

MSc project proposal

Formalizing Blockchain — the Calculation Way

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

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

Motivation

With the advent and increasing popularity of cryptocurrencies such as Bitcoin and Ethereum, 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.

However, there seems to be no reported experience in using calculational proofs, namely the algebra of programming [1, 2]. The main aim of this project is to challenge such algebraic methods in the blockchain domain 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.

The first workshop on formal methods for blockchain took place in October 2019, as part of the 3rd World Congress in Formal Methods (FM'19). This inaugurated a series of events which aim at ensuring safety and quality in blockchain technologies by use of formal methods techniques. (See footnote 2.)

¹HASLab/ U.Minho & INESC TEC.

² Namely: FMBC'19, FMBC'20, FMBC'21 and FMBC'22.

These have included theorem proving and formal semantics definition but not calculational proofs advocated by the algebra of programming. On the other hand, very simple exercises carried out in lab assignments in the Algebra of Programming course at U. Minho have shown that blockchain components such as e.g. Merkle trees 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 package libraries such as `haskoin` and `blockchain`, trying to identify generic patterns that arise in such libraries and can be identified as *certified components* of 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 as delivered as *certified components* of blockchain software.

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).

Date: October 12, 2022

Student: _____

Supervisor: _____