

## Contact Information

Discord Username: markusmak#5980

Email: markusmak12@gmail.com

## Question 1: Hello World

Github Link: [https://github.com/markusmak/zku\\_background/blob/main/hello\\_world.sol](https://github.com/markusmak/zku_background/blob/main/hello_world.sol)

### Code Snippet

```
1 // SPDX-License-Identifier: GPL-3.0
2 pragma solidity >=0.4.16 <0.9.0;
3
4
5 // Create Hello World contract
6 contract HelloWorld {
7
8     // Declare unsigned integer
9     uint integer;
10
11     // Set function to set the unsigned integer
12     function setInteger(uint x) public {
13         integer = x;
14     }
15
16     // Get function to retrieve the unsigned integer
17     function getInteger() public view returns (uint) {
18         return integer;
19     }
20
21 }
```

### Contract Deployment

[vm] from: 0x5b3...eddC4 to: HelloWorld.(constructor) value: 0 wei data: 0x608...70033 logs: 0 hash: 0xb2e...72b1c		Debug
status	true Transaction mined and execution succeed	
transaction hash	0xb2e5f3a3e66a1da2e19e40454e2152bdf25ec2e51c0d7a04b6e960a072b1c	
from	0x5b380da701c568545dcfcb03fcb877556beddc4	
to	HelloWorld.(constructor)	
gas	8000000 gas	
transaction cost	125677 gas	
execution cost	125677 gas	
hash	0xb2e5f3a3e66a1da2e19e40454e2152bdf25ec2e51c0d7a04b6e960a072b1c	
input	0x608...70033	
decoded input	()	
decoded output	-	
logs	[]	
val	0 wei	

## Question 2: Ballot

Github Link: [https://github.com/markusmak/zku\\_background/blob/main/ballot.sol](https://github.com/markusmak/zku_background/blob/main/ballot.sol)

### Code Snippet

```
51 // batch give rights to vote by chairperson
52 function giveBatchRightToVote(address[] memory voter) external {
53     // save gas by running chairperson check only once
54     require(
55         msg.sender == chairperson,
56         "Only chairperson can give right to vote."
57     );
58     // set loop to iterate through individual voter
59     for (uint i = 0; i < voter.length; i++) {
60         // remove voter voted check to avoid unnecessary revert and improve gas
61         require(voters[voter[i]].weight == 0);
62         voters[voter[i]].weight = 1;
63     }
64 }
```

### Contract Deployment

The screenshot shows a transaction receipt for the deployment of the Ballot contract. The transaction was successful, with a status of 'true Transaction mined and execution succeed'. The transaction hash is 0xb97412fcd911d9b3b5b870e9450d63a37f60a231866fc010ffa70cbf6b1badf5. The transaction was sent from 0x533806a701c568545dcfc803fc8875f56beddc4 to the Ballot constructor. The gas used was 80000000, with a transaction cost of 1228579 gas and an execution cost of 1228579 gas. The input data is 0x608...4a712, which decodes to a JSON object containing a proposal name. The decoded output is an empty array, and the logs are also empty. The value transferred was 0 wei.

Field	Value
status	true Transaction mined and execution succeed
transaction hash	0xb97412fcd911d9b3b5b870e9450d63a37f60a231866fc010ffa70cbf6b1badf5
from	0x533806a701c568545dcfc803fc8875f56beddc4
to	Ballot.(constructor)
gas	80000000 gas
transaction cost	1228579 gas
execution cost	1228579 gas
hash	0xb97412fcd911d9b3b5b870e9450d63a37f60a231866fc010ffa70cbf6b1badf5
input	0x608...4a712
decoded input	{ "bytes32[] proposalNames": [ "0x0541646d6b76d57af601be17e777b93592d8d4e4a096c57876a91c84f4a712" ] }
decoded output	-
logs	[]
val	0 wei

### Function call - giveRightToVote

The screenshot shows a transaction receipt for the giveRightToVote function call. The transaction was successful, with a status of 'true Transaction mined and execution succeed'. The transaction hash is 0x4de4a5fed8a5fe72b32b9f11ad84e4594eb55a95d1a2d470bc660b968a74946c. The transaction was sent from 0x533806a701c568545dcfc803fc8875f56beddc4 to the Ballot.giveRightToVote(address) function. The gas used was 80000000, with a transaction cost of 48657 gas and an execution cost of 48657 gas. The input data is 0x9e7...35cb2, which decodes to a JSON object containing an address voter. The decoded output is an empty array, and the logs are also empty. The value transferred was 0 wei.

Field	Value
status	true Transaction mined and execution succeed
transaction hash	0x4de4a5fed8a5fe72b32b9f11ad84e4594eb55a95d1a2d470bc660b968a74946c
from	0x533806a701c568545dcfc803fc8875f56beddc4
to	Ballot.giveRightToVote(address) 0xd8b34580fc3511b59c6073ad0e668a2833fa8
gas	80000000 gas
transaction cost	48657 gas
execution cost	48657 gas
hash	0x4de4a5fed8a5fe72b32b9f11ad84e4594eb55a95d1a2d470bc660b968a74946c
input	0x9e7...35cb2
decoded input	{ "address voter": "0xb88483f64d9C6d12Cf9b849Ae674d3315835cb2" }
decoded output	[]
logs	[]
val	0 wei

*Function call - giveBatchRightToVote (10 addresses)*

The screenshot displays a transaction debug interface with the following details:

- [vm] from:** 0x5B3...eddC4 to: Ballot.giveBatchRightToVote(address[]) 0x7EF...8CB47 value: 0 wei data: 0xfca...c160c logs: 0 hash: 0x372...b61f0
- status:** true Transaction mined and execution succeed
- transaction hash:** 0x372949c25da0dae15eaf700d9240c819f9459e195b54caab3a59e5cb79b61f0
- from:** 0x5B3Bda6a701c56545dcfc803fcb875f56beddc4
- to:** Ballot.giveBatchRightToVote(address[]) 0x7EF2e0048f5bade046f68f797943daF4ED8CH47
- gas:** 8000000 gas
- transaction cost:** 257186 gas
- execution cost:** 257186 gas
- hash:** 0x372949c25da0dae15eaf700d9240c819f9459e195b54caab3a59e5cb79b61f0
- input:** 0xfca...c160c
- decoded input:**

```
{
  "address": "vote", [
    "0x309930c481177e78E4f571ceCa8A9e22C02db",
    "0x78731D3Ca6b7E34ac0F824c2a70C18A495cabab",
    "0x81722E2D72F0905503197092ac16c9146587f2",
    "0x17FA0A8E2F92297579C23069C10bF84546c372",
    "0x1c680f78f3270c046039d897A8dFD3f92021678",
    "0x03C4Fcd478cBc944FAB34eF940767739D1ff",
    "0x1a202A34a72D944a8C76D3F2B3eC3Ca669E454c",
    "0x2b9986a801c92f44A4c07A6ff9DabA830c700c",
    "0xCA35b7d915458EF540a6e68dfe2F4488fa733c",
    "0x14723a09acff6d2A60DcdF7aA4Af308FD0C160C"
  ]
}
```
- decoded output:** ()
- logs:** []
- val:** 0 wei

*Gas Analysis*

giveRightToVote - 48657 gas

giveBatchRightToVote - 257186 gas

giveBatchRightToVote per address gas =  $257186 / 10 = 25718.6$

Gas saved =  $(48657 - 25718.6) / 48657 = 47\%$