User Manual

1. As Election Administrator

1.1. Setup Election Administrator Page

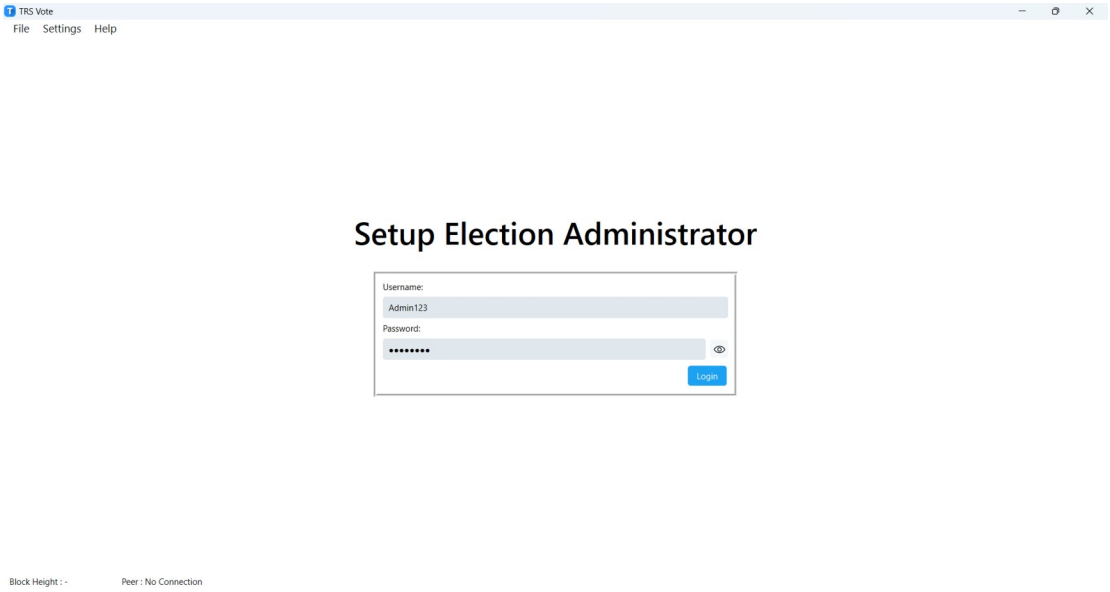

Figure 1

Figure 1 represents the setup process of the genesis block page, which serves as the initial block in a blockchain application. This page is crucial in determining the administrator of the election system. It is designed to appear when there are no existing blocks in the application. Once a username and password are set during this setup, the user who provided these credentials will assume the role of the blockchain administrator.

The genesis block is the foundation of the blockchain and contains important information that sets the initial state of the system. In the context of an election application, the genesis block plays a vital role in establishing the administrator who will have privileged access and control over the blockchain network.

During the setup process depicted in Figure 1, the user is prompted to provide a username and password. These credentials will be used to authenticate and authorize the individual as the administrator. By setting these login credentials, the user gains administrative privileges, allowing them to perform crucial tasks such as managing the blockchain network, creating polling, adding member to polling and ensuring the integrity and security of the election system.

1.2. Main Menu Election Administrator Page

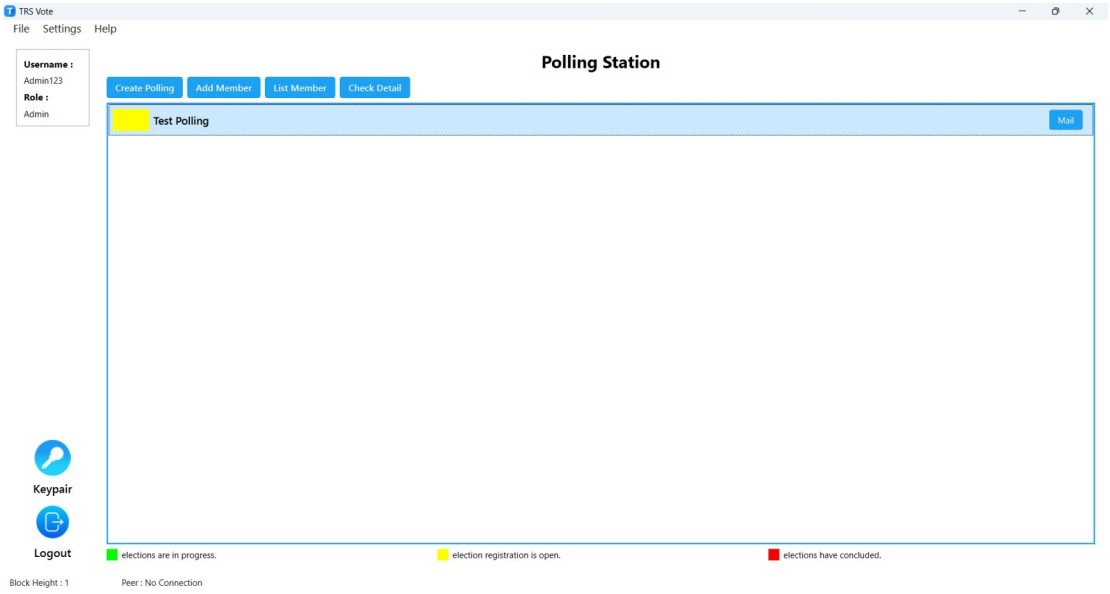

Figure 2

The main menu of the election administrator consists of a list of polling within the blockchain. This menu provides several options for managing the election process. There are four buttons available:

- "Create Polling" Button: This button allows the administrator to create a new polling event. Clicking on this button will redirect the user to the create polling page, where they can define the details and parameters of the new polling event.
- "Add Member" Button: Clicking on this button will display a dialog or prompt where the administrator can add members to a specific polling event. The administrator can register individuals as candidates or voters for that particular polling event.
- "List Member" Button: This button provides a list of members who have already registered for a specific polling event. This list includes both candidates and voters who have been added to the polling. The administrator can view and manage the registered members from this page.
- "Check Detail" Button: By clicking this button, the administrator can access detailed information about a specific polling event. This includes the start date, end date, and ring size used in that particular polling.

The administrator can also see the current state of the polling through color flags. Each polling event in the list will be represented by a color flag indicating its current state:

- Yellow Flag: This yellow flag signifies that the registration for the polling event is open. The administrator has the ability to add new members (candidates or voters) to the polling as long as the maximum member limit has not been reached. As an election administrator, you will see a "Mail" button displayed on the right side. Clicking on this button will redirect you to the mail page, where you can view the registration details of users who want to participate in that polling.

- Green Flag: A green flag indicates that the polling event is in progress. At this stage, the administrator cannot add new members. Voters who have already registered for the polling can cast their votes and choose candidates from the registered members.
- Red Flag: This color flag signifies that the election has concluded. It will display a "Result" button on the right side. Clicking on this button will redirect the administrator to the result page, which will show the real count and outcome of the polling event.

1.3. Create Polling Page

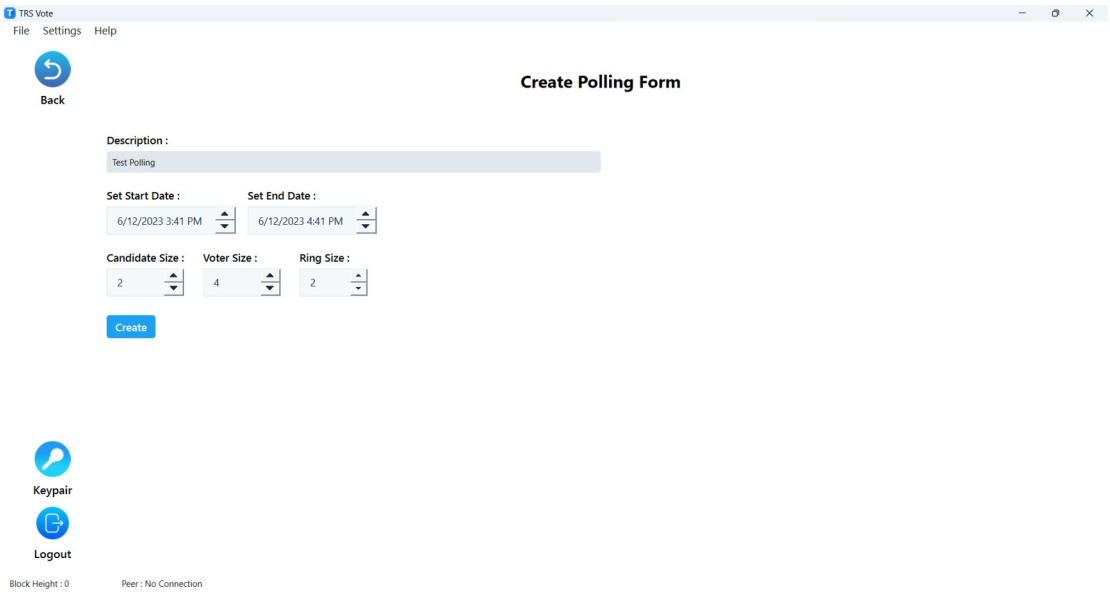

Figure 3

Figure 3 represents the "Create Polling" page, which contains a form with various fields and options to set up a new polling event. The page consists of the following elements:

- Description Field: This field allows the administrator to enter a description or title for the polling event. The description helps to provide information about the purpose or context of the election.
- QDateTimeEdit for Start Date and End Date: These fields are used to specify the start and end dates for the polling event. The administrator can select the desired dates and times using the QDateTimeEdit widget.
- Spinboxes for Candidate Size, Voter Size, and Ring Size: These spinboxes enable the administrator to set the desired sizes for different aspects of the polling event:
    - Candidate Size: This spinbox determines the maximum number of candidates allowed in the polling event. The administrator can set a specific limit based on the requirements of the election.
    - Voter Size: This spinbox sets the maximum number of voters who can participate in the polling event. The administrator can define the maximum number of registered voters based on the scope and scale of the election.
    - Ring Size: This spinbox is used to specify the size of the ring of traceable ring signature. The administrator can set the ring size based on the desired level of privacy and security.
- Create Button: This button triggers the creation of the polling event with the specified parameters. Once all the necessary information is provided, clicking this button will initiate the process of setting up the polling event within the blockchain system.

1.4. Form Member Registration Dialog

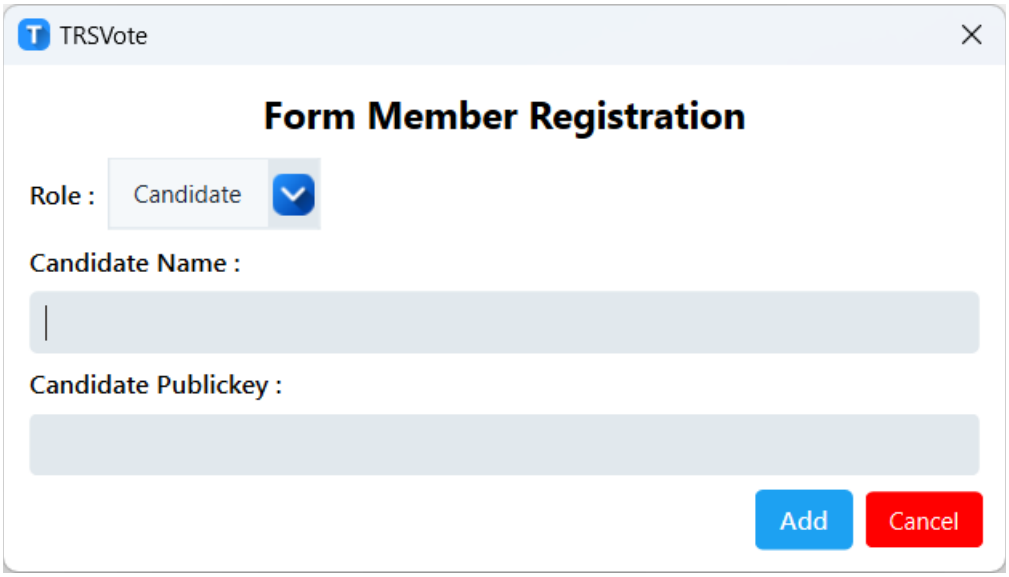

Figure 4

Figure 4 represents the "Member Registration" dialog, which appears after clicking the "Add Member" button in the main menu of the election administrator, specifically after selecting a polling event. The dialog allows the administrator to register new members for the chosen polling event. The "Member Registration" dialog consists of the following components:

Drop-down for Selecting Member Role: This drop-down menu enables the administrator to choose the role of the member being added to the polling event. The available options are "Candidate" or "Voter."

Candidate Name Field: If the administrator selects "Candidate" as the member role, this field appears, allowing the administrator to enter the candidate's name.

Candidate Public Key Field: If the administrator selects "Candidate" as the member role, this field is displayed. It allows the administrator to input the candidate's public key, which is an important cryptographic identifier.

Voter Public Key Field: If the administrator selects "Voter" as the member role, this field is shown. It enables the administrator to enter the voter's public key, which is used for authentication purposes.

Add Button: This button is used to add the member to the polling event with the provided details. Clicking on the "Add" button confirms the registration of the member.

Cancel Button: This button allows the administrator to cancel the member registration process.

1.5. Mail Page

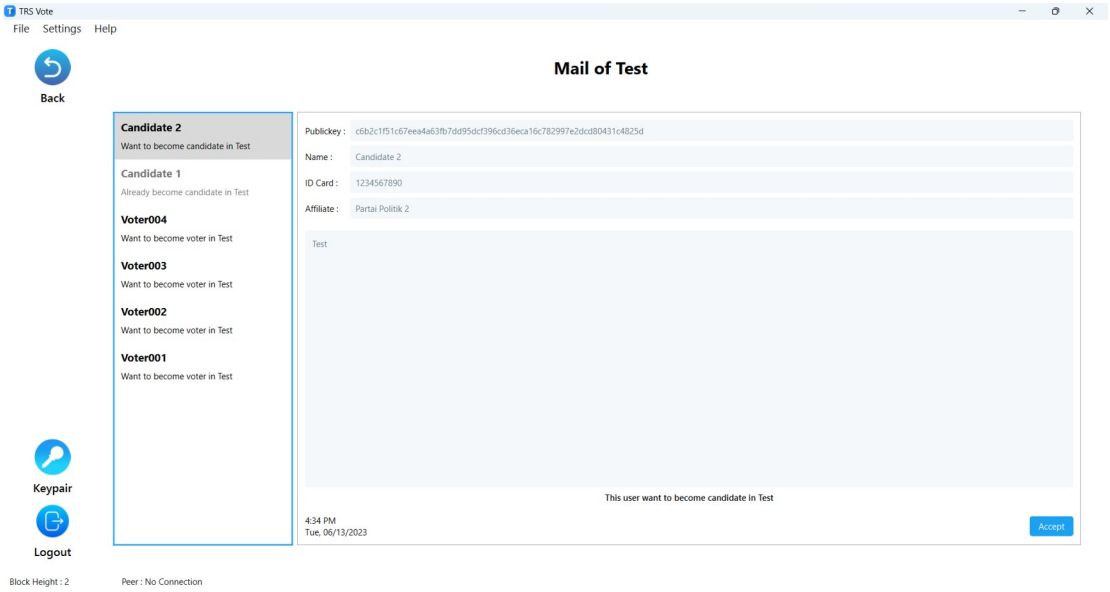

Figure 5

Figure 5 represents the "Mail" page, which is accessed by clicking the "Mail" button on the right side of a polling event in the main menu of the election administrator. This page displays the user requests to become a member of the selected polling event. The "Mail" page provides the following features:

- User Requests List: This section presents a list of user requests who have expressed their desire to become a member of the polling event. Each user request is listed, allowing the administrator to review and consider their membership.
- User Detail Display: When the administrator selects a specific user request from the list, the user's details are displayed on the right side of the page. This includes information such as the user's name, email address, and any other relevant details provided during the registration process.
- Accept Button: This button enables the administrator to accept the selected user as a member of the polling event. By clicking the "Accept" button, the user's membership is confirmed, and they are officially added to the polling event.

1.6. List Member Page

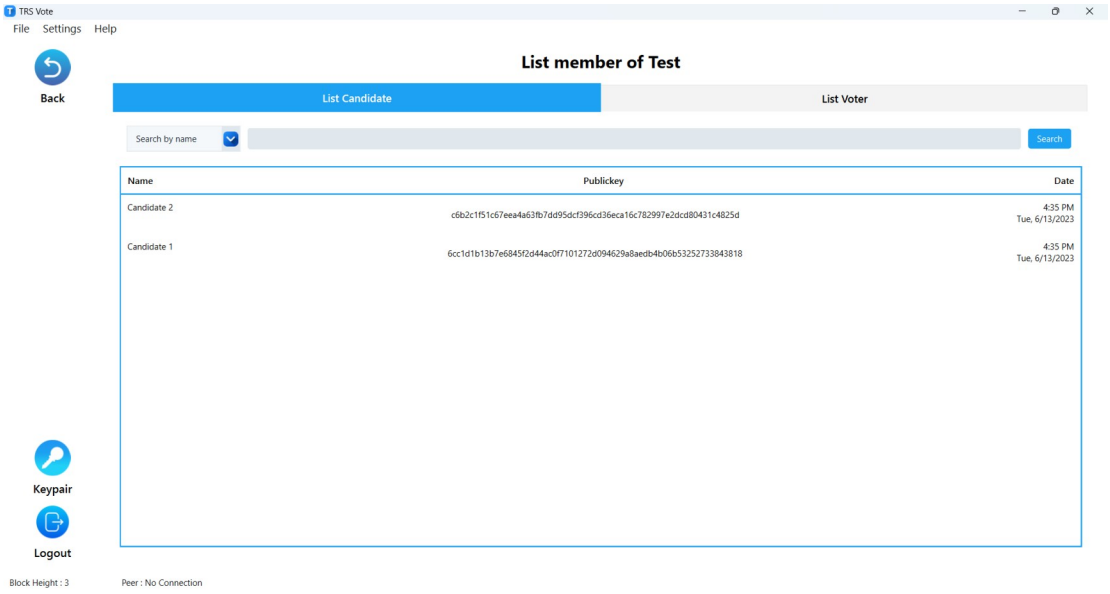

Figure 6

Figure 6 represents the "List Member" page, which is accessed by clicking the "List Member" button in the main menu of the election administrator. This page provides two tabs: "List Candidate" and "List Voter," allowing the administrator to view the registered members categorized accordingly. The "List Member" page consists of the following components:

- List Candidate Tab: This tab displays a list of registered candidates for the polling event. The list includes candidate names, their corresponding public keys, and the date when they were added as candidates.
- List Voter Tab: This tab presents a list of registered voters for the polling event. It displays the public keys of the voters and the date when they were added.
- Search Field and Search Button: These elements allow the administrator to search for specific members within the list. The search functionality can be performed based on the member's name or public key for candidates, and only by public key for voters.

The "List Member" page facilitates efficient management of the registered members for the polling event. By categorizing candidates and voters separately, it provides a clear overview of the member composition. The search feature further enhances usability by allowing administrators to quickly locate specific members based on their names or public keys.

2. As User

2.1. Login Page

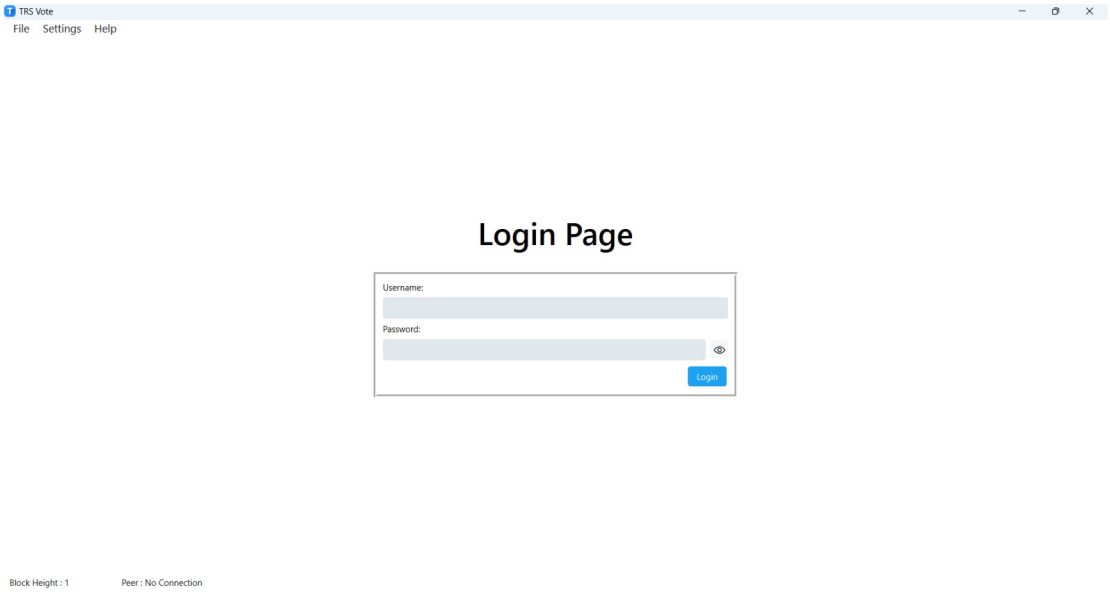

Figure 7

Figure 7 represents the "Login" page, which consists of a username field, a password field, and a login button. This page serves as the entry point for users to authenticate themselves and gain access to the system. The components of the "Login" page include:

- Username Field: This field allows users to input their unique username, which serves as their identification within the system. The username is typically associated with an individual account or profile.
- Password Field: Users are required to enter their corresponding password in this field. The password is securely stored and used to verify the user's identity during the login process. It is crucial to implement proper password security measures, such as hashing and salting, to protect user credentials.

- Login Button: Clicking this button triggers the login process. The system verifies the provided username and password combination against the stored credentials to determine whether access should be granted. Successful authentication allows the user to proceed further into the system, while incorrect or invalid credentials may result in an error message or a denied login attempt.

2.2. Main Menu User Page

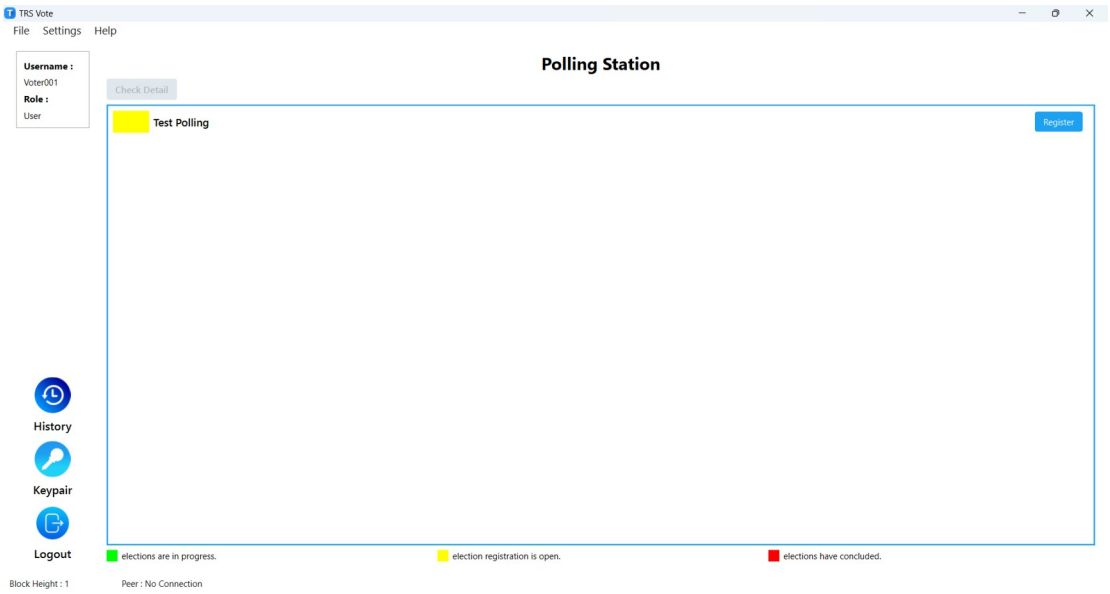

Figure 8

Figure 8 represents the "Main Menu User" page, which serves as the user interface for regular users in the blockchain-based election system. This page is similar to the "Main Menu Election Administrator" page, but with a few notable differences. The "Main Menu User" page includes the following elements:

- Navigation Bar: The navigation bar provides options for users to access different functionalities. In contrast to the election administrator page, there are three buttons in the user's navigation bar:

- History Button: This button allows users to view their voting history or past participation in previous polling events.
- Keypair Button: Clicking this button enables users to manage their cryptographic key pairs, which are crucial for secure authentication and interaction within the blockchain network.
- Logout Button: Users can click this button to log out from their current session and end their access to the system.

- Register Button: Instead of the "Mail" button found in the election administrator page, the user page displays a "Register" button. Clicking this button opens a dialog where users can request registration for a specific polling event. Users can express their interest in becoming a member (either as a candidate or voter) for the selected polling event.

2.3. History Page

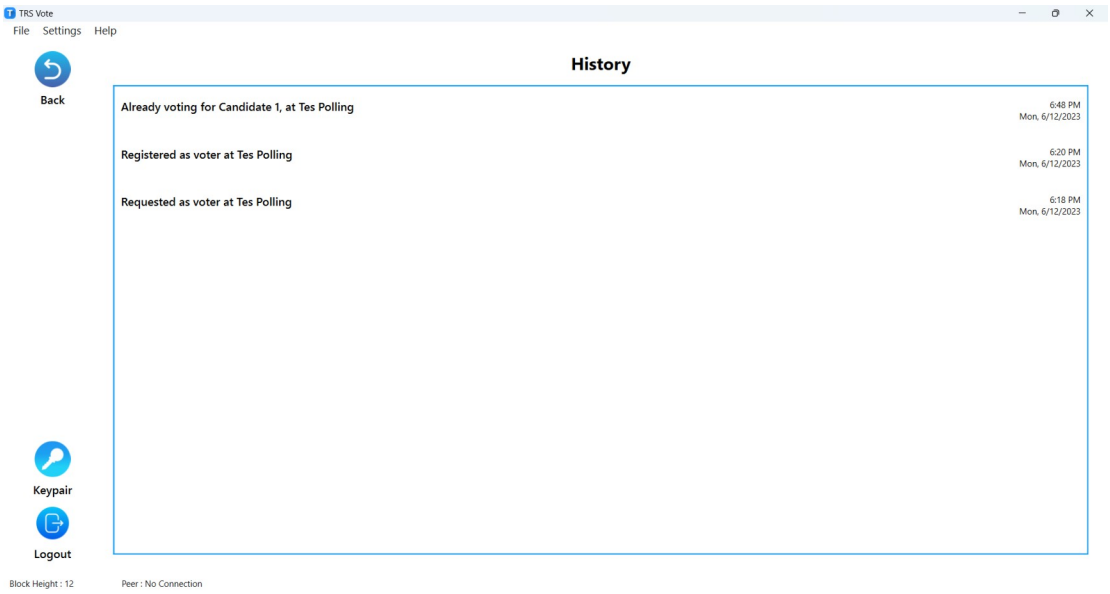

Figure 9

Figure 9 represents the "History" page, which provides a record of the user's activities within the blockchain-based election system. This page displays a chronological overview of the user's interactions and actions, including the following information:

Requested Activities: This section presents a log of the user's requests made at specific times. These requests may include actions such as requesting registration for a polling event.

Member Registration Activities: This section logs the user's registration activities for specific polling events. It shows the date and time when the user registered as a member (either as a candidate or a voter) for a particular polling event.

Voting Activities: This section captures the user's voting history. It records the date and time when the user cast their vote for a specific candidate and polling event.

2.4. Form Registration Dialog

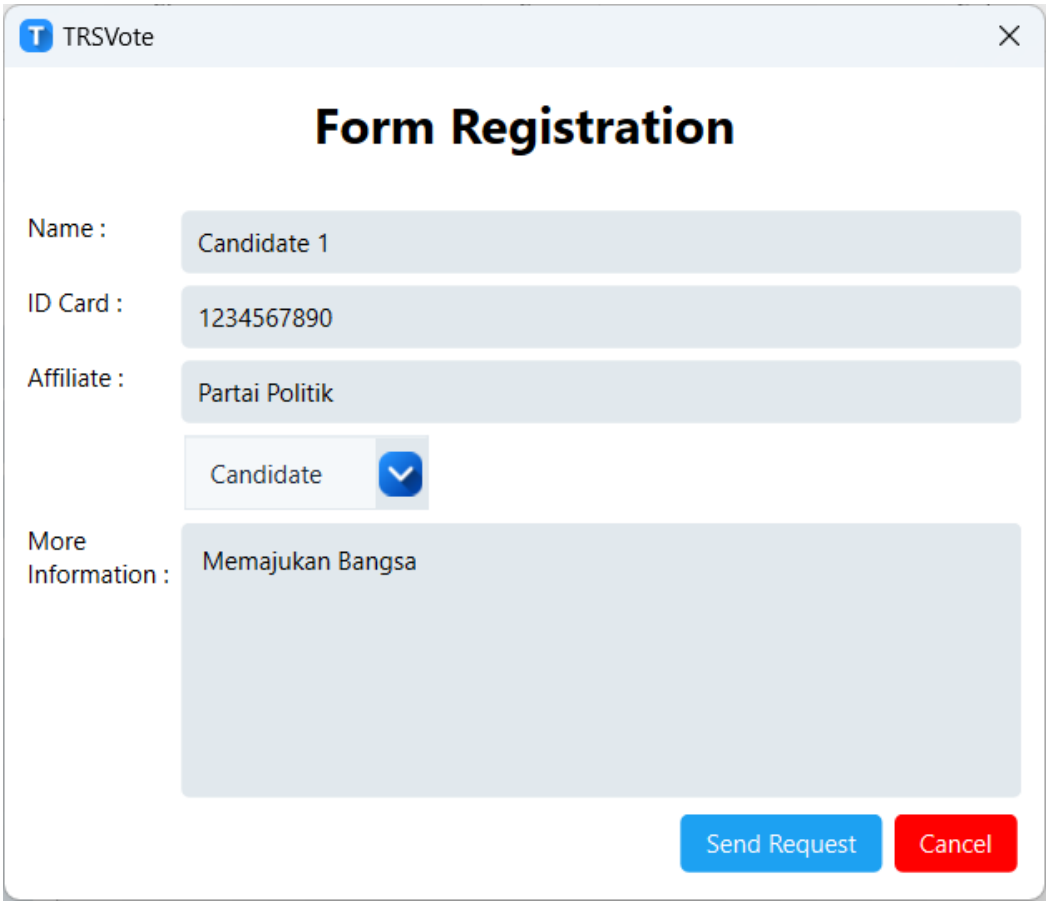

Figure 10

Figure 10 represents the "Registration Form Dialog," which appears after clicking the "Register" button in a specific polling event. This dialog facilitates the registration process for users who wish to participate in the selected polling event. The "Registration Form Dialog" consists of the following fields:

- Name: This field allows the user to enter their name, which serves as an identification for the registration process.

- ID Card: This field enables users to provide their ID card information, which may be required for verification purposes and ensuring the integrity of the election process.
- Affiliate: This field allows users to specify their affiliation, such as a political party, organization, or any relevant group they are associated with.
- More Information: This field provides users with an opportunity to provide additional information that may be relevant to their registration, such as qualifications, experience, or any other details required by the polling event.

Role Dropdown: This dropdown menu enables users to select their desired role within the polling event, either as a "Candidate" or a "Voter." Users can choose the appropriate role based on their intention to run as a candidate or participate as a voter.

Send Request Button: This button initiates the submission of the registration request to the election administrator. By clicking this button, users indicate their interest in participating in the polling event and request approval from the administrator.

Cancel Button: This button allows users to cancel the registration process without submitting the form.

2.5. Ballot Dialog

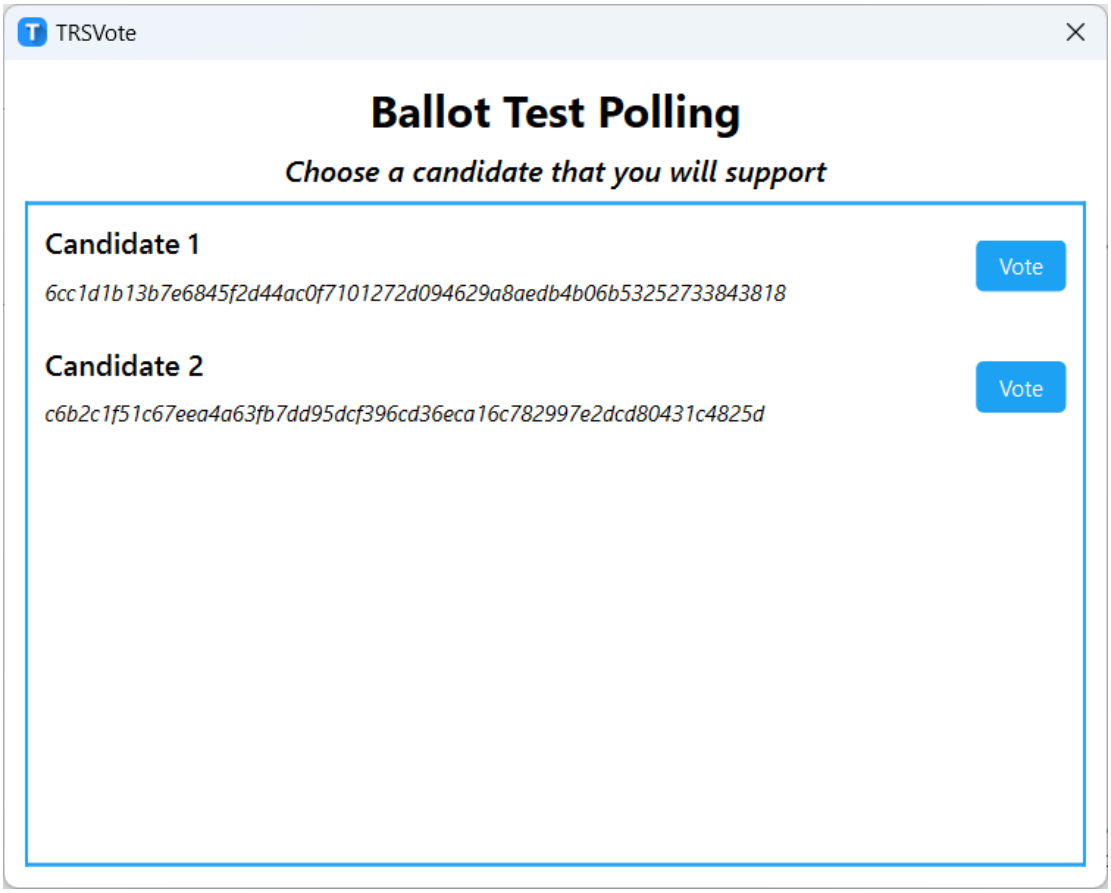

Figure 11

Figure 11 represents the "Ballot Dialog," which is accessible only to registered voters within a specific polling event. This dialog is displayed when a user clicks the "Vote" button in the main menu for a polling event in which they are registered. The "Ballot Dialog" provides the following features:

- Candidate List: This section displays a list of candidates participating in the polling event. Each candidate's name and public key are shown to facilitate identification.

- Vote Buttons: On the left side of each candidate, a "Vote" button is located. Users can select their preferred candidate by clicking the corresponding "Vote" button.
- Confirmation: Once a user clicks the "Vote" button for a specific candidate, a confirmation prompt is shown, ensuring that the user's selection is accurate. This step helps prevent accidental or erroneous voting.
- Submit Vote: After confirming their choice, users can click the "Submit Vote" button to officially cast their vote for the selected candidate.

2.6. Detail Polling Dialog

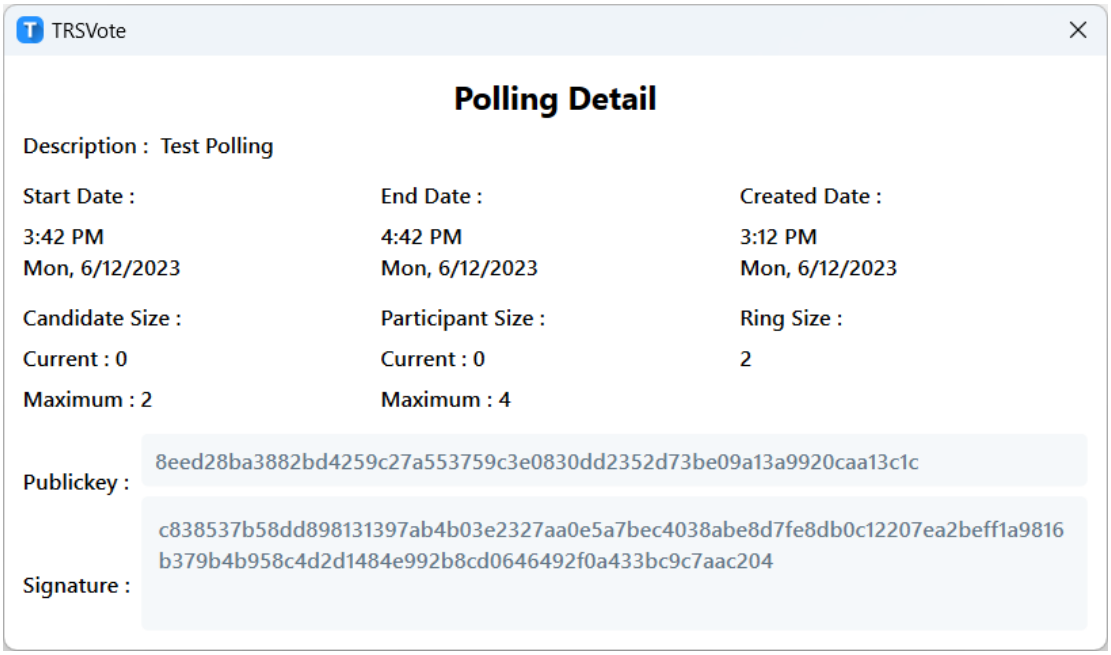

Figure 12

Figure 12 represents the "Polling Detail Dialog," which is accessed by clicking the "Check Detail" button in the main menu after selecting a specific polling event. This

dialog provides detailed information about the polling event, including the following details:

- Start Date and End Date: This information indicates the duration of the polling event, specifying when it begins and when it concludes.
- Created Date: This date signifies when the polling event was initially created or set up within the blockchain-based election system.
- Ring Size: The ring size refers to the number of participants involved in the cryptographic protocol used within the polling event. It indicates the size of traceable ring signature.
- Candidate Current and Max Size: These values represent the current number of candidates registered for the polling event and the maximum allowed number of candidates, respectively. It provides an overview of the candidate roster and the capacity for candidate participation.
- Voter Current and Max Size: Similarly, these values indicate the current number of voters registered for the polling event and the maximum allowed number of voters, respectively. It offers insights into the voter turnout and the capacity for voter participation.

2.7. Result Page

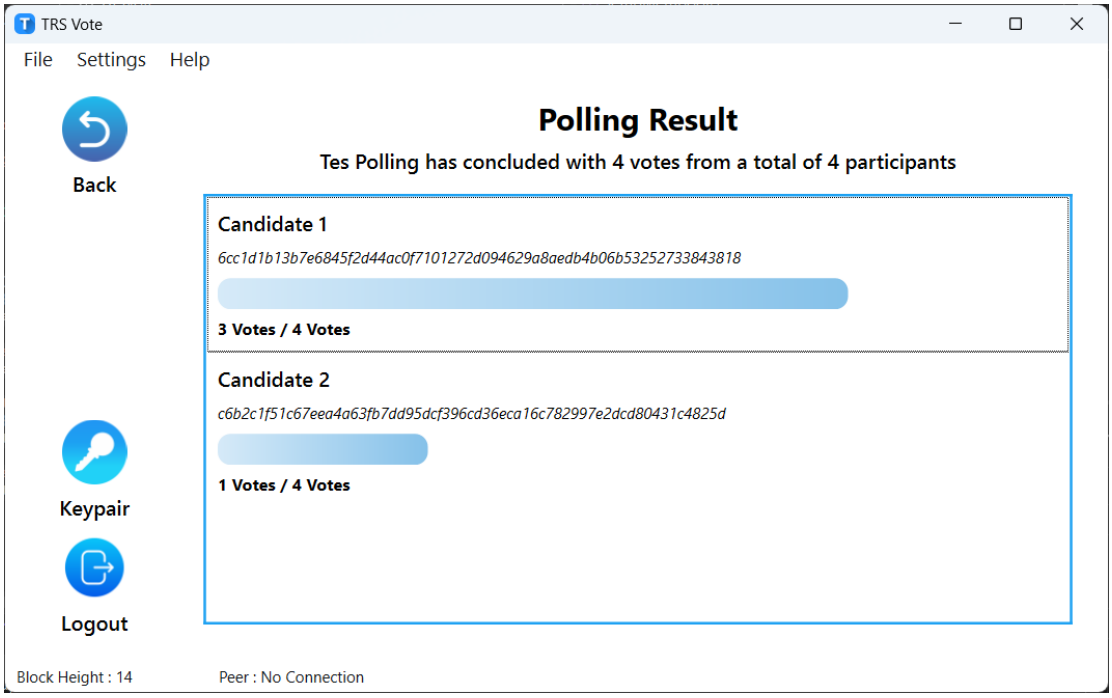

Figure 13

Figure 13 represents the "Result Page" that is accessed by clicking the "Result" button in a specific polling event from the main menu. This page displays the outcome of the polling event, providing information about the candidates and their respective vote counts. The "Result Page" includes the following elements:

- Candidate List: This section presents a list of candidates who participated in the polling event. Each candidate is identified by their name and public key, ensuring accurate identification.
- Vote Count: Next to each candidate, the page shows the number of votes received by the candidate. This information is presented in the format of "X / Y," where "X" represents the number of votes obtained by the candidate, and "Y" represents the total number of votes cast in the polling event.

- Graphic Bar: The design incorporates a graphical representation, such as a bar chart, to visually depict the vote counts for each candidate. This provides a quick and intuitive overview of the relative vote distribution among the candidates.

2.8. Keypair Dialog

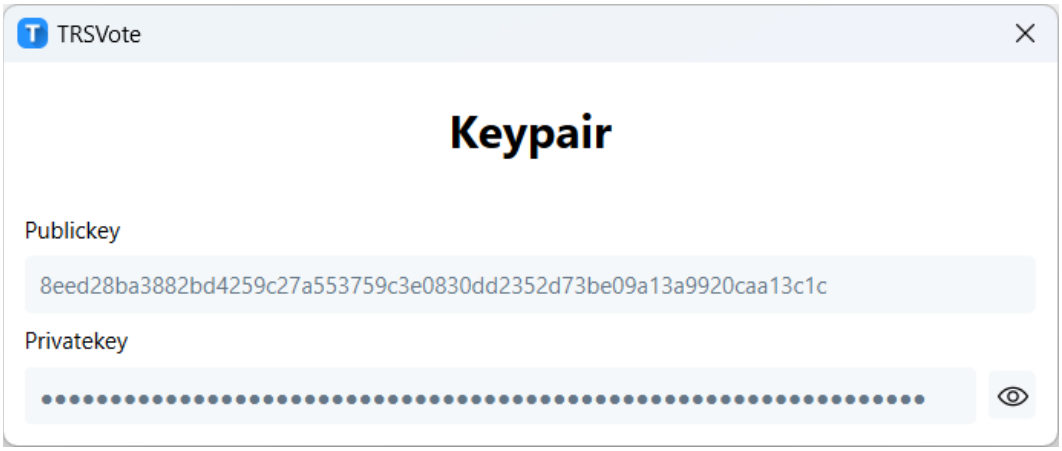

Figure 14

Figure 14 represents the "Keypair Dialog" that appears when the user clicks on the "Keypair" button in the navigation bar. This dialog displays the user's public key and private key, which are crucial for authentication within the blockchain system.

It is important to note that the authentication mechanism in the blockchain utilizes the ed25519 asymmetric encryption algorithm and AES encryption. Additionally, the traceable ring signature scheme is employed to ensure privacy and security.

The "Keypair Dialog" provides users with access to their public and private keys, enabling them to securely engage in transactions and activities within the blockchain system. It is crucial to emphasize the importance of safeguarding the private key to prevent unauthorized access and maintain the security of the user's account and interactions within the blockchain network.