АНАЛІЗ ШЛЯХІВ УДОСКОНАЛЕННЯ ПАТЕРНУ ОНОВЛЕННЯ СМАРТ-КОНТРАКТІВ DIAMOND STANDARD

Бучіхін А.А., Болтьонков В.О.
Національний університет "Одеська політехніка", м.Одеса

У роботі розглянуто питання недоліків найбільш розвиненого патерну оновлення смарт-контрактів на EVM-сумісних блокчейнах – ERC-2535 Diamond Standard [1]. Створена з метою надання можливості організовувати протокол як набір вставних модулів логіки з єдиним місцем всіх його даних, реалізація розробленого патерну залишила в собі такі недоліки, як контроль доступу до даних у неструктурованому сховищі, вартість викликів між обновлюваними модулями логіки, вартість маршрутизації викликів, вартість оновлення маршрутизації, колізії селекторів функцій та статичність головного модуля логіки, що містить логіку оновлення самого протоколу.

Розроблене вдосконалення базується на новій пропозиції – EIP-7702 [2], яка буде додана в оновленні Pectra найближчим часом [3]. Вона вводить новий тип транзакції – 0x04, що дозволяє EOA-гаманцям поводитися як смарт-контракт, адреса якого вказана в цій транзакції, допоки нова така транзакція не прибере цю поведінку, видаливши адресу з вказівника. Це нововведення дозволило дешево оновлювати та виконувати код делегованого контракту, зробивши EOA статичними адресами обновлюваних модулів логіки. Перевагою таких адрес стала можливість використання Sparse Merkle Tree [4] для хешування всіх цих адрес в єдиному корені, який можна зберігати у головному контракті як константу. При цьому докази наявності зазначених адрес у корені не змінюватимуться завдяки передчасній генерації всіх EOA-гаманців.

Для користування таким протоколом створюється бібліотека, яка містить усі адреси та докази для взаємодії з функціями протоколу як зі звичайними. Проблеми зі сховищем вирішено комбінацією Diamond Storage [5] та нещодавно доданого ERC-7201 [6], із створенням просторів для різних контекстів. Розроблений патерн усуває всі недоліки свого попередника і є набагато ефективнішим за нього.

Література:

1. Mudge N. ERC-2535: Diamonds, Multi-Facet Proxy [Електронний ресурс] – Ethereum Improvement Proposals, no. 2535, Feb 2020. – URL: https://eips.ethereum.org/EIPS/eip-2535.

2. Buterin V., Wilson S., Dietrichs A., lightclient. EIP-7702: Set EOA account code [Електронний ресурс] – Ethereum Improvement Proposals, no. 7702, May 2024. – URL: https://eips.ethereum.org/EIPS/eip-7702.

3. Ethereum Foundation. Pectra Testnet Announcement [Електронний ресурс] – Ethereum Foundation Blog, Feb 2025 p. – URL: https://blog.ethereum.org/2025/02/14/pectra-testnet-announcement.

4. Baylina J., Bellés M. Sparse Merkle Trees [Електронний ресурс] – URL: https://docs.iden3.io/publications/pdfs/Merkle-Tree.pdf.

5. Mudge N. How Diamond Storage Works [Електронний ресурс] – DEV Community, 18.09.2020 (ред. 17.09.2022). – URL: https://dev.to/mudgen/how-diamond-storage-works-90e.

6. Giordano F., Croubois H., García E., Lau E. ERC-7201: Namespaced Storage Layout [Електронний ресурс] – Ethereum Improvement Proposals, no. 7201, June 2023. – URL: https://eips.ethereum.org/EIPS/eip-7201.