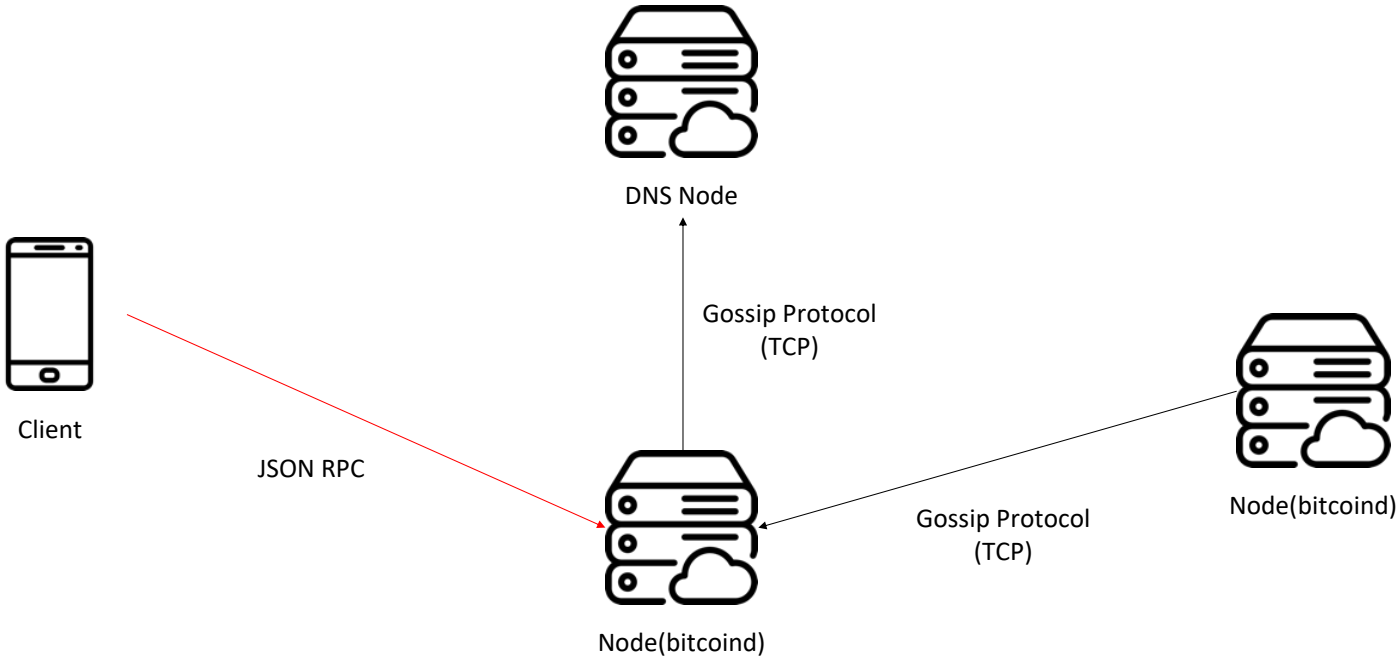
Blockchain 1.0 - Bitcoin

Chapter 1

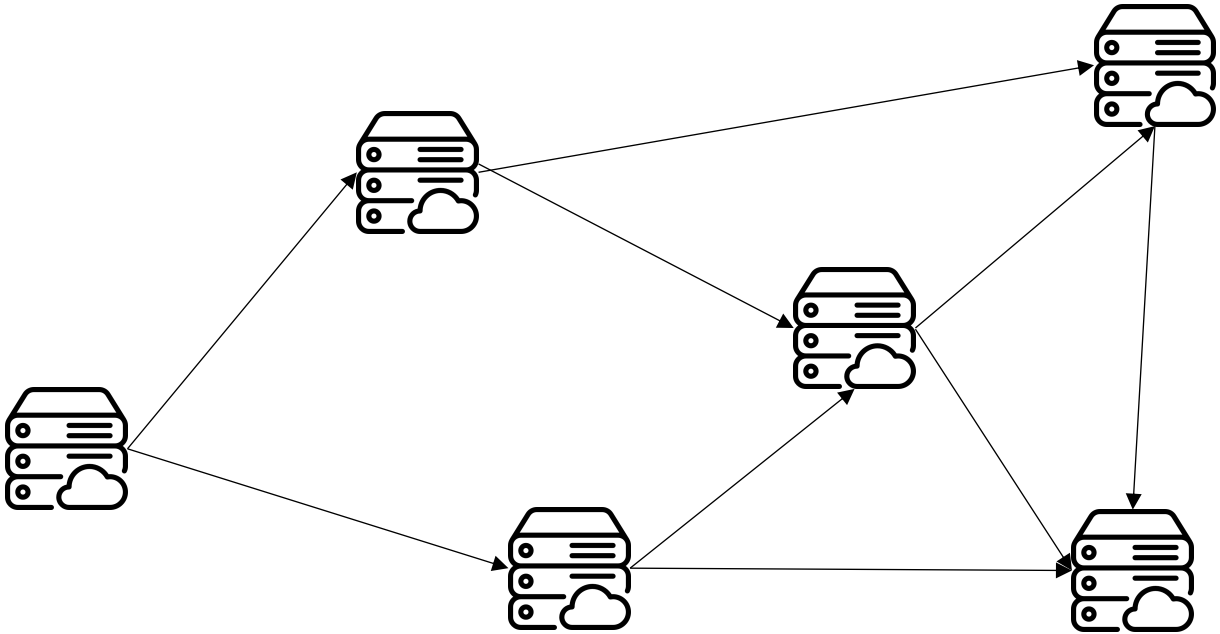
Blockchain 1.0 - Bitcoin

P2P Network

Bitcoin 통신 방법

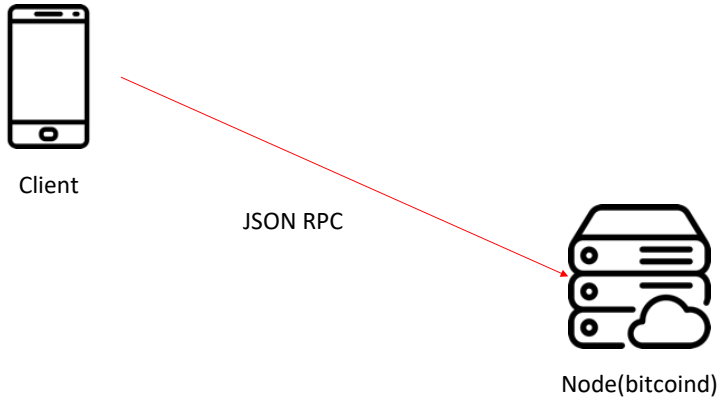


Bitcoin 통신 방법



Bitcoin Client와 통신

1) Bitcoind와 원격 연결(Port 8223) 한다.
2) 블록체인 데이터 조회
   → getblock, gettransaction
3) Wallet 관리
   → ImportPrivKey, GetBalance
4) Transaction 생성
   → sendtoaddress, signrawtransactionwitwallet



최초 네트워크 참여

1) DNS Address 에서 주소를 찾는다.
2) 해당 주소로 연결 시도(version/verack)
3) 실패 시 소스 내 하드코드 된 DNS Address에 연결 시도
4) 첫 노드 연결 성공시 해당 노드가 가지고 있는 노드 IP 리스트 수신
* 메인넷은 700여개, 테스트넷은 10개의 주소 리스트 보유

- seed.bitcoin.sipa.be
- dnsseed.bluematt.me
- dnsseed.bitcoin.dashjr.org
- seed.bitcoinstats.com
- seed.bitcoin.jonasschnelli.ch
- seed.btc.petertodd.org

DNS Node

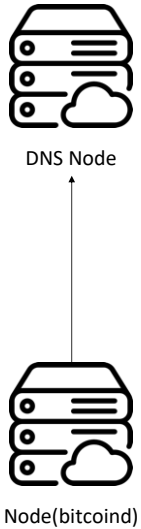
Node(bitcoind)

github.com/bitcoin/bitcoin/blob/v23.0/src/chainparamsseeds.h

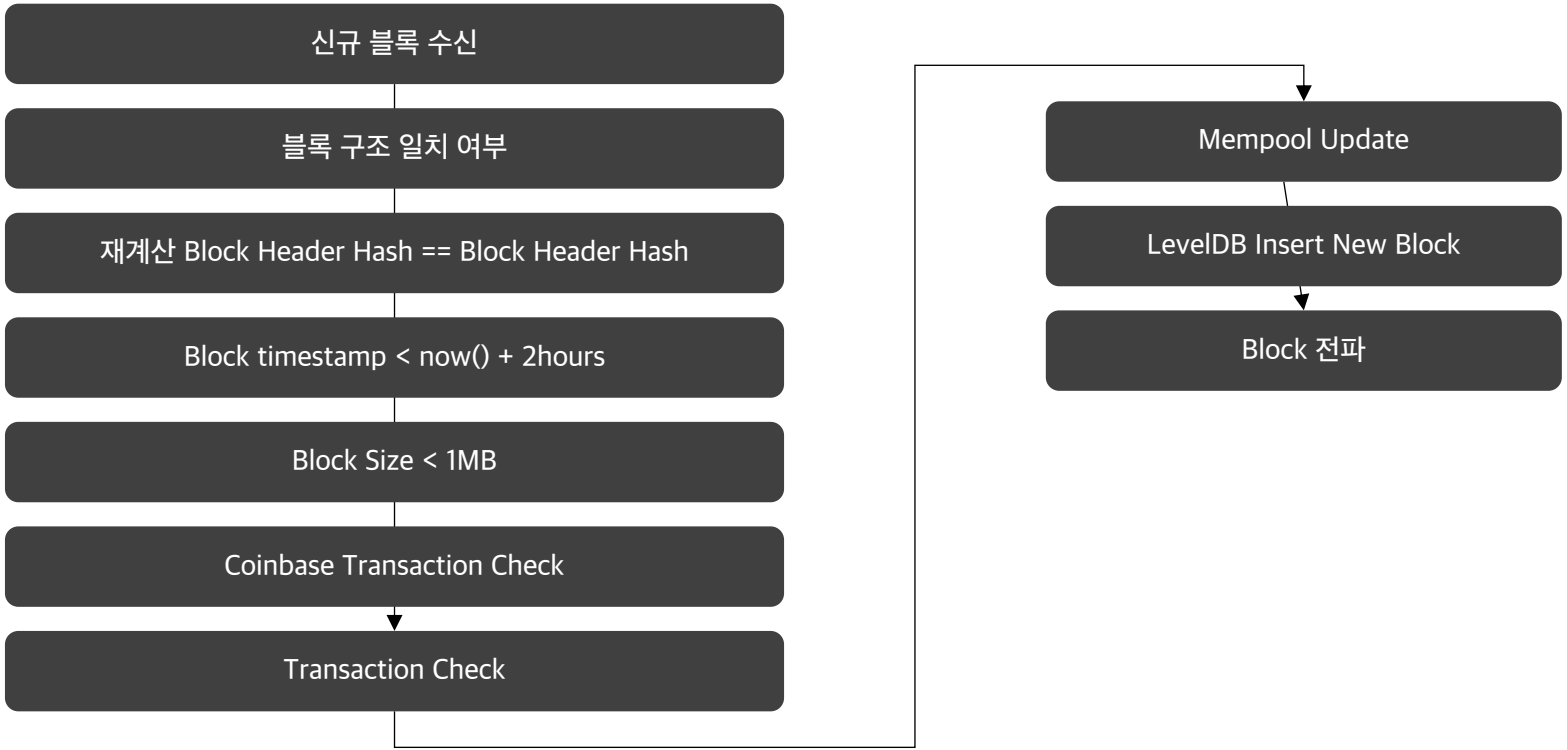
```
/**
 * List of fixed seed nodes for the bitcoin network
 * AUTOGENERATED by contrib/seeds/generate-seeds.py
 *
 * Each line contains a BIP155 serialized (networkID, addr, port) tuple.
 */
static const uint8_t chainparams_seed_main[] = {
    0x01,0x04,0x02,0x25,0x1e,0x90,0x22,0x49,
    0x01,0x04,0x02,0x8a,0xae,0x9e,0x20,0x8d,
    0x01,0x04,0x02,0x98,0x4e,0x7c,0x20,0x8d,
    0x01,0x04,0x05,0x08,0x12,0x9a,0x20,0x8d,
    0x01,0x04,0x05,0x2d,0x4a,0x32,0x20,0x8d,
```

Block Sync

1) Ping/Pong
   → Network에 Blockchain 다운 받기 위해 연결된 다른 노드들에 Ping 전송
2) Header Download (getheaders / headers)
   → 80bytes의 작은 Block Header 들을 먼저 다운.
3).Block Download(getdata)
   → Genesis Block +1 부터 시작하여 최근 Block 까지 Transaction을 포함한 전체 데이터를 다운로드 진행
4) Block Validation
   → Genesis Block부터 Block을 다운 받을 때 마다 검증 진행(Rule에 따라)

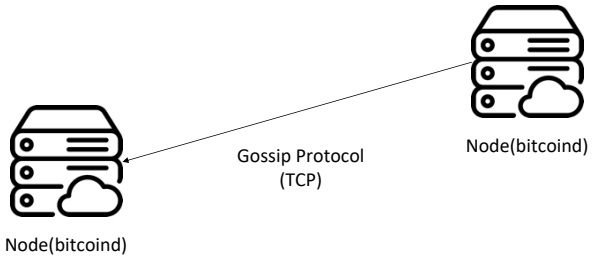


Block 검증

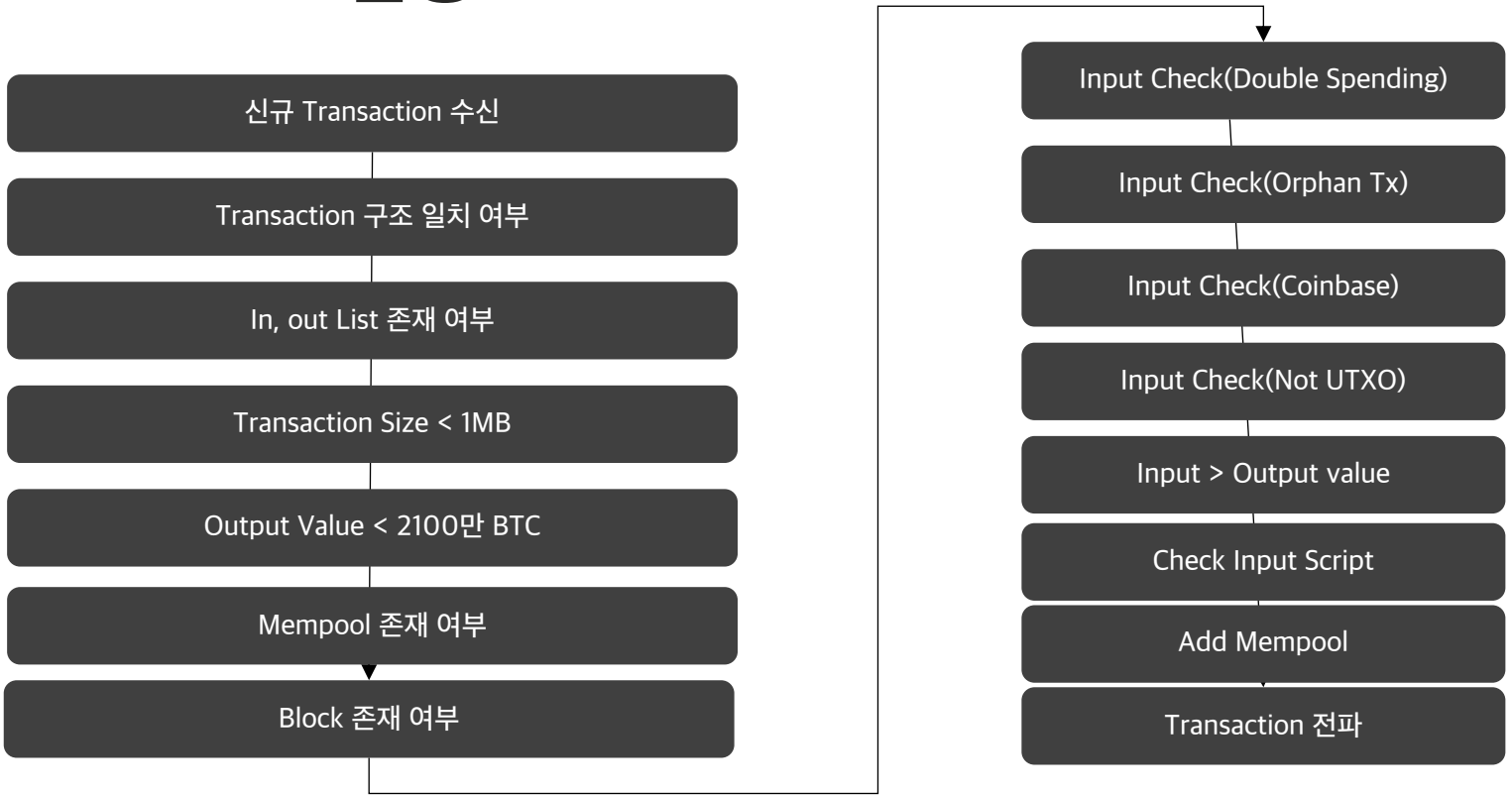

신규 블록 수신
블록 구조 일치 여부
재계산 Block Header Hash == Block Header Hash
Block timestamp < now() + 2hours
Block Size < 1MB
Coinbase Transaction Check
Transaction Check
Mempool Update
LevelDB Insert New Block
Block 전파

Transaction 전파

1) Transaction을 다른 노드에게서 전파 받는다.
2) 이미 받은 Transaction 인지 확인한다.
3) 없는 경우) 다른 노드에게 전파한다.(inv(msg_tx))
   → 새로운 Transaction txid를 전달한다.
4) 상대노드가 없는 경우 getdata를 요청 받는다.
   → MSG_TX와 txid를 전달 받는다.
5) 새로운 Transaction을 전달한다.
6) 연결된 모든 Node에게 전달될 때 까지 수행한다.



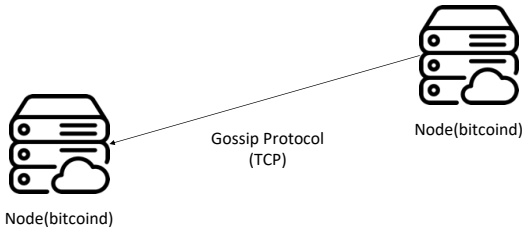
Transaction 검증



Block 전파

* Mining에 성공한 Block은 아래 방법 없이 Block 전체 데이터를 모든 노드에게 바로 전송

1) Ping
   → Network에 Blockchain 다운 받기 위해 연결된 다른 노드들에 Ping 전송
2) 전달 받은 Block Header를 전달한다.
3) 아직 전달 받지 못한 Block인 경우 headers와 getdata를 모두 요청한다.
   → headers에는 내가 가진 최신 Block Header List를 보낸다.
4) 새로운 Block과 그 사이 Block을 노드에게 전달한다.



합의 알고리즘의 필요성

Bitcoin P2P 네트워크 상에서의 흐름을 보면,
모두 나와 연결된 특정 Node에게서 전달 받은 Data를 신뢰하며 나의 Database를 업데이트 한다.

→ 내가 전달 받은 데이터가 조작되거나 하여 다른 노드와 다른 경우는 어떻게 할까?