

Experiment No. 5

Aim: Deploying a Voting/Ballot Smart Contract

Theory:

1. Relevance of require Statements in Solidity Programs

In Solidity, the require statement acts as a **guard condition** within functions. It ensures that only valid inputs or authorized users can execute certain parts of the code. If the condition inside require is not satisfied, the function execution stops immediately, and all state changes made during that transaction are reverted to their original state. This rollback mechanism ensures that invalid transactions do not corrupt the blockchain data.

For example, in a **Voting Smart Contract**, require can be used to check:

- Whether the person calling the function has the right to vote (require(voters[msg.sender].weight > 0, "Has no right to vote");).
- Whether a voter has already voted before allowing them to vote again.
- Whether the function caller is the **chairperson** before granting voting rights.

Thus, require statements enforce **security, correctness, and reliability** in smart contracts. They also allow developers to attach error messages, making debugging and contract interaction easier for users.

2. Keywords: mapping, storage, and memory

- **mapping:**

A mapping is a special data structure in Solidity that links keys to values, similar to a hash table. Its syntax is mapping(keyType => valueType). For example:

```
mapping(address => Voter) public voters;
```

Here, each address (Ethereum account) is mapped to a Voter structure. Mappings are very useful for contracts like **Ballot**, where you need to associate voters with their data (whether they voted, which proposal they chose, etc.). Unlike arrays, mappings do not have a length property and cannot be iterated over directly, making them **gas efficient** for lookups but limited for enumeration.

- **storage:**

In Solidity, storage refers to the **permanent memory** of the contract, stored on the Ethereum blockchain. Variables declared at the contract

level are stored in storage by default. Data stored in storage is persistent across transactions, which means once written, it remains available unless explicitly modified. However, because writing to blockchain storage consumes gas, it is more expensive. For example, a voter's information saved in the voters mapping remains available throughout the contract's lifecycle.

- **memory:**

In contrast, memory is **temporary storage**, used only for the lifetime of a function call. When the function execution ends, the data stored in memory is discarded. Memory is mainly used for temporary variables, function arguments, or computations that don't need to be permanently stored on the blockchain. It is cheaper than storage in terms of gas cost. For instance, when handling proposal names or temporary string manipulations, memory is often used.

Thus, a smart contract developer must **balance between storage and memory** to ensure efficiency and cost-effectiveness.

3. Why bytes32 Instead of string?

In earlier implementations of the Ballot contract, bytes32 was used for proposal names instead of string. The reason lies in **efficiency and gas optimization**.

- **bytes32** is a **fixed-size type**, meaning it always stores exactly 32 bytes of data. This makes storage simple, comparison operations faster, and gas costs lower. However, it limits proposal names to 32 characters, which is not very flexible for user-friendly names.
- **string** is a **dynamically sized type**, meaning it can store text of variable length. While it is easier for developers and users (since names can be written normally), it requires more complex handling inside the Ethereum Virtual Machine (EVM). This increases gas usage and may slow down comparisons or manipulations.

To make the system more user-friendly, modern implementations of the Ballot contract often convert from bytes32 to string. Tools like the **Web3 Type Converter** help developers easily switch between these two types for deployment and testing.

In summary, bytes32 is used when performance and gas efficiency are priorities, while string is preferred for readability and ease of use.

Code:

```
// SPDX-License-Identifier: GPL-3.0
pragma solidity ^0.8.20;
```

```
/**  
 * @title Ballot  
 * @dev Implements voting process along with vote delegation  
 */  
//Prajwal Pandey D20A / 37  
contract Ballot {  
  
    struct Voter {  
        uint weight; // weight is accumulated by delegation  
        bool voted; // if true, that person already voted  
        address delegate; // person delegated to  
        uint vote; // index of the voted proposal  
    }  
  
    struct Proposal {  
        string name; // short name of proposal  
        uint voteCount; // number of accumulated votes  
    }  
  
    address public chairperson;  
  
    mapping(address => Voter) public voters;  
    Proposal[] public proposals;  
  
    /**  
     * @dev Create a new ballot to choose one of `proposalNames`.  
     */  
    constructor(string[] memory proposalNames) {  
        require(proposalNames.length > 0, "Must provide proposals");  
  
        chairperson = msg.sender;  
        voters[chairperson].weight = 1;  
  
        for (uint i = 0; i < proposalNames.length; i++) {  
            proposals.push(Proposal({  
                name: proposalNames[i],  
                voteCount: 0  
            }));  
        }  
    }  
  
    /**  
     * @dev Give `voter` the right to vote on this ballot.  
     * Can only be called by chairperson.  
     */
```

```

function giveRightToVote(address voter) external {
    require(msg.sender == chairperson, "Only chairperson can give right to vote");
    require(!voters[voter].voted, "The voter already voted");
    require(voters[voter].weight == 0, "Voter already has right to vote");

    voters[voter].weight = 1;
}

<*/
* @dev Delegate your vote to the voter `to`.
*/
function delegate(address to) external {
    Voter storage sender = voters[msg.sender];

    require(sender.weight != 0, "You have no right to vote");
    require(!sender.voted, "You already voted");
    require(to != msg.sender, "Self-delegation is disallowed");

    // Follow delegation chain
    while (voters[to].delegate != address(0)) {
        to = voters[to].delegate;
        require(to != msg.sender, "Found loop in delegation");
    }

    Voter storage delegate_ = voters[to];

    require(delegate_.weight >= 1, "Delegate has no right to vote");

    sender.voted = true;
    sender.delegate = to;

    if (delegate_.voted) {
        proposals[delegate_.vote].voteCount += sender.weight;
    } else {
        delegate_.weight += sender.weight;
    }
}

<*/
* @dev Give your vote (including delegated votes) to proposal `proposal`.
*/
function vote(uint proposal) external {
    require(proposal < proposals.length, "Invalid proposal");

    Voter storage sender = voters[msg.sender];
}

```

```
require(sender.weight != 0, "Has no right to vote");
require(!sender.voted, "Already voted");

sender.voted = true;
sender.vote = proposal;

proposals[proposal].voteCount += sender.weight;
}

/** 
 * @dev Computes the winning proposal.
 */
function winningProposal() public view returns (uint winningProposal_) {
    uint winningVoteCount = 0;

    for (uint p = 0; p < proposals.length; p++) {
        if (proposals[p].voteCount > winningVoteCount) {
            winningVoteCount = proposals[p].voteCount;
            winningProposal_ = p;
        }
    }
}

/** 
 * @dev Returns the name of the winning proposal.
 */
function winnerName() external view returns (string memory winnerName_) {
    winnerName_ = proposals[winningProposal()].name;
}
```

Output Screenshot:

1. Compiled Ballot.sol contract

```

1 // SPDX-License-Identifier: GPL-3.0
2 pragma solidity ^0.8.20;
3
4 /**
5  * @title Ballot
6  * @dev Implements voting process along with voter registration
7  */
8 //Prajwal Pandey D20A / 37
9 contract Ballot {
10
11     struct Voter {
12         uint weight;           // weight is accumulated
13         bool voted;           // if true, that person has voted
14         address delegate;     // person delegated to
15         uint vote;            // index of the voted proposal
16     }
17
18     struct Proposal {
19         string name;          // short name of proposal
20         uint voteCount;       // number of accumulated votes
21     }
22
23     address public chairperson;
24
25     mapping(address => Voter) public voters;
26     Proposal[] public proposals;
27 }
```

2. Deploying and running of the contract

Parameter	Value
Estimated Gas	3000000
Custom	
Value	0 Wei
Contract	Ballot - contracts/3_Ballot.sol
EVM Version	osaka
Deploy	proposalNames: ["Prajwal", "Alice", "Bob"]
Calldata	
Parameters	
transact	
At Address	
Load contract from Address	
Transactions recorded	1
Run transactions using the latest compilation result	

Transaction Details:

- [vm] from: 0x5B3...eddC4 to: Ballot.(constructor) value: 0 wei
- data: 0x608...00000 logs: 0 hash: 0x48f...eb53a
- status: 1 Transaction mined and execution succeed
- transaction hash: 0x48f36969f69bf96a27e44a0871bd5dc58f8d263ad5d0a5f50e
- block hash: 0x170dd2f882538143b7d6234200ab15e8b2e59c296fa6fa1580
- block number: 1
- contract address: 0xd9145CCE52D386f254917e481e844e9943F39138
- from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
- to: Ballot.(constructor)
- transaction cost: 1305526 gas
- execution cost: 1146848 gas
- output: 0x608060405234801561000f575f5ffd5b506004361061008657f1b1d16108059578063609ff1bd146101115780639e7b8d6114610146104b578063e2ba53f01461017e576108086565b80630121b93c7f88b146108a65780632e4176cF146108d75780635c19a95c146108a4600480360381019061009f190610baF565b61019c565b61081019061080b9190610baF565b61031e565b6048516100ce925180910390f35b6108dF6103d3565b6040516100ec9190610cc6f35b61010f600480360381019061010a9190610d09565b6103f7f08565b6040516101269190610d34565b60405188910390f35b610

3. Loading the Proposal Candidate's Names (string)

```

101     proposals[proposal].voteCount += sender.weight;
102 }
103
104 /**
105 * @dev Computes the winning proposal.
106 */
107 function winningProposal() public view returns (uint winningP
108 uint winningVoteCount = 0;
109
110 for (uint p = 0; p < proposals.length; p++) {
111     if (proposals[p].voteCount > winningVoteCount) {
112         winningVoteCount = proposals[p].voteCount;
113         winningProposal_ = p;
114     }
115 }
116
117 /**
118 * @dev Returns the name of the winning proposal.
119 */
120 function winnerName() external view returns (string memory wi
121

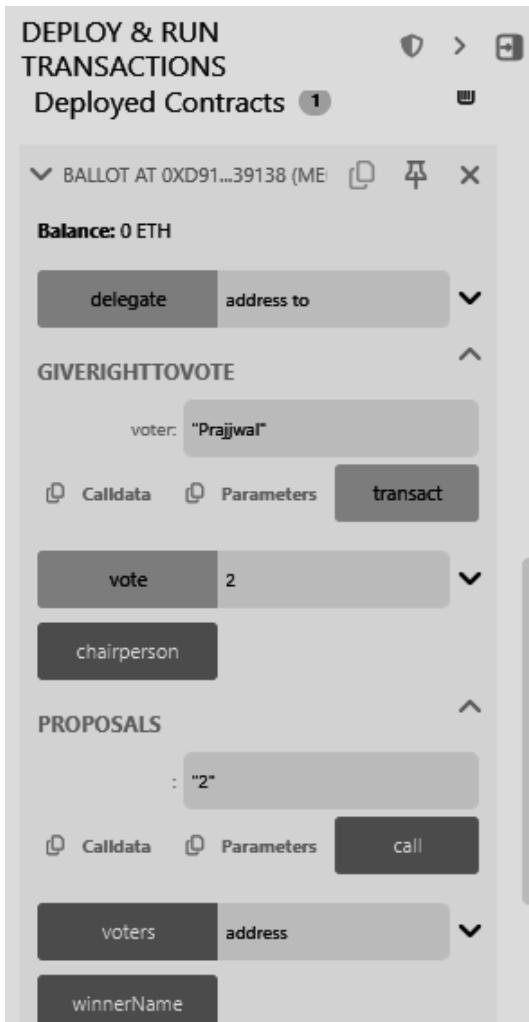
```

Explain contract

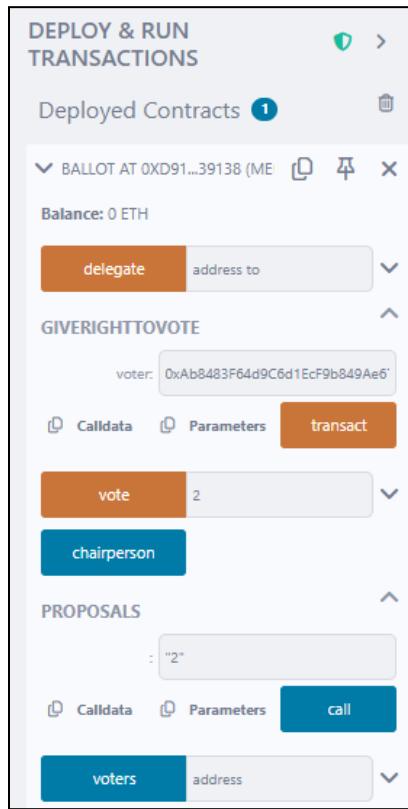
0 Listen on all transactions Filter with transaction hash or address
to: Ballot.winnerName() data: 0xe0...55t0

4. Viewing the details of the Proposal Candidate

5. Giving the right to an account other than and by the chairman



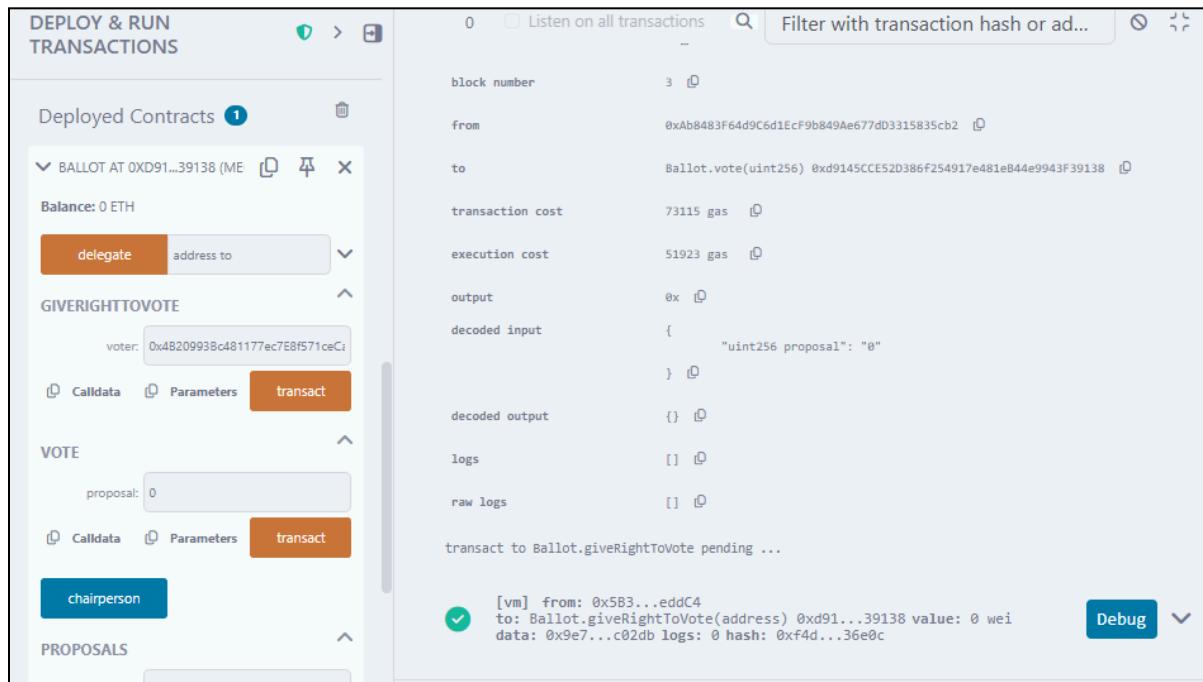
6. Selecting the account which was given the right to vote and then writing the proposal candidate's index to vote.



7. We can view the Voter's Information

Field	Value
transaction hash	0x53130d35c3b4f97b1f77560d71cb9628788cd1e9edb2aec3ab93d2682e8b8575
block hash	0x579700816fb3215f7fbe4a065027dd77ab42f5e6ef3394d6006b3ca480df751c
block number	3
from	0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2
to	Ballot.vote(uint256) 0xd9145CCE52D386f254917e481eB44e9943F39138
transaction cost	73115 gas
execution cost	51923 gas
output	0x
decoded input	{ "uint256 proposal": "0" }
decoded output	{}
logs	[]
raw logs	[]

8. Selecting the account of the delegator and then writing the address of the voter to be delegated to.

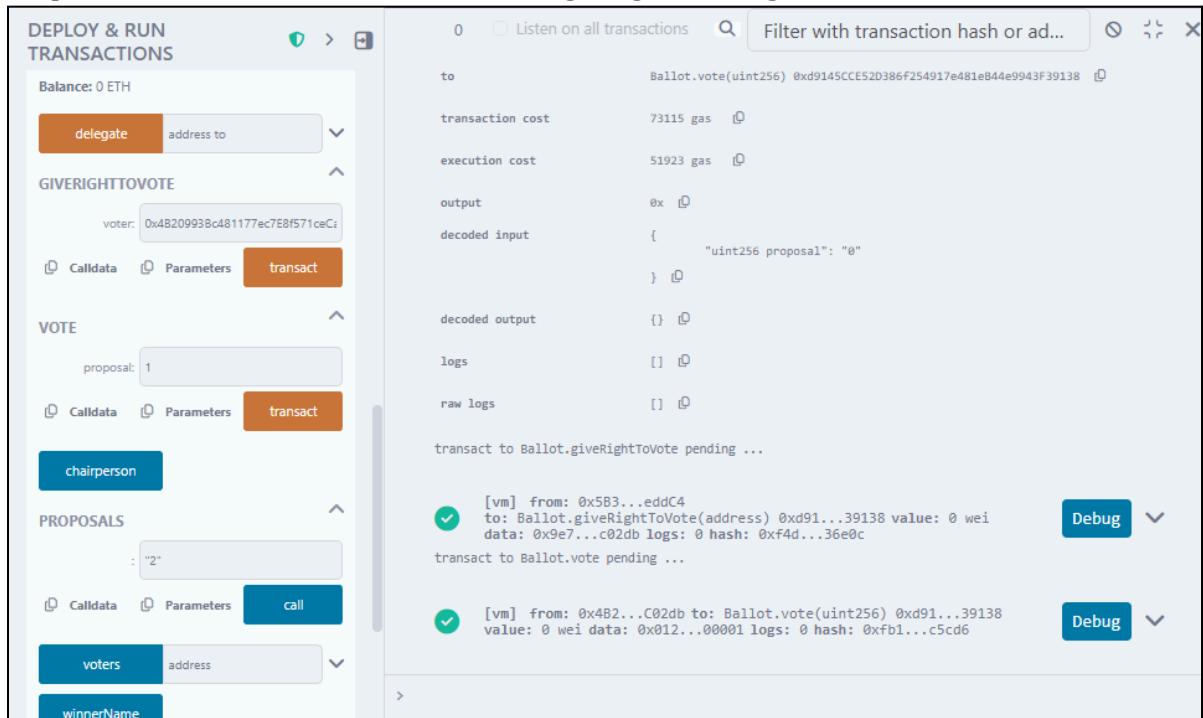


The screenshot shows the "DEPLOY & RUN TRANSACTIONS" interface. In the left sidebar, under "PROPOSALS", there is a "GIVERIGHTTOTOVOTE" section. It has a "voter" field containing the address `0x4B209938c481177ec7E8f571ceCi`. Below this, there is a "delegate" button and a "Parameters" dropdown. The "Parameters" dropdown is expanded, showing a "delegate" field and an "address to" field, both of which are currently empty. There is also a "Calldata" and a "transact" button. The right panel displays transaction details for a recent transaction:

- block number: 3
- from: `0xAb8483F64d9C6d1EcF9b849Ae677d03315835cb2`
- to: `Ballot.vote(uint256) 0xd9145CCE52D386F254917e481eB44e9943F39138`
- transaction cost: 73115 gas
- execution cost: 51923 gas
- output: `0x`
- decoded input: `{ "uint256 proposal": "0" }`
- decoded output: `{ }`
- logs: `[]`
- raw logs: `[]`

A message at the bottom says "transact to Ballot.giveRightToVote pending ...". At the bottom right, there is a "Debug" button.

9. Proposal Candidate's Information before giving the Delegate's vote.



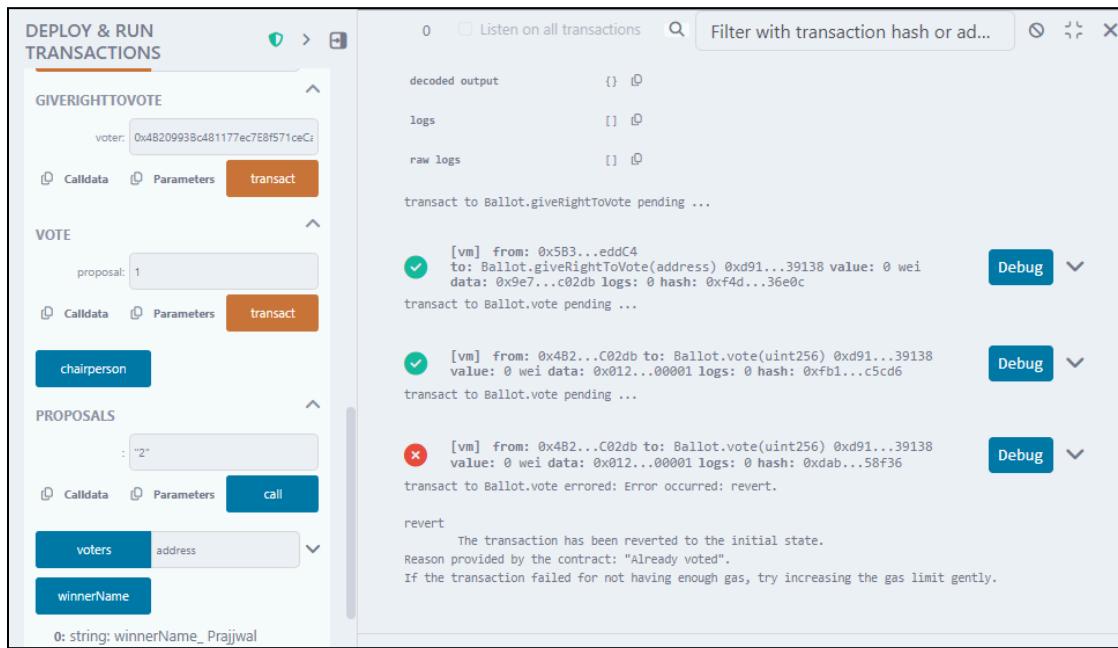
This screenshot shows the same "DEPLOY & RUN TRANSACTIONS" interface as the previous one, but with different parameters. In the "PROPOSALS" sidebar, the "GIVERIGHTTOTOVOTE" section now has a "proposal" field set to `1`. The "Parameters" dropdown is still expanded, showing the "delegate" and "address to" fields. The "Calldata" and "call" buttons are visible. The right panel shows the transaction details again:

- to: `Ballot.vote(uint256) 0xd9145CCE52D386F254917e481eB44e9943F39138`
- transaction cost: 73115 gas
- execution cost: 51923 gas
- output: `0x`
- decoded input: `{ "uint256 proposal": "0" }`
- decoded output: `{ }`
- logs: `[]`
- raw logs: `[]`

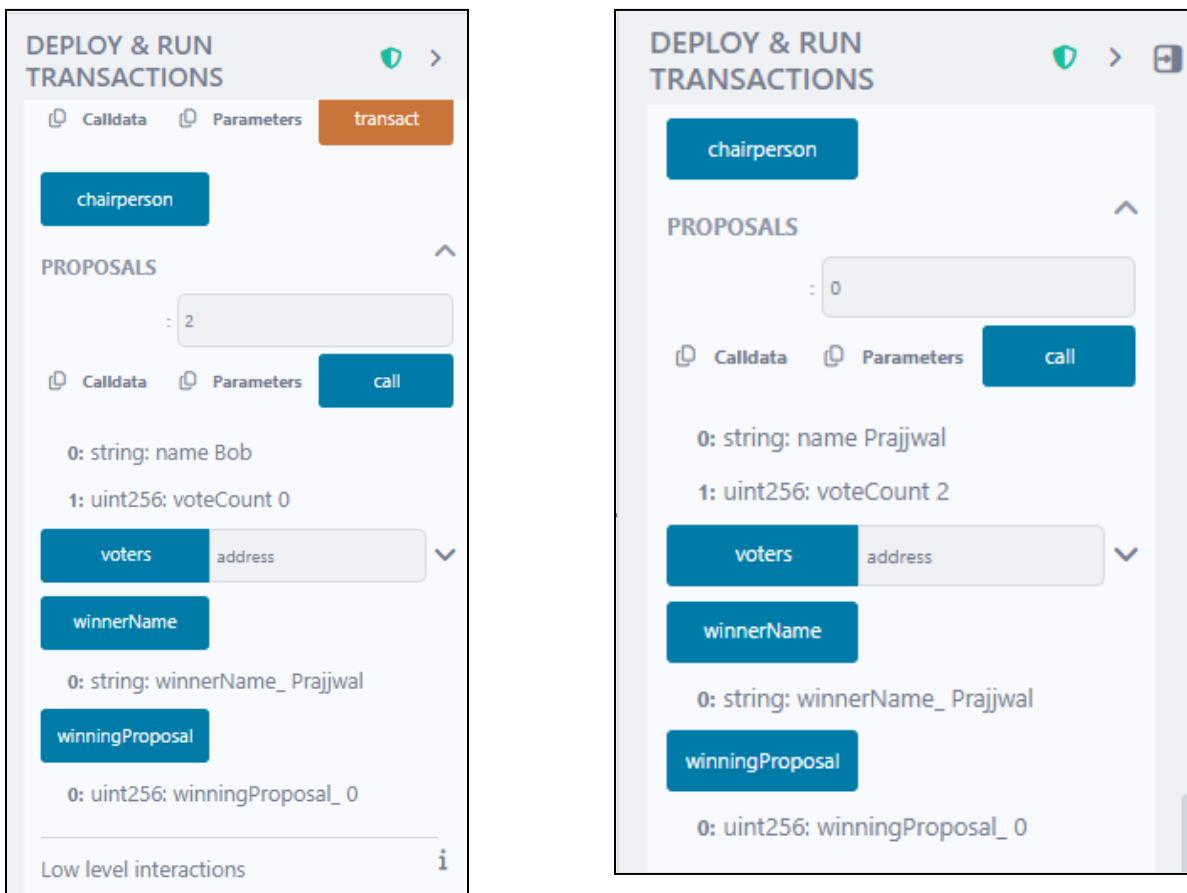
A message at the bottom says "transact to Ballot.giveRightToVote pending ...". At the bottom right, there is a "Debug" button. Another transaction is listed below it:

- [vm] from: `0x5B3...eddC4`
- to: `Ballot.vote(uint256) 0xd9145CCE52D386F254917e481eB44e9943F39138`
- value: 0 wei
- data: `0x9e7...c02db`
- logs: `0`
- hash: `0xf4d...36e0c`

A message at the bottom says "transact to Ballot.vote pending ...". At the bottom right, there is another "Debug" button.



10. In this final screenshot we can see that after the delegation's vote the weight of one vote of the one voter who was delegated is the number of people who delegated the voter as their voter (Default weight of any voter is 1).



Conclusion: In this experiment, a Voting/Ballot smart contract was deployed using Solidity on the Remix IDE. The concepts of require statements, mapping, and data location specifiers like storage and memory were explored to understand their role in ensuring security, efficiency, and correctness in smart contracts. The difference between using bytes32 and string for proposal names was also studied, highlighting the trade-off between gas efficiency and readability. Overall, the experiment provided practical insights into the design and deployment of voting contracts on the blockchain.

