УДК 004.056:004.6

БЕЗПЕЧНІСТЬ ЗБЕРІГАННЯ КЛЮЧІВ У EVM-БЛОКЧЕЙНАХ

Зражевець К.П.
Науковий керівник – к.т.н., доцент Куля Ю.Е.
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна
тел. +38(050) 100-20-37

This work is an overview of various solutions for storing and securing private keys in EVM-compatible blockchains. It discusses hardware wallets, which are physical devices storing private keys in a secure environment, hot wallets that store keys on internet-connected devices, and cold wallets that store keys on devices without constant internet connection. The text also covers multi-signature technology, which requires signatures from multiple parties to execute a transaction, and protocol-level security mechanisms that utilize asymmetric encryption or distributed key storage. Additionally, the importance of backup and restoration of keys, different access levels, two-factor authentication, regular software updates, and risk management is addressed.

В EVM-сумісних блокчейнів можуть бути використані різні рішення для збереження та захисту приватних ключів.

1) Апаратні гаманці – фізичні пристрої, які зберігають приватні ключі в безпечному середовищі, відрізняючись від інтернет-з'єднаних пристроїв. Наприклад, Ledger Nano S та Trezor.
2) Гарячі гаманці – це програмні гаманці, які зберігають ключі на пристроях з підключенням до Інтернету, забезпечуючи швидкий доступ до коштів. Наприклад, MetaMask та MyEtherWallet.
3) Холодні гаманці – це програмні гаманці, які зберігають ключі на пристроях без постійного з'єднання до Інтернету, забезпечуючи високий рівень безпеки. Наприклад, Electrum та Armory [1].

Мультипідпис – це технологія, яка вимагає підпису декількох сторін для здійснення транзакції. Це дозволяє створити додатковий рівень безпеки, оскільки зловмисникам потрібно скомпрометувати кілька приватних ключів для доступу до коштів. Такі гаманці зазвичай використовуються для спільного управління активами або корпоративних рахунків [2].

Безпека ключів на рівні протоколу: деякі EVM-сумісні блокчейни можуть використовувати вбудовані механізми безпеки для захисту приватних ключів на рівні протоколу. Це може включати рішення, які використовують асиметричне шифрування, щоб передавати ключі між учасниками мережі, або розподілене зберігання ключів, де кожен учасник мережі зберігає лише частину ключа.

Резервне копіювання та відновлення ключів: безпека приватних ключів також забезпечується шляхом створення резервних копій та можливості відновлення в разі втрати або пошкодження пристрою. Це може включати використання мнемонічних фраз для відновлення ключів або регулярне створення резервних копій гаманця на безпечному пристрої.

Використання різних рівнів доступу: ще одним способом забезпечення безпеки приватних ключів є створення різних рівнів доступу до коштів. Наприклад, можна створити гаманець з обмеженим доступом для повсякденних витрат, а гаманець з повним доступом використовувати для зберігання великих сум коштів або управління корпоративними активами. Такий підхід дозволяє зменшити ризик втрати великих сум коштів у разі компрометації одного з гаманців, оскільки доступ до основних активів обмежений [3]. Двофакторна автентифікація: для додаткової безпеки приватних ключів, деякі гаманці та платформи можуть пропонувати двофакторну автентифікацію. Найпопулярніші методи 2FA включають одноразові паролі (OTP), які надсилаються через SMS або генеруються спеціальними додатками, та біометричні методи, такі як відбитки пальців чи розпізнавання обличчя.

Регулярне оновлення програмного забезпечення: щоб забезпечити найвищий рівень безпеки для приватних ключів, важливо регулярно оновлювати програмне забезпечення гаманця та пристроїв, на яких він встановлений. Виробники апаратних та програмних гаманців часто випускають оновлення, які включають покращення безпеки та виправлення вразливостей. Слідкування за оновленнями і своєчасне їх встановлення може допомогти запобігти можливим атакам.

Управління ризиками: крім того, важливо розуміти та управляти ризиками, пов'язаними зі зберіганням приватних ключів. Це може включати розподіл активів між декількома гаманцями, використання різних методів зберігання ключів та регулярне перевіряння своїх рішень з погляду безпеки.

Список використаних джерел:

1. ConsenSys: EVM-Compatible Blockchain Security Features https://consensys.net/blockchain-use-cases/evm-compatible-blockchain-security-features/
2. CoinCentral: What is Multisig? https://coincentral.com/what-is-multisig/
3. Crypto Security Best Practices https://www.coindesk.com/learn/bitcoin-101/crypto-security-best-practices