The Chinese University of Hong Kong

Department of Information Engineering

FTEC5520 –Applied Blockchain & Cryptocurrency

Lab1 Report guidance

Ethereum Infrastructure Setup & Practice

Please edit this file directly but submitted a PDF version to blackboard finally.

# 1 Question Answering:

Answers for each question: there will be 3 questions, but you only need to finish the questions before task6.

**Q1:** What do you need to change in commands if you want to connect to real public world Ethereum network? (1 mark) Hint: puppeth is a private Ethereum network manager, pls consider another approach Please list the main steps and explain why.

***Answer:***

***1) Compared with private network that genesis should be defined, in public network that there are historical blocks, so previous records need to be downloaded.***

***2) To connect to the mainnet network (real public world Ethereum network),***

***use geth, run the command:***

***geth --datadir ~/blockchain --networkid 1***

***Here the "--datadir ~/blockchain" means where to store the blockchain,***

***"--networkid" is used to specify the network ID, 1 is the ID of the mainnet network.***

**Q2:** 1) Please describe the process of mining, what are the main steps for finding a new block with Ether? (0.5 mark)

***Answer:***

***the process of mining:***

***a) use proof of work (PoW) to finish the construction of a new block***

***for example, hashing calculation with a Nonce, commands like:***

***miner.start()***

***b) when finding the Nonce, broadcast to the entire network***

***c) chain the new block and get reward***

2) What’s the content of a new mined Ethereum block, and how to identify a block in the blockchain network except using block number? (0.5 mark)

Answer:

***contents:***

***a) Timestamp – the time when the block mined.***

***b) Block number – the length of the blockchain in blocks.***

***c) Difficulty – the effort required to mine the block.***

***d) mixHash – a unique identifier for that block.***

***e) A parent hash – the unique identifier for previous block.***

***f) Transactions list – the transactions included in the block.***

***g) State root – the entire state of the system: account balances, contract storage, contract code and account nonces are inside.***

***h) Nonce – a hash that, with the mixHash, show the proof of work.***

***identify a block:***

***- mixHash – a unique identifier for that block***

**Q3:** If you want to deploy the voting smart contract on the blockchain you created in tast1~5, what should you do? If you want to deploy your smart contract on other types of Eth networks like main net, Rinkeby, modern test net, etc, what should you do? (1 mark)

***Answer:***

***deploy on the blockchain created in tast1~5:***

***1) Install nodejs, ganache-cli, Solidity compiler (solc) and web3***

***2) Write and compile the smart contract***

***for example, generate bytecode.***

***set Ether for gas.***

***3) Deployment script & Access to an Ethereum node***

***run your own or via an API, use ‘deploy / send / then’ method.***

***(sending a transaction containing the code of the compiled smart contract)***

***deploy on other types of Eth networks:***

***1) install Meta-mask Chrome Extension, then run on the bowser***

***2) Create a wallet at meta-mask***

***3) Select any one test network, e.g. mainnet/Rinkeby/modern test net, etc***

***4) Add some dummy Ethers in your wallet***

***5) Use editor remix to write the smart contract in Solidity***

***6) Create a .sol extension file***

**7) Deploy contract by pressing the deploy button in Remix window**

# 2 Screen Capture of Main Steps:

Your screenshots must include these parts at least and detailed description of each screenshots:

1. Puppeth procedure.

e.g. your description 1

(copy your image1 here)

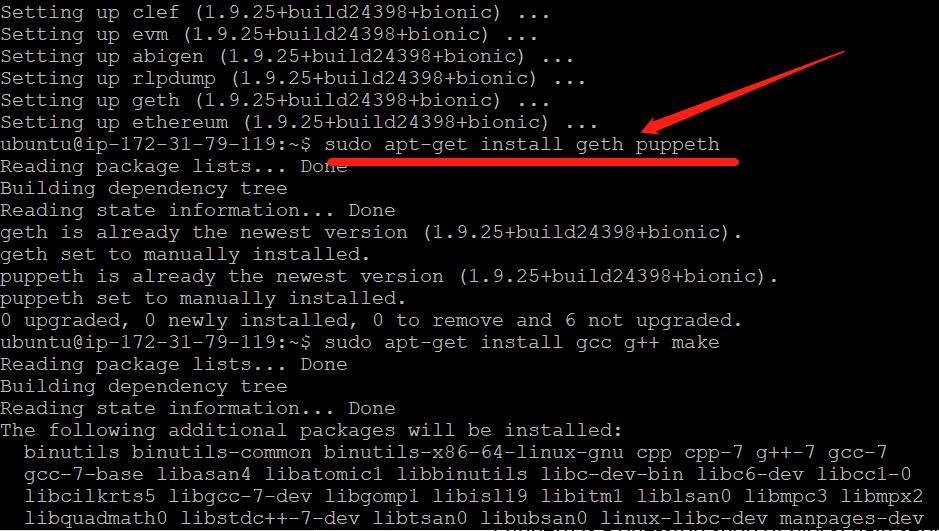
your description 2

(copy your image2 here)

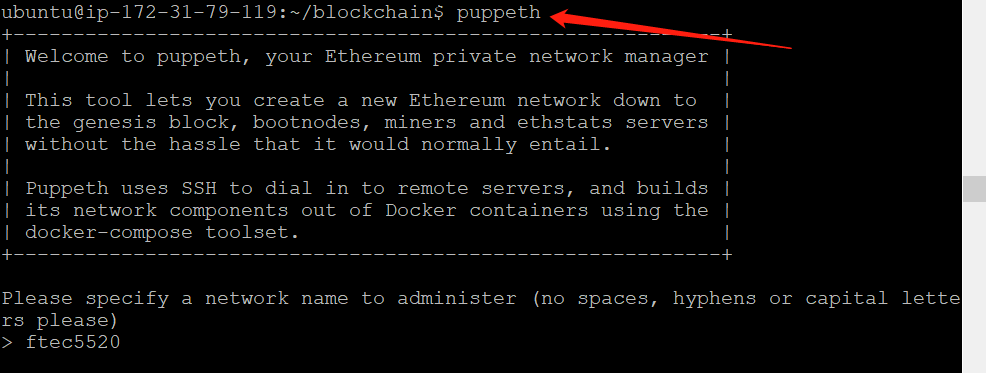
…

Puppeth is a one-stop shop of blockchain service management tools.

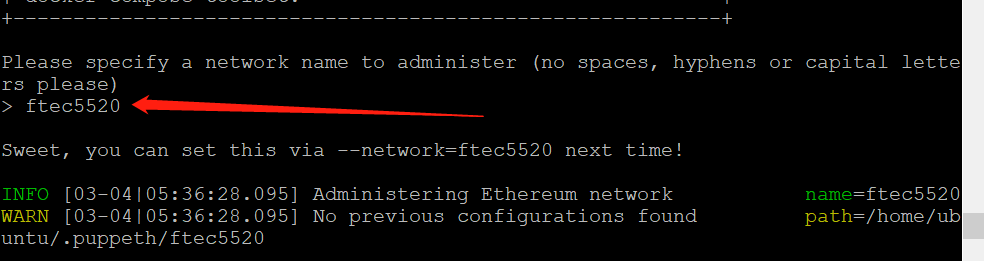
1. Install Puppeth



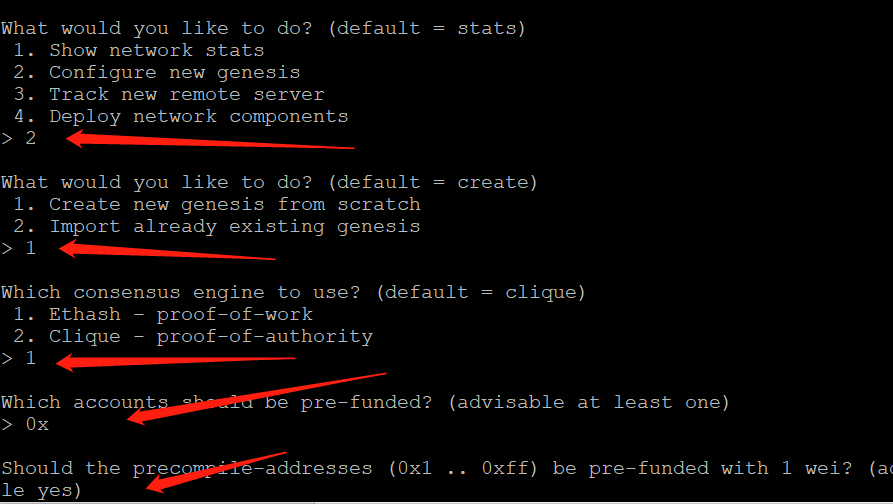
1. Use the Puppeth to generate the genesis block of my private blockchains.



1. Give a network name for administration.

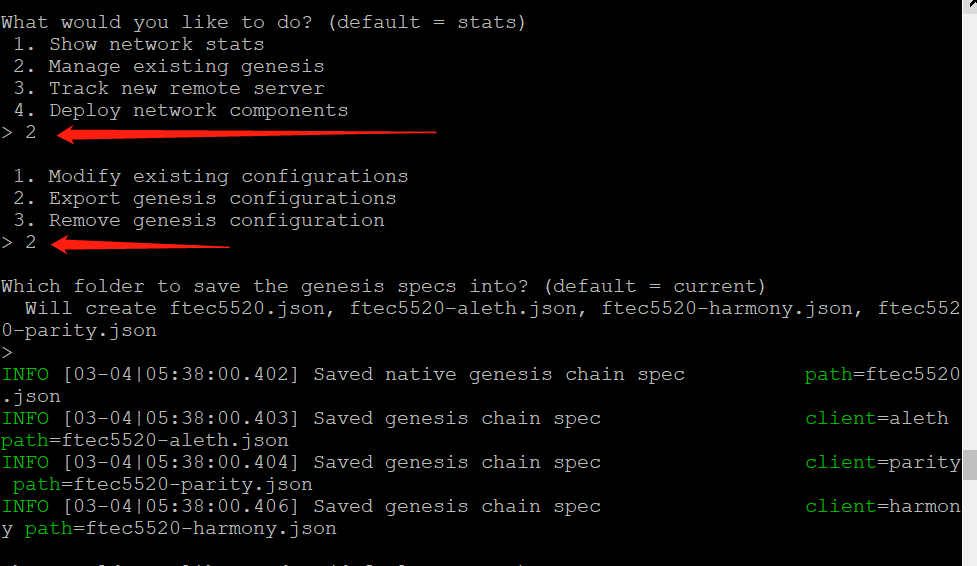


1. Configure and create new genesis, then choose POW, others default.



1. After creating genesis, manage and export it by saving as 4 files:

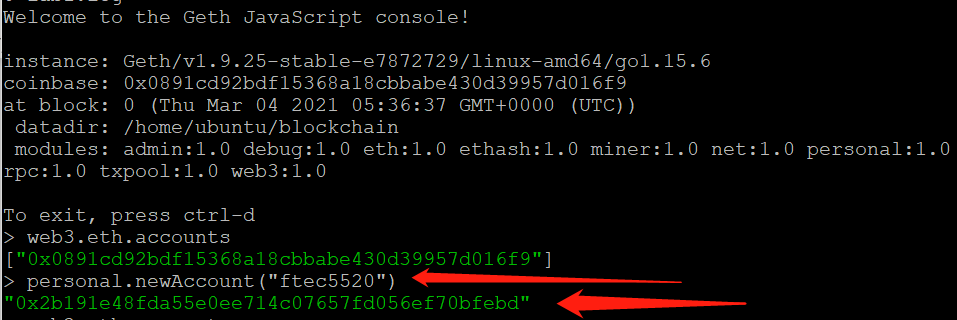
ftec5520.json, ftec5520-aleth.json, ftec5520-harmony.json, ftec5520-parity.json



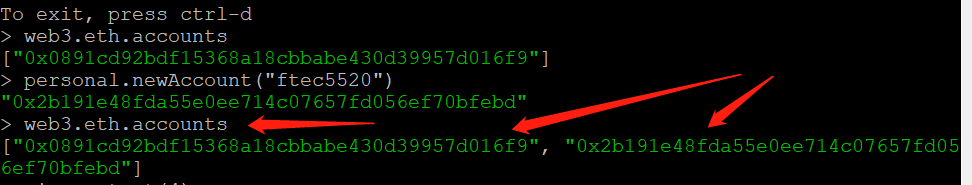
1. The content of your ftec5520.json after modified the difficulty.
2. Set the “chainId” as 5520, and “difficulty” 10.



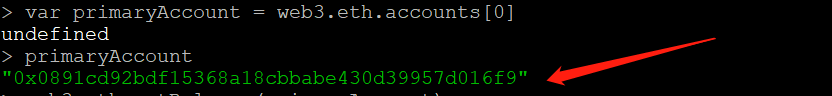
1. The creation step of Ethereum account with returned HASH value or account address (either using "geth account new" in CLI or "personal.newAccount("ftec5520" in Geth console)
2. Use “personal.newAccount("ftec5520")” command line to create account.



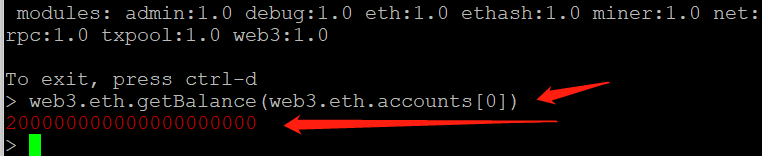
1. Use "web3.eth.accounts" to show the accounts addresses (hash values in [ ]) you created in CLI or Geth console
2. There are now 2 accounts, show them by “web3.eth.accounts”.



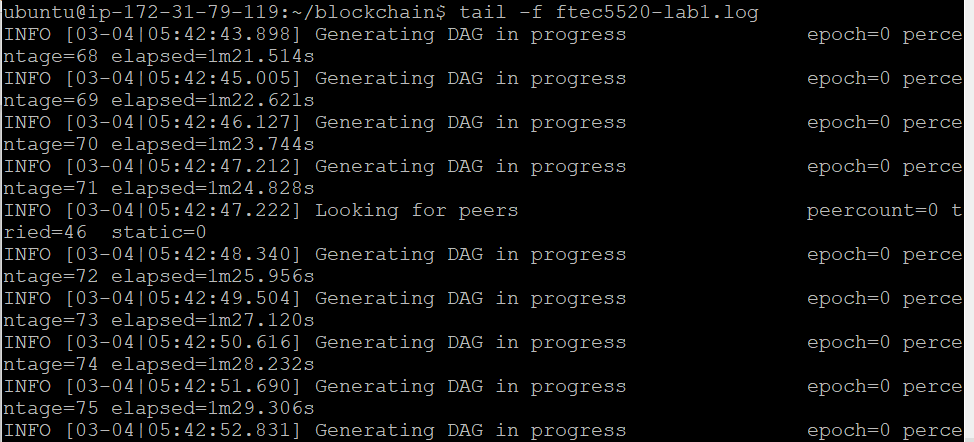
1. Use "web3.eth.accounts[0]" to show the account address of your first account or pimaryAccount
2. Set “web3.eth.accounts[0]” as “primaryAccount”, and show it.



1. Use "web3.eth.getBalance(web3.eth.accounts[0])" to show your balance of your accounts[0]
2. After mining for tens of minutes, the balance is huge:



1. The process of mining including "Generating the DAG process..." and the mined block successfully if any (). Otherwise, please just list two screen capture of mining: one for the beginning, the other for the end. **Note:** There should be **at least half hour** from the beginning to the end to let the node mine for enough epochs. Please let the mining process run a long time about half hour, you can do some other things during the period and come back to see the result.
2. The beginning:



1. Mined block successfully:

