

Background Assignment

Github Link: <https://github.com/joellje/zku.ONE>

Course registration email: joellimjeeen@hotmail.com

Discord username: joellje#8135

Before Optimization

The screenshot displays the Remix IDE interface for deploying a smart contract. The top editor shows the `HelloWorld.sol` code, which includes a pragma statement for Solidity version `>=0.7.0 <0.9.0`, a `contract HelloWorld` definition with a state variable `uint value;`, a constructor `constructor(uint _value)` that initializes `value`, and two public functions: `set(uint x)` to update `value` and `get()` to return `value`.

The left sidebar shows the deployment configuration: Environment is set to `JavaScript VM (London)`, the account is `0x583...addC4 (0.99999999)`, the gas limit is `3000000`, and the contract name is `HelloWorld - contracts/HelloWorld.sol`. The `Deploy` button is highlighted.

The bottom console shows the deployment transaction details:

- Status: `True Transaction mined and execution returned`
- Transaction hash: `0xa53b772b0e0221d0e759628f805198a6c3bde24c13ef7d0d704d7586d45`
- From: `0xa53b0a4701c5658564c2d53f0d87f5f6a4dc4`
- Gas: `8000000 gas`
- Transaction cost: `150798 gas`
- Execution cost: `150798 gas`
- Hash: `0xa53b772b0e0221d0e759628f805198a6c3bde24c13ef7d0d704d7586d45`
- Input: `0x00...0000`
- Decoded output: `-`
- Gas: `0 wei`

Figure 1: HelloWorld.sol and deployment

After Optimization

✓ [vm]	from: 0x5B3...eddC4 to: Ballot.giveRightToVote(address[]) 0xd91...39138 value: 0 wei data: 0x858...a733c logs: 0 hash: 0x49b...54c19
status	true Transaction mined and execution succeed
transaction hash	0x49b066573f589255ef6bc36f38bf4146b672d25704dabc8c9132477802654c19
from	0x5B38Da6a701c568545dcFcb03FcB875f56beddC4
to	Ballot.giveRightToVote(address[]) 0xd9145CCE52D386f254917e481eB44e9943F39138
gas	80000000 gas
transaction cost	279263 gas
execution cost	279263 gas
hash	0x49b066573f589255ef6bc36f38bf4146b672d25704dabc8c9132477802654c19
input	0x858...a733c
decoded input	{ "address[] votersarray": ["0xab8483f64d9c6d12cf9b848Ae677d3315035cb2", "0x4B20993bc481177ec7E8f571ceCaE8A9e22C02db", "0x78731D3Ca6b7E34ac0F824c42a7c18A495cabab", "0x617F2E2fD72FD9D5503197092aC168c91465E7f2", "0x17F6AD8Ef982297579C203069C1DbFFE4348c372", "0x5c680f7Bf3E7ce046039Bd8FABdFD3f9F5021678", "0x03C6FcED478cBbC9a4FAB34eF9f40767739D1ff7", "0x1aE0EA34a72D944a8C7603FfB3eC30a6669E454C", "0x0A098Eda01Ce92ff4A4CCb7A4FFb5A43EBC70DC", "0xC35b7d915458EF540aDe6068dFe2F44E8fa733c"] }
decoded output	()
logs	[]
val	0 wei

Figure 2: 10 Addresses using 1 Transaction (new version)

Transaction Cost: 279263 gas

Execution Cost: 279263 gas

✓ [vm]	from: 0x5B3...eddC4 to: Ballot.(fallback) 0xd91...39138 value: 0 wei data: 0x9e7...35cb2 logs: 0 hash: 0x559...74462
status	true Transaction mined and execution succeed
transaction hash	0x559alb0b7fbc531d2027d9f68e0f352822751c14e610fa3a986ea90788274462
from	0x5B38Da6a701c568545dcFcb03FcB875f56beddC4
to	Ballot.(fallback) 0xd9145CCE52D386f254917e481eB44e9943F39138
gas	80000000 gas
transaction cost	48657 gas
execution cost	48657 gas
hash	0x559alb0b7fbc531d2027d9f68e0f352822751c14e610fa3a986ea90788274462
input	0x9e7...35cb2
decoded input	-
decoded output	-
logs	[]
val	0 wei

Figure 3: 1 Address using 1 Transaction (old version)

Transaction Cost: 48657 gas

Execution Cost: 48657 gas

The Transaction Cost is the same for each transaction. Total Transaction Cost for giving 10 voters the right to vote by calling the “giveRightToVote” function 10 times would be 486570 gas. This is almost double the 279263 gas required with the improved script.