3131100727 · 软件安全

胡玉斌 / 202111054

October 13, 2021

Thesis proposal

1 Idea

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, 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 (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. The EOSIO blockchain has supported Wasm. Furthermore, in Ethereum 2.0, Wasm VM is the replacement of Ethereum VM (EVM).

We need a tool which is inspired by program fixing techniques for traditional programs such as C or Java, and are designed specifically for smart contracts in WebAssembly.

2 Research Questions

1. How to detect the Vulnerability?
2. How to solve the problem of path explosion in symbolic execution?
3. Effectiveness in Patch Generation
4. Runtime Performance

3 Roadmap

Date	Progress	
2021-10-1 ~ 2021-10-15	Investigation	Investigate the feasibility of related issues and the current academic progress
2021-10-16 ~ 2021-11-15	Implemention	Structure and implement the proposed ideas
2021-11-15 ~ END	optimization	Optimize the tools implemented and the algorithm strategies

4 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.