

## Blockchain TP

### 1. Installation d'Ethereum sur Ubuntu

```
R ception de :7 http://fr.archive.ubuntu.com/ubuntu bionic/universe amd64 libjsonrpcpp-dev amd64 0.7.0-1build2 [86,9 kB]
496 ko r ceptionn s en 2s (294 ko/s)
(Lecture de la base de donn es... 93147 fichiers et r pertoires d j  install s.)
Suppression de libcurl4-gnutls-dev:amd64 (7.58.0-2ubuntu3.21) ...
S lection du paquet libargtable2-0 pr c demment d s lectionn .
(Lecture de la base de donn es... 93123 fichiers et r pertoires d j  install s.)
Pr paration du d paquetage de ../0-libargtable2-0_13-1_amd64.deb ...
D paquetage de libargtable2-0 (13-1) ...
S lection du paquet libcurl4-openssl-dev:amd64 pr c demment d s lectionn .
Pr paration du d paquetage de ../1-libcurl4-openssl-dev_7.58.0-2ubuntu3.21_amd64.deb ...
D paquetage de libcurl4-openssl-dev:amd64 (7.58.0-2ubuntu3.21) ...
S lection du paquet libjsonrpcpp-common0 pr c demment d s lectionn .
Pr paration du d paquetage de ../2-libjsonrpcpp-common0_0.7.0-1build2_amd64.deb ...
D paquetage de libjsonrpcpp-common0 (0.7.0-1build2) ...
S lection du paquet libjsonrpcpp-client0 pr c demment d s lectionn .
Pr paration du d paquetage de ../3-libjsonrpcpp-client0_0.7.0-1build2_amd64.deb ...
D paquetage de libjsonrpcpp-client0 (0.7.0-1build2) ...
S lection du paquet libjsonrpcpp-server0 pr c demment d s lectionn .
Pr paration du d paquetage de ../4-libjsonrpcpp-server0_0.7.0-1build2_amd64.deb ...
D paquetage de libjsonrpcpp-server0 (0.7.0-1build2) ...
S lection du paquet libjsonrpcpp-stub0 pr c demment d s lectionn .
Pr paration du d paquetage de ../5-libjsonrpcpp-stub0_0.7.0-1build2_amd64.deb ...
D paquetage de libjsonrpcpp-stub0 (0.7.0-1build2) ...
S lection du paquet libjsonrpcpp-dev pr c demment d s lectionn .
Pr paration du d paquetage de ../6-libjsonrpcpp-dev_0.7.0-1build2_amd64.deb ...
D paquetage de libjsonrpcpp-dev (0.7.0-1build2) ...
Param trage de libjsonrpcpp-common0 (0.7.0-1build2) ...
Param trage de libargtable2-0 (13-1) ...
Param trage de libjsonrpcpp-server0 (0.7.0-1build2) ...
Param trage de libjsonrpcpp-stub0 (0.7.0-1build2) ...
Param trage de libjsonrpcpp-client0 (0.7.0-1build2) ...
Param trage de libcurl4-openssl-dev:amd64 (7.58.0-2ubuntu3.21) ...
Param trage de libjsonrpcpp-dev (0.7.0-1build2) ...
Traitement des actions diff r es (« triggers ») pour man-db (2.8.3-2ubuntu0.1) ...
Traitement des actions diff r es (« triggers ») pour libc-bin (2.27-3ubuntu1.5) ...
```

### 2. Cr ation de Compte

Apr s avoir cr   un nouveau r pertoire « private-ethereum », j'ai cr   un compte avec le mot de passe « admin ». Ce mot de passe a   t  choisi car c'  st un mot de passe classique que l'on peut retrouver facilement.

```
michel@michel:~/private-ethereum$ geth --datadir data account new
INFO [11-04|10:40:43.375] Maximum peer count          ETH=50 LES=0 total=50
INFO [11-04|10:40:43.376] 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: 0xc75b4046623497148aa003DA08022f946d53fcd4
Path of the secret key file: data/keystore/UTC--2022-11-04T10-41-01.1104392352--c75b4046623497148aa003da08022f946d53fcd4

- 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!
```

De la même manière, on créer un deuxième compte avec le mot de passe « admin2 »

```
michel@michel:~/private-ethereum$ geth --datadir data account new
INFO [11-04|10:44:51.318] Maximum peer count          ETH=50 LES=0 total=50
INFO [11-04|10:44:51.320] 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: 0x7ae645d84934e08667a8c500d71bbc0eca86660f
Path of the secret key file: data/keystore/UTC--2022-11-04T10-44-58.1421499932--7ae645d84934e08667a8c500d71bbc0eca86660f

- 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!
```

On peut visualiser la liste des comptes avec la commande :

**geth --datadir data account list**

```
michel@michel:~/private-ethereum$ geth --datadir data account list
INFO [11-04|10:46:20.807] Maximum peer count          ETH=50 LES=0 total=50
INFO [11-04|10:46:20.808] Smartcard socket not found, disabling  err="stat /run/pcscd/pcscd.comm:
no such file or directory"
WARN [11-04|10:46:20.826] Sanitizing cache to Go's GC limits      provided=1024 updated=328
INFO [11-04|10:46:20.828] Set global gas cap              cap=50,000,000
Account #0: {c75b4046623497148aa003da08022f946d53fcd4} keystore:///home/michel/private-ethereum/data
/keystore/UTC--2022-11-04T10-41-01.1104392352--c75b4046623497148aa003da08022f946d53fcd4
Account #1: {7ae645d84934e08667a8c500d71bbc0eca86660f} keystore:///home/michel/private-ethereum/data
/keystore/UTC--2022-11-04T10-44-58.1421499932--7ae645d84934e08667a8c500d71bbc0eca86660f
```

### 3. Création du bloc de genèse

On crée le fichier « genesis.json ». Dans ce fichier on copie les données du fichier « genesis.json » du serveur pour pouvoir récupérer un bloc de genèse identique à celui du serveur.

```
{
  "config": {
    "chainId": 202204,
    "homesteadBlock": 0,
    "eip150Block": 0,
    "eip155Block": 0,
    "eip158Block": 0,
    "byzantiumBlock": 0,
    "constantinopleBlock": 0,
    "petersburgBlock": 0,
    "ethash": {}
  },
  "difficulty": "1",
  "gasLimit": "8000000",
  "alloc": {
    "fa5a8b5860c5d458b7c8b4f483d714994efff39c": { "balance": "300000" },
    "2af32dcbb109605819415311ebdb01af6ee1beb31": { "balance": "300000" }
  }
}
```

On initialise le bloc de genèse en entrant la commande :

**geth --datadir data genesis.json**

```
michel@michel:~/private-ethereum$ geth init --datadir data genesis.json
INFO [11-16|14:13:14.394] Maximum peer count                ETH=50 LES=0 total=50
INFO [11-16|14:13:14.397] Smartcard socket not found, disabling err="stat /run/pcscd/pcscd.comm:
no such file or directory"
WARN [11-16|14:13:14.400] Sanitizing cache to Go's GC limits provided=1024 updated=328
INFO [11-16|14:13:14.402] Set global gas cap                cap=50,000,000
INFO [11-16|14:13:14.405] Allocated cache and file handles database=/home/michel/private-eth
ereum/data/geth/chaindata cache=16.00MiB handles=16
INFO [11-16|14:13:14.490] Opened ancient database           database=/home/michel/private-eth
ereum/data/geth/chaindata/ancient/chain readonly=false
INFO [11-16|14:13:14.491] Writing custom genesis block
INFO [11-16|14:13:14.495] Persisted trie from memory database nodes=3 size=397.00B time="95.571
µs" gcnodes=0 gcsizes=0.00B gctime=0s livenodes=1 liveness=0.00B
INFO [11-16|14:13:14.496] Successfully wrote genesis state database=chaindata hash=4a4649..f
60f87
INFO [11-16|14:13:14.497] Allocated cache and file handles database=/home/michel/private-eth
ereum/data/geth/lightchaindata cache=16.00MiB handles=16
INFO [11-16|14:13:14.591] Opened ancient database           database=/home/michel/private-eth
ereum/data/geth/lightchaindata/ancient/chain readonly=false
INFO [11-16|14:13:14.592] Writing custom genesis block
INFO [11-16|14:13:14.594] Persisted trie from memory database nodes=3 size=397.00B time="88.848
µs" gcnodes=0 gcsizes=0.00B gctime=0s livenodes=1 liveness=0.00B
INFO [11-16|14:13:14.596] Successfully wrote genesis state database=lightchaindata hash=4a46
49..f60f87
michel@michel:~/private-ethereum$ _
```

#### 4. Création du bootnode

```
michel@michel:~/private-ethereum$ bootnode
Fatal: Use -nodekey or -nodekeyhex to specify a private key
michel@michel:~/private-ethereum$ bootnode --genkey=boot.key
michel@michel:~/private-ethereum$ bootnode --nodekey=boot.key
enode://5a1c704f111524ba423e268c37c9f12d326adb5985511533a6ff41ba7d28f61659356f730e5af40656c66de0d9d1
68b610e130a7b051cab1c907eb926bbb38ec@127.0.0.1:0?discport=30301
Note: you're using cmd/bootnode, a developer tool.
We recommend using a regular node as bootstrap node for production deployments.
INFO [11-16|14:17:04.131] New local node record seq=1,668,608,224,128 id=83fd78f7
3d12b2f9 ip=<nil> udp=0 tcp=0
_
```

```
michel@michel:~/private-ethereum2$ bootnode --nodekey=boot.key --writeaddress 127.0.0.1:30303
cf01b827070052ea359f59c0c9ef738090375226382bda7ec96dff6a256cee1316867cbe56fd540333bf8251b08f9a1b690e
79574c06eb1e958b6281952173b3
```

## 5. Synchronisation avec le serveur

Côté client :

```
michel@michel:~/private-ethereum2$ geth --networkid 202204 --datadir data --bootnodes enode://fc8a3dcfd340daa4c3bddd4b60eea788c00ce60893bd9ff8493be6be0fa82ec81b5dc9e1a5dca3641951c11924b2223ede95684aecb7ccb6faafb03ebf12048907d@146.190.232.50:30303
```

```
WARN [11-16|14:31:27.689] Error reading unclean shutdown markers error="leveldb: not found"
WARN [11-16|14:31:27.690] Engine API enabled protocol=eth
WARN [11-16|14:31:27.693] Engine API started but chain not configured for merge yet
INFO [11-16|14:31:27.694] Starting peer-to-peer node instance=Geth/v1.10.26-stable-e5eb32ac/linux-amd64/go1.18.5
INFO [11-16|14:31:27.697] Resuming state snapshot generation root=8748fe..671ce0 accounts=0 slots=0 storage=0.00B dangling=0 elapsed=12.475ms
INFO [11-16|14:31:27.707] Generated state snapshot accounts=2 slots=0 storage=82.00B
INFO [11-16|14:31:27.748] New local node record seq=1,668,609,087,741 id=90f85c06a222f348 ip=127.0.0.1 udp=30303 tcp=30303
INFO [11-16|14:31:27.759] IPC endpoint opened url=/home/michel/private-ethereum2/data/geth.ipc
INFO [11-16|14:31:27.760] Generated JWT secret path=/home/michel/private-ethereum2/data/geth/jwtsecret
INFO [11-16|14:31:27.765] Started P2P networking self=enode://ec885863009d60f62870a0aaab4647729da89ebd9da57aad7d266559d567df2db78a5b0ebd57dcfd32af279761b83676272271f6160f7ee672d623f83f1c1792@127.0.0.1:30303
INFO [11-16|14:31:27.769] WebSocket enabled url=ws://127.0.0.1:8551
INFO [11-16|14:31:27.770] HTTP server started endpoint=127.0.0.1:8551 auth=true prefix= cors=localhost vhosts=localhost
INFO [11-16|14:31:27.853] Etherbase automatically configured address=0xc75b4046623497148aa003D9A08022f946d53fcd4
Welcome to the Geth JavaScript console!

instance: Geth/v1.10.26-stable-e5eb32ac/linux-amd64/go1.18.5
coinbase: 0xc75b4046623497148aa003D9A08022f946d53fcd4
at block: 0 (Thu Jan 01 1970 00:00:00 GMT+0000 (UTC))
datadir: /home/michel/private-ethereum2/data
modules: admin:1.0 debug:1.0 engine:1.0 eth:1.0 ethash:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txpool:1.0 web3:1.0

To exit, press ctrl-d or type exit
> net.listening
true
> INFO [11-16|14:32:02.765] Looking for peers peercount=0 tried=1 static=0
```

```
INFO [11-17|10:36:12.596] Block synchronisation started
INFO [11-17|10:36:13.413] Downloader queue stats receiptTasks=0 blockTasks=0 items=579.99B throttle=8192
WARN [11-17|10:36:14.050] Large chain reorg detected number=0 hash=8b84e7..1f9cc9 drop=71 dropfrom=0e2ee2..0dc335 add=71 addfrom=2874d3..99b6e4
INFO [11-17|10:36:14.204] Imported new chain segment blocks=106 txs=0 mgas=0.000 elapsed=787.189ms mgasps=0.000 number=106 hash=15ecd3..6a803f dirty=46.99KiB
INFO [11-17|10:36:17.870] Imported new chain segment blocks=1 txs=0 mgas=0.000 elapsed=6.431ms mgasps=0.000 number=107 hash=6d0dfd..0bae3f dirty=47.43KiB
```

Côté serveur :

```
INFO [11-17|08:18:46.302] Block synchronisation started
INFO [11-17|08:18:46.302] Mining aborted due to sync
```

On peut remarquer que le client s'est synchronisé avec le serveur et donc les hash des différents blocs est le même du côté client que du côté serveur.

### Soft Fork avec le serveur :

Les clients ont miné en local ce qui a conduit à un soft Fork. Le nombre de blocks est de 71 sur l'ordinateur client tandis que le serveur possède seulement 50 blocks.

[illegible]

## 6. Transaction

On effectue une transaction d'un wallet créé sur le serveur à un wallet créé par un nœud. On peut remarquer que le nombre d'éther a augmenté. On peut le visualiser sur le serveur mais aussi sur les ordinateurs clients car ils sont synchronisés.

```
> INFO [11-17|10:48:37.887] Imported new chain segment          blocks=1   txs=0 mgas=0.000 elaps
psed=12.166ms mgasps=0.000 number=243 hash=29ebcd..64356f dirty=56.75KiB
> eth.getBalance(eth.accounts[0])
0
> WARN [11-17|10:48:42.727] Snapshot extension registration failed    peer=7bcee16b err="peer connect
ed on snap without compatible eth support"
INFO [11-17|10:48:46.964] Imported new chain segment          blocks=1   txs=1 mgas=0.021 elaps
ed=11.868ms mgasps=1.769 number=244 hash=795049..6060f2 dirty=57.01KiB
INFO [11-17|10:48:47.237] Looking for peers                    peercount=1 tried=114 static=0
> eth.getBalance(eth.accounts[0])
25000
> INFO [11-17|10:48:57.404] Looking for peers                    peercount=1 tried=46 static=0
INFO [11-17|10:49:02.429] Imported new chain segment          blocks=1   txs=0 mgas=0.000 elaps
ed=12.470ms mgasps=0.000 number=245 hash=9a69ca..a6aae4 dirty=57.04KiB
INFO [11-17|10:49:07.414] Looking for peers                    peercount=1 tried=78 static=0
```