ReFX: 型に基づくスマートコントラクト自動検証器

ReFX: A type-based automated verifier for smart contracts

陳然・齋藤大聖・河田旺・西田雄気・五十嵐淳・末永幸平（京都大学情報学研究科）
古瀬淳（ダイラムダ株式会社）

課題：スマートコントラクトの安全性

最近のブロックチェーンにはスマートコントラクトというプログラムを動かす仕組みがあり、取引の自動化などに使われている。しかし、スマートコントラクトにバグがあると、暗号通貨が盗まれ、莫大な金銭的損失が生まれてしまうことがある。本研究では、プログラムが仕様を満たしていることを検査する形式検証手法を提案する。

本研究の内容

ブロックチェーン“Tezos”で動作するスマートコントラクトの自動検証手法

「ブロック」というデータ単位が鎖のように連結するデータベースである。P2Pネットワークによる分散的保存及び自律的な管理が特徴である。

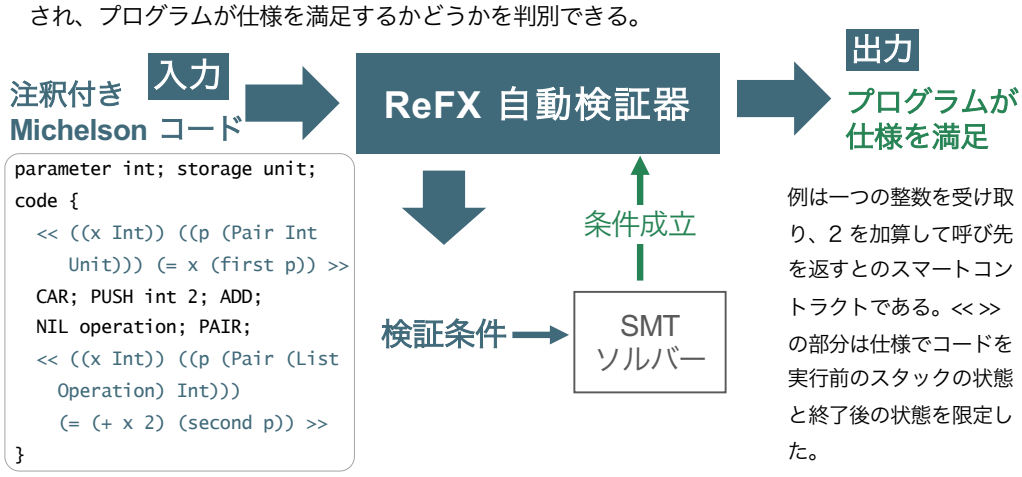
Proof-of-Stake 合意モデルに基づいた第3世代ブロックチェーン技術の暗号通貨である。プロトコルが自身を修正でき、スマートコントラクトと形式検証を支持する。

ブロックチェーン上のアカウントに付随するプログラムである。送金されると自動的に実行され、プログラム中で再び送金を引き起こし、第三者を介さずにトランザクションを処理できる。

仕様通りに作動することを保証するための検証である。それを自動化することで、ユーザが安全で信頼できるプログラムを高速に開発することができる。

ReFX の構造

本研究は、Tezos のスマートコントラクトを書くプログラム言語 **Michelson** に対して、形式検証の手法で **ReFX 自動検証器**を開発した。元 Michelson コードに仕様を表現する注釈を加えて ReFX 自動検証器に入力すると検証条件を生成する。検証条件は SMT ソルバーに推論され、プログラムが仕様を満足するかどうかを判別できる。



例は一つの整数を受け取り、2 を加算して呼び先を返すとのスマートコントラクトである。<< >> の部分は仕様でコードを実行前のスタックの状態と終了後の状態を限定した。

形式検証の必要性

形式検証は、論理学でプログラムの正しさ証明する手法である。手動テストは人のミスやテストケースのデザインなどの原因で信頼性が不安定だが、形式検証は数学によってどんな入力でも正しく動作することが保証できる。その中、型システムという数学モデルがよく使われているが、本研究では篩型（Refinement types）という型を導入した。

技術的内容のコア：篩型

篩型は要素の基本型と属性を関連つけられた型である。普通のプログラミング言語の型システムでは int や float などの基本型をよく使われているが、篩型はさらに値の範囲などの属性を限定したものである。例えば、$\{v : int \mid v \neq 0\}$ は値が 0 でない整数型と意味している。篩型の一つの特徴は経路敏感性である。`if(x != 0){y = 1 / x;}` とのブランチ文を考えよう。基本型のみの型システムでは除算の異常について推論が難しい。篩型を導入すると、もしこの文が実行前の環境で x の型が int であれば、ブランチの中での x の篩型は $\{v : int \mid v \neq 0\}$ となって、次の除算が異常を起こさないと保証できる。篩型に基いた型推論も自動化する必要がある。SMT ソルバーを用いた自動検証アルゴリズムもよく研究されている。