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

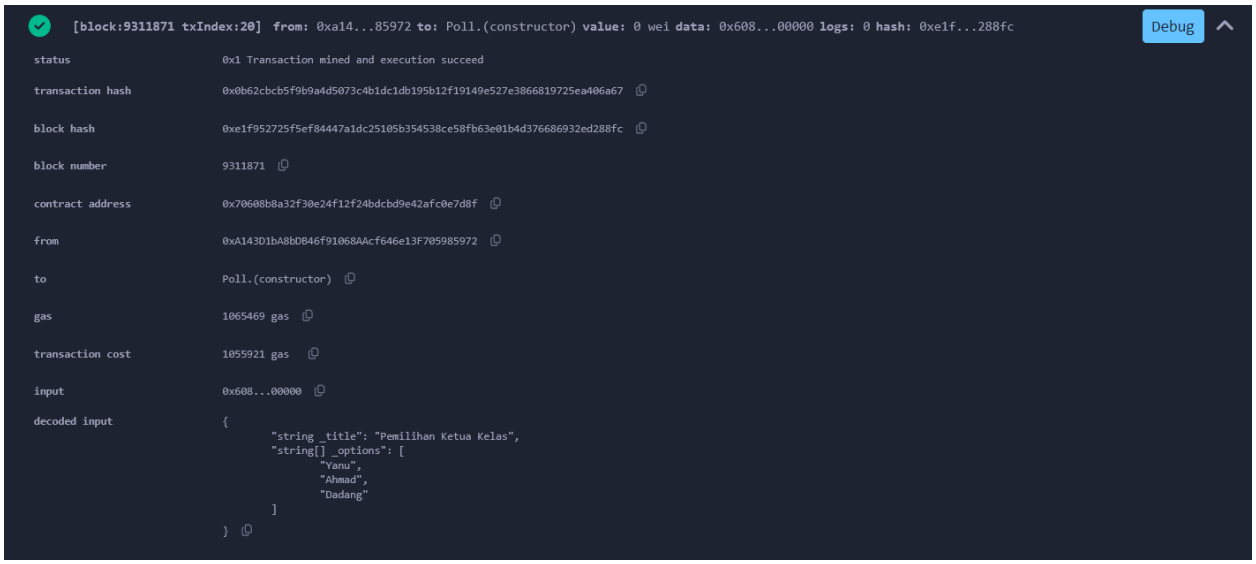
Untuk mendapatkan Testnet Tokens Sepolia ETH, didapatkan melalui halaman https://cloud.google.com/application/web3/faucet/ethereum/sepolia dan dengan tx hash 0xd23d03c83785f3a8e0bcdf0c59cc5e4691e23fa704c9eb2055cd26bd5eb3d06b

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



Pemanggilan fungsi optionsCount untuk mendapatkan angka banyak kandidat

Melakukan Vote untuk optionsIndex 1 (Ahmad)
Tx Hash = 0x1e1340e5e70352dc2386e61adecca5d0c50f8935aa59b509036f8aa9fc017211

Melakukan Vote lagi dengan address yang sama untuk optionIndex2
Tx Hash = 0xa53fd61942eb674b0d7442a9232743b86933d488fdced22d1b0bbfd587ed694e

Gagal karena pada seharusnya address dihitung sudah melakukan vote.

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

Close Poll menggunakan Owner
Tx Hash = 0x45bf826bf2609261df9c5cb6ed7aca2dc825ecb96276640e61292702af870438

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).