Contest Proposal: SMV Smart Contract Informal Audit Respin

Short Description

The contestants shall provide the informal reaudit of the central SMV smart contracts (*Demiurge, Faucet, Padawan, Proposal*), hereinafter referred to as "smart contracts", where the detailed description of the "informal audit" is described below. All debot contracts are excluded from the present contest.

All the participants are highly encouraged to reuse the results of the initial audit, checking for fixes, omitting the unchanged areas so decreasing the efforts required to complete the contest.

Motivation

While this contract was already audited, the verdict was that many changes are required, too many to accept the modified version by a superficial review. So the preliminary decision to respin Phase 0 and Phase 1 was made at the ForMet Subgov weekly meeting.

The procedure is going according to the Charter Update #11 where the total budget for Phase 0 respin equals to 60% of the budget of the original audit .

Prerequisites

Before entering the informal audit process, each smart contract must comply with the following rules:
- The smart contract must be compilable with the latest version of *tondev* tool
- All smart contracts must be submitted with detailed documentation
- The smart contract's developers must set up a Telegram group for discussions as well as a slot for one-hour voice meetings at least once a week
- All the smart contracts being audited must be covered by unit and integration tests
- All the tests must pass

Location

The source code is available at https://github.com/RSquad/dens-smv at branch *master* with hash code equal to **fbdfe4bca3c372b02cacf9788b4ad37112d0da2c**.

Contest Terms

Contestants shall submit a document in PDF format that covers:
● All the errors found
● All the warnings found
● All the "bad code" (long functions, violation of abstraction levels, poor readability etc.) Foundings

Errors and warnings should be submitted to the developers as early as possible, during the contest, so that the code can be fixed immediately.

The document should also contain a high-level description of the code, and any information showing that the contest had a good understanding of the infrastructure and of the code.

Contest Dates

10 Aug 2021 - 17 Aug 2021

Proposed Prices

The total contest budget is **60 kTON**, whereby 95% are allocated to the contestant awards and 5% are allocated to the jury reward.

The contestant awards are distributed as follows:
- Place 1 - 30 kTON
- Place 2 - 18 kTON
- Place 3 - 9 kTON

The Jury

The Jury shall be formed from acknowledged experts in the fields of security, smart contract audit, and formal verification fields, whereby:

- Jurors whose team(s) intend to provide submissions in this contest shall lose their right to vote in this contest
- Each juror shall vote by rating each submission on a scale of 0 to 10 (0 equalling rejection of the proposal); a juror may abstain from voting if they do not see themselves sufficiently qualified to judge such proposal
- A juror that has voted on a submission shall provide detailed feedback on it

Jury Guidelines

- The main goal of the jury is to check how the provided audit is useful in terms of decreasing the bug risk for the contract being audited
- All the requirements mentioned above are considered as mandatory otherwise some points have to be taken from the corresponding application
- The usage of industry-adopted 3rd party tools should bring additional points in case the motivation of their usage has been clearly demonstrated
- Any team that managed to find a non-minor bug must be placed higher than a team that failed to do it
- Any bugs related to the kind of the exceptions as well those related to the logging or retrieving the state are considered as minor and should not be taken into account for the ranking

Jury Rewards

The total budget for jury rewards is 5% of the above-mentioned contest reward budget, or
3 kTON.

This amount shall be distributed between jurors who have voted **and** provided feedback on submissions.

The proportion of the total budget assigned to a juror shall be defined according to the extent of this juror's participation in the contest, i.e. the count of votes cast by this juror divided by the total votes cast count for this contest.

Procedural Limitations

- Only one submission per contestant shall be accepted. Multiple submissions, including but not limited to updated versions of the initial submission, are not allowed.
- Submissions shall be made within the time frame defined above in the **Contest Dates** section. Late submissions shall be rejected by the Jury.
- All submissions shall contain the contestant's contact information (preferably a Telegram ID) to ensure that the jury can match the submission to the specific contestant. If such contact information is missing, the submission shall be rejected.
- If the submission contains links to external material (reports on further work by the contestant), this material shall have the contestant's contact details (preferably a Telegram ID), to ensure that the jury can match the material to the specific contestant. If such contact information is missing, the submission shall be rejected.

Disclaimer

Anyone can participate, but Free TON cannot distribute tokens to US citizens or US entities.