MSc project proposal

Formally Understanding Blockchain by Reverse Engineering

Candidate: DIOGO JOÃO SILVA DE ARAÚJO
Supervisor: JOSÉ NUNO OLIVEIRA [1]

Master in Computer Engineering (MEI)
University of Minho, Braga, Portugal
2022/23

Motivation

Blockchains are decentralized transactional ledgers that rely on cryptographic hash functions for guaranteeing the integrity of the stored data. Participants on the network reach agreement on what valid transactions are through consensus algorithms.

Blockchains may also provide support for Smart Contracts. Smart Contracts are scripts of an ad-hoc programming language that are stored in the blockchain and that run on the network. They can interact with the ledger's data and update its state. These scripts can express the logic of possibly complex contracts between users of the blockchain. Thus, Smart Contracts can facilitate the economic activity of blockchain participants.

With the emergence and increasing popularity of cryptocurrencies such as Bitcoin and Ethereum, it is now of utmost importance to have strong guarantees of the behaviour of blockchain so ware. These guarantees can be brought by using Formal Methods. Indeed, Blockchain software encompasses many topics of computer science where using Formal Methods techniques and tools is relevant: consensus algorithms to ensure the liveness and the security of the data on the chain, programming languages specifically designed to write smart contracts, cryptographic protocols, such as zero-knowledge proofs, used to ensure privacy, etc.

xxxxx

Meanwhile, the same principle was explored in a more accessible way that does not require such technical knowledge [3]. However, such experiments did not go beyond the exploratory phase.

[1] HASLab/ U.Minho & INESC TEC.

Goals

The aim of this dissertation is to start from .....

This work can be framed in the broad discipline of formal methods applied to software design, stepping up the paradigm of deriving correct-by-construction programs from logic specifications.

Research plan

The theoretical background of the proposed work requires familiarity with [2, 6, 4], whose study in depth is part of the overall research plan, structured in four main steps:

Background and state of the art – The first months will be devoted to the study of the state of the art and technical background related to the project, including previous work in the same application domain [3].

Writing the PDR report – The outcome of the previous step will be embodied in the pre-dissertation report (PDR) that will delimit and characterise the problem to be addressed in the future master's dissertation.

Contribution – Main body of research evolving towards the main aim of the project: the design of a software development strategy from specifications that follow the GC pattern, leading to correct-by-construction artifacts, with possible automation using the Galculator tool — which will need to be refactored from its legacy state [3].

Writing up - Incorporating all final results and suggestions for future work in the master's dissertation.

Deliverables

This project is expected to deliver, besides the PDR report and the dissertation itself:

- an InfoBlender talk;
- a conference paper.

Planned schedule

Task	Oct	Nov	Dez	Jan	Fev	Mar	Apr	May	Jun	Jul
Background and SOA	●	●	●							
PDR preparation		●	●	●						
Contribution				●	●	●	●	●	●	
Writing up							●	●	●	●

References

1. P.F. Silva and J.N. Oliveira. 'Galculator': functional prototype of a Galois-connection based proof assistant. In *PPDP '08: 10th int. ACM SIGPLAN conf. on Principles and practice of declarative programming*, pages 44–55. ACM, 2008. .

2. R. Bird and O. de Moor. *Algebra of Programming*. Series in Computer Science. Prentice-Hall, 1997.

3. R.C. Backhouse. *Mathematics of Program Construction*. Univ. of Nottingham, 2004. Draft of book in preparation, available from the author's website. 608 pages.

4. J.N. Oliveira. Biproducts of Galois connections, 2020. Contributed talk to the IFIP WG 2.1 Meeting #79, Otterlo (NL), January 2020.

Date: October 9, 2022

Student: _____

Supervisor: _____