Name: Taoyue Xia (James) Date: 2021/08/16 Section: ST10701

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

**Professor’s Comments:**

**Part Ⅰ**

1. **(a).** Firstly, the smart contract can be used for token systems, to collect money via initial coin offerings. Secondly, the smart contract can be used for identity and reputation systems, as a decentralized identity manage system. Thirdly, the smart contract can be used for Decentralized Autonomous Organizations, where members vote to trigger certain methods in smart contract like the transfer of money. Finally, the smart contract can be used for election and voting systems, ensuring that a specific wallet can vote only once.

**(b).** Firstly, smart contract can be used for financial services like payments, in which way the money transfer will be faster and transparent, and do not need a third party to intervene. Secondly, smart contract can be used for supply chains, automating supply chains with visibility and transparency, leading to fewer frauds. Thirdly, smart contract can be used for mortgage, fastening the process and be more convenient.

**(c).** Asset Token: 0x90ea44ea9de0c016f3ac5068b0597ed3cc75525b.

Identity: 0xd9485499499d66b175cf5ed54c0a19f1a6bcb61a

Payment: 0xa0b73e1ff0b80914ab6fe0444e65848c4c34450b

Supply chain: 0x6710c63432a2de02954fc0f851db07146a6c0312

DAO: 0xc00e94cb662c3520282e6f5717214004a7f26888

1. **(a).** Gas is a certain fee costed when executing some opcode.

**(b).** The spare gas will be returned to your account.

**(c).** STOP: Gas cost 0

PUSH1 0xff: Gas Cost 3

PUSH4 0x00000000: Gas cost 3

JUMP: Gas cost 8

SHA3: Gas cost 30

CALL: Gas cost 700

CREATE: Gas cost 32000

SELFDESTRUCT: Gas cost 5000 (refund 24000).

1. Ethereum prevents double spending using the property **nonce**, by attaching an increasing number to every transaction.
2. If messages are published to blockchain, it is possible to be intercepted and it is possible to lose money.

The blockchain can be in the same state among all the nodes by setting a global state for all the blocks.

1. **(a).** 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.

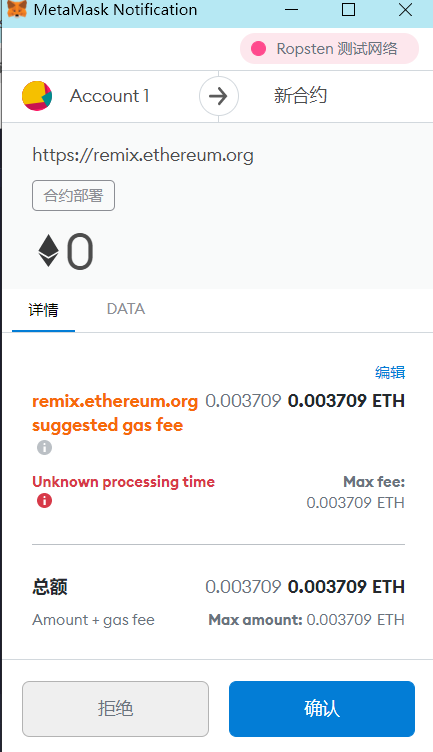
Fourthly, the nonce is too high or too low.

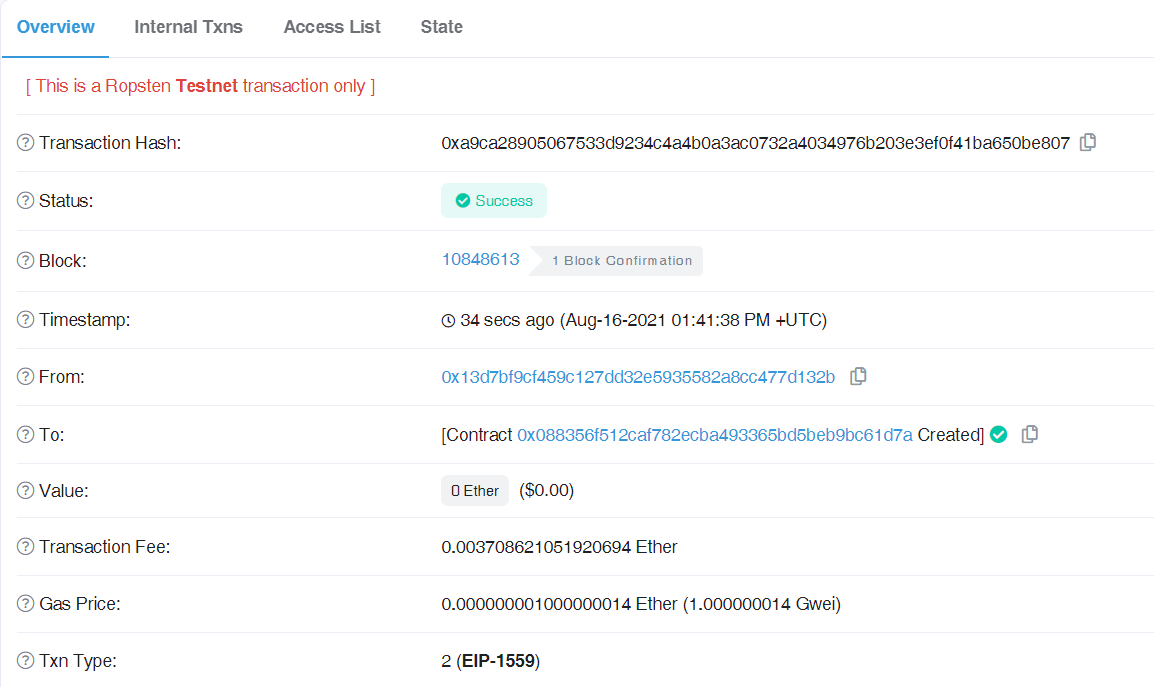
**(b).** One reason is that the gas provided is not enough.

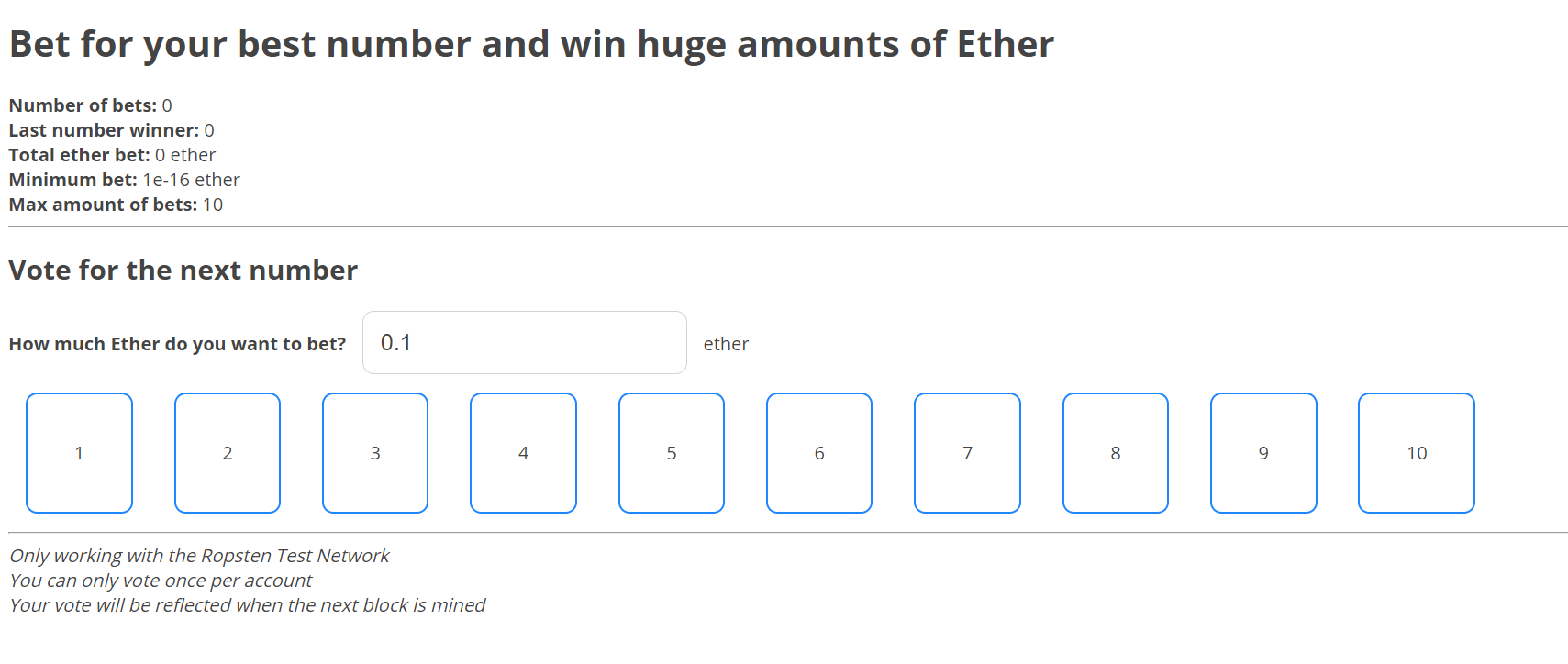
The other reason is that sometimes one may execute multiple transactions at once, and the rejection will probably because the liquidity is not enough to fill at the quoted price.

**(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.

**Part Ⅱ**

****

****

****