MSc project proposal

Formalizing Blockchain — the Calculation Way

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

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

Motivation

With the advent and increasing popularity of cryptocurrencies it is of utmost importance to have strong behaviour guarantees of the blockchain software they rely upon.

Ensuring correct behavior can be brought by using formal methods (FM) and, indeed, there is a series of workshops devoted to formal methods applied to blockchain software.[2] Particular techniques such as theorem proving and formal semantics have been successfully applied to blockchain, for instance.

However, there seems to be no reported experience in using calculational proofs, namely the algebra of programming [1, 2], in this domain. The main aim of this project is to challenge such algebraic methods in the blockchain arena and to see how they compare to the other formal approaches.

Goals

Blockchains are decentralized transactional ledgers that rely on cryptographic hash functions for guaranteeing the integrity of stored data. Agreement on what valid transactions are is achieved through consensus algorithms. Blockchains also support so-called smart contracts that are stored in the blockchain and run on the network by interacting with the ledger's data and updating its state.

Formal methods for blockchain (FMBC) is a relatively new research subject. The first FMBC workshop took place in October 2019, as part of the 3rd World Congress in Formal Methods [3]. This inaugurated a series of events which aim at ensuring safety and quality in blockchain technologies by use of formal method techniques. (See footnote 2.) These have included theorem proving

[1] HASLab/ U.Minho & INESC TEC.
[2] Namely: FMBC'19, FMBC'20, FMBC'21 and FMBC'22.

over formal semantics definition (e.g. [4]) but not calculational proofs advocated by the algebra of programming (e.g. [1]) and supported by model-checking (e.g. as in [5], a piece of work similar to what is intended in this project). On the oher hand, preliminary exercises carried out as lab assignments in the context of [2] have shown that blockchain components such as e.g. Merkle trees [6] can be tackled rather easily and effectively in that way.

The main aim of this dissertation is to start from such exercises and, by inspecting hackage libraries such as haskoin and blockchain, trying to identify generic patterns that arise in such libraries that can be identified and delivered as *certified components* for blockchain software.

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 [1, 2], 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.

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: analysis and reverse specification of blockchain software, trying to identify generic patterns that arise in such libraries and can be identified and delivered as *certified components* for blockchain software construction.

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:

- a presentation of the work in the InfoBlender talk-series of HASLab;
- 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. R. Bird and O. de Moor. *Algebra of Programming*. Series in Computer Science. Prentice-Hall, 1997.

2. J.N. Oliveira. Program Design by Calculation, 2019. Draft of textbook in preparation, current version: October 2019. Informatics Department, University of Minho (PDF).

3. E. Sekerinski and N. Moreira *et al*, editors. *Formal Methods. FM 2019 International Workshops - Porto, Portugal, October 7-11, 2019, Revised Selected Papers, Part I*, volume 12232 of *Lecture Notes in Computer Science*. Springer, 2020.

4. M.J. Gabbay, A. Jakobsson, and K. Sojakova. Money grows on (proof-)trees: The formal FA1.2 ledger standard. In B. Bernardo and D. Marmsoler, editors, *3rd Int. Workshop on FMBC (FMBC@CAV 2021)*, volume 95 of *OASIcs*, pages 2:1–2:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.

5. J.N. Oliveira and M.A. Ferreira. Alloy meets the algebra of programming: A case study. *IEEE Trans. Soft. Eng.*, 39(3):305–326, 2013. .

6. R.C. Merkle. A digital signature based on a conventional encryption function. In Carl Pomerance, editor, *Advances in Cryptology - CRYPTO '87, Proceedings*, volume 293 of *LNCS*, pages 369–378. Springer, 1987.

Date: October 14, 2022

Student: _____

Assinado por: **JOSÉ NUNO FONSECA DE OLIVEIRA**
Num. de Identificação: 03283612
Data: 2022.10.14 17:37:41 +0100

Supervisor: _____

Degree Director: _____