6th Workshop on Trusted Smart Contracts

In Association with Financial Cryptography 2022

May 6, 2022

Title: Protocol-based smart contract generation

Authors: Afonso Falcão, Andreia Mordido, and Vasco T. Vasconcelos.

Abstract

The popularity of smart contracts is on the rise, yet breaches in reliability and security linger. Among the many facets of smart contract reliability, we concentrate on faults rooted in out-of-order interactions with contract endpoints. We propose SmartScribble, a protocol language to describe valid patterns of interaction between users and endpoints. SmartScribble not only ensures correct interactive behaviour but also simplifies smart contract coding. From a protocol description, our compiler generates a smart contract that can then be completed by the programmer with the relevant business logic. The generated contracts rely on finite state machines to control endpoint invocations. As a proof of concept, we target Plutus, the contract programming language for the Cardano blockchain. Preliminary evaluation points to a 75% decrease in the size of the code that developers must write, coupled with an increase of reliability by enforcing the specified patterns of interaction.