# Automatically Fixing Vulnerabilities in WebAssembly

Yubin Hu

yubin.hu@bupt.edu.cn

November 2, 2021

# Blockchain

**Define**

**Blockchain** is a public list of records which are linked together.

- Thanks to the underlying cryptography mechanism, the records in the blockchain can resist against modification.

# Smart Contracts

**Define**

**Smart Contracts**, once deployed on the blockchain network, become an unchangeable commitment between the involving parties.

- Because of that, they have the potential to revolutionize many industries such as financial institutes and supply chains.
- However, like traditional programs, smart contracts are subject to code-based vulnerabilities, which may cause huge financial loss and hinder its applications.

# WebAssembly

**Define**

**WebAssembly** (abbreviated Wasm) is a binary instruction format for a stack-based virtual machine.

- Wasm is designed as a portable compilation target for programming languages, enabling deployment on the web for client and server applications.
- The WebAssembly virtual machines can be embedded into Web browsers or blockchain platforms.
- Furthermore, in Ethereum 2.0, Wasm VM is the replacement of Ethereum VM (EVM).

# Goal

In this work, I propose a tool, which automatically fixes potential vulnerable smart contracts in WebAssembly.

# Research Question I

Research Question

How to detect the vulnerability?

**Vulnerabilities**

- Reentrancy
- Missing Input Validation
- Locked EthereumUnhandled Exception
- *tx.origin* Vulnerability
- Arithmetic Vulnerability

**Vulnerability Detection**

- symbolic execution

# Research Question II

**Research Question**

How to solve the problem of path explosion in symbols execution?

- loop bound
- call depth
- template-based fix patterns
- different levels depend on vulnerabilities

# Research Question III

**Research Question**

Effectiveness in patch generation.

- Overall Results
- Transaction Usage
- Failed Patch

# Reference

*[1] Nguyen T D , Pham L H , Sun J . sGUARD: Towards Fixing Vulnerable Smart Contracts Automatically[J]. 2021.*

*[2] Rodler M , Li W , Karame G O , et al. EVMPatch: Timely and Automated Patching of Ethereum Smart Contracts[J]. 2020.*