Vulnerabilities Detection in Smart Contracts

Sundas Munir

Halmstad University, sundas.munir@hh.se,

Smart contracts are computer programs that execute on blockchains. They have the potential to revolutionize various sectors, such as cryptocurrency, supply chain management, energy, NFTs, gaming, and real estate. However, their usage raises cybersecurity concerns due to potential vulnerabilities and the risk of exploitation by malicious actors. Specifically, errors and bugs in smart contracts can lead to financial losses and compromise the integrity of transactions. Common types of bugs and vulnerabilities include syntax errors, logical errors, security vulnerabilities, and runtime errors.

In addition to these issues, some security vulnerabilities arise in smart contracts due to traditional concurrency concerns, such as non-determinism (ND), in the Ethereum ecosystem. Our research focuses on addressing three sources of non-determinism and their resulting vulnerabilities in Ethereum:

1. Methods are invoked in an arbitrary order because Ethereum schedules transactions in non-deterministic (ND) order, resulting in vulnerabilities we term ND-1 issues.
2. Inputs from users or other smart contracts and asynchronous callbacks perform non-deterministic state changes, resulting in vulnerabilities we term ND-2 issues.
3. Externally called contracts could behave non-deterministically, e.g., re-enter or throw, resulting in vulnerabilities we term ND-3 issues.

Our research proposes approaches to mitigate non-deterministic problems in Ethereum by focusing on these issues, improving bug detection rates while minimizing false positives. Specifically,

1. Our proposed approach for ND-1 issues detects 27% more instances of ND-1 with 84% fewer false positives. The patterns we introduced are novel and detect new instances of ND-1 issues.
2. Our proposed approach for ND-2 issues detects 6x more instances of ND-2 with 18x fewer false positives. Our study finds that ND-2 issues are still prevalent in current contracts.
3. Our proposed approach for ND-3 issues detects 5x more instances of ND-3 with 2x fewer false positives. The patterns we introduced are novel and detect new instances of ND-3 issues.

Therefore, our proposed approaches aim to enhance the reliability and security of smart contracts. This is crucial for their widespread adoption and effectiveness in the blockchain ecosystem.