Блокчейн для безпеки ідентифікації та автентифікації

УДК 004.056.5:004.738
Віктор Чешун[1], Євген Майор[2], Наталія Купчик[3]

Хмельницький національний університет, [1]cheshunvn@khmnu.edu.ua, [2]evmaior@khmnu.edu.ua, [3]nataliiakupchyk@khmnu.edu.ua

У традиційних системах ідентифікації дані користувачів зберігаються централізовано, що робить ці системи вразливими до кібератак. Замість цього, блокчейн може використовуватися для зберігання ідентифікаційних даних у розподіленій мережі, де кожен блок містить криптографічно захищену інформацію про користувача. Це забезпечує більшу безпеку, оскільки немає одного центрального пункту вразливості.

Технологія блокчейн не зберігає цифрові дані, замість цього у хронологічній послідовності фіксуються всі перевірені транзакції. Ці транзакції об'єднуються в блоки, які в свою чергу утворюють ланцюжки. Спроби змінити або видалити будь-які записи призведе до порушення цілісності ланцюжка блоків.

Основним призначенням цієї технології є захист персональних даних за допомогою криптографії. Після формування транзакційних даних в блоки вони проходять криптографічну перевірку та записуються в базу даних. Усі дані, пов'язані з блокчейном, зберігаються у децентралізованій мережі з високим рівнем захисту. Доступ до цієї мережі здійснюється за допомогою спеціальних криптографічних ключів, що робить неможливим підроблення інформації, яка знаходиться в мережі [1].

Смарт-контракти, подібно до звичайних контрактів, визначають угоду між двома або більше сторонами. Однак смарт-контракти використовують код для використання переваг технології блокчейн, таких як ефективність, прозорість та безпека. Вони можуть автоматизувати процеси завдяки своїй цифровій природі [2].

Покроковий опис роботи смарт-контракту: 1) Перший крок передбачає створення та узгодження між сторонами угоди, що буде закріплена у смарт-контракті; 2) Смарт-контракт встановлює умови його виклику або виконання. Це може бути здійснено автоматично, якщо виконуються певні попередньо визначені умови; 3) На цьому етапі визначається логіка смарт-контракту через програмування. Смарт-контракт складається з комп'ютерного коду, який містить логіку виконання угоди та управління даними; 4) Для забезпечення безпеки та конфіденційності використовується шифрування. Дані передаються та зберігаються у безпечному форматі. Крім того, використовується технологія блокчейну для зберігання даних та підтвердження їх унікальності; 5) Коли виконуються умови, визначені в смарт-контракті, він автоматично виконується. Після виконання смарт-контракту дані обробляються та результати записуються у блокчейн; 6) Після виконання смарт-контракту всі вузли мережі оновлюють свої дані, щоб відобразити новий стан. Зміни в мережі реєструються у блокчейні, і після підтвердження їх не можна змінити або вилучити.

Для поліпшення рівня захисту та перевірки ідентичності задіяне використання унікальних біометричних даних. Ці дані можуть бути використані для надійної аутентифікації особи та її ідентичності. Пропонується інтегрувати біометричні дані

в систему блокчейну з метою забезпечення ще вищого рівня безпеки та конфіденційності.

Дослідження підкреслює важливість використання біометричних даних у контексті блокчейну для покращення систем ідентифікації. Шляхом використання смарт-контрактів у приватній блокчейн-інфраструктурі, дослідники розробили механізм, що спрощує систему біометричної автентифікації обличчя та забезпечує її безпеку. Цей метод демонструє високу продуктивність та ефективність на різних наборах даних, що свідчить про його потенціал для застосування в різних галузях, включаючи IoT [3].

Зберігання біометричних даних тягне за собою правові аспекти, тому використання технології нульового знання (Zero-knowledge proof) може вирішити цю проблему. ZKP - це криптографічний протокол, що дозволяє переконати одну сторону у правильності певного факту, не розголошуючи конкретні дані. У контексті зберігання біометричних даних в блокчейні ZKP використовується для підтвердження достовірності даних без їх розкриття. Користувач генерує докази, що його біометричні дані відповідають певним параметрам, але сторона перевірки не отримує доступ до самого зображення чи даних. Такий підхід забезпечує високий рівень конфіденційності та безпеки при зберіганні чутливих даних в блокчейні.

За допомогою смарт-контрактів на блокчейні можна розробити систему ідентифікації та автентифікації, яка забезпечить користувачам контроль над їхніми особистими даними та приватністю. Ця система дозволить користувачам керувати доступом до своїх ідентифікаційних даних та надавати їх іншим сторонам тільки за власною згодою, що підвищить рівень довіри та безпеки. Використання блокчейну для реалізації цієї системи дозволить забезпечити надійність, унікальність та безпеку даних, а також забезпечить стійкість до зловживань та атак. Такий підхід може бути корисним для різноманітних сфер, включаючи фінанси, медицину, торгівлю та інші галузі, де важливо забезпечити високий рівень захисту особистих даних та конфіденційності.

Інтеграція біометричних даних у систему блокчейну відкриває шлях до надійної та безпечної ідентифікації. Це поєднання забезпечує не лише високий рівень захисту особистих даних, але й відкриває нові можливості для автентифікації та авторизації користувачів. Впровадження цього підходу в системи ідентифікації може мати значний вплив на різні сфери, від фінансів до медицини, сприяючи підвищенню безпеки та конфіденційності особистих даних.

1. Blockchain технології та захист даних. URL: https://newline.tech/blockchain-technology-and-protecting-data-uk/ (дата звернення: 11.04.2024).
2. How smart contracts work with blockchain: A step-by-step guide. URL: https://www.britannica.com/money/how-smart-contracts-work (дата звернення: 11.04.2024).
3. Salem, S.H.G., Hassan, A.Y., Moustafa, M.S. et al. Blockchain-based biometric identity management. Cluster Comput (2023). https://doi.org/10.1007/s10586-023-04180-x