УДК 004.04

В. А. Шатайло
Н. О. Черневський

АНАЛІЗ СТІЙКОСТІ БЛОКЧЕЙН-ПЛАТФОРМ ДО КІБЕРАТАК

Вінницький Національний Технічний Університет

Анотація
У даній роботі розглянуто основні аспекти функціонування блокчейн-технологій, їх можливості та обмеження.
Ключові слова: Блокчейн, криптографія, криптовалюта, безпека.

Abstract
This work examines the main aspects of the functioning of blockchain technologies, their possibilities and limitations.
Keywords: Blockchain, cryptography, cryptocurrency, security.

Вступ

Блокчейн-технологія, яка за останні роки стала справжньою революцією в цифровій економіці, є не просто новим засобом обробки даних, а фундаментально новим підходом до зберігання та передачі інформації [1]. Основна ідея полягає в тому, що дані зберігаються у вигляді блоків, які формують ланцюг і містять інформацію про всі попередні операції. Кожен блок підтверджується всіма учасниками мережі (нодами), і якщо хтось намагається змінити інформацію, це миттєво помічають інші. Це схоже на книгу обліку, яку одночасно ведуть і контролюють тисячі користувачів: зміни в одному місці стають видимими для всіх.

Огляд та аналіз

Розглянемо приклад: уявімо, що Олена хоче відправити Павлу криптовалюту. Коли вона створює запит на переказ, ця транзакція потрапляє до блокчейну, де її перевіряють та підтверджують інші учасники мережі. Як тільки транзакція підтверджена, її записують у блок, і цей блок стає частиною незмінного ланцюжка. Важливість полягає в тому, що ні Олена, ні Павло, ні хто-небудь інший не зможуть змінити цей запис — він залишиться в блокчейні назавжди. Це робить блокчейн надзвичайно корисним для запису важливих операцій, таких як фінансові транзакції, контракти, записи про права власності.

Власне, блокчейн і створений для зберігання криптовалютних операцій, таких як біткоїн, який був першою реалізацією цієї технології. Біткоїн надає людям змогу переказувати кошти безпосередньо один одному, без участі банків чи державних органів [4]. Наприклад, уявіть собі ситуацію, коли хтось хоче перевести кошти зі США до України. Зазвичай це займає кілька днів через банки і передбачає додаткові витрати на комісії. Однак через біткоїн та інші криптовалюти переказ здійснюється практично миттєво, безпосередньо між користувачами і з мінімальними комісіями, незалежно від відстані чи кордонів.

Захищеність блокчейну також пояснюється його децентралізацією — замість зберігання даних на одному сервері, як у традиційних системах, дані розподіляються між тисячами пристроїв по всьому світу. Це означає, що навіть якщо хакери намагатимуться зламати одну частину мережі, їм не вдасться знищити або змінити дані, оскільки вони існують і контролюються на інших пристроях. Наприклад, у випадку зі звичайним банком, злом сервера може призвести до крадіжки особистих даних або навіть коштів користувачів [5]. У блокчейні подібний злом потребуватиме отримання контролю над більшістю обчислювальної потужності всієї мережі, що в більшості випадків є надзвичайно складним, а іноді й практично неможливим завданням.

Втім, блокчейн теж має свої уразливості. Одна з них — атака 51%, коли група зловмисників отримує контроль над більш ніж половиною обчислювальної потужності мережі. Це дає їм можливість змінювати блоки і навіть здійснювати подвійні витрати — ситуацію, коли одні й ті ж кошти використовуються в різних транзакціях. В історії криптовалют таке траплялося з менш популярними

монетами, де мережа була менш захищеною, аніж у біткоїна. Наприклад, у 2018 році криптовалюта Verge зазнала атаки 51%, в результаті якої зловмисники змогли викрасти кошти, маніпулюючи записами у блокчейні [3].

Інша вразливість пов'язана зі смарт-контрактами, які використовуються в блокчейнах для виконання автоматизованих угод. Смарт-контракти — це програмний код, який автоматично виконує умови угоди, записані у ньому. Наприклад, можна налаштувати смарт-контракт для управління спільним інвестиційним фондом: кожен, хто вносить гроші, автоматично отримує частку від прибутку. Проте якщо код смарт-контракту містить помилку, хакери можуть скористатися нею для маніпуляцій. Так сталося в 2016 році з децентралізованою платформою The DAO на основі блокчейну Ethereum, коли через вразливість у смарт-контракті зловмисникам вдалося викрасти близько $60 млн [2].

Криптографія є ще одним важливим аспектом захисту блокчейну. Наприклад, для кожної транзакції генерується унікальний цифровий підпис, заснований на криптографічному алгоритмі, який підтверджує автентичність даних і гарантує, що транзакція була відправлена саме тим, хто її створив. Завдяки цьому неможливо підробити транзакцію чи змінити її без дозволу власника. Однак з появою квантових комп'ютерів поточні методи криптографії можуть стати менш ефективними, і тому дослідники вже працюють над квантово-стійкими алгоритмами, які можуть протистояти потужності квантових обчислень.

Висновки

Отже, блокчейн пропонує високий рівень захищеності і прозорості для цифрових транзакцій, але залишається вразливим до певних загроз. З огляду на постійний розвиток технологій, критично важливо досліджувати нові способи захисту, вдосконалювати існуючі алгоритми і забезпечувати стабільну роботу смарт-контрактів. Удосконалення безпеки блокчейну є не тільки технічним завданням, а й обов'язковою умовою для підтримки довіри користувачів і широкого впровадження цієї технології у світовій економіці.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What is Blockchain Technology? How Does Blockchain Work? [Електронний ресурс]. – Режим доступу: https://www.simplilearn.com/tutorials/blockchain-tutorial/blockchain-technology

2. Що таке DAO у криптовалюті: як працює децентралізоване управління на блокчейні [Електронний ресурс]. – Режим доступу: https://trusteeglobal.com/academy/shho-take-dao-u-kryptovalyuti-yak-praczyuye-deczentralizovane-upravlinnya-na-blokchejni/

3. Блокчейн Verge знову зазнав атаки 51% [Електронний ресурс]. – Режим доступу: https://happycoin.club/uk/blokcheyn-verge-snova-podvergsya-atake-51/

4. Що таке блокчейн і як він працює? [Електронний ресурс]. – Режим доступу: https://academy.binance.com/uk/articles/what-is-blockchain-and-how-does-it-work

5. (Не)безпечний блокчейн. Як шахраї крадуть криптовалюту [Електронний ресурс]. – Режим доступу: https://mind.ua/publications/20250712

Шатайло В'ячеслав Андрійович — студент групи 2СП-21б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький Національний Технічний Університет, Вінниця, e-mail: viacheslavshatailo@gmail.com

Черневський Назар Олександрович — студент групи 2СП-21б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький Національний Технічний Університет, Вінниця, e-mail: chernevskijnazar@gmail.com

Shatailo Viacheslav Andriyovych — student of group 2SP-21b, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: viacheslavshatailo@gmail.com

Chernevskyi Nazar Oleksandrovich — student of group 2SP-21b, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: chernevskijnazar@gmail.com