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

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

**Professor’s Comments:**

1. **(a).** Storage maintains contract state variables permanently, which cost ethers to call between functions. Memory is used to store temporary variables, which are erased between function calls, and cost less.

**(b).** Because 0 is a fixed value, which can be a constant state stored in the storage. When any value is set to 0, it can quickly be set to the state. However, when setting a value from 0 to other values, it should firstly be decided the state, then it can be changed, which is more complex.

**(c).** Gas prices are denoted in gwei, which is ether. Assume that each SSTORE operation cost 20000 gas to store a 256-bit word according to the yellow paper, then for 1 KiB = 1024 Bytes = 8192 bits = 32 words, it should cost about 640000 gas. Assume that 1 gas costs 50 gwei, then the 1KiB data will cost 50 \* 640000 = 32000000 gwei = 0.032 ether, which is about 0.032 \* 3343.47 = $106.99.

**(d).** It costs 758369 gas, which is about 758369 \* 50 = 37918450 gwei = 0.038 ether. And it is finally equal to 0.038 \* 3343.47 = $127.05.

**(e).** First one is computing consumption, which can be higher than estimated. Second one is the assignment process, which may cost additional gas. Third one is that creating the transaction hash can cause additional gas.

1. **(a).** In a multi-sig wallet, there are three keys associated with the wallet, instead of only one private key. Then rules can be set like one needs two of the three keys to use the wallet or so on.

Parity is an Ethereum client which allows users to access the basic ether and token wallet functions, as well as interact with smart contracts deployed on the Ethereum Blockchain.

**(b).** This function can be used at any time after the contract is being deployed, which enables attackers to reset the ownership and usage parameters of existing wallet. To prevent this from happening, we can set the initWallet() function as the constructor, which can be called only when the contract is created, preventing it from being called again.

1. An interface cannot inherit other interfaces and abstract contracts, and all of its functions cannot be implemented.

An abstract contract is that at least one of its functions cannot be implemented.

A library contains codes that can be reused in different contracts.

1. **(a).** Yes, because pure functions can be seen as a subset of view functions, which do not modify the state, but also do not read from the state.

**(b).** Yes, because view functions are read only, which do not change states. Therefore, they cost nothing.

**(c).** Yes, because without a payable function, any ether sent to a function will be reverted by default.

**(d).** Yes, the difference between them is the range. **int** can hold values, including half negative and half positive. However, **uint** can only hold values that are not signed, which means the values should be greater or equal to 0.

**(e).** Yes, because tx.origin refers to the external account that starts the transaction. Then if the message sender is the original account, it cannot be smart contracts.

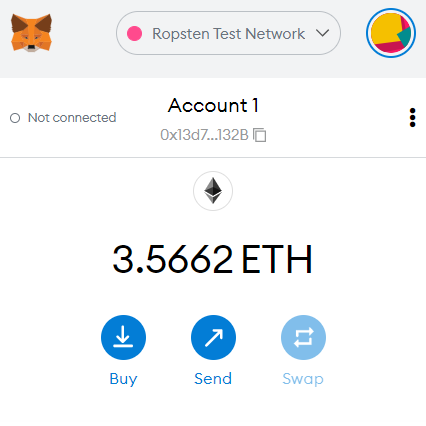
1. **(a).** The Ethereum Test Network is a simulation of Ethereum, while having the same environment and conditions found on the Ethereum network. We can use virtual ethers to deploy contracts and test our programs without real cryptocurrency.

**(b).** The three largest Ethereum test networks are **Ropsten**, **Rinkeby** and **Kovan**. **Ropsten**’s block time is the longest, approximately 30 seconds and uses proof of work. It accepts Geth and Parity both. Furthermore, users can be anonymous, meaning that they do not leak any privacy.

**Rinkeby**’s block time is shorter, which is about 15 seconds, and uses proof of authority consensus. It only accepts Geth. Furthermore, users should link their Twitter or Facebook account to verify their identity.

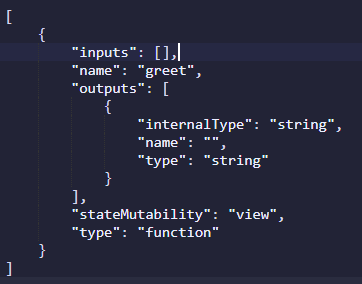
**Kovan**’s block time is the shortest, which is about 4 seconds, and uses proof of authority consensus. It only accepts Parity. Furthermore, users should link their github account to verify their identity.

**(c).**

****

**(d). **

**(e). ABI:**

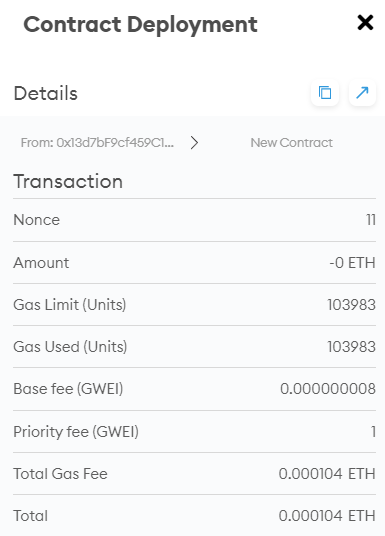


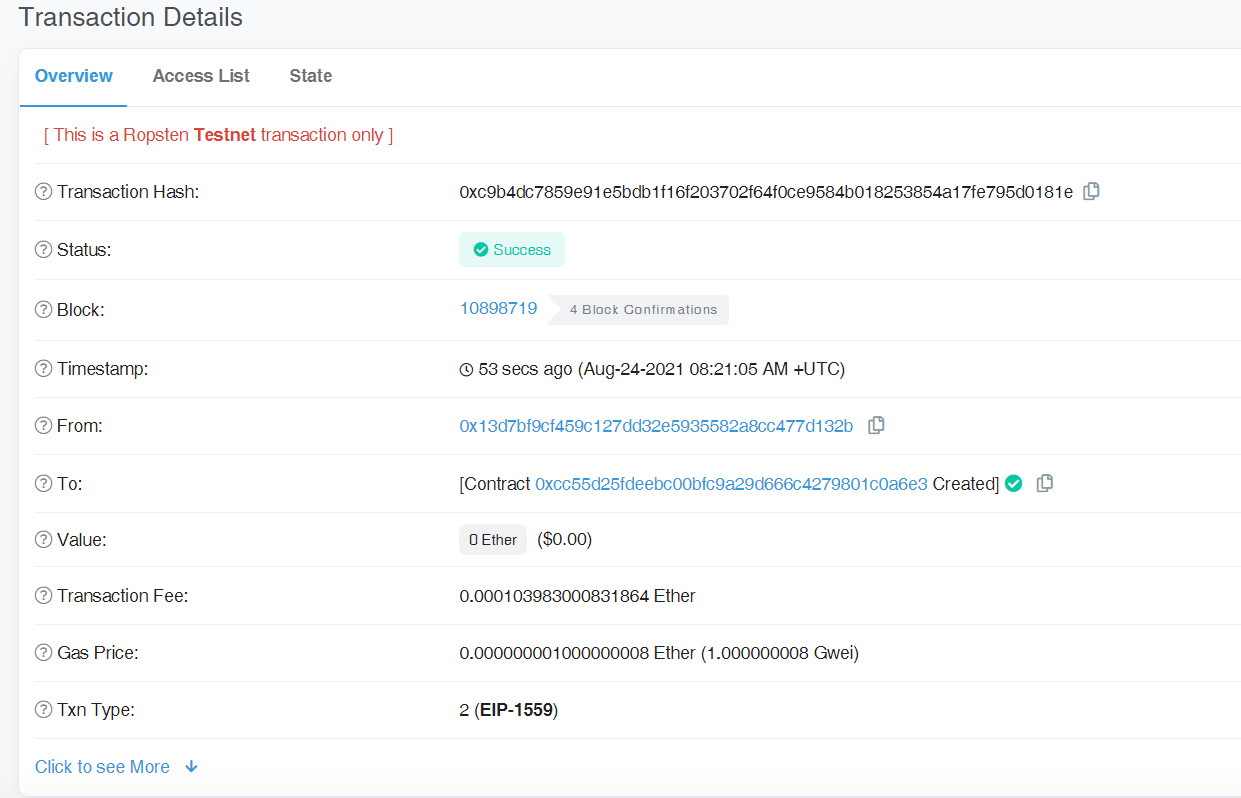
ABI can let users obviously see the name of the function, input field, outputs and type, and the type of function.

**(f). --bin-runtime** shows the code that is actually placed on the blockchain.

**--bin** shows the code placed on the blockchain and the code of the constructor.

**(g).**





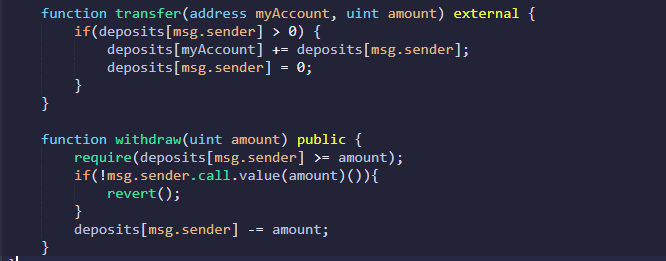
The output can be seen in the decoded output.

1. **(a).** The basic function of this contract is money deposition and withdrawal if the amount of money in the deposit is greater than that of called.

**(b).** It is used to handle the failure case of subcalls. If there encounters some exception when sending ether to a contract, it will revert and return the money to the original account or contract.

**(c).** If a function makes an external call to an untrusted contract before it takes effect, then if attackers can control the untrusted contract, they can make a recursive call to the original function, in this case the withdrawal function, which can withdraw all the money in the deposit.

**(d).**



With the above transfer function called after the revert of withdraw, all ethers will be transferred to my account, and the users account will contain no ether.

**(e).** We should use ***send()*** or ***transfer()*** functions rather than ***call()*** to maintain the security.