Hipo Audit Report

Impact levels

Low – issues that are unlikely to happen and/or affect any funds.
Informational – code style and similar.

Issues by severity

Low

Potentially inconsistent timestamp calculation

The `get_times` function in `treasury.fc` has some calculations that may become invalid if the network config undergoes significant changes – specifically, if `elections_start_before` ever differs from `elections_end_before` by less than 600 seconds. Code link
Suggested fix:
Check if `participate_since` is less than `next_round_since - elections_start_before`, if it does, then set it to that value, and set `participate_until` to some value between `participate_since` and `election_end`, for example, to their average.

Incorrect sort key calculation

In the `request_sort_key` function in `utils.fc` `loan_amount_round` has at most the lowest 80 bits set, `loan_amount_round_comp` is its negated counterpart, and therefore has all bits after the lowest 80 set to `1`, it is then added into the final sort key, affecting the fields that come further in the key. This may affect sorting order. Code link
Suggested fix:
Add `& ((1 << 80) - 1)` after loan_amount_round_comp in the final key calculation.

Missing late participation check

In the `participate_in_election` function in `treasury.fc` there is a check to prevent early participation, but there is no check to prevent late participation. This is not normally a problem, but it may become one in case the network is stopped, for example. Code link
Suggested fix:
Add a check to prevent participation on a round in which the protocol may no longer participate.

Missing sender checks

The `stake_coins` and `withdraw_tokens` functions in `wallet.fc` do not check their sender. Code link 1, Code link 2

Suggested fix:

Add a sender check – these actions should only be invoked by the user (or perhaps by the treasury through the text interface). If they are also meant to be invoked by the driver, then the driver must also be passed in the initial action and saved in the storage to be checked later.

Informational

Extraneous `impure` modifiers

Some functions in `utils.fc` do not need the `impure` modifier. Code link

Suggested fix:

Remove the extraneous modifiers.