# Testing Methodology for the Voting Information System

## Description:

The development of the testing methodology for the voting information system involves a detailed analysis of testing all system components, excluding the frontend folder. The main focus is on ensuring the system's reliability, security, functionality, and performance.

## General Testing Goals

The testing of the system is aimed at ensuring reliability, security, functionality, and performance. The task of testing is to guarantee the correct operation of the system at all levels:

* **Data Handling:** Verifying the integrity, availability, and correctness of data storage.
* **Security:** Ensuring protection from unauthorized access, falsifications, and data leaks.
* **Smart Contracts:** Verifying the business logic implemented in the smart contracts, including creating polls, counting votes, and managing them.
* **User Functions:** Ensuring the correct operation of all functions such as user registration, voting, creating polls, and administration.

## Types of Tests and Testing Levels

The following types of testing are important for the voting system:

* **Unit Testing:** Testing the functionality of individual system components such as smart contracts, data repositories, API gateways, and other elements.
* **Integration Testing:** Testing the interaction between different components of the system, for example, the API gateway with the blockchain network, transaction correctness, and component interactions (such as adding questions to the voting or casting votes).
* **System Testing:** Testing the entire system as a whole, including testing system usage scenarios by users and administrators.
* **Security Testing:** Verifying data protection, user authentication, and protection against unauthorized access and data falsification.
* **Performance Testing:** Testing system performance under heavy loads, such as a large number of concurrent users.

In our system's testing, unit testing and system testing will be performed.

## Testing Methodology for Smart Contracts

The smart contracts will be tested using the following methods:

* Developing unit tests to verify all functions of the smart contracts.
* Using tools to test contracts on a local network, which will simulate the blockchain environment to test smart contracts without using real transactions.
* Testing the business logic of smart contracts, including verifying vote counting, poll creation, and management to ensure the correct execution of operations at all levels of interaction with the system.

## Blockchain Network Interaction Testing Process

The interaction with the blockchain network will be tested as follows:

* Verifying the interaction of the API gateway with the blockchain network via gRPC to ensure the correctness of data exchange between the system and the blockchain.
* Testing the correctness of blockchain records to ensure data reliability.
* Verifying the correctness of transactions in the blockchain, such as the correct recording of votes and the changing of data states after each vote.
* Network functionality testing, including verifying consensus operation and interaction with network nodes to ensure the correct operation of the entire system.

## Security Testing

A crucial part of testing is ensuring the security of the system. The security testing methodology includes:

* Vulnerability testing, including protection against request spoofing attacks and other types of threats.
* Verifying authentication and authorization of users to exclude unauthorized access.
* Checking the confidential data protection mechanism, such as passwords and votes, using cryptographic methods.
* Testing the fault tolerance of the security system, including verifying the system's operation in case of unauthorized access attempts or other attacks.