УДК 004.05
Синюшкіна М.Д.,[1], Неласа Г.В.[2]
[1] студ. гр. БК-813м НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

АВТОМАТИЗОВАНИЙ АУДИТ СМАРТ-КОНТРАКТІВ MARKETPLACE ЗАСТОСУНКУ: СТРАТЕГІЇ БЕЗПЕКИ

З роками концепція Web 3.0 проходила крізь етапи еволюції, від початкової ідеї про семантичну мережу до більш децентралізованої версії Інтернету, побудованої за допомогою блокчейну. Однією з головних ідей Web 3.0 є переклад усього веб-контенту, написаного людськими мовами, у машиночитану форму, що дозволить алгоритмам і програмам визначати значення повідомлень і встановлювати з'єднання на їх основі [1].

У Web3 кожен вміст є цифровим активом. Завдяки Web3 більше нікому не ділитеся своїми конфіденційними даними. Навіть купувати або продавати банкам [1]. З цієї причини з'явилися криптовалюти – ще одне відоме та всюдисуще явище. Платежі в криптовалюті пропонують сторонам свободу, якої не існувало в Web 2.0 – не потрібно нікому звітувати, хто це робить і на що витрачаються гроші.

При розробці додатків «нового покоління» дотримуються децентралізації організації даних, у тому числі їх зберігання. Децентралізація, у свою чергу, є ключем до успішного впровадження криптовалют і смарт-контрактів в економіку: усуває потребу в довірі, а отже, в посередниках і централізованих структурах.

Тому ідеальний стан Web3 – це ефективна бізнес-модель, яка не використовує ієрархічні структури та традиційні фінансові інструменти.

При аудиті смарт-контрактів у контексті Web3, однією з ключових вимог є забезпечення безпеки та надійності системи [2]. Децентралізація організації даних та їх зберігання є однією з основних стратегій, яка використовується для забезпечення цілісності та невід'ємності смарт-контрактів у розподіленій мережі.

Під час аудиту смарт-контрактів важливо перевірити, чи відповідає код вимогам безпеки. Для цього використовуються різноманітні техніки, включаючи аналіз потенційних вразливостей, перевірку наявності захисту від атак, валідацію вхідних даних та інші методи аналізу [3]. Важливо також переконатися, що механізми захисту даних та конфіденційності реалізовані належним чином та враховують усі можливі ризики.

Крім того, у контексті Web3 велика увага приділяється використанню криптовалют та забезпеченню безпеки та відповідності регуляторним вимогам у цій сфері. Такі аспекти, як захист приватності користувачів, безпека транзакцій та відповідність нормативним вимогам, викликають

особливий інтерес при аудиті смарт-контрактів, оскільки вони безпосередньо впливають на фінансову та особисту безпеку користувачів.

При аудиті смарт-контрактів, особливу увагу зазвичай приділяють вразливостям, що стосуються контрактів, таким як переповнення, відмова в обслуговуванні, викладення конфіденційних даних та інші [3]. OWASP Top 10 може служити важливим джерелом для визначення потенційних загроз безпеці та розробки стратегій їх усунення.

Крім того, існують інші стандарти та рекомендації, спрямовані на забезпечення безпеки програмного забезпечення, які можуть бути застосовані при аудиті смарт-контрактів. Наприклад, CERT Secure Coding Standards включає набір практик з безпеки програмування, які можуть допомогти у виявленні та усуненні потенційних вразливостей у смарт-контрактах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Introduction to smart contracts – [Електронний ресурс]. – Режим доступу: https://ethereum.org/en/developers/docs/smart-contracts/

2. Comparison of smart contract generation methods. – [Електронний ресурс]. – Режим доступу https://www.researchgate.net/figure/Comparison-ofsmart-contract-generation-methods_tbl1_360503282

3. H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, J. J. Kishigami, ‘‘Blockchain contract: A complete consensus using blockchain,’’ in Proc. IEEE 4th Global Conf. Consum. Electron. (GCCE), Жовтень, 2015, с. 577–578.