# Ethereum Smart Contract Analysis Tools: A Systematic Review

**Article** *in* IEEE Access · April 2022

DOI: 10.1109/ACCESS.2022.3169902

CITATIONS
6

READS
793

**5 authors**, including:

Satpal Singh Kushwaha
Manipal University Jaipur
**17** PUBLICATIONS **48** CITATIONS
SEE PROFILE

Sandeep Joshi
Manipal University Jaipur, India
**58** PUBLICATIONS **288** CITATIONS
SEE PROFILE

Dilbag Singh
NYU Langone Medical Center
**128** PUBLICATIONS **3,517** CITATIONS
SEE PROFILE

Manjit Kaur
Gwangju Institute of Science and Technology
**115** PUBLICATIONS **3,289** CITATIONS
SEE PROFILE

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



*Digital Object Identifier*

# Ethereum Smart Contract Analysis Tools: A Systematic Review

**SATPAL SINGH KUSHWAHA[1], SANDEEP JOSHI[1], (Senior Member, IEEE), DILBAG SINGH[2], (Member, IEEE), MANJIT KAUR[2], (Member, IEEE), and HEUNG-NO LEE[2], (Senior Member, IEEE)**

[1]Department of Computer Science and Engineering, Manipal University Jaipur, Jaipur-Ajmer Express Highway, Jaipur, India.
[2]School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology, Gwangju 61005, South Korea.

Corresponding author: Heung-No Lee (e-mail: heungno@gist.ac.kr).

This work was supported in part by the National Research Foundation of Korea (NRF) Grant funded by the Korean government (MSIP) (NRF-2021R1A2B5B03002118) and This research was supported by the Ministry of Science and ICT (MSIT), Korea, under the ITRC (Information Technology Research Center) support program(IITP-2021-0-01835) supervised by the IITP(Institute of Information & Communications Technology Planning & Evaluation)

**ABSTRACT** Blockchain technology and its applications are gaining popularity day by day. It is a ground-breaking technology that allows users to communicate without the need of a trusted middleman. A smart contract (self-executable code) is deployed on the blockchain and auto executes due to a triggering condition. In a no-trust contracting environment, smart contracts can establish trust among parties. Terms and conditions embedded in smart contracts will be imposed immediately when specified criteria have been fulfilled. Due to this, the malicious assailants have a special interest in smart contracts. Blockchains are immutable means if some transaction is deployed or recorded on the blockchain, it becomes unalterable. Thus, smart contracts must be analyzed to ensure zero security vulnerabilities or flaws before deploying the same on the blockchain because a single vulnerability can lead to the loss of millions. For analyzing the security vulnerabilities of smart contracts, various analysis tools have been developed to create safe and secure smart contracts. This paper presents a systematic review on Ethereum smart contracts analysis tools. Initially, these tools are categorized into static and dynamic analysis tools. Thereafter, different sources code analysis techniques are studied such as taint analysis, symbolic execution, and fuzzing techniques. In total, 86 security analysis tools developed for Ethereum blockchain smart contract are analyzed regardless of tool type and analysis approach. Finally, the paper highlights some challenges and future recommendations in the field of Ethereum smart contracts.

**INDEX TERMS** Ethereum, Smart Contract, blockchain, cryptocurrency, decentralized, Dapp, Vulnerabilities, Security, Analysis tool.

## I. INTRODUCTION

BLOCKCHAIN technology [1] gained the interest of the research community in the year 2008 when a white paper was published by Satoshi Nakamoto [2] on a double-spending problem in peer-to-peer decentralized network [3, 6]. Now the popularity of blockchain technology is rapidly increasing day by day, such that countries and giant financial institutions are planning to deploy their operational processes on the same technology [4, 5]. In blockchain technology transactions, the trusted third parties are removed with the help of a consensus mechanism. Smart contracts work on the application layer of blockchain. Blockchain technology became popular after Satoshi Nakamoto's white paper on the double-spending problem in a peer-to-peer network. In blockchain technology transactions, the trusted third parties are removed with the help of a consensus mechanism. Today, Ethereum is the most widely used blockchain platform. Ethereum is Turing complete to code smart contracts with developers' constraints.

A smart contract [8, 9] is a contractual agreement embedded in a self-enforceable piece of code. The parties in the agreement agree to interact with each other based on some predefined constraints, such that whenever a condition is met, the predefined operations will execute automatically. Smart Contracts provide higher transparency without the need for trusted third parties. Figure1 depicts the structure [12, 14] of Ethereum smart contract.

The smart contract has many use cases in various real-life areas. Following are some of the use cases:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



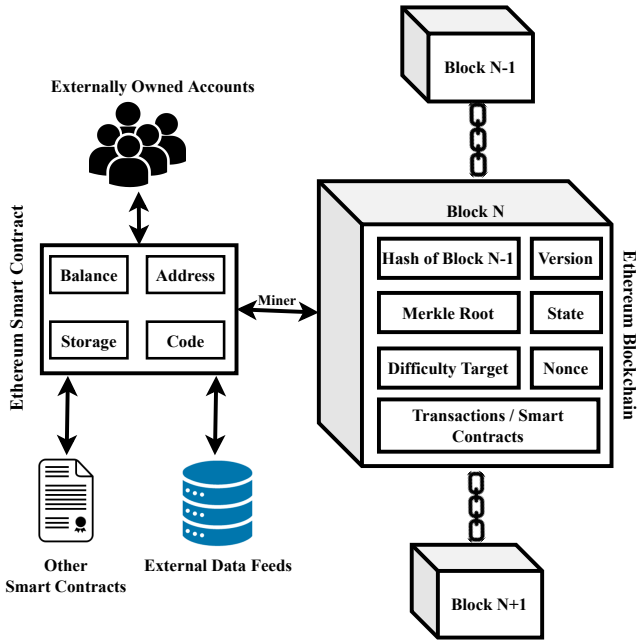


**FIGURE 1.** Ethereum blockchain based smart contract

- **Financial Contracts:** The governing rules of a financial product or service can be coded in the form of a smart contract to facilitate claims settlements and automated financial transactions. The DeFi (Decentralized Finance) services or applications can address a large market of financial transactions without a bank. The DeFi applications can be more advantageous than traditional ones regarding round-the-clock borderless availability.
- **Prediction Markets:** The growth in the prediction market is not according to time due to the involved risk in the same. Smart contracts can revolutionize the field of the prediction market. There are several gaming fields where the players have been betting for a long time without trusting the third party. So the concept of the Ethereum smart contract can be utilized in the prediction of the auction, election, and any betting game.
- **Digital Identity:** In traditional systems, identity management and trust management are facilitated by Public Key Infrastructure or PKI. The certificate-based PKIs have a problem with the certificate tree isolation. The Ethereum smart contracts can manage digital identities and build trust.
- **Supply Chain Management:** The Ethereum smart contracts can reduce the complexity in the supply chain by using the automatic verification process. The traditional supply chain system lacks transparency and traceability, which blockchain-based smart contracts can effectively improve.
- **Health Care Industry:** The smart contract can be applied in various application areas in the healthcare industry like health insurance, medical research, patient data management, and drugs supply chain management. Smart contracts can help effectively manage patients' medical history data management.
- **Tokenization ICO/DAICO:** The ERC-20 is one of the essential Ethereum smart contract standards. The ERC-20 is a set of rules to keep track of all types of fungible Ethereum tokens. ERC -20 is short of Ethereum Request for Comments 20. It employs an application programming interface within smart contracts. ERC-721 is one other type of token which is non-fungible. The ERC-20 token represents a single entity, whereas ERC-721 represents a set of resources.

But smart contracts [7, 10, 11] are vulnerable to attacks due to security flaws present in there due to several reasons like features of blockchain, coding issues, etc. As smart contracts store cryptocurrencies as their balances, attackers can take benefit of these security vulnerabilities [36, 37, 38, 39], which can result in enormous losses. For analyzing smart contracts, several security analysis tools [44, 48] have been developed. Our survey will focus only on analysis tools associated with the Ethereum blockchain smart contract. We present a detailed review of 86 analysis tools for the Ethereum blockchain-based smart contract, covering all the analysis tools present in the literature or on the web, irrespective of their type and analysis approach.

### A. RELATED WORK

Many review articles have been published by researchers in this domain with different-different viewpoints. Harz et.al. [15] examined ten verification tools along with their respective languages and verification methods. Angelo et. al. [16] surveyed 27 smart contract analysis tools with different-different points of view like open-source availability, development, working methodology, and security vulnerabilities. Liu and Liu [17], surveyed 53 papers for security vulnerabilities and correctness aspects. They discussed 18 tools in different-different categories like semantic analysis, behavioral analysis, formal verification, etc. Tang et al. [45] surveyed 15 analysis tools and their related vulnerabilities. Ante [18] studied the smart contracts concerning citation statistics distribution of keywords of several smart contract platforms and discussed very few analysis tools like Oyente and SmartCheck. Almakhour et al. [19] surveyed smart contract analysis tools by categorizing them into verification tools and vulnerability analysis tools for Ethereum blockchain smart contracts. They discussed 25 tools in two categories: formal verification for correctness and Vulnerability detection for security assurance. T. Durieux et. al. [56] performed a pragmatic survey of 9 automatic analysis tools on 47587 Ethereum smart contracts and found that 97% of contracts are vulnerable. Ghaleb et. al. [49] focused only on static analysis tools and proposed a technique named SolidiFI for evaluating the performance of static analysis tools. Tolmach et. al. [50] studied various verification tools by considering the formal modeling and verification techniques. D. He et.

al. [51] studied security vulnerabilities related to Ethereum smart contract and their defense mechanism and some of the security audit methods. They discussed only three analysis tools: Oyente, Porosity, and Mythrill. Grishchenko et. al. [52] surveyed 11 security and verification tools but focused their discussion on the static analysis tool named EtherTrust and formal verification tools. Anna Veca et. al. [53] surveyed 26 analysis tools for Ethereum smart contracts concerning smart contract testing and code analysis. Pinna et.al. [54] presented n pragmatic study on the specific type of Ethereum smart contract (with the topmost number of transactions means financial smart contract) deployed on Ethereum blockchain but covers a little about analysis tools. Bin Hu et. al. [55] surveyed 39 analysis tools concerning methodology, input, and availability of source code. All the above surveys discussed analysis tools related to specific vulnerabilities or specific fields like verification tools. None of the above surveys covers all the Ethereum smart contract analysis tools associated with the analysis of the Ethereum smart contract. This paper presents 86 analysis tools for the Ethereum blockchain-based smart contract to cover this research gap.

### B. MOTIVATION

In a no-trust contracting environment, smart contracts can establish trust among parties. Terms and conditions embedded in smart contracts will be imposed immediately when specified criteria have been fulfilled. So, the smart contract, which is just a piece of code, executes the terms and conditions without the need of any third person. Thus, smart contracts must be analyzed to ensure zero security vulnerabilities or flaws before deploying them on the blockchain because a single vulnerability can lead to terrific losses [36]. Thus, it becomes necessary to analyze the security vulnerabilities of smart contracts to develop safe and secure smart contracts.

The existing review articles have discussed only a limited set of Ethereum smart contract analysis tools. Even most of the existing review articles are limited to specific types of tools. Hu et. al. [55] discussed 39 tools, which was the highest among all review articles. Therefore, this paper presents a detailed systematic survey of smart contract analysis tools for the Ethereum blockchain. The overall objective is to discuss maximum analysis tools to highlight some challenges and future recommendations in Ethereum smart contracts.

### C. RESEARCH QUESTIONS

Smart contracts [40, 41, 42, 43] can be developed on various blockchain platforms, which have their features and challenges. Still, Ethereum is mainly used as a very prominent smart contract development platform, so we focus only on analysis tools for smart contracts related to Ethereum blockchain and systematized these analyses tools regardless of their type or analysis approach. The literature lacks an organized survey of Ethereum blockchain-based analysis tools covering all the tools. Systematic study methods of Kitchenham et al. [12] and Peterson et al. [13] are used for defining the following research questions:

- **Research Question 1:** What are the static analysis tools available for Ethereum blockchain smart contracts?
- **Research Question 2:** Which dynamic analysis tools are available for the Ethereum blockchain smart contract?
- **Research Question 3:** For Ethereum blockchain smart contracts, what kind of analysis approaches are employed by static/dynamic analysis tools?
- **Research Question 4:**What are the five most common vulnerabilities detected by analysis tools?

### D. INCLUSION AND EXCLUSION OF ARTICLES

To address the research questions, we identified 670 research articles from Web of Science (WoS) that are published between 2016 to 2021. Out of these research articles, 525 articles are excluded based on exclusion criteria, and 132 articles are included based on inclusion criteria. Duplicated, survey, and review articles are excluded from the selected articles. Also, articles in which only tools comparisons are presented are also avoided. Mainly those papers are selected which contain Ethereum in their abstracts.

### E. CONTRIBUTIONS

This paper contributes a systematic review of analysis tools for Ethereum blockchain smart contracts from 2016 to December 2021. This work provides a thorough understanding of the analysis tools for Ethereum smart contracts. The main contributions of this paper are as follows:

1) A systematic review of Ethereum smart contracts analysis tools is presented.
2) The analysis tools are categorized into static and dynamic analysis categories. These categories are further divided into subcategories based on the input type of the tools, such as solidity code, EVM byte code, or both.
3) Different sources code analysis techniques are studied, such as taint analysis, symbolic execution, and fuzzing techniques.
4) In total, 86 security analysis tools in Ethereum blockchain smart contract are analyzed regardless of tool type and analysis approach.
5) Finally, the paper highlights some challenges and future recommendations in the field of Ethereum smart contracts.

### F. PAPER OUTLINE

The remaining structure of the article is as follows : Section II briefly describes some famous vulnerabilities associated with Ethereum blockchain smart contracts, Section III illustrates a detailed description of all Ethereum smart contract analysis tools, Section IV presents a comparison with related work, limitations of the present survey, and possible future research directions. Finally, Section V concludes this study by exhibiting an outline of the contributions.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



## II. SECURITY VULNERABILITIES IN ETHEREUM BLOCKCHAIN SMART CONTRACT

Several researchers presented many types of vulnerabilities [47] associated with Ethereum blockchain smart contract [32, 33, 34, 35] in literature. Li et al. [30] surveyed 20 different-different vulnerabilities, Zhu et al. [31] studied 11 types of vulnerabilities, Luu et al. [9] presented security vulnerabilities in their survey, Atzei et al. [145] studied some specific security vulnerabilities, Tang et al. [45] presented 15 security vulnerabilities, Huashan Chen et. al [46] presented 40 vulnerabilities under several root causes. Following are some of the most discussed Ethereum smart contract vulnerabilities

- **Timestamp Dependency [9]:** It occurs when the block timestamp is used to trigger a condition to initiate the execution of a critical operation. If the block timestamp is used to create randomness, it can be compromised by the malicious attacker.
- **Reentrancy [24, 25, 26]:** It is one of the most famous vulnerabilities related to the Ethereum smart contract. It was first reported in 2016 from the renowned DAO attack [27], which caused a loss of 60 million US dollars. It occurs due to repeatedly calling of a function of the caller contract by the callee contract before the function completed its execution. Due to this, the state variables of the function are not updated after each function call and create a very serious issue.
- **Transaction Ordering Dependency [22]:** It occurs due to concurrent order of transaction execution. The miners decide the transaction execution sequence. A malicious miner may select or not select a specific transaction to mine, which ultimately results in wrong execution results if the transactions are dependent on each other.
- **tx.origin [8]:** The "tx.origin" is used for authorization purposes. Still, the attacker can utilize the same for a phishing attack. "msg.sender" should be used in place of "tx.origin" for authentication purposes.
- **Block-hashBlock Number [8, 20]:** It also occurs when the block has, or block number is used to generate randomness by generating random numbers. But a miner can act maliciously to manipulate or modify the same for its benefit.
- **Gas Related Issues [14, 27, 28]:** There can be several gas-related issues like sending a transaction with insufficient gas, useless code in the smart contract, or gas costly loops present in the contract. Gas is used as a transnational fee to execute instructions of the smart contract like each type of operation requires a different gas, which is charged in Ether (Wei-smallest unit of Ether).
- **Delegate Call [29]:** It was first reported in one of the other famous attacks on the Ethereum smart contract Parity wallet. It occurs because of using EVM opcodes maliciously by the callee contract to update the state variables of the caller's contract.
- **Arithmetic UnderflowOverflow [21]:** It occurs due to solidity data type range, which means values of arithmetic operation cross the range limit of data type on upside or downside and give a chance to the attacker to manipulate the values of state variables. It was first reported in attacks on BEC tokens.
- **Freezing Ether [45]:** It was also reported the first attack against the Parity wallet. It occurs because the user of the contract cannot spend money due to the dependency on other contract's money spending function, and the function doesn't allow to spend the money.
- **Unchecked Call [46]:** It occurs due to improper exception handling in the solidity code. When the return value of execution is not adequately checked and proper measures are not taken, the malicious user can benefit from that.
- **Self Destruct [30]:** The "self destruct" is a method the owner uses to kill its contract to delete its byte code and free the storage. But the attacker can kill a contract if there is poor authentication in the contract. It was first reported in the Parity wallet bug.
- **Access Control [31]:** It is the case when inadequate authorization or authentication is used while coding the smart contract. An attacker can maliciously use the same to access the critical functions.
- **Denial of Service [14, 23]:** It occurs due to the malicious intention of the user to disrupt the execution of another user's caller contract by reverting the call every time.

## III. ANALYSIS TOOLS FOR ETHEREUM SMART CONTRACT

Smart contracts must execute according to the user's need or owner of the smart contract. Security vulnerabilities [30, 31, 45, 46] or bugs may not allow the smart contract to perform its operation for which it was coded and be the reason for tremendous losses. Analysis tools [68, 74, 114, 127] are necessary to check and analyze the smart contract for any security flaw. Because the immutability [101] nature of the blockchain does not allow any type of alteration in the code of smart contract after deployment of the same on the blockchain. This Section presents the categorization of Ethereum smart contract analysis tools into two main categories.

Further, these two main categories are divided into two subcategories based on the initial input on the tool for analysis purposes. Some of the tools take both Solidity and Byte code as input. One tool named FSolidM [97] generates solidity code by taking input some formal specifications. Figure 2 shows the categorization of Analysis tools for smart contracts associated with the Ethereum blockchain.

Several analysis tools have been invented since 2016. We have considered the tools invented up to November 2021. Figure 3 shows the year-wise evolution of analysis tools for Ethereum blockchain-based smart contracts. The majority of the tools developed to date are static analysis tools. Authors

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



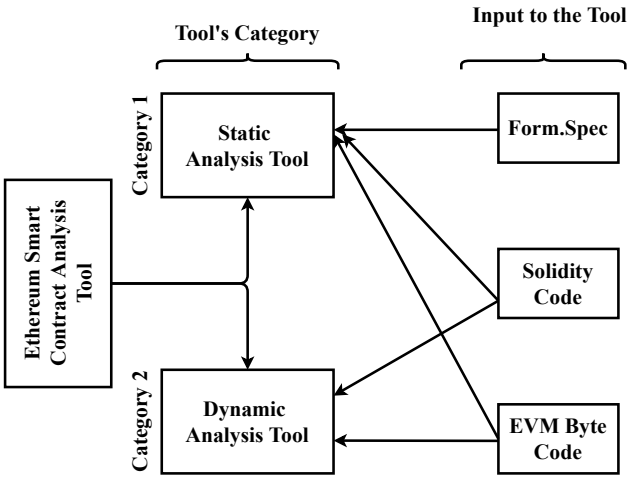


**FIGURE 2.** Categorization of analysis tools based on type of analysis and type of input to the tool

justified in their articles the benefits of their tool's analysis approach.

Figure 4 depicts different-different tools in each category, and figure 5 shows the share of each category of the tool among the total analysis tools invented for Ethereum blockchain-based smart contract. Data used in the figure 5 is collected in our survey.

Now we will give a detailed overview of each tool under each category. First, we will describe static analysis tools under subcategory input to the tool is Solidity code

### A. CATEGORY 1: STATIC ANALYSIS TOOLS

1) Input to the Tool: Solidity code

- **ContractWard [78]:** It is a static analysis tool that takes solidity as input and was invented in 2019. It is an automatic vulnerability finding tool. Wei Wang etàl proposed this system for detecting vulnerabilities at a large level with machine learning algorithms. ContractWard detects six vulnerabilities: Timestamp Dependency, Reentrancy, Arithmetic Overflow and Underflow, Callstack Depth, and Transaction-Ordering Dependence. It depends on the Oyente tool for label generation for each contract with six labels. ContractWard works in the following six steps: Step 1: Collection of smart contracts from Ethereum's official website. Step 2: Transformation of source code to opcode for simplification. Step 3: 1619 bigram features are extracted from the simplified opcodes of step 2. Then each smart contract is labeled with six labels corresponding to each type of vulnerability from C1 to C6. Step 4: For multi-label classification, the OvR algorithm is employed. Step 5: Classification and balancing are done in this step. Step 6: Balanced training sets are used for creating detection models.
- **Echidna [82]:** It is a publicly available open-source static analysis tool that takes solidity or viper code as input and was invented in 2020. It is an Ethereum smart contract fuzzer developed in Haskell, which supports three properties such as user-defined properties, assertion checking, and gas use estimation. Echidna works in two steps: 1. Pre-processing: In this step, it leverages Slither to analyze smart contracts. 2. Fuzzing Campaign: In this step, random transactions are generated, and property violations are detected. Echidna is very easy to use and supports most contract development frameworks. It is very fast to produce results very quickly.
- **Eth2Vec [86]:** It is a command-line-based static analysis tool, invented in 2021. It employs the machine learning approach for analyzing smart contracts to learn the features of vulnerable EVM byte code. It creates a model for feature extraction by training the tool using training data. Then, matching the similarity in the code of EVM and target EVM detects the vulnerabilities.
- **Ethainter [87]:** It is a static analysis tool invented in the year 2020. It analyses information flow with data sanitization in Ethereum smart contracts. It enhances the tainted information flow by tainting the guard conditions. Ethainter efficiently detects Seif Destruct, Delegate Cal, Unchecked, variable tainting type vulnerabilities.
- **EthVer [143]:** It is a static analysis tool invented in the year 2020. It performs automatic formal verification of smart contracts. Then tool translates the smart contract into formal models known as the Markov decision process and then verifies the same using a formal verification tool known as PRISM model checker.
- **FEther [96]:** It is a publicly available static analysis tool implemented in Coq and invented in 2019. It takes an input of solidity code and analyzes the same using a combination of symbolic execution and high order logic theorem proving. FEther's functional correctness is verified in Coq. FEther's processing is divided into three parts: The first one is a Parser, the second one is an ISA based on Lolisa semantics, and the third one is a validation checking mechanism.
- **FSPVM [98]:** It is a static analysis tool implemented in Coq and invented in 2020. It supports ERC-20 token standard. FSPVM symbolically analyses the Ethereum smart contract solidity code and checks for security vulnerabilities by employing Hoare style logic in Coq. FSPVM combines the virtual machine platforms with static security issues checking, based on an extension of Curry-Howard isomorphism.
- **GasGauge [99]:** It is a static analysis tool developed in the year 2021. It employs fuzz testing to detect vulnerabilities. It efficiently detects out of gas denial of service vulnerability in Ethereum blockchain-based smart contracts. The tool is divided into three phases: the Detection phase, Identification phase, and Correction phase. All the stages of the tool can work alone or together to analyze Ethereum smart contracts.
- **Gastap [103]:** It is a static analysis tool developed in

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



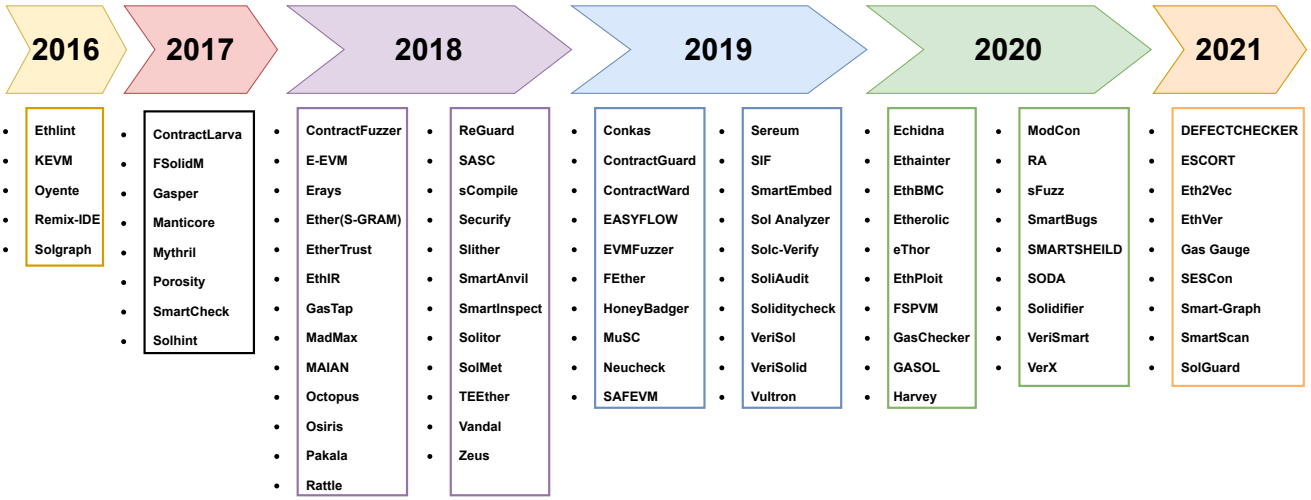


**FIGURE 3.** Year wise evolution of Analysis tools for Ethereum blockchain based smart contract

2018. This tool takes input for analyzing the EVM byte code or disassembled EVM byte code or solidity code. It deduces the gas bounds requirements for its functions and finally compares the deduced gas requirement with the genuine gas limit paid by the user. The difference between the deduced gas limit and the actual gas limit paid will show the gas-related vulnerabilities.

- **MuSc [111]:** It is a publicly available open-source static mutation testing tool implemented in Java and invented in 2019. MuSc generates mutants of smart contracts at the abstract syntax tree level. These AST-generated mutants are converted to source code for compilation, execution, and testing. It also supports the user-defined test net.
- **NeuCheck [112]:** Ning Lu et. al. proposed this static analysis tool in 2019, which takes solidity as input. NeuCheck is developed in Java. To avoid missing semantics and the transformation of solidity code to an intermediate representation, NeuCheck introduced the syntax tree in the syntactical analyzer. For this transformation, NeuCheck takes use of a solidity parser which is developed in ANTLR. NeuCheck works in three steps: 1. Parse the source code to an intermediate representation. 2. Then, the second step for analyzing the syntax tree utilizes the open-source XML library working. 3. The third and last step notifies users about the location of security issues in the smart contract.
- **Pakala [116]:** It is a publicly available open-source static analysis tool implemented in Python and invented in 2018. It is a symbolic execution tool for Ethereum Virtual Machine byte code. It used Z3 as an abstraction layer and added a SHA3 layer on top of it. It employs two steps to detect vulnerabilities. In the first step, it executes byte code to find outcomes, and in the second step, it analyses the outcome to find something terrible corresponding to a vulnerability.
- **Remix IDE [117]:** It is an open-access tool, which provides an easy way to write and analyze smart contracts in solidity code. It is a JavaScript implementation of Ethereum Virtual Machine with a browser-based user's interface, invented in 2016 and written in JavaScript. It can be used either in the web version or desktop version. Its source code is available in GitHub Repository. Presently there are 21 analysis modules under four categories are listed in Remix IDE v0.10.1, which are Security, Gas Economy, ERC Miscellaneous. Remix-analyser is a library that works beneath of RemixIDE Solidity Static Analysis plugin.
- **SASC [129]:** It is a static analysis tool invented in 2018 and developed in C (83%), Python (15.7%), Mark file(0.5%). It comprises two main functions a) Invocation Relationship Analysis b)Logic Risk Expansion and Location. This tool detects timestamp dependency, tx.origin, divide by zero vulnerabilities.
- **sCompile [130]:** It is a static analysis tool invented in 2018 and developed in Python. This tool is based on automatically identifying monetary transaction's related critical program paths and concentrating on those that possibly contravene essential properties.
- **SESCon [133]:** It is a static analysis tool invented in the year 2021. It employs taint analysis to analyze the Ethereum smart contracts. The tool has three main modules: XPath module, Vulnerable patterns modules, and Taint module. The XPath module takes an input of the solidity code and converts the same to an abstract syntax tree. The Vulnerable pattern module creates vulnerable patterns from vulnerable smart contracts. The Taint module takes input from the above modules and products the vulnerability report.
- **SIF [135]:** It is a publicly available open-source static analysis tool implemented in C++ and invented in 2019. Apart from analysis, SIF also supports query instrumen-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



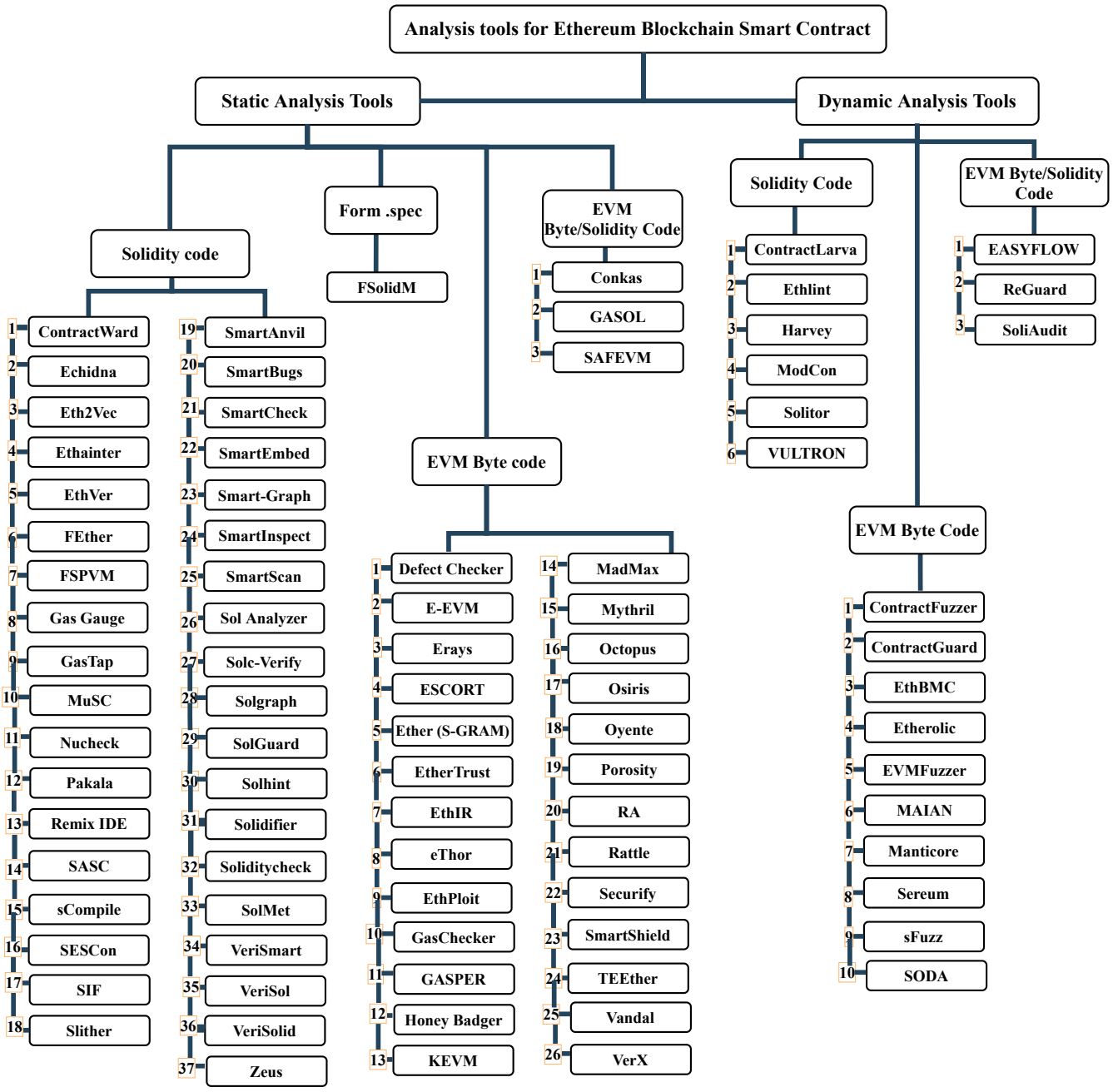


**FIGURE 4.** Categorywise Ethereum smart contract analysis tools

tation and code generation at the abstract syntax tree level. It takes an input of abstract syntax tree generated by solidity compiler and user-defined query for code instrumentation and finally generates instrumented solidity code. It detects arithmetic Overflow or Underflow.

- **Slither [136]:** It is a publicly available open-source static analysis framework invented in 2018 and developed in Python. It takes solidity code as input to analyze. It uses an intermediate representation known as SlithIR. The Slither employs data flow analysis and taints tracking approaches to detect vulnerabilities. It can be used for automated vulnerabilities detection, automated optimization detection, code understanding, and assisted code review. The open-source version of this tool detects approximately 20 bugs like shadowing, uninitialized variables, re-entrancy, suicidal contracts, locked ether, or arbitrary sending of ether.
- **SmartAnvil [137]:** It is a publicly available open-source platform invented in 2018 and developed in Smalltalk. It is constructed around various modules to cover the multiple aspects of smart contract analysis. SmartAnvil platform contains three components' tools: 1) SmaCC-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



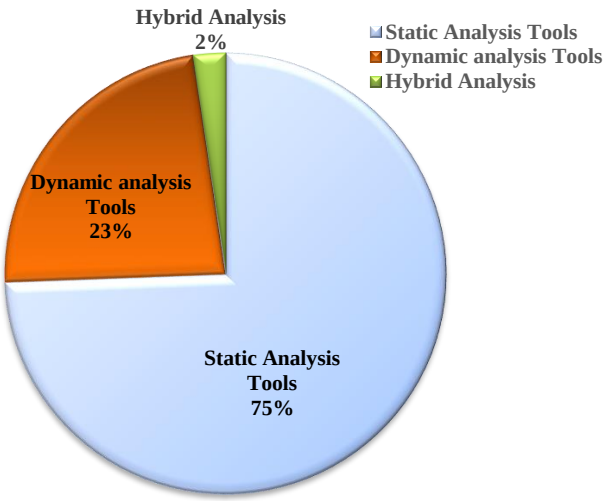


**FIGURE 5.** Category-wise share of Ethereum smart contract analysis tools

Solidity: a parser used to represent or support solidity smart contract's static code. 2) SmartInspect: It is used to inspect the internal state of the Solidity smart contract. 3) Ukulele: It is a query language that helps to fetch required data from the blockchain.

- **SMARTBUGS [138]:** It is a publicly available open-source static analysis framework implemented in Python and invented in 2020. It supports ten tools for analyzing the smart contract. This tool comprises 5 components: command-line interpreter, tool's configuration, docker's image of tools, dataset, and SMARTBUGS runner. Apart from the command line interface, the SMARTBUGS also has a web interface to interact.
- **SmartCheck [139]:** It is a publicly available open-source static analysis tool invented in 2017 and developed in Java. SmartCheck employs a lexical and syntactical analysis approach to analyze the smart contract. An XML parse tree is generated as an intermediate representation using ANTLR (a parser generator) and a custom Solidity grammar. XPath queries are used to process intermediate representation for detecting vulnerabilities patterns. It detects approximately 20 types of vulnerabilities like implicit visibility level, compiler version not fixed, arithmetic division, style guide violation, etc.
- **SmartEmbed [140]:** It is a publicly available open-source static analysis tool implemented in JavaScript and invented in 2019. It is a web-based service tool that detects repetitive contracts. The core component of SmartEmbed is the similarity checker, which takes an input of bug embedding matrix, code embedding matrix, and embedding vector and finally outputs the bug report and clone report.
- **Smart-Graph [141]:** It is a static analysis tool invented in the year 2021. It takes an input of the solidity source code and creates a graphical visualization. The tool has a web-based graphical user interface that is very easy to use and can be accessed using any browser. At the web GUI the tool takes the smart contract address and generates the graphical diagram of the same.
- **SmartInspect [57]:** It is a static analysis tool implemented in Pharo and invented in 2018. It is a mirror-based reflection system. It inspects the known smart contracts at the source code level to analyze the instructiveness and distribution. The reflective approach of SmartInspect permits the user to view the content of any contract without needing to redeploy it.
- **SmartScan [58]:** It is a static/dynamic analysis tool invented in the year 2021. For detecting the denial of service or DoS vulnerability, it combines static and dynamic analysis. SmartScan works in two steps: First, it statically analyses the smart contract to detect denial of service vulnerability-related patterns. Then, the second step uses dynamic analysis to confirm their exploitability.
- **SolAnalyzer [61]:** It is an open-source static analysis framework invented in 2019 and developed in GO. It allows fully automatic analysis of Ethereum smart contracts and reduces false positives. SolAnalyzer detects vulnerabilities in three phases Phase 1). Instrumentation with assertion via Solidity Instrumentation Framework (SIF). Phase 2). Input generation for instrumented smart contracts. Phase 3). Execution in the Ethereum virtual machine and analysis of instrumented contracts. For checking the efficiency and effectiveness of SolAnalyzer, there is another component in this framework named MuContract, which creates several faulty versions of original smart contracts by seeding artificial vulnerabilities.
- **Solc-Verify [62]:** It is a publicly available open-source static analysis tool invented in 2019 and developed in C++ and Solidity. It employs formal verification methods to analyze Ethereum blockchain-based smart contracts. Very easy to integrate with other developer tools. It verifies Solidity smart contracts with a modular software verification approach. Solc-Verify can be employed as an add-on to the open-source Solidity compiler. Solc-Verify detects re-entrancy and integer overflow/underflow vulnerabilities.
- **Solgraph [118]:**It is a publicly available open-source static analysis command-line tool invented in 2016 and developed in JavaScript. Solgraph visualizes the control flow of the function in a Solidity smart contract. It generates a DOT graph to depict the control flow of the functions. DOT is a graphical description language used to visualize functions' control flow and show the relations between the objects. Solgraph uses this DOT graph to identify potential security vulnerabilities in solidity smart contracts.
- **SolGuard [144]:** It is a static analysis tool invented in the year 2021. It was developed by extending the existing static analysis tool named Solhint. It mainly

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



detects external call-related vulnerabilities by checking the order of the state variables, address type parameters, delegate call invocations, and patterns related to denial of service in the smart contracts related to decentralized robotic applications.

- **Solhint [122]:**It is a publicly available open-source static analysis command-line tool invented in 2017 and developed in Java. Solhint uses an antlr4-based implementation of the Solidity parser that enables efficient parsing and validation performance. The tool has flexible configuration options like using a predefined set of rules, a default customized rule set, and code-level configuration rule management. Solent uses three major commands 1) **/*.sol: by this command, it receives a list of file patterns to analyze. 2)stdin: It provides validating source code to standard input. 3) init config: It creates a basic configuration file, which can also be customized if needed.
- **Solidifier [64]:** It is a static analysis tool developed in the year 2020. This tool takes input for analysis of the solidity code. Rather than finding specific behavioral patterns, it detects errors and bad states that do not conform to the developer's intent or detects the falsifying behavioral properties, which the developers can correct.
- **Soliditycheck [65]:** It is a publicly available static analysis tool invented in 2019 and developed in C++. It uses regular expressions to locate security problems in smart contracts. Soliditycheck's main processing is divided into four steps: 1)Formatting the codes. 2) Keywords filtering from the formatted code. 3) Detection and prevention. 4) Detection report and preventive contract. At the end of the fourth step, it shows a detection report of 18 types of security problems except for re-entrancy and integer overflow problem and outputs contract that prevent problems after inserting code.
- **SolMet [67]:** It is a publicly available open-source static analysis tool invented in 2018 and developed in Java. It is a static source code metrics generator to measure smart contracts' size and complexity attributes. Parsing the solidity source code uses a generated parser which the modified version of antlr4 grammar [https://github.com/solidityj/solidity-antlr4]. SolMet proposes the following source code metrics for a smart contract: SLOC, LLOC, CLOCNF, WMC, and NL.
- **VeriSmart [70]:** It is a publicly available open-source static analysis tool implemented in OCaml and invented in 2020. It is an automatized and scalable analysis tool based on a domain-specific smart contract verification language. It starts analysis from basic path construction, the generation of verification conditions, then collecting unproven paths, then performing domain-specific refinement, then processing, and at last efficient validity/invalidity checking. It detects all CVE related vulnerabilities.
- **VeriSol [71]:** It is a publicly available open-source static analysis tool invented in 2019 and developed in C#. It is a general-purpose solidity verifier used to check the assertion in a solidity smart contract. VeriSol converts the Solidity program's semantics to Boogie, a low-level intermediate verification language. It uses the CORRAL [24], a bounded model checking tool that helps Boogie generate witnesses to assertion violations.
- **VeriSolid [72]:** It is a static analysis tool implemented in JavaScript and invented in 2019. It is a formal verification framework that allows the creation of solid source code from validated prototypes which ultimately allows the correct design development of the smart contract. It is constructed on top of another static analysis tool named FSolidM.
- **Zeus [75]:** It is a company tool, developed in 2018 by IBM Research India for static analysis of the solidity smart contracts. It is a symbolic model checking framework consisting of three components: policy builder, source code translator, and verifier. Solidity smart contract and policies against which the smart contract is to be verified are taken as input. It then inserts policies predicates as assertions at correct program points. Then this policy asserted code is converted to LLVM bytecode. Then at the end the verifier checks for policy violations.

Table 1 presents a comparative analysis of static analysis tools with solidity code as input. The comparative analysis is based on some criteria like either the tool is a company tool or academic tool, source code of the tool is available or not (means source code is freely available to access or evaluate the tool on Github or some other web location), the tool has either command-line interface or web interface, the year of advent and the implementation language or development language of the tool.

### 2) Input to the Tool: EVM Byte Code

- **DEFECTCHECKER [80]:** It is a static analysis tool invented in the year 2021 and developed in Java. It is based on symbolic execution and has four processing sections: Inputter, CFG Builder, Feature Detector, and Defect Identifier. It takes as input the byte code and then extracts the opcodes from that. Then all the opcodes are categorized into different-different categories for symbolic execution. Then a control flow graph is constructed to detect the defects in the smart contract.
- **E-EVM [83]:** It is a publicly available open-source static analysis tool invented in 2018 and developed in Python. It visualizes the emulated execution of the smart contract on Ethereum Virtual Machine. It works on the byte code of the smart contract by displaying control flow, opcode, and stack for each step of the contract's program execution. The front end of E-EVM is written in JavaScript, and the back end is written in Python.
- **Erays [84]:** It is a publicly available open-source static analysis tool invented in 2018 and developed in Python.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



**TABLE 1.** Comparative analysis of Static Analysis Tools (with Solidity code as Input)

| Tool | Source Code | Organization | Academic | Command Line Interface | Web Interface | Year | Platform |
|---|---|---|---|---|---|---|---|
| ContractWard | ✗ | ✗ | ✓ | ✓ | ✗ | 2019 | - |
| Echidna | ✓ | ✗ | ✗ | ✓ | ✗ | 2020 | Haskel |
| Eth2Vec | ✗ | ✗ | ✓ | ✓ | ✗ | 2021 | - |
| Ethainter | ✗ | ✗ | ✓ | ✓ | ✗ | 2020 | - |
| EthVer | ✗ | ✗ | ✓ | ✓ | ✗ | 2021 | - |
| FEther | ✓ | ✗ | ✗ | ✓ | ✗ | 2019 | Coq |
| FSPVM | ✗ | ✗ | ✓ | ✓ | ✗ | 2020 | Coq |
| Gas Gauge | ✗ | ✗ | ✓ | ✓ | ✗ | 2021 | - |
| GasTap | ✓ | ✗ | ✓ | ✗ | ✓ | 2018 | Python |
| MuSC | ✓ | ✗ | ✗ | ✓ | ✗ | 2019 | JAVA |
| Neucheck | ✗ | ✗ | ✓ | ✓ | ✗ | 2019 | JAVA |
| Pakala | ✓ | ✗ | ✗ | ✓ | ✗ | 2018 | Python |
| Remix-IDE | ✓ | ✗ | ✗ | ✗ | ✓ | 2016 | Java Script |
| SASC | ✗ | ✗ | ✓ | ✓ | ✗ | 2018 | C (83%), Python (15.7%), Markfile(0.5%) |
| sCompile | ✗ | ✗ | ✓ | ✓ | ✗ | 2018 | Python |
| SESCon | ✗ | ✗ | ✓ | ✓ | ✗ | 2021 | - |
| SIF | ✓ | ✗ | ✗ | ✓ | ✗ | 2019 | C++ |
| Slither | ✓ | ✗ | ✗ | ✓ | ✗ | 2018 | Python |
| SmartAnvil | ✓ | ✗ | ✗ | ✓ | ✗ | 2018 | - |
| SmartBugs | ✓ | ✗ | ✗ | ✓ | ✗ | 2020 | Python |
| SmartCheck | ✓ | Smart Check | ✗ | ✓ | ✗ | 2017 | JAVA |
| SmartEmbed | ✓ | ✗ | ✗ | ✗ | ✓ | 2019 | Java Script |
| Smart-Graph | ✗ | ✗ | ✓ | ✗ | ✓ | 2021 | - |
| SmartInspect | ✗ | ✗ | ✓ | ✓ | ✗ | 2018 | Pharo |
| SmartScan | ✗ | ✗ | ✓ | ✗ | ✓ | 2021 | - |
| Sol Analyzer | ✓ | ✗ | ✓ | ✓ | ✗ | 2019 | GO |
| Solc-Verify | ✓ | ✗ | ✗ | ✓ | ✗ | 2019 | C++, Solidity |
| Solgraph | ✓ | ✗ | ✗ | ✓ | ✗ | 2016 | Java Script |
| SolGuard | ✗ | ✗ | ✓ | ✓ | ✗ | 2021 | - |
| Solhint | ✓ | Protofire | ✗ | ✓ | ✗ | 2017 | JAVA |
| Solidifier | ✓ | ✗ | ✓ | ✓ | ✗ | 2020 | - |
| Soliditycheck | ✓ | ✗ | ✓ | ✓ | ✗ | 2019 | C++ |
| SolMet | ✓ | ✗ | ✗ | ✓ | ✗ | 2018 | JAVA |
| VeriSmart | ✓ | Software Analysis Laboratory, Korea University | ✓ | ✓ | ✗ | 2020 | Ocaml |
| VeriSol | ✓ | ✗ | ✗ | ✓ | ✗ | 2019 | C# |
| VeriSolid | ✓ | ✗ | ✓ | ✗ | ✓ | 2019 | Java Script |
| Zeus | ✗ | ✗ | ✓ | ✓ | ✗ | 2018 | - |

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



It is a reverse engineering tool that analyses EVM byte code of Ethereum blockchain smart contracts. It generates a high-level pseudo-code for the EVM byte code. Erays works in eight steps starting from disassembly from hex string to EVM instructions, then basic blocks, then control flow graph is recovered from these basic blocks, then EVM's stack-based instruction are lifted to registered based instruction. Then it performs data flow optimizations following the aggregation to an intermediate representation. Then control flow structure is recovered using structural analysis algorithms. Then validation is performed to transform the contract into more readable expressions. Erays has limitations like it cannot capture operation on complex types.

- **ESCORT [85]:** It is a static analysis tool invented in the year 2021. It employs a Deep Neural Network (DNN)-based approach to analyze Ethereum blockchain smart contracts vulnerability detection framework. It supports lightweight transfer learning on invisible security issues, thus is extensible and oversimplified. The ESCORT is composed of two components: (i) the First component extracts the features and semantics of the Ethereum smart contract (ii) The second component takes an input of features from the first component and consists of Multiple branch structures. Each branch from this multiple branch structure works on a specific security vulnerability.
- **Ether (S-GRAM) [89]:** It is a semantic-aware security-aware framework. It was developed in Python based on the S-Gram artifact in 2018. To detect vulnerabilities, it works in two phases: the model construction phase and the security auditing phase. It uses a combination of N-gram language modeling and lightweight static semantic labeling to learn statistical regularities of contract tokens and finally capture high-level semantics to predict potential vulnerabilities.
- **EtherTrust [91]:** It is a publicly available open-source automated static analysis tool invented in 2018 and developed in JavaScript. Its analysis is based on the horn clause. For discharging proof obligations, it relies on Z3 theorem prover. It shows a formal guarantee and supports the analysis of EVM byte code. It detects Single entrance and independence from the transaction environment.
- **EthIR [92]:** It is a publicly available open-source static analysis tool invented in 2018 and developed in Python. It is an Ethereum byte code analyzer and depends on Oyente to generate the control flow graph. It converts the control flow graph to a rule-based intermediate representation. It then uses SACO, a high-level static analyzer, to analyze its intermediate rule-based representation of EVM byte code.
- **eThor [93]:** It is an EVM byte code static analyzer invented in JavaScript in 2020. The author employs the HoRSt (specification and implementation framework for static analysis) to implement eThor. eThor is built on the top of the reachability analysis realized by horn clause resolution, which abstracts the contract's execution behavior to query about the abstracted property over abstract executions instead.
- **EthPloit [94]:** It is a static analysis tool invented in the year 2020. This tool uses a fuzzing approach for exploit generation in smart contracts exploit generators based on fuzzing. The workflow of EthPloit is divided into five parts starting from Static analysis, test-case generation, test case execution, trace analysis, and feedback handling. It generates exploits related to Unchecked Transfer Value, Vulnerable Access Control, Exposed secret, etc.
- **GasChecker [100]:** It is a static analysis tool invented in the year 2020. GasChecker mainly works on gas-related bugs in smart contracts. The tool analyses smart contracts based on ten gas inefficient codes or programming patterns. Symbolic execution is employed as GasChecker's analysis approach to detect gas-related security issues in the Ethereum virtual machine byte code.
- **Gasper [102]:** It is a static analysis tool invented in Python in the year 2017. Gasper analyzes the EVM byte code of the smart contract to identify the gas costly pattern. Gasper identifies 7 gas costly patterns in two categories: unnecessary code-related patterns and gas costly loop-related patterns. So, Gasper is a gas costly pattern checker based on symbolic execution and work on byte code.
- **HoneyBadger [105]:** It is a publicly available open-source static analysis tool invented in 2019 and developed in Python. It performs a systematic analysis of honeypot smart contracts. It employs symbolic execution with a defined heuristic for exposing honeypots by investing their pervasiveness, actions, and influence on the Ethereum blockchain. Its structure contains three types of analysis pipeline named symbolic analysis, cash flow analysis, and honeypot analysis. Each type of analysis uses Z3 SMT solver to check the satisfiability of constraints.
- **KEVM [106]:** It is a publicly available open-source static analysis tool invented in 2016 and developed with a mixture of markdown syntax and k specification language. The KEVM formation is divided into two components states. The first one is the active VM state or virtual machine state for executing transactions and contracts. Another one is the network state which records a log of account information.
- **MadMax [107]:** It is a publicly available open-source static analysis tool invented in 2018. It uses Gigahose IR to perform static analysis. Gigahose IR is a lifter that converts low-level Ethereum virtual machine byte code into high-level IR (intermediate representations). MadMax automatically detects gas-focused vulnerabilities. MadMax employs a combination of two analysis approaches. The first is a control-flow-analysis-based

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



decompiler, and the second is declarative program-structure queries. This approach identifies high-level area-specific concepts.

- **Mythril [123]:** It is a publicly available open-source analysis tool implemented in Python programming language in 2017 by ConsenSys, a software engineering leader in the blockchain space. Ethereum Virtual Machine byte code is given as input for analysis in this tool. Mythril not only analyses Ethereum blockchain-based smart contracts but also works for other blockchain platforms. Mythril uses three approaches for analyzing smart contracts: symbolic execution, SMT solving, and taint analysis. It can also be used in combination with other tools.
- **Octopus [124]:** It is a publicly available open-source static analysis tool implemented in Python and invented in 2017 and sponsored by QuoScient Technologies. It is a vulnerability detection model for WASM and blockchain smart contracts. Octopus can work as a disassembler to translate bytecode into assembly representation. It can generate a control flow graph and call flow graph. It employs symbolic execution to find new paths into the program.
- **Osiris [113]:** It is a publicly available open-source static analysis tool implemented in Python and invented in 2018. For detecting arithmetic vulnerabilities, it employs a combination of two approaches, which are symbolic execution and taint analysis. It can detect three types of integer vulnerabilities arithmetic, truncation, and signedness bugs.
- **Oyente [9]:** It is a publicly available open-source static analysis tool implemented in Python and invented in 2016. It is one of the oldest tools which employs symbolic execution for analyzing smart contracts and statically analyzing the program code path by a path. Its main architectural components are CFG builder, Explorer, Core analyzer, Validator. The Explorer and Validator use Z3 bit-vector solver to eliminate provably infeasible traces from consideration.
- **Porosity [115]:** It is a publicly available open-source static analysis tool implemented in C++ and invented in 2017 by Comae technology. It is a decompiler and vulnerability analysis tool for Ethereum blockchain and generates readable solidity syntax contracts. As per the author, the tool is not maintained for a long time, and he suggested using another tool.
- **RA [119]:** It is a static analysis tool invented in the year 2020. The complete form of the RA is "Re-entrancy Analyser." So as per the name, it is a re-entrancy attack hunter. It employs a combinational approach of symbolic execution and constraints solver in two ways, i.e., symbolic simulation of re-entrancy vulnerability and then verification of the same. It also supports the analysis of inter-contract behavior. Its architectural design contains three components CFManager, VM, and Verifier. The CFManager conducts the symbolic simulation process of re-entrancy vulnerability. Verifier assisted by VM executes the vulnerability verification process.
- **Rattle [120]:** It is a publicly available open-source static analysis tool implemented in Python and invented in 2018 Trail of Bits. It is a binary static analysis framework and can analyze deployed smart contracts. It recovers the original control flow graph by a flow-sensitive analysis of EVM byte code. Then it converts the control flow graph into SSA (Single Static Assignment) register form. At last, optimizing SSA removes DUPs, SWAPs, PUSHs, and POPs.
- **Securify [131]:** It is a publicly available open-source static analysis tool implemented in Java and invented in 2018. It is a fully automated security analyzer and indicates the behavior of a smart contract associated with a given feature to check it is either safe or not. The input to this tool is EVM byte code and a set of security patterns. Security employs two steps analysis process. The first step performs the symbolic execution of the contracts dependency graph and extracts specific semantic data. The second step checks for compliance and violation pattern for proving if a property holds or not.
- **SmartSheild [59]:** It is a static analysis tool invented in the year 2020. It is a type of Ethereum virtual machine byte code rectification tool. It rectifies three security vulnerabilities: missing checks for failing external calls, missing checks for out-of-bound arithmetic operations, and state changes after external calls. It extracts semantic information related to Ethereum virtual machine byte code from abstract syntax tree generated from source code and non-rectified EVM byte code. It performs byte code relocation and validation and, in the end, produces rectification reports and rectified contracts by using the information from control flow transformation and data guard insertion.
- **TEEther [14]:** It is a static analysis tool implemented in Python and invented in the year 2018. It is an exploit generation tool for smart contracts. The process of exploit generation is divided into five modules. The first module is a CFG generation module, the second module is a path generation module, the third is a constraint generation module, and the last is an exploit generation module. TEEther uses Z3 as a constraint solver.
- **Vandal [69]:** It is a publicly available open-source static analysis tool implemented in Python and invented in the year 2018. Its analysis pipeline transforms the Ethereum virtual machine byte code to semantic logic relations. It phrases the vulnerability analysis into souffle' which is a declarative language. Vandal's analysis pipeline process is divided into several stages: scrapper, disassembler, decompiler, and extractor, which finally produces the logic relations.
- **VerX [73]:** It is a static analysis tool invented in the year 2020. It verifies the temporal properties of smart contracts. It employs the combination of symbolic exe-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



**TABLE 2.** Comparative analysis of Static Analysis Tools (with EVM Byte code as Input)

| Tool | Source Code | Organization | Academic | Command Line Interface | Web Interface | Year | Platform |
|---|---|---|---|---|---|---|---|
| DEFECTCHECKER | ✗ | ✗ | ✓ | ✓ | ✗ | 2021 | JAVA |
| E-EVM | ✓ | ✗ | ✗ | ✓ | ✗ | 2018 | Python |
| Erays | ✓ | ✗ | ✗ | ✓ | ✗ | 2018 | Python |
| ESCORT | ✗ | ✗ | ✓ | ✓ | ✗ | 2021 | - |
| Ether (S-GRAM) | ✗ | ✗ | ✓ | ✓ | ✗ | 2018 | Python (Based on S-gram artifact) |
| EtherTrust | ✓ | ✗ | ✗ | ✓ | ✗ | 2018 | Java, Javascript |
| EthIR | ✓ | ✗ | ✗ | ✓ | ✗ | 2018 | Python |
| eThor | ✗ | ✗ | ✓ | ✓ | ✗ | 2020 | Java Script |
| EthPloit | ✗ | ✗ | ✓ | ✓ | ✗ | 2020 | - |
| GasChecker | ✗ | ✗ | ✓ | ✓ | ✗ | 2020 | - |
| Gasper | ✗ | ✗ | ✓ | ✓ | ✗ | 2017 | Python |
| HoneyBadger | ✓ | ✗ | ✗ | ✓ | ✗ | 2019 | Python |
| KEVM | ✓ | ✗ | ✗ | ✓ | ✗ | 2016 | Mixture of markdown syntax and K specification language. |
| MadMax | ✓ | ✗ | ✗ | ✓ | ✗ | 2018 | GogaHose IR |
| Mythril | ✓ | ConsenSys | ✗ | ✓ | ✗ | 2017 | Python |
| Octopus | ✓ | quoscient | ✗ | ✓ | ✗ | 2018 | Python |
| Osiris | ✓ | ✗ | ✗ | ✓ | ✗ | 2018 | Python |
| Oyente | ✓ | ✗ | ✗ | ✓ | ✗ | 2016 | Python |
| Porosity | ✓ | Camae | ✗ | ✓ | ✗ | 2017 | C++ |
| RA | ✓ | ✗ | ✗ | ✓ | ✗ | 2020 | Python |
| Rattle | ✓ | Trail of Bits | ✗ | ✓ | ✗ | 2018 | Python |
| Securify | ✓ | Chain Security (Closed Version) | ✗ | ✓ | ✗ | 2018 | JAVA |
| SMARTSHEILD | ✗ | ✗ | ✓ | ✓ | ✗ | 2020 | - |
| TEEther | ✗ | ✗ | ✓ | ✓ | ✗ | 2018 | Python |
| Vandal | ✓ | ✗ | ✗ | ✓ | ✗ | 2018 | Python |
| VerX | ✗ | ✗ | ✓ | ✗ | ✓ | 2020 | - |

cution and abstraction during transaction execution. A new symbolic execution engine for Ethereum virtual machine is used by the VerX, which avoids the shortcomings of the existing execution engine.

### 3) Input to the Tool: EVM Byte Code / Solidity Code

- **Conkas [125]:** It is a publicly available open-source static analysis tool implemented in Python and invented in 2019. The cookies analysis methodology is based on symbolic execution. It takes an input of solidity code or Ethereum virtual machine byte code. Cookies use Z3 as an SMT solver and Rattle for intermediate representation.
- **GASOL [142]:** It is a static analysis tool invented in the year 2020. GASOL is an analysis tool and optimization tool for gas-related issues. After analyzing the selected types of EVM instructions, GASOL returns the upper bound of the cost of execution of the function. This tool estimates the gas cost of a running function and informs the users about any vulnerability related to gas in the same.
- **SAFEVM [128]:** It is a publicly available open-source static analysis tool implemented in Python and invented in 2019. It is a verification tool with a verification engine for the C program. It can take Solidity or EVM byte code input for analysis purposes along with assert and required authentication annotation and outputs a verification result. It depends on Oyente for generating control flow graphs and EthIR framework for generating rule-based representation. It can detect the division by zero, out-of-bounds access vulnerabilities efficiently.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



Table 2 presents a comparative analysis of static analysis tools with EVM byte code as input.

#### 4) Input to the Tool: Form. Spec

- **FSolidM [97]:**It is a publicly available open-source static analysis tool implemented in JavaScript and invented in 2017. It allows defining contract as FSM (Finite State Machine) with the precise and clear-out specification. It is a web-based tool built on top of the WebGME. This tool provides a security plugins mechanism to prevent security vulnerabilities in smart contracts. It is the only tool that generates solidity code according to the specifications defined by the user.

Table 3 summarizes the same type of information as in Tables 1 and 2 for static analysis tools like a year of advent, development programming language, source code availability, etc. Table 4 summarizes the same type of information for the tools with input both solidity code and EVM byte code. Some companies develop some tools. The respective company name is mentioned in front of the respective tool's name for such tools.

Table 4 presents the relationship between the tools (with solidity code as input, EVM byte code, and both respectively) and their checked or detected vulnerabilities and their employed analysis approach. Some tools are only analysis tools. They do not detect or check any vulnerability but analyze the smart contract by code transformation into some other form or by visualizing it into some kind of graphical representation, which makes the analysis very easier. Table 5 depicts the same type of information as presented in Table 4 but for the tools with input either only as solidity code or both the solidity code and EVM byte code.

### B. CATEGORY 2: DYNAMIC ANALYSIS TOOL

#### 1) Input to the Tool: Solidity Code

- **ContractLarva [77]:** It is a publicly available open-source dynamic analysis tool implemented in Haskell and TeX and invented in 2017. It is a runtime verification tool and works on solidity code. This tool instruments the Ethereum smart contract using event triggering and monitoring logic. It uses dynamic event automata for specifying properties that help monitor the events. The tool captures two types of events: control flow events and data flow events.
- **Ethlint [126]:** It is a publicly available open-source dynamic analysis tool implemented in JavaScript and invented in 2016. It was formally known as Solium. It checks the solidity code for style and security issues. It derives ideas from ESLint, a static analyzer for JavaScript code and Solidity Parser.
- **Harvey [104]:** It is a dynamic analysis tool invented in the year 2020. Harvey is a grey-box fuzzer for smart contracts, which is nothing but a lightweight test generation approach to detect vulnerabilities and security bugs. Harvey mainly detects two types of bugs, the first one is assertion violations defined in SWC 110 and the other one is memory access errors defined in SWC 124.
- **ModCon [110]:** It is a dynamic analysis tool implemented in JavaScript and invented in 2020. It is a model-based testing framework, defines test oracles using user-defined models, and works for both permissioned and permission-less blockchain platforms. ModCon has a web-based frontend and JavaScript-based back-end. It takes an input of the smart contract and a test model specification from the user.
- **Solitor [66]:** It is a dynamic analysis tool implemented in Java and invented in 2018. Solitor is short for Solidity monitor. In this tool, the user can specify the behavior using annotations. These annotations can be used at runtime to check whether specific properties hold or not.
- **Vultron [28]:** It is a publicly available open-source dynamic analysis tool implemented in JavaScript and invented in 2019. It proposes an approach to building an oracle to detect irregular transactions over a normal one. A broad spectrum of downstream analysis techniques like testing, fuzzing, verification, and symbolic execution can be enabled by this oracle. Its other name is ContraMaster.

Tables 6, 7, and 8 presents a comparative analysis of dynamic analysis tools with solidity code, EVM byte code and both as input respectively.

#### 2) Input to the Tool: EVM Byte Code

- **ContractFuzzer [76]:** It is a publicly available open-source dynamic analysis tool implemented in GO and invented in 2018. It is a fuzzing tool to detect security vulnerabilities in Ethereum smart contracts. It uses ABI specifications of smart contracts for generating fuzzing inputs. It classifies test oracles to detect security vulnerabilities. Smart contract's run time behavior is logged by instrumenting the Ethereum virtual machine. Finally, these logs are analyzed to find out security vulnerabilities.
- **ContractGuard [79]:** It is a dynamic analysis tool implemented in JavaScript and invented in 2019. It employs a practical anomaly-based intrusion detection system approach. It raises the alarm to the administrators when detecting some abnormal behavior and rolls back the changes in the smart contracts state to the previous safe state.
- **EthBMC [88]:** It is a dynamic analysis tool developed in the year 2020. This tool takes input for the analysis of EVM byte code. It is an automatized vulnerability detector based on symbolic execution. It explores the available state space a program can reach. It encodes the attackers' goal using some constraints, and then that constraint is solved by using the SMT solver. It works efficiently on parity bug vulnerabilities.
- **Etherolic [90]:** It is a dynamic analysis tool implemented in Rust and invented in 2020. Etherolic's anal-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



**TABLE 3.** Comparative analysis of Static Analysis Tools (with both Solidity code and EVM Byte code as Input)

| Tool | Source Code | Organization | Academic | Command Line Interface | Web Interface | Year | Platform |
|---|---|---|---|---|---|---|---|
| Conkas | ✓ | ✗ | ✗ | ✓ | ✗ | 2019 | Python |
| GASOL | ✗ | ✗ | ✓ | ✓ | ✗ | 2020 | - |
| SAFEVM | ✓ | ✗ | ✗ | ✗ | ✓ | 2019 | Python |
| FSolidM | ✓ | ✗ | ✓ | ✗ | ✓ | 2017 | Java Script |

ysis methodology is based on the combination of dynamic taint tracking and console testing to analyze Ethereum virtual machine byte code. It identifies vulnerabilities as well as generates exploits to trigger unknown errors. It can detect Integer Overflow/Underflow, Bad Randomness, Re-entrancy, Locked Ether, Unhandled Exceptions, Denial of Service, Short addresses, etc.

- **EVMFuzzer [95]:** It is a publicly available open-source dynamic analysis tool implemented in Python and invented in 2019. For detecting vulnerabilities, it uses differential fuzzing techniques. It feeds seed contracts into a benchmark EVM and targets EVM to discover the discrepancies in the outcomes. These discrepancies are finally used to detect vulnerabilities by cross-referencing outputs.
- **MAIAN [108]:** It is a publicly available open-source dynamic analysis tool implemented in Python and invented in the year 2018. It employs symbolic analysis and a concrete validation approach. It uses systematic approaches for discovering a violation of specific properties in smart contracts. The specific properties are safety properties and liveness properties.
- **Manticore [109]:** It is a publicly available open-source dynamic analysis tool implemented in Python in 2017 by Trell of Bits. It is a dynamic symbolic execution analysis tool. User customization is allowed in Manticore for analysis purposes. Its architecture is divided into primary and secondary components. The primary components are the Ethereum execution modules and the core engine. The secondary components include the API module, event system module, and SMT-LIB module.

  **Sereum [132]:** It is a dynamic analysis tool implemented in JavaScript and implemented in 2019. Sereum is short of secured Ethereum. It protects deployed smart contracts against re-entrancy vulnerability attacks. It employs the run-time monitoring and validation approach in a backward-compatible way. This tool also employs taint tracking to monitor the execution of a smart contract and monitor the data flow from storage variables.
- **sFuzz [134]:** It is a publicly available open-source dynamic analysis tool implemented in C++ and invented in 2020. It employs the approach of feedback-guided adaptive fuzzing. The test generation problem is transformed into an optimization problem in this approach. Then this optimization problem is solved by using some form of feedback. A genetic algorithm is employed at the top level by this tool.
- **SODA [60]:** It is a publicly available open-source dynamic analysis tool implemented in GO and invented in 2020. SODA is compatible with any blockchain compatible with Ethereum Virtual Machine. It is embedded with eight apps with new methods which can easily detect major vulnerabilities in Ethereum blockchain-based smart contracts like invalid input data, re-entrancy incorrect check for authorization, no check after contract, unexpected function invocation.

### 3) Input to the tool: EVM Byte Code / Solidity Code

Following dynamic analysis tools analyze the Ethereum smart contract by taking as input both the solidity code or EVM byte code.

- **EasyFlow [81]:** It is a publicly available open-source dynamic analysis tool implemented in the GO programming language and invented in 2019. It employs the taint analysis approach to track the propagation of involved units. It monitors the transaction processes using the taint analysis component and declares the smart contract vulnerable in three categories which are "safe", "overflow" and "potential overflow".
- **ReGuard [121]:** It is a dynamic analysis tool implemented in Python and invented in 2018. It is a fuzzing-based analyzer for Ethereum smart contracts. It performs fuzz testing on the smart contract and generates diverse transactions iteratively. It records critical execution traces during the run time and dynamically identifies re-entrancy vulnerability by feeding them to re-entrancy automata.
- **SoliAudit [63]:** It is a dynamic testing tool invented in the year 2019. SoliAudit is a fuzzing and vulnerability analysis tool based on machine learning and fuzz testing approach. It analyses solidity code in machine code, i.e., opcode, to verify 13 kinds of top vulnerabilities: access control, denial of service, bad randomness, front running, arithmetic, time manipulation, unchecked low-level calls, short addresses, re-entrancy. The approach used by this tool does not require expert knowledge or

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



**TABLE 4.** Static analysis tool (with input as solidity code) checked vulnerabilities and analysis approach

| | Checked Vulnerability | | | | | | | | | | | | | Analysis Approach | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Tool | Timestamp Dependancy | Reentrency | *TOD | tx.origin | Blockhash/Block Number | Gas Related Isssues | Delegate Call | **Underflow/Overflow | Freezing Ether | Unchecked Call | Self Destruct | Access Control | Denial of Service | Symbolic Execution | Dis-assembler | Graphic Visualizer | Fuzz Testing | Constraint Solving | Machine Learning | Code Instrumentation | Mutation Testing | Code Transformation | Formal Verification | Abstract Interpretation |
| ContractWard | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Echidna | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Eth2Vec | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Ethainter | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| EthVer | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| FEther | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| FSPVM | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Gas Gauge | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| GasTap | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| MuSC | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| Neucheck | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| Pakala | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Remix-IDE | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| SASC | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| sCompile | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| SESCon | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| SIF | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Slither | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| SmartAnvil | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| SmartBugs | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| SmartCheck | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| SmartEmbed | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ |
| Smart-Graph | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| SmartInspect | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ |
| SmartScan | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| Sol Analyzer | ✓ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Solc-Verify | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Solgraph | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Solguard | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| Solhint | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Solidifier | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Soliditycheck | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| SolMet | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ |
| VeriSmart | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| VeriSol | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| VeriSolid | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Zeus | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

*TOD-Transaction Ordering Dependency, **Related to Arithmetic

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



**TABLE 5.** Static analysis tool (with input as only solidity code or both solidity code and EVM byte code )checked vulnerabilities and analysis approach

| | Checked Vulnerability | | | | | | | | | | | | | Analysis Approach | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Tool | Timestamp Dependancy | Reentrency | *TOD | tx.origin | Blockhash/Block Number | Gas Related Isssues | Delegate Call | **Underflow/Overflow | Freezing Ether | Unchecked Call | Self Destruct | Access Control | Denial of Service | Symbolic Execution | Dis-assembler | Graphic Visualizer | Fuzz Testing | Constraint Solving | Machine Learning | Code Instrumentation | Mutation Testing | Code Transformation | Formal Verification | Abstract Interpretation |
| Conkas | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| DEFECTCHECKER | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| E-EVM | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Erays | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| ESCORT | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Ether (S-GRAM) | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| EtherTrust | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ |
| EthIR | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| eThor | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| EthPloit | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| FSolidM | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| GasChecker | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| GASOL | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Gasper | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| HoneyBadger | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| KEVM | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| MadMax | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Mythril | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Octopus | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Osiris | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Oyente | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Porosity | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| RA | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Rattle | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| SAFEVM | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Securify | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ |
| SMARTSHEILD | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| TEEther | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Vandal | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| VerX | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

*TOD-Transaction Ordering Dependency, **Related to Arithmetic

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



**TABLE 6.** Comparative analysis of Dynamic Analysis Tools with Solidity code as Input

| Tool | Source Code | Organization | Academic | Command Line Interface | Web Interface | Year | Platform |
|---|---|---|---|---|---|---|---|
| ContractLarva | ✓ | ✗ | ✗ | ✓ | ✗ | 2017 | Haskell(70%) TeX(30%) |
| Ethlint | ✓ | ✗ | ✗ | ✓ | ✗ | 2016 | JavaScript |
| Harvey | ✗ | ✗ | ✓ | ✓ | ✗ | 2020 | - |
| ModCon | ✗ | ✗ | ✓ | ✗ | ✓ | 2020 | JavaScript |
| Solitor | ✓ | ✗ | ✓ | ✓ | ✗ | 2018 | Java |
| VULTRON | ✓ | ✗ | ✗ | ✓ | ✗ | 2019 | Java Script |

**TABLE 7.** Comparative analysis of Dynamic Analysis Tools with EVM Byte code as Input

| Tool | Source Code | Organization | Academic | Command Line Interface | Web Interface | Year | Platform |
|---|---|---|---|---|---|---|---|
| ContractFuzzer | ✓ | ✗ | ✗ | ✓ | ✗ | 2018 | Go |
| ContractGuard | ✗ | ✗ | ✓ | ✓ | ✗ | 2019 | Java Script |
| EthBMC | ✓ | ✗ | ✗ | ✓ | ✗ | 2020 | Rust |
| Etherolic | ✗ | ✗ | ✓ | ✓ | ✗ | 2020 | Rust |
| EVMFuzz | ✓ | ✗ | ✓ | ✓ | ✗ | 2019 | Python |
| MAIAN | ✓ | ✗ | ✗ | ✓ | ✓ | 2018 | Python |
| Manticore | ✓ | Trail of Bits | ✗ | CLI and Python API | ✗ | 2017 | Python |
| Sereum | ✗ | ✗ | ✓ | ✓ | ✗ | 2019 | - |
| sFuzz | ✓ | ✗ | ✗ | ✓ | ✗ | 2020 | C++ |
| SODA | ✓ | ✗ | ✗ | ✓ | ✗ | 2020 | Go |

**TABLE 8.** Comparative analysis of Dynamic Analysis Tools with both Solidity code and EVM Byte code as Input

| Tool | Source Code | Organization | Academic | Command Line Interface | Web Interface | Year | Platform |
|---|---|---|---|---|---|---|---|
| EASYFLOW | ✓ | ✗ | ✗ | ✓ | ✓ | 2019 | Go |
| ReGuard | ✗ | ✓ | ✗ | ✓ | ✗ | 2018 | Python |
| SoliAudit | ✗ | ✗ | ✓ | ✓ | ✗ | 2019 | - |

predefined patterns.

Tables 7, 8, and 9 present a comparative analysis of the same type of information as presented in Tables 2, 3, and 4. Table 7 presents the comparative analysis for dynamic analysis tools with solidity code as input. Table 8 presents the comparative analysis for dynamic analysis tools with EVM byte code as input. Table 9 presents the comparative analysis for dynamic analysis tools with input both solidity code and EVM byte code. Table 10 presents the relationship between the tools (with solidity code as input) and their checked or detected vulnerabilities and their employed analysis approach.

## IV. DISCUSSION

This paper presents a systematic review of Ethereum blockchain-based smart contract analysis tools irrespective of their type and analysis approach. For this purpose, we covered 86 analysis tools and referred to 145 research papers from the literature and other online resources from 2016 to 2021. This section covers the comparison of this survey with the related work, limitations of the survey, and the future research directions, which help the researchers and smart contract tools developers to set future research directions in this domain. The most popular top five vulnerabilities checked or detected by most of the tools are re-entrance, arithmetic overflow/underflow, gas-related, timestamp dependency, and transaction ordering dependency. Figure 6 depicts the share of each of these vulnerabilities concerning checking or detecting by static or dynamic analysis tools.

The most popular top five analysis approaches employed by most tools are symbolic execution, fuzz testing, constraint solving, code instrumentation, and code transformation. Figure 7 depicts the share of each of these analysis approaches

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



**TABLE 9.** Dynamic analysis tools checked vulnerabilities and analysis approach

| | Checked Vulnerability | | | | | | | | | | | | | Analysis Approach | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Tool | Timestamp Dependancy | Reentrency | *TOD | tx.origin | Blockhash/Block Number | Gas Related Isssues | Delegate Call | **Underflow/Overflow | Freezing Ether | Unchecked Call | Self Destruct | Access Control | Denial of Service | Symbolic Execution | Dis-assembler | Visualizer | Fuzz Testing | Taint analysis | Machine Learning | Code Instrumentation | Mutation Testing | Model Based Testing | Formal Verification |
| ContractFuzzer | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| ContractGuard | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| ContractLarva | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| EASYFLOW | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| EthBMC | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Etherolic | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Ethlint | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| EVMFuzz | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Harvey | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| MAIAN | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Manticore | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| ModCon | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| ReGuard | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Sereum | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| sFuzz | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| SODA | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| SoliAudit | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Solitor | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| VULTRON | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

*TOD-Transaction Ordering Dependency, **Related to Arithmetic

concerning the use by static or dynamic analysis tools.

We selected some tools from each category and performed an experimental analysis. Some of these chosen tools have already been practically evaluated in the past on different data sets. We used a group of 30 contracts tagged with the top 5 vulnerabilities mentioned in Figure 6 and downloaded them from the SolidiFI Benchmark[146] data set. The SolidiFI Benchmark is a remote data set smart contracts with 9369 tagged vulnerabilities. Figure 8 depicts the average execution time of each selected tool on the 30 smart contracts. The Slither, Solhint, and Smart check perform better in average execution time. The Average Execution time of the Manticore is very high as compared to other tools. Figure 9 shows the detected vulnerabilities results by each tool, and Figure 10 shows the false-positive results of each selected tool on 30 contracts. The performance of the Slither, Mythril, and Oyente is better than other tools chosen for comparison in terms of vulnerability detection. The Slither and Mythril detect the maximum number of vulnerabilities related to re-entrency and arithmetic underflow/overflow issues. The false-positive rate of the Mythril and Securify is high than other selected tools. The false-positive rate of the SmartCheck, and HoneyBadger is low as compared to other tools. VeriSmart, RA, sFuzz, SODA, and VeriSolid are some of the latest tools which have not been explored so much in the past. The false-positive rate of these tools is meager as compared to other tools. The RA and VeriSolid are specific tools for Re-entrency vulnerabilities. The VeriSmart is a particular tool for arithmetic overflow/underflow vulnerabilities.

In case of an attack on smart contracts, no one is liable for any losses due to the decentralized nature of blockchain. Involved parties need to be bound for any loss that occurred due to the legitimate design of the smart contract because the smart contract code permits the breach. The DAO (Decentralized Autonomous Organization) was the first and one of the famous attacks on a smart contract which caused the loss

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



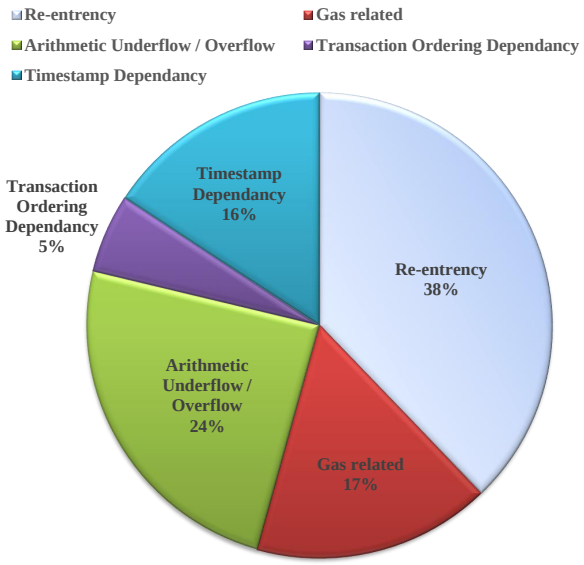


**FIGURE 6.** Top five vulnerabilities share checked or detected by static or dynamic analysis

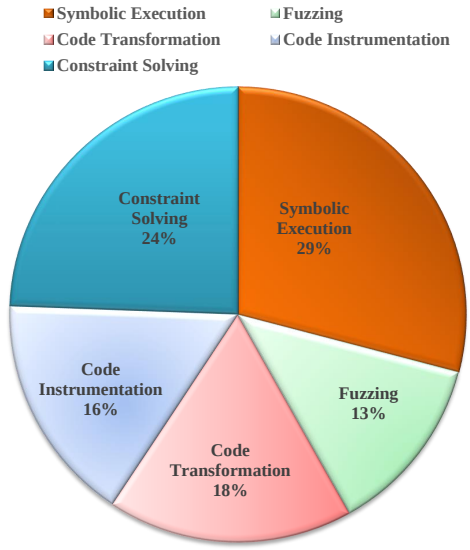


**FIGURE 7.** Top five analysis approaches share with respect to use by static or dynamic analysis

of 60 Million US dollars. The existing tools are unable to deal with the liability issues. Because of this, smart contracts must be analyzed for security issues in advance before being deployed on the blockchain.

### A. COMPARISON WITH RELATED WORK

This systematic review can be considered an extension to the existing surveys in the Ethereum blockchain-based smart contract analysis tools. To fill the research gap, this paper covers a deep insight of 86 analysis tools divided into two main categories static analysis and dynamic analysis. Then the tools are further divided into sub-categories based on input to the tool for analysis. It is found that this review

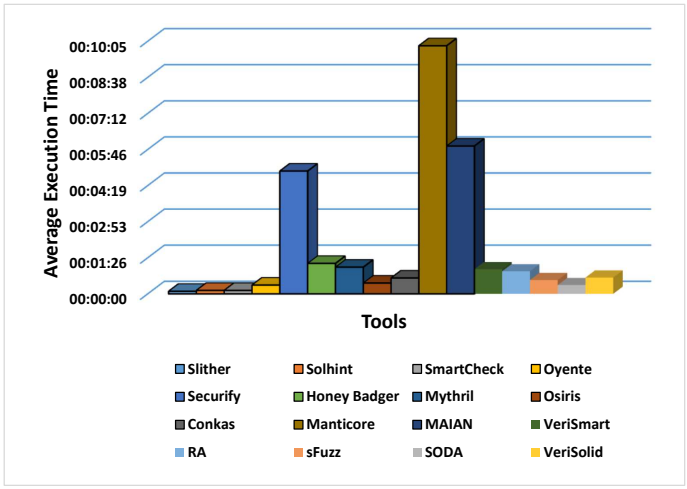


**FIGURE 8.** Average execution time of each tool on 30 contracts

covers most of the tools as compared to any other survey in this domain. To highlight the future research direction in this domain we considered the most recent literature. Figure 8 depicts the comparison of the present survey and related work in terms of the number of tools discussed.

### B. LIMITATIONS

The Ethereum blockchain is the most prominent one, and most of the research has the maximum share of the same. So, our discussion is mainly related to the Ethereum blockchain-based smart analysis tools. But other blockchain platforms also have essential concerns. Our discussion doesn't consider those analysis approaches that give any tool name to their approach. The same is left for future research. Following are some limitations of this review:

1) Our discussion compares the tools with different-different aspects like source code availability, development platform, checked vulnerabilities, etc., but does not cover the high-level description related to the full flesh working of the tools.
2) There are several other analysis tools for other blockchain-based smart contracts like Solana, Hyperledger, etc. Our discussion mainly covers the analysis tools related to Ethereum blockchain smart contract because it has the maximum share in the literature related to smart contracts.
3) This review should not be considered complete because several new analysis tools and approaches are being proposed and developed day by day. Our discussion does not cover the analysis tools proposed in the pre-prints articles.
4) Some research articles don't have any name for the detection approach or model proposed. Such articles are not covered in this review.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



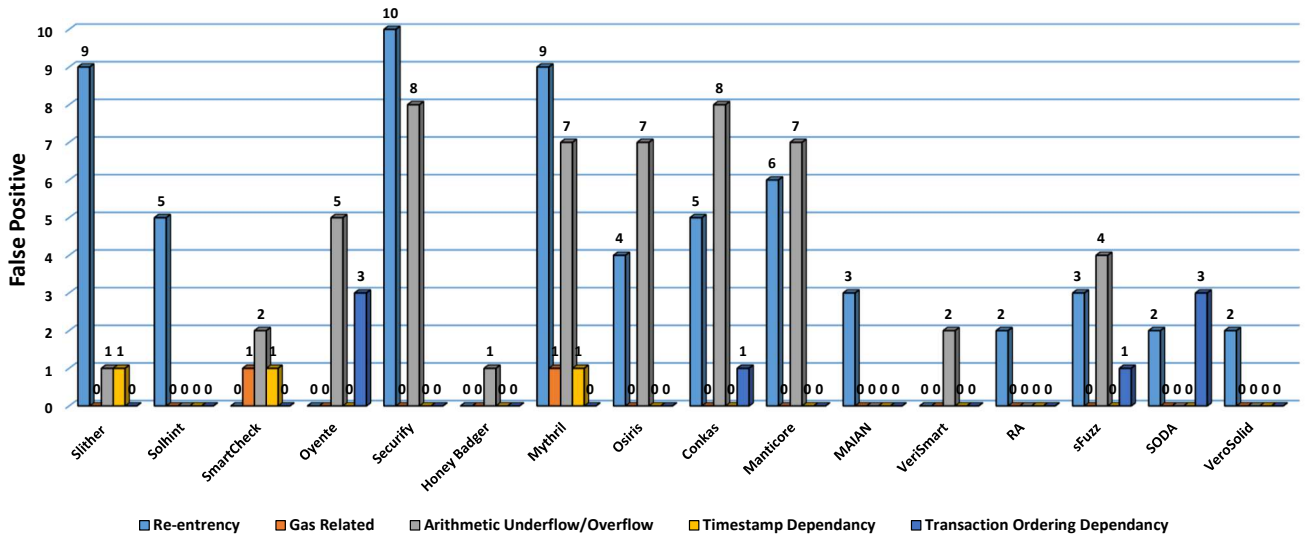


**FIGURE 9.** Top 5 vulnerabilities detection performance of each selected tools

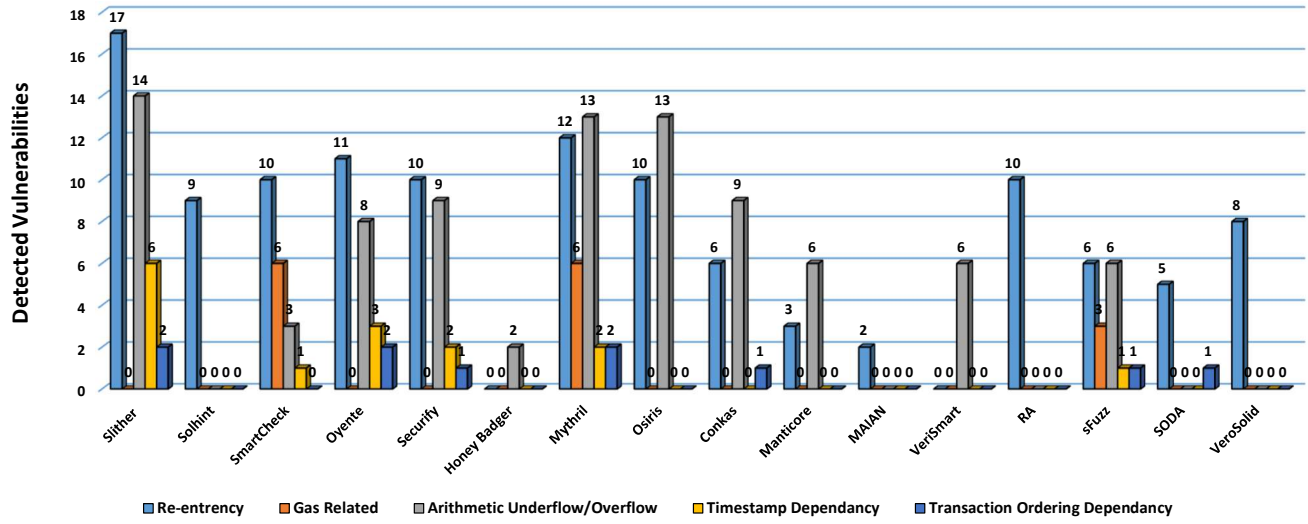


**FIGURE 10.** False positive rate of each tool on top 5 vulnerabilities

### C. FUTURE RESEARCH DIRECTIONS

Blockchain technology is changing day by day at a very fast pace. So several new functionalities and features will be added to the Ethereum blockchain in the near future. So more new security vulnerabilities will be discovered. So it may lead to the development of new and advanced analysis tools for detecting such types of vulnerabilities. No tool is found in the survey which checks or detects all the vulnerabilities presented in the literature. A lot of work is suggested to be done in this direction. Following are some of the future research directions:

1) We found that most of the tools' source code is not openly accessible for evaluation purposes. So, for building trust among the research community, the source code must be openly available for evaluation.
2) Most of the Ethereum smart contract analysis tools mostly check or detect only some of the famous Ethereum smart contract vulnerabilities. A standard benchmark should be suggested by the research community for evaluating the effectiveness of any analysis tool.
3) The majority of the Ethereum smart contract analysis tools employ the static analysis approach. But for the complete analysis of a smart contract, both static and dynamic analysis is necessary to detect or check all the vulnerabilities.
4) The research lacks very few tools for designing and creating new smart contracts. Such types of tools should be developed that will be an aid for the research community for developing safe smart contracts.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3169902, IEEE Access



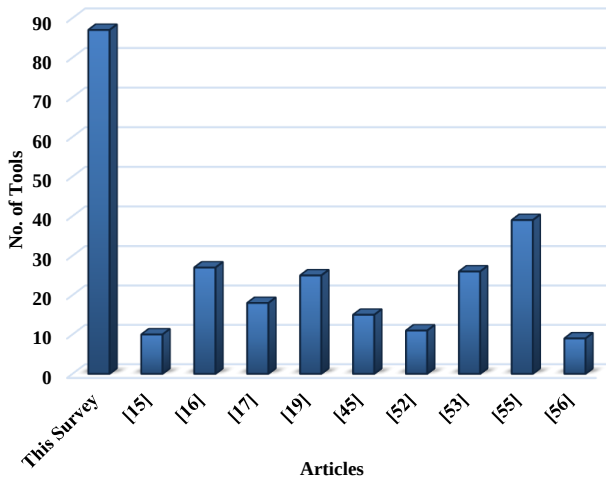


**FIGURE 11.** Comparison of present survey and related work in terms of number of tools discussed

## V. CONCLUSION

The Ethereum smart contracts security analysis is of essential concern, and various analysis tools have been developed for creating safe and secure smart contracts. This paper presented a systematic review of Ethereum smart contracts analysis tools. Initially, 670 articles were selected from various databases such as ACM, IEEE explores, Elsevier, Springer, and Scopus. 132 articles were selected by using various inclusion and exclusion criteria. Besides it, 13 additional articles and online sources were also utilized. 86 security analysis tools in the Ethereum blockchain smart contract were analyzed regardless of tool type and analysis approach. These tools were categorized into static and dynamic analysis tools. After that, different source code analysis techniques were studied, such as taint analysis, symbolic execution, and fuzzing techniques. It was found that the most popular vulnerability checked and detected by most of the static and dynamic analysis tools is 're-entrancy'. The most popular analysis methodology employed by static analysis tools is symbolic execution and fuzz testing by dynamic analysis tools. Most of the tools have utilized static analysis, and some tools were found that employ a combination of static and dynamic analysis, i.e., hybrid analysis. It is concluded that hybrid analysis-based tools have considered more than 95% of security flaws. Finally, the paper highlights some challenges and future recommendations in Ethereum smart contracts.

## REFERENCES

[1] A. Averin and O. Averina, "Review of Blockchain Technology Vulnerabilities and Blockchain-System Attacks," 2019, doi: 10.1109/FarEastCon.2019.8934243.

[2] C. S. Wright, "Bitcoin: A Peer-to-Peer Electronic Cash System," SSRN Electronic Journal. 2019, doi: 10.2139/ssrn.3440802.

[3] C. K. Frantz and M. Nowostawski, "From institutions to code: Towards automated generation of smart contracts," in Proceedings - IEEE 1st International Workshops on Foundations and Applications of Self-Systems, FAS-W 2016, 2016, pp. 210–215.

[4] M. In and F. Of, "Dubai Aims to Be a City Built on Blockchain Where Financial Regulation Goes in a Republican Era," Wall Street Journal, pp. 3–6, 2017, [Online]. Available: https://www.wsj.com/articles/dubai-aims-to-be-a-city-built-on-blockchain-1493086080.

[5] S. Kim and G. C. Deka, Eds., Advanced Applications of Blockchain Technology, vol. 60. Singapore: Springer Singapore, 2020.

[6] M. Singh and S. Kim, "Blockchain technology for decentralized autonomous organizations," in Advances in Computers, vol. 115, 2019, pp. 115–140.

[7] M. Bartoletti and L. Pompianu, "An Empirical analysis of smart contracts: platforms, applications, and design patterns," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2017, vol. 10323 LNCS, pp. 494–509, doi: 10.1007/978-3-319-70278-0_31.

[8] M. Wöhrer and U. Zdun, "Design Patterns for Smart Contracts in the Ethereum Ecosystem," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1513-1520, doi: $10.1109/\text{Cybermatics}_2018.2018.00255$.

[9] L. Luu, D. H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in Proceedings of the ACM Conference on Computer and Communications Security, 2016, vol. 24-28-Octo, pp. 254–269, doi: 10.1145/2976749.2978309.

[10] D. Bayer, S. Haber, and W. S. Stornetta, "Improving the Efficiency and Reliability of Digital Time-Stamping," Seq. II, pp. 329–334, 1993, doi: 10.1007/978-1-4613-9323_24.

[11] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F. Y. Wang, "An Overview of Smart Contract: Architecture, Applications, and Future Trends," in IEEE Intelligent Vehicles Symposium, Proceedings, 2018, vol. 2018-June, pp. 108–113, doi: 10.1109/IVS.2018.8500488.

[12] B. A. Kitchenham, D. Budgen, and O. Pearl Brereton, "Using mapping studies as the basis for further research - A participant-observer case study," Information and Software Technology, vol. 53, no. 6, pp. 638–651, 2011, doi: 10.1016/j.infsof.2010.12.011.

[13] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering," 12th International Conference on Evaluation and Assessment in Software Engineering EASE 2008, 2008, doi: 10.14236/ewic/ease2008.8.

[14] J. Krupp and C. Rossow, "TEETHER: Gnawing at ethereum to automatically exploit smart contracts," in Proceedings of the 27th USENIX Security Symposium,

2018, pp. 1317–1333.

[15] Harz, D., and Knottenbelt, W.J. (2018). Towards safer smart contracts: a survey of languages and verification methods. http://arxiv.org/abs/ 1809.09805.

[16] Angelo, M.D., and Salzer, G. (2019). A survey of tools for analyzing Ethereum smart contracts. In IEEE International Conference on Decentralized Applications and Infrastructures, DAPPCON 2019, Newark, CA, USA, April 4–9, 2019, pp. 69–78.

[17] Liu, J., and Liu, Z. (2019). A survey on security verification of blockchain smart contracts. IEEE Access 7, 77894–77904.

[18] Ante, L. (2020). Smart contracts on the blockchain—a bibliometric analysis and review. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3576393.

[19] Almakhour, M., Sliman, L., Samhat, A.E., and Mellouk, A. (2020). Verification of smart contracts: a survey. Pervasive Mobile Comput. 67, 101227.

[20] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," International Journal of Network Security, vol. 19, no. 5, pp. 653–659, 2017, doi:10.6633/IJNS.201709.19(5).01.

[21] E. Mik, "Smart contracts: terminology, technical limitations and real world complexity," Law, Innovation and Technology, vol. 9, no. 2, pp. 269–300, 2017, doi:10.1080/17579961.2017.1378468.

[22] M. Di Angelo and G. Salzer, "A survey of tools for analyzing ethereum smart contracts," Proc. - 2019 IEEE International Conference on Decentralized Applications and Infrastructures, DAPPCON 2019, pp. 69–78, 2019, doi: 10.1109/DAPPCON.2019.00018.

[23] W. Chen, Z. Zheng, E. C. H. Ngai, P. Zheng, and Y. Zhou, "Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum," IEEE Access, vol. 7, pp. 37575–37586, 2019, doi: 10.1109/ACCESS.2019.2905769.

[24] T. Min, H. Wang, Y. Guo, and W. Cai, "Blockchain games: A survey," IEEE Symposium on Computational Intelligence and Games, CIG, vol. 2019-Augus, pp. 1–8, 2019, doi:10.1109/CIG.2019.8848111.

[25] C. Liu, H. Liu, Z. Cao, Z. Chen, B. Chen, and B. Roscoe, "ReGuard: Finding reentrancy bugs in smart contracts," in Proceedings - International Conference on Software Engineering, 2018, pp. 65–68, doi: 10.1145/3183440.3183495.

[26] J. W. Liao, T. T. Tsai, C. K. He, and C. W. Tien, "SoliAudit: Smart Contract Vulnerability Assessment Based on Machine Learning and Fuzz Testing," in 2019 6th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2019, 2019, pp. 458–465, doi: 10.1109/IOTSMS48152.2019.8939256.

[27] B. Ghaleb, A. Al-Dubai, E. Ekonomou, M. Qasem, I. Romdhani, and L. Mackenzie, "Addressing the DAO Insider Attack in RPL's Internet of Things Networks," IEEE Commun. Lett., vol. 23, no. 1, pp. 68–71, 2019, doi: 10.1109/LCOMM.2018.2878151.

[28] H. Wang, Y. Li, S. W. Lin, L. Ma, and Y. Liu, "VULTRON: Catching vulnerable smart contracts once and for all," Proc. - 2019 IEEE/ACM 41st International Conference on Software Engineering: New Ideas Emerging Results, ICSENIER 2019, pp. 1–4, 2019, doi: 10.1109/ICSE-NIER.2019.00009.

[29] B. C. Gupta and S. K. Shukla, "A Study of Inequality in the Ethereum Smart Contract Ecosystem," 2019 6th International Conference on Internet of Things: Systems, Management and Security IOTSMS 2019, pp. 441-449, 2019, doi: 10.1109/IOTSMS48152.2019.8939257.

[30] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen. (2020). "A survey on the security of blockchain systems", Future Generation Computer Systems, vol 107, bll 841– 853, 2020. https://doi.org/10.1016/j.future.2017.08.020

[31] L. Zhu, B. Zheng, M. Shen, F.Gao, H. Li, and K. Shi, "Research on the Security of Blockchain Data: A Survey", CoRR, vol abs/1812.02009, 2018. doi:10.1007/s11390-020-9638-7

[32] S. Khan, F. Loukil, C. Guegan,E. Benkhelifa, and A.Hani, "Blockchain smart contracts: Applications, challenges, and future trends", Peer-to-Peer Networking and Applications 14, 2901–2925 (2021). https://doi.org/10.1007/s12083-021-01127-0

[33] Z. Wang, H. Jin, W. Dai, K. Choo, and D. Zou, "Ethereum smart contract security research: survey and future research opportunities", Frontiers of Computer Science 15, 152802 (2021). https://doi.org/10.1007/s11704-020-9284-9

[34] Teng Hu, Xiaolei Liu, Ting Chen, Xiaosong Zhang, Xiaoming Huang, Weina Niu, Jiazhong Lu, Kun Zhou, and Yuan Liu, "Transaction-based classification and detection approach for Ethereum smart contract",Information Processing Management, Volume 58, Issue 2, 2021, 102462, ISSN 0306-4573, https://doi.org/10.1016/j.ipm.2020.102462.

[35] A. Bhardwaj,H. Shah, A. Shankar, M. Alazab, M. Kumar, and T. Gadekalllu, "Penetration testing framework for smart contract Blockchain", Peer-to-Peer Netw. Appl. 14, 2635–2650 (2021). https://doi.org/10.1007/s12083-020-00991-6

[36] Anna Vacca, Andrea Di Sorbo, Corrado A. Visaggio, and Gerardo Canfora, "A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges", Journal of Systems and Software, Volume 174, 2021, 110891, ISSN 0164-1212, https://doi.org/10.1016/j.jss.2020.110891.

[37] Z. Liu, P. Qian, X. Wang, Y. Zhuang, L. Qiu and X. Wang, "Combining Graph Neural Networks with Expert Knowledge for Smart Contract Vulnerability Detection," in IEEE Transactions on Knowledge and Data Engineering, doi: 10.1109/TKDE.2021.3095196.

[38] Rameder, H. (2021). "Systematic Review of Ethereum Smart Contract Security Vulnerabilities, Analysis Methods and Tools" [Diploma Thesis,

Technische Universität Wien]. reposiTUm. https://doi.org/10.34726/hss.2021.86784

[39] J. Chen, X. Xia, D. Lo,J. Grundy, and X. Yang, "Maintenance-related concerns for post-deployed Ethereum smart contract development: issues, techniques, and future challenges" Empirical Software Engineering 26, 117 (2021). https://doi.org/10.1007/s10664-021-10018-0

[40] Z. Wan, X. Xia, D. Lo, J. Chen, X. Luo and X. Yang, "Smart Contract Security: A Practitioners' Perspective," 2021 IEEE/ACM 43rd International Conference on Software Engineering (ICSE), 2021, pp. 1410-1422, doi: 10.1109/ICSE43902.2021.00127.

[41] Palina Tolmach, Yi Li, Shang-Wei Lin, Yang Liu, and Zengxiang Li. 2021. "A Survey of Smart Contract Formal Specification and Verification", ACM Comput. Surv. 54, 7, Article 148 , 38 pages. DOI:https://doi.org/10.1145/3464421

[42] S. Ji, D. Kim and H. Im, "Evaluating Countermeasures for Verifying the Integrity of Ethereum Smart Contract Applications," in IEEE Access, vol. 9, pp. 90029-90042, 2021, doi: 10.1109/ACCESS.2021.3091317.

[43] N. A. Noor Aidee, M. G. M. Johar, M. H. Alkawaz, A. Iqbal Hajamydeen and M. S. Hamoud Al-Tamimi, "Vulnerability Assessment on Ethereum Based Smart Contract Applications," 2021 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS), 2021, pp. 13-18, doi: 10.1109/I2CACIS52118.2021.9495892.

[44] Rajesh Gupta, Mohil Maheshkumar Patel, Arpit Shukla, and Sudeep Tanwar, "Deep learning-based malicious smart contract detection scheme for internet of things environment", Computers Electrical Engineering, 2021, 107583, ISSN 0045-7906, doi: 10.1016/j.compeleceng.2021.107583.

[45] Tang X., Zhou K., Cheng J., Li H., and Yuan Y. (2021) The Vulnerabilities in Smart Contracts: A Survey. In: Sun X., Zhang X., Xia Z., Bertino E. (eds) Advances in Artificial Intelligence and Security. ICAIS 2021. Communications in Computer and Information Science, vol 1424. Springer, Cham. doi: 10.1007/978-3-030-78621-2 -14

[46] H. Chen, M. Pendleton, L. Njilla, and S. Xu, "A Survey on Ethereum Systems Security," ACM Computing Surveys, vol. 53, no. 3, pp. 1–43, 2020.doi: 10.1145/3391195

[47] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur and H. -N. Lee, "Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract," in IEEE Access, vol. 10, pp. 6605-6621, 2022, doi: 10.1109/ACCESS.2021.3140091.

[48] R. Lawler, "Someone stole $ 120 million in crypto by hacking a DeFi website," The Verge, 03-Dec-2021. [Online]. Available: https://www.theverge.com, [Accessed: 11-Dec-2021].

[49] Ghaleb and K. Pattabiraman. 2020. How effective are smart contract analysis tools? Evaluating smart contract static analysis tools using bug injection. arXiv:2005.11613

[50] P. Tolmach, Y. Li, S.-W. Lin, Y. Liu, and Z. Li, "A Survey of Smart Contract Formal Specification and Verification," ACM Computing Surveys, vol. 54, no. 7, pp. 1–38, 2022.

[51] D. He, Z. Deng, Y. Zhang, S. Chan, Y. Cheng and N. Guizani, "Smart Contract Vulnerability Analysis and Security Audit," in IEEE Network, vol. 34, no. 5, pp. 276-282, September/October 2020, doi: 10.1109/MNET.001.1900656.

[52] Grishchenko I., Maffei M., and Schneidewind C. (2018) Foundations and Tools for the Static Analysis of Ethereum Smart Contracts. In: Chockler H., Weissenbacher G. (eds) Computer Aided Verification. CAV 2018. Lecture Notes in Computer Science, vol 10981. Springer, Cham. https://doi.org/10.1007/978-3-319-96145-3_4

[53] A. Vacca, A.Sorbo, CA. Visaggio, and G. Canfora, "A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges." Journal of Systems and Software 174 (2021): 110891.

[54] A. PINNA, S. IBBA, G. BARALLA, R.TONELLI, and MICHELE MARCHESI2, "A massive analysis of ethereum smart contracts empirical study and code metrics." IEEE Access 7 (2019): 78194-78213.

[55] B. HU, Z. Zhang, J. Liu,Y. Liu,J. Yin, R. Lu, and X. Lin 2021. A comprehensive survey on smart contract construction and execution: paradigms, tools, and systems. Patterns, 2(2), p.100179. doi:10.1016/j.patter.2020.100179.

[56] T. Durieux, J. F. Ferreira, R. Abreu, and P. Cruz, "Empirical review of automated analysis tools on 47,587 Ethereum smart contracts," Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering, 2020.

[57] S. Bragagnolo, H. Rocha, M. Denker, and S. Ducasse, "SmartInspect: Solidity smart contract inspector", 2018 IEEE 1st International Workshop on Blockchain Oriented Software Engineering, IWBOSE 2018 - Proceedings, vol 2018-January, bll 9–18, 2018.doi = 10.1109/IWBOSE.2018.8327566

[58] N. F. Samreen and M. H. Alalfi, "SmartScan: An approach to detect Denial of Service Vulnerability in Ethereum Smart Contracts", Proceedings - 2021 IEEE/ACM 4th International Workshop on Emerging Trends in Software Engineering for Blockchain, WETSEB 2021, bll 17–26, 2021.

[59] Y. Zhang, S. Ma, J. Li, K. Li, S. Nepal, and D. Gu, "SMARTSHIELD: Automatic Smart Contract Protection Made Easy", SANER 2020 - Proceedings of the 2020 IEEE 27th International Conference on Software Analysis, Evolution, and Reengineering, bll 23–34, 2020.doi:10.1109/SANER48275.2020.9054825

[60] T. Chen, R. Cao, T. Li, X. Luo, G. Gu, Y. Zhang, Z. Liao,H. Zhu, and G.Chen, "SODA: A Generic Online Detection Framework for Smart Contracts", in Proceedings 2020 Network and Distributed System Security Symposium, 2020.doi:10.14722/ndss.2020.24449

[61] S. Akca, A. Rajan, and C. Peng, "SolAnalyser: A Framework for Analysing and Testing Smart Contracts", Proceedings - Asia-Pacific Software Engineering Conference, APSEC, vol 2019-December, bll 482–489, 2019.doi:10.1109/APSEC48747.2019.00071

[62] Á. Hajdu, and D. Jovanović, "SOLC-VERIFY: A modular verifier for solidity smart contracts", Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol 12031 LNCS, bll 161–179, 2020.doi:10.1007/978-3-030-41600-3_11

[63] J. W. Liao, T. T. Tsai, C. K. He, and C. W. Tien, "SoliAudit: Smart Contract Vulnerability Assessment Based on Machine Learning and Fuzz Testing", 2019 6th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2019, bll 458–465, 2019.doi:10.1109/IOTSMS48152.2019.8939256

[64] P. Antonino. and A. W. Roscoe, "Formalising and verifying smart contracts with Solidifier: a bounded model checker for Solidity ", in Proceedings of the 36th Annual ACM Symposium on Applied Computing, 2021, bll 1788–1797.doi:10.1145/3412841.3442051

[65] P. Zhang, F. Xiao, and X. Luo, "SolidityCheck: Quickly Detecting Smart Contract Problems Through Regular Expressions", bll 1–21, 2019.

[66] L. Stegeman, "Solitor: Runtime Veri cation of Smart Contracts", 2018.

[67] P. Hegeds, "Towards analyzing the complexity landscape of solidity based ethereum smart contracts", Proceedings - International Conference on Software Engineering, bll 35–39, 2018.doi:10.1145/3194113.3194119

[68] S. S. Kushwaha, and S. Joshi (2021) An Overview of Blockchain-Based Smart Contract. In: Smys S., Palanisamy R., Rocha Á., Beligiannis G.N. (eds) Computer Networks and Inventive Communication Technologies. Lecture Notes on Data Engineering and Communications Technologies, vol 58. Springer, Singapore. https://doi.org/10.1007/978-981-15-9647-6_70

[69] L. Brent, A. Jurisevic, M. Kong, E. Liu, F. Gauthier, V. Gramoli, R. Holz, B. Scholz, "Vandal: A Scalable Security Analysis Framework for Smart Contracts", bll 1–28, 2018.

[70] S. So, M. Lee, J. Park, H. Lee, en H. Oh, "VERISMART: A highly precise safety verifier for ethereum smart contracts", Proceedings - IEEE Symposium on Security and Privacy, vol 2020-May, bll 1678–1694, 2020.doi:10.1109/SP40000.2020.00032

[71] Wang, Y., Lahiri, S. K., Chen, S., Pan, R., Dillig, I., Born, C., and Naseer, I. (2018). Formal Specification and Verification of Smart Contracts. c. http://arxiv.org/abs/1812.08829

[72] A. Mavridou, A. Laszka, E. Stachtiari, and A. Dubey, "VeriSolid: Correct-by-Design Smart Contracts for Ethereum", Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol 11598 LNCS, bll 446–465, 2019.doi:10.1007/978-3-030-32101-7_27

[73] A. Permenev, D. Dimitrov, P. Tsankov, D. Drachsler-Cohen, and M. Vechev, "VerX: Safety verification of smart contracts", Proceedings - IEEE Symposium on Security and Privacy, vol 2020-May, bll 1661–1677, 2020.doi:10.1109/SP40000.2020.00024

[74] T. M. Hewa, Y. Hu, M. Liyanage, S. S. Kanhare and M. Ylianttila, "Survey on Blockchain-Based Smart Contracts: Technical Aspects and Future Research," in IEEE Access, vol. 9, pp. 87643-87662, 2021, doi: 10.1109/ACCESS.2021.3068178.

[75] S. Kalra, S. Goel, M. Dhawan, and S. Sharma, "ZEUS: Analyzing Safety of Smart Contracts", in Proceedings 2018 Network and Distributed System Security Symposium, 2018, vol 18, bll 5489–5501.doi:10.14722/ndss.2018.23082

[76] B. Jiang, Y. Liu, and W. K. Chan, "ContractFuzzer: Fuzzing smart contracts for vulnerability detection", ASE 2018 - Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering, bll 259–269, 2018.doi:10.1145/3238147.3238177

[77] S. Azzopardi, J. Ellul, and G. J. Pace, "Monitoring smart contracts: Contractlarva and open challenges beyond", Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol 11237, no November, bll 113–137, 2019.doi:10.1007/978-3-030-03769-7_8

[78] W. Wang, J. Song, G. Xu, Y. Li, H. Wang, and C. Su, "ContractWard: Automated Vulnerability Detection Models for Ethereum Smart Contracts", IEEE Transactions on Network Science and Engineering, vol 8, no 2, bll 1133–1144, 2021.doi:10.1109/TNSE.2020.2968505

[79] X. Wang , J. He, Z. Xie, and G. Zhao, Member, IEEE, and Shing-Chi Cheung , Senior Member, IEEE, "Contractguard: Defend ethereum smart contract with embedded intrusion detection", Chinese Journal of Network and Information Security, vol 6, no 2, bll 35–55, 2020.doi:10.11959/j.issn.2096-109x.2020025

[80] J. Chen, X. Xia, D. Lo, J. Grundy, X. Luo, and T. Chen, "DEFECTCHECKER: Automated Smart Contract Defect Detection by Analyzing EVM Bytecode", IEEE Transactions on Software Engineering, vol 5589, no c, bll 1–19, 2021.doi:10.1109/TSE.2021.3054928

[81] J. Gao, H. Liu, C. Liu, Q. Li, Z. Guan, and Z. Chen, "EASYFLOW: Keep ethereum away from overflow", Proceedings - 2019 IEEE/ACM 41st International Conference on Software Engineering: Companion, ICSE-Companion 2019, no April 2018, bll 23–26,

2019.doi:10.3892/mmr.2018.9614

[82] G. Grieco, W. Song, A. Cygan, J. Feist, and A. Groce, "Echidna: Effective, usable, and fast fuzzing for smart contracts", ISSTA 2020 - Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis, bll 557–560, 2020.doi:10.1145/3395363.3404366

[83] R. Norvill, B. B. F. Pontiveros, R. State, and A. Cullen, "Visual emulation for Ethereum's virtual machine", IEEE/IFIP Network Operations and Management Symposium: Cognitive Management in a Cyber World, NOMS 2018, bll 1–4, 2018.doi:10.1109/NOMS.2018.8406332

[84] Y. Zhou, D. Kumar, S. Bakshi, J. Mason, A. Miller, and M. Bailey, "Erays: Reverse engineering Ethereum's opaque smart contracts", Proceedings of the 27th USENIX Security Symposium, bll 1371–1385, 2018.

[85] O. Lutz, H. Chen, H. Fereidooni, C. Sendner, A. Dmitrienko, A. Sadeghi, and F. Koushanfar ESCORT: Ethereum Smart COntRacTs Vulnerability Detection using Deep Neural Network and Transfer Learning, vol 1. Association for Computing Machinery, 2021.

[86] N. Ashizawa, N. Yanai, J. P. Cruz, and S. Okamura, "Eth2Vec: Learning Contract-Wide Code Representations for Vulnerability Detection on Ethereum Smart Contracts", BSCI 2021 - Proceedings of the 3rd ACM International Symposium on Blockchain and Secure Critical Infrastructure, co-located with ASIA CCS 2021, bll 47–59, 2021.doi:10.1145/3457337.3457841

[87] L. Brent, N. Grech, S. Lagouvardos, B. Scholz, and Y. Smaragdakis, "Ethainter: A smart contract security analyzer for composite vulnerabilities", Proceedings of the ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI), bll 454–469, 2020.doi:10.1145/3385412.3385990

[88] J. Frank, C. Aschermann, T. Holz, "ETHBMC: A bounded model checker for smart contracts", Proceedings of the 29th USENIX Security Symposium, bll 2757–2774, 2020.

[89] H. Liu, C. Liu, W. Zhao, Y. Jiang, and J. Sun, "S-gram: Towards semantic-aware security auditing for ethereum smart contracts", ASE 2018 - Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering, bll 814–819, 2018.doi:10.1145/3238147.3240728

[90] M. Ashouri, "Etherolic: A practical security analyzer for smart contracts", Proceedings of the ACM Symposium on Applied Computing, no March, bll 353–356, 2020.doi:10.1145/3341105.3374226

[91] I. Grishchenko, M. Maffei, and C. Schneidewind, "EtherTrust: Sound Static Analysis of Ethereum bytecode", Technische Universität Wien, Tech. Rep, bll 1–41, 2018.

[92] E. Albert, P. Gordillo, B. Livshits, A. Rubio, I. Sergey, "EthIR: A Framework for High-Level Analysis of Ethereum Bytecode", Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol 11138 LNCS, bll 513–520, 2018.doi:10.1007/978-3-030-01090-4_30

[93] C. Schneidewind, I. Grishchenko, M. Scherer, and M. Maffei, "EThor: Practical and Provably Sound Static Analysis of Ethereum Smart Contracts", Proceedings of the ACM Conference on Computer and Communications Security, bll 621–640, 2020.doi:10.1145/3372297.3417250

[94] Q. Zhang, Y. Wang, J. Li, and S. Ma, "EthPloit: From Fuzzing to Efficient Exploit Generation against Smart Contracts", SANER 2020 - Proceedings of the 2020 IEEE 27th International Conference on Software Analysis, Evolution, and Reengineering, bll 116–126, 2020.doi:10.1109/SANER48275.2020.9054822

[95] Y. Fu, M. Ren, F. Ma, H. Shi, X. Yang, Y. Jiang,H. Li, and X .Shi, "EVMFuzzer: Detect EVM vulnerabilities via fuzz testing", ESEC/FSE 2019 - Proceedings of the 2019 27th ACM Joint Meeting European Software Engineering Conference and Symposium on the Foundations of Software Engineering, bll 1110–1114, 2019.doi:10.1145/3338906.3341175

[96] Z. Yang, and H. Lei, "FEther: An extensible definitional interpreter for smart-contract verifications in Coq", IEEE Access, vol 7, bll 37770–37791, 2019.doi:10.1109/ACCESS.2019.2905428

[97] A. Mavridou, and A. Laszka, "Tool Demonstration: FSolidM for designing secure ethereum smart contracts", Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol 10804 LNCS, bll 270–277, 2018.doi:10.1007/978-3-319-89722-6_11

[98] Z. Yang, H. Lei, and W. Qian, "A Hybrid Formal Verification System in Coq for Ensuring the Reliability and Security of Ethereum-Based Service Smart Contracts", IEEE Access, vol 8, bll 21411–21436, 2020.doi:10.1109/ACCESS.2020.2969437

[99] B. Nassirzadeh, H. Sun, S. Banescu, and V. Ganesh, "Gas Gauge: A Security Analysis Tool for Smart Contract Out-of-Gas Vulnerabilities", no August, 2021.

[100] T. Chen, Y. Feng, Z. Li, H. Zhou, X. Luo, X. Li, X. Xiao, and X. Zhang, "GasChecker: Scalable Analysis for Discovering Gas-Inefficient Smart Contracts", IEEE Transactions on Emerging Topics in Computing, vol 9, no 3, bll 1433–1448, 2021.doi:10.1109/TETC.2020.2979019

[101] F. Hofmann, S. Wurster, E. Ron and M. Böhmecke-Schwafert, "The immutability concept of blockchains and benefits of early standardization", Proc. ITU Kaleidoscope Challenges Data-Driven Soc. (ITU K), pp. 1-8, 2017.

[102] T. Chen, X. Li, X. Luo, and X. Zhang, "Under-optimized smart contracts devour your money", SANER 2017 - 24th IEEE International Conference on Software Analysis, Evolution, and Reengineering, bll

442–446, 2017.doi:10.1109/SANER.2017.7884650

[103] E. Albert, P. Gordillo, A. Rubio, and I. Sergey, "Running on fumes: Preventing out-of-gas vulnerabilities in ethereum smart contracts using static resource analysis", Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol 11847 LNCS, bll 63–78, 2019.doi:10.1007/978-3-030-35092-5_5

[104] V. Wüstholz, and M. Christakis, "Harvey: A greybox fuzzer for smart contracts", ESEC/FSE 2020 - Proceedings of the 28th ACM Joint Meeting European Software Engineering Conference and Symposium on the Foundations of Software Engineering, bll 1398–1409, 2020.doi:10.1145/3368089.3417064

[105] C. F. Torres, M. Steichen, and R. State, "The art of the scam: Demystifying honeypots in ethereum smart contracts", Proceedings of the 28th USENIX Security Symposium, bll 1591–1607, 2019.http://arxiv.org/abs/1902.06976

[106] E. Hildenbrandt, M. Saxena, N. Rodrigues, X. Zhu, P. Daian, D. Guth, B. Moore, D. Park, Y. Zhang, A. S¸tefanescu, G. Rosu, "KEVM: A complete formal semantics of the ethereum virtual machine", Proceedings - IEEE Computer Security Foundations Symposium, vol 2018-July, bll 204–217, 2018.doi:10.1109/CSF.2018.00022

[107] N. Grech, M. Kong, A. Jurisevic, L. Brent, B. Scholz, and Y. Smaragdakis, "MadMax: Surviving out-of-gas conditions in ethereum smart contracts", Proceedings of the ACM on Programming Languages, vol 2, no OOPSLA, 2018.doi:10.1145/3276486

[108] I. Nikolić, A. Kolluri, I. Sergey, P. Saxena, and A. Hobor, "Finding the greedy, prodigal, and suicidal contracts at scale", ACM International Conference Proceeding Series, bll 653–663, 2018. doi:10.1145/3274694.3274743

[109] M Mossberg, F Manzano, E Hennenfent, Alex Groce, G. Grieco, J. Feist, T. Brunson, and A. Dinaburg, "Manticore: A user-friendly symbolic execution framework for binaries and smart contracts", Proceedings - 2019 34th IEEE/ACM International Conference on Automated Software Engineering, ASE 2019, bll 1186–1189, 2019.doi:10.1109/ASE.2019.00133

[110] Y. Liu, Y. Li, S. W. Lin, and Q. Yan, "ModCon: A model-based testing platform for smart contracts", ESEC/FSE 2020 - Proceedings of the 28th ACM Joint Meeting European Software Engineering Conference and Symposium on the Foundations of Software Engineering, bll 1601–1605, 2020. doi:10.1145/3368089.3417939

[111] Z. Li, H. Wu, J. Xu, X. Wang, L. Zhang, and Z. Chen, "MuSC: A tool for mutation testing of ethereum smart contract", Proceedings - 2019 34th IEEE/ACM International Conference on Automated Software Engineering, ASE 2019, bll 1198–1201, 2019.doi:10.1109/ASE.2019.00136

[112] N. Lu, B. Wang, Y. Zhang, W. Shi, and C. Esposito, "NeuCheck: A more practical Ethereum smart contract security analysis tool", Software - Practice and Experience, vol 51, no 10, bll 2065–2084, 2021. doi:10.1002/spe.2745

[113] C. F. Torres, and J. Schütte, "Osiris", Nature, vol 143, no 3625, bll 674–675, 1939.doi:10.1038/143674d0

[114] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng,and M. Imran, "An overview on smart contracts: Challenges advances and platforms", Future Gener. Comput. Syst., vol. 105, pp. 475-491, 2020.

[115] M. Suiche, "Porosity: A Decompiler For Blockchain-Based Smart Contracts Bytecode", Def Con, vol 25, bl 30, 2017.

[116] Pakala, Aug. 2021, [online] Available:https://github.com/palkeo/pakala

[117] Remix-IDE, June 2021, [online] Available:https://github.com/ethereum/remix-ide

[118] Solgraph, Aug. 2021, [online] Available:https://github.com/raineorshine/solgraph

[119] Y. Chinen, N. Yanai, J. P. Cruz, and S. Okamura, "RA: Hunting for Re-Entrancy Attacks in Ethereum Smart Contracts via Static Analysis", Proceedings - 2020 IEEE International Conference on Blockchain, Blockchain 2020, bll 327–336, 2020.doi:10.1109/Blockchain50366.2020.00048

[120] C. O. N. Montreal, "reCON Montreal 2018", 2018.https://github.com/trailofbits/publications

[121] C. Liu, H. Liu, Z. Cao, Z. Chen, B. Chen, and B. Roscoe, "ReGuard: Finding reentrancy bugs in smart contracts", Proceedings - International Conference on Software Engineering, bll 65–68, 2018. doi:10.1145/3183440.3183495

[122] Solhint, Aug. 2021, [online] Available: https://protofire.github.io/solhint

[123] Mythril, Aug. 2021, [online] Available:https://github.com/ConsenSys/mythril

[124] Octopus, Nov. 2021, [online] Available:https://github.com/pventuzelo/octopus

[125] Conkas, Dec. 2021, [online] Available:https://github.com/nveloso/conkas

[126] Ethlint, Dec. 2021, [online] Available:https://github.com/duaraghav8/Ethlint

[127] C. G. Harris, "The risks and challenges of implementing ethereum smart contracts", Proceedings of IEEE international conference on blockchain and cryptocurrency (ICBC)

[128] E. Albert, J. Correas, P. Gordillo, G. Román-Díez, and A. Rubio, "SafeVM: A safety verifier for ethereum smart contracts", ISSTA 2019 - Proceedings of the 28th ACM SIGSOFT International Symposium on Software Testing and Analysis, bll 390–393, 2019. doi:10.1145/3293882.3338999

[129] E. Zhou, S. Hua, B. Pi, J. Sun, Y. Nomura, K.Yamashita, and H. Kurihara, "Security Assurance for Smart Contract", 2018 9th IFIP International Con-

ference on New Technologies, Mobility and Security, NTMS 2018 - Proceedings, vol 2018-January, bll 1–5, 2018. doi:10.1109/NTMS.2018.8328743

[130] J. Chang, B. Gao, H. Xiao, J. Sun, Y. Cai, and en Z. Yang, "sCompile: Critical Path Identification and Analysis for Smart Contracts", Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol 11852 LNCS, bll 286–304, 2019.doi:10.1007/978-3-030-32409-4_18

[131] P. Tsankov, A. Dan, D. Drachsler-Cohen, A. Gervais, F. Bünzli, and M. Vechev, "Securify: Practical security analysis of smart contracts", Proceedings of the ACM Conference on Computer and Communications Security, no June, bll 67–82, 2018.doi:10.1145/3243734.3243780

[132] M. Rodler, W. Li, G. O. Karame, and L. Davi, "Sereum: Protecting Existing Smart Contracts Against Re-Entrancy Attacks", no February, 2019.doi:10.14722/ndss.2019.23413

[133] A. Ali, Z. U. Abideen, and K. Ullah, "SESCon: Secure Ethereum Smart Contracts by Vulnerable Patterns' Detection", Security and Communication Networks, vol 2021, bll 1–14, Sep 2021.doi:10.1155/2021/2897565

[134] T. D. Nguyen, L. H. Pham, J. Sun, Y. Lin, and Q. T. Minh, "Sfuzz: An efficient adaptive fuzzer for solidity smart contracts", Proceedings - International Conference on Software Engineering, bll 778–788, 2020.doi:10.1145/3377811.3380334

[135] C. Peng, S. Akca, and A. Rajan, "SIF: A Framework for Solidity Contract Instrumentation and Analysis", Proceedings - Asia-Pacific Software Engineering Conference, APSEC, vol 2019-December, bll 466–473, 2019.doi:10.1109/APSEC48747.2019.00069

[136] J. Feist, G. Grieco, and A. Groce, "Slither: A static analysis framework for smart contracts", Proceedings - 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain, WETSEB 2019, bll 8–15, 2019.doi:10.1109/WETSEB.2019.00008

[137] M. Denker, Blockchain and Web 3.0. Routledge, 2019.doi:10.4324/9780429029530

[138] J. F. Ferreira, P. Cruz, T. Durieux, and R. Abreu, "SmartBugs: A Framework to Analyze Solidity Smart Contracts", Proceedings - 2020 35th IEEE/ACM International Conference on Automated Software Engineering, ASE 2020, bll 1349–1352, 2020.doi:10.1145/3324884.3415298

[139] S. Tikhomirov, E. Voskresenskaya, I. Ivanitskiy, R. Takhaviev, E. Marchenko, and Y. Alexandrov, "SmartCheck: Static analysis of ethereum smart contracts", Proceedings - International Conference on Software Engineering, no October, bll 9–16, 2018. doi:10.1145/3194113.3194115

[140] Z. Gao, V. Jayasundara, L. Jiang, X. Xia, D. Lo, and J. Grundy, "SmartEmbed: A Tool for Clone and Bug Detection in Smart Contracts through Structural Code Embedding", Proceedings - 2019 IEEE International Conference on Software Maintenance and Evolution, ICSME 2019, bll 394–397, 2019.doi:10.1109/ICSME.2019.00067

[141] G. A. Pierro, "Smart-Graph: Graphical Representations for Smart Contract on the Ethereum Blockchain", Proceedings - 2021 IEEE International Conference on Software Analysis, Evolution and Reengineering, SANER 2021, bll 708–714, 2021.doi:10.1109/SANER50967.2021.00090

[142] E. Albert, J. Correas, P. Gordillo, and G. Román-Díez, A. Rubio (2020) GASOL: Gas Analysis and Optimization for Ethereum Smart Contracts. In: Biere A., Parker D. (eds) Tools and Algorithms for the Construction and Analysis of Systems. TACAS 2020. Lecture Notes in Computer Science, vol 12079. Springer, Cham. https://doi.org/10.1007/978-3-030-45237-7_7

[143] L. Mazurek (2021) EthVer: Formal Verification of Randomized Ethereum Smart Contracts. In: Bernhard M. et al. (eds) Financial Cryptography and Data Security. FC 2021 International Workshops. FC 2021. Lecture Notes in Computer Science, vol 12676. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-63958-0_30

[144] P. Praitheeshan, L. Pan, X. Zheng, A. Jolfaei, and R. Doss, 2021. SolGuard: Preventing external call issues in smart contract-based multi-agent robotic systems. Information Sciences, 579, pp.150166. https://doi.org/10.1016/j.ins.2021.08.007

[145] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts (SoK),"In: Maffei M., Ryan M. (eds) Principles of Security and Trust. POST 2017. Lecture Notes in Computer Science, vol 10204. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-54455-6$_8$

[146] SolidiFI Benchmark, March. 2021, [online] Available:https://github.com/smartbugs/SolidiFI-benchmark