ZKU.One Background Assignment

mail: [enricobottazzi@icloud.com](mailto:enricobottazzi@icloud.com)

discord Username: enrico.eth#8998

Github repo: <https://github.com/enricobottazzi/zku.One>

1. Program a super simple “Hello World” smart contract: store an unsigned integer and then retrieve it. Please clearly comment your code. Once completed, deploy the smart contract on [Remix](http://remix.ethereum.org/" \t "_blank). Include the .sol file and a screenshot of the Remix UI once deployed in your final submission pdf (more info about submission formatting below).

* HelloWorld.sol screenshot

Text

Description automatically generated

* HelloWorld.sol file: <https://github.com/enricobottazzi/zku.One/blob/master/contracts/HelloWorld.sol>

1. On the documentation page, the “Ballot” contract demonstrates a lot of features on Solidity. Read through the script and try to understand what each line of code is doing, then implement the Possible Improvements by reducing the number of transactions in the “giveRightToVote” function while maintaining the same functionality of the program.
2. Deploy your script on Remix and compare the difference in gas fees between the original script and the improved script when giving 10 voters the right to vote. Once completed, submit (via pdf or Github) (1) your improved version of the contract (.sol file) with comments describing the changes you made, and (2) screenshots (before and after) of the gas fees for the transaction(s) to give 10 voters the right to vote. All code to be submitted either in pdf (only code snippets where ever required) or via Github links ( copy the repo/pull-request links and the commit in the pdf).

**Goal**: giving 10 voters the right to vote. List of addresses:

“0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB”, “0x617F2E2fD72FD9D5503197092aC168c91465E7f2”, “0x17F6AD8Ef982297579C203069C1DbfFE4348c372”, “0x5c6B0f7Bf3E7ce046039Bd8FABdfD3f9F5021678”, “0x03C6FcED478cBbC9a4FAB34eF9f40767739D1Ff7”, “0x1aE0EA34a72D944a8C7603FfB3eC30a6669E454C”, “0x0A098Eda01Ce92ff4A4CCb7A4fFFb5A43EBC70DC”, “0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c”, “0x14723A09ACff6D2A60DcdF7aA4AFf308FDDC160C”, “0x4B0897b0513fdC7C541B6d9D7E929C4e5364D2dB”

* BallotV0 (*before improvement* version) => <https://github.com/enricobottazzi/zku.One/blob/master/contracts/BallotV0.sol>

Graphical user interface, text

Description automatically generated

Gas cost to execute *giveRightToVote* to a single address = 48657 gas

Gas cost to execute *giveRightToVote* to 10 addresses = 486570 gas

* BallotV6 (*after gas improvement* version): <https://github.com/enricobottazzi/zku.One/blob/master/contracts/BallotV6.sol>

Text

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

Gas cost to execute *giveRightToVote* to 10 addresses = 277197 gas (BallotV6)

Gas cost to execute *giveRightToVote* to 10 addresses = 486570 gas gas (BallotV0

**Improvement between V0 and V6 = 209373 gas**