Report on the outcomes of a Short-Term Scientific Mission[1]

Action number: CA20111

Grantee name: Emilio Tuosto

[1] This report is submitted by the grantee to the Action MC for approval and for claiming payment of the awarded grant. The Grant Awarding Coordinator coordinates the evaluation of this report on behalf of the Action MC and instructs the GH for payment of the Grant.

Details of the STSM

Title: Behavioural Types for Smart ContractsS

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

Description of the work carried out during the STSM

Description of the activities carried out during the STSM. Any deviations from the initial working plan shall also be described in this section.

(max. 500 words)

The STSM started, as planned, by analysing how suitable existing behavioural type systems are for the analysis of smart contracts. This feasibility analysis was conducted by considering smart contracts taken from a public repository. The analysis determined some weaknesses in state of the art type systems due to several factors. Firstly, restrictions are usually imposed on the number of instances of components involved in the contracts; the analysis of smart constracts requires to abstract away from the number of instances. Secondly, most of the typing systems do not support data flow analysis which seems to be crucial for the analysis of properties of smart contracts like liquidity. Finally, basically all existing typing systems assume a point-to-point communication mechanisms while smart contract rely on a sort of method invocation mechanism to represent interactions of participants; although in principle one could consider to represent method invocation in terms of point-to-point communications, our preliminary analysis suggests that behavioural types based on method invocation would be desirable.

The outcome of our analysis led us to sketch specific behavioural types for smart contracts. A key design factor is to have roles fully abstract away from the number of instances. As a first attempt, we considered the analysis of a basic property of smart contract: the correct use of the 'revert' feature. In many of the examples taken from the public repository, we noticed that sometimes contracts do not correctly 'revert' on method invocations that do not meet the expected preconditions. This kind of errors may lead to serious attacts to the contracts (indeed liquidity can be spoiled if contracts do not correctly revert); interestingly, static analysis can flag such errors. We therefore skected a first simple typing discipline to control the use of 'revert'. We identified a first typing discipline that abstracts from payloads and can be used to type check 'control-flow' conditions for 'revert'. Both this typing disciplines, as planned, can be concretised as variants of choreography automata. In particular, an adaptation of asserted constraint automata will lay out the ground for the static analysis of usage of 'revert', and later for liquidity.

We also investigated extensions to represent data-flow conditions, but this requires more work.

The final part of the mission was dedicated to the exploration of tool development. A starting point will be to transfer the java typestate checker developed in Lisbon to languages to program smart contracts. In particular, we will consider solidity.

Description of the STSM main achievements and planned follow-up activities

Description and assessment of whether the STSM achieved its planned goals and expected outcomes, including specific contribution to Action objective and deliverables, or publications resulting from the STSM. Agreed plans for future follow-up collaborations shall also be described in this section.

(max. 500 words)

Most of the goals of the mission were achieved. The STSM was useful to spell out the requirements for

a typing discipling of solidity-like smart contracts so to apply our theory to Ethereum's smart contracts. In particular, one of the outcomea of the visit is a variant of choregraphy automata for the analysis of the usage of 'revert' in smart contracts. A particularly promising route is the adaptation of this variant to asserted choreography automata for the static analysis of properties such as liquidity. The identification of well-formedness conditions is however just started and will require more work.

The preliminary results of this STSM are quite encouraging. We have just started to work on the topics amd it is foreseable that initial results on this topics will be submitted for publication by the beginning of next year. The collaboration between Prof. Ravara and Prof. Tuosto will continue. Soon Prof. Ravara will visit Prof. Tuosto in Italy together with one of the developers that are adapting the java typestate checker to smart contracts in order to continue the research planned in this STSM. In the forthcoming visit we will study the well-formedness conditions on the variant of asserted choreography automata defined in this STSM. Also, we will start the adaptation of the java typestate checker for the analysis of solidity smart contracts.

This initial results are paving the way for a larger research project. To develop this project we will use some funds that the GSSI, the institute of Prof. Tuosto, has allocated to sponsor a PhD scholarhip for the Italian National School on Blockchain. The initial results of this STSM are spot on for the topics of the scholarship. Also, the activities of the STSM attracted the interest of Dr. Maurizio Murgia, a researcher at GSSI, who is an expert on smart contracts. This paves the way for collaborations with other groups. More precisely, we believe that we can collaborate with Prof. Massimo Bartoletti in Cagliari and Prof. Roberto Zunino in Trento who are active on the formal analysis of smart contracts and have co-authored papers on this topic with Dr. Murgia (and papers on behavioural types with Prof. Tuosto).