DOI: https://doi.org/10.36059/978-966-397-308-1-25

АУДИТ СМАРТ-КОНТРАКТІВ

Шандиба Дмитро Володимирович
аспірант
Державної науково-навчальної установи
«Академія фінансового управління»

Смарт-контракти – це комп'ютерні програми, які запускаються автоматично під час виконання певних умов. Смарт-контракти – це адаптивні інструменти, які можуть відслідковувати рух матеріальної та інтелектуальної власності, а також полегшувати та перевіряти фінансові транзакції. Оскільки смарт-контракти мають право розподіляти цінні ресурси між складними системами та здебільшого є автономними, безпека та узгодженість мають вирішальне значення. Тому розуміння ймовірності та критичного характеру можливих недоліків або виявлених помилок має важливе значення для безпеки смарт-контракту.

У 2022 році криптовалютна індустрія пережила найбільшу в історії хакерську активність, внаслідок якої криптовалютні проекти втратили понад 3,8 мільярда доларів. Протоколи DeFi зазнали найбільших збитків: загалом було викрадено 3,1 мільярда доларів. Ця статистика викликає занепокоєння, і власники проектів мають бути обережними щодо можливості того, що їхні проекти стануть мішенню. Тому вкрай важливо захищати свої смарт-контракти, щоб забезпечити безпеку проекту та його користувачам [5].

Вразливість безпеки в коді смарт-контракту може мати руйнівні наслідки, зокрема крадіжку всіх активів, що зберігаються у смарт-контракті. У 2021 році в автоматизованого маркет-мейкера (AMM) Uranium Finance було вкрадено 50 мільйонів доларів США через єдину друкарську помилку у смарт-контракті.

Також у 2021 році Compound Finance виплатила 80 мільйонів доларів США незароблених винагород через помилку в одному символі. У 2022 році з Wormhole Bridge було вкрадено 320 мільйонів доларів США через помилку в одному із смарт-контрактів [6].

Вразливість – це все, що може вплинути на безперебійну та безпечну роботу смарт-контракту. Це може бути помилка в обчисленні змінної, непотрібні привілеї творцю, та багато іншого. Зазвичай ризики смарт-контрактів класифікуються за п'ятьма категоріями [5].

Критичний ризик – це той ризик, який впливає на безпечне функціонування платформи та має бути усуненим до запуску. Користувачам не слід інвестувати будь-які проекти з визначеними критичними ризиками.

Основний ризик може включати проблеми централізації та логічні помилки. За певних обставин ці основні ризики можуть призвести до втрати коштів та контролю над проектом.

Середній ризик може не становити прямого ризику для кінцевого користувача, але може вплинути на загальне функціонування платформи.

Незначний ризик може бути будь-якими з перерахованих вище, але в меншому масштабі. Як правило, вони не порушують загальної цілісності проекту, але можуть бути зменшити ефективність смарт-контрактів.

Інформаційна помилка часто є рекомендацією щодо покращення стилю коду або певних операцій, щоб відповідати передовим галузевим практикам. Зазвичай вони впливають загальне функціонування коду.

Ризики централізації. Централізація є ризиком як для власників проектів, так і для користувачів. Якщо одній адресі надано виконавчі привілеї, а потім його закритий ключ скомпрометовано, розробники ризикують втратити контроль над своїм проектом, а користувачі контроль над своїми грошима. Проекти, які витягують кошти своїх інвесторів, часто мають переваги централізованих привілеїв. Уникнення непотрібної централізації – це один зі способів, за допомогою якого проекти можуть отримати довіру спільноти.

Смарт-контракти можуть містити приховані вразливості, які можуть призвести до втрати грошей або переривання бізнес-операцій. У світі блокчейн навіть дрібні проблеми безпеки негативно впливають на репутацію та інвестиційні рішення [1].

Аудит безпеки смарт-контрактів є дуже поширеним в екосистемі децентралізованих фінансів (DeFi). Аудит смарт-контракту – це всебічний аналіз безпеки коду та функціональності смарт-контракту. Метою аудиту є виявлення будь-яких потенційних вразливостей чи проблем безпеки, які можуть вплинути на здатність контракту функціонувати належним чином. Як правило, аудитори вивчають код смарт-контрактів, складають звіт та надають його проекту для покращень. Потім випускається остаточний звіт з докладним описом всіх помилок та вже виконаної роботи для вирішення проблем з продуктивністю або безпекою.

Смарт-контракти можна перевіряти за допомогою ручних або автоматизованих підходів, а саме: Ручний аудит передбачає, що група аудиторів переглядає кожен рядок коду на наявність проблем із компіляцією та повторним введенням. Це також може допомогти у виявленні інших вразливостей безпеки, які часто не беруть до уваги, наприклад неефективних методів кодування. Оскільки цей метод дозволяє виявляти приховані дефекти, він вважається найбільш точним та повним.

Автоматизований підхід до аудиту смарт-контрактів використовує програмне забезпечення для виявлення помилок, що допомагає аудиторам визначити точне місце, відповідальне за помилки. Однак, автоматизоване програмне забезпечення може не завжди розуміти контекст і пропускати деякі вразливості під час перевірки [7].

Аудит безпеки особливо цінний для DeFi проектів, які розраховують обробляти блокчейн-транзакції на мільйони доларів або величезну кількість користувачів. Аудит зазвичай проходить у чотири етапи:

1. Смарт-контракти надаються аудиторській групі для первинного аналізу.

2. Аудиторська група представляє свої висновки по проекту для вживання заходів.

3. Команда проекту вносить зміни з урахуванням виявлених проблем.

4. Аудиторська група випускає свій остаточний звіт з урахуванням всіх нових змін або помилок, що залишаються.

Деякі постачальники аудиторських послуг також вважаються лідерами галузі, що робить їх аудит ціннішим в очах інвесторів [5].

Аудит смарт-контрактів проводиться за стандартною процедурою і може незначною мірою відрізнятися у різних аудиторських компаній. Нижче наводиться типова процедура (табл. 1).

Таблиця 1

Типова процедура аудиту смарт-контрактів

Фаза аудиту	**Зміст**
ЗБІР ДАНИХ	Щоб забезпечити гарантовану інтеграцію сторонніх смарт-контрактів, аудитори збирають специфікації коду та вивчають архітектуру. Це допомагає аудиторам зрозуміти цілі проекту та визначити його обсяг.
ЗАПУСК ТЕСТІВ	Аудитори перевіряють проект, щоб перевірити кожну функцію смарт-контракту. Фахівці з аудиту використовують різні інструменти (як ручні, так і автоматизовані), щоб гарантувати, що тести перевіряють весь код смарт-контракту.
ВИБІР МЕТОДУ АУДИТУ	Оскільки ручний аудит ефективніший, аудитори часто перевіряють смарт-контракти без допомоги програмного забезпечення. За такого підходу можна ефективно виявляти такі вразливості, як випереджаючі атаки
ФОРМУВАННЯ ПОЧАТКОВОГО ЗВІТУ	Після завершення аудиту робиться попередній звіт, щоб команда проекту могла виправити виявлені помилки та вразливості. Деякі постачальники послуг смарт-контрактів мають команду експертів, які допомагають виправити кожну знайдену помилку.
ФОРМУВАННЯ ОСТАТОЧНОГО АУДИТОРСЬКОГО	Після виправлення помилок публікується остаточний звіт з урахуванням будь-яких дій, здійснених командою. Аудиторський звіт надається наприкінці процесу аудиту.

ЗВІТУ	Очікується, що з метою прозорості, проекти мають ділитися своїми звітами із спільнотою. У більшості звітів проблеми класифікуються за серйозністю, наприклад, критичні, серйозні, незначні тощо. У звіті також буде вказано статус проблеми, оскільки проекти надають час на її вирішення до випуску остаточного звіту.

Джерело: Security Аудит Смарт-Контрактів [7]

Не варто ставитись до аудиту як до стовідсоткової гарантії безпеки проекту. Навіть при актуально пройденому аудиті всіх смарт-контрактів, у відомої компанії залишається ще багато джерел ризику. Варто проводити власний аналіз проекту, вивчати його економіку та принцип роботи.

Формальна верифікація забезпечує систематичний й автоматизований спосіб перевірки логіки та поведінки контракту на відповідність його бажаним властивостям [7]. Це спрощує виявлення і виправлення будь-яких потенційних помилок чи багів. Потім аудитори використовують автоматизовані інструменти перевірки правильності цих тверджень.

Список використаних джерел:

1. Аналіз і перевірка специфікацій та вихідного коду смарт-контрактів. URL: https://www.h-x.technology/ua/services/smart-contract-audit-ua.
2. Аудит смарт-контрактів. URL: https://datami.ua/services/audit-smart-kontraktiv.
3. Степанов М. Основи роботи та безпеки смарт-контрактів. URL: https://www.h-x.technology/ua/blog-ua/deals-in-the-digital-age-ua.
4. Що таке аудит безпеки смарт-контрактів? URL: https://academy.binance.com/uk/articles/what-is-a-smart-contract-security-audi.
5. Що таке аудит смарт-контракту. URL: https://tsecrypto.com/article/shho-take-audyt-smart-kontraktu.
6. Що таке формальна верифікація смарт-контрактів? URL: https://academy.binance.com/uk/articles/what-is-formal-verification-of-smart-contracts
7. Security Аудит Смарт-Контрактів. URL: https://avada-media.ua/ua/services/security-audit-smart-kontraktov.