

РИЗИКИ КІБЕРБЕЗПЕКИ NFT-ТЕХНОЛОГІЇ ТА МЕТОДИ ЇХ ВИРІШЕННЯ

SECURITY RISKS OF NFT TECHNOLOGY AND METHODS FOR ADDRESSING THEM

NFT (невзаємозамінні токени) стрімко завоювали популярність у різних галузях – від цифрового мистецтва та ігор до фінансів і управління інтелектуальною власністю. Ключовими причинами цього є їх можливість надання підтвердження права власності та походження активу. NFT досі розглядаються як шлях до створення прозорої та підзвітної цифрової екосистеми. Проте разом із поширенням даної технології збільшилась кількість випадків шахрайства та фішингу, зломів гаманців, використання вразливостей смарт-контрактів та атак на мережу блокчейн. Згідно зі звітами, щорічні втрати через кіберзагрози у блокчейн-екосистемах сягають мільйонів доларів.

Проте, попри зростання популярності NFT, наразі немає усталених підходів для мінімізації ризиків. Це робить дослідження у цій сфері необхідними для подальшого розвитку екосистеми.

Аналіз ризиків технології NFT включає аналіз вразливостей смарт-контрактів, пов'язаних з ними атаки, атаки на мережу блокчейн, зокрема атаки маршрутизації, атаки 51%, атаки на протоколи блокчейну[1] та криптографічні атаки.

Мінімізація можливих ризиків невзаємозамінних токенів досягається підвищенням безпеки смарт-контрактів, зокрема їх аудитом, вирішенням вразливостей згідно OWASP Smart Contract Top 10 [2], а також впровадженням використання звернень до стороннього джерела інформації, відомого як оракул, для отримання інформації про транзакції. Дана реалізація здійснена за допомогою Chainlink API, яке дозволяє отримати рівень довіри до адреси та історію його попередніх транзакцій для подальшої оцінки ризиків транзакції.

Важливим аспектом пом'якшення ризиків є методи боротьби з поширеними атаками на блокчейн-мережі, зокрема атакою затемнення, атаками 51% та атаками пов'язаними з подвійною витратою. Також одною з основних сторін захисту є використання децентралізованих та мультифакторних рішень для підвищення безпеки гаманців та орієнтованих на безпеку платформ для створення та торгівлі NFT.

У підсумку, рішення повинні бути спрямовані на комплексний підхід до ідентифікації, аналізу та вирішення ризиків, забезпечуючи більш надійну та безпечну інфраструктуру для використання невзаємозамінних токенів, що є ключовим в умовах зростання популярності NFT у різних сферах життєдіяльності.

Література

1. Framework for Determining the Suitability of Blockchain: Criteria and Issues to Consider. URL: https://www.researchgate.net/publication/353073634_Framework_for_Determining_the_Suitability_of_Blockchain_Criteria_and_Issues_to_Consider.
2. OWASP Smart Contract Top 10. URL: <https://owasp.org/www-project-smart-contract-top-10/>.