Finding Vulnerabilities in Smart Contracts

Michele Massetti
big.michelemassetti@gmail.com
Karlsruhe Institute of Technologies
Karlsruhe, Baden-Württemberg, Germany

ABSTRACT

Blockchain is a revolutionary technology that enables users to communicate in a trust-less manner. The most prominent change brought by this technology is the mode of business between organizations: they do not need anymore a trusted third party. It is a distributed ledger technology based on a decentralized peer-to-peer (P2P) network. Since Bitcoin was deployed, many blockchain systems have been born with more capabilities, which have allowed them to fit many different use cases. Smart Contracts, which are programs running on blockchain systems, could extend the potentiality of blockchain from a platform for financial transactions to an all-purpose utility. The development of innovative and prominent applications is a consequence of them, such as NFT marketplaces, music royalty tracking, supply chain and logistics monitoring, voting mechanism, cross-border payments, and many others. Finding bugs and vulnerabilities in them is necessary for assuring their correct behaviour. This paper deals with the way for finding the vulnerabilities in Ethereum blockchain-based smart contracts. We review related works regarding the classification of the most common vulnerabilities and tools which support their detection.

KEYWORDS

Solidity, Software, Vulnerability, Blockchain

1 INTRODUCTION

Nowadays, the major platform for decentralized decentralized finance (DeFi) and applications (dApps) is Ethereum. It can be described as the "internet of Blockchain". Its ecosystem consists of the underlying blockchain, a large variety of smart contracts deployed on it, a wide range of valuable assets.

This growing technology has attaracted many investors, indeed, according CoinGeko, the crypto market's value is standing around $2 trillion. On the other hand, interest in such a market has grown even among malicious attackers. Attacks such as the "Parity Wallet Hack" and the "Decentralized Autonomous Organization Attack" cost millions of dollars simply because of naive bugs in the smart contract code. Blockchain and smart contract technologies have multiple aims, but unfortunately, new applications based on them still contain bugs and multiple vulnerabilities, which cause several issues for the end-users. Most of the use of this technology relates to finance or certifications, therefore integrity, authentication and authorisation in transactions are mandatory.

The research field behind blockchain technology is growing, as well as the one concerning its security and accordingly, many analysis tools were developed. These incorporate various strategies for performing the analyses, concerning the technical aspects of smart contracts, so these would work differently according to the object of the analysis.

Among the many aspects of smart contract, our systematic literature review focuses on studies related to vulnerabilities and analysis tools for their detection. We will try to give an answer to the following research questions:

- Which are the main vulnerabilities in Smart Contracts?
- Which methodologies are implemented by analysis tools?
- How should we behave for the detection of Vulnerabilities?

In Section 2, we compare the actual papers and works regarding this topic. Section 3 explains the objective of our analysis: Smart Contracts Vulnerabilities. We give a taxonomy for the main vulnerabilities regarding Solidity. The classification of analysis tools is shown in Section 4. We discuss about the main strategies implemented by those. Options

- In the last Section 5 we try to define a guideline for detecting vulnerabilities.
- In the last Section 5 we give an overview, defining the suitable cases which the tools work better.
- In the last section 5 we propose a real case.

2 RELETED WORKS

- Papers about vulenrabilities detection for defing a taxonomy
- papers regarding comperison between tools
- papers of the tools that we want to have a Look

Kushwaha et al. [1]

3 VULNERABILITIES IN SOLIDITY

4 SECURITY ANALYSIS TOOLS

I create a table with the most common vulnerabilities like reentrancy, arithmetic operations, DOS, self distruction. Post some codes. I explain the most typologies of tools. Tools with and without specification. Fuzzers, symbolic analysis, formal specification. Level of abstraction of the tools.

5 CONCLUSION

I would propose 3 options:

- propose a real case of analysis: I select a real wolrd exploit and I use the tools for analyses it.
- give a guideline for developers, how they should behave. So having a look of vulenrabilities and using the cited tools.
- an overview of the tools relating with the vulnerabilities.

Colloquium on Vulnerability Discovery 2022, August 1st, 2022, KIT, Karlsruhe, Germany

ACKNOWLEDGEMENTS

REFERENCES

[1] Satpal Singh Kushwaha, Sandeep Joshi, Dilbag Singh, Manjit Kaur, and Heung-No Lee. 2022. Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract. *IEEE Access* 10 (2022), 6605–6621. https://doi.org/10.1109/ACCESS.2021.3140091

A RESEARCH METHODS

A.1 Part One