Voting with Blockchain

Name: Pranav Chopde

Parties Involved:

1. **Admin/Owner:** The Admin, also known as the Owner, has the highest authority in the system. They have the ability to initiate and end elections, reset the entire election for a fresh start, add new candidates, and declare the winner at the end of the election. It's likely that the owner would be an election commission or a trusted third-party organization responsible for overseeing the entire election process.

2. **Candidate:** A Candidate is someone who is contesting in the election. They register themselves for the election and have their names, party, and other details stored in the system. Candidates are expected to deposit a certain amount of cryptocurrency as a form of commitment to the election process. At the end of the election, the deposit may be returned or confiscated based on whether they reach a minimum vote threshold.
3. **Voters:** Voters are the primary participants of the election. They have the ability to vote for candidates during the election. Each voter has a unique address and is registered in the system with a specific name and number of votes they are allowed to cast. Voters also have the ability to delegate their votes to another registered voter. After casting their votes or delegating them, the count of votes they have left decreases accordingly.

Features of the application:

1. **constructor()**: This function is automatically run when the contract is deployed. Here, the address of the account that deployed the contract (msg.sender) is set as the contract owner.

2. **adminOnly**(): This is a modifier that restricts access to certain functions. The keyword 'require' ensures that the function can only be called by the owner of the contract.

3. **transferOwnership**(): This function transfers the ownership of the contract to a new owner. It can only be called by the current owner (admin), as it uses the adminOnly modifier.

4. **setMinimumDeposit**(): This function allows the contract owner to set the minimum deposit amount for candidates. This function can only be called when the election hasn't started.

5. **addCandidate**(): This function allows the owner to add a candidate. It checks for certain conditions like if the election has already started, if the candidate's address is not null, if the candidate is not the owner of the contract, if the candidate is not already registered, and if the candidate name and party are not empty.

6. **submitDeposit**(): This function allows candidates to submit their deposit. It first checks if the election has started, if the candidate ID is valid, if the candidate is the one making the deposit, if the deposit meets the minimum deposit amount, and if the candidate is registered.

7. **withdrawNomination**(): This function allows candidates to withdraw their nomination and get back 80% of their deposit. The candidate can only withdraw if the election has not started.

8. **removeCandidate**(): This function can be used by the admin to remove a candidate from the election. It checks if the candidate ID is valid and if the candidate is registered.

9. **displayCandidate**(): This function is used to view the details of a particular candidate. It returns the candidate's name, proposal, party, and address.

10. **addVoter**(): This function allows the owner to add a voter. It checks certain conditions such as if the election has already started, if the voter's address is not null, if the voter is not already registered, and if the voter name is not empty. Each voter gets a default of 1 vote.

11. **viewVoterProfile**(): This function is used to view the details of a particular voter. It returns the voter's name, the ID of the candidate they voted for, and whether their vote was delegated.

12. **startElection**(): This function can only be called by the admin to start the election. Before starting the election, it checks if the election has not already started or ended, and if there is at least one candidate. It also disqualifies any candidates who haven't deposited the minimum amount.

13. **delegateVote**(): This function allows voters to delegate their voting rights to another voter. It checks if the delegating voter has voting rights left, if they are not delegating to themselves, if the delegate is a registered voter, and if the election is ongoing. It then transfers the voting rights of the delegating voter to the delegate.

14. **castVote**(): This function allows voters to cast their vote for a candidate. It first checks if the election is ongoing, if the candidate exists, and if the voter has voting rights left. It then decreases the voter's voting rights by one and increases the candidate's vote count by one.

15. **endElection**(): This function can only be called by the admin and is used to end the election. It first checks if the election is currently ongoing. After the election ends, the total number of votes is calculated and a minimum threshold is set (in this case 16% of total votes). It then iterates over all the candidates and returns their deposits if they received more than the minimum threshold of votes, else the deposit is confiscated and transferred to the owner.

16. **showWinner**(): This function can only be called by the admin and returns the name, party, and vote count of the winner. It first checks if the election has ended. It then

calculates the highest vote count and creates an array of candidates with the highest vote count. In case of a tie, it selects a winner randomly using a lottery system based on the block timestamp and difficulty.

17. **showElectionResult**(): This function is used to display the election results of a particular candidate. It checks if the candidate exists and if the election has ended. It then returns the candidate's name, party, and vote count.

18. **resetElection**(): This function can only be called by the admin and is used to reset the elections for conducting fresh elections. It checks if the election has ended before resetting. It then resets the state variables such as the list of candidates, votes, candidates count, and voters count. The election status is also reset to the initial status.