

TP BLOCKCHAIN

Création et configuration d'une Blockchain
Privée Ethereum

Compte rendu Ishika HOSSAIN

Groupe 3 :

- Ishika HOSSAIN
- Anthénéa KASDI
- Inès DERNONCOURT
- Cindy MUTHUKRISHNAN

Table des matières

INTRODUCTION.....	3
I. Installation d'Ethereum	3
II. Création de comptes pour le réseau privé Ethereum	4
III. Création du Genesis File	6
IV. Configuration du Bootnode	8
V. Configuration de notre Ethereum Private Blockchain et minage.....	9
VI. Démarrage des nœuds	12

INTRODUCTION

Voici les informations préliminaires nécessaires pour la réalisation de ce TP :

Groupe 3
Serveur : ESME 3
IP : 64.225.66.111

Étant un groupe constitué de 4 personnes, le TP s'est déroulé de la manière suivante :

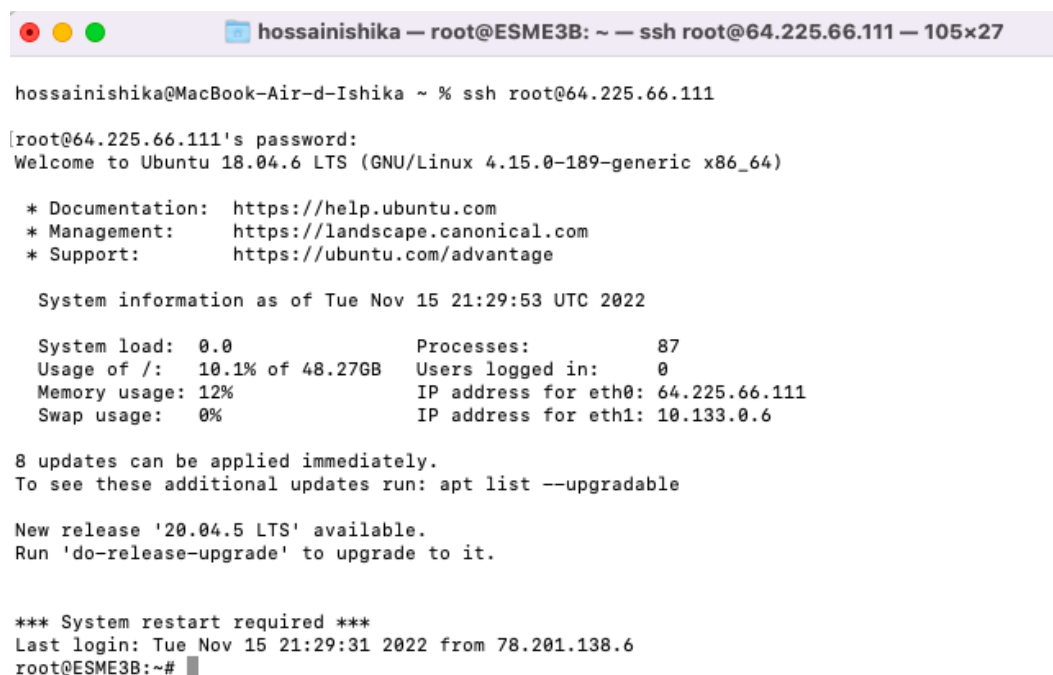
- J'étais le serveur (ESME3B avec l'adresse IP 64.225.66.111) ;
- Anthénée, Cindy et Inès étaient donc les clients en utilisant leurs machines virtuelles Ubuntu sur VirtualBox.

I. Installation d'Ethereum

Cette étape consiste en l'installation d'Ethereum sur le serveur afin de créer un réseau privé Ethereum.

Ayant un PC MAC, la connexion au serveur s'effectue facilement grâce au protocole SSH à partir du terminal.

La commande à taper pour se connecter au serveur est donc : `ssh root@64.225.66.111`



```
hossainishika — root@ESME3B: ~ — ssh root@64.225.66.111 — 105x27

hossainishika@MacBook-Air-d-Ishika ~ % ssh root@64.225.66.111
[root@64.225.66.111's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-189-generic x86_64)

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

System information as of Tue Nov 15 21:29:53 UTC 2022

System load:  0.0               Processes:    87
Usage of /:   10.1% of 48.27GB  Users logged in:  0
Memory usage: 12%              IP address for eth0: 64.225.66.111
Swap usage:   0%               IP address for eth1: 10.133.0.6

8 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

New release '20.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** System restart required ***
Last login: Tue Nov 15 21:29:31 2022 from 78.201.138.6
root@ESME3B:~#
```

Toutes les commandes pour installer Ethereum sur le serveur ont donc été exécutées avec comme fenêtre finale sur le terminal :

```
hossainishika — root@ESME3B: ~ — ssh root@64.225.66.111 — 124x50
Get:2 http://mirrors.digitalocean.com/ubuntu bionic-updates/main amd64 libcurl4 amd64 7.58.0-2ubuntu3.21 [220 kB]
Get:3 http://mirrors.digitalocean.com/ubuntu bionic/universe amd64 libargtable2-0 amd64 13-1 [13.6 kB]
Get:4 http://mirrors.digitalocean.com/ubuntu bionic-updates/main amd64 libcurl4-openssl-dev amd64 7.58.0-2ubuntu3.21 [302 kB]
Get:5 http://mirrors.digitalocean.com/ubuntu bionic/universe amd64 libjsonrpcpp-common0 amd64 0.7.0-1build2 [24.5 kB]
Get:6 http://mirrors.digitalocean.com/ubuntu bionic/universe amd64 libjsonrpcpp-client0 amd64 0.7.0-1build2 [20.4 kB]
Get:7 http://mirrors.digitalocean.com/ubuntu bionic/universe amd64 libjsonrpcpp-server0 amd64 0.7.0-1build2 [21.1 kB]
Get:8 http://mirrors.digitalocean.com/ubuntu bionic/universe amd64 libjsonrpcpp-stub0 amd64 0.7.0-1build2 [27.1 kB]
Get:9 http://mirrors.digitalocean.com/ubuntu bionic/universe amd64 libjsonrpcpp-dev amd64 0.7.0-1build2 [86.9 kB]
Fetched 875 kB in 0s (3817 kB/s)
(Reading database ... 89066 files and directories currently installed.)
Removing libcurl4-gnutls-dev:amd64 (7.58.0-2ubuntu3.21) ...
(Reading database ... 89042 files and directories currently installed.)
Preparing to unpack .../0-curl_7.58.0-2ubuntu3.21_amd64.deb ...
Unpacking curl (7.58.0-2ubuntu3.21) over (7.58.0-2ubuntu3.19) ...
Preparing to unpack .../1-libcurl4_7.58.0-2ubuntu3.21_amd64.deb ...
Unpacking libcurl4:amd64 (7.58.0-2ubuntu3.21) over (7.58.0-2ubuntu3.19) ...
Selecting previously unselected package libargtable2-0.
Preparing to unpack .../2-libargtable2-0_13-1_amd64.deb ...
Unpacking libargtable2-0 (13-1) ...
Selecting previously unselected package libcurl4-openssl-dev:amd64.
Preparing to unpack .../3-libcurl4-openssl-dev_7.58.0-2ubuntu3.21_amd64.deb ...
Unpacking libcurl4-openssl-dev:amd64 (7.58.0-2ubuntu3.21) ...
Selecting previously unselected package libjsonrpcpp-common0.
Preparing to unpack .../4-libjsonrpcpp-common0_0.7.0-1build2_amd64.deb ...
Unpacking libjsonrpcpp-common0 (0.7.0-1build2) ...
Selecting previously unselected package libjsonrpcpp-client0.
Preparing to unpack .../5-libjsonrpcpp-client0_0.7.0-1build2_amd64.deb ...
Unpacking libjsonrpcpp-client0 (0.7.0-1build2) ...
Selecting previously unselected package libjsonrpcpp-server0.
Preparing to unpack .../6-libjsonrpcpp-server0_0.7.0-1build2_amd64.deb ...
Unpacking libjsonrpcpp-server0 (0.7.0-1build2) ...
Selecting previously unselected package libjsonrpcpp-stub0.
Preparing to unpack .../7-libjsonrpcpp-stub0_0.7.0-1build2_amd64.deb ...
Unpacking libjsonrpcpp-stub0 (0.7.0-1build2) ...
Selecting previously unselected package libjsonrpcpp-dev.
Preparing to unpack .../8-libjsonrpcpp-dev_0.7.0-1build2_amd64.deb ...
Unpacking libjsonrpcpp-dev (0.7.0-1build2) ...
Setting up libjsonrpcpp-common0 (0.7.0-1build2) ...
Setting up libargtable2-0 (13-1) ...
Setting up libjsonrpcpp-server0 (0.7.0-1build2) ...
Setting up libcurl4:amd64 (7.58.0-2ubuntu3.21) ...
Setting up libjsonrpcpp-stub0 (0.7.0-1build2) ...
Setting up libjsonrpcpp-client0 (0.7.0-1build2) ...
Setting up libcurl4-openssl-dev:amd64 (7.58.0-2ubuntu3.21) ...
Setting up curl (7.58.0-2ubuntu3.21) ...
Setting up libjsonrpcpp-dev (0.7.0-1build2) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for libc-bin (2.27-3ubuntu1.6) ...
root@ESME3B:~#
```

II. Création de comptes pour le réseau privé Ethereum

1. Créons dans un premier temps, un répertoire pour notre réseau privé qu'on appellera « private-ethereum » :

```
hossainishika — root@ESME3B: ~/private-ethereum — ssh root@64.225.66.111 — 124x50
[root@ESME3B:~# mkdir private-ethereum
[root@ESME3B:~# cd private-ethereum
```

2. Accédons à ce répertoire et créons 2 comptes « wallet ».

Création du premier compte « wallet » :

```
hossainishika — root@ESME3B: ~/private-ethereum — ssh root@64.225.66.111 — 124x50
[root@ESME3B:~# mkdir private-ethereum
[root@ESME3B:~# cd private-ethereum
[root@ESME3B:~/private-ethereum# geth --datadir data account new
INFO [11-04|10:54:36.761] Maximum peer count          ETH=50 LES=0 total=50
INFO [11-04|10:54:36.762] Smartcard socket not found, disabling  err="stat /run/pcscd/pcscd.comm: no such file or director
y"
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: 0x8bf6f8C459Db71707BB60fD5ea86Bd2895c60E00
Path of the secret key file: data/keystore/UTC--2022-11-04T10-54-49.918641579Z--8bf6f8c459db71707bb60fd5ea86bd2895c60e00

- 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!

root@ESME3B:~/private-ethereum#
```

Création du second compte « wallet » :

```
[root@ESME3B:~/private-ethereum# geth --datadir data account new
INFO [11-04|10:56:20.438] Maximum peer count          ETH=50 LES=0 total=50
INFO [11-04|10:56:20.438] Smartcard socket not found, disabling  err="stat /run/pcscd/pcscd.comm: no such file or director
y"
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: 0x5C7Ec9BD1bbeeBE8Af2aeD7EBB7484F7e42D329d
Path of the secret key file: data/keystore/UTC--2022-11-04T10-56-37.448370776Z--5c7ec9bd1bbebe8af2aed7ebb7484f7e42d329d

- 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!
```

À chaque création de compte « wallet », un mot de passe est demandé car notre clé privée est cryptée avec ce mot de passe.

Le mot de passe fourni a un rôle important car il permet à l'utilisateur d'effectuer des actions comme envoyer une transaction ou même déverrouiller notre compte. Et pour effectuer chacune de ces actions, ce mot de passe sera demandé : il est donc important de s'en souvenir.

Vérifions la création des deux comptes en listant tous les comptes :

```
[root@ESME3B:~/private-ethereum# geth --datadir data account list
INFO [11-04|10:58:50.186] Maximum peer count           ETH=50 LES=0 total=50
INFO [11-04|10:58:50.187] Smartcard socket not found, disabling err="stat /run/pcscd/pcscd.comm: no such file or director
y"
WARN [11-04|10:58:50.189] Sanitizing cache to Go's GC limits provided=1024 updated=664
INFO [11-04|10:58:50.189] Set global gas cap           cap=50,000,000
Account #0: {8bf6f8c459db71707bb60fd5ea86bd2895c60e00} keystore:///root/private-ethereum/data/keystore/UTC--2022-11-04T10-54
-49.918641579Z--8bf6f8c459db71707bb60fd5ea86bd2895c60e00
Account #1: {5c7ec9bd1bbebe8af2aed7ebb7484f7e42d329d} keystore:///root/private-ethereum/data/keystore/UTC--2022-11-04T10-56
-37.448370776Z--5c7ec9bd1bbebe8af2aed7ebb7484f7e42d329d
root@ESME3B:~/private-ethereum#
```

La liste représente les comptes « wallet » créés sur notre réseau privée Ethereum. On voit bien la liste des comptes créés précédemment (Account #0 et Account #1) avec leur adresse ainsi que leur « keystore », qui est un fichier contenant la clé privée de portefeuille cryptée.

III. Création du Genesis File

Le fichier Genesis « ***genesis.json*** » a été créé sur le serveur avec les informations suivantes :

- ```
- chainId : 12345678
- Adresse du compte 0 : 8bf6f8c459db71707bb60fd5ea86bd2895c60e00
- Adresse du compte 1 : 5c7ec9bd1bbeebe8af2aed7ebb7484f7e42d329d
```

```
hossainishika — root@ESME3B: ~/private-ethereum — ssh root@64.225.66.111 — 124x50
GNU nano 2.9.3 genesis.json

{
 "config": {
 "chainId": 12345678,
 "homesteadBlock": 0,
 "eip150Block": 0,
 "eip155Block": 0,
 "eip158Block": 0,
 "byzantiumBlock": 0,
 "constantinopleBlock": 0,
 "petersburgBlock": 0,
 "ethash": {}
 },
 "difficulty": "1",
 "gasLimit": "8000000",
 "alloc": {
 "8bf6f8c459db71707bb60fd5ea86bd2895c60e00": { "balance": "3000000000000000000" },
 "5c7ec9bd1bbebe8af2aed7ebb7484f7e42d329d": { "balance": "4000000000000000000" }
 }
}
```

Voici à quoi correspondent les paramètres du fichier Genesis <sup>[1]</sup><sub>SEP</sub>

**chainId** : Valeur numérique qui permet d'informer les autres la chaîne sur laquelle on se trouve.

**homesteadBlock** : dès qu'il est défini sur 0, ça signifie que nous utilisons la version Homestead d'Ethereum.

**eip150Block** : EIP signifie **E**thereum **I**mprovement **P**roposal . Comme Ethereum est en open source, n'importe quel utilisateur peut faire des propositions sous forme de discussions et de code. Certains sont acceptés et d'autres peuvent être rejetés. EIP150 est donc l'une de ces propositions qui a été acceptée. Cet EIP est entré en vigueur sur le bloc 2463000 et concernait principalement l'augmentation des prix du gaz en réponse aux problèmes de déni de service.

**eip155Block**: Aide à prévenir les « simple replay attack », qui se produisent lorsqu'un cybercriminel écoute une communication réseau sécurisée, l'intercepte, puis la retarde ou la renvoie frauduleusement pour inciter le destinataire à faire ce que veut le pirate.

**eip158Block**: Traite les comptes vides. Ce nouveau protocole a commencé à traiter les comptes vides comme inexistant, économisant de l'espace sur la Blockchain.

**byzantiumBlock**: Améliore les attributs de confidentialité, d'évolutivité et de sécurité d'Ethereum.

**constantinopleBlock** : Le hard fork Constantinople est un hard fork, contenant 5 EIP dont l'EIP-1234 qui a réduit de 33 % les récompenses en blocs pour les mineurs et l'EIP-1283 qui permet une attaque par réentraînement (reentrancy attack).

**ethash** : Indique au client que nous utilisons Ethash, l'algorithme de proof of work d'Ethereum, pour extraire des blocs. <sup>[1]</sup><sub>SEP</sub>

**difficulty** : Valeur déterminant à quel point il est difficile de miner un bloc.

**gaslimit** : Nombre maximal de calculs que tout bloc de cette chaîne peut prendre en charge.

**alloc** : Champ déterminant qui commence avec combien d'éther pour démarrer la blockchain.

Voici le résultat après l'instanciation du répertoire de données :

```
hossainishika — root@ESME3B: ~/private-ethereum — ssh root@64.225.66.111 — 124x50
root@ESME3B:~/private-ethereum# geth init --datadir data genesis.json
INFO [11-04|11:16:05.524] Maximum peer count ETH=50 LES=0 total=50
INFO [11-04|11:16:05.526] Smartcard socket not found, disabling err="stat /run/pcscd/pcscd.comm: no such file or director
y"
WARN [11-04|11:16:05.548] Sanitizing cache to Go's GC limits provided=1024 updated=664
INFO [11-04|11:16:05.549] Set global gas cap cap=50,000,000
INFO [11-04|11:16:05.554] Allocated cache and file handles database=/root/private-ethereum/data/geth/chaindata cache
=16.00MiB handles=16
INFO [11-04|11:16:05.597] Opened ancient database database=/root/private-ethereum/data/geth/chaindata/ancie
nt/chain readonly=false
INFO [11-04|11:16:05.597] Writing custom genesis block
INFO [11-04|11:16:05.599] Persisted trie from memory database nodes=3 size=409.00B time="223.566µs" gcnodes=0 gcsiz
e=0.00B gctime=0s livenodes=1 livesize=0.00B
INFO [11-04|11:16:05.600] Successfully wrote genesis state database=chaindata hash=a054c8..1677ab
INFO [11-04|11:16:05.600] Allocated cache and file handles database=/root/private-ethereum/data/geth/lightchaindata
cache=16.00MiB handles=16
INFO [11-04|11:16:05.631] Opened ancient database database=/root/private-ethereum/data/geth/lightchaindata/
ancient/chain readonly=false
INFO [11-04|11:16:05.631] Writing custom genesis block
INFO [11-04|11:16:05.633] Persisted trie from memory database nodes=3 size=409.00B time="119.695µs" gcnodes=0 gcsiz
e=0.00B gctime=0s livenodes=1 livesize=0.00B
INFO [11-04|11:16:05.637] Successfully wrote genesis state database=lightchaindata hash=a054c8..1677ab
root@ESME3B:~/private-ethereum#
```

## IV. Configuration du Bootnode

Implémentons bootnode dans notre réseau privé :

```
hossainishika — root@ESME3B: ~/private-ethereum — ssh root@64.225.66.111 — 124x50
root@ESME3B:~/private-ethereum# bootnode
Fatal: Use -nodekey or -nodekeyhex to specify a private key
root@ESME3B:~/private-ethereum#
```

On obtient le lien enode correspondant à notre bootnode. Le port utilisé est le port 30301. Instanciation réussie avec la sortie suivante :

```
root@ESME3B:~/private-ethereum# bootnode --genkey=boot.key
root@ESME3B:~/private-ethereum# bootnode --nodekey=boot.key
enode://9a0798077877ae136ef2917af614c073e994d7db84efd0f046e83f60bb6793180e70515aa08a4f599e7654e664dd384cbd53266bcf4c
ba6b83ffc0665c0257c80127.0.0.1:0?discport=30301
Note: you're using cmd/bootnode, a developer tool.
We recommend using a regular node as bootstrap node for production deployments.
INFO [11-04|11:19:18.142] New local node record seq=1,667,560,758 id=8f9b6a2a87889f2e ip=<nil> udp=0 tcp=0
```

Vérifions que nous possédons bien la même adresse comme identifiant :

```
root@ESME3B:~/private-ethereum# bootnode --nodekey=boot.key --writeaddress
9a0798077877ae136ef2917af614c073e994d7db84efd0f046e83f60bb6793180e70515aa08a4f599e7654e664dd384cbd53266bcf4c
ba6b83ffc0665c0257c8
root@ESME3B:~/private-ethereum#
```



## V. Configuration de notre Ethereum Private Blockchain et minage

- Commençons à miner sur le serveur en lançant la commande suivante :

```
geth --mine --networkid 12345678 --http.port 30301 --nat extip:64.225.66.111 --miner.etherbase=0x8bf6f8c459db71707bb60fd5ea86bd2895c60e00 --datadir data console
```

- 12345678 : correspond à notre chainId.
- 64.225.66.111 : correspond à l'adresse IP du serveur.
- 8bf6f8c459db71707bb60fd5ea86bd2895c60e00 : adresse du compte 0

```
hossainishika — root@ESME3B: ~/private-ethereum — ssh root@64.225.66.111 — 170x41

root@ESME3B:~/private-ethereum# geth --mine --networkid 12345678 --http.port 30301 --nat extip:64.225.66.111 --miner.etherbase=0x8bf6f8c459db71707bb60fd5ea86bd2895c60e00 --datadir data console
INFO [11-05|17:17:16.711] Maximum peer count ETH=50 LES=0 total=50
INFO [11-05|17:17:16.715] Smartcard socket not found, disabling err="stat /run/pcscd/pcscd.comm: no such file or directory"
WARN [11-05|17:17:16.740] Sanitizing cache to Go's GC limits provided=1024 updated=664
INFO [11-05|17:17:16.742] Set global gas cap cap=50,000,000
INFO [11-05|17:17:16.747] Allocated trie memory caches clean=99.00MiB dirty=166.00MiB
INFO [11-05|17:17:16.747] Allocated cache and file handles database=/root/private-ethereum/data/geth/chaindata cache=332.00MiB handles=524,288
INFO [11-05|17:17:16.854] Opened ancient database database=/root/private-ethereum/data/geth/chaindata/ancient/chain readonly=false
INFO [11-05|17:17:16.857]

INFO [11-05|17:17:16.858] Chain ID: 12345678 (unknown)
INFO [11-05|17:17:16.858] Consensus: Ethash (proof-of-work)
INFO [11-05|17:17:16.858]
INFO [11-05|17:17:16.858] Pre-Merge hard forks:
INFO [11-05|17:17:16.858] - Homestead: 0 (https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/homestead.md)
INFO [11-05|17:17:16.858] - Tangerine Whistle (EIP 150): 0 (https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/tangerine-whistle.md)
INFO [11-05|17:17:16.858] - Spurious Dragon/1 (EIP 155): 0 (https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/spurious-dragon.md)
INFO [11-05|17:17:16.858] - Spurious Dragon/2 (EIP 158): 0 (https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/spurious-dragon.md)
INFO [11-05|17:17:16.858] - Byzantium: 0 (https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/byzantium.md)
INFO [11-05|17:17:16.859] - Constantinople: 0 (https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/constantinople.md)
INFO [11-05|17:17:16.859] - Petersburg: 0 (https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/petersburg.md)
INFO [11-05|17:17:16.859] - Istanbul: <nil> (https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/istanbul.md)
INFO [11-05|17:17:16.859] - Berlin: <nil> (https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/berlin.md)
INFO [11-05|17:17:16.859] - London: <nil> (https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/london.md)
INFO [11-05|17:17:16.859] The Merge is not yet available for this network!
INFO [11-05|17:17:16.859] - Hard-fork specification: https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/paris.md
INFO [11-05|17:17:16.859]

INFO [11-05|17:17:16.859]
INFO [11-05|17:17:16.860] Disk storage enabled for ethash caches dir=/root/private-ethereum/data/geth/ethash count=3
```



- Vérifions le genesis block :

[illegible]

- Lançons la commande de mining suivante : `miner.start(1)`

```

INFO [11-05 | 17:59:07.972] Successfully sealed new block
INFO [11-05 | 17:59:07.973] block reached canonical chain
INFO [11-05 | 17:59:07.973] mined potential block
INFO [11-05 | 17:59:07.974] Commit new sealing work
INFO [11-05 | 17:59:07.974] Commit new sealing work
INFO [11-05 | 17:59:10.760] Generating DAG in progress
INFO [11-05 | 17:59:14.050] Looking for peers
INFO [11-05 | 17:59:14.786] Successfully sealed new block
INFO [11-05 | 17:59:14.786] block reached canonical chain
INFO [11-05 | 17:59:14.786] mined potential block
INFO [11-05 | 17:59:14.787] Commit new sealing work
INFO [11-05 | 17:59:14.787] Commit new sealing work
INFO [11-05 | 17:59:24.127] Looking for peers
INFO [11-05 | 17:59:24.595] Successfully sealed new block
INFO [11-05 | 17:59:24.596] block reached canonical chain
INFO [11-05 | 17:59:24.596] mined potential block
INFO [11-05 | 17:59:24.596] Commit new sealing work
INFO [11-05 | 17:59:24.596] Commit new sealing work
INFO [11-05 | 17:59:25.917] Generating DAG in progress
INFO [11-05 | 17:59:30.776] Successfully sealed new block
INFO [11-05 | 17:59:30.776] block reached canonical chain
INFO [11-05 | 17:59:30.776] mined potential block
INFO [11-05 | 17:59:30.778] Commit new sealing work
INFO [11-05 | 17:59:30.778] Commit new sealing work
INFO [11-05 | 17:59:34.283] Looking for peers
INFO [11-05 | 17:59:40.414] Generating DAG in progress
INFO [11-05 | 17:59:44.263] Successfully sealed new block
INFO [11-05 | 17:59:44.263] block reached canonical chain
INFO [11-05 | 17:59:44.263] mined potential block
INFO [11-05 | 17:59:44.281] Commit new sealing work
INFO [11-05 | 17:59:44.282] Commit new sealing work
INFO [11-05 | 17:59:44.423] Looking for peers

number=26 sealhash=c98b2d..0ab88b hash=2881e5..5f0d0f elapsed=10.377s
number=19 hash=65cb95..24795d
number=26 hash=2081e5..5f0d0f
number=27 sealhash=9d79d9..c1a59b uncles=0 txs=0 gas=0 fees=0 elapsed="427.453µs"
epoch=1 percentage=14 elapsed=4m6.746s
peercount=0 tried=122 static=0
number=27 sealhash=9d79d9..c1a59b hash=395b5d..2e7b8c elapsed=6.812s
number=20 hash=09883d..26b91f
number=27 hash=395b5d..2e7b8c
number=28 sealhash=68dd7e..d405b3 uncles=0 txs=0 gas=0 fees=0 elapsed="245.729µs"
number=28 sealhash=68dd7e..d405b3 uncles=0 txs=0 gas=0 fees=0 elapsed="734.943µs"
peercount=1 tried=61 static=0
number=28 sealhash=68dd7e..d405b3 hash=3c34c7..83813b elapsed=9.808s
number=21 hash=65fcc1..f5c436
number=28 hash=3c34c7..83813b
number=29 sealhash=b004a9..82ef65 uncles=0 txs=0 gas=0 fees=0 elapsed="262.732µs"
number=29 sealhash=b004a9..82ef65 uncles=0 txs=0 gas=0 fees=0 elapsed="595.274µs"
epoch=1 percentage=15 elapsed=4m21.983s
number=29 sealhash=b004a9..82ef65 hash=db741a..fcbff4 elapsed=6.179s
number=22 hash=67342b..4db751
number=29 hash=db741a..fcbff4
number=30 sealhash=dd5b8d..7da0f0 uncles=0 txs=0 gas=0 fees=0 elapsed="224.518µs"
number=30 sealhash=dd5b8d..7da0f0 uncles=0 txs=0 gas=0 fees=0 elapsed="637.449µs"
peercount=0 tried=107 static=0
epoch=1 percentage=16 elapsed=4m36.400s
number=30 sealhash=dd5b8d..7da0f0 hash=b0b474..f5f0e9 elapsed=13.985s
number=23 hash=2c58ca..9c9caf
number=30 hash=b0b474..f5f0e9
number=31 sealhash=fc557a..c61d7a uncles=0 txs=0 gas=0 fees=0 elapsed="254.471µs"
number=31 sealhash=fc557a..c61d7a uncles=0 txs=0 gas=0 fees=0 elapsed="738.023µs"
peercount=0 tried=117 static=0

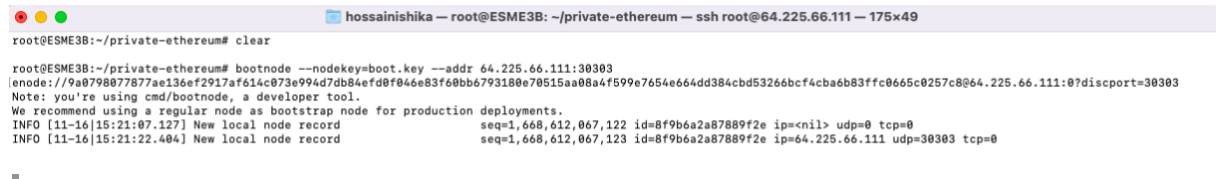
```

- Vérifions la création du block 1

[illegible]

- Quittons la console geth et affectons notre adresse ip à notre nœud grâce à la commande suivante :

```
bootnode --nodekey=boot.key --addr 64.225.66.111:30303
```



```
hossainishika — root@ESME3B: ~/private-ethereum — ssh root@64.225.66.111 — 175x49
root@ESME3B:~/private-ethereum# clear

root@ESME3B:~/private-ethereum# bootnode --nodekey=boot.key --addr 64.225.66.111:30303
[enode://9a0798077877ae136ef2917af614c073e994d7db84efd0f04e83f60bb6793180e70515aa08a4f599e7654e664dd384cbd53266bcf4c6a6b83ffc0665c0257c8@64.225.66.111:0?discport=30303
Note: you're using cmd/bootnode, a developer tool.
We recommend using a regular node as bootstrap node for production deployments.
INFO [11-16|15:21:07.127] New local node record seq=1,668,612,067,122 id=8f9b6a2a87889f2e ip=<nil> udp=0 tcp=0
INFO [11-16|15:21:22.404] New local node record seq=1,668,612,067,123 id=8f9b6a2a87889f2e ip=64.225.66.111 udp=30303 tcp=0
```

## VI. Démarrage des nœuds

---

- Commande lancée côté serveur :

```
geth --networkid 12345678 --nat extip:64.225.66.111 --datadir data console
> net.listening
```

- Commande lancée côté client :

```
geth --networkid 12345678 --datadir data --bootnodes
enode://f0c175d4ddf4432e3e915e4d5d1137f5073853a3d5ceeffe627a781a5dff
1dc4f97412ba71dc1578ed29e2ee77aaa629c0eb33d65d0a970fabaa92c3691d19
d8@64.225.66.111:30303 console
> net.listening
```



Voici ce qu'on aperçoit côté serveur :

```

root@ESME3B:~/private-ethereum# geth --networkid 12345678 --nat extip:64.225.66.111 --datadir data console
INFO [11-16|14:29:19.121] Maximum peer count ETH=50 LES=0 total=50
INFO [11-16|14:29:19.124] Smartcard socket not found, disabling
WARN [11-16|14:29:19.141] Sanitizing cache to Go's GC limits err="stat /run/pcscd/pcscd.comm: no such file or directory"
INFO [11-16|14:29:19.142] Set global gas cap provided=1024 updated=664
INFO [11-16|14:29:19.147] Allocated trie memory caches cap=50,000,000
INFO [11-16|14:29:19.148] Allocated cache and file handles clean=99.00MiB dirty=166.00MiB
INFO [11-16|14:29:19.182] Opened ancient database database=/root/private-ethereum/data/geth/chaindata cache=332.00MiB handles=524,288
INFO [11-16|14:29:19.184] database=/root/private-ethereum/data/geth/chaindata/ancient/chain readonly=false
INFO [11-16|14:29:19.184] -----
INFO [11-16|14:29:19.184] Chain ID: 12345678 (unknown)
INFO [11-16|14:29:19.184] Consensus: Ethash (proof-of-work)
INFO [11-16|14:29:19.184] Pre-Merge hard forks:
INFO [11-16|14:29:19.184] - Homestead: 0 (https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/homestead.md)
INFO [11-16|14:29:19.184] - Tangerine Whistle (EIP 150): 0 (https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/tangerine-whistle.md)
INFO [11-16|14:29:19.184] - Spurious Dragon/1 (EIP 155): 0 (https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/spurious-dragon.md)
INFO [11-16|14:29:19.184] - Spurious Dragon/2 (EIP 158): 0 (https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/spurious-dragon.md)
INFO [11-16|14:29:19.184] - Byzantium: 0 (https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/byzantium.md)
INFO [11-16|14:29:19.184] - Constantinople: 0 (https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/constantinople.md)
INFO [11-16|14:29:19.185] - Petersburg: 0 (https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/petersburg.md)
INFO [11-16|14:29:19.185] - Istanbul: <nil> (https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/istanbul.md)
INFO [11-16|14:29:19.185] - Berlin: <nil> (https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/berlin.md)
INFO [11-16|14:29:19.185] - London: <nil> (https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/london.md)
INFO [11-16|14:29:19.185] The Merge is not yet available for this network!
INFO [11-16|14:29:19.185] - Hard-fork specification: https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/paris.md
INFO [11-16|14:29:19.185] -----
INFO [11-16|14:29:19.187] Disk storage enabled for ethash caches dir=/root/private-ethereum/data/geth/ethash count=3
INFO [11-16|14:29:19.187] Disk storage enabled for ethash DAGs dir=/root/.ethash count=2
INFO [11-16|14:29:19.188] Initialising Ethereum protocol network=12,345,678 dbversion=8
INFO [11-16|14:29:19.191] Loaded most recent local header number=52 hash=84f992..be4616 td=6,847,169 age=1w3d20h
INFO [11-16|14:29:19.191] Loaded most recent local full block number=52 hash=84f992..be4616 td=6,847,169 age=1w3d20h
INFO [11-16|14:29:19.191] Loaded most recent local fast block number=52 hash=84f992..be4616 td=6,847,169 age=1w3d20h
INFO [11-16|14:29:19.215] Loaded local transaction journal transactions=0 dropped=0
INFO [11-16|14:29:19.216] Regenerated local transaction journal transactions=0 accounts=0
WARN [11-16|14:29:19.216] Switch sync mode from snap sync to full sync
INFO [11-16|14:29:19.218] Gasprice oracle is ignoring threshold set threshold=2
WARN [11-16|14:29:19.218] Engine API enabled protocol=eth
WARN [11-16|14:29:19.219] Engine API started but chain not configured for merge yet
INFO [11-16|14:29:19.220] Starting peer-to-peer node instance=Geth/v1.10.26-stable-e5eb32ac/linux-amd64/go1.18.5
INFO [11-16|14:29:19.371] Mapped network port proto=tcp extport=30303 intport=30303 interface=ExtIP(64.225.66.111)
INFO [11-16|14:29:19.390] Mapped network port proto=udp extport=30303 intport=30303 interface=ExtIP(64.225.66.111)
INFO [11-16|14:29:19.403] New local node record seq=1,667,668,636,886 id=7f3efd948e267ed1 ip=64.225.66.111 udp=30303 tcp=30303
INFO [11-16|14:29:19.408] IPC endpoint opened path=/root/private-ethereum/data/geth.ipc
INFO [11-16|14:29:19.408] Loaded JWT secret file url=ws://127.0.0.1:8551
INFO [11-16|14:29:19.410] WebSocket enabled

```

On écoute tous les ports :

```
> net.listening
true
> WARN [11-16|14:30:52.859] Snapshot extension registration failed peer=88f932f1 err="peer connected on snap without compatible eth support"
INFO [11-16|14:30:53.398] Looking for peers peercount=0 tried=146 static=0
```

Une fois que la synchronisation entre le serveur et les clients s'est bien effectuée, on s'assure que les premiers blocks sont identiques sur le server mais également chez le client :

*Côté serveur :*

*Côté Client :*

[illegible][illegible]

On remarque bien qu'il s'agit du même block, avec le même numéro de hash.

Côté serveur, on commence également à miner au sein de la blockchain :

```
hossainishika — root@ESME3B: ~/private-ethereum — ssh root@64.225.66.111 — 167x49
> miner.start(1)
INFO [11-16|16:52:06.899] Updated mining threads threads=1
INFO [11-16|16:52:06.900] Transaction pool price threshold updated price=1,000,000,000
null
> INFO [11-16|16:52:06.901] Commit new sealing work number=53 sealhash=c561bb..c8ede2 uncles=0 txs=0 gas=0 fees=0 elapsed="521.596µs"
INFO [11-16|16:52:06.902] Commit new sealing work number=53 sealhash=c561bb..c8ede2 uncles=0 txs=0 gas=0 fees=0 elapsed=1.323ms
INFO [11-16|16:52:14.681] Looking for peers peercount=4 tried=171 static=0
WARN [11-16|16:52:17.856] Snapshot extension registration failed peer=93cf0652 err="peer connected on snap without compatible eth support"
WARN [11-16|16:52:21.013] Snapshot extension registration failed peer=181502b5 err="peer connected on snap without compatible eth support"
INFO [11-16|16:52:23.164] Generating DAG in progress epoch=1 percentage=0 elapsed=14.266s
INFO [11-16|16:52:25.227] Looking for peers peercount=3 tried=119 static=0
WARN [11-16|16:52:29.105] Snapshot extension registration failed peer=c1bb7cc4 err="peer connected on snap without compatible eth support"
INFO [11-16|16:52:32.653] Successfully sealed new block number=53 sealhash=c561bb..c8ede2 hash=172f0f..0df89d elapsed=25.752s
INFO [11-16|16:52:32.653] \ mined potential block number=53 hash=172f0f..0df89d
INFO [11-16|16:52:32.654] Commit new sealing work number=54 sealhash=fc062b..d1b77c uncles=0 txs=0 gas=0 fees=0 elapsed="154.322µs"
INFO [11-16|16:52:32.654] Commit new sealing work number=54 sealhash=fc062b..d1b77c uncles=0 txs=0 gas=0 fees=0 elapsed="406.957µs"
INFO [11-16|16:52:35.542] Looking for peers peercount=3 tried=131 static=0
INFO [11-16|16:52:36.707] Generating DAG in progress epoch=1 percentage=1 elapsed=27.808s
INFO [11-16|16:52:45.558] Looking for peers peercount=3 tried=114 static=0
INFO [11-16|16:52:50.409] Generating DAG in progress epoch=1 percentage=2 elapsed=41.510s
INFO [11-16|16:52:54.095] Successfully sealed new block number=54 sealhash=fc062b..d1b77c hash=0fde6e..4b2017 elapsed=21.441s
INFO [11-16|16:52:54.096] \ mined potential block number=54 hash=0fde6e..4b2017
INFO [11-16|16:52:54.110] Commit new sealing work number=55 sealhash=73062b..af4507 uncles=0 txs=0 gas=0 fees=0 elapsed="156.665µs"
INFO [11-16|16:52:54.110] Commit new sealing work number=55 sealhash=73062b..af4507 uncles=0 txs=0 gas=0 fees=0 elapsed="452.119µs"
INFO [11-16|16:52:55.665] Looking for peers peercount=3 tried=153 static=0
INFO [11-16|16:52:57.077] Successfully sealed new block number=55 sealhash=73062b..af4507 hash=81efc4..486ff1 elapsed=2.966s
INFO [11-16|16:52:57.077] \ mined potential block number=55 hash=81efc4..486ff1
INFO [11-16|16:52:57.077] Commit new sealing work number=56 sealhash=0f928b..85d240 uncles=0 txs=0 gas=0 fees=0 elapsed="120.847µs"
INFO [11-16|16:52:57.077] Commit new sealing work number=56 sealhash=0f928b..85d240 uncles=0 txs=0 gas=0 fees=0 elapsed="355.713µs"
INFO [11-16|16:53:04.296] Generating DAG in progress epoch=1 percentage=3 elapsed=55.398s
INFO [11-16|16:53:05.869] Looking for peers peercount=3 tried=179 static=0
INFO [11-16|16:53:06.233] Successfully sealed new block number=56 sealhash=0f928b..85d240 hash=e2c03b..8ea5c1 elapsed=9.156s
INFO [11-16|16:53:06.233] \ mined potential block number=56 hash=e2c03b..8ea5c1
INFO [11-16|16:53:06.234] Commit new sealing work number=57 sealhash=6bc038..b96197 uncles=0 txs=0 gas=0 fees=0 elapsed="196.531µs"
INFO [11-16|16:53:06.234] Commit new sealing work number=57 sealhash=6bc038..b96197 uncles=0 txs=0 gas=0 fees=0 elapsed="479.902µs"
INFO [11-16|16:53:09.656] Successfully sealed new block number=57 sealhash=6bc038..b96197 hash=89b042..1b2067 elapsed=3.421s
INFO [11-16|16:53:09.656] \ mined potential block number=57 hash=89b042..1b2067
INFO [11-16|16:53:09.675] Commit new sealing work number=58 sealhash=444fa5..b52027 uncles=0 txs=0 gas=0 fees=0 elapsed="195.002µs"
INFO [11-16|16:53:09.675] Commit new sealing work number=58 sealhash=444fa5..b52027 uncles=0 txs=0 gas=0 fees=0 elapsed="468.302µs"
INFO [11-16|16:53:11.881] Successfully sealed new block number=58 sealhash=444fa5..b52027 hash=202568..c62974 elapsed=2.206s
INFO [11-16|16:53:11.882] \ mined potential block number=58 hash=202568..c62974
INFO [11-16|16:53:11.900] Commit new sealing work number=59 sealhash=258893..e205ea uncles=0 txs=0 gas=0 fees=0 elapsed="357.921µs"
INFO [11-16|16:53:11.901] Commit new sealing work number=59 sealhash=258893..e205ea uncles=0 txs=0 gas=0 fees=0 elapsed="784.356µs"
INFO [11-16|16:53:14.038] Successfully sealed new block number=59 sealhash=258893..e205ea hash=7d1606..c3d149 elapsed=2.137s
INFO [11-16|16:53:14.038] \ mined potential block number=59 hash=7d1606..c3d149
INFO [11-16|16:53:14.054] Commit new sealing work number=60 sealhash=49930a..0fc583 uncles=0 txs=0 gas=0 fees=0 elapsed="171.673µs"
INFO [11-16|16:53:14.054] Commit new sealing work number=60 sealhash=49930a..0fc583 uncles=0 txs=0 gas=0 fees=0 elapsed="470.399µs"
INFO [11-16|16:53:16.117] Looking for peers peercount=3 tried=110 static=0
INFO [11-16|16:53:16.123] Successfully sealed new block number=60 sealhash=49930a..0fc583 hash=cc8c15..e38e4a elapsed=2.069s
```

On essaye d'envoyer des transactions entre serveurs et clients :

- On déverrouille le compte 0 du serveur afin d'envoyer la transaction au client :

```
personal.unlockAccount(eth.accounts[0])
```

```
[> personal.unlockAccount(eth.accounts[0])
Unlock account 0x8bf6f8c459db71707bb60fd5ea86bd2895c60e00
Passphrase: INFO [11-17|09:36:36.867] Looking for peers peercount=0 tried=92 static=0

true
```

- On envoie ensuite une transaction d'une valeur de 25000 à l'un des clients :

```
eth.sendTransaction({to: "0xd528027ab46f76700e7b5e59326132b37ba52b03", from:
eth.accounts[0], value: 25000})
```



- ```
eth.getBalance("0x8bf6f8c459db71707bb60fd5ea86bd2895c60e00")
```