УДК 681.301

Д. І. Лясковська[1]
В. І. Маліновський[2]

ПІДХОДИ ТА СПОСОБИ ЗАХИСТУ КЛЮЧОВОЇ ІНФОРМАЦІЇ В МЕРЕЖАХ БЛОКЧЕЙН

[1] **Вінницький національний технічний університет**

Анотація.
Розглянуто технологію блокчейн, характерні особливості та основні вразливості. Визначено можливі способи зберігання ключів гаманців блокчейн. Розглянуто технологію Multisig та її використання в мережах блокчейн.
Ключові слова: Блокчейн, Біткоїн, Ефір, криптовалюта, мультипідпис.

Abstract.
Blockchain technology, characteristics and main vulnerabilities are considered. Possible ways to store keychain wallet keys are identified. MultiSig technology and its use in blockchain networks are considered.
Keywords: Blockchain, Bitcoin, Ether, cryptocurrency, MultiSig.

Вступ

У зв'язку зі збільшенням вартості криптовалюти Біткоїну (Bitcoin) на торговому ринку збільшилась зацікавленість людей в криптовалюті та технології блокчейн-мереж вцілому. Вважається, що інформаційні системи на основі технології блокчейн майже не мають вразливостей, а клієнт, що використовує вказану інформаційну систему не несе ніяких матеріальних збитків. Однак технологія блокчейн має низку вразливостей та потенційних ризиків впровадження кіберзагроз.

Метою роботи є аналіз технології блокчейн, її недоліків та можливі способи протидіїї дослідженим вразливостям.

Результати дослідження

Блокчейн – це технологія розподіленого децентралізованого мережевого зберігання, оброблення і передавання даних зі синхронізацією, у якій дані зберігаються і розподілені між великою кількістю вузлів базі даних, що доступні всім користувачам мережі.

До характерних особливостей технології блокчейн відносяться: децентралізація, прозорість, необмеженість, надійність, стійкість до модифікації даних.

Серед відомих вразливостей технології блокчейн є атака 51%, атака подвійної витрати, крадіжка або втрата ключової пари, інші порушення і перехоплення даних авторизації та аутентифікації користувачів.

Доступ до гаманця користувача здійснюється за допомогою пари приватного та публічного ключів. Особливу увагу в інформаційній системі на основі блокчейн потрібно приділити захисту приватного ключа гаманця, адже знання приватного ключа дає змогу повністю управляти гаманцем користувача. У разі втрати або крадіжки приватного ключа користувач не має змоги відновити ключову інформацію, що призводить до втрати можливості управління гаманцем.

Управління гаманцем відбувається за допомогою: десктопного гаманця, з використанням сторонніх сервісів або апаратного гаманця.

При використанні десктопного гаманця приватний ключ захищається за допомогою паролю, який зберігається локально на комп'ютері користувача. Перевагою використання даного гаманця заключаються в безпеці та невеликій вартості.

Сторонні сервіси виступають в ролі посередника між користувачем і кінцевою системою. Простота використаня сторонніх сервісів є зручною для користувача, але все управління безпекою делегується на сервіс.

Апаратні гаманці зберігають ключі доступу на спеціальних фізичних пристроях. Для виконання

транзакції потрібне підтвердження користувача у вигляді представлення біометрії або паролю на самому пристрою. Перевагами використання апаратного гаманця є безпеку, недоступність через глобальну мережу інтернет. Недоліком використання даного гаманця є велика вартість пристрою.

Для підвищення рівня захисту ключової інформації гаманця використовують мультипідпис.

Мультипідпис (MultiSig) – це технологія підписання транзакцій декількома приватними ключами для підвищення рівня безпеки та конфіденційності в процесі схвалення відправки транзакцій. Використання MultiSig дозволяє розділити право управління гаманцем між декількома приватними ключами, що дає змогу знизити ризик втрати доступу до гаманця в разі втрати або крадіжки одного з приватних ключів. Дана технологія являє собою спеціальний тип електронного цифрового підпису. До основних переваг Multisig відноситься: підвищена безпека, можливість проведення транзакції з використанням третьої сторони, яка виступає взаємодовіреним гарантом. Multisig може використовуватись, як двохфакторна автентифікація для доступу до керування гаманця.

Реалізація MultiSig зележить від мережі в якій вона використовується. В мережі Біткоїн технологія MultiSig підримується на етапі створення гаманця. Використання в мережі Ефіра технології MultiSig не передбачається. Аналогом MultiSig для мережі Ефіра виступають специфічні смарт-контракти, за допомогою яких одна транзакція підписується декількома адресами.

Висновки

Технологія блокчейн вважається перспективним напрямком для подальших досліджень. На основі даної технології було розроблено багато інформаційних систем перш за все пов'язаних з фінансами.

Інформаційні системи побудовані на основі блокчейн повинні мати якомога менше програмних вразливостей, якими може скористатись зловмисник. Тому використання технології MultiSig та смарт-контрактів є можливим рішенням для підвищення безпеки зберігання та використання ключів гаманців.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Данило Скічко, Тетяна Гріненко, Олексій Нарєжній Безпека технології блокчейн для децентралізованих систем — «GLOBAL CYBER SECURITY FORUM 2019» 2019. — 98 с.

2. GDPR та блокчейн: поєднати непоєднане: веб-сайт. URL: https://legalitgroup.com/gdpr-ta-blokchejn-poyednati-nepoyednane/ (дата звернення: 04.03.2021).

3. Что такое мультиподпись? Что такое кольцевая подпись?: веб-сайт. URL: https://forklog.com/chto-takoe-multipodpis/ (дата звернення: 03.03.2021).

4. Гаманці Multisig: веб-сайт. URL: https://exbase.io/uk/wiki/gamanczi-multisig (дата звернення: 04.03.2021).

Лясковська Діана Ігорівна — студентка групи 1БС-17б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, Україна. E-mail: lyaskovskad@gmail.com

Маліновський Вадім Ігорович — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, Україна.

Науковий керівник: ***Маліновський Вадім Ігорович*** — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, Україна.

Liaskovska Diana I. — Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : lyaskovskad@gmail.com

Malinovskyi Vadym I. — PhD(Eng), Associate professor, Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine.