Ennio Meier

Marco Steiner

Graduate Candidates	Ennio Meier, Marco Steiner
Examiner	Prof. Dr Thomas Bocek
Co-Examiner	Sven Stucki, Procivis AG, Zürich, ZH
Subject Area	Software Engineering - Core Systems

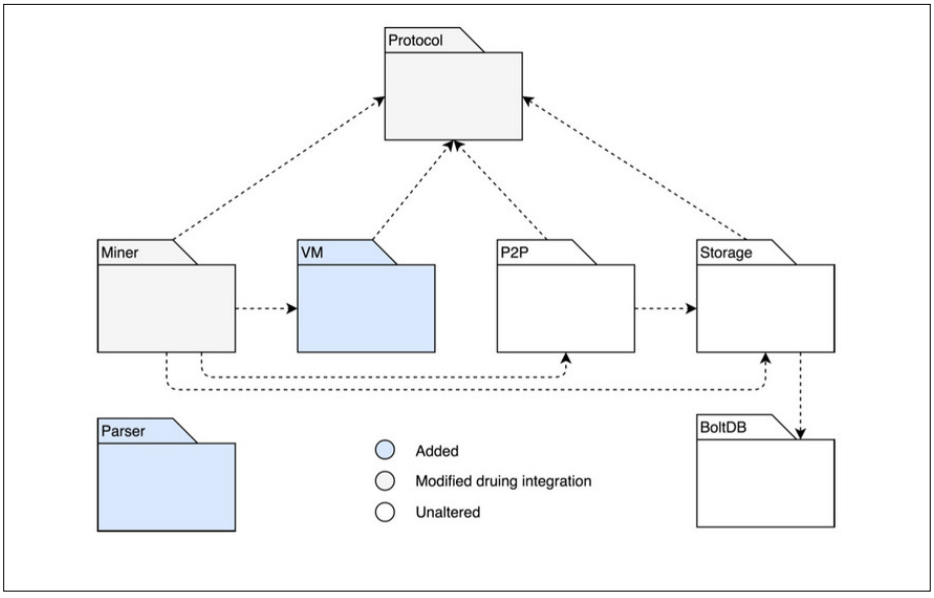
Integrating Smart Contracts into the Bazo Blockchain

Building the foundation for decentralized applications

Bazo Blockchain logo

```
1  # This is a simple program which calls a function
2  PUSH 55780
3  PUSH 5
4  CALL addNums 2
5  HALT # stops execution
6
7  addNums:
8  LOAD 0
9  LOAD 1
10 ADD
11 RET
```

Basic contract with function call written in «Enhanced Bazo Byte Code»



UML Package Diagram

Introduction: This thesis focuses on the integration of smart contracts into the Bazo Blockchain with the goal of creating a platform for decentralized applications. Smart contracts are programs that are stored on a blockchain and can be triggered by transactions. Smart contracts offer opportunities in automation and bring along advantages provided by blockchains such as immutability, public visibility of transactions and decentralization. As blockchains are trust-less protocols, it is guaranteed that smart contracts are executed as intended.

Solution: The integration of smart contracts was solved by implementing a virtual machine that executes the instructions sent by a transaction. This stack based virtual machine uses byte arrays as base type, which enables the virtual machine to deal with numbers of arbitrary length. Working with elements of arbitrary size requires taking the length of the elements into account, when calculating the gas cost, in addition to the base cost of the instruction type. Furthermore, the virtual machine was embedded within the mining application, which required to alter the blockchain protocol and the mining application.

Result: As a result, smart contracts can be deployed and transactions that call functions of smart contracts can be executed. Calling a smart contract function leads to the execution of the contract in the virtual machine and persisting the result in the blockchain. The Bazo Blockchain continues to be a research project, this means its not ready for production use due to complex setup and handling. Follow-up theses could simplify the development of smart contracts for the Bazo Blockchain by creating a high-level programming language that can be compiled to Bazo virtual machine instructions.