

zku.ONE Background Assignment

Name	Value
course registration email	giordano3102lucas@gmail.com
discord username	giordano-lucas#9939
github repo (code)	https://github.com/giordano-lucas/zkuOne/tree/main/backgroundAssignment

Hello World

Code

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.7.0 <0.9.0;

/**
 * @title HelloWorld
 * @dev store an unsigned integer and then retrieve it
 */
contract HelloWorld {

    uint256 number;
    /**
     * @dev Store value in variable
     * @param num value to store
     */
    function store(uint256 num) public {
        number = num;
    }
    /**
     * @dev Return value
     * @return value of 'number'
     */
    function retrieve() public view returns (uint256){
        return number;
    }
}
```

Screenshot of the Remix UI

The screenshot displays the Remix IDE interface. On the left, the 'DEPLOY & RUN TRANSACTIONS' panel is active, showing the 'HelloWorld' contract being deployed. The 'GAS LIMIT' is set to 3000000, and the 'VALUE' is 0 Wei. The 'CONTRACT' is 'HelloWorld - contracts/helloWorld.sol'. Below the deployment options, there are sections for 'Transactions recorded' (2), 'Deployed Contracts' (showing 'HELLOWORLD AT 0xBBD...DCA0E'), and 'Low level interactions' (with a 'Transact' button). The main editor shows the 'helloWorld.sol' file with Solidity code. The right sidebar shows the 'ContractDefinition HelloWorld' with 1 reference(s). The bottom panel displays the transaction history and logs, including the creation of the HelloWorld contract and subsequent calls to 'store' and 'retrieve'.

Improved Ballot : idea description

In the current Ballot implementation, to give the right to vote, we need to make 10 different call the `giveRightToVote` which introduces a large gas fee cost. To deal with this, we can pass an array of all the addresses we want to give the right to vote to another function that I called `giveMultipleRightsToVote`. In this function, we simply iterate over all voters and call the `__giveRightToVote` to make the code modular.

Note: we had to define another internal function because the :

```
require(msg.sender == chairperson, "Only chairperson can give right to vote.");
```

would fail

Improved Ballot : implementation

Code (only relevant functions)

```
// Internal : Give `voter` the right to vote on this ballot.
function __giveRightToVote(address voter) internal {
    // check that the voter has not voted yet
    require(
        !voters[voter].voted,
        "The voter already voted."
    );
    // cannot give a vote right to someone
    // who already has the right
    require(voters[voter].weight == 0);
    voters[voter].weight = 1;
}

// Give `voter` the right to vote on this ballot.
// May only be called by `chairperson`.
function giveRightToVote(address voter) external {
    // If the first argument of `require` evaluates
    // to `false`, execution terminates and all
    // changes to the state and to Ether balances
    // are reverted.
    // This used to consume all gas in old EVM versions, but
    // not anymore.
    // It is often a good idea to use `require` to check if
    // functions are called correctly.
    // As a second argument, you can also provide an
    // explanation about what went wrong.
    require(
        msg.sender == chairperson,
        "Only chairperson can give right to vote."
    );
    __giveRightToVote(voter);
}

// Give all voters in `_voters` the right to vote on this ballot.
// May only be called by `chairperson`.
function giveMultipleRightsToVote(address[] memory _voters) external
{
    // If the first argument of `require` evaluates
    // to `false`, execution terminates and all
    // changes to the state and to Ether balances
    // are reverted.
    // This used to consume all gas in old EVM versions, but
    // not anymore.
    // It is often a good idea to use `require` to check if
    // functions are called correctly.
    // As a second argument, you can also provide an
    // explanation about what went wrong.
    require(
        msg.sender == chairperson,
        "Only chairperson can give right to vote."
    );
    // iterate over all _voters and call the giveRightToVote function
```

screenshots (before and after) of the gas fees for the transaction(s) to give 10 voters the right to vote.

```
[{"0x50726f706f73616c204100000000000000000000000000000000000000000000","0x50726f706f73616c204200000000000000000000000000000000000000000000","0x50726f706f73616c204300000000000000000000000000000000000000000000"}]
```

```
[vm] from: 0x5B3...eddC4 to: UpdatedBallot.giveRightToVote(address) 0xd91...39138 value: 0 wei data: 0x9e7...db7e6 logs: 0
hash: 0xd4f...e5f0e
```


Debug

⬆

status	true Transaction mined and execution succeed
transaction hash	0xd4f6f74ce05f07a80794e16ce3ffe172bfe7clef352a3f8b12fbb29b459e5f0e 🔗
from	0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 🔗
to	UpdatedBallot.giveRightToVote(address) 0xd9145CCE52D386f254917e481eB44e9943F39138 🔗
gas	80000000 gas 🔗
transaction cost	48708 gas 🔗
execution cost	48708 gas 🔗
hash	0xd4f6f74ce05f07a80794e16ce3ffe172bfe7clef352a3f8b12fbb29b459e5f0e 🔗
input	0x9e7...db7e6 🔗
decoded input	<pre>{ "address voter": "0xc504111e4083FF15Ba74A24A38Bc161eeceDB7E6" }</pre> 🔗
decoded output	<pre>{}</pre> 🔗
logs	<pre>[]</pre> 🔗 🔗
val	0 wei 🔗

Batch `giveRightToVote` using the `giveMultipleRightsToVote` function

transact to UpdatedBallot.giveMutlipleRightsToVote pending ...

 [vm] from: 0x5B3...eddC4 to: UpdatedBallot.giveMutlipleRightsToVote(address[]) 0xd91...39138 value: 0 wei data: 0x86c...96d9c logs: 0 hash: 0x213...08134
 Debug

status	true Transaction mined and execution succeed
transaction hash	0x2137ad28086aec229b3f00f1654d3ad64ef43e16b2caf7ea24bb99e5bfa08134
from	0x5B38Da6a701c568545dcfcB03FcB875f56beddC4
to	UpdatedBallot.giveMutlipleRightsToVote(address[]) 0xd9145CCE52D386f254917e481eB44e9943F39138
gas	80000000 gas
transaction cost	279428 gas
execution cost	279428 gas
hash	0x2137ad28086aec229b3f00f1654d3ad64ef43e16b2caf7ea24bb99e5bfa08134
input	0x86c...96d9c
decoded input	<pre>{ "address[] _voters": ["0x96331B0c60b10d0B061FA0eC801ecF8B314B68d8", "0x69dc7e4A8Dd1a23A31009D41495F5EC26C56fB91", "0x03C98fa6d4c9399ebdC4428192727A6d35b1Ae06", "0x6a67Ca7Ef25b24e969D6631019FF64Ef35babd97", "0x08F8ffb7498c3fe5720ffEc01B06ca01564BfC0e", "0x8Fa1763ba22F90ecd1360E30f2AB47BE789D88f2", "0x2d9ac8F87d8d4027c627D019bd2105570dbA11Fc", "0x17e746669f35FFf4a46881FEBcd58A067725f526", "0x2343DFB59521bfC0Dd8209c3E54Bec27cbdb94D9", "0x4230B1F13F760Dc24dE9987AFE74c3acb1796d9C"] }</pre>
decoded output	{}

giveMutlipleRightsToVote argument: ["0x96331B0c60b10d0B061FA0eC801ecF8B314B68d8",
 "0x69dc7e4A8Dd1a23A31009D41495F5EC26C56fB91",
 "0x03C98fa6d4c9399ebdC4428192727A6d35b1Ae06",
 "0x6a67Ca7Ef25b24e969D6631019FF64Ef35babd97",
 "0x08F8ffb7498c3fe5720ffEc01B06ca01564BfC0e",
 "0x8Fa1763ba22F90ecd1360E30f2AB47BE789D88f2",
 "0x2d9ac8F87d8d4027c627D019bd2105570dbA11Fc",
 "0x17e746669f35FFf4a46881FEBcd58A067725f526",
 "0x2343DFB59521bfC0Dd8209c3E54Bec27cbdb94D9",
 "0x4230B1F13F760Dc24dE9987AFE74c3acb1796d9C"]

In this case, we see that we paid : **279428 gas** which is 1.7x less than what we would pay if we use 10 separated transactions