

ВИКОРИСТАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ДЛЯ ЗБЕРІГАННЯ ЛОГІВ І КЛЮЧІВ У VPN-ІНФРАСТРУКТУРІ

Вінницький національний технічний університет

Анотація

Дана робота досліджує концепцію децентралізованої VPN-інфраструктури на основі блокчейн-технологій. Традиційні VPN-системи мають вразливість через централізоване зберігання логів та ключів, що створює ризик компрометації. Запропонована концепція передбачає використання блокчейну для децентралізованого зберігання логів доступу та ключів шифрування, що підвищує безпеку, прозорість та відмовостійкість системи. Також пропонується новий механізм динамічної ротації ключів залежно від рівня загрози та активності користувача. Розглянуті переваги та технічні виклики реалізації такої системи, а також перспективи її застосування в корпоративному секторі.

Ключові слова: VPN (віртуальна приватна мережа); блокчей; децентралізація; безпека; ключі шифрування; смарт-контракти; відмовостійкість; конфіденційність; корпоративна безпека; кібербезпека.

Abstract

This paper explores the concept of decentralized VPN infrastructure based on blockchain technologies. Traditional VPN systems are vulnerable due to centralized storage of logs and keys, which creates a risk of compromise. The proposed concept involves using blockchain for decentralized storage of access logs and encryption keys, which increases the security, transparency, and fault tolerance of the system. A new mechanism for dynamic key rotation depending on the threat level and user activity is also proposed. The advantages and technical challenges of implementing such a system are considered, as well as the prospects for its application in the corporate sector.

Keywords: VPN (virtual private network); blockchain; decentralization; security; encryption keys; smart contracts; fault tolerance; confidentiality; corporate security; cybersecurity.

Вступ

Сучасні VPN-системи зазвичай покладаються на централізовані сервери для зберігання ключів та логів. Це означає, що вся критично важлива інформація знаходиться в одному місці, і якщо цей сервер буде зламано або виведено з ладу, компанія може втратити контроль над своїм VPN, а зловмисники – отримати доступ до конфіденційних даних.

VPN (Virtual Private Network) є основним інструментом для забезпечення конфіденційності та безпеки корпоративних мереж. Однак традиційні VPN-рішення мають низку вразливостей, зокрема централізоване зберігання логів та криптографічних ключів, що створює єдину точку відмови та підвищує ризик компрометації.

Запропонована концепція передбачає інтеграцію блокчейн-технологій у VPN-інфраструктуру для децентралізованого зберігання логів доступу та ключів шифрування, що дозволить підвищити безпеку, прозорість і відмовостійкість системи.

Основна частина

У класичних VPN-рішеннях журнали активності та ключі зберігаються на серверах провайдера або корпоративних хостах. Це призводить до таких ризиків:

1. Єдина точка відмови – централізоване зберігання даних означає, що атака або злам VPN-сервера може призвести до втрати всіх логів і ключів.

2. Можливість маніпуляції даними – адміністратори або сторонні особи можуть змінювати або видаляти логи активності, приховуючи сліди компрометації.

3. Ризик несанкціонованого доступу – централізовані сервери можуть стати мішенню для хакерських атак або компрометації внутрішніми співробітниками.

Блокчейн – це незмінна, безпечна та прозора технологія. Ці переваги роблять його ідеальним союзником для захисту цифрових інфраструктур. Блокчейн пропонує багатообіцяючі перспективи для захисту інформаційних систем і розробки кіберінструментів, які повністю або частково покладаються на цю технологію.

Блокчейн можна визначити як «реєстрацію, велику базу даних, яка одночасно використовується для всіх її користувачів, усі з яких також є власниками цієї книги, і всі вони можуть записувати в неї дані відповідно до певних правил, встановлених високо захищеним комп'ютерним протоколом із використанням криптографії».

Іншими словами, це велика книга, в якій дані зашифровані та захищені за допомогою процесів децентралізації та консенсусу, які забезпечують безпеку як технології (через консенсус), так і даних (через незмінну та децентралізовану інтеграцію) [1].

Пропонується використовувати блокчейн як сховище ключів. Тобто коли користувач підключається до VPN, генерується сеансовий ключ (AES-256 або ChaCha20) для шифрування з'єднання. Цей ключ шифрується ще одним рівнем безпеки – довготривалим ключем, який у свою чергу ділиться на частини (Shamir's Secret Sharing) та розподіляється між вузлами блокчейну. Щоб отримати доступ до ключа, потрібно підтвердження з кількох незалежних вузлів, що робить неможливим його викрадення шляхом злому одного сервера. Таким чином, навіть якщо зломисник отримає доступ до частини блокчейн-мережі, він не зможе зібрати повний ключ без доступу до всіх вузлів.

Однією з проблем VPN є можливість маніпулювання логами – адміністратор сервера може змінити або видалити записи активності користувачів, що ускладнює виявлення загроз або аудит безпеки.

Необхідно зберігати логи у блокчейні, що гарантує їхню незмінність:

- кожен запис VPN-з'єднання (час підключення, IP-адреса, використаний сервер) хешується та додається в блокчейн;

- використання SHA-3 та механізму "ланцюга блоків" означає, що змінити або видалити ці дані неможливо – будь-яка модифікація буде одразу помітною [2];

- доступ до логів можливий тільки через смарт-контракти, які обмежують коло осіб, що можуть їх переглядати (наприклад, лише керівництво компанії або незалежний аудитор).

Такий підхід забезпечує високу прозорість та неможливість приховати підозрілу активність, що критично важливо для компаній із суворими вимогами до безпеки.

Щоб забезпечити безпечний доступ до ключів і логів, пропонується використовувати смарт-контракти на Ethereum.

Якщо адміністратор або користувач VPN запитує доступ до логів або ключів, смарт-контракт перевіряє його права. Також усі запити логуються в блокчейні, що унеможливорює несанкціоновані зміни. І якщо виявляється спроба підробки або зміни даних, система блокує доступ і повідомляє про можливу атаку.

Завдяки цьому компанія отримує автоматизовану систему контролю, де немає необхідності довіряти одному адміністратору або провайдеру VPN – усі дії підтверджуються блокчейном, що гарантує їхню достовірність. [3]

Переваги даного підходу:

- неможливість підробити або змінити дані – усі ключі та логи розподілені між вузлами, а будь-яка спроба зміни буде зафіксована;

- відсутність єдиної точки відмови – навіть якщо один вузол мережі вийде з ладу, система продовжить функціонувати;

- високий рівень конфіденційності – адміністраторам та провайдерам VPN не потрібно довіряти керування всією системою, оскільки контроль здійснюється автоматично;

- можливість роботи в Zero Trust середовищах – корпоративні VPN можуть функціонувати без необхідності повної довіри до адміністратора або сервера.

Окрім базового використання блокчейну, пропонується новий механізм динамічної ротації ключів залежно від рівня загрози та активності користувача.

Спочатку система аналізує VPN-трафік у реальному часі. Потім при виявленні аномалій (наприклад, підключення з невідомого IP або різка зміна обсягу трафіку) генерується новий ключ. Старий ключ автоматично додається у блокчейн і стає недоступним для використання. І як результат користувач отримує оновлений ключ без розриву VPN-з'єднання.

Переваги такого підходу:

- виключення ризику повторного використання скомпрометованого ключа;

- захист від атак на VPN-сервер, оскільки ключі не зберігаються в одному місці;

- автоматичне оновлення без необхідності ручного управління адміністратором.

Висновки

Розглянута концепція децентралізованої VPN-інфраструктури на основі блокчейну відкриває нові можливості для корпоративної безпеки. Замість традиційного підходу, коли управління логами та ключами здійснюється централізовано, що створює потенційні ризики злову або маніпуляції даними, запропонована система дозволяє рівномірно розподіляти інформацію між вузлами, мінімізуючи можливість її компрометації.

Основні переваги цього рішення:

- висока відмовостійкість – у разі виходу з ладу окремого сервера мережа продовжує функціонувати без втрати даних.

- захист від маніпуляцій – збереження логів у блокчейні унеможлиблює їхнє підроблення або приховування.

- безпека ключів – секретний ключ розділяється та зберігається в розподіленій мережі, що знижує ризик його викрадення.

- прозоре управління доступом – використання смарт-контрактів виключає вплив людського фактора при перевірці прав доступу.

Така система може бути особливо ефективною в умовах підвищених кіберзагроз, коли компанії потребують не тільки потужного шифрування даних, а й гарантії того, що їхні журнали з'єднань та ключі залишаться в безпеці навіть у разі внутрішніх загроз або компрометації окремих вузлів мережі.

Проте, для повноцінної реалізації такого рішення необхідно подолати низку технічних викликів, зокрема оптимізацію швидкості доступу до блокчейну, оскільки запис та зчитування даних у розподіленій мережі потребує більше ресурсів, ніж у централізованих рішеннях. Також важливим аспектом є масштабованість – у разі збільшення кількості користувачів система повинна залишатися стабільною та швидкодіючою.

У майбутньому подібні технології можуть стати стандартом у сфері корпоративних VPN-рішень, забезпечуючи не лише високий рівень безпеки, а й повну довіру до збережених даних без необхідності покладатися на адміністратора чи провайдера. Це відкриває

перспективи для розробки автономних, самокерованих VPN-систем, де рівень захисту залежатиме не від людини, а від математичних алгоритмів і криптографічних принципів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cybersecurity and Blockchain: What are the prospects? [Електронний ресурс]. Режим доступу: <https://incyber.org/en/article/cybersecurity-blockchain-what-prospects/>
2. Хеш-функція SHA-3 [Електронний ресурс]. Режим доступу: <https://ukr.media/criptovalyta/362440/>
3. What is Ethereum? [Електронний ресурс]. Режим доступу: https://www.fidelitydigitalassets.com/sites/g/files/djuvja3256/files/acquiadam/1024435.2.0%20FDA%20Ethereum%20Report_final%20design.pdf

Гулевата Анжеліка Андріївна – студентка групи 2KITC-216, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: gulevataanzhelika@gmail.com

Науковий керівник: **Грицак Анатолій Васильович** – доцент каф. Менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: grytsak.a.v@gmail.com

Hulevata Anzhelika Andreivna – student of group 2CITS-21b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: gulevataanzhelika@gmail.com

Supervisor: **Hrytsak Anatolii Vasyliovych** – docent of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: grytsak.a.v@gmail.com