スマートコントラクトの ガス消費量の Resource Aware MLを 用いた静的解析

2021/2/10

五十嵐・末永研究室

小野　雄登

研究背景

- スマートコントラクト
- ガス
- コントラクトの実行コストを抑える
  →ガス消費量の静的解析

本研究の概要

- スマートコントラクトのガス消費量の静的解析を行う
- Tezos, Michelson
- Resource Aware ML
- 方針
  1. RAMLでのライブラリの設計
  2. コントラクトを模倣するプログラムの実装
  3. そのプログラムを解析

Resource Aware ML

- OCaml文法を備えた関数型プログラミング言語
- プログラムのリソース消費量を解析するツールとして使える
- 4つのメトリック

  →本研究ではtickメトリックを用いる

Michelsonプログラム

- プログラムの構成
  →初期スタックの型宣言＋命令列
- 命令はスタックを書き換える

RAMLライブラリ

- スタックの要素をヴァリアント型tで表す
- スタックは型tのリスト
- 命令
- プログラム

ガス消費量の見積もり

- interpreter cost
- tickメトリック
- ライブラリの各命令においてtick関数を呼び出す
- tickメトリックによる解析でプログラムのガス消費量を見積もる

解析例

- サンプルプログラム
- 解析結果
  - 基本的なスタック操作や条件分岐などの命令
    → 正しく見積もれた
  - リストの再帰を行う命令(ITERなど)
    → 解析不可能
  - コストがスタックの要素の値に依存する命令(ADDなど)
    → 正しく見積れなかった

まとめ

- RAMLを用いてMichelsonプログラムのガス消費量の静的解析を行った
- Michelsonの各命令を模倣するRAMLライブラリ
- コントラクトを模倣するRAMLプログラムをライブラリを用いて実装
- tickメトリックによるinterpreter costの見積もり