

БЕЗПЕЧНИЙ МЕНЕДЖЕР ПАРОЛІВ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Вінницький національний технічний університет

Анотація

У роботі запропоновано концепцію безпечного менеджера паролів на основі технології блокчейн. Розглянуто переваги використання децентралізованого підходу до збереження паролів, що забезпечує захист від злому та втрати даних. Описано алгоритм роботи системи, а також потенційні виклики, пов'язані з масштабованістю та ефективністю.

Ключові слова: блокчейн, менеджер паролів, кібербезпека, криптографія, децентралізація

Abstract

The paper presents the concept of a secure password manager based on blockchain technology. The advantages of using a decentralized approach to password storage, which ensures protection against hacking and data loss, are considered. The system's operating algorithm is described, as well as potential challenges related to scalability and efficiency.

Keywords: blockchain, password manager, cybersecurity, cryptography, decentralization

Вступ

У сучасному цифровому світі кібербезпека є однією з ключових проблем, з якими зустрічаються користувачі та організації. Зростання кількості онлайн-сервісів та необхідність запам'ятовування великої кількості паролів призводить до використання слабких або повторюваних комбінацій, що значно підвищує ризик компрометації даних. Традиційні менеджери паролів[1], що зберігають дані централізовано, можуть стати мішенню для хакерських атак, оскільки злом такого сервісу ставить під загрозу велику кількість користувачів одночасно.

Блокчейн-технології пропонують новий підхід до управління паролями, забезпечуючи децентралізацію, криптографічний захист та прозорий механізм доступу. Використання розподілених реєстрів усуває єдину точку відмови, а смарт-контракти можуть автоматизувати управління доступом без посередників. У даній роботі розглянуто концепцію безпечного менеджера паролів на блокчейні, його архітектуру, алгоритми роботи, а також переваги та виклики, пов'язані з впровадженням цієї технології.

Метою дослідження є покращення доступності в засобах управління паролями шляхом усунування єдиної точки відмови.

Результати дослідження

Запропонований підхід до створення безпечного менеджера паролів на основі блокчейн-технологій[2] було проаналізовано з точки зору безпеки, продуктивності та ефективності управління даними. Основні переваги такого підходу включають децентралізоване збереження інформації,

неможливість підробки або видалення записів, а також підвищену стійкість до хакерських атак. Водночас існують певні виклики, такі як швидкість обробки транзакцій, вартість використання блокчейн-мережі та складність інтеграції з відомими сервісами.

Розроблено архітектуру мобільного застосунку для керування паролями на основі блокчейну, показано на рисунку 1.

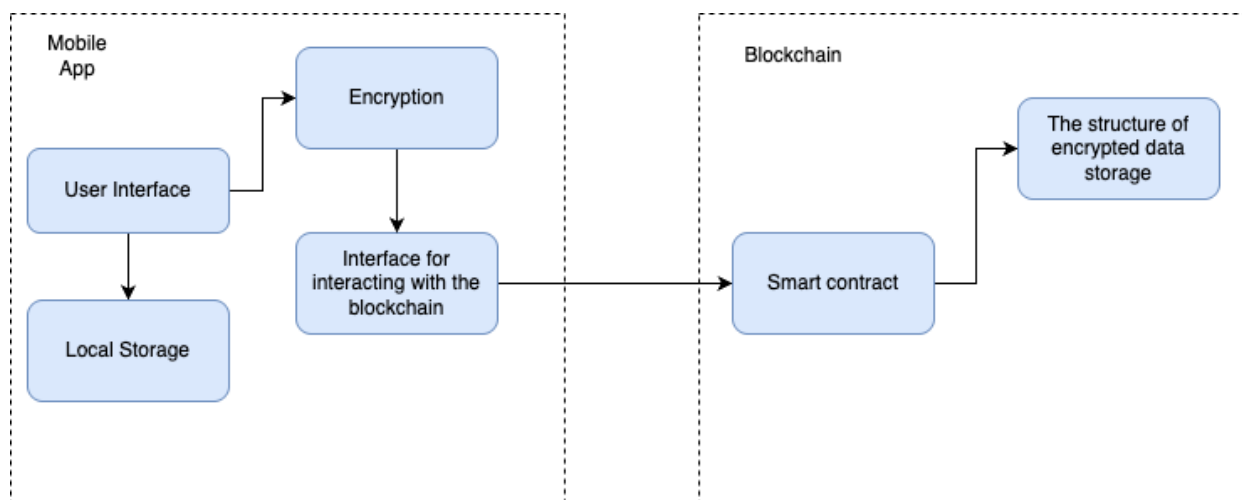


Рисунок 1. Архітектура безпечного менеджера паролів

Також аналіз показав, що блокчейн-менеджери паролів забезпечують значно вищий рівень безпеки порівняно з традиційними рішеннями, проте їхня продуктивність і вартість залишаються відкритими питаннями для подальшого дослідження. Особливу увагу необхідно приділити оптимізації швидкості роботи, розробці ефективних механізмів відновлення доступу та зниженню вартості використання блокчейн-інфраструктури.

Висновки

Запропонований блокчейн-менеджер паролів забезпечує високий рівень безпеки та захисту конфіденційних даних завдяки децентралізованому збереженню інформації та криптографічним методам автентифікації. На відміну від традиційних рішень, блокчейн-менеджер усуває єдину точку відмови, що значно знижує ризик злому та компрометації даних. Смарт-контракти дозволяють автоматизувати процеси управління доступом, підвищуючи ефективність роботи системи.

Водночас існують певні виклики, зокрема швидкість обробки транзакцій, вартість використання блокчейн-інфраструктури та складність інтеграції з існуючими сервісами. Для широкого впровадження такої технології необхідна подальша оптимізація продуктивності, розробка ефективних механізмів відновлення доступу та зниження витрат на транзакції.

Перспективними напрямками досліджень є вдосконалення алгоритмів шифрування, впровадження гібридних рішень для підвищення продуктивності, а також розробка користувацьких інтерфейсів, які забезпечать зручність та доступність використання блокчейн-менеджера паролів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Bitwarden. Mode of access: <https://bitwarden.com/help> (accessed: 20.03.2025).
2. SAASPASS. Mode of access: <https://saaspass.com/about> (accessed: 20.03.2025).

Ткачук Максим Ігорович — студент групи ІБС-24м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: max200325622@gmail.com

Науковий керівник: **Баришев Юрій Володимирович** — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: yuriy.baryshev@vntu.edu.ua.

Maksym Tkachuk — student of 1BC-24M group, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: max200325622@gmail.com

Scientific supervisor: **Yurii Baryshev** — PhD (eng), associated professor of information protection department, Vinnytsia National Technical University, Vinnytsia, email: yuriy.baryshev@vntu.edu.ua