КРИПТОГРАФІЧНІ МЕХАНІЗМИ ЗАХИСТУ СМАРТ-КОНТРАКТІВ

Мокрій В.С., В'юхін Д.О., Власов А.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Смарт-контракти є елементом технології блокчейн, здатним автоматично виконувати угоди між сторонами без залучення третіх осіб. Їхня безпека базується на застосуванні криптографічних методів, де геш-функції відіграють центральну роль. Геш-функція являє собою математичний алгоритм, який перетворює вхідні дані на вихідне значення (геш) фіксованої довжини.

Метою доповіді є аналіз криптографічних механізмів, що застосовуються для захисту смарт-контрактів, зокрема алгоритмів гешування, їх стійкості до атак і практичного застосування у блокчейн-системах.

Геш-функції застосовуються у смарт-контрактах для забезпечення захисту конфіденційної інформації, формування цифрових підписів та механізмів довіри.

Вони також слугують для створення унікальних ідентифікаторів транзакцій і користувачів. У фінансових блокчейн-додатках ці функції є основою для доказів нульового розголошення, що дозволяє особам підтверджувати знання певних даних, не розкриваючи їх [1].

Проте використання геш-функцій у смарт-контрактах не позбавлене ризиків. Наприклад, можливі атаки методом грубої сили, використання веселкових таблиць та криптоаналітичні атаки. Зокрема, атаки на день народження можуть бути використані для виявлення колізій, а атаки розширення довжини - для маніпулювання хешем. Згідно з дослідженням, застарілі алгоритми, такі як MD5 і SHA-1, були зламані, отже, їх не можна використовувати у смарт-контрактах.

Окрім вибору надійного алгоритму, важливим є його правильне втілення у код смарт-контракту. Навіть найміцніші геш-функції можуть виявитися марними, якщо реалізація містить логічні похибки або слабкі місця. Частими помилками є повторне використання одних і тих же даних для гешування, неправильне формування повідомлень чи ігнорування принципів криптографічної ентропії. Отже, надзвичайно важливо не тільки обрати сучасні алгоритми, але й дотримуватися найкращих практик програмування та пройти аудит безпеки.

Для підвищення рівня безпеки необхідно застосовувати надійні криптографічні алгоритми, такі як SHA-256 та Keccak-256, які використовуються в блокчейнах Bitcoin і Ethereum. Додатково, рекомендується використовувати алгоритми гешування з сіллю, що ускладнює генерацію гешів за допомогою таблиць, а також алгоритми з регульованою складністю, такі як Argon2, які підвищують витрати ресурсів на злом [3].

Також важливо впровадити механізми, які забезпечують стійкість до квантових обчислень, оскільки розвиток квантових комп'ютерів може зробити традиційні геш-функції вразливими. Наприклад, алгоритм SHA-3 (Keccak) вважається більш стійким до потенційних квантових атак у майбутньому [4].

Аналіз показав, що геш-функції MD5 і SHA-1 більше не відповідають сучасним вимогам безпеки через їх низьку стійкість до колізій та наявність успішних атак. SHA-256 та Keccak-256 забезпечують високий рівень криптографічної надійності, що робить їх основними алгоритмами безпеки для блокчейнів, таких як Bitcoin і Ethereum. Якщо замінити SHA-1 на SHA-3, то системи стануть більш стійкими до потенційних атак, зокрема загроз з боку квантових комп'ютерів, завдяки вдосконаленій архітектурі та високій криптографічній стійкості.

Окрім технічних нюансів, значущу роль у безпеці смарт-контрактів відіграє грамотне керування ключами. Втрата секретного ключа може призвести до повного контролю над контрактом з боку третіх осіб. З цією метою застосовуються апаратні гаманці, захищені середовища виконання (TEE), а також методи децентралізованого зберігання ключів, які мінімізують ймовірність компрометації. Надійне керування ключами є основоположним елементом загальної стратегії кібербезпеки в екосистемі блокчейн.

Захист смарт-контрактів вимагає не лише використання надійних геш-функцій. Також необхідний комплексний підхід, що включає застосування додаткових механізмів захисту, таких як багатофакторна автентифікація, оновлення алгоритмів та аудит безпеки. Крім того, для зменшення ризику атак рекомендується використовувати багаторівневий підхід до безпеки, що поєднує кілька методів шифрування. Використання сучасних криптографічних методів може допомогти зменшити ризик атаки та підвищити довіру до блокчейн-програм.

Список літератури

1. Вимоги до безпеки смарт-контрактів у фінансових застосунках: ключові аспекти та рекомендації. URL: https://cryptoznannya.com.ua/vimogi-do-bezpeki-smart-kontraktiv-u-finansovix-zastosunkax/.

2. Аналіз і обгрунтування використання наявних блокчейн-рішень для захисту цифрових активів. URL:https://openarchive.nure.ua/entities/publication/64a5900f-8de4-4582-ad1b-7cf88140bf85.

3. 8 найкращих практик для забезпечення безпеки блокчейну. URL: https://www.h-x.technology/ua/blog-ua/8-best-practices-for-blockchain-security-ua.

4. Зражевський К.П. Дослідження рішень щодо збереження безпеки ключів у блокчейн-технологіях: кваліфікаційна робота (магістерська). ХНУРЕ, 2023.URL:https://openarchive.nure.ua/server/api/core/bitstreams/8622fcbb-630b-4c03-ba51-89cfc4a77bc8/content.