6th Workshop on Trusted Smart Contracts

In Association with Financial Cryptography 2022

May 6, 2022

Title: Dispute-free Scalable Open Vote Network using zk-SNARKs

Authors: Muhammad Elsheikh and Amr M. Youssef.

Abstract

The Open Vote Network is a self-tallying decentralized e-voting protocol suitable for boardroom elections. Currently, it has two implementations as Ethereum smart contracts: the first has a scalability issue since all the computations have been performed on-chain. This issue was solved partially in the second implementation by assigning a part of the heavy computations to an off-chain untrusted administrator in a verifiable manner. As a side effect, this implementation became not dispute-free; there is a need for a tally dispute phase where an observer interrupts the protocol when the administrator cheats the tally result. In this work, we propose a new smart contract design to tackle the problems in the previous implementations by (i) performing all the heavy computations off-chain hence achieving higher scalability, and (ii) utilizing zero-knowledge Succinct Non-interactive Argument of Knowledge (zk-SNARKs) to verify the correctness of the off-chain computations, hence maintaining the dispute-free property. To demonstrate the effectiveness of our design, we develop a prototype and conduct multiple experiments for different numbers of voters.