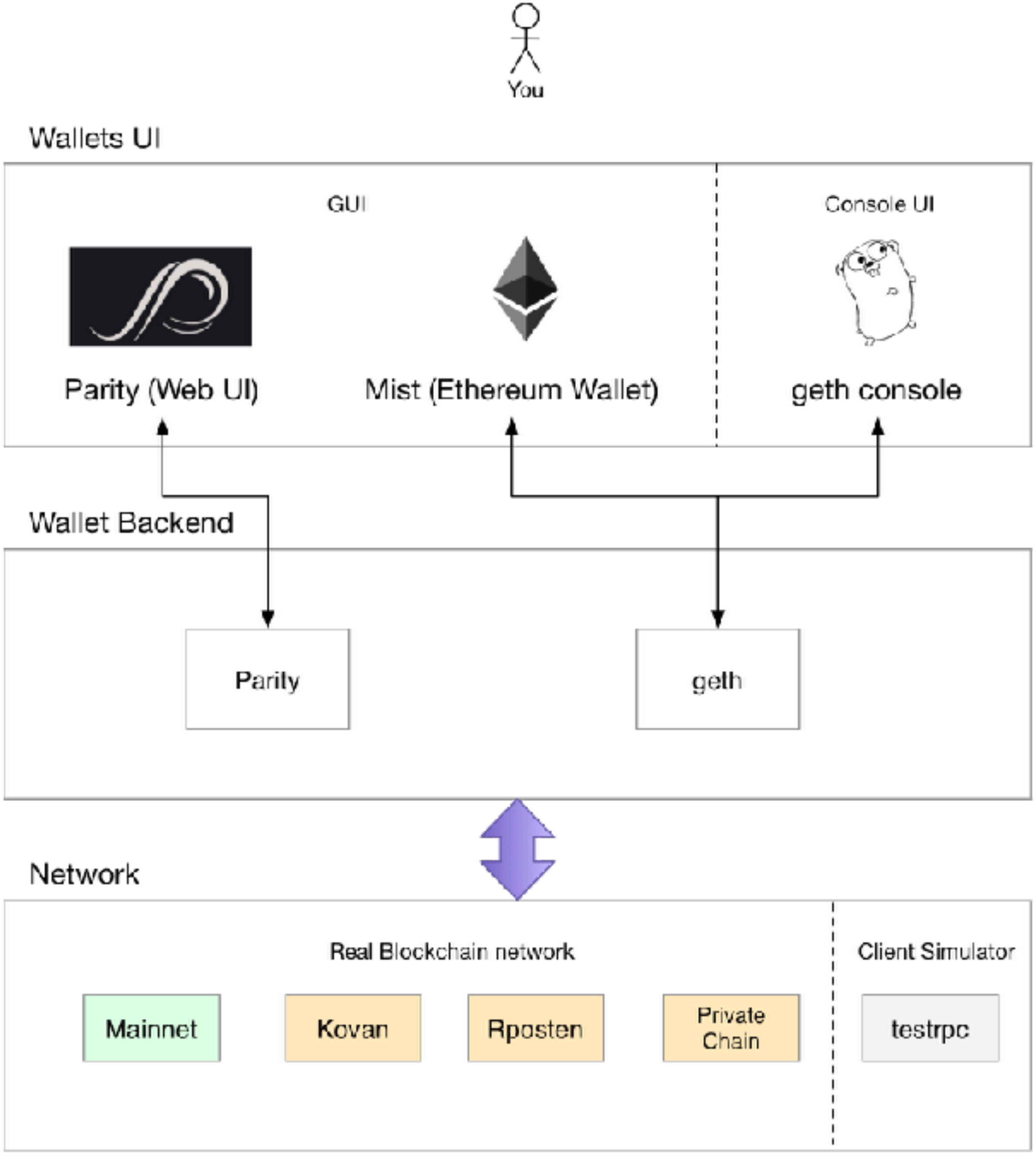
使用Geth佈建Ethereum Private Chain與挖礦

盧瑞山 教授、唐林誼


You
Wallets UI
GUI
Console UI
Parity (Web UI)
Mist (Ethereum Wallet)
geth console
Wallet Backend
Parity
geth
Network
Real Blockchain network
Client Simulator
Mainnet
Kovan
Rposten
Private Chain
testrpc

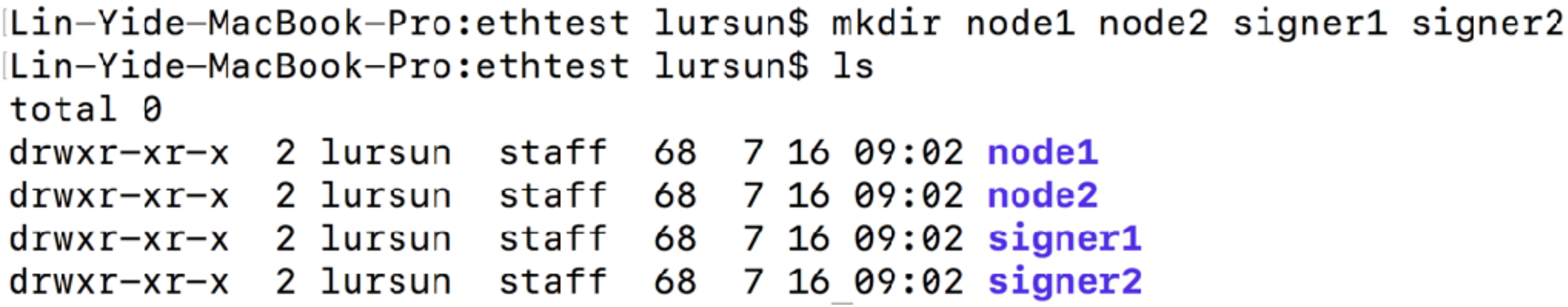
準備工具geth

- 可以在這下載到geth,亦可自行編譯,本範例使用 1.6.6
  https://ethereum.github.io/go-ethereum/downloads/

- Mac OS 可以
  brew tap ethereum/ethereum
  brew install ethereum

建立區塊鏈目錄

- 先建立好區塊鏈目錄 mkdir node1 node2 signer1 signer2



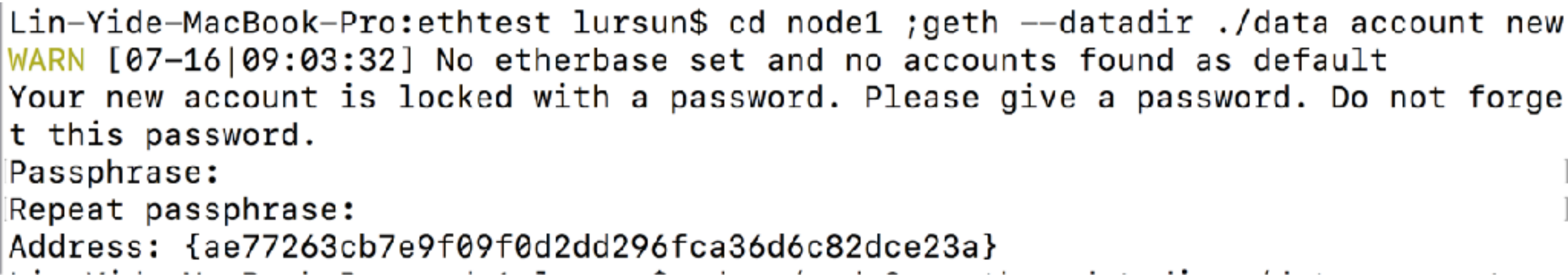
```
[Lin-Yide-MacBook-Pro:ethtest lursun$ mkdir node1 node2 signer1 signer2
[Lin-Yide-MacBook-Pro:ethtest lursun$ ls
total 0
drwxr-xr-x  2 lursun  staff  68  7 16 09:02 node1
drwxr-xr-x  2 lursun  staff  68  7 16 09:02 node2
drwxr-xr-x  2 lursun  staff  68  7 16 09:02 signer1
drwxr-xr-x  2 lursun  staff  68  7 16 09:02 signer2
```

建立Ethereum帳號

- cd node1 ;geth --datadir ./data account new
  設定密碼即會產生一組帳號，帳號密碼記住之後用到

- 如法炮製
  cd ../node2 ;geth --datadir ./data account new
  cd ../signer1 ;geth --datadir ./data account new
  cd ../signer2 ;geth --datadir ./data account new

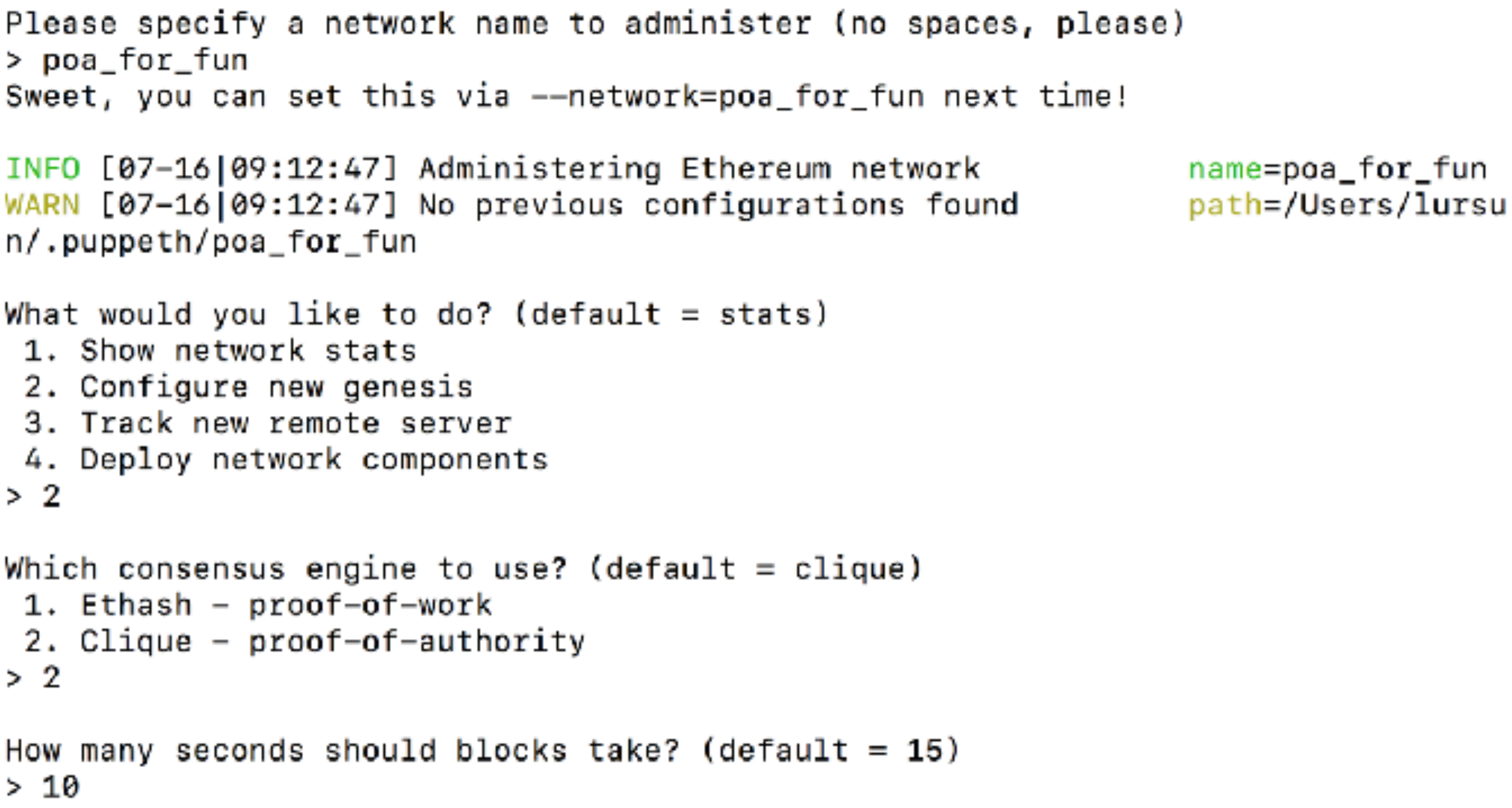
- 範例四組帳號（隨機）
  ae77263cb7e9f09f0d2dd296fca36d6c82dce23a
  311b96ecfcfbd9dda3b8da45144391550c2a1e96
  02176d46a71ffab971c35dbfea551d56d61c2666
  4ac7b40218f57b82386c0ee45f70c4180310d229



```
Lin-Yide-MacBook-Pro:ethtest lursun$ cd node1 ;geth --datadir ./data account new
WARN [07-16|09:03:32] No etherbase set and no accounts found as default
Your new account is locked with a password. Please give a password. Do not forge
t this password.
Passphrase:
Repeat passphrase:
Address: {ae77263cb7e9f09f0d2dd296fca36d6c82dce23a}
```

建立創世區塊

- 使用 puppeth 這互動式工具
- # puppeth
- 輸入網路名稱
  >poa_for_fun
- 選擇 設定創世區塊
  >2
- 選擇 Clique PoA共識
  >2
- 設定出塊時間(秒)
  >10



```
Please specify a network name to administer (no spaces, please)
> poa_for_fun
Sweet, you can set this via --network=poa_for_fun next time!

INFO [07-16|09:12:47] Administering Ethereum network           name=poa_for_fun
WARN [07-16|09:12:47] No previous configurations found         path=/Users/lursu
n/.puppeth/poa_for_fun

What would you like to do? (default = stats)
 1. Show network stats
 2. Configure new genesis
 3. Track new remote server
 4. Deploy network components
> 2

Which consensus engine to use? (default = clique)
 1. Ethash - proof-of-work
 2. Clique - proof-of-authority
> 2

How many seconds should blocks take? (default = 15)
> 10
```

- 指定打包角色
  >前一頁 某個 Signer 帳號

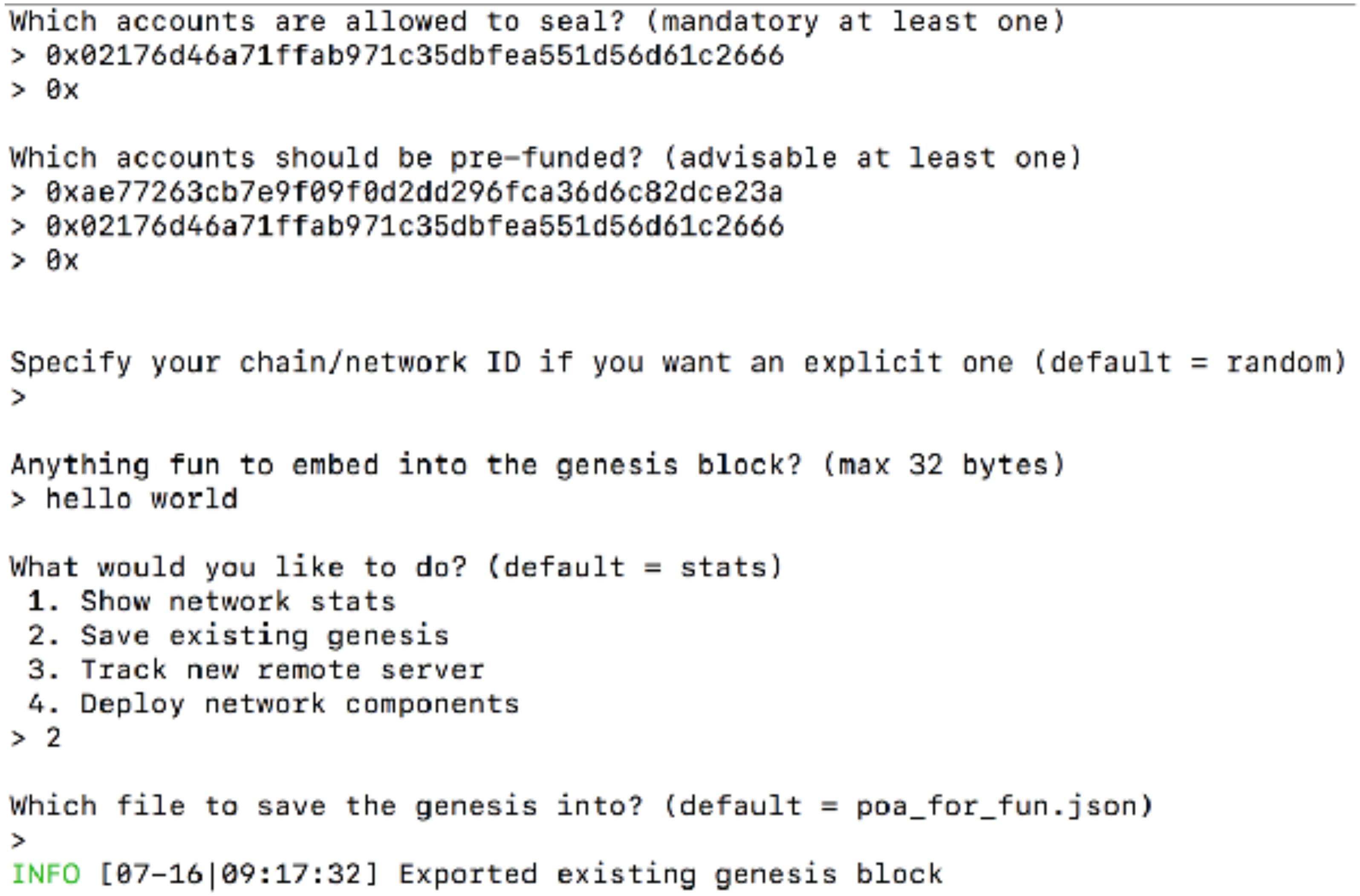
- 指定幾個帳號一點ether(以太幣)
  >前一頁 某個 Signer 帳號 和 Node帳號

- 設定網路ID
  >直接Enter 用隨機

- 寫一些資訊到創世塊
  >皆可

- 選擇存擋
  >2

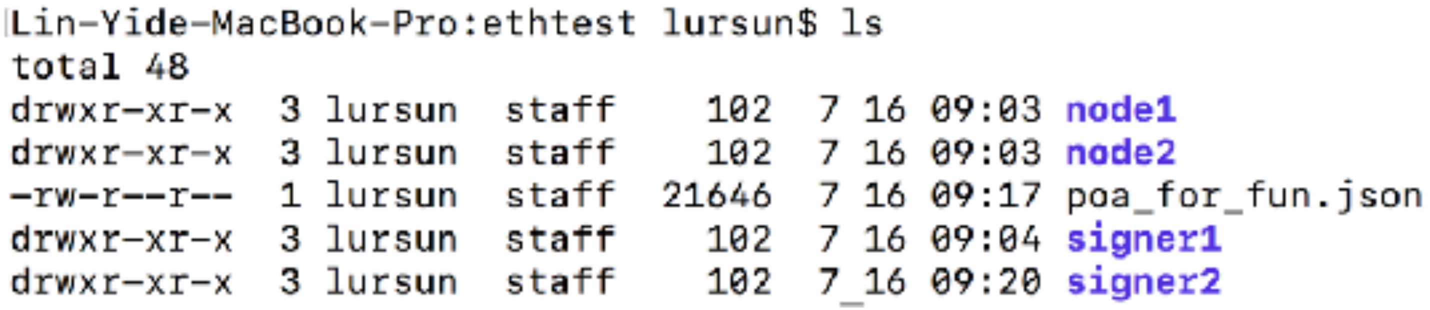
- 檔名
  >直接Enter 預設



```
Which accounts are allowed to seal? (mandatory at least one)
> 0x02176d46a71ffab971c35dbfea551d56d61c2666
> 0x

Which accounts should be pre-funded? (advisable at least one)
> 0xae77263cb7e9f09f0d2dd296fca36d6c82dce23a
> 0x02176d46a71ffab971c35dbfea551d56d61c2666
> 0x


Specify your chain/network ID if you want an explicit one (default = random)
>

Anything fun to embed into the genesis block? (max 32 bytes)
> hello world

What would you like to do? (default = stats)
 1. Show network stats
 2. Save existing genesis
 3. Track new remote server
 4. Deploy network components
> 2

Which file to save the genesis into? (default = poa_for_fun.json)
>
INFO [07-16|09:17:32] Exported existing genesis block
```

- Ctrl + c 跳離

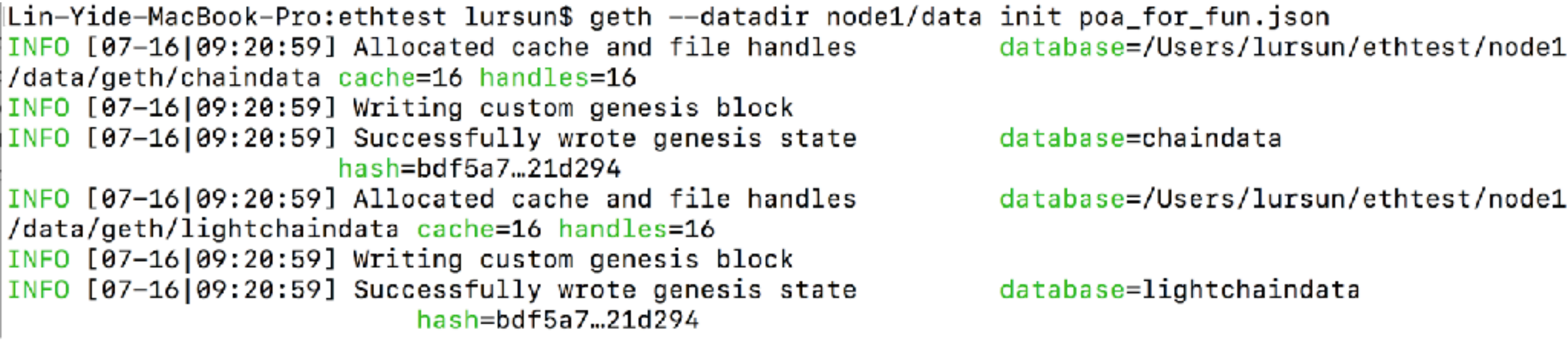
- ls
  node1 node2 signer1 signer2 xxxxxxx.json



```
Lin-Yide-MacBook-Pro:ethtest lursun$ ls
total 48
drwxr-xr-x  3 lursun  staff    102  7 16 09:03 node1
drwxr-xr-x  3 lursun  staff    102  7 16 09:03 node2
-rw-r--r--  1 lursun  staff  21646  7 16 09:17 poa_for_fun.json
drwxr-xr-x  3 lursun  staff    102  7 16 09:04 signer1
drwxr-xr-x  3 lursun  staff    102  7 16 09:20 signer2
```

初始化各目錄

- geth --datadir node1/data init xxxxxxx.json
- geth --datadir node2/data init xxxxxxx.json
- geth --datadir signer1/data init xxxxxxx.json
- geth --datadir signer2/data init xxxxxxx.json

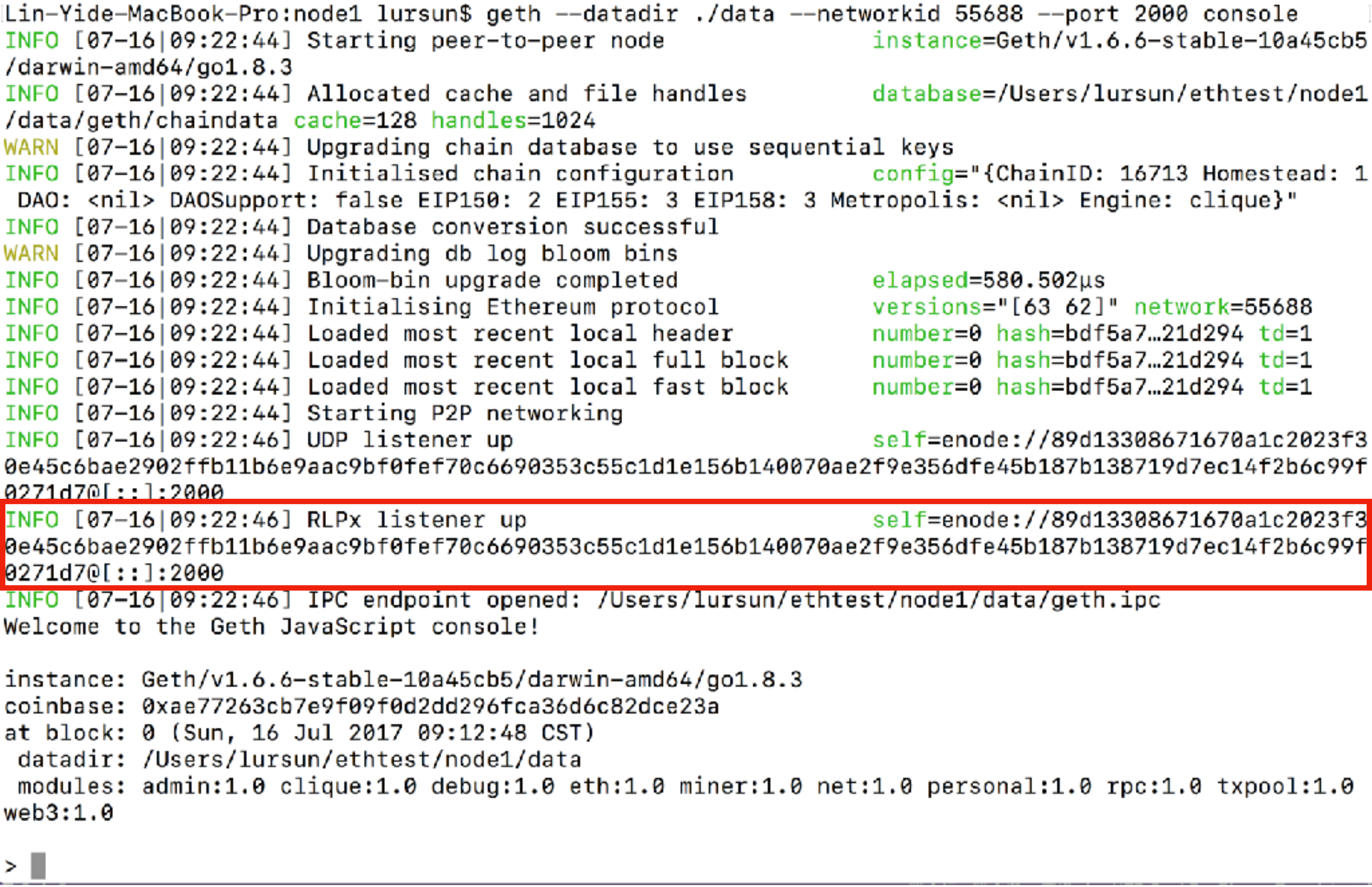


```
Lin-Yide-MacBook-Pro:ethtest lursun$ geth --datadir node1/data init poa_for_fun.json
INFO [07-16|09:20:59] Allocated cache and file handles         database=/Users/lursun/ethtest/node1
/data/geth/chaindata cache=16 handles=16
INFO [07-16|09:20:59] Writing custom genesis block
INFO [07-16|09:20:59] Successfully wrote genesis state         database=chaindata
                   hash=bdf5a7…21d294
INFO [07-16|09:20:59] Allocated cache and file handles         database=/Users/lursun/ethtest/node1
/data/geth/lightchaindata cache=16 handles=16
INFO [07-16|09:20:59] Writing custom genesis block
INFO [07-16|09:20:59] Successfully wrote genesis state         database=lightchaindata
                       hash=bdf5a7…21d294
```

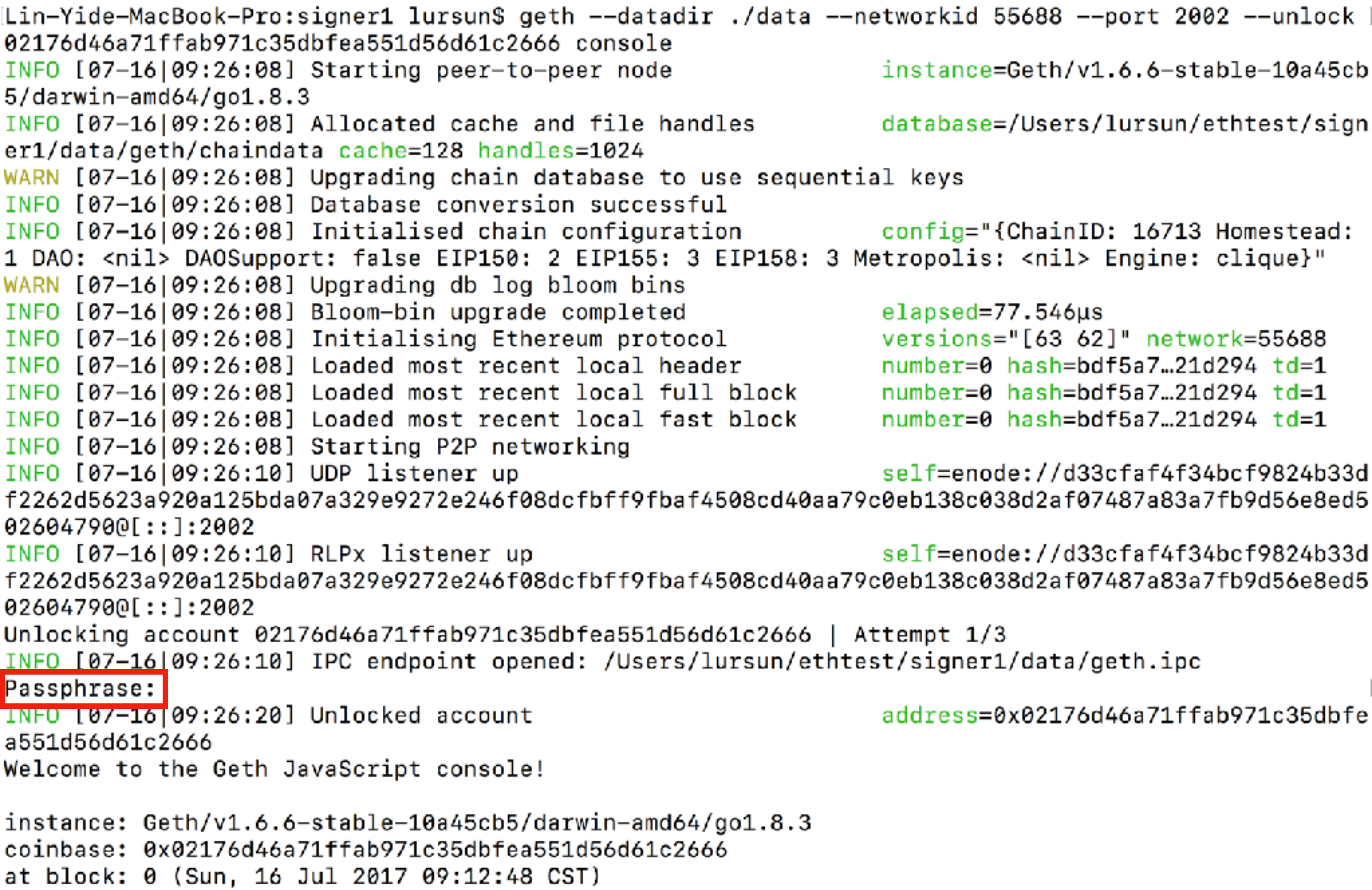
啟動節點

- 移動到各節點目錄
  geth --datadir ./data --networkid 55688 --port 2000 console
  geth --datadir ./data --networkid 55688 --port 2001 console
  geth --datadir ./data --networkid 55688 --port 2002 console
  geth --datadir ./data --networkid 55688 --port 2003 console

- 注意 要打包的 要改成
  geth --datadir ./data --networkid 55688 --port 200x --unlock 帳號 console
  然後要輸入密碼



```
Lin-Yide-MacBook-Pro:node1 lursun$ geth --datadir ./data --networkid 55688 --port 2000 console
INFO [07-16|09:22:44] Starting peer-to-peer node               instance=Geth/v1.6.6-stable-10a45cb5
/darwin-amd64/go1.8.3
INFO [07-16|09:22:44] Allocated cache and file handles         database=/Users/lursun/ethtest/node1
/data/geth/chaindata cache=128 handles=1024
WARN [07-16|09:22:44] Upgrading chain database to use sequential keys
INFO [07-16|09:22:44] Initialised chain configuration          config="{ChainID: 16713 Homestead: 1
 DAO: <nil> DAOSupport: false EIP150: 2 EIP155: 3 EIP158: 3 Metropolis: <nil> Engine: clique}"
INFO [07-16|09:22:44] Database conversion successful
WARN [07-16|09:22:44] Upgrading db log bloom bins
INFO [07-16|09:22:44] Bloom-bin upgrade completed              elapsed=580.502µs
INFO [07-16|09:22:44] Initialising Ethereum protocol           versions="[63 62]" network=55688
INFO [07-16|09:22:44] Loaded most recent local header          number=0 hash=bdf5a7…21d294 td=1
INFO [07-16|09:22:44] Loaded most recent local full block      number=0 hash=bdf5a7…21d294 td=1
INFO [07-16|09:22:44] Loaded most recent local fast block      number=0 hash=bdf5a7…21d294 td=1
INFO [07-16|09:22:44] Starting P2P networking
INFO [07-16|09:22:46] UDP listener up                          self=enode://89d13308671670a1c2023f3
0e45c6bae2902ffb11b6e9aac9bf0fef70c6690353c55c1d1e156b140070ae2f9e356dfe45b187b138719d7ec14f2b6c99f
0271d7@[::]:2000
INFO [07-16|09:22:46] RLPx listener up                         self=enode://89d13308671670a1c2023f3
0e45c6bae2902ffb11b6e9aac9bf0fef70c6690353c55c1d1e156b140070ae2f9e356dfe45b187b138719d7ec14f2b6c99f
0271d7@[::]:2000
INFO [07-16|09:22:46] IPC endpoint opened: /Users/lursun/ethtest/node1/data/geth.ipc
Welcome to the Geth JavaScript console!

instance: Geth/v1.6.6-stable-10a45cb5/darwin-amd64/go1.8.3
coinbase: 0xae77263cb7e9f09f0d2dd296fca36d6c82dce23a
at block: 0 (Sun, 16 Jul 2017 09:12:48 CST)
 datadir: /Users/lursun/ethtest/node1/data
 modules: admin:1.0 clique:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txpool:1.0
web3:1.0

> 
```



```
Lin-Yide-MacBook-Pro:signer1 lursun$ geth --datadir ./data --networkid 55688 --port 2002 --unlock
02176d46a71ffab971c35dbfea551d56d61c2666 console
INFO [07-16|09:26:08] Starting peer-to-peer node               instance=Geth/v1.6.6-stable-10a45cb
5/darwin-amd64/go1.8.3
INFO [07-16|09:26:08] Allocated cache and file handles         database=/Users/lursun/ethtest/sign
er1/data/geth/chaindata cache=128 handles=1024
WARN [07-16|09:26:08] Upgrading chain database to use sequential keys
INFO [07-16|09:26:08] Database conversion successful
INFO [07-16|09:26:08] Initialised chain configuration          config="{ChainID: 16713 Homestead:
1 DAO: <nil> DAOSupport: false EIP150: 2 EIP155: 3 EIP158: 3 Metropolis: <nil> Engine: clique}"
WARN [07-16|09:26:08] Upgrading db log bloom bins
INFO [07-16|09:26:08] Bloom-bin upgrade completed              elapsed=77.546µs
INFO [07-16|09:26:08] Initialising Ethereum protocol           versions="[63 62]" network=55688
INFO [07-16|09:26:08] Loaded most recent local header          number=0 hash=bdf5a7…21d294 td=1
INFO [07-16|09:26:08] Loaded most recent local full block      number=0 hash=bdf5a7…21d294 td=1
INFO [07-16|09:26:08] Loaded most recent local fast block      number=0 hash=bdf5a7…21d294 td=1
INFO [07-16|09:26:08] Starting P2P networking
INFO [07-16|09:26:10] UDP listener up                          self=enode://d33cfaf4f34bcf9824b33d
f2262d5623a920a125bda07a329e9272e246f08dcfbff9fbaf4508cd40aa79c0eb138c038d2af07487a83a7fb9d56e8ed5
02604790@[::]:2002
INFO [07-16|09:26:10] RLPx listener up                         self=enode://d33cfaf4f34bcf9824b33d
f2262d5623a920a125bda07a329e9272e246f08dcfbff9fbaf4508cd40aa79c0eb138c038d2af07487a83a7fb9d56e8ed5
02604790@[::]:2002
Unlocking account 02176d46a71ffab971c35dbfea551d56d61c2666 | Attempt 1/3
INFO [07-16|09:26:10] IPC endpoint opened: /Users/lursun/ethtest/signer1/data/geth.ipc
Passphrase:
INFO [07-16|09:26:20] Unlocked account                         address=0x02176d46a71ffab971c35dbfe
a551d56d61c2666
Welcome to the Geth JavaScript console!

instance: Geth/v1.6.6-stable-10a45cb5/darwin-amd64/go1.8.3
coinbase: 0x02176d46a71ffab971c35dbfea551d56d61c2666
at block: 0 (Sun, 16 Jul 2017 09:12:48 CST)
```

連線各節點

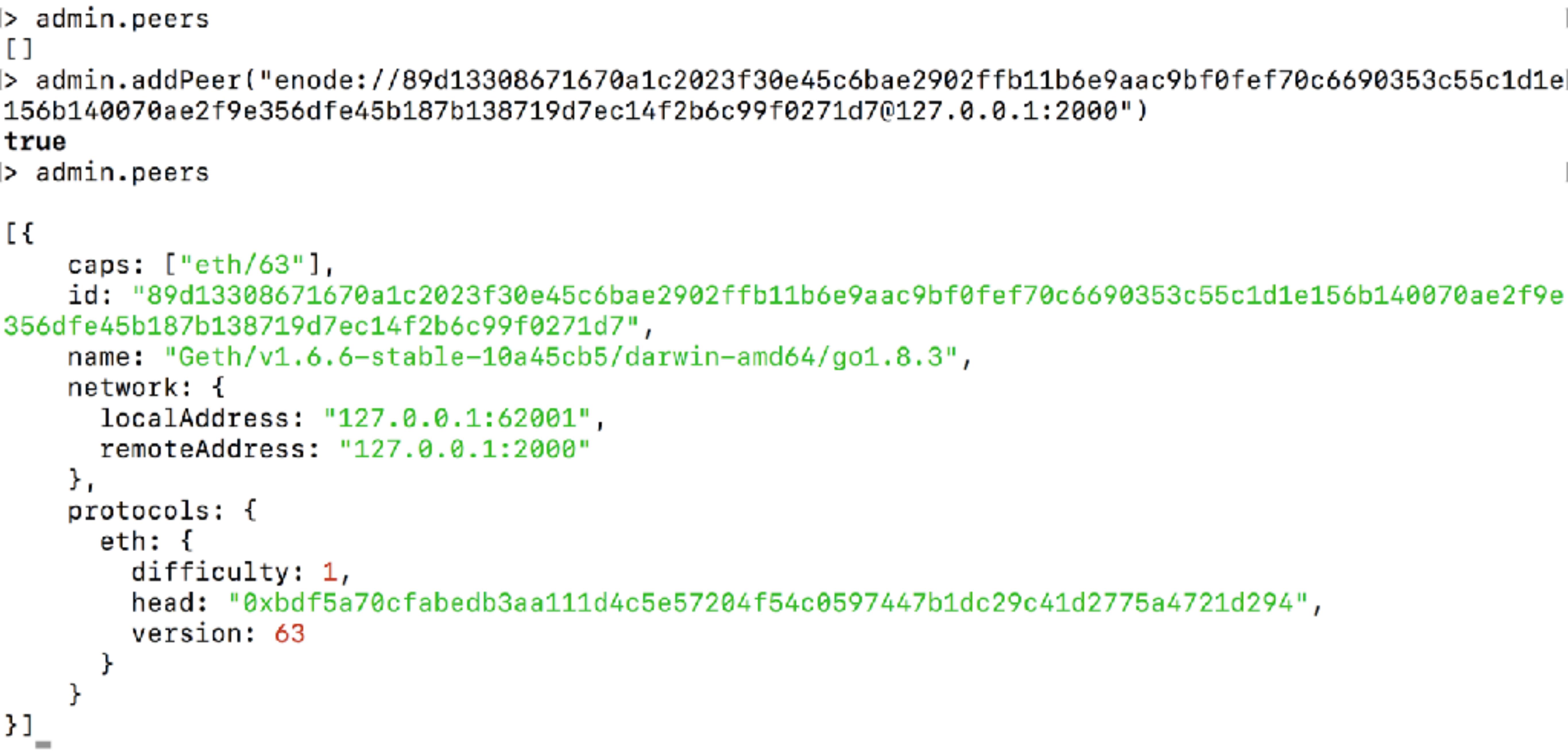
- 其中一個找到 RLPx listener up 這行 複製 enode://＊＊＊＊＊＊＊＊＊@[::]:200x

- 改成 enode://＊＊＊＊＊＊＊＊＊@127.0.0.1:200x

- 可以用 admin.peers 查看節點變化(不含自己)

- 在其他各節點console 下指令

```
admin.addPeer("enode://＊＊＊＊＊＊＊＊＊@127.0.0.1:200x")
```



```
> admin.peers
[]
> admin.addPeer("enode://89d13308671670a1c2023f30e45c6bae2902ffb11b6e9aac9bf0fef70c6690353c55c1d1e
156b140070ae2f9e356dfe45b187b138719d7ec14f2b6c99f0271d7@127.0.0.1:2000")
true
> admin.peers

[{
    caps: ["eth/63"],
    id: "89d13308671670a1c2023f30e45c6bae2902ffb11b6e9aac9bf0fef70c6690353c55c1d1e156b140070ae2f9e
356dfe45b187b138719d7ec14f2b6c99f0271d7",
    name: "Geth/v1.6.6-stable-10a45cb5/darwin-amd64/go1.8.3",
    network: {
      localAddress: "127.0.0.1:62001",
      remoteAddress: "127.0.0.1:2000"
    },
    protocols: {
      eth: {
        difficulty: 1,
        head: "0xbdf5a70cfabedb3aa111d4c5e57204f54c0597447b1dc29c41d2775a4721d294",
        version: 63
      }
    }
}]
```

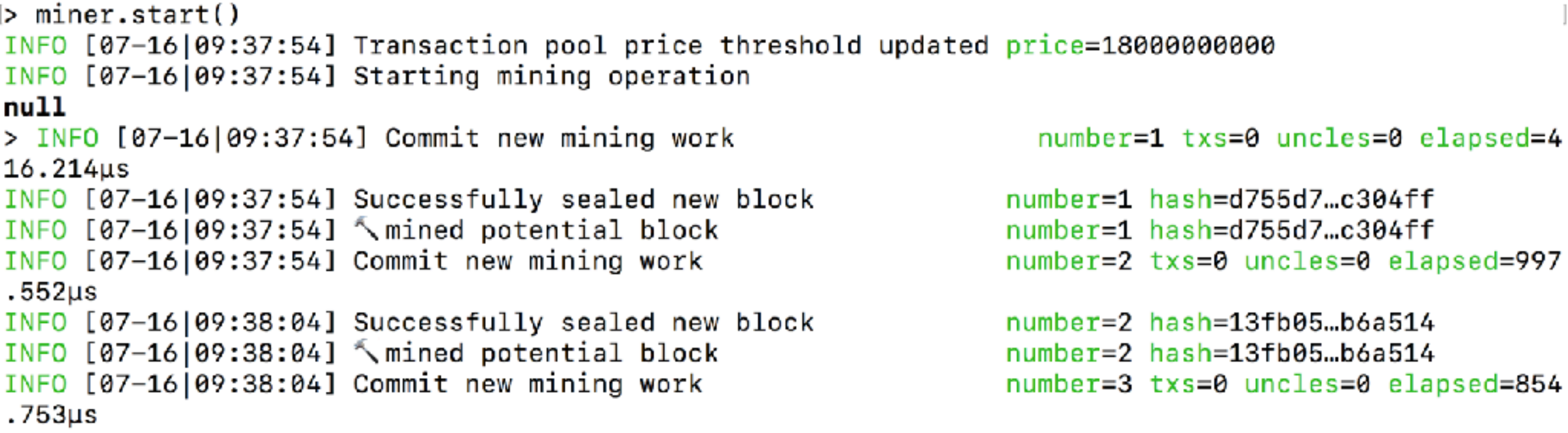
- 最後被連線的 admin.peers 有三個節點

- 而主動連線的 admin.peers 只有一個節點

挖礦

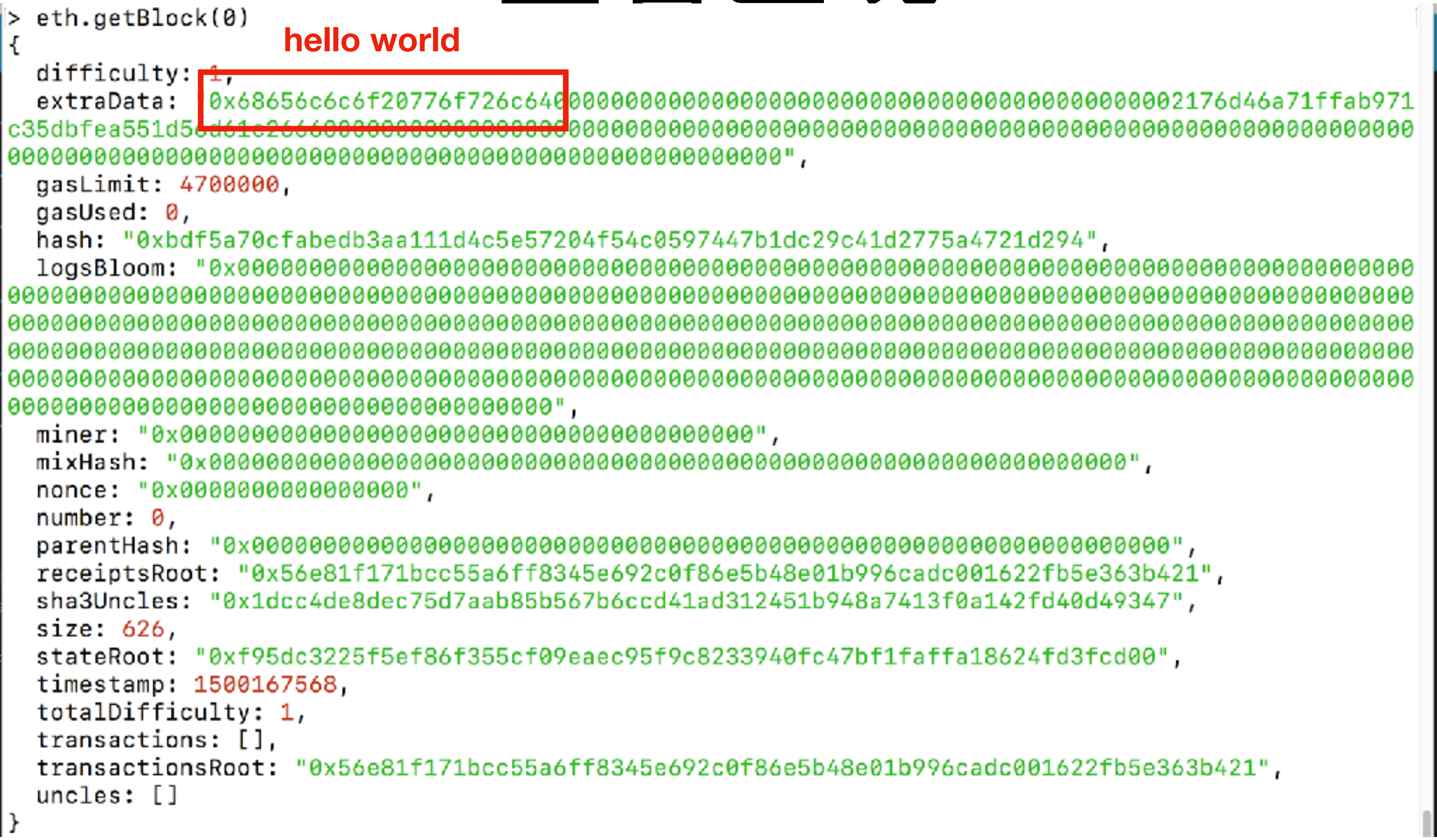
- 在 有 --unlock 的console 及是某個可打包Signer的 console

- miner.start() 開始挖礦



```
> miner.start()
INFO [07-16|09:37:54] Transaction pool price threshold updated price=18000000000
INFO [07-16|09:37:54] Starting mining operation
null
> INFO [07-16|09:37:54] Commit new mining work                   number=1 txs=0 uncles=0 elapsed=4
16.214µs
INFO [07-16|09:37:54] Successfully sealed new block             number=1 hash=d755d7…c304ff
INFO [07-16|09:37:54] 🔨mined potential block                   number=1 hash=d755d7…c304ff
INFO [07-16|09:37:54] Commit new mining work                    number=2 txs=0 uncles=0 elapsed=997
.552µs
INFO [07-16|09:38:04] Successfully sealed new block             number=2 hash=13fb05…b6a514
INFO [07-16|09:38:04] 🔨mined potential block                   number=2 hash=13fb05…b6a514
INFO [07-16|09:38:04] Commit new mining work                    number=3 txs=0 uncles=0 elapsed=854
.753µs
```

查看區塊



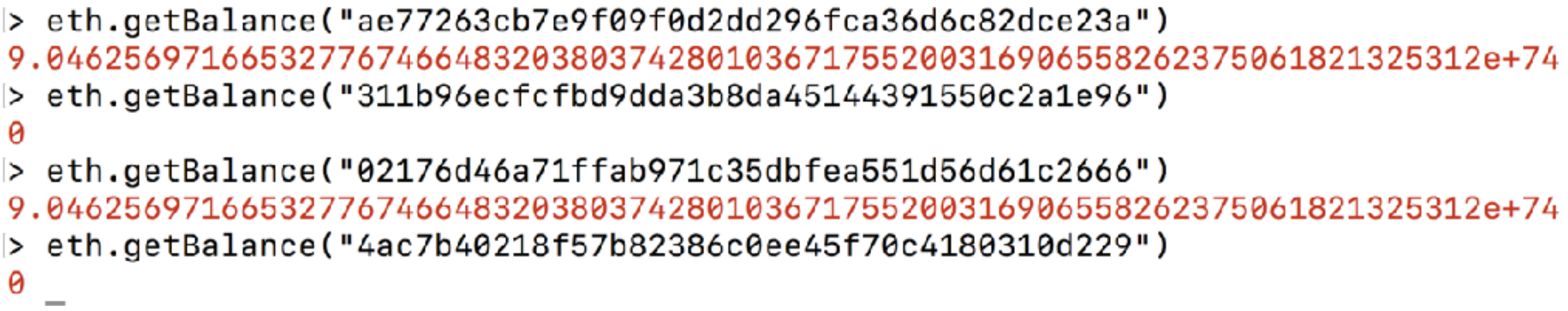
hello world

```
> eth.getBlock(0)
{
  difficulty: 1,
  extraData: "0x68656c6c6f20776f726c6400000000000000000000000000000000000000000002176d46a71ffab971
c35dbfea551d56d61e26660000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000",
  gasLimit: 4700000,
  gasUsed: 0,
  hash: "0xbdf5a70cfabedb3aa111d4c5e57204f54c0597447b1dc29c41d2775a4721d294",
  logsBloom: "0x0000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000",
  miner: "0x0000000000000000000000000000000000000000",
  mixHash: "0x0000000000000000000000000000000000000000000000000000000000000000",
  nonce: "0x0000000000000000",
  number: 0,
  parentHash: "0x0000000000000000000000000000000000000000000000000000000000000000",
  receiptsRoot: "0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421",
  sha3Uncles: "0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347",
  size: 626,
  stateRoot: "0xf95dc3225f5ef86f355cf09eaec95f9c8233940fc47bf1faffa18624fd3fcd00",
  timestamp: 1500167568,
  totalDifficulty: 1,
  transactions: [],
  transactionsRoot: "0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421",
  uncles: []
}
```

查看餘額

- 可用 eth.getBalance("帳號") 查看

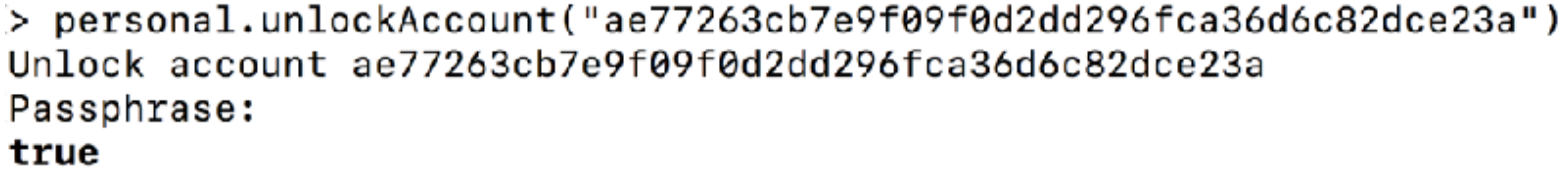
- 前面在設定創世塊時，可以發現所指定的帳號餘額不為0



```
> eth.getBalance("ae77263cb7e9f09f0d2dd296fca36d6c82dce23a")
9.04625697166532776746648320380374280103671755200316906558262375061821325312e+74
> eth.getBalance("311b96ecfcfbd9dda3b8da45144391550c2a1e96")
0
> eth.getBalance("02176d46a71ffab971c35dbfea551d56d61c2666")
9.04625697166532776746648320380374280103671755200316906558262375061821325312e+74
> eth.getBalance("4ac7b40218f57b82386c0ee45f70c4180310d229")
0
  _
```

交易

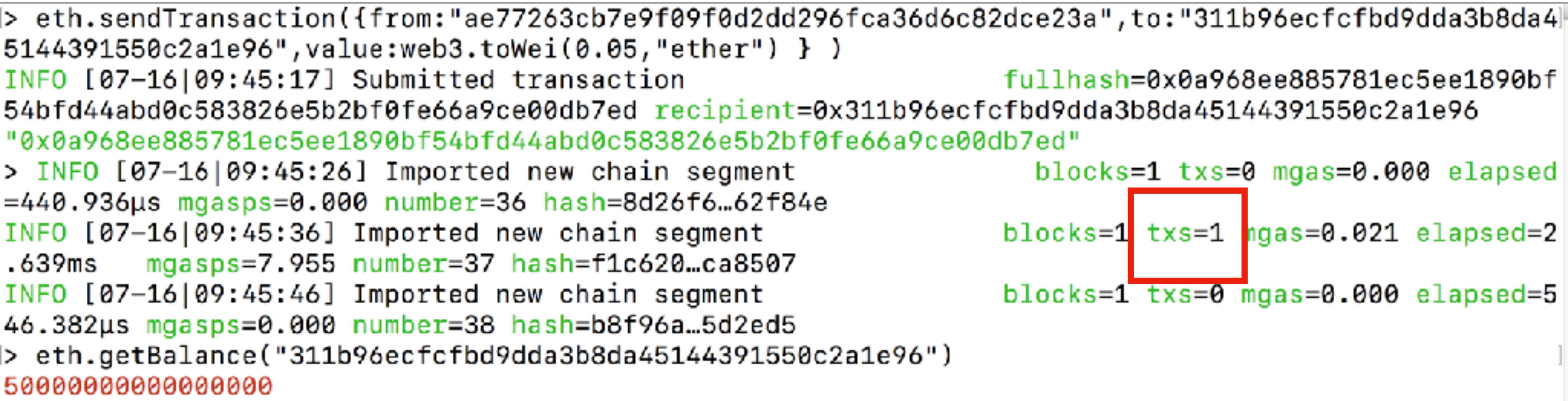
- personal.unlockAccount("當前node console 帳號") 要輸入密碼



```
> personal.unlockAccount("ae77263cb7e9f09f0d2dd296fca36d6c82dce23a")
Unlock account ae77263cb7e9f09f0d2dd296fca36d6c82dce23a
Passphrase:
true
```

- eth.sendTransaction({ from:"當前console帳號",to:"收款帳號",value:web3.toWei(0.05,"ether") })

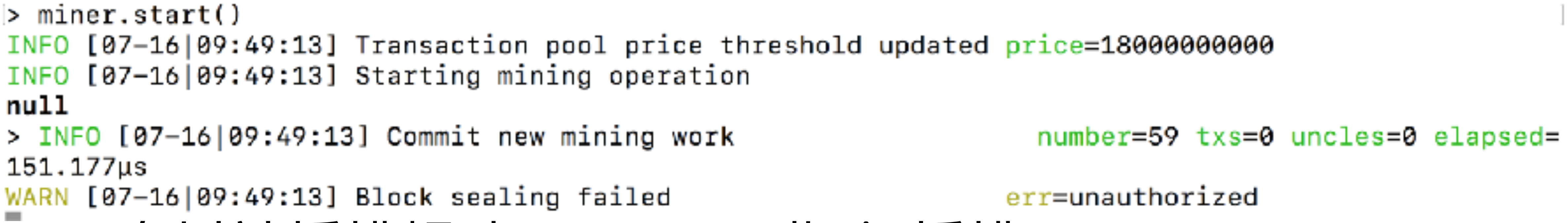
- 經過打包後,可用 eth.getBalance("帳號") 查看餘額變化



```
> eth.sendTransaction({from:"ae77263cb7e9f09f0d2dd296fca36d6c82dce23a",to:"311b96ecfcfbd9dda3b8da4
5144391550c2a1e96",value:web3.toWei(0.05,"ether") } )
INFO [07-16|09:45:17] Submitted transaction                fullhash=0x0a968ee885781ec5ee1890bf
54bfd44abd0c583826e5b2bf0fe66a9ce00db7ed recipient=0x311b96ecfcfbd9dda3b8da45144391550c2a1e96
"0x0a968ee885781ec5ee1890bf54bfd44abd0c583826e5b2bf0fe66a9ce00db7ed"
> INFO [07-16|09:45:26] Imported new chain segment               blocks=1 txs=0 mgas=0.000 elapsed
=440.936µs mgasps=0.000 number=36 hash=8d26f6…62f84e
INFO [07-16|09:45:36] Imported new chain segment               blocks=1 txs=1 mgas=0.021 elapsed=2
.639ms    mgasps=7.955 number=37 hash=f1c620…ca8507
INFO [07-16|09:45:46] Imported new chain segment               blocks=1 txs=0 mgas=0.000 elapsed=5
46.382µs mgasps=0.000 number=38 hash=b8f96a…5d2ed5
> eth.getBalance("311b96ecfcfbd9dda3b8da45144391550c2a1e96")
50000000000000000
```

增加信任打包者

- 在沒有授權的 singer miner.start() 會失敗



```
> miner.start()
INFO [07-16|09:49:13] Transaction pool price threshold updated price=18000000000
INFO [07-16|09:49:13] Starting mining operation
null
> INFO [07-16|09:49:13] Commit new mining work                    number=59 txs=0 uncles=0 elapsed=
151.177µs
WARN [07-16|09:49:13] Block sealing failed                       err=unauthorized
```

- 在以被授權帳號console 下指令 授權 clique.propose("0x需被授權打包帳號")

- 回到原本沒有授權的 signer miner.start() 及開始挖礦

- PS:挖礦也需要事先解鎖 personal.unlockAccount("當前signer console 帳號")