

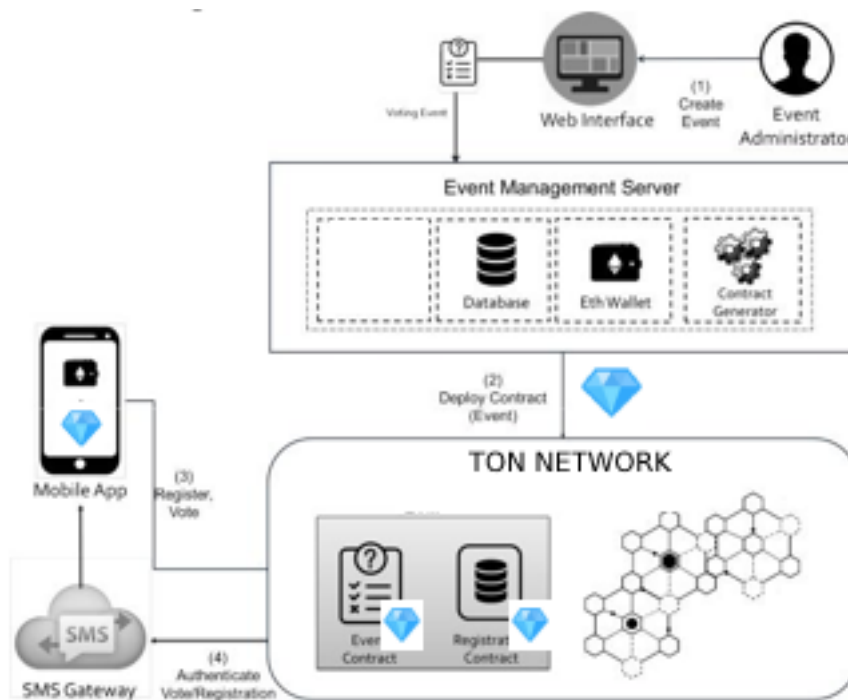
FREE TON DGO SYSTEM

System Components

The proposed platform consists of the following components:

1) Web application:

The web application aids event administrators in creating and managing new voting events. Each Voting event is represented as a separate Smart Contract in Blockchain network. The administrator fills-in the list of questions and their corresponding answers and then initiate an HTTP request to the Event Management Server containing the entered data. The goal of this Web application is to be available as an Application Programming Interface (API) allowing any user to create new voting events.



2) Event Management Server:

The main goal of the Event Management Server is to deploy the Smart Contract to the network with the data (questions and answers) received from the web application. Therefore, it contains an FREE TON Wallet(address) which is required to deploy the contract, a full node to interface the FREE TON network, and a database to store the list of contract addresses which will be fetched later by the mobile application.

3) Smart contracts: Two types of smart contracts exist in our system:

1) Registration contract,

2) Voting contract. The registration contract is deployed once for all voting events. It serves at securely registering and authenticating the voters. The voting contract is written once at development time, and deployed several times by the Event Management Server with different questions and answers specified by the event administrator as explained previously. Appendices A and B list the code of both contracts.

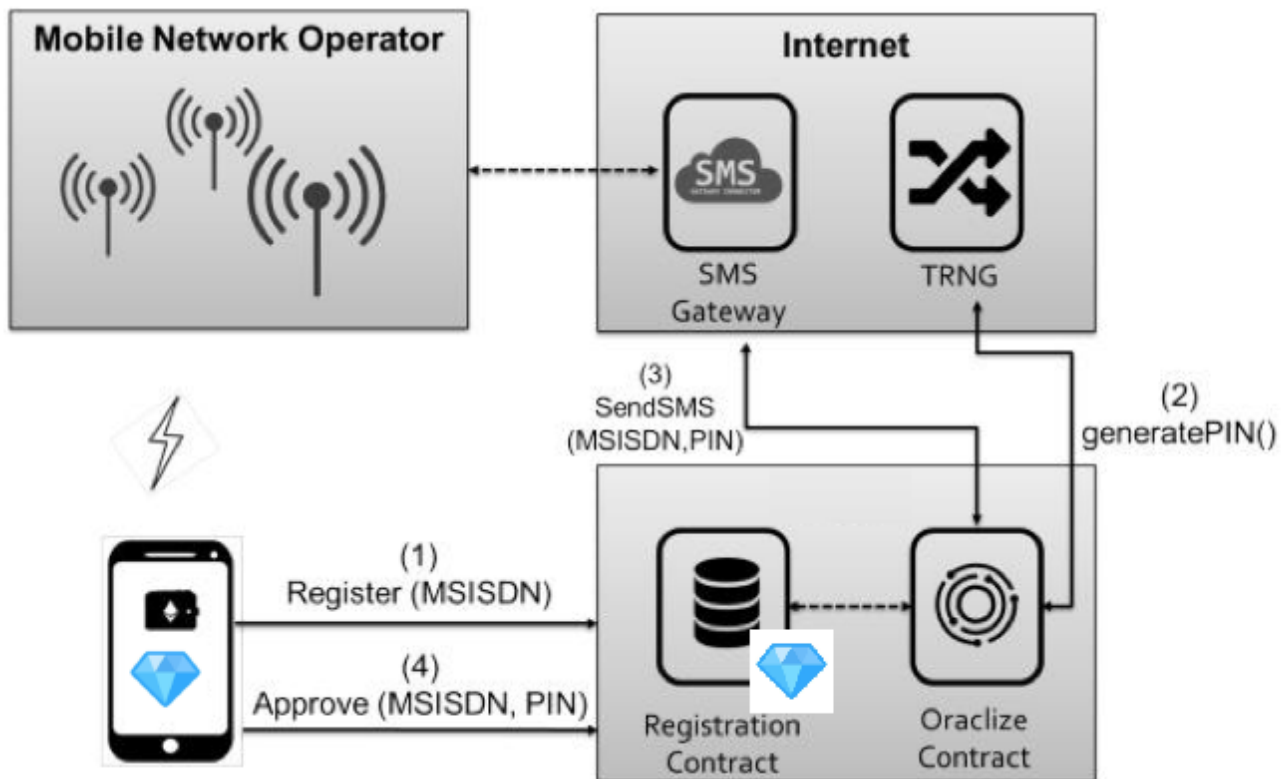
4) SMS Gateway: An SMS Gateway is ultimately mandatory in our system as it plays an important role in authenticating the users via sending SMS messages to the destined MSISDNs.

5) Mobile application: The mobile application is used by voters to register themselves in the system and then vote. It also provides the users the ability to fetch events, view questions and options, and visualize in real-time the results. Moreover, the application provides a detailed report showing the voting event statistics related to the frequency of votes per time slot, location, and others.

Registration & Configuration

To become an eligible voter, a user must first register to the system. Fig. 2 describes the voter's registration mechanism. Upon launching the application for the first time, the application automatically retrieves the user's MSISDN (phone number) from the Subscriber Identity Module (SIM card).

Registration and Voting require the EOA to possess sufficient Crystal as transactions to the Blockchain cost GAS which is priced in Crystal. The application generates an empty FREE TON wallet and requests the user to fill it through the wallet management function method as described in .



Once the user has sufficient Crystal balance, the `Register(MSISDN)` function is called with the user's MSISDN as a parameter.

The smart contract then validates that the MSISDN does not exist in the list of approved phone numbers. Then, it sends an HTTP request through the Oraclize contract to a True Random Number Generator

{TRNG} server to generate a random Personal Identification Number {PIN} code. Oraclize is a service that offers a secure connection between the smart contracts and external web APIs. When the PIN is generated, the contract again interfaces Oraclize to contact the Short Message Service (SMS) Gateway which in turn sends an SMS to the MSISDN containing the PIN as payload. Once the SMS is received by the MSISDN, the user then enters the PIN code to the application which will invoke the Approve(MSISDN, PIN) function. The contract then validates the received transaction by checking if its address (Msg. Sender) matches the address of the first register call, and checks if the PIN is correct

Creating a Voting Event

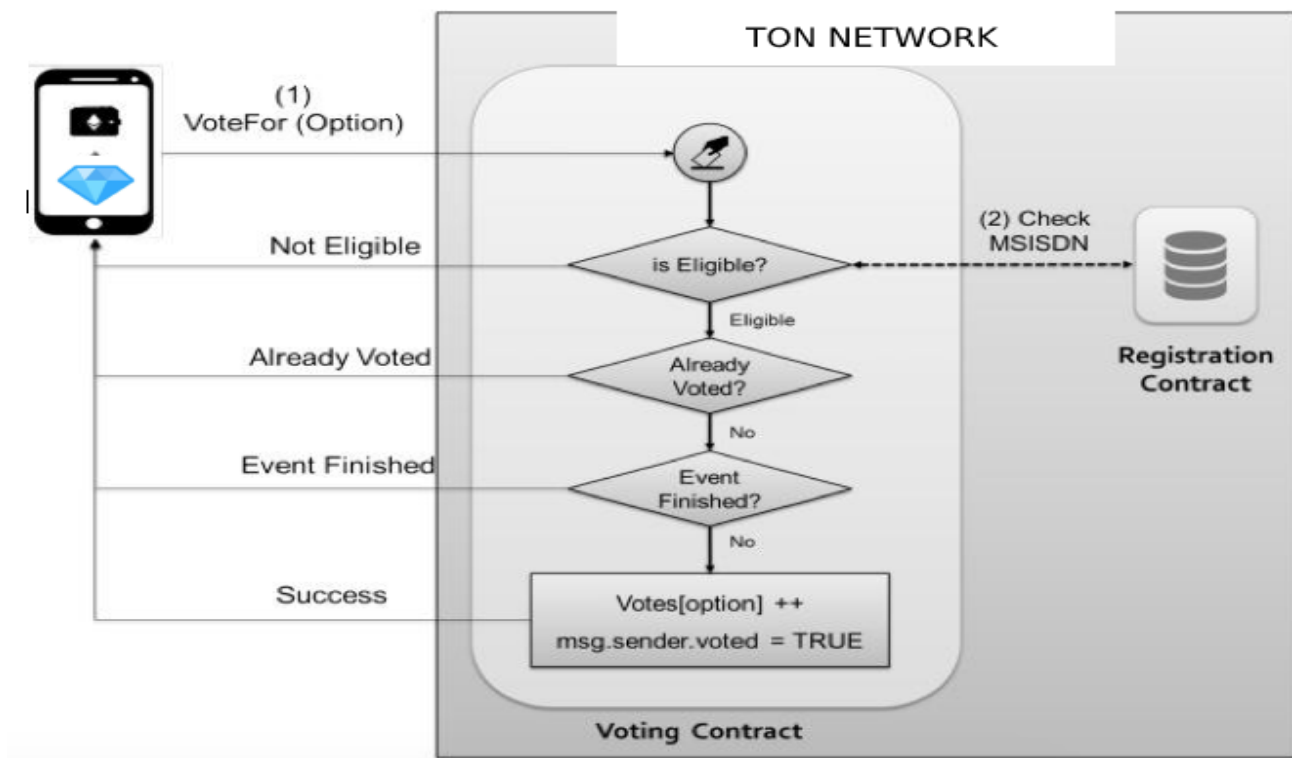
An event organizer uses the web application discussed previously to create a new voting event. This organizer will be able to monitor ongoing event statistics through graphs, charts and textual representations updated at a real-time.

To create a new event, the event organizer is requested to input the question(s) and the corresponding answer(s) through the web.

Technically, creating a voting event means creating a voting contract on the Blockchain. Therefore, this transaction must be charged for the event organizer as transactions cost in FREE TON. To simplify this process for organizers, a payment API is integrated into the web application allowing the organizer to pay using fiat currency for the transaction. After securing the transaction cost, the web app deploys the contract to FREE TON the network. The address of the newly created smart contract will be returned to the organizer and also stored in the database to track it later in the mobile application.

Voting

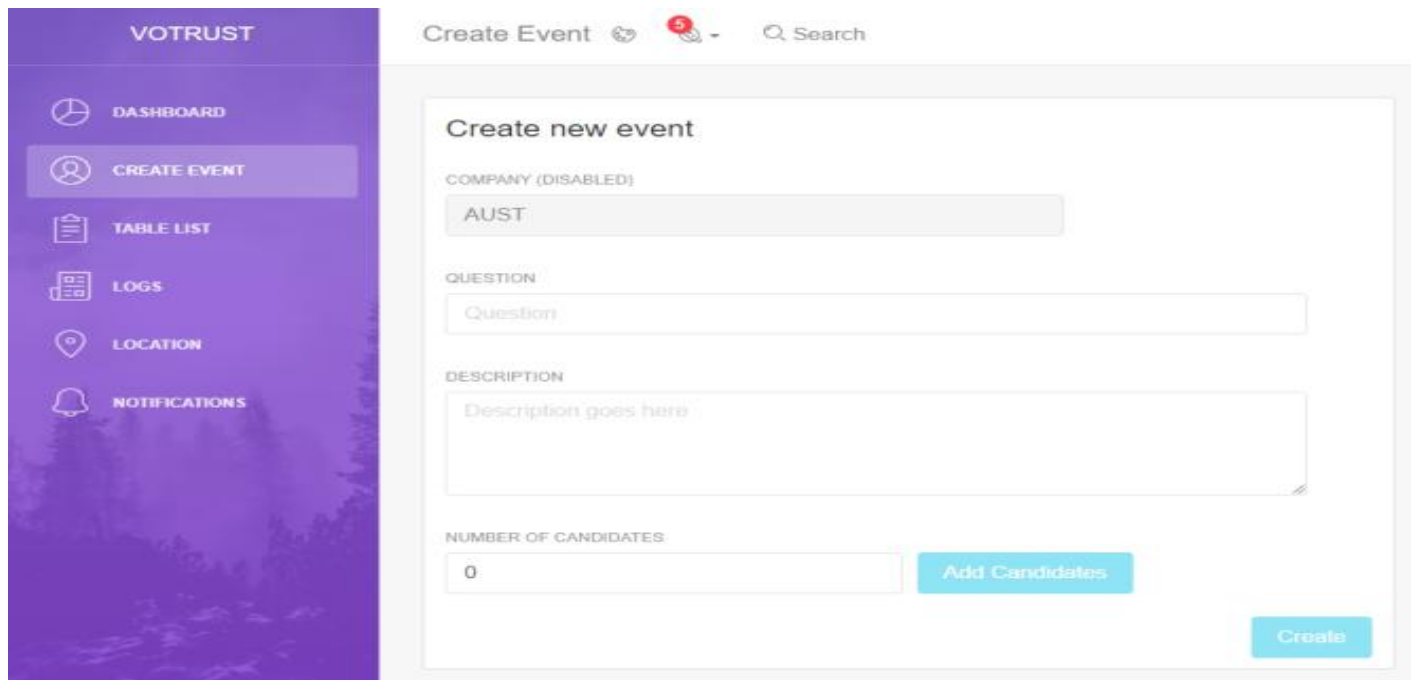
The voting mechanism is depicted in Fig. 3. While Voting, the application calls the `VoteFor(string option)` method of the designated smart contract deployed on the EVM. Next, the voting contract contacts the registration contract to check if the user is already registered. Then, it checks if the user already voted or the event is finished. If the conditions are satisfied, the contract increments the count of the selected option, marks the user as voted, and returns a success message to the application.



The contract automatically rejects duplicate votes, allowing to restrict one vote per MSISDN. This is considered the major advantage of our system compared to the others.

IMPLEMENTATION AND RESULTS

To validate the proposed system, we implemented the solution using various technologies. Solidity, a contract-oriented programming language for writing both registration and voting smart contracts, NodeJS Server side scripting for the Event Management Server, Web3js to interface the light client, and HTML5 web-app compiled using Apache Cordova for the mobile side. The Ropsten Testnet is used to simulate the Blockchain network. Twilio is used as the SMS gateway API



The screenshot shows the 'VOTRUST' web application interface. On the left is a purple sidebar with navigation links: DASHBOARD, CREATE EVENT (highlighted), TABLE LIST, LOGS, LOCATION, and NOTIFICATIONS. The main content area is titled 'Create new event' and includes a 'COMPANY (DISABLED)' dropdown menu with 'AUST' selected. Below this is a 'QUESTION' input field with the placeholder text 'Question'. A larger 'DESCRIPTION' text area contains the placeholder 'Description goes here'. At the bottom, there is a 'NUMBER OF CANDIDATES' input field with the value '0', an 'Add Candidates' button, and a 'Create' button.

shows the web page used by event organizers to create a new voting event.

