Contest Proposal: Anonymous Token Design Contest Proposal

Submission period: May 7, 2021 00:01 UTC - June 30, 2021 at 23:59 UTC

Voting period: 20 days

Background and Description

Anonymous token protocol. Faster and cheaper alternative to ZCash. No need for the introduction.

Recent community discussion revealed there are several anonymous token protocol design considerations circulating around and no clear publicly audible design description is present. This means, before announcing the anonymous token protocol implementation contest, there is a need to determine the particular design to for the implementation and agree on it to avoid misunderstandings.

Instructions for participants

This contest supposes participants to design the anonymous token protocol using Groth16 proof verification mechanism or any other primitive.

General requirements

- Protocol design should address transactions involving "token" transactions (in terms of protocol application logic) to become theoretically untraceable.
- Formal description with provable statements (with formal proofs present, for sure).
- The design may involve Groth16 verification usage (technical specification may involve \`VERGRTH16\` TVM instruction usage).
- Technical specification is better to be compatible with TIP-3 token standard.

Evaluation criteria and winning conditions

- A participant should do a presentation of her solution at a convenient time agreed with DevEx members. A solution should include tests with clear instructions.
- In case a test does not cover some scenarios, then jurors can develop their own tests, but it should reduce such a submission score.
- The solution should be “safe” (no formal definition of safety is possible to be used in here). “Nothing up my sleeve” motto should be aligned to.
- Traditional paper-alike format should be preferred.
- Submissions should be compared based on efficiency (justified speed of proof generation and verification) and simplicity (for development).

Voting

- Jurors whose team(s) intend to participate in this contest by providing submissions lose their right to vote in this contest.
- A jury from other sub-governance groups could be added to this contest to provide additional technical expertise.
- Each juror will vote by rating each submission on a scale of 1 to 10.
- Jurors should provide feedback on each submission.
- The jury will reject duplicate, subpar, incomplete, or inappropriate submissions.

Reward

Only submissions with an average score equal to or more than 6.0 can get a reward.

1st prize	120 000 TONs
2nd prize	100 000 TONs
3rd prize	80 000 TONs
4th prize	50 000 TONs
5th prize	30 000 TONs
6th place	23,000 TONs
7th place	21,000 TONs
8th place	19,000 TONs
9th place	17,000 TONs
10th place	15,000 TONs

Note: In case the winning submissions amount is less than the number of rewards available, any remaining rewards are not subject to distribution and are considered void.

Jury rewards

An amount equal to 15% of all total tokens actually awarded will be distributed equally between all jurors who vote and provide feedback. Both voting and feedback are mandatory in order to collect the reward.

Governance rewards

An amount equal to 2 % of the prize fund will be allocated to members who participated in organizing the contest, to be distributed equally among them:

- @nemothenoone
- @prigolovko
- @Futurizt
- @anovi

Procedural remarks

- Participants must upload their work correctly so it can be viewed and accessible in the formats described. If work is inaccessible or does not fit the criteria described, the submission may be rejected by jurors.

- Participants must submit their work before the closing of the filing of applications. If not submitted on time, the submission will not count.
- Participants are free to ask/resolve any questions and propose any suggestions at the AMA event planned to be held no later than May 20, 2021. Exact timing will be agreed in DevEx Telegram chat-group.