TIC-BLK4

Rapport de réalisation

Etape 1

Tutorial 1 - Set up a private Blockchain network

Thomas SIMOES

Installation de Geth:

```bash
#! /bin/bash

sudo add-apt-repository ppa:ethereum/ethereum
cp install/source.list /etc/apt/sources.list.d/ethereum-bionic.list
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 2A518C819BE37D2C2031944D1C52189C923F6CA9
sudo apt-get update
sudo apt-get install ethereum

mkdir -p ../ethereum
mkdir -p ../ethereum/account/keystore
mkdir -p ../ethereum/genesis/keystore

mkdir -p ./tmp
```

Création d'un nouveau compte:

- Script de création de compte:

```bash
#! /bin/bash

if [ $# -eq 0 ]; then
    exit
fi

geth --datadir ../ethereum/account account  new --password $1
cp ../ethereum/account/keystore/* ../ethereum/genesis/keystore
```

- Retour du script:

```
[debian@debian:~/Documents/ethereum/script$ ./new_account.sh password/debian.txt
INFO [10-04|10:46:27.545] Maximum peer count                       ETH=50 LES=0 total=50
INFO [10-04|10:46:27.545] Smartcard socket not found, disabling    err="stat /run/pcscd/pcscd.comm: no such file or directory"

Your new key was generated

Public address of the key:   0x96C195c866dd41576316Af22dC52a43426bcb13F
Path of the secret key file: ../ethereum/account/keystore/UTC--2019-10-04T08-46-27.545627401Z--96c195c866dd41576316af22dc52a43426bcb13f

- 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!
[debian@debian:~/Documents/ethereum/script$ ls ../ethereum/genesis/keystore/UTC--2019-10-04T08-46-27.545627401Z--96c195c866dd41576316af22dc52a43426bcb13f
../ethereum/genesis/keystore/UTC--2019-10-04T08-46-27.545627401Z--96c195c866dd41576316af22dc52a43426bcb13f
[debian@debian:~/Documents/ethereum/script$ ./new_account.sh password/ubuntu.txt
INFO [10-04|10:47:08.884] Maximum peer count                       ETH=50 LES=0 total=50
INFO [10-04|10:47:08.884] Smartcard socket not found, disabling    err="stat /run/pcscd/pcscd.comm: no such file or directory"

Your new key was generated

Public address of the key:   0x9ED607F98C332cC6dEFAf22b8f7ee9dFCBD73F76
Path of the secret key file: ../ethereum/account/keystore/UTC--2019-10-04T08-47-08.885157232Z--9ed607f98c332cc6defaf22b8f7ee9dfcbd73f76

- 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!
```

Initialisation de Geth:

- Script de démarrage:

```
#! /bin/bash

mkdir -p ./config
geth --datadir ../ethereum/genesis init ./config/genesis.json
```

- Retour:

```
[debian@debian:~/Documents/ethereum/script$ ./genesis.sh
INFO [10-04|10:50:51.777] Maximum peer count                       ETH=50 LES=0 total=50
INFO [10-04|10:50:51.777] Smartcard socket not found, disabling     err="stat /run/pcscd/pcscd.comm: no such file or directory"
INFO [10-04|10:50:51.779] Allocated cache and file handles          database=/home/debian/Documents/ethereum/ethereum/genesis/geth/chaindata cache=16.00MiB handles=16
INFO [10-04|10:50:51.791] Writing custom genesis block
INFO [10-04|10:50:51.792] Persisted trie from memory database       nodes=3 size=413.00B time=368.835µs gcnodes=0 gcsize=0.00B gctime=0s livenodes=1 livesize=0.00B
INFO [10-04|10:50:51.792] Successfully wrote genesis state          database=chaindata hash=e8a816…b882aa
INFO [10-04|10:50:51.792] Allocated cache and file handles          database=/home/debian/Documents/ethereum/ethereum/genesis/geth/lightchaindata cache=16.00MiB handles=16
INFO [10-04|10:50:51.800] Writing custom genesis block
INFO [10-04|10:50:51.801] Persisted trie from memory database       nodes=3 size=413.00B time=485.625µs gcnodes=0 gcsize=0.00B gctime=0s livenodes=1 livesize=0.00B
INFO [10-04|10:50:51.802] Successfully wrote genesis state          database=lightchaindata hash=e8a816…b882aa
```

Geth JavaScript Console:

```
eth.log  bootstrap_node.sh  config  genesis.sh  install  install.sh  new_account.sh  nohup.out  password  run.sh  templates  tmp
[debian@debian:~/Documents/ethereum/script$ ./run.sh
WARN [10-04|10:55:43.887] Sanitizing cache to Go's GC limits        provided=1024 updated=665
INFO [10-04|10:55:43.889] Maximum peer count                       ETH=50 LES=0 total=50
INFO [10-04|10:55:43.889] Smartcard socket not found, disabling     err="stat /run/pcscd/pcscd.comm: no such file or directory"
INFO [10-04|10:55:43.890] Starting peer-to-peer node                instance=Geth/v1.9.6-stable-bd059680/linux-amd64/go1.11.5
INFO [10-04|10:55:43.890] Allocated trie memory caches              clean=166.00MiB dirty=166.00MiB
INFO [10-04|10:55:43.890] Allocated cache and file handles          database=/home/debian/Documents/ethereum/ethereum/genesis/geth/chaindata cache=332.00MiB handles=524288
INFO [10-04|10:55:43.916] Opened ancient database                   database=/home/debian/Documents/ethereum/ethereum/genesis/geth/chaindata/ancient
INFO [10-04|10:55:43.916] Initialised chain configuration           config="{ChainID: 2019 Homestead: 0 DAO: <nil> DAOSupport: false EIP150: <nil> EIP155: 0 EIP158: 0 Byzantium: 0 Constantinople: <nil> Petersburg: <nil> Istanbul: <nil> Eng
ine: unknown}"
INFO [10-04|10:55:43.916] Disk storage enabled for ethash caches    dir=/home/debian/Documents/ethereum/ethereum/genesis/geth/ethash count=3
INFO [10-04|10:55:43.916] Disk storage enabled for ethash DAGs      dir=/home/debian/.ethash count=2
INFO [10-04|10:55:43.916] Initialising Ethereum protocol            versions=[63] network=2019 dbversion=7
INFO [10-04|10:55:43.934] Loaded most recent local header           number=0 hash=e8a816…b882aa td=400 age=50y5mo3w
INFO [10-04|10:55:43.934] Loaded most recent local full block       number=0 hash=e8a816…b882aa td=400 age=50y5mo3w
INFO [10-04|10:55:43.934] Loaded most recent local fast block       number=0 hash=e8a816…b882aa td=400 age=50y5mo3w
INFO [10-04|10:55:43.935] Loaded local transaction journal          transactions=0 dropped=0
INFO [10-04|10:55:43.935] Regenerated local transaction journal     transactions=0 accounts=0
INFO [10-04|10:55:43.939] Allocated fast sync bloom                 size=332.00MiB
INFO [10-04|10:55:43.942] Initialized fast sync bloom               items=3 errorrate=0.000 elapsed=2.526ms
INFO [10-04|10:55:43.956] New local node record                     seq=2 id=762db1fa076ee748 ip=127.0.0.1 udp=30303 tcp=30303
INFO [10-04|10:55:43.957] Started P2P networking                    self=enode://cacca5ccc35df03f85502baf6e0b892ac6bcacf462fdd4b020b57b0c071aaa3fe82cb3ca47558c9356b7d2dd951f5808c15543369a3c3cbd38c5c88e776bf474@127.0.0.1:30303
INFO [10-04|10:55:43.960] IPC endpoint opened                       url=/home/debian/Documents/ethereum/ethereum/genesis/geth.ipc
INFO [10-04|10:55:44.074] Etherbase automatically configured        address=0x96C195c866dd41576316Af22dC52a43426bcb13F
Welcome to the Geth JavaScript console!

instance: Geth/v1.9.6-stable-bd059680/linux-amd64/go1.11.5
coinbase: 0x96c195c866dd41576316af22dc52a43426bcb13f
at block: 0 (Thu, 01 Jan 1970 01:00:00 CET)
 datadir: /home/debian/Documents/ethereum/ethereum/genesis
 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 txpool:1.0 web3:1.0

> e
encodeURI encodeURIComponent escape eth ethash eval
> e
encodeURI encodeURIComponent escape eth ethash eval
> eth
eth ethash
> eth.
eth._requestManager       eth.defaultAccount        eth.getBlockByHash        eth.getHeaderByHash       eth.getStorageAt          eth.iban                  eth.sendRawTransaction
eth.accounts              eth.defaultBlock          eth.getBlockByNumber      eth.getHeaderByNumber     eth.getSyncing            eth.icapNamereg           eth.sendTransaction
eth.blockNumber           eth.estimateGas           eth.getBlockNumber        eth.getMining             eth.isSyncing             eth.sign
eth.call                  eth.fillTransaction       eth.getBlockTransactionCount eth.getMining          eth.getTransactionCount   eth.mining                eth.signTransaction
eth.chainId               eth.filter                eth.getBlockUncleCount    eth.getPendingTransactions eth.getTransactionFromBlock eth.namereg             eth.submitTransaction
eth.coinbase              eth.gasPrice              eth.getCode               eth.getProof              eth.getTransactionReceipt eth.pendingTransactions   eth.submitWork
eth.compile               eth.getAccounts           eth.getCoinbase           eth.getProtocolVersion    eth.getUncle              eth.protocolVersion       eth.syncing
eth.constructor           eth.getBalance            eth.getCompilers          eth.getRawTransaction     eth.getWork               eth.resend
eth.contract              eth.getBlock              eth.getGasPrice           eth.getRawTransactionFromBlock eth.hashrate         eth.sendIBANTransaction
> eth.
eth._requestManager       eth.defaultAccount        eth.getBlockByHash        eth.getHeaderByHash       eth.getStorageAt          eth.iban                  eth.sendRawTransaction
eth.accounts              eth.defaultBlock          eth.getBlockByNumber      eth.getHeaderByNumber     eth.getSyncing            eth.icapNamereg           eth.sendTransaction
eth.blockNumber           eth.estimateGas           eth.getBlockNumber        eth.getMining             eth.isSyncing             eth.sign
eth.call                  eth.fillTransaction       eth.getBlockTransactionCount eth.getMining          eth.getTransactionCount   eth.mining                eth.signTransaction
eth.chainId               eth.filter                eth.getBlockUncleCount    eth.getPendingTransactions eth.getTransactionFromBlock eth.namereg             eth.submitTransaction
eth.coinbase              eth.gasPrice              eth.getCode               eth.getProof              eth.getTransactionReceipt eth.pendingTransactions   eth.submitWork
eth.compile               eth.getAccounts           eth.getCoinbase           eth.getProtocolVersion    eth.getUncle              eth.protocolVersion       eth.syncing
eth.constructor           eth.getBalance            eth.getCompilers          eth.getRawTransaction     eth.getWork               eth.resend
eth.contract              eth.getBlock              eth.getGasPrice           eth.getRawTransactionFromBlock eth.hashrate         eth.sendIBANTransaction
> eth.accounts
["0x96c195c866dd41576316af22dc52a43426bcb13f", "0x9ed607f98c332cc6defaf22b8f7ee9dfcbd73f76"]
>
```

Commande pour récupérer les Ether:

```
[> web3.fromWei(eth.getBalance(0x96c195c866dd41576316af22dc52a43426bcb13f), "ether")
Error: invalid address
    at web3.js:3930:15
    at web3.js:5025:28
    at map (<native code>)
    at web3.js:5024:12
    at web3.js:5050:18
    at web3.js:5075:23
    at <anonymous>:1:15

[> web3.fromWei(eth.getBalance("0x96c195c866dd41576316af22dc52a43426bcb13f"), "ether")
 100000
[> web3.fromWei(eth.getBalance("0x9ed607f98c332cc6defaf22b8f7ee9dfcbd73f76"), "ether")
 120000
```

Configuration et lancement du bootnode:

Lancement d'un noeud membre:

Lancement d'une instance Geth pour miner:

Réalisation d'une transaction:

```
Welcome to the Geth JavaScript console!

instance: Geth/v1.9.6-stable-bd059680/linux-amd64/go1.11.5
coinbase: 0x96c195c866dd41576316af22dc52a43426bcb13f
at block: 19 (Fri, 04 Oct 2019 11:32:55 CEST)
 datadir: /home/debian/Documents/ethereum/ethereum/genesis
 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 txpool:1.0 web3:1.0

> eth.accounts
["0x96c195c866dd41576316af22dc52a43426bcb13f", "0x9ed607f98c332cc6defaf22b8f7ee9dfcbd73f76"]
> eth.sendTransaction({ from: eth.accounts[0], to: eth.accounts[1], value: Web3.toWei(1000, "ether")});
TypeError: 'toWei' is not a function
    at <anonymous>:1:74

> eth.sendTransaction({ from: eth.accounts[0], to: eth.accounts[1], value: web3.toWei(1000, "ether")});
WARN [10-04|11:35:15.555] Served eth_sendTransaction              reqid=14 t=8.411079ms err="authentication needed: password or unlock"
Error: authentication needed: password or unlock
    at web3.js:3143:20
    at web3.js:6347:15
    at web3.js:5081:36
    at <anonymous>:1:1

> personal.un
personal.unlockAccount personal.unpair
> personal.un
personal.unlockAccount personal.unpair
> personal.unlockAccount(eth.accounts[1])
Unlock account 0x9ed607f98c332cc6defaf22b8f7ee9dfcbd73f76
Password:
true
> eth.sendTransaction({ from: eth.accounts[0], to: eth.accounts[1], value: web3.toWei(1000, "ether")});
WARN [10-04|11:35:42.990] Served eth_sendTransaction              reqid=19 t=1.923758ms err="authentication needed: password or unlock"
Error: authentication needed: password or unlock
    at web3.js:3143:20
    at web3.js:6347:15
    at web3.js:5081:36
    at <anonymous>:1:1

> web3.fromWei(eth.getBalance("0x96c195c866dd41576316af22dc52a43426bcb13f"), "ether")^C
> personal.un
personal.unlockAccount personal.unpair
> personal.unlockAccount(eth.accounts[0])
Unlock account 0x96c195c866dd41576316af22dc52a43426bcb13f
Password:
true
> eth.sendTransaction({ from: eth.accounts[0], to: eth.accounts[1], value: web3.toWei(1000, "ether")});
INFO [10-04|11:36:09.313] Setting new local account               address=0x96C195c866dd41576316Af22dC52a43426bcb13F
INFO [10-04|11:36:09.314] Submitted transaction                   fullhash=0x250173852a2f1aa8ba44bb8f483a096599e9cad27a035dd0142066bd0c3cb803 recipient=0x9ED607F98C332cC6dEFAf22b8f7ee9dFCBD73F76
"0x250173852a2f1aa8ba44bb8f483a096599e9cad27a035dd0142066bd0c3cb803"
>
> 
```