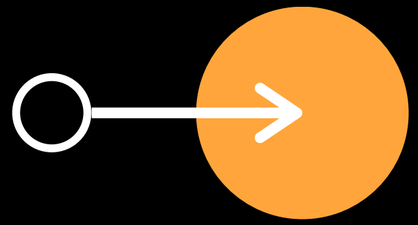
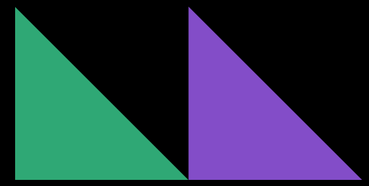
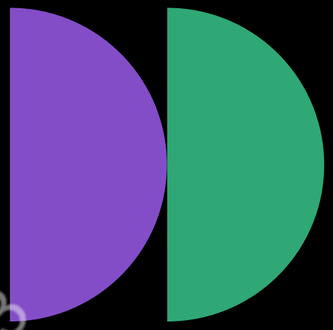
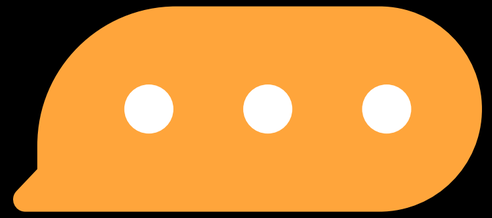
короткий посібник





Що таке аудит смарт-контракту





У 2022 році криптовалютна індустрія пережила найбільшу в історії хакерську активність, внаслідок якої криптовалютні проєкти втратили понад 3,8 мільярда доларів. Протоколи DeFi зазнали найбільших збитків: загалом було вкрадено 3,1 мільярда доларів.

Ця статистика викликає занепокоєння, і власники проєктів мають бути обережними щодо можливості того, що їхні проєкти стануть мішенню. Тому вкрай важливо захищати свої смарт-контракти, щоб забезпечити безпеку проєкту та його користувачам.

Тут у гру вступає аудит смарт-контрактів.

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.

Яким є процес аудиту смарт-контракту?

Процес аудиту смарт-контрактів є складним і використовує ряд різних методів перевірки. Зазвичай все починається з перевірки на вразливості. Цей процес складається з двох частин: формальної та ручної перевірки.

Формальна перевірка — це автоматизований процес, який перевіряє кожну змінну смарт-контракту на відповідність кожному можливому значенню, яке вона може мати.

Уявіть собі тисячі паралельних всесвітів одночасно, у кожному з яких змінилося щось одне. Механізм **формальної перевірки** їх перевіряє та підіймає тривогу щодо проблем, які можуть вплинути на **логічну цілісність контракту**.

Ручна перевірка — це саме те, на що це схоже: аудитор переглядає кожен рядок коду та ретельно перевіряє його на наявність відомих уразливостей та помилок коду.

Після цих двох етапів, команда аудитора готує звіт про вразливості та ризики надсилає його проєкту разом із рекомендаціями щодо усунення виявлених проблем.

Які бувають типи вразливостей смарт-контрактів?

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:

- **Критичний ризик** – це той ризик, який впливає на безпечне функціонування платформи та має бути усуненим до запуску. Користувачам не слід інвестувати будь-які проєкти 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 проєктом.
- **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 проєкту, 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.

Найрозповсюдженіші вразливості смарт-контрактів

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

Залежність від мітки часу. На відміну від звичайних програм, середовище виконання смарт-контракту знаходиться на боці майнера або валідатора. Коли логіка контракту залежить від поточного часу, майнер може маніпулювати поточним часом, щоб вплинути на результат виконання та досягти заздалегідь визначеної мети.

Вразливість випадкових чисел. Зловмисник може точно вгадати випадкове число, згенероване контрактом, у випадку якщо за початкове значення береться загальновідома змінна.

Орфографічні помилки. Конструктори зазвичай використовуються для ініціалізації контракту та визначення власника контракту. Компілятор не помітить неправильного написання функції під час програмування, внаслідок чого функція стане загальнодоступною, тому будь-хто може викликати її спрацювання.

Скільки коштує аудит смарт-контракту?

Вартість аудиту смарт-контрактів варіюється в залежності від розміру та складності програми. Як правило, аудитори смарт-контрактів беруть від $5,000 до $15,000, але можуть брати більше залежно від розміру та складності контракту. Процес аудиту смарт-контракту (перший аудит) може тривати від двох до 14 днів.

Аудит може зайняти до місяця для великих проектів чи протоколів. Проєкт отримує рекомендації щодо внесення виправлень після завершення початкового аудиту. Після цього проводиться перевірка виправлення, що зазвичай займає один день.

Топ аудиторських фірм смарт-контрактів

Аудит безпеки смарт-контрактів був вперше проведений компанією CertiK. BNB Smart Chain, Bancor та Huobi пройшли аудит CertiK. Крім того, перш ніж інвестувати в якийсь проєкт, інвестиційний фонд біржі Binance проводить аудит цього проєкту за допомогою CertiK.

Chainsulting – інша відома фірма з аудиту смарт-контрактів, заснована у 2017 році. Серед її основних клієнтів – 1inch, MakerDAO та багато інших відомих протоколів DeFi.

Компанія OpenZeppelin надає аудиторські послуги Coinbase та Ethereum Foundation, двом мастодонтам у світі блокчейнів. Крім того, платформа забезпечує створення безпечних смарт-контрактів Ethereum за допомогою своїх модульних шаблонів контрактів.


GOOD LUCK!