Contest: Zero-Knowledge Voting Protocol Implementation

Contest dates: August 9, 2021 00:01 UTC - January 14, 2022 at 23:59 UTC

Voting period: 14 days

This is a proposal for the relaunch of the Zero-Knowledge Voting Protocol Implementation contest migrated from here: https://devex.gov.freeton.org/proposal?proposalAddress=0%3A22564170cd6e54121e89ff1338dd5ceca174530be2bd318c4521fefeebf8bb52

Background and Description

In January, 2021, a contest called Challenge MIT/Harvard paper on Blockchain Faults in Election Systems was held, which crowdsourced arguments to defend the position that secure blockchain based elections are possible. As a result, community arguments were summarized in a joint Free TON community paper, which was used by the GBA to foster a discussion with US election officials.

=nil; Foundation, as an initial member of the Free TON community developed an upgraded version of the TON Virtual Machine, which includes cryptographic primitives required for usage of zero-knowledge proof verification within virtualized applications. =nil; Foundation also prepared C++ (https://github.com/nilfoundation/cpp-ton) and Rust-y (https://github.com/nilfoundation/rust-ton) ZK proof verification instruction-enhanced TON protocol implementations.

Now Free TON has all of the required technologies to run a blockchain mass voting implementation contest.

Voting protocols inherently imply voter anonymity, but they should also support voter registration by authorities, so they usually get designed as Zero-Knowledge protocols (e.g. https://eprint.iacr.org/2017/585.pdf or https://eprint.iacr.org/2019/1270.pdf)

This document proposes the Zero-Knowledge voting protocol implementation contest on top of the newly introduced TVM Groth16 verification instruction.

Instructions for participants

Contestants are expected to create a voting protocol using the newly introduced `VERGRTH16` instruction and make it usable with the FreeTON protocol.

General requirements

- Must be a correctly functioning in-TVM virtualized application deployed either to https://net.ton.dev (https://net.ton.live) or to https://fld.ton.dev (https://fld.ton.live).

- Must contain a description of a participant's protocol with formal security proofs.
- Must Involve VERGRTH16 TVM instruction usage.
- Must ensure the bulletin maintains its integrity.
- Must ensure the ballot box is a non-malleable one.
- Must ensure that the ballot guarantees privacy of the voting message while also guaranteeing that the voter cannot reproduce their vote.
- Must allow the voter to verify the inclusion of their vote, and also ensure that others cannot coerce the voter to create a false ballot.
- The ballot must only be generated for eligible voters.
- Must ensure that voting results uniquely correspond to the ballots in the public board.
- Must ensure that ballots do not reveal voter identity to any entities, even authorities.
- Must ensure that ballots are unique to only the individual voting and there is no possibility for proxy votes.
- Must contain the following actor roles:
    - Voter.
    - Verifier.
    - Ballot Issuer.
- Must contain definitions for the following items:
    - Ballot. Required not to disclose the Voter's decision until the Ballot Issuer decides to.
    - Voter Registry. Proves a particular Voter is eligible to vote.
- Must contain a Ballot Issuer Voter registration procedure:
    - Voter generates some public identifier.
    - Voter submits the public identifier to the Ballot Issuer.
    - Ballot Issuer introduces the Voter's identifier to the Voter Registry.

Security requirements

- Fraudulent ballot generation complexity should be no less than EdDSA over Ed25519 brute force complexity (not an extremely formal requirement, but it is okay since the public voter identifier could be, for example, a EdDSA public key).
- Voting results disclosure should be not possible until the voting is ended.

Evaluation criteria and winning conditions

- Apart from uploading a submission, a code should be submitted in accordance with https://github.com/freeton-org/readme and deployed either to https://main.ton.dev (https://ton.live) or to https://fld.ton.dev (https://fld.ton.live).
- Each contestant should present their solution at a convenient time agreed upon in advance with Cryptography Sub-governance members. A solution should include tests with clear instructions.
- If a test does not cover some scenarios, then jurors can develop their own tests; however, if the burden falls on the jurors, the contest submissions scores should lose some points.
- The solution should have an open source license.

- The solution should contain at least a draft of the architecture description which is implied to contain following parts:
    - In-TVM part. Proof verification part. This part is supposed to be done with `VERGRTH16` instruction usage and executed within the TVM.
    - Native part. Circuit definition. Proof generator.

Instructions for jurors

Jurors must verify the correctness of the protocol submitted by each contestant to the test cluster as follows:

- To reproduce every use case scenario (voter registration, voting, vote count)
- To confirm the solution complies to the architecture description.
- To confirm the solution complies to protocol requirements.

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 6.00 can get a reward.

- 1st prize..... 600,000 TONs
- 2nd prize..... 300,000 TONs
- 3nd prize..... 100,000 TONs

Total prizes: 1,000,000 TONs

Note: If the number of winning submissions 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
- @anovi
- @nbering

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.
- Submission description document format. Submission description should be formatted as a PDF document to avoid post-deadline submission changes.
- Accessibility. All the submissions must be accessible for the Jury, so please double-check your submission. If the submission is inaccessible or does not fit the criteria described, jurors may reject the submission.
- Timing. Contestants must submit their work before the closing of the filing of applications. If not submitted on time, the submission will not count.
- Contact information. All submissions must contain the contestant's contact information, preferably a Telegram username by which jurors can verify that the submission belongs to the individual who submitted it. If not, jurors may reject your submission.
- Content. The content published in the forum and the provided PDF file should not differ, except for formatting. Otherwise, jurors may reject the submission.
- Well-formed links. If your submission has links to the work performed, the content of those links must have the contestant's contact details, preferably a Telegram username, so jurors can match it and verify whom the work belongs to. If not, jurors may reject your submission.

Adding Formal Verification Subgov team to the Jury members of contest

In addition to the regular Cryptography Subgov Jury Members, it is proposed to add the following

Formal Verification Subgov Initial Members to the contest jury list:

1. Sergey EGOROV @sergeyegorovspb
   67dd20b9a760ae538a7f24ebfbaaf09a7075b4617a7ad09c19503c2551f57d81
   0:d0e20274758acb651930c5b9b7dfda330583624f0e4d0b8ffc63bc287c69c5e3 *
2. Andrey LYASHIN @andruiman
   cec27f6cfdadadc5da135875d5988019bd8a760fe6e16fe1f49459cf6d18f9e7
   0:0a98551dd36a5dc65f4510362f3528dd195862a054aa70fcdd7ca8925a54ece4 *
3. Fabrice LE FESSANT @fabrice_dune
   4aca372ed9695ab42cc8ba7fd7f56d11c2401611c2d513bbc28beb5c7f4363a1
   0:24a44423bc7edc2598b50ae87267bd06bc53455328e837dae32b9b7592716de7 *
4. Thomas SIBUT-PINOTE @ThomasSibutPinote
   50384ec36bee19914526f436a0adf57d0c35389934b5aaca15db5b5e89f42aa0
   0:95d0f87463175d9cfeb5fd62df6699d56de1fdecb5d823cae21de84aaba3ed12 *
5. Evgeniy Shishkin @unboxedtype
   6ff61c1a7bb09795f7b5d5514dd710efb72e9557654d362ef208fde545ba7a33
   0:ef3813861e4717bc5b34bbdc13b3498ad2b0198100f87b9fa28cd080854c4ad8

Контест: Имплементация протокола голосования с использованием доказательств с нулевым разглашением.

Даты проведения: 9 Августа 2021 00:00 UTC - 7 Ноября 2021 23:59 UTC.

Период голосования: 15 дней.

Описание

В январе 2021 года был проведен конкурс под названием “Challenge MIT/Harvard paper on Blockchain Faults in Election Systems”, в котором собраны аргументы в защиту позиции, согласно которой безопасные выборы на основе блокчейна возможны. В результате аргументы сообщества были собраны в совместном документе сообщества Free TON, который был использован GBA для обсуждения с представителями избирательных комиссий США.

=nil; Foundation, будучи первоначальным членом сообщества Free TON, разработал обновленную версию виртуальной машины TON, которая включает криптографические примитивы, необходимые для использования проверки доказательства с нулевым разглашением в виртуализированных приложениях. =nil; Foundation также подготовил расширенную имплементацию протокола TON на C++ (https://github.com/nilfoundation/cpp-ton) и на Rust (https://github.com/nilfoundation/rust-ton).

Теперь Free TON имеет все необходимые технологии для проведения конкурса по внедрению массового голосования на блокчейне.

Протоколы голосования по своей сути подразумевают анонимность избирателя, но они также должны поддерживать регистрацию избирателей властями, поэтому они обычно разрабатываются как протоколы с нулевым разглашением (например, https://eprint.iacr.org/2017/585.pdf или https: // eprint.iacr.org/2019/1406.pdf).

В этом документе предлагается конкурс реализации протокола голосования с нулевым разглашением информации поверх недавно представленной инструкции проверки TVM Groth16.

Инструкции для участников

Ожидается, что участники конкурса создадут протокол голосования с использованием недавно представленной инструкции VERGRTH16 и сделают ее пригодной для использования с протоколом FreeTON.

Основные требования

Решение должно:

- Быть корректно функционирующим виртуализированным приложением FreeTON, развернутым либо на https://main.ton.dev (https://ton.live), либо на https://fld.ton.dev(https://fld.ton.live).
- Включать в себя формальное описание протокола, содержащее доказательства.
- Включать использование инструкции VERGRTH16 TVM.
- Обеспечивать валидность бюллетеня.
- Обеспечивать целостность урны для голосования.
- Гарантировать конфиденциальность голоса в бюллетене, а также гарантировать, что избиратель не сможет дублировать свой голос.
- Позволить избирателю проверить включение своего голоса, а также гарантировать, что другие не могут заставить избирателя создать фальшивый бюллетень.
- Бюллетень должен быть создан только для избирателей, имеющих право голоса.
- Гарантировать, что результаты голосования взаимно-однозначно соответствуют бюллетеням на общественной доске.
- Обеспечить, чтобы бюллетени не раскрывали личность избирателя никаким организациям, даже властям.
- Гарантировать, что бюллетени являются подходящими только для индивидуального голосования и нет возможности для голосования по доверенности.
- Содержать следующие роли:
    - Избиратель.
    - Верификатор.
    - Эмитент бюллетеней.
- Содержать определения для следующих элементов:
    - Бюллетень. Требуется не разглашать решение избирателя до тех пор, пока об этом не примет эмитент бюллетеней.
    - Реестр избирателей. Доказывает, что конкретный избиратель имеет право голоса.
- Содержать порядок регистрации избирателя, выдавшего бюллетень:
    - Избиратель генерирует некий публичный идентификатор.
    - Избиратель отправляет публичный идентификатор эмитенту Бюллетеней.
    - Эмитент бюллетеней вносит идентификатор избирателя в Реестр избирателей.

Требования безопасности

- Сложность создания поддельного бюллетеня должна быть не меньше, чем сложность перебора подписи EdDSA на Ed25519 (не очень формальное требование, но это нормально, поскольку публичный идентификатор избирателя может быть, например, открытым ключом EdDSA).
- Раскрытие результатов голосования не должно быть возможным до окончания голосования.

Критерии оценки и условия выигрыша

- Помимо загрузки заявки, код должен быть отправлен в соответствии с GitHub - freeton-org/readme и развернут либо на https://main.ton.dev (https://ton.live), либо на https://net.freeton.nil.foundation 1 (https://nil.ton.live или https://live.freeton.nil.foundation).
- Каждый участник должен представить свое решение в время, заранее согласованное с членами Cryptography SG. Решение должно включать тесты с четкими инструкциями.
- Если тест не охватывает некоторые сценарии, члены жюри могут разработать свои собственные тесты; однако, если бремя будет ложиться на жюри, результаты конкурсных работ должны потерять несколько баллов.
- Решение должно иметь лицензию с открытым исходным кодом.
- Решение должно содержать как минимум черновик описания архитектуры, которое, как предполагается, должно содержать следующие части:
    - Часть In-TVM. Часть проверки доказательства. Эта часть должна выполняться с использованием инструкции VERGRTH16 и выполняться внутри TVM.
    - Нативная часть. Определение схемы. Генератор доказательств.

Инструкции для судей

Члены жюри должны проверить правильность протокола, представленного каждым участником тестового кластера, следующим образом:

- Воспроизвести каждый сценарий использования (регистрация избирателей, голосование, подсчет голосов)
- Подтвердить соответствие решения описанию архитектуры.
- Подтвердить, что решение соответствует требованиям протокола.

Голосование

- Судьи, чьи команды намереваются участвовать в этом конкурсе, предоставляя материалы, теряют право голоса в этом конкурсе.

- К этому конкурсу может быть добавлено жюри из других саб-говернансов для предоставления дополнительной технической экспертизы.
- Каждый член жюри будет голосовать, оценивая каждую заявку по шкале от 1 до 10.
- Члены жюри должны давать отзывы по каждому представлению.
- Жюри отклонит дублирующиеся, некачественные, неполные или несоответствующие материалы.

Вознаграждение

Только заявки со средним баллом, большим или равным 6,00, могут получить награду.

1 место ..... 600 000 TON
2 место ..... 300 000 TON
3 место ..... 100 000 TON

Всего призов: 1’000’000 TON

Примечание: если количество выигравших заявок меньше количества доступных наград, любые оставшиеся награды не подлежат распределению и считаются недействительными.

Награды жюри

Сумма, равная 15% от всех фактически присужденных токенов, будет равномерно распределена между всеми членами жюри, которые голосуют и предоставляют отзывы. Как голосование, так и обратная связь являются обязательными для получения награды.

Награды за подготовку контеста

Сумма, равная 2% от призового фонда, будет выделена участникам, участвовавшим в организации конкурса, и равно распределена между ними:

@nemothenoone

@prigolovko

@anovi

@nbering

Процедурные замечания

- Участники должны правильно загружать свои работы, чтобы их можно было просматривать и использовать в описанных форматах. Если работа недоступна или не соответствует описанным критериям, работа может быть отклонена членами жюри.
- Участники должны представить свои работы до закрытия приема заявок. Если решение не подано вовремя, отправка не засчитывается.
- Формат документа с описанием решения. Описание решения должно быть отформатировано как документ PDF, чтобы избежать изменений после крайнего срока подачи.
- Доступность. Все работы должны быть доступны жюри, поэтому, пожалуйста, проверьте их еще раз. Если представление недоступно или не соответствует описанным критериям, члены жюри могут отклонить его.
- Время. Конкурсанты должны представить свои работы до окончания приема заявок. Если не подано вовремя, отправка не засчитывается.
- Контакты. Все материалы должны содержать контактную информацию участника.
- Содержание. Контент, опубликованный на форуме, и предоставленный PDF-файл не должны отличаться, за исключением форматирования. В противном случае члены жюри могут отклонить заявку.
- Корректные ссылки. Если в заявке есть ссылки на выполненную работу, содержание этих ссылок должно иметь контактные данные участника, желательно имя пользователя Telegram, чтобы члены жюри могли сопоставить его и проверить, кому принадлежит работа. В противном случае члены жюри могут отклонить вашу заявку.