МЕТОДИ ВЕРИФІКАЦІЇ БЕЗПЕКИ СМАРТ-КОНТРАКТІВ

Мокрій В.С., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Смарт-контракти є одним з найбільш поширених застосувань технології блокчейн на сьогоднішній день. Вони дозволяють виконувати угоди між сторонами автоматично, без посередників, роблячи процес швидким, прозорим і дешевшим. Саме завдяки цим перевагам смарт-контракти використовуються в широкому спектрі додатків у фінансовому секторі, страхуванні, торгівлі та системах DeFi. Але є важливий мінус: як тільки контракт поміщений на блокчейн, його вже неможливо змінити. В результаті будь-які помилки в коді залишаться назавжди і можуть призвести до значних втрат. Це пояснює, чому питання безпеки смарт-контрактів є такими важливими в наші дні.

Статистика підтверджує необхідність такого аналізу. За даними SlowMist, у 2024 році сталося 99 атак смарт-контрактів, що призвело до збитків на суму понад 214 мільйонів доларів [1]. У першій половині 2025 року ситуація погіршилася. Загалом у Web3 сталося 35 нових інцидентів із загальними збитками, що перевищили 3, 1 мільярда доларів США, більшість із яких були спричинені помилками коду [2]. Крім того, звіт Hacken показує, що лише в першій половині 2025 року недоліки в смарт-контрактах спричинили збитки на суму понад 6 мільярдів доларів [3]. Ці цифри говорять самі за себе: передчасне ігнорування автентифікації коду має катастрофічні наслідки.

Метою доповіді є розгляд статичного аналізу як одного з основних методів перевірки безпеки смарт-контрактів.

Цей метод набагато дешевше і безпечніше, ніж вирішення проблеми після завантаження системи. Статичний аналіз дозволяє виявити помилки, які найчастіше призводять до атаки: дублікати викликів функцій, цифрові переповнення або скорочення, неправильний контроль доступу, помилки в логіці виконання.

Існують спеціалізовані інструменти для реалізації цього підходу на практиці. Наприклад, Slither може швидко перевіряти контракти, написані в Solidity, і створювати докладні звіти для розробників. MythX - це комерційна хмарна платформа, інтегрована в середовище розробки, яка поєднує в собі можливості статичного та динамічного аналізу, що робить її універсальним інструментом для повної перевірки. Один із найперших інструментів – Oyente, довів, що навіть базовий аналіз коду може своєчасно виявляти критичні вразливості, включаючи атаки повторного входу [4].

Досліджуючи тестовий смарт-контракт з можливостями переказу коштів, усі три інструменти виявили різні вразливості. Slither визначив, що функція transferFunds() не перевіряє обмеження доступу, тобто будь-який користувач може її викликати, а також виявив можливість повторного виклику функції (re-entrancy) у методі withdraw(), коли зовнішні контракти можуть повторно викликати контракт до завершення виконання транзакції. MythX підтвердив ці

вразливості і додатково виявив ризик переповнення чисельної змінної у змінній balance, що може призвести до некоректного оновлення балансу користувача при великих сумах переказу. Oyente особливо акцентував на атаку повторного входу (Re-Entry) у функції withdraw(), відтворивши сценарій, коли зовнішній контракт може повторно викликати withdraw() і витягти кошти кілька разів до оновлення стану балансу.

Цей приклад показує, що інструменти статичного аналізу можуть доповнювати один одного: Slither швидко виявляє загальні помилки доступу та повторного виклику, MythX аналізує потенційні чисельні проблеми, а Oyente дозволяє моделювати конкретні сценарії атаки. Комбіноване використання цих інструментів може забезпечити більш комплексну та надійну автентифікацію для смарт-контрактів, дозволяючи розробникам закривати критичні вразливості ще до розгортання блокчейну.

Незважаючи на те що статичний аналіз не моделює фактичне виконання контракту, а складні логічні помилки можуть залишатися непоміченими та іноді створювати помилкові спрацьовування, він залишається основою для безпечної автентифікації коду. Його застосування дозволяє закрити вразливість до того, як контракт буде розгорнуто в блокчейні.

Щоб підвищити безпеку блокчейн-додатків, технології запобігання, особливо статичний аналіз, формують основу довіри до блокчейн-рішень і покращують рівень безпеки цифрових активів [5]. Статичний аналіз - це більш доступний, швидший і практичний метод, який можна застосовувати безперервно під час розробки, а не динамічне тестування та ресурсомісткі формальні перевірки. Тому його використання є необхідним етапом у створенні надійних смарт-контрактів і невід'ємною частиною комплексної стратегії захисту блокчейн-систем.

Список літератури

1. SlowMist. 2025 Mid-Year Blockchain Security and AML Report. URL: https://slowmist.medium.com/slowmist-2025-mid-year-blockchain-security-and-aml-report-3dfc535971fb

2. SlowMist. Annual Blockchain Security & AML Report 2024. URL: https://www.slowmist.com/report/2024-Blockchain-Security-and-AML-Annual-Report(EN).pdf

3. Tsankov, P., Dan, A., Drachsler-Cohen, D., Gervais, A., Buenzli, F., & Vechev, M. (2018, October). Securify: Practical security analysis of smart contracts. In Proceedings of the 2018 ACM SIGSAC conference on computer and communications security (pp. 67-82)..

4. Hacken. H1-2025 Web3 Security Report. URL: https://hacken.io/insights/q1-2025-security-report/

5. Терещенко Г. Ю., Кириченко І. В. Аналіз і обґрунтування використання наявних блокчейн-рішень для захисту цифрових активів. ХНУРЕ, 2024.