Секція 4

**ПРОБЛЕМИ БЕЗПЕКИ ТА МАСШТАБОВАНОСТІ В СИСТЕМІ ETHEREUM, ПОВ’ЯЗАНІ ІЗ ЗАСТОСУВАННЯМ СМАРТКОНТРАКТІВ**

Юрченко А. Є., Шафоростов М. О.

Харківський національний університет радіоелектроніки, Харків, Україна

Смартконтракти – це програми, що забезпечують автоматизоване виконання угод між сторонами, для якого посередник не потрібен [1]. Вони є наріжним елементом багатьох децентралізованих облікових систем – платформ смартконтрактів. Смартконтракти можуть застосовуватися для розроблення похідних фінансових засобів, ідентифікаційних систем, файлових сховищ і т. ін.

Саме в межах блокчейн-платформи Ethereum смартконтракти вперше набули широкого поширення. Основними складниками смартконтрактів Ethereum є функції, події та змінні стану. Здебільшого для їх написання використовується повна за Тьюрінгом мова Solidity. Після компіляції код смартконтракту перетворюється на байт-код для віртуальної машини Ethereum і зберігається в блокчейні за допомогою транзакції створення контракту. Кожний успішно збережений смартконтракт розпізнається за унікальною адресою [2].

**Мета доповіді** – проаналізувати вплив застосування смартконтрактів на безпеку та масштабованість системи Ethereum.

Для аналізу використовуються статистичні дані про проведення транзакцій та виконання смартконтрактів у системі Ethereum, а також інформація про відомі вразливості. Уразливості, які розглядаються, поділяються на групи за 3 основними причинами: «мова Solidity», «віртуальна машина», «будова блокчейна» [2].

Також пропонуються шляхи вдосконалення смартконтрактів, як-от використання різних мов програмування, розробляння бібліотек безпечних контрактів та вдосконалення механізмів передзапускної верифікації контрактів.

**Список літератури**

1. Buterin V. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2014. URL: https://ethereum.org /669c9e2e2027310b6b3cdce6e1c52962/Ethereum\_Whitepaper\_-\_Buterin\_2014.pdf (дата звернення: 30.03.2023).
2. Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract / S. S. Kushwaha та ін. *IEEE Access*. 2022. Т. 10. С. 6605–6621.

Арсеній Євгенович Юрченко, студент факультету КІУ, arsenii.iurchenko@nure.ua .

Михайло Олександрович Шафоростов, асистент кафедри БІТ, +380508863066, mykhailo.shaforostov@nure.ua .