АРХІТЕКТУРА ТА ОСНОВНІ ЗАГРОЗИ БЕЗПЕЦІ ДЕЦЕНТРАЛІЗОВАНИХ ВЕБ3-ДОДАТКІВ

Буряківська І.В., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Web3 (dApps) (або Веб3 додатки) − це програмні системи, у яких ключова бізнес-логіка виконується як смарт-контракти в децентралізованому реєстрі, тоді як статус і право власності на цифрові активи підтверджуються консенсусом розподіленої мережі, а не довіреним оператором [1]. На відміну від традиційних веб-додатків, безпека яких значною мірою залежить від надійного периметра на стороні сервера, у Web3 код контракту є загальнодоступним, його виконання є незворотним, а помилка в логіці безпосередньо призводить до фінансових втрат [2].

Метою доповіді є систематизація архітектурних компонентів Web3-додатків та основних загроз їх безпеці. **У доповіді** розглянуто типову багаторівневу dApp-архітектуру, класи вразливостей смарт-контрактів, атаки користувачів та заходи щодо зменшення ризиків. Показано, що безпека Web3-додатку визначається не тільки правильністю коду контракту, а й надійністю всього ланцюжка взаємодії − від гаманця користувача до позаланцюгової інфраструктури.

Типова архітектура dApp складається з чотирьох рівнів. Перший − це клієнтський рівень: веб-інтерфейс, який взаємодіє з гаманцем користувача, де зберігається закритий ключ і підписуються транзакції. Другий − рівень смарт-контрактів, який працює у віртуальній машині блокчейну, такій як EVM [1]. Третій рівень − це доступ до мережі через повні вузли та провайдери RPC. Четвертий рівень архітектури, компоненти поза ланцюгом: децентралізовані системи зберігання даних, такі як IPFS [3], індексатори даних і оракули, що передають зовнішні дані в смарт-контракти. Незважаючи на те, що система децентралізована на рівні контракту, інтерфейс, записи DNS і провайдери RPC на практиці часто залишаються централізованими, створюючи додаткові точки відмови та поверхню атаки. Загрози безпеці децентралізованих Веб3-додатків можна розділити на кілька груп. Перша група включає вразливі місця логіки смарт-контрактів: повторний вхід, який використовувався під час атаки на DAO у 2016 році; помилки контролю доступу; цілочисельне переповнення; залежність результату від порядку транзакцій; і небезпечне використання зовнішніх викликів [2]. Друга група включає економічні атаки на протоколи децентралізованих фінансів: маніпулювання цінами в оракулах, зокрема шляхом використання флеш-позик, і використання недоліків у механізмах ліквідації та управління [4]. Третя група пов’язана з порядком включення транзакцій у блок: «front-running» і «вартість, яку можуть витягувати майнери та валідатори» (MEV) дозволяють змінювати порядок транзакцій для особистої вигоди та становлять ризик для стабільності консенсусу [5]. Також варто виділити флеш-позики: кредит без застави в межах однієї транзакції

здешевлює атаки на ціновий оракул [6]. Необхідно виділити атаки на міжланцюгові мости (Cross-chain Bridges), які забезпечують передавання цифрових активів і повідомлень між різними блокчейн-мережами. Основними векторами атак є компрометація ключів валідаторів мосту, підроблення або повторне використання міжланцюгових повідомлень, помилки перевірки підтверджень транзакцій та вразливості механізмів блокування і випуску токенів. Успішна експлуатація таких недоліків може призвести до несанкціонованої емісії активів або втрати заблокованих коштів.

Атаки, спрямовані проти користувачів та інфраструктури, становлять окрему категорію: фішинг, підробка інтерфейсу через зламані DNS-сервери або CDN, зловмисні запити на підписи (наприклад, надання необмежених прав на спільний доступ до токенів) і компрометація приватних ключів і адміністративних облікових записів. Контракти з проксі-контрактом становлять додатковий ризик, оскільки зловмисник, який отримав контроль над адміністративною роллю, може втрутитися в логіку протоколу.

Для мінімізації цих ризиків доцільно застосовувати комплексний підхід. На етапі розробки: шаблон «checks-effects-interactions», перевірені бібліотеки смарт-контрактів, статичний аналіз, фаззинг та формальна перевірка критичних модулів. На операційному рівні: незалежні аудити, механізми мультипідпису та timelock для адміністративних операцій, використання децентралізованих оракулів усереднення цін, обмеження обсягу транзакцій та моніторинг підозрілих транзакцій у реальному часі. На рівні користувача: апаратні гаманці, моделювання транзакцій перед підписанням та обмеження прав на витрати токенів.

Тому забезпечення безпеки Web3-додатків вимагає комплексного підходу до системи в цілому: смарт-контракти, інфраструктура і поведінка користувачів утворюють єдину модель загрози. Серед перспективних напрямів подальших досліджень − автоматизоване виявлення вразливостей у контрактах та методи протидії MEV.

Список літератури

1. Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper. 2014.

2. Atzei N., Bartoletti M., Cimoli T. A Survey of Attacks on Ethereum Smart Contracts (SoK). Principles of Security and Trust (POST 2017). Lecture Notes in Computer Science. Vol. 10204. Berlin: Springer, 2017.

3. Benet J. IPFS – Content Addressed, Versioned, P2P File System. arXiv:1407.3561. 2014.

4. Zhou L., Xiong X., Ernstberger J. et al. SoK: Decentralized Finance (DeFi) Attacks. 2023 IEEE Symposium on Security and Privacy (SP). 2023.

5. Daian P., Goldfeder S., Kell T. et al. Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability. 2020 IEEE Symposium on Security and Privacy (SP). 2020.

6. Qin K., Zhou L., Livshits B., Gervais A. Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit. Financial Cryptography (FC 2021). LNCS. Vol. 12674. 2021.