

블록체인 명세서

- REQ 1-1) 가상 머신 구성

```
above with their current state. For more information about a specific VM, run `vagrant status NAME`.
```

```
C:\Users\multicampus\workspace>vagrant ssh eth0
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-154-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

System information as of Wed Sep  1 01:48:27 UTC 2021

System load:  0.11           Processes:            99
Usage of /:   2.8% of 38.71GB Users logged in:          0
Memory usage: 6%            IP address for enp0s3: 10.0.2.15
Swap usage:   0%            IP address for enp0s8: 192.168.50.10

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.
   https://ubuntu.com/blog/microk8s-memory-optimisation

0 updates can be applied immediately.

New release '20.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Aug 30 08:59:36 2021 from 10.0.2.2
vagrant@eth0:~$
```

- REQ 1-2) 이더리움 eth0 노드 구성
geth는 가상 머신 상에서 동작하도록 구축

REQ 1-3) 이더리움 eth1 노드 구성

```
Setting up ethereum (1.10.8+build27284+bionic) ...
vagrant@eth0:~$ geth version
Geth
Version: 1.10.8-stable
Git Commit: 26675454bf93bf904be7a43cce6b3f550115ff90
Architecture: amd64
Go Version: go1.16.4
Operating System: linux
COMPATIBLE
```

geth는 가상 머신 상에서 동작하도록 구축

```

Hit:3 http://archive.ubuntu.com/ubuntu bionic InRelease
Hit:4 http://archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:5 http://archive.ubuntu.com/ubuntu bionic-backports InRelease
Get:6 http://ppa.launchpad.net/ethereum/ethereum/ubuntu bionic/main amd64 Packages [2776
Get:7 http://ppa.launchpad.net/ethereum/ethereum/ubuntu bionic/main Translation-en [828
Fetched 19.0 kB in 2s (10.3 kB/s)
Reading package lists... Done
vagrant@ubuntu-bionic:~$ sudo apt-get install ethereum
Reading package lists... Done
Building dependency tree

```

- REQ 2-1) 계정 생성

--datadir 에 계정 생성 : geth 서버경로에 새 계정을 생성한다

geth --1-datadir ~/dev/blockchain account new

```

vagrant@eth0:~$ geth --datadir ~/dev/blockchain account new
INFO [09-01|06:50:52.107] Maximum peer count          ETH=50 LES=0 total=50
INFO [09-01|06:50:52.108] Smartcard socket not found, disabling err="stat /run/pcscd/pcscd.comm: no such file or directory"
Your new account is locked with a password. Please give a password. Do not forget this password.
Password:
Repeat password:
Your new key was generated

Public address of the key: 0x046198b8499e1069c7f11fDFBa3B5B8Da1eC7639
Path of the secret key file: /home/vagrant/dev/blockchain/keystore/UTC--2021-09-01T06-50-57.488854977Z--046198b8499e1069c7f11fdfba3b5b8da

- You can share your public address with anyone. Others need it to interact with you.
- You must NEVER share the secret key with anyone! The key controls access to your funds!
- You must BACKUP your key file! Without the key, it's impossible to access account funds!
- You must REMEMBER your password! Without the password, it's impossible to decrypt the key!

```

- REQ 2-2) genesis.json 파일로 설정해준다

블록 헤더 항목	설명
config	제네시스 블록의 설정값을 정의합니다.
chainid	블록체인을 식별하는 정수값을 입력합니다. "값이 비어있으면 안됩니다."
homesteadBlock	홈스테드를 적용하는 하드 포크 블록 번호를 뜻한다. 제네시스 블록은 0을 설정합니다.
eip155Block	이더리움 개선 제안(EIPs)의 155번 논의(한 번 이루어진 거래 정보를 이용해 재사용하는 리플레이 공격을 방지)를 적용한 하드 포크 블록 번호입니다.
eip158Block	이더리움 개선 제안(EIPs)의 158번 논의 (빈 계정 empty accounts)를 어떻게 다룰 것인지에 관한 프로토콜 변경)를 적용한 하드 포크 블록 번호입니다. 제네시스 블록은 0을 설정
nonce	mixHash와 함께 해당 블록에 충분한 양의 작업 증명 연산을 실행했음을 증명하는 값이다.
timestamp	블록체인에 저장한 시간입니다.. 유닉스의 타임 스탬프 형식입니다.
parent Hash	부모 블록 (이전 블록) 헤더의 해시값입니다.
gasLimit	해당 블록에서 사용할 수 있는 가스의 최대 크기입니다.
difficulty	해당 생성 난이도를 뜻합니다. 이전 블록의 생성 난이도와 타임스탬프, 블록 번호를 이용해 계산합니다.
mix Hash	nonce와 함께 해당 블록에 충분한 양의 작업 증명 연산을 실행했음을 증명합니다. 증명하는 시간을 단축하려고 일종의 중간값인 Pre-validation을 함께 넣어졌습니다. 가벼운 검증(Lightweight) 검증 때 활용합니다.
coinbase	블록을 생성하려고 채굴 했을 때 보상을 받는 계정 주소입니다.
alloc	제네시스 블록을 생성할 때 특정 계정에 미리 정해진 액수의 디어를 지급해 블록을 만들 수 있습니다.

파일안에 들어갈 각 요소들에 대한 설명

- REQ2-3) 채굴

```
To exit, press ctrl-d
> miner.start()
[INFO] [09-01|06:57:40.451] Updated mining threads threads=2
[INFO] [09-01|06:57:40.451] Transaction pool price threshold updated price=1,000,000,000
null
> [INFO] [09-01|06:57:40.452] Commit new mining work number=1 sealhash=3f7f82..7ef432 uncles=0 txs=0 gas=0 fees=0 elapsed="276.893us"
[INFO] [09-01|06:57:42.969] Successfully sealed new block number=1 sealhash=3f7f82..7ef432 hash=e845e5..e5cca0 elapsed=2.517s
[INFO] [09-01|06:57:43.044] □□□mined potential block number=1 hash=e845e5..e5cca0
[INFO] [09-01|06:57:42.981] Commit new mining work number=2 sealhash=1e53d9..817142 uncles=0 txs=0 gas=0 fees=0 elapsed="270.555us"
[INFO] [09-01|06:57:43.518] Generating ethash verification cache epoch=1 percentage=99 elapsed=3.018s
[INFO] [09-01|06:57:43.523] Generated ethash verification cache epoch=1 elapsed=3.024s
> [INFO] [09-01|06:57:45.029] Successfully sealed new block number=2 sealhash=1e53d9..817142 hash=bae78d..e27013 elapsed=2.048s
[INFO] [09-01|06:57:45.030] □□□mined potential block number=2 hash=bae78d..e27013
[INFO] [09-01|06:57:45.066] Commit new mining work number=3 sealhash=f74c6b..54a5ae uncles=0 txs=0 gas=0 fees=0 elapsed="337.794us"
[INFO] [09-01|06:57:50.100] Generating DAG in progress epoch=1 percentage=0 elapsed=6.575s
[INFO] [09-01|06:57:50.133] Successfully sealed new block number=3 sealhash=f74c6b..54a5ae hash=cf8017..943c28 elapsed=5.067s
[INFO] [09-01|06:57:50.134] □□□mined potential block number=3 hash=cf8017..943c28
[INFO] [09-01|06:57:50.136] Commit new mining work number=4 sealhash=ea0cf7..17beed uncles=0 txs=0 gas=0 fees=0 elapsed=2.105ms
[INFO] [09-01|06:57:58.191] Generating DAG in progress epoch=1 percentage=1 elapsed=14.665s
[INFO] [09-01|06:57:58.191] Generating DAG in progress epoch=1 percentage=1 elapsed=14.665s
> [INFO] [09-01|06:58:06.391] Successfully sealed new block number=4 sealhash=ea0cf7..17beed hash=499cf5..5f0d62 elapsed=16.254s
[INFO] [09-01|06:58:06.391] □□□mined potential block number=4 hash=499cf5..5f0d62
[INFO] [09-01|06:58:06.395] Commit new mining work number=5 sealhash=64518d..d371a3 uncles=0 txs=0 gas=0 fees=0 elapsed="276.682us"
[INFO] [09-01|06:58:07.391] Generating DAG in progress epoch=1 percentage=2 elapsed=23.866s
[INFO] [09-01|06:58:13.993] Generating DAG in progress epoch=1 percentage=3 elapsed=30.468s
[INFO] [09-01|06:58:14.164] Successfully sealed new block number=5 sealhash=64518d..d371a3 hash=2adf96..2242e7 elapsed=7.769s
[INFO] [09-01|06:58:16.213] □□□mined potential block number=5 hash=2adf96..2242e7
[INFO] [09-01|06:58:14.164] Commit new mining work number=6 sealhash=ec0a80..48d432 uncles=0 txs=0 gas=0 fees=0 elapsed="283.465us"
[INFO] [09-01|06:58:24.674] Successfully sealed new block number=6 sealhash=ec0a80..48d432 hash=ffbebc..a38272 elapsed=10.509s
[INFO] [09-01|06:58:24.674] □□□mined potential block number=6 hash=ffbebc..a38272
[INFO] [09-01|06:58:24.676] Commit new mining work number=7 sealhash=f87b03..6bb7c0 uncles=0 txs=0 gas=0 fees=0 elapsed=1.285ms
[INFO] [09-01|06:58:24.681] Generating DAG in progress epoch=1 percentage=4 elapsed=41.156s
[INFO] [09-01|06:58:30.108] Successfully sealed new block number=7 sealhash=f87b03..6bb7c0 hash=58a29c..ad77aa elapsed=5.432s
[INFO] [09-01|06:58:30.109] □□□mined potential block number=7 hash=58a29c..ad77aa
```

채굴시작: miner.start()

채굴종료: miner.stop()

명령어 : geth --networkid 921 --datadir ~/dev/blockchain --nodiscover --port 30303 --rpc --rpcport "8545" --maxpeers 2 --rpcaddr "0.0.0.0" --rpccorsdomain "*" --rpcapi "eth, net, web3, miner, debug, personal, rpc" console

```

modules: admin:1.0 debug:1.0 eth:1.0 ethash:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 export:1.0 web3:1.0
To exit, press ctrl-d
> eth.accounts
["0x046198b8499e1069c7f11fd6ba3b5b8da1ec7639", "0x17cf00bd768cd243c5168813d6e54f97285b2d4c"]
> eth.
eth._requestManager      eth.getBlockNumber      eth.getTransactionReceipt
eth.accounts             eth.getBlockTransactionCount  eth.getUncle
eth.blockNumber          eth.getBlockUncleCount    eth.getWork
eth.call                 eth.getCode               eth.hashrate
eth.chainId              eth.getCoinbase           eth.iban
eth.coinbase             eth.getCompilers          eth.icapNamereg
eth.compile              eth.getGasPrice           eth.isSyncing
eth.constructor          eth.getHashrate           eth.maxPriorityFeePerGas
eth.contract             eth.getHeaderByHash       eth.mining
eth.createAccessList     eth.getHeaderByNumber    eth.namereg
eth.defaultAccount       eth.getMaxPriorityFeePerGas  eth.pendingTransactions
eth.defaultBlock         eth.getMining             eth.protocolVersion
eth.estimateGas          eth.getPendingTransactions  eth.resend
eth.feeHistory           eth.getProof              eth.sendIBANTransaction
eth.fillTransaction      eth.getProtocolVersion    eth.sendRawTransaction
eth.filter               eth.getRawTransaction     eth.sendTransaction
eth.gasPrice             eth.getRawTransactionFromBlock  eth.sign
eth.getAccounts          eth.getStorageAt          eth.signTransaction
eth.getBalance           eth.getSyncing            eth.submitTransaction
eth.getBlock            eth.getTransaction        eth.submitWork
eth.getBlockByHash       eth.getTransactionCount   eth.syncing
eth.getBlockByNumber     eth.getTransactionFromBlock
> eth.getB
eth.getBalance           eth.getBlockByHash       eth.getBlockNumber      eth.getBlockUncle
eth.getBlock            eth.getBlockByNumber     eth.getBlockTransactionCount
> eth.getBalance(eth.accounts[0])
9420000000000000000
> eth.getBalance(eth.accounts[1])
0
>

```

- REQ 3-1) 트랜잭션 생성

personal.unlockAccount(from) 에러시

```

[09-03] [01:48:33.162] server personal_unlockAccount
= "account unlock with HTTP access is forbidden"
GoError: Error: account unlock with HTTP access is forbidden at web3.js:6357:37(47)
    at native
    at <eval>:1:24(3)
> exit

```

—allow-insecure-unlock 을 이용해 강제적으로 unlock시켜줌

```

[09-03] [01:52:22.140] Blockchain stopped
vagrant@eth0:~$ geth --networkid 921 --datadir ~/dev/blockchain --nodiscover --port 30303 --r
pc --rpcport "8545" --maxpeers 2 --rpcaddr "0.0.0.0" --rpcorsdomain "*" --rpcapi "eth, net,
web3, miner, debug, personal, rpc" --allow-insecure-unlock console

```

send

```

true
> tx_hash = eth.sendTransaction(tx)
INFO [09-03|01:56:53.425] Setting new local account          address=0x046198b8499e1069
C7f11FDfBa3B5B8Da1eC7639
INFO [09-03|01:56:53.426] Submitted transaction              hash=0xf615fe99bc423a7f12b
158218fe922a1e8fbddad83c3af36c10d9f7b015d3339 from=0x046198b8499e1069C7f11FDfBa3B5B8Da1eC7639
nonce=0 recipient=0x17cf00bd768cd243c5168813d6e54f97285b2d4c value=0
"0xf615fe99bc423a7f12b158218fe922a1e8fbddad83c3af36c10d9f7b015d3339"
>

```

- REQ 3-2) 트랜잭션 결과

트랜잭션 서명

```

raw: "0xf86d018504a817c80083015f909417cf00bd768cd243c5168813d6e54f97285b2d4c88016345785d8a0
008041a0c97af22f6551b65b66900c1bb381a5ccfedd1e0b24c8a99f6c97d7b06c6065eca062e369506e9b434709
4f952a4f26db2428a8fba48772e988b25ba03fe02a0e6",
tx: {
  gas: "0x15f90",
  gasPrice: "0x4a817c800",
  hash: "0xe5feb1e45fbcdc19c8952276b5649bd2fc2e5eee3a94eb11898783197bfe03c1",
  input: "0x",
  maxFeePerGas: null,
  maxPriorityFeePerGas: null,
  nonce: "0x1",
  r: "0xc97af22f6551b65b66900c1bb381a5ccfedd1e0b24c8a99f6c97d7b06c6065ec",
  s: "0x62e369506e9b43470914f952a4f26db2428a8fba48772e988b25ba03fe02a0e6",
  to: "0x17cf00bd768cd243c5168813d6e54f97285b2d4c",
  type: "0x0",
  v: "0x41",
  value: "0x16345785d8a0000"
}

```

트랜잭션 결과

```

function()
> eth.getTransaction(tx_hash)
{
  blockHash: null,
  blockNumber: null,
  from: "0x046198b8499e1069c7f11fdFba3b5b8da1ec7639",
  gas: 90000,
  gasPrice: 20000000000,
  hash: "0xe5feb1e45fbcdc19c8952276b5649bd2fc2e5eee3a94eb11898783197bfe03c1",
  input: "0x",
  nonce: 1,
  r: "0xc97af22f6551b65b66900c1bb381a5ccfedd1e0b24c8a99f6c97d7b06c6065ec",
  s: "0x62e369506e9b43470914f952a4f26db2428a8fba48772e988b25ba03fe02a0e6",
  to: "0x17cf00bd768cd243c5168813d6e54f97285b2d4c",
  transactionIndex: null,
  type: "0x0",
  v: "0x41",
  value: 1000000000000000000
}

```

