블록체인 과제4

토큰과 투표시스템

학번:

이름: 김태훈

1. 코드 설명

(1) token.sol

```
function burn(uint256 _value) public onlyOwner{    infinite gas
    require(balanceOf[msg.sender]>=_value,"Insufficient balance");
    balanceOf[msg.sender] -= _value;
    totalSupply -= _value;
    emit Transfer(msg.sender, address(0), _value);
}
function mint(uint256 _value) public onlyOwner{    infinite gas
    totalSupply += _value;
    balanceOf[msg.sender] += _value;
    emit Transfer(address(0), msg.sender, _value);
}
```

burn과 mint는 컨트렉트 소유자만 호출할 수 있다. burn은 컨트렉트 소유자의 balance와 totalSupply에서 각각 _value를 빼서 총 공급량을 줄인다. mint는 반대로 컨트렉트 소유자의 balance와 totalSupply에서 각각 _value를 더하여 총 공급량을 늘린다.

(2) voting.sol

```
function vote(address candidate, uint256 voteCount) public{    infinite gas
    require(votingActive,"vote is ended");
    require(registeredCandidates[candidate],"Not a registered candidate");
    require(voteContract.balanceOf(msg.sender) >= voteCount,"Insufficient tokens");
    require(voteContract.getAllowance(msg.sender,address(this))>=voteCount,"Insufficient approve tokens");
    voteContract.transferFrom(msg.sender, address(this),voteCount);
    votesReceived[candidate] += voteCount;
    votesCast[msg.sender] += voteCount;

    emit VoteCasted(candidate, voteCount);
}
```

voting.sol에서 vote함수는 먼저 투표가 진행 중인지, 후보자가 등록하였는지, sender의 토큰 balance가 voteCount보다 같거나 큰지, 이 컨트렉트가 sender로부터 받을 수 있는 토큰의 양이 voteCount보다 같거나 큰지를 검사하고, transferFrom()을 통하여 토큰을 받는다. 그리고 해당 후보자의 득표수를 늘리고, sender가 행사한 투표권의 수를 증가시킨다.

2. 동작 과정

(1) voting 컨트렉트 생성

voting contract를 생성한다. 토큰의 가격은 1 ether로 한다. 그리고 token 컨트렉트에서 voting 컨트렉트

로 일정량의 token을 전송한다.

(2) 후보자 등록


```
[
        {
                "from": "0x33283581288832A260C76A4141e19E2A943CD4B6D",
                "topic": "0xa0ac4f59dabb0ddc4b8b883adda9e055e02c796b2cde2ed80fdb11a38f77e5c9",
                "event": "CandidateRegistered",
                "args": {
                        "0": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2",
                        "_candidate": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2"
                }
        }
]
```


0xAb... 가 후보자로 등록한다.

(3) 토큰 구매 및 approve


```
{
        "from": "0xD4Fc541236927E2EAf8F27606bD7309C1Fc2cbee",
        "topic": "0xddf252ad1be2c89b69c2b068fc378daa952ba7f163c4a11628f55a4df523b3ef",
        "event": "Transfer",
        "args": {
                "0": "0x33283581288832A260C76A4141e19E2A943CD4B6D",
                "1": "0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB",
                "2": "2",
                "_from": "0x33283581288832A260C76A4141e19E2A943CD4B6D",
                "_to": "0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB",
                "_value": "2"
        }
}
```

```
[
        {
                "from": "0xD4Fc541236927E2EAf8F27606bD7309C1Fc2cbee",
                "topic": "0x8c5be1e5ebec7d5bd14f71427d1e84f3dd0314c0f7b2291e5b200ac8c7c3b925",
                "event": "Approval",
                "args": {
                        "0": "0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB",
                        "1": "0x33283581288832A260C76A4141e19E2A943CD4B6D",
                        "2": "1",
                        "_owner": "0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB",
                        "_spender": "0x33283581288832A260C76A4141e19E2A943CD4B6D",
                        "_value": "1"
                }
        }
]
```


voting 컨트렉트에서 토큰을 구매하고, token 컨트렉트에서 해당 토큰을 voting 컨트렉트가 가져갈 수 있도록 approve 한다.

(4) 투표


```
},
{
        "from": "0x33283581288832A260C76A4141e19E2A943CD4B6D",
        "topic": "0xd0e6c39f2e086dc49f1524b47725526a56945cd1ff661f37976f1725a1e56986",
        "event": "VoteCasted",
        "args": {
                "0": "0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db",
                "1": "1",
                "_candidate": "0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db",
                "_votes": "1"
        }
}
```

```
{
        "address _candidate": "0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db"
}

{
        "0": "uint256: 1"
}
```


이제 투표할 수 있고, 투표하면 투표한 후보자의 득표수가 증가한다.