

## SMARTSCRIBBLE: SAFER SMART CONTRACTS



Speaker

**Afonso Falcão**

Affiliation

**LASIGE, DI-FCUL**

When

**June 22, 14h00**

Where

**Zoom**

### Abstract

Blockchain is considered one of the technologies of the future. Over the last years, a myriad of blockchain-based solutions has been discovered and implemented. At the centre of this revolution are smart contracts, scripts deployed on the blockchain that automatically execute procedures that usually involve assets. Unfortunately, several well-known attacks exploited vulnerabilities in smart contracts leading to huge monetary losses.

In this talk, I will present SmartScribble: a programming language for the specification of protocols for smart contracts. Protocols in SmartScribble describe valid patterns of interaction between user and endpoints. From a protocol specification, our compiler automatically generates a smart contract, to which the developer can add relevant business logic. SmartScribble relies on finite state machines to control endpoint invocation. As a proof-of-concept, we target Plutus, the contract programming language for the Cardano Blockchain. Preliminary evaluation points to a 75% decrease in the amount of code that developers write coupled with increased reliability of the contracts.

### Bio

I am an MSc student at FCUL working at LASIGE research unit. I have also completed my BSc in Informatics Engineering in FCUL.

Over the last year, I have been mainly focused on studying blockchain and smart contracts programming languages - the subject of my master thesis. I have also worked on other projects such as Waste2Block (a blockchain-based solution for waste management) and non-blockchain projects such as AlarmBot ([https://github.com/LendaDeAfonselio/Alarm\\_Bot](https://github.com/LendaDeAfonselio/Alarm_Bot))