
Remo Pfister

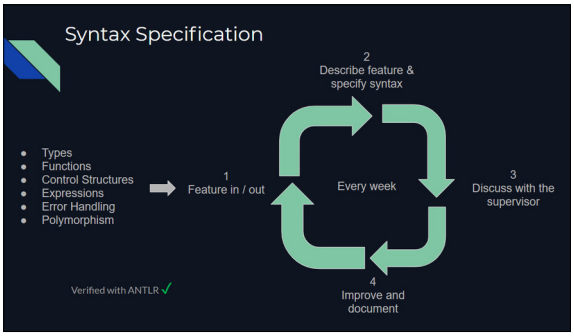

Keerthikan THURAIRATNAM

Students	Remo Pfister, Keerthikan THURAIRATNAM
Examiner	Prof. Dr. Thomas Bocek
Subject Area	Software Engineering - Core Systems

Lazo: Smart Contract Language for Bazo Blockchain

Language Design and Specification

Bazo Logo



Procedure

Introduction: The study work focuses on designing a smart contract language (named "Lazo") for the Bazo blockchain. The Bazo blockchain is a research blockchain to test different mechanisms and algorithms. In the current version, a Proof of Stake consensus algorithm and a virtual machine to execute Bazo intermediate language (opcodes) are integrated. However, writing smart contracts in Bazo opcodes is time consuming and error-prone. The goal of this study work is to design a high-level language which is easier to read and write smart contracts.

Procedure / Result: Before designing Lazo, 24 existing smart contract languages are collected and roughly analyzed to identify the key characteristics of a language for the blockchain. Thereafter, three popular and well elaborated languages, namely Solidity, Vyper and Scilla, were analyzed in great detail. Their supported features, syntax and contract examples were also documented. With the acquired knowledge about smart contracts, Lazo language was designed in an agile manner.

Result: As a result, Lazo is designed to be a statically typed, imperative and non-turing complete programming language. All language features are documented with illustrative code snippets. The Lazo grammar is also written in ANTLR and verified with Java. Furthermore, contract examples from Solidity are translated to Lazo in order to prove that the real-world use cases can be programmed with Lazo as well.

In a follow-up thesis, a compiler could be developed to compile Lazo programs into Bazo virtual machine instructions.

```
1  version 1.0
2
3  contract SimpleContract{
4      Map<address, int> payments
5
6      [Payable]
7      [Pre: msg.coins > 0]
8      function void pay() {
9          payments[msg.sender] += msg.coins
10     }
11 }
```

Contract Example in Lazo