Static Analysis for Gas Consumption of Smart Contracts Using Resource Aware ML

Yuto Ono

Abstract

Since the development of BitCoin in 2008, a variety of cryptocurrencies based on blockchain technology have been developed. Many cryptocurrencies support *smart contracts*, which are programs executed on a blockchain. A smart contract is used to execute a transaction involving cryptocurrencies automatically.

There is a concept of *gas consumption* in smart contracts. Gas is the fee for the computational resources used to execute a contract. When a contract is executed, the execution of each instruction consumes gas corresponding to its computational cost. If the total consumption exceeds the prespecified amount, the execution of the program is aborted immediately and the effect of the program execution is rolled back. One who would like to execute a contract is required to pay cryptocurrency equal to the expected amount of the gas consumption in advance, which is not refunded even if the execution is aborted due to an out of gas error. A method to statically analyze the gas consumption is therefore required to avoid such trouble.

greater than or equal to the (expected?) amount of the ...

Resource Aware ML (RAML) is one of the methods to analyze the execution cost of a program. RAML is a functional programming language equipped with the OCaml syntax. Using the potential-based amortized analysis, which is an analysis of the costs of a sequence of operations whose costs vary depending on the state of the data structure, RAML automatically and statically analyzes the resource consumption bounds for a given program for a specified metric.

This study proposes a method to statically analyze the gas consumption of a smart contract of cryptocurrency Tezos using RAML. A Tezos smart contract is written in a stack-based programming language Michelson. To this end, we implemented a library in RAML each of which imitates the behavior of each Michelson instruction. Using this library, we can write a RAML program that imitates the behavior of a Michelson program. Then, we can estimate the gas

each of whichが具体的に何を指しているのか良くわからないので明記すると良いです。each code in the library?

一文で書いて文構造が複雑になるなら、二文にした方が良いです

consumption of the program by analyzing it with RAML.

Since a Michelson instruction rewrites the stack, we implemented a RAML function that imitates each Michelson instruction as one with `(t list → t list)`, where `t` is the variant type that expresses stack elements and `t list` is the type that expresses a stack. Then we can implement a RAML program that imitates the behavior of a Michelson program as one that applies the functions in our library to the initial stack.

Although the gas consumption of an? execution of a Tezos contract consists of several types of costs, we aim at estimating the *interpreter cost*, which is for executing a Michelson program. For this purpose, we use the *tick metric* of RAML, which is used for defining the quantity of custom resource consumption. We can define the resource consumption of a function by calling a certain function provided by RAML. We implemented the library so that each function calls the function that expresses its interpreter cost. By encoding a contract with our library as a RAML program, 小文字にする We can estimate the interpreter cost of the contract by analyzing the RAML program with the tick metric.

We encoded several Michelson contracts to RAML programs using our library and analyzed them to estimate the gas consumption. The analysis was successful for the contracts that consisted only of instructions of basic stack operations and conditional branches; the estimation was correct for these contracts. However, the analysis was not successful for contracts that contain instructions for recursion on lists. RAML could not analyze the interpreter cost of contracts that contain instructions whose gas consumption depends on the contents of the stack.

Extension of the library to cover more Michelson instructions and to handle recursion on lists are left as future work. We also plan to study other types of costs than the interpreter cost and estimate them.