TIP-3 Token Contract Verification (Phase 1)

Short Description

Initial documentation for TIP-3 Token contract formal verification.

Motivation

Contest should provide a set of specifications necessary in order to perform TIP-3 Token contract security audit and formal verification.

Term

Each participant should answer the following:

1. Describe Algorithm for high level code Analysis
2. Describe main contract business scenarios
3. Describe possible security issues (bugs, leading or not to attacks)
4. Describe possible attack vectors (what is attack: money loss/freezing, contract misbehaviour). Create a hierarchy for different issues (criticality, etc)
5. First level specification (on the top of main scenarios, informal)
6. Description of how contract acts
7. Description of what functions are to be called in the main flows
8. Interacting (if any) with other contracts
9. Decision of what "big" parts we'd like to axiomatize (other contracts, TVM etc)

The answers should be provided in the following form:

- Business-level specification written in the natural language
- Should be represented in a form of set of common sense logical statements

- Logical statements must be accompanied by diagrams and flowcharts (block diagrams)
- Role-action matrices must be included into the report (what roles exist in the contract and what actions are supposed by them)
- Table of possible attacks and malfunctions must be included into the report with severity or each attack or malfunction clearly indicated and prioritized (critical, major etc.)

Contracts Source Code:

There are three types of TIP-3 contracts currently available. Providing specifications for Fungible Token is a must, the rest is optional but will provide extra points.

https://github.com/tonlabs/ton-labs-contracts/tree/master/cpp

Contest Dates: 23 November 2020 — 07 December 2020

Proposed prices:

1 place — 50 000

2 place — 25 000

3 place — 10 000

Places 4 and 5 — 2 500 each

The jury:

Jury should be formed from known experts in the field of security, smart contract audit and formal verification fields only

Jury rewards:

An amount equal to 5% of all total tokens actually awarded and distributed will go to each juror for performing their civic duty to the community and taking the time to judge each submission and provide feedback.