1. Token Swap Contract

- Explanation

There are 3 contracts in TokenSwap.sol file. One is a TokenM contract, another one is a TokenN contract and the last is a Swap contract. TokenM and TokenN are both ERC20 token contract and they are able to be swaped each other on the swap contract.

Users buy one token(M token) by paying ether and they can swap it with another kind of token(N token). At this time, I set ratio and fee on the swap contract so admin of the contract can adjust them even after deploying the contract.

Swap will be able to executed within expired time so if the time is over, the transaction will be failed.

- Test Cases

Let’s assume that Alice is decided to swap 1 TokenM with TokenN. The admin of the contract set the ratio to 0.8 and fee to 5% so Alice will get (1 * 0.8 * (1 - 0.05)) = 0.76 TokenN by swaping 1 TokenM.

In the other case, Bob is decided to swap 2 TokenN with TokenM and the ratio is 1.5 and the fee is 3%. In this case, he will get (2 * 1.5 * (1 - 0.03)) = 2.91 TokenM by swap.

2. MultiSig Wallet

- Explanation

MultiSig.sol is a multi sign wallet smart contract which enable us to execute transactions by signing required times rather than signing by only one owner.

The contract logic is as follows:

I set owners array and required times when deploying contract. Here, owners array is a list of owners who have right to sign the transactions and required times is a number which is minimum to execute the transaction.

So firstly, the owner submit a transaction and this transaction is added to transaction list with ID. Then, owners who in the owners array confirm the transaction. At this time, the confirmed number must be greater than required times(m) to execute transactions (m out of n).
Finally, this transaction send specific amount of money to the destination address. Here, I use call method to send ether from msg.sender to a destination address.

- Test Cases

Alice is gonna send 1 ether to Bob but it need to be admitted by his parents and wife. In this case, owners array consists of Alice, his wife, his mother and father. At least 2 owners must confirm the transaction to sending money to Bob. So the required number is 2.

Alice submit the transaction and his mother and father confirm it but his wife doesn’t. But the transaction is finally confirmed cause 2 owners confirm it.
Finally, the tracnsaction sending 1 ether to Bob is executed successfully.

In the above case, if his wife and his mother don’t admit Alice’s transaction, it will be failed cause confirmed number is less than required times.