Name Wang Runzhi (Arron) Date: 2021.8.19

Section: ST10701-G1

Assignment / Lab #1

Part1-Exercises

1

(a) Supply chain/Healthcare/Digital identity/Finance

(b)

Estate distribution.

Although the smart contract is still in its infancy, its potential is obvious. If you can develop a simple enough user interface, it can solve many legal problems, such as updating your will. As in the case of gambling or SF express, once smart saving confirms the trigger condition - you are dead - the contract begins to be executed, and your property will be divided immediately.

Physical world

The Internet of things is developing continuously. More and more intelligent devices are connected to the network every day. Some leading developers have begun to combine the Internet of things and blockchain technology, so many blockchain based digital currencies or digital assets can actually represent an object.

automobile insurance

Smart contracts access the IOT sensor data of smart cars, thus simplifying the auto insurance process. Theft, car accident and other claims will be automatically triggered, so insurance customers can get insurance compensation in time.

2

(a) This is something similar to the handling fee. Each transaction requires a certain amount of gas.

(b)Sorry,i don't know.

(c)From big to small：

-SELFDESTRUCT(ifnonewaccountiscreated)

-CREATE

-SHA3

-JUMP

-PUSH40x00000000=PUSH10xff

-STOP

(The call is complicate,so i am not put it in this)

3、Because the Ethereum have Nonce.In the communication application of various authentication protocols, it is ensured that the authentication information is not reused to resist replay attacks.

4、This is to protect security. Mesaage contains a lot of private information. If you write to blockchain, it will be intercepted, and personal information may be exposed and stolen.Blockchain has a centrally controlled world state to avoid this situation.Blockchain has a centrally controlled world state to avoid this situation. It can ensure that all nodes in a chain are a statw.

5、

(a)1. Firstly, the sender does not have enough ether to afford the payment transfer or gas. Secondly, the signature of the sender is false. Thirdly, the gas consumption of transaction exceeds the maximum gas limit. Fourthly, the nonce is too high or too low.

(b). One reason is that the gas provided is not enough. The other reason is that sometimes one may execute multiple transactions at once, and the rejection will probably because the liquidity is not enough to fill at the quoted price.

(c). Because although transaction failed, the miners still execute part of the transaction, which takes computation power. And the sender needs to pay for the gas consumed by the process of computing.

Sorry, GitHub is a little difficult for me. I didn't finish it within the specified time. I'll make it up after completion.

Total in points(100 points total):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Professor’s Comments: