

Blockchain Lab

Assignment-3

Name: Aditya Pathak

Subgroup: 3NC2

Roll Number: 102115044

```

1 // SPDX-License-Identifier: GPL-3.0
2 pragma solidity >=0.7.0 <0.9.0;
3
4 // Aditya Pathak | 102115044 | 3NC2
5 // Blockchain Assignment 3
6
7 contract Ballot {
8     struct Voter {
9         uint weight;
10        bool voted;
11        address delegate;
12        uint vote;
13    }
14
15    struct Proposal {
16        string name;
17        uint voteCount;
18    }
19
20    address public chairperson;
21    mapping(address => Voter) public voters;
22    Proposal[] public proposals;
23
24    constructor(string[] memory proposalNames) { infinite gas 895200 gas
25        chairperson = msg.sender;
26        voters[chairperson].weight = 1;
27
28        for (uint i = 0; i < proposalNames.length; i++) {
29            proposals.push(Proposal({
30                name: proposalNames[i],
31                voteCount: 0
32            }));
33        }
34    }
35
36    function giveRightToVote(address voter) public { 29325 gas
37        require(msg.sender == chairperson, "Only chairperson can give right to vote.");
38        require(!voters[voter].voted, "The voter already voted.");
39        require(voters[voter].weight == 0);
40        voters[voter].weight = 1;
41    }
42
43    function delegate(address to) public { infinite gas
44        Voter storage sender = voters[msg.sender];
45        require(!sender.voted, "You already voted.");
46        require(to != msg.sender, "Self-delegation is disallowed.");
47
48        while (voters[to].delegate != address(0)) {

```

0 ☐ listen on all transactions

Code (I)


```



47
48     while (voters[to].delegate != address(0)) {
49         to = voters[to].delegate;
50         require(to != msg.sender, "Found loop in delegation.");
51     }
52     sender.voted = true;
53     sender.delegate = to;
54     Voter storage delegate_ = voters[to];
55     if (delegate_.voted) {
56         proposals[delegate_.vote].voteCount += sender.weight;
57     } else {
58         delegate_.weight += sender.weight;
59     }
60 }
61
62 function vote(uint proposal) public {    ⛽ infinite gas
63     Voter storage sender = voters[msg.sender];
64     require(sender.weight != 0, "Has no right to vote");
65     require(!sender.voted, "Already voted.");
66     sender.voted = true;
67     sender.vote = proposal;
68     proposals[proposal].voteCount += sender.weight;
69 }
70
71 function winningProposal() public view    ⛽ infinite gas
72     returns (uint winningProposal_)
73 {
74     uint winningVoteCount = 0;
75     for (uint p = 0; p < proposals.length; p++) {
76         if (proposals[p].voteCount > winningVoteCount) {
77             winningVoteCount = proposals[p].voteCount;
78             winningProposal_ = p;
79         }
80     }
81 }
82
83 function winnerName() public view    ⛽ infinite gas
84     returns (string memory winnerName_)
85 {
86     winnerName_ = proposals[winningProposal()].name;
87 }
88 }

```


Code (II)




DEPLOY & RUN TRANSACTIONS ✓ >

ENVIRONMENT 

Remix VM (Shanghai)  

VM


ACCOUNT 

0x787...cabaB (99.9999999)   


GAS LIMIT

3000000


VALUE

0 Wei 

CONTRACT

Ballot - voteDelegation.sol 




evm version: shanghai

Deploy ['aditya', 'pathak', 'durgesh'] 


☐ Publish to IPFS


At Address Load contract from Address


Deployed Contracts

 BALLOT AT 0xD91...39138 (ME  

Balance: 0. ETH


delegate address to 


giveRightTo... address voter 

vote 1 

chairperson

0: address: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4


proposals uint256 

voters address 


winnerName

0: string: winnerName_ pathak

winningProp...

Low level interactions 

CALLDATA

 **Transact**

Deployment

✓	[vm] from: 0x5B3...eddC4 to: Ballot.(constructor) value: 0 wei data: 0x608...00000 logs: 0 hash: 0x25b...be3ea creation of Ballot pending...	Debug	▼
✓	[vm] from: 0x5B3...eddC4 to: Ballot.(constructor) value: 0 wei data: 0x608...00000 logs: 0 hash: 0x252...4f065 call to Ballot.chairperson	Debug	▼
CALL	[call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: Ballot.chairperson() data: 0x2e4...176cf transact to Ballot.giveRightToVote pending ...	Debug	▼
✓	[vm] from: 0x5B3...eddC4 to: Ballot.giveRightToVote(address) 0xd91...39138 value: 0 wei data: 0x9e7...cabab logs: 0 hash: 0xb91...d05fc transact to Ballot.giveRightToVote pending ... transact to Ballot.giveRightToVote errored: Error occured: revert. revert The transaction has been reverted to the initial state. Note: The called function should be payable if you send value and the value you send should be less than your current balance. Debug the transaction to get more information.	Debug	▼
✗	[vm] from: 0x5B3...eddC4 to: Ballot.giveRightToVote(address) 0xd91...39138 value: 0 wei data: 0x9e7...cabab logs: 0 hash: 0x6dc...a4f36 transact to Ballot.vote pending ...	Debug	▼
✓	[vm] from: 0x787...cabaB to: Ballot.vote(uint256) 0xd91...39138 value: 0 wei data: 0x012...00001 logs: 0 hash: 0x696...23a20 call to Ballot.winnerName	Debug	▼
CALL	[call] from: 0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB to: Ballot.winnerName() data: 0xe2b...a53f0	Debug	▼

Transactions on Terminal