OCamlからEVMバイトコードへのコンパイラ

山下拓真[*1*2]　吉岡拓真[*2]　池渕未来[*1*2]　今井宜洋[*1]
[*1]株式会社proof ninja　[*2]京都大学

Motivation

スマートコントラクトとは、ブロックチェーン上にプログラムを書き込むことでそのプログラムを自動的に実行できるようにする仕組み

⚠ **脆弱性を突いた攻撃の被害が大きい**

⚠ **デプロイすると変更が不可**

→ **Coqでの検証により脆弱性の検査をしたい**
👎 SolidityではCoqでの検証が難しい

→ Coqの検証に適した**OCaml**でスマートコントラクトを書けるようにする

Solidity

スマートコントラクトを記述するために用いられている言語の一つ。**EVM(Ethereum Virtual Machine)**という実行環境で動作するバイトコードにコンパイルできる。

Approach

2

Sample.ml

Yul

Solidityの中間言語として開発された言語。Solidityのコンパイラsolcでコンパイル可。

To do

1. OCamlからYulのコンパイラ**OCaml2EVM**の制作
2. OCamlでコントラクトのプログラムを記述

Current Status

1. OCaml2EVM
   - ✅ Let式
   - ✅ 関数適用
   - ✅ 逐次実行
   - ✅ If式
   - レコード、高階関数、etc.

2. 実用的なサンプル
   - ✅ ERC20
   - Uniswap-v1(WIP)

   etc.

送金や**承認**（BがAのトークンをいくらか扱うことを許す）などが可能

ERC20のトークン↔ETHの変換が可能。レートも自動的に計算。

今後の展望

- Coqによる検証