Short-Term Scientific Mission Grant
- APPLICATION FORM[1] -

Action number: CA20111

Applicant name: Prof. Emilio Tuosto

Details of the STSM

Title: Behavioural Types for Smart Contracts

Start and end date: 14/07/2022 to 22/07/2022

Goals of the STSM

Purpose and summary of the STSM.

(max.200 word)

The applicant will combine his experties on (asserted) choreography automata with the one of Prof. Ravara on type-state programming in order to start the development of a behavioural types framework for the static analysis of smart contracts. The main goals are

(i) to identify suitable sufficient condition to statically ensure the correctness of smart contracts

(ii) to automatically infer conditions from actual contracts that can be used to guarantee correctness through reachability analysis.

We will also explore the possibility of developing tools providing 'push-button' solution for the verification of smart contract based on behavioural type checking. The goal is to extend prototype tools supporting the behavioural type framework.

Working Plan

Description of the work to be carried out by the applicant.

(max.500 word)

Smart contracts are used to establish agreements among distributed and mutually distrusted parties without the mediation of (trusted) intermediaries. Essentially, smart contracts are distributed protocols that exchange information in order to establish global consensus on e.g., financial transactions, or transfer of assets.

Despite various claims about the robustness of smart contracts, weaknesses have emerged in some of the most popular platforms executing those contracts. For instance, vulnerabilities such as reentrancy

[1] This form is part of the application for a grant to visit a host organisation located in a different country than the country of affiliation. It is submitted to the COST Action MC via-e-COST. The Grant Awarding Coordinator coordinates the evaluation on behalf of the Action MC and informs the Grant Holder of the result of the evaluation for issuing the Grant Letter.

and mishandled exceptions have been exploited in the DAO attack or bugs in some libraries lead to an attack to Ethereum “freezing” about 160 million USD.

This STSM aims to develop static analysis techniques for smart contracts. Our investigation will hinge on behavioural types and reltated techniques. More precisely we will explore the use of global type systems as specifications of “correct” smart contracts in the vein of the tradition of of behavioural types. More precisely, behavioural type systems have so far proved themselves rather suitable in guaranteeing various soundness and liveness properties of message-passing systems (e.g., deadlock freedom, progress, session fidelity). Also, behavioural types have been advocated as a suitable formal approach to type-state programming since they can statically enforce expected usages of programming interfaces. Both these (complementary) features are key for the the static analysis of smart contracts. For instance, an Ethereum smart contract can be envisaged as a list of functions enabling the transfer of resources (‘ether’ in the Ethereum’s jargon) from one contract to another. Unintended invocations of such functions may lead to unexpected transactions or, in the worst case, to fraudulent executions that damage honest participants or corrept the global state of the system.

The plan of the STSM is to lay down a behavioural type framework that allows to statically guarantee properties of smart contracts. This will be attained by identifying suitable well-formedness conditions of global types that guarantee the correctness smart contracts that can be typed against the projections of the global specification. A promising direction is the use of choreography automata, a recently proposed class of global types. These models seems suitable for two reasons. Firstly, they are close to informal practices whereby developers design smart contracts in terms of state machines; this will facilitate the adoption of the models. Secondly, choreography automata have been extended with assertion methods that appear to be necessary to formalise relevant properties of smart contracts such as liquidity. The collaboration will also consider how to combine the tools developed by the groups of Prof. Ravara and of the applicant in a toolchain featuring ‘push-button’ solution for the static analysis of smart contracts.

Expected outputs and contribution to the Action MoU objectives and deliverables.

Main expected results and their contribution to the progress towards the Action objectives (either research coordination and/or capacity building objectives) and deliverables.

(max.500 words)

The outputs of this STSM will mainly contribute towards the aims of WG3.

An immediate output of the visit will be the identifications of strengths and weaknesses of (asserted) choreography automata as a formal model of global specifications of smart contracts and their relation to the behavioural typestate systems developed in Lisbon. The STSM will trigger the the possibility of further outputs in the long run. We expect to develop approaches for the static analysis of smart contract and to render them into tool-supported ‘push-button’ solutions. More specifically, we will explore the possibility of chaining tools such as the Java typestate checker (https://github.com/jdmota/java-typestate-checker) developed in Lisbon and the ChorGram tool chain developed in L’Aquila (https://bitbucket.org/eMgssi/stable_chorgram/wiki/Home) to support choreography automata.

Eventually, this exploratory investigation should be transferred to a tool supported solution for Solidity (the language of Ethereum smart contracts) in the spirit of what done by the group of Prof. Ravara for Java (https://github.com/RonaldoCorte/SmartContracts).