6th Workshop on Trusted Smart Contracts

In Association with Financial Cryptography 2022

May 6, 2022

Title: Fides: A System for Verifiable Computation Using Smart Contracts

Authors: Mahmudun Nabi, Sepideh Avizheh, and Reihaneh Safavi-Naini.

Abstract

Verifiable computation allows a resource-constrained client to outsource their computation to powerful servers, and efficiently verify their received results. Cryptographic verifiable computation systems, despite their elegant designs, have limited application in practice because of the computational cost and difficulty of correct and flexible implementation of complex cryptographic systems. An attractive approach to verifiably compute general functions is to use more than one server to compute the same function, and decide the computation result based on the submitted results of all servers. In this paper, we propose a system for delegation of computation to two cloud servers using a smart contract (SC), that guarantees correct computation results as long as at least one of the two servers is honest. Our work adapts the Refereed Delegation of Computation (RDoC) model of Canetti, Riva and Rothblum (ACM CCS'11) to the SC setting. This was first considered by Avizheh et al. (ACM CCSW'19) who showed that the direct employment of RDoC in the smart contract setting will be insecure because of the copy attack, where a server copies the result of the other server, and becomes possible due to the transparency of SC. However, the implementation of their protocol was left as future work. Our work is a new SC-aided RDoC design with proved security that significantly reduces the computation of the smart contract. Additionally, it provides security against the misbehaviours of the client and an implementation of the design over the Ethereum blockchain. The proposed system, which is called Fides, is the first implementation of SC-aided RDoC. We discuss the challenges of this implementation and our design decisions, and present the cost analysis of the system for an example computation. We also propose extensions of our work and directions for future research.