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.

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

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 **??**. We discuss about the main strategies implemented by those. Options

- In the last Section 6 we try to define a guideline for detecting vulnerabilities.
- In the last Section 6 we give an overview, defining the suitable cases which the tools work better.
- In the last section 6 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

An overview of classification of Vulnerabilities in Solidity is given in this section. Classifications by scholars and community taxonomies are the strating point for drowing our own classification. These knoledges are used for having our own classification; we depicted which ones are the most relevant vulnerabilities for our work. The term vulnerability is used in a similar sense than is common in computer security. It refers to a weakness or limitation of a smart contract that may result in security problems. A vulnerability represents even the way the attacker can exploit the contract. This includes locked or stolen resources, breaches of confidentiality or data integrity, and state changes in the environment of smart contracts that were not detected by developers or users, therefor they possibly be exploited by a malicious part.

3.1 Vulnerabilities Classification and examples

We summeries 8 different Vulnerabilities, providing a definition and a real-world example.

Reentrancy. It is one of the vulnerabilities much more exploited during the recent year. Many attacks occured and could steal great amount of many to vulnerable protocol. A reentrancy attack can occur when a function makes an external call to another untrusted contract before it resolves any effects. A recursive call back to the original function is made by the attacker, before the function could updated the state of the state of the variables. The goal is repeating interactions that would have otherwise not run after the effects were resolved. The function withdraw, line 8 to 16 Listing 1, implements this bug, because the balance of the user is updated after the external call. The attacker, with the usage of a malicious smart contract, can call again the vulnerable function. It is run multiple time, without updating the balance, withrawing all the funds. There are several countermeasures for this type of bug: semaphores logic can be implemented with the modifiers, the update of the variable can be moved before the external call. The external call can be safe if the developer checks the amount of gas used, in order to avoid an attacker can modify the control flow.

```
1  contract EtherStore {
2      mapping(address => uint) public balances;
3      ...
4      //vulnerable function exploited by the attacker
5      function withdraw() public {
6          uint bal = balances[msg.sender];
7          require(bal > 0);
8
9          (bool sent, ) = msg.sender.call{value: bal}("");
10         require(sent, "Failed to send Ether");
11
12         balances[msg.sender] = 0;
13     }
14     ...
15 }
```

Listing 1: Reentrancy

Unexpected Ether balance. An exploites can generated a Dos attack when the smart contract strictly assume a specific token balance. It is always possible to forcibly send ether to a contract (without triggering its fallback function), using selfdestruct, or by mining to the account. Smart Contracts which rely on code execution for every ether sent to the contract can be vulnerable to attacks where ether is sent. In the provided example (Listing 2), the function play() has a require at line 5, which checks no players can play when the balance reaches the predefined threshold. The function claimReward(), allows the user to withdraw, when the balance reaches the threshold. An attacker can send ether to this contract, for manipulating its balance. If it was greater than the threshold, the functions would always revert because of the require. As a consequence, no one could withdraw the funds and call the function play().

```
1   ...
2   function play() public payable {
3         require(msg.value == 0.5 ether); // each play is
              0.5 ether
4         uint currentBalance = this.balance + msg.value;
5         // ensure no players after the game as finished
6         require(currentBalance <= finalMileStone);
7         // if at a milestone credit the players account
8         if (currentBalance == payoutMileStone1) {
9             redeemableEther[msg.sender] +=
                  mileStone1Reward;
10        }
11        else if (currentBalance == payoutMileStone2) {
12            redeemableEther[msg.sender] +=
                  mileStone2Reward;
13        }
14        else if (currentBalance == finalMileStone ) {
15            redeemableEther[msg.sender] += finalReward;
16        }
17        return;
18  }
19  function claimReward() public {
20    // ensure the game is complete
21    require(this.balance == finalMileStone);
22    // ensure there is a reward to give
23    require(redeemableEther[msg.sender] > 0);
24    redeemableEther[msg.sender] = 0;
25    msg.sender.transfer(redeemableEther[msg.sender]);
26  }
27  ...
```

Listing 2: Unexpected Ether

Overflows & Underflows. The Ethereum Virtual Machine (EVM) defineds fixed-size data types for integers. An example is the identifier uint8, unsign integer over 8 bit, for variables means the variable can only store numbers in the range [0,255]. The attacker can craft the input value of a vulnerable contract's function in order to force a specific operation. In the contract TimeLock in Listing 3, an attacker could forge a parameter of the function function increaseLockTime, in oder to set lockTime to 0 because of Overflows. So it can call withraw and passing the require at line 17. The most common way for solving these issues is to build or use mathematical libraries which replace the standard math operators. OppenZepplin is a company, dealing with Blockchain technologies. It has done a great job in building and auditing secure libraries which can be leveraged by the Ethereum community. SafeMath library can be found in most of the deployed smart contracts.

```
1  contract TimeLock {
2
3      mapping(address => uint) public balances;
4      mapping(address => uint) public lockTime;
5
6      function deposit() public payable {
7          balances[msg.sender] += msg.value;
8          lockTime[msg.sender] = now + 1 weeks;
9      }
10
11     function increaseLockTime(uint _secondsToIncrease)
           public {
12         lockTime[msg.sender] += _secondsToIncrease;
13     }
14
15     function withdraw() public {
16         require(balances[msg.sender] > 0);
17         require(now > lockTime[msg.sender]);
18         msg.sender.transfer(balances[msg.sender]);
19         balances[msg.sender] = 0;
20     }
21 }
```

Listing 3: Overflows & Underflows

Block Timestamp Manipulation. ispart of the cathegory of vulnerabilities that can be exploited by corrupt miners. A miner cac forge the timestamp by a few seconds, for obtaing benefits. The timestamp dependence vulnerability occurs from a flawed comprehension of timekeeping. It enables the Ethereum network to be detached from the synchronized global clock. The block timestamp can be used as entropy for random numbers, locking funds for periods of time and various state-changing conditional statements that are time-dependent. Since the smart contract permits miners to put up a timestamp within 30 seconds of block validation, this gives a miner more opportunity for exploitation. Listing 4 shows a function (a fallback) which implements the logic of a lottery. The users can send ether to this contract, which accepts just one transaction per block. If the block is a multiple of 15, the user receives all the funds. This function is based on the timestamp of the balck, a malicious miner could adjust the timestamp for getting the win.

```
  ...
  // fallback function used to make a bet
  function () public payable {
        require(msg.value == 10 ether); // must send 10
             ether to play
        require(now != pastBlockTime); // only 1
             transaction per block
        pastBlockTime = now;
        if(now % 15 == 0) { // winner
            msg.sender.transfer(this.balance);
        }
  }
  ...
```

Listing 4: Block Timestamp

Call to the unknown. The smart contracts workflow might be manipulated by the invocation of third party or untrusted code. The callee can implemnt malicous code which can be run and modify the normal execution of the calleer. For an untrusted, malicious party, it might be possible to inject code in a way, that can influence the contracts behavior unexpectedly and maliciously. A common case is the reentrancy, which can involve the Solidity functions .call(), .send() and .transfer(). Mistyped direct function calls or using the wrong function signature are classified as this type of vulnerability. The contract CallerContract in Listing 5 is an example of this vulnerability. An attacker could call the function caller, passing as parameter the address of a malicious contract, which implement a malicious fallback. In that case the fallback would be triggered, bacause the contract does not have any function with that name.

```
cotract CalleeCotract{
  fucntion toBeCalled(){
    //do some operations
  }
}

contract CallerContract{
  functionn caller(address a){
    toBeCalled(a).toBeCalled();
  }
}

contract Malicious{
  fallback(){
    //the attack
  }
}
```

Listing 5: Call to the unknown

Transaction Ordering Dependence. Miners are responsable for the creation and certification of the blocks on the blockchain. Inside those, the transactions are stores, but their order is not guaranteed by design and the miners can easily manipulate that. Consequently, this makes the smart contracts vulnerable to the transaction order dependency, it can be classified as a type of race condition. The vulenrability relies on smart contracs critical decision are based on the order of transaction. Moreover, if two dependent transactions are invoked by the same contract then ordering of transactions must affect the states of blockchain. So we can have a case of race condition, even with a miner without malicious aims.

The smart contract MarketPlace(Listing 6) implements the logic of a market place. The users can buy an arbitrary amount of stock and the owner can set the price. In this case the variable price is influenced by two functions. If the owner of the contract would be a miner, it could manipulate the order of transaction. The miner-seller can influence the transaction orders and update the price after the buy request was sent, but before it is processed, effectively increasing the anticipated price for the buyer. The seller can just modify the price, while a user is buying and it can effect its action.

```
contract MarketPlace {
  uint256 price;
  uint256 stock;
  address owner;
  constructor() {
    owner= msg.sender;

  }
  modifier onlyOwner(){
    require(msg.sender==owner);
    _;
  }
  function updatePrice(uint256) onlyOwner {

  }
  function buy(uint256 amount){
    require(stock>=amount);
    require (msg.value >=amount*price);
    stock-=quant;
  }
}
```

Listing 6: Transaction Ordering Dependence

Denial Of Service (DOS). Denial of service attack is a cathegory of attack, which involeves all those one which have the aim to disturb the functionality or stop the execution of the target system. In the context of smart contracts, we can provide some example of this cathegory, which involve multiple strategies for breaking the normal flow execution of the program.

Listing 7 shows a simpliefied contract for auction. The function refundUsers() has the responsibility to refund all the bidder. The function contains a loop, so it can get the amount of the bid of the user and refund it. The bug relies on the the require inside the loop. If the transaction returns false, the require fails, so all the transactions are reverted, consequently all the previous refunds are reverted. A malicious contract can be implemented for taking part to the function, but that one reverts every time it receives ether. In

this way, the function refundUsers() would always revert and no users can be refunded.

```
1  contract Auction {
2    mapping (address=>uint256) allBids;
3    mapping (uint256=>address) users;
4    uint256 nUsers;
5    uint256 lastrefund;
6    ...
7    function refundUsers() {
8
9      for(uint256 i = lastrefund; i<nUsers;i++){
10       address user=users[i];
11       uint256 amount= allBids[user];
12       (bool sent, )= user.call{value: amount}("");
13       require(sent);
14     }
15
16   }
17   ...
18 }
```

Listing 7: Denial of Service/Out of Gas

Out of Gas. In Ethereum, we have to pay for each computational operation, measured in the unit called gas. In the Ethereum documentation, gas is defined as follows: "Gas refers to the unit that measures the amount of computational effort required to execute specific operations on the Ethereum network. Since each Ethereum transaction requires computational resources to execute, each transaction requires a fee. Gas refers to the fee required to conduct a transaction on Ethereum successfully."

The sender pays the transaction fee, previously specifying the gas limit, If the payed amount exceeds the fee, it will receive a refund when the transaction finishes. If the actual execution cost of the transaction exceeds the gas limit, the transaction will fail with an out of gas error. We used Listing 7 for showing an example of DOS, but it implements an out of gas vulnerability too. The amount of gas depends on the number of the for loop's iteration. If the number of iteration grows too much, the function would always revert. A malicious attacker can manipulate the number of iterations, using a great number of wallet for the bid.

Unchecked CALL/SEND Return Values. There a number of ways of performing external calls in solidity. The transfer() method is the most common way for exchanging ether between smart contracts. It reverts if the something goes wrong and function does not succeed. However, the send() and call() function can also be used and, for more versatile external call. These functions return a boolean indicating if the call succeeded or failed. A common bug relies on the return value is not checked, rather the developer expects a revert to occur.

The user can call the function withdrawEmergency() at line 4, Listing 8, for withdrawing all its funds. The function updates the value of the mapping balances, setting the balance of the user to zero. If the function does not succeed, it does not revert. The funds of the user would be stacked insed the contract. Moreover the amount of ether in the contract is miscomputed.

```
1  contract Bank{
2    mapping (address=> uint256) balances;
3    ...
4    function withdrawEmergency() public {
5      require(balances[msg.sender] > 0);
6      uint256 amount= balances[msg.sender];
7      balances[msg.sender] = 0;
8      etherLeft -= _amount;
9      msg.sender.send(amount);
10   }
11   ...
12 }
```

Listing 8: Unchecked CALL/SEND Return Values

4 METHODS FOR FINDING VULNERABILITIES

Static analysis. refers to a class of methods that examine the source code or bytecode of a contract without execut- ing it. Most methods listed below are static.

Dynamic analysis. means to observe a contract while executing (parts of) it in the original context.

Disassembling. means to translate EVM bytecode into bet- ter readable assembly language, where machine operations and storage addresses are represented symbolically.

Decompilation. is the process of transforming EVM byte- code to a more compact representation on a higher abstrac- tion level (like intermediate or Solidity code) to enhance the readability of the code or to ease data flow analysis.

Control flow graph (CFG). is a directed graph, where the basic blocks of a program serve as the nodes. An arc connects node A with node B if it is possible that block B gets executed immediately after block A. The arc may be labeled by the condition under which this path is chosen.

Formal verification. means verification by formal methods with the aim of proving or disproving system properties rigorously. As a prerequisite, all components referenced by such a property as well as their behavior must have been specified formally. E.g., to verify properties of smart contracts on bytecode level formally, we need a formal specification of the EVM and of the properties.

Dynamic CFG. is similar to a CFG with the difference that arcs indicate the actual control flow encountered during a particular execution of the code.

Model checking. is a technique for automatically verifying correctness properties of finite-state systems. It requires a model of the system which is then checked against a given specification.

Call graph. is a directed graph, where the nodes are functions. There is an arc from node A to node B if function A calls function B.

Abstract Syntax Tree (AST). represents the syntactic struc- ture of Solidity code as a tree. It occurs as an intermediate product when compiling Solidity to bytecode. Often, it is better suited for analyzing Solidity code.

Symbolic execution. means to execute code using symbols instead of concrete values for the variables. Operations on these symbols lead to algebraic terms, and conditional statements give rise to propositional formulas that char- acterize the branches. A particular part of the code is reachable if the conjunction of formulas on the path to this part is satisfiable, which can be checked by SMT-solvers.

5 REAL-WORLD CASE

6 CONCLUSION

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