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

Action number: CA20111

Applicant name: Elvis Gerardin KONJOH SELABI

Details of the STSM

Title: Model-Checking Smart Contracts

Start and end date: 14/04/2025 to 25/04/2025

Detail of the cost in EUROS: € 2496.00

As reference, you can use the daily allowances by country for ITCGs (https://europroofnet.github.io/itcg-daily-allowance/) and the associated Excel sheet (https://europroofnet.github.io/_pages/grant.xlsx).

- Transport (upload screen capture): € 299

- Hotel/day (upload screen capture): € 2197

- Food/day:

TOTAL: € 2496.00

Goals of the STSM

Purpose and summary of the STSM.

Smart contracts have become a critical component of blockchain technology, enabling secure, self-executing agreements between distributed parties without the need for intermediaries. However, vulnerabilities in smart contract implementations, such as the reentrancy attack in the DAO hack or bugs in Ethereum libraries, highlight the importance of formal verification to ensure the correctness and reliability of these contracts.

This Short-Term Scientific Mission (STSM) will explore the application of the data-aware Petri-nets (DPNs) and the corresponding tools developed at DTU to verify a coordination model for smart contracts based on behavioral types (https://link.springer.com/chapter/10.1007/978-3-031-62697-5_13) developed by the applicant.

The primary goal is to apply model-checking techniques for the formal verification of smart contracts. More precisely, we aim to combine formal verification techniques to behavioural type models of smart contracts in order long-term goal to improve their reliability and increase their trustworthiness. The STSM will move the first steps towards the integration of the different models and methodologies.

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.

Working Plan

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

During the STSM we will explore how DPNs can be used to model-check smart contracts modelled as Data-Aware Finite State Machine (DAFSM). In particular, the STSM will trigger the study of whether DPNs can effectively check properties of DAFSMs.

We will start by evaluating the suitability of DPNs for model checking DAFSMs. This will be done by manually modelling simple examples and testing them with the existing tool. This will initiate the analyses of the expressiveness of DPNs with respect relevant properties of smart contracts and identify possible limitations in applying the tool to these models.

Next we will explore the process of converting a DAFSM into a DPNs. Specifically, we will analyse whether semantic-preserving encodings of DAFSM into DPNs as well as how general properties of our behavioral type can be expressed in the DPNs logics. In the STSM we will identify realistic smart contract to model and verify. We will formalise key questions such as What properties should the encoding have? (e.g., modularity?, compositionality?, etc.) Are the encoding effective? (e.g., is the size of encoded DAFSM tractable?)

Finally, we will establish the requirements necessary for the interoperability of the tools developed at DTU and the one developed by the applicant.

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

Main expected results and their contribution to the progress towards the Action objectives (https://europroofnet.github.io/objectives/) and deliverables (https://europroofnet.github.io/deliverables/).

Working groups to which this mission contributes:

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

An immediate output of this visit will be the identification of the strengths and weaknesses of possible encodings. And a set of benchmarks for assessing both the expressiveness and the feasibility of the approach. The analysis will determine the potential of the model-checking approach supported by DPNs for the verification of smart contracts. This will pave the way to the development of formal verification methods for smart contracts, applying model-checking techniques to ensure correctness in blockchain applications.

In the medium term, this research could lead to the formal modelling and analysis of real smart contracts. We expect to integrate the tools and perform an initial experimental evaluation within six months from the STMS. Moreover, on a long-term scale, we expect to develop a framework allowing us to perform statistical model checking of smart contracts that would allow us to perform quantitative analysis of smart contracts.