УДК 004.056

МЕТОДЫ ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ СМАРТ-КОНТРАКТОВ

Ястребов Андрей (Университет ИТМО)
Научный руководитель – кандидат технических наук, доцент Федоров И.Р.
(Санкт-Петербургский государственный университет аэрокосмического приборостроения, Университет ИТМО)

Введение. В быстро развивающейся цифровой экономике технология блокчейн стала важным инструментом для обеспечения прозрачности, безопасности и децентрализации. Смарт-контракты, являющиеся одним из важнейших функционалов данной технологии, произвели революцию в традиционных транзакционных парадигмах, автоматизируя соглашения и обеспечивая их выполнение без посредников. Однако растущая зависимость от смарт-контрактов также подчёркивает критическую необходимость в их безопасности и надёжности. Даже незначительные уязвимости могут привести к серьёзным финансовым потерям, ущербу репутации и утрате доверия. В рамках данной работы проведен обзор существующих методов тестирования безопасности смарт-контрактов.

Основная часть. В данной работе предлагается обзор существующих методов тестирования безопасности смарт-контрактов:

1. Статический анализ [1] - метод тестирования смарт-контрактов, при котором контракт анализируется без прямого выполнения кода;
2. Символическое исполнение [2] - метод, имитирующий выполнение смарт-контракта таким образом, что фактические входные данные заменяются специальными отслеживаемыми символьными параметрами;
3. Формальный анализ [3] - метод, преобразующий смарт-контракты в формальные представления и использующий автоматизированные проверки для получения выводов о свойствах их безопасности;
4. Трассировка выполнения - метод тестирования смарт-контрактов путем отслеживания и изучения транзакций, отправленных на смарт-контракт или учетную запись;
5. Синтез кода - метод, целью которого является создание безопасных и защищенных от определенных уязвимостей смарт-контрактов;
6. Перехват транзакций - метод, при котором анализируются отправляемые внутрь блокчейн-сети транзакции;
7. Фаззинг-тестирование [4] - метод, представляющий собой совокупность различных подходов к генерации тестовых входных данных для выявления уязвимостей в смарт-контрактах.

Выводы. В ходе исследования был проведен анализ существующих методов тестирования смарт-контрактов. В ходе анализа было выявлено, что благодаря своей актуальности и результативности, наиболее предпочтительным методом тестирования для дальнейших исследований является фаззинг-тестирование.

Список использованных источников:

1. Марков. А.С., Фадин А.А. Статический анализ безопасности кода // Программная инженерия и информационная безопасность. 2013 № 1, стр 50

2. James C King. 1976. Symbolic execution and program testing. Commun. ACM 19, 7 (1976), 385–394.

3. Everett Hildenbrandt, Manasvi Saxena, Nishant Rodrigues, Xiaoran Zhu, Philip Daian, Dwight Guth, Brandon Moore, Daejun Park, Yi Zhang, Andrei Stefanescu, et al. 2018. Kevm: A complete formal semantics of the ethereum virtual machine. In 2018 IEEE 31st Computer Security Foundations Symposium (CSF). IEEE, 204–217.

4. Christof Ferreira Torres, Antonio Ken Iannillo, Arthur Gervais, et al. 2021. CONFUZZIUS: A Data Dependency-Aware Hybrid Fuzzer for Smart Contracts. (2021).