Cài đặt Geth (private ethereum blockchain)

* Cài đặt Geth trên Centos 7

1. Download geth tại địa chỉ <https://geth.ethereum.org/downloads/>

<https://github.com/ethereum/go-ethereum/wiki/Installing-Geth>

|  |
| --- |
| $ add-apt-repository -y ppa:ethereum/ethereum  $ apt-get update  $ apt-get install geth |

1. Thiết lập và cấu hình (<https://medium.com/blockchainbistro/set-up-a-private-ethereum-blockchain-and-deploy-your-first-solidity-smart-contract-on-the-caa8334c343d>)

Ở bước này cần làm 2 việc sau

* Configuring genesis block
* Initiating the chain data in blockchain
  1. Cấu hình khố genesis

genesis.json file

|  |
| --- |
| {    "config": {      "chainId": 2020,      "homesteadBlock": 0,      "eip150Block": 0,      "eip155Block": 0,      "eip158Block": 0    },    "alloc": {},    "coinbase": "0x0000000000000000000000000000000000000000",    "difficulty": "0x400",    "extraData": "",    "gasLimit": "0x2fefd8",    "nonce": "0x0000000000000042",    "mixhash": "0x0000000000000000000000000000000000000000000000000000000000000000",    "parentHash": "0x0000000000000000000000000000000000000000000000000000000000000000",    "timestamp": "0x00"  } |
|  |

Giải thích các trường trong genesis file

(<https://gist.github.com/0mkara/b953cc2585b18ee098cd>)

<https://medium.com/blockchainbistro/set-up-a-private-ethereum-blockchain-and-deploy-your-first-solidity-smart-contract-on-the-caa8334c343d>

<https://medium.com/coinmonks/ethereum-setting-up-a-private-blockchain-67bbb96cf4f1>

**Config:** Đây là phần quan trọng nhất trong cấu hình blockchain và nó có các thuộc tính sau.

**chainId:** Mã định danh của private blockchain. Mỗi private blockchain sẽ có mã định danh này khác nhau

**homesteadBlock:**  homestead là phiên bản phát hành đầu tiên của Ethereum. Vì các lập trình viên sử dụng phiên bản này nên giá trị của thuộc tính này được đặt là ‘0’.

**eip150Block/ eip155Block/ eip158Block:** EIP là viết tắt của “Ethereum Improvement Proposals”. Những thông tin này đã được thực hiện để phát hành Homestead. Đối với private blockchain các thông tin này không cần thiết nên được đặt là ‘0’.

**alloc:** Cho phép xác định danh sách các địa chỉ và cấp ETH cho các địa chỉ này. Đó là chức năng của Ethereum dùng đê xử lý giai đoạn “Ether pre-sale” (bán trước ETH). Đối với private blockchian, ta có thể khai thác ETH nhanh chóng nên không sử dụng tùy chọn này.

**coinbase:** còn được gọi là etherbase là tài khoản mặc định. Giá trị này được đặt là địa chỉ của người khai thác khi một khối mới được tạo.

**difficulty:** Xác định độ khó của mạng khi khai thác 1 khối. Độ khó càng cao, các công cụ khai khác phải tính toán càng nhiều để khai thác được 1 khối hợp lệ. Giá trị này được sử dụng để kiểm soát thời gian tạo ra khối mới trong phạm vi mục tiêu. Đối với private blockchain ta nên đặt nó bằng giá trị thấp để đảm bảo các khối được khai thác nhanh hơn dẫn đến các giao dịch sẽ nhanh hơn.

**gasLimit:** Xác đinh lượng gas tối đa có thể được sử dụng trong một khối. Giá trị càng cao thì 1 khối có thể chứa được càng nhiều giao dịch.

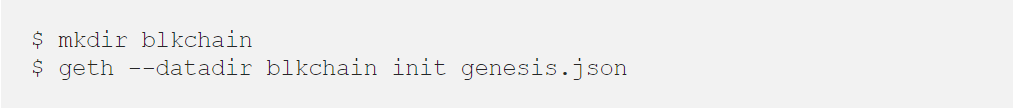
**nonce:** Giá trị hash 64-bit ngẫu nhiên được các nhà khai thác phải đi tìm. Giá trị nonce cuối cùng là kết quả của quá trình lặp quá trình khai thác (Mining Target), thuật toán có thể khám phải một giá trị nonce thỏa mãn mục tiêu khai thác.

**mixHash:** Sự kết hợp giữa nonce và mixHash phải thỏa mãn điều kiện toán học được mô tả trong Yellowsheet. Nó cho phép xác định rằng khối này đã được khai thác và hợp lệ.

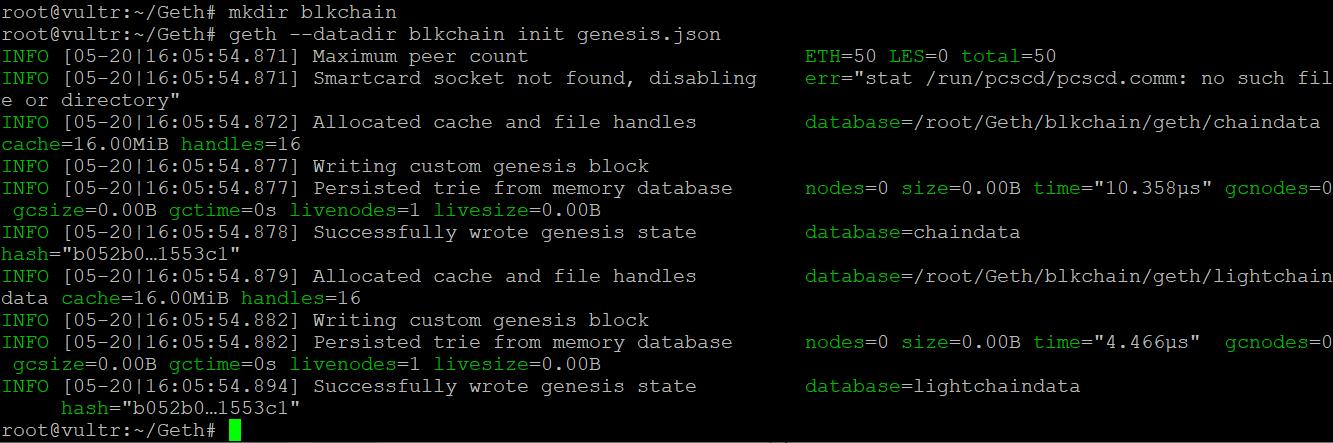
**parentHash:** Hàm băm Keccak 256-bit băm toàn bộ thông tin của khối cha (bao gồm cả nonce và mixHash). Tạo liên kết tới khối cha giúp xây dựng hệ thống blockchain an toàn hơn. Trong khối genesis giá trị này bằng 0 và chỉ duy nhất trong khối này.

**timeStamp:** Giá trị này cho phép xác định thứ tự của các khối trong blockchain. Ngoài ra nó còn giúp xác định khoảng thời gian giữa 2 khối liên tiếp để điều chỉnh độ khó trong mạng cho hệ thống có thể hoạt động ổn định. Nếu khoảng thời gian này quá lớn, độ khó và thời gian dự kiến của khối tiếp theo sẽ giảm.

* 1. **Tạo thư mục lưu trữ blockchain**



Dòng thứ 2 khởi tạo blockchain và dữ liệu blockchain sẽ được lưu trữ trong thư mục blkchain. Thư mục này sẽ tăng kí thước khi dữ liệu được thêm vào blockchain.



Khởi tạo thành công

* 1. Khởi tạo và chạy private blockchain

Chúng ta cần thiết lập geth chạy như một dịch vụ trên centos để có thể kết nối qua HTTP-RPC và có được thông tin trên blockchain.

Để làm được điều này chúng ta cài đặt ‘supervisor’, nó sẽ chịu trách nhiệm tự động khởi động geth khi server khởi động và khởi động lại nếu nó bị lỗi không không mong muốn.

|  |
| --- |
| $ apt-get install supervisor |

Tạo file cấu hình cho supervisor để nó chạy geth. Tạo file /etc/supervisor/conf.d/geth.conf và điền vào:

|  |
| --- |
| [program:geth]  command=/usr/bin/geth --networkid 1508 --datadir=~/Geth/blkchain --nodiscover --gasprice 0 --rpc --rpcport 8545 --rpcaddr "0.0.0.0" --rpccorsdomain "\*" --rpcapi "admin,eth,net,web3,personal,miner"  autostart=true  autorestart=true  stderr\_logfile=/var/log/supervisor/geth.err.log  stdout\_logfile=/var/log/supervisor/geth.out.log |

Lưu ý: --rpcaddr “0.0.0.0” cho mục đích phát triển và thử nghiệm. Vì nó cho phép tất cả các kết nối đến

Bây giờ chỉ cần khởi động lại trình giám sát để khởi động geth:

|  |
| --- |
| $ supervisorctl reload |

ở local dùng để kết nối đến geth

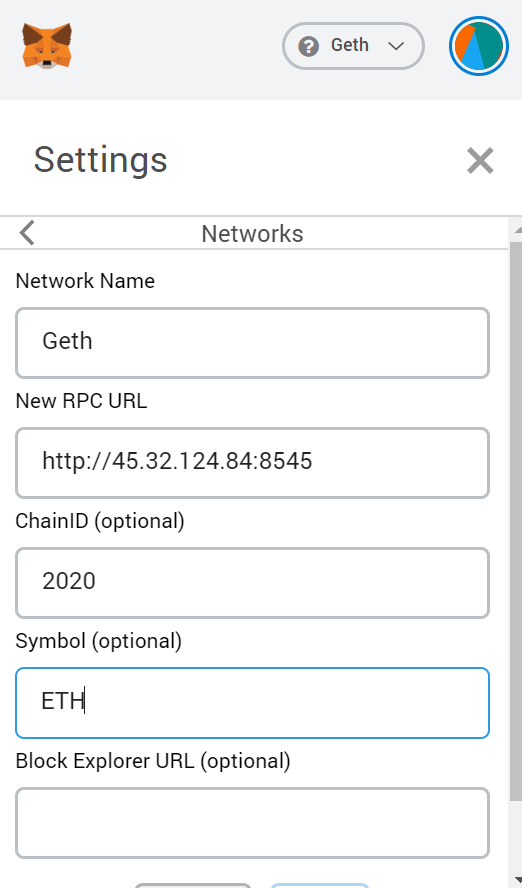
|  |
| --- |
| $ geth attach http://45.32.124.84:8545 |

Để xem log file real-time của geth xem có được mine hay không

Địa chỉ này được cấu hình trong supervisor

|  |
| --- |
| **root@vultr:/#** cd var/log/supervisor  **root@vultr:/var/log/supervisor#** tail -f geth.err.log |

Setup metamask để connnect tới geth



# Cài đặt Explorer đọc dữ liệu trên blockchain

* 1. Clone explorer (<https://github.com/carsenk/explorer>)

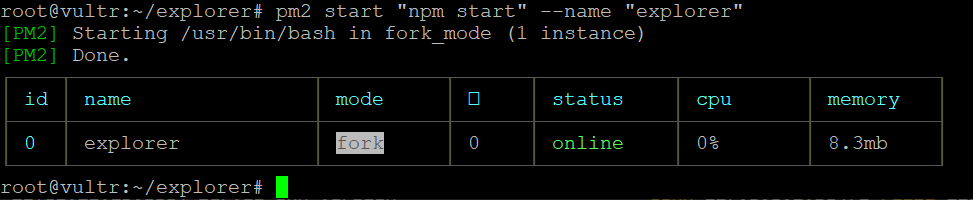
|  |
| --- |
| 1. git clone https://github.com/carsenk/explorer 2. npm install 3. bower install 4. npm start |

1.2. Cài đặt pm2, trình quản lý ứng dụng nodejs. Giúp các ứng dụng chạy dưới nền như dịch vụ

|  |
| --- |
| sudo npm install -g pm2 |

|  |
| --- |
| $ pm2 start "npm start" --name "explorer" |

(<https://pm2.keymetrics.io/docs/usage/process-management/>)



Các ứng dụng đang chạy dưới PM2 sẽ được khởi động lại tự động nếu ứng dụng gặp sự cố hoặc bị tắt, nhưng cần thực hiện thêm một bước để ứng dụng khởi chạy khi khởi động hệ thống (khởi động hoặc khởi động lại).

|  |
| --- |
| $ pm2 startup systemd |

1.3. Cấu hình nginx

<https://www.digitalocean.com/community/tutorials/how-to-set-up-a-node-js-application-for-production-on-ubuntu-16-04#prerequisites>

test cú pháp config file

|  |
| --- |
| sudo nginx -t |

Khởi động lại nginx

|  |
| --- |
| $ sudo systemctl restart nginx |

Kết quả sau khi thực hiện xong:

Private blockchain: : [http://45.32.124.84:8545](http://45.32.124.84:8545/),

Explorer: <http://45.32.124.84/>

Connect tới private blockchain tại máy khác:

|  |
| --- |
| $ geth attach http://45.32.124.84:8545 |

Tạo user

|  |
| --- |
| > personal.newAccount("<YOUR\_PASSPHRASE>") |

Tài khoản đầu tiên được tạo tự động được gán thành coinbase

> eth.coinbase

để kiểm tra

hoặc thay đổi tài khoản coinbase

|  |
| --- |
| > miner.setEtherbase(web3.eth.accounts[0]) |

Bắt đầu khai thác

* Kiểm tra số dư tài khoản

|  |
| --- |
| > eth.getBalance(eth.coinbase) |

- Khai thác

|  |
| --- |
| > miner.start() |

-

- Dừng khai thác

|  |
| --- |
| > miner.stop() |

Danh sách user

|  |  |  |
| --- | --- | --- |
| **code** | **Public address** | **Password (passphrase)** |
| personal.newAccount(“miner”) | 0x407eff44c4489ad878648a84680e884a8fe50aa2 | miner |
| personal.newAccount("superadmin") | 0xfe02f9af2452712702889caea679482585e08a9d | superadmin |
| personal.newAccount("notary") | 0xeeba06f6a6d1b203a124b75578c63ae3346b70b1 | notary |
| personal.newAccount("owner1") | 0xb5a2b3dbfce7f970c46055082dd427d1a4ebd92d | owner1 |
| personal.newAccount("owner2") | 0x42df9988c2d725bc467605283408f2d59f392c14 | owner2 |

* Deploy các hợp đồng
* Địa chỉ RoleBaseAcl: 0xa5fb3c4304eADB2DB3f2Ee4CfF71522baE0eC1fa

<http://45.32.124.84/#/address/0xa5fb3c4304eADB2DB3f2Ee4CfF71522baE0eC1fa>

* Địa chỉ RealEstate:

0xf784c599C98613E6eC09734a4c141f00e77556BA

<http://45.32.124.84/#/address/0x407eff44c4489ad878648a84680e884a8fe50aa2>