

# Tugas Smart Contract Development

Tazkia Nizami / 13522032

Cerita: Anda ingin membuat sistem polling sederhana untuk memilih ketua kelas. Setiap alamat hanya boleh memilih sekali, dan pilihan disimpan dalam tally.

Tugas Teknis: Buat kontrak Poll dengan daftar opsi, fungsi vote(uint optionIndex), dan tally(uint optionIndex).

Tambahan: Ditambahkan fitur Open dan Close Poll untuk mencoba fungsionalitas onlyOwner

Untuk mendapatkan Testnet Tokens Sepolia ETH, didapatkan melalui halaman

<https://cloud.google.com/application/web3/faucet/ethereum/sepolia> dan dengan tx hash [0xd23d03c83785f3a8e0bcdf0c59cc5e4691e23fa704c9eb2055cd26bd5eb3d06b](https://sepolia.etherscan.io/tx/0xd23d03c83785f3a8e0bcdf0c59cc5e4691e23fa704c9eb2055cd26bd5eb3d06b)

Source Code Smart Contract (13522032\_Skenario5.sol)

```
pragma solidity ^0.8.24;

/// @title Poll (Simple Polling) - Skenario 5
contract Poll {
    address public owner;
    string public title;

    string[] public options; // string nama kandidat
    uint256[] public tallies; // perhitungan jumlah pemilih per
    kandidat

    // Tracker sebuah address udah milih
    mapping(address => bool) public hasVoted;

    // Events
    event Voted(address indexed voter, uint256 indexed
    optionIndex);

    bool public isOpen;
    event PollClosed(address indexed by);
    event PollOpened(address indexed by);

    // Modifiers
    modifier onlyOwner() {
        require(msg.sender == owner, "Only owner");
        _;
    }

    modifier pollOpen() {
        require(isOpen, "Polling Closed");
        _;
    }
```

```

    }

    constructor(string memory _title, string[] memory _options) {
        require(_options.length >= 2, "Minimal 2 kandidat");
        owner = msg.sender;
        title = _title;
        options = _options;
        tallies = new uint256[](_options.length);
        isOpen = true;
    }

    /// @notice Jumlah opsi
    function optionsCount() external view returns (uint256) {
        return options.length;
    }

    /// @notice Voting satu kali untuk satu kandidat
    /// @param optionIndex indeks opsi [0..options.length-1]
    function vote(uint256 optionIndex) external pollOpen {
        require(!hasVoted[msg.sender], "Sudah vote");
        require(optionIndex < options.length, "Invalid");

        // Proses voting
        hasVoted[msg.sender] = true;
        tallies[optionIndex] += 1;

        emit Voted(msg.sender, optionIndex);
    }

    /// @notice Lihat tally sebuah opsi
    function tally(uint256 optionIndex) external view returns
(uint256) {
        require(optionIndex < options.length, "Invalid");
        return tallies[optionIndex];
    }

    /// @notice Tutup polling (hanya owner)
    function close() external onlyOwner {
        require(isOpen, "Already closed");
        isOpen = false;
        emit PollClosed(msg.sender);
    }

    /// @notice Buka kembali polling (hanya owner)
    function open() external onlyOwner {
        require(!isOpen, "Already open");
        isOpen = true;
        emit PollOpened(msg.sender);
    }
}

```

Network: Sepolia

Alamat Kontrak : 0x70608b8A32f30e24F12f24bDcBD9E42aFC0E7d8f

Tx Hash : 0x0b62cbcb5f9b9a4d5073c4b1dc1db195b12f19149e527e3866819725ea406a67

✓ [block:9311871 txIndex:20] from: 0xa14...85972 to: Poll.(constructor) value: 0 wei data: 0x608...00000 logs: 0 hash: 0xe1f...288fc Debug ^

status	0x1 Transaction mined and execution succeed
transaction hash	0x0b62cbcb5f9b9a4d5073c4b1dc1db195b12f19149e527e3866819725ea406a67
block hash	0xe1f952725f5ef84447a1dc25105b354538ce58fb63e01b4d376686932ed288fc
block number	9311871
contract address	0x70608b8a32f30e24f12f24bdcdb9e42afc0e7d8f
from	0xA143D1bA8bD846f91068AAcf646e13F705985972
to	Poll.(constructor)
gas	1065469 gas
transaction cost	1055921 gas
input	0x608...00000
decoded input	<pre>{   "string_title": "Pemilihan Ketua Kelas",   "string[]_options": [     "Yanu",     "Ahmad",     "Dadang"   ] }</pre>

Pemanggilan fungsi optionsCount untuk mendapatkan angka banyak kandidat

call to Poll.optionsCount

call [call] from: 0xA143D1bA8bD846f91068AAcf646e13F705985972 to: Poll.optionsCount() data: 0xa1a...dbabb Debug ^

from	0xA143D1bA8bD846f91068AAcf646e13F705985972
to	Poll.optionsCount() 0x70608b8A32f30e24F12f24bDcBD9E42aFC0E7d8f
input	0xa1a...dbabb
output	00000000000000000000000000000003
decoded input	{}
decoded output	<pre>{   "0": "uint256: 3" }</pre>
logs	[]
raw logs	[]

Melakukan Vote untuk optionsIndex 1 (Ahmad)

Tx Hash = 0x1e1340e5e70352dc2386e61adecca5d0c50f8935aa59b509036f8aa9fc017211

```
[block:9311918 txIndex:17] from: 0xa14...85972 to: Poll.vote(uint256) 0x706...e7d8f value: 0 wei data: 0x012...00001 logs: 1 hash: 0x293...7c283 Debug ^

status      0x1 Transaction mined and execution succeed

transaction hash  0x1e1340e5e70352dc2386e61adecca5d0c50f8935aa59b509036f8aa9fc017211

block hash      0x293314aa0fbc59e5d36a0727f4bd73717694363b890f543b50675e8866c7c283

block number    9311918

from            0xA143D1bA8b0846f91068AAcf646e13F705985972

to              Poll.vote(uint256) 0x70608b8a32f30e24f12f24bdc9e42afc0e7d8f

gas             75289 gas

transaction cost 74411 gas

input           0x012...00001

decoded input    {
                  "uint256 optionIndex": "1"
                }

decoded output    -
```

Melakukan Vote lagi dengan address yang sama untuk optionIndex2

Tx Hash = 0xa53fd61942eb674b0d7442a9232743b86933d488fdced22d1b0bbfd587ed694e

```
[block:9311929 txIndex:4] from: 0xa14...85972 to: Poll.vote(uint256) 0x706...e7d8f value: 0 wei data: 0x012...00002 logs: 0 hash: 0x2d0...e4f3b Debug ^

status      0x0 Transaction mined but execution failed

transaction hash  0xa53fd61942eb674b0d7442a9232743b86933d488fdced22d1b0bbfd587ed694e

block hash      0x2d09d404cd41c848fc815358a865fc64dbf0379b7132bb0f2fd7872e59de4f3b

block number    9311929

from            0xA143D1bA8b0846f91068AAcf646e13F705985972

to              Poll.vote(uint256) 0x70608b8a32f30e24f12f24bdc9e42afc0e7d8f

gas             3000000 gas

transaction cost 26282 gas

input           0x012...00002

decoded input    {
                  "uint256 optionIndex": "2"
                }

decoded output    -
```

Gagal karena pada seharusnya address dihitung sudah melakukan vote.

Pemanggilan Tally untuk index 1 untuk melihat berapa suara untuk kandidat index 1

```
CALL [call] from: 0xA143D1bA8bDB46f91068AAcf646e13F705985972 to: Poll.tally(uint256) data: 0xed8...00001

from 0xA143D1bA8bDB46f91068AAcf646e13F705985972

to Poll.tally(uint256) 0x70608b8A32f30e24F12f24bDcBD9E42aFC0E7d8f

input 0xed8...00001

output 00000000000000000000000000000001

decoded input {
  "uint256 optionIndex": "1"
}

decoded output {
  "0": "uint256: 1"
}

logs []

raw logs []
```

Close Poll menggunakan Owner

Tx Hash = 0x45bf826bf2609261df9c5cb6ed7aca2dc825ecb96276640e61292702af870438

```
[block:9312235 txIndex:7] from: 0xa14...85972 to: Poll.close() 0x706...e7d8f value: 0 wei data: 0x43d...726d6 logs: 1 hash: 0xee7...58e7f Debug ^

status 0x1 Transaction mined and execution succeed

transaction hash 0x45bf826bf2609261df9c5cb6ed7aca2dc825ecb96276640e61292702af870438

block hash 0xee795de8ee3cab1066dff420c5bbae347fc1b8eedca0610bcb0884feb058e7f

block number 9312235

from 0xA143D1bA8bDB46f91068AAcf646e13F705985972

to Poll.close() 0x70608b8A32f30e24F12f24bDcBD9E42aFC0E7d8f

gas 29943 gas

transaction cost 24952 gas

input 0x43d...726d6

decoded input {}

decoded output -

logs [
  {
    "from": "0x70608b8A32f30e24F12f24bDcBD9E42aFC0E7d8f",
    "topic": "0x231b4a6a9796cffff3206eb206f970c5e4f68248af093e30cf9e3d04857a6e66",
    "event": "PollClosed",
    "args": {
      "0": "0xA143D1bA8bDB46f91068AAcf646e13F705985972"
    }
  }
]
```

## Praktik Keamanan

- Menggunakan visibility eksplisit,
- Modifier onlyOwner untuk kontrol open/close,
- Pola Checks-Effects-Interactions (CEI) pada vote; event diterapkan untuk auditabilitas (Voted, PollClosed, PollOpened).