|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Contract Name** | **Purpose/Application domain** | **Administration** | **Vote input** | **Winning Strategy** | **Winning variable** |
| Ballot.sol | Used to vote for multiple proposals | chairperson | uint[] **weights**,  bytes32[] **voterNames**,  uint[] **proposalIds** | Proposal with the most votes win | winningProposal |
| DemaxBallotFactory.sol | Used to vote for 2 proposals | Governor | uint **proposal** | Proposal with the most votes win | YES/NO |
| Gatekeeper.sol | Used in Panvala network  Used to vote for multiple slates | Gatekeeper | address **voter**,  bytes32 **commitHash**,  uint **numTokens** | Slate with the most votes win | contest.winner |
| ibaVoter.sol | Used to vote for multiple proposals | Chainperson | address **chainperson**, uint256 **ballot**,  uint256 **proposalNum** | Proposal with the most votes win | winner |
| localElection | Originally planned for 2019 Hong Kong local elections.  Used to vote for council. | Owner | uint256 **voterID**,  uint256 **hashedEmail**,  string memory **council**, string memory **singleVote** | Council with the most valid votes win | councilVoterNumber[council] |
| PLCRVotingCheckpoint.sol | Used in Polymath Network where the issuer or board members can propose an agenda to get the opinion of the investors over it.  Used to vote for multiple proposals | Admin | uint256 **\_ballotId**,  bytes32 **\_secretVote** | Proposal with the most votes win | winningProposal |
| Redenom.sol | Used in Redenom DAO to vote for start-up projects to be funded by Redenom.  Used to vote for multiple projects | onlyAdmin | uint **\_id** | Project with the most votes and is active win | \_winningProject |
| TACVoting.sol | Used in Taekwondo Cooperative to vote in taekwondo matches.  Used to vote for multiple matches | - | uint64 **electionId**,  uint64 **matchId** | Match with the most votes win | Elections[electionId].winningMatch |
| TomiQuery2.sol | Used to vote for 2 proposals | Governor | address **user**,  uint256 **proposal** | Proposal with the most votes win | YES/NO |
| WeightedVoteCheckpoint.sol | Used in Polymath Network.  Used to vote for multiple proposals | Admin | uint256 \_**ballotId**, uint256 \_**proposalId** | Proposal with the most votes win | winningProposal |

# Voting Criteria

**Majority Criterion**

If a candidate wins by more than 50% of the votes, then that candidate should win the election by another method.

Evaluation: If the majority winner does not win by another method, then this criterion is violated. If majority winner does win by another method, then it is not violated.

**Condorcet** **Criterion**

If a candidate wins by head-to-head (pairwise) over every other candidate, then that candidate should win the election.

Evaluation: If one candidate wins over all others when paired up and does not win by another method, then the criterion is violated. If by another method, the head-to-head winner still wins, then the criterion is not violated.

**Irrelevant Alternatives Criterion**

The election results should not change if a losing candidate is left out.

Evaluation: A candidate drops out. Look at the 1st place votes. If another candidate wins, then it is violated. If original winner still wins, then the criterion is not violated.

**Monotonicity Criterion**

A candidate wins an election. Voter preference changes before the re-election only favour the winner; the winner should still win the election.

Evaluation: Voter preference changes favouring the winner and re-election winner different, it is violated. Voter preference changes favouring the winner and re-election winner the same, it is not violated.

# Voting Methods

**Plurality Method**

The choice with the most first-preference votes is declared the winner. Ties are possible, and would have to be settled through some sort of run-off vote.

Problem with Plurality Method:

If there are 3 or more choices, it is possible that a choice could lose but when compared to one-to-one comparison could be preferred over the plurality winner. This violates the Condorcet Criterion.

**Borda Method**

Points are assigned to candidates based on their ranking, for example: 1 point for last, 2 points for second-to-last. The point values for all ballots are totalled and the candidate with the largest point total is the winner.

Problem with Borda Method:

A candidate could receive majority of the first-choice votes and still lose the election. This violates the Majority Criterion.

**Pairwise Comparison**

For each pair of candidates (there are C(N,2) of them), we calculate how many voters prefer each. The candidate of the pair whom most voters prefer is awarded one point, and the loser get 0 points. If there is a tie, each candidate gets half a point. At the end, the candidate with the most points wins.

This satisfies the Condorcet Criterion, Majority Criterion, and Monotonicity Criterion.

Problem with Pairwise Comparison:

Violates the Independence of Irrelevant Alternatives Criterion.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Plurality Criterion | Monotonicity Criterion | Condorcet Criterion | Irrelevant Alternatives Criterion |
| Plurality Method | Satisfies | Satisfies | Violates | Violates |
| Borda Method | Violates | Satisfies | Violates | Violates |
| Pairwise Comparison | Satisfies | Satisfies | Satisfies | Violates |

Check each contract, which criteria they violate or satisfy. Download ubuntu virtual machine to run code

# Contracts Fairness Criteria Analysis

## Ballot.sol

### 1. Plurality Criterion

Plurality criterion is **satisfied**. As seen from the results function, the proposal with the most votes win.

Text

Description automatically generated

### 2. Monotonicity Criterion

Monotonicity criterion is **satisfied**.

### 3. Condorcet Criterion

Condorcet criterion is **violated**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Number of voters | 1 | 3 | 3 | 3 |
| 1st choice | A | A | B | C |
| 2nd choice | B | C | C | A |
| 3rd choice | C | B | A | B |

According to the plurality method, proposal A wins with 4 votes. However, using the Method of Pairwise Comparisons,

comparing proposals **A** and **B**:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Number of voters | 1 | 3 | 3 | 3 |
| 1st choice | A | A | B |  |
| 2nd choice | B |  |  | A |
| 3rd choice |  | B | A | B |

A has 7 votes and B has 3 votes, hence proposal A is the winner.

Comparing proposals **A** and **C**:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Number of voters | 1 | 3 | 3 | 3 |
| 1st choice | A | A |  | C |
| 2nd choice |  | C | C | A |
| 3rd choice | C |  | A |  |

A has 4 votes and C has 6 votes, hence proposal C is the winner.

Comparing proposals **B** and **C**:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Number of voters | 1 | 3 | 3 | 3 |
| 1st choice |  |  | B | C |
| 2nd choice | B | C | C |  |
| 3rd choice | C | B |  | B |

B has 4 votes and C has 6 votes, hence proposal C is the winner.

Since proposal C wins all pairwise comparisons against other proposals, proposal C is the Condorcet candidate and winner. However according to the plurality method, proposal A is the winner. Hence the condorcet criterion is violated.

### 4. Irrelevant Alternatives Criterion

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Number of voters | 6 | 5 | 4 | 2 |
| 1st choice | A | D | C | B |
| 2nd choice | B | B | D | C |
| 3rd choice | D | C | B | D |
| 4th choice | C | A | A | A |

According to the plurality method, proposal A wins with 6 votes.

However, if proposal D, which was a losing proposal, is removed:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Number of voters | 6 | 5 | 4 | 2 |
| 1st choice | A |  | C | B |
| 2nd choice | B | B |  | C |
| 3rd choice |  | C | B |  |
| 4th choice | C | A | A | A |

Proposal B wins with 7 votes. Hence this violates the irrelevant alternatives criterion.

## DemaxBallotFactory.sol

### 1. Plurality Criterion

Plurality criterion is **satisfied**. As seen from the results function, proposals[YES] and proposals[NO] are int values denoting the number of votes for each proposal. The proposal with higher number of votes is the winner.

Text

Description automatically generated

### 2. Monotonicity Criterion

Monotonicity criterion is **satisfied**.

### 3. Condorcet Criterion

Condorcet criterion is **not applicable** since there is only 2 proposals in the election.

### 4. Irrelevant Alternatives Criterion

Irrelevant alternatives criterion is **not applicable** since there is only 2 proposals in the election.

## Gatekeeper.sol

### 1. Majority Criterion

Majority criterion is satisfied. The winner need to have more than 50% of votes to win, else a runoff is initialized.

### 2. Monotonicity Criterion

Monotonicity criterion is **satisfied**.

### 3. Condorcet Criterion

Condorcet criterion is **violated**. Explanation same as Ballot.sol.

### 4. Irrelevant Alternatives Criterion

Irrelevant alternatives criterion is **violated**. Explanation same as Ballot.sol.

## ibaVoter.sol

### 1. Plurality Criterion

Plurality criterion is **satisfied**. As seen from the results function, the proposal with higher number of votes is the winner.

Text

Description automatically generated

### 2. Monotonicity Criterion

Monotonicity criterion is **satisfied**.

### 3. Condorcet Criterion

Condorcet criterion is **violated**. Explanation same as Ballot.sol.

### 4. Irrelevant Alternatives Criterion

Irrelevant alternatives criterion is **violated**. Explanation same as Ballot.sol.

## PLCRVotingCheckpoint.sol

### 1. Plurality Criterion

Plurality criterion is **satisfied**. As seen from the results function, the proposal with higher number of votes is the winner.

Text

Description automatically generated

### 2. Monotonicity Criterion

Monotonicity criterion is **satisfied**.

### 3. Condorcet Criterion

Condorcet criterion is **violated**. Explanation same as Ballot.sol.

### 4. Irrelevant Alternatives Criterion

Irrelevant alternatives criterion is **violated**. Explanation same as Ballot.sol.

## Redenom.sol

### 1. Plurality Criterion

Plurality criterion is **satisfied**. As seen from the results function, the proposal with higher number of votes is the winner.

### Text Description automatically generated

### 2. Monotonicity Criterion

Monotonicity criterion is **satisfied**.

### 3. Condorcet Criterion

Condorcet criterion is **violated**. Explanation same as Ballot.sol.

### 4. Irrelevant Alternatives Criterion

Irrelevant alternatives criterion is **violated**. Explanation same as Ballot.sol.

## TACVoting.sol

### 1. Plurality Criterion

Plurality criterion is **satisfied**. As seen from the results function, the proposal with higher number of votes is the winner.

Text

Description automatically generated

### 2. Monotonicity Criterion

Monotonicity criterion is **satisfied**.

### 3. Condorcet Criterion

Condorcet criterion is **violated**. Explanation same as Ballot.sol.

### 4. Irrelevant Alternatives Criterion

Irrelevant alternatives criterion is **violated**. Explanation same as Ballot.sol.

## TomiQuery2.sol

### 1. Plurality Criterion

Plurality criterion is **satisfied**. As seen from the results function, proposals[YES] and proposals[NO] are int values denoting the number of votes for each proposal. The proposal with higher number of votes is the winner.

Text

Description automatically generated

### 2. Monotonicity Criterion

Monotonicity criterion is **satisfied**.

### 3. Condorcet Criterion

Condorcet criterion is **not applicable** since there is only 2 proposals in the election.

### 4. Irrelevant Alternatives Criterion

Irrelevant alternatives criterion is **not applicable** since there is only 2 proposals in the election.

## WeightedVoteCheckpoint.sol

### 1. Plurality Criterion

Plurality criterion is **satisfied**. As seen from the results function, the proposal with higher number of votes is the winner.

Text

Description automatically generated

### 2. Monotonicity Criterion

Monotonicity criterion is **satisfied**.

### 3. Condorcet Criterion

Condorcet criterion is **violated**. Explanation same as Ballot.sol.

### 4. Irrelevant Alternatives Criterion

Irrelevant alternatives criterion is **violated**. Explanation same as Ballot.sol.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Contract Name | Majority Criterion | Monotonicity Criterion | Condorcet Criterion | Irrelevant Alternatives Criterion |
| Ballot.sol | Satisfies | Satisfies | Violates | Violates |
| DemaxBallotFactory.sol | Satisfies | Satisfies | Satisfies / Not Applicable | Not Applicable |
| Gatekeeper.sol | Satisfies | Violates | Violates | Violates |
| ibaVoter.sol | Satisfies | Satisfies | Violates | Violates |
| localElection.sol |  |  |  |  |
| PLCRVotingCheckpoint.sol | Satisfies | Satisfies | Violates | Violates |
| Redenom.sol | Satisfies | Satisfies | Violates | Violates |
| TACVoting.sol | Satisfies | Satisfies | Violates | Violates |
| TomiQuery2.sol | Satisfies | Satisfies | Satisfies / Not Applicable | Not Applicable |
| WeightedVoteCheckpoint.sol | Satisfies | Satisfies | Violates | Violates |

Introduce voting smart contracts, workflow, how they create ballot and vote. Write more on the contracts, show complicated workflow, show steps

Ballot.sol Workflow

Text

Description automatically generated

Figure : Step 1

1. Create a list of proposal names that is to be included in the ballot. In the figure above, 3 proposal names are created: “A”, “B”, “C”. These proposals will be added into the ballot.



Figure : Step 2

2. Create a ballot with the proposal names previously created.

Text

Description automatically generated

Figure : Step 3

3. Since this smart contract allows batch voting, we can create arrays for the weights, voter names and their respective proposal ID that they wish to vote for. In the figure above, both Tom and Harry have a voting weight of 1. Harry intends to vote for the first proposal, “A”, and Tom is voting for the second proposal, “B”. The vote function will use these arrays to apply their individual votes.



Figure : Step 4

4. Once the ballot is over, the winner will be computed.

Text

Description automatically generated

Figure : Step 5

5. To reset and start a new ballot, create a list of new proposal names, and reset the ballot using these new names.