Static Resource Analysis of Smart Contracts – Milestone 6

Nick Roberts

Carnegie Mellon University

`nroberts@andrew.cmu.edu`

April 5, 2018

1 Summary of updates

For this milestone, I added support for receiving external calls from another contract on the blockchain (maintaining compatibility with the Ethereum ABI for this interaction), and I began to plan and write my report.

2 Accomplishments

Since last milestone, I have:

- Fixed a design flaw related to bindings to EVM primitives. Before, partial application of these bindings was prohibited; now, the language supports this feature. The user may choose to partially apply functions at the cost of closure creation, which can run quite expensive.

- Added support to the runtime for receiving external calls from another contract.

- Wrote some code examples to include in my report; planned structure of report; wrote some sections of the report, including the abstract and the motivation.

2.1 Meeting the milestone

My goal as stated in the previous milestone document was to support cross-contract calls, one half of which I have completed: my compiler supports contracts acting as the callee. I could easily add support for acting as a caller, but with a slightly cumbersome API: the code could send a sequence of bytes to another contract, and receive back a sequence of bytes. More work is required to institute a more reasonable (and type-safe) API for acting as the caller; this is what I intend to focus on for the next milestone.

3 Looking ahead

Meeting of the Minds is rapidly approaching, so I am shifting more resources to working on the report and the poster. I'm unclear on the process of poster design and printing—I plan on asking Professor Mowry about this in my meeting with him.

3.1 Revisions to future milestones

As I stated in the previous milestone, static resource analysis will probably not feature in the final project except as something to discuss in the "Future Work" section of the report.

3.2 Resources needed

There are no further resources needed at this time.