УДК 681.3.07

АНАЛІЗ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ УПРАВЛІННЯ КРИПТОВАЛЮТНИМИ АКТИВАМИ

Сілагін Олексій, Кукунін Сергій, Марков Дмитро

Вінницький національний технічний університет

Анотація

Аналізується методологія створення веб-додатків для управління криптовалютними активами, що одержали назву «криптовалютних гаманців». Робиться висновок, що за критерієм оптимального співвідношення зручності і безпеки на сьогоднішній день найбільш перспективними є мобільні гаманці з прив'язкою до відбитку пальця або FACE ID

Abstract

The methodology for creating web applications for managing cryptocurrency assets, called "cryptocurrency wallets," is analyzed. It is concluded that, by the criterion of optimal balance of convenience and safety, by far the most promising are mobile wallets with fingerprint or FACE ID.

Вступ

На початку третього тисячоліття з'явилися революційні веб-технології, які окрім технічного, мали також соціальний ефект. Мова йде про блокчейн технології та пов'язані з ними криптовалюти. Блокчейн - це децентралізована база даних, заснована на одноранговій мережі, загальному реєстрі і криптографії публічного і приватного ключа. Коли цифрова угода здійснюється в блокчейн, вона групується в криптографічно захищеному блоці з іншими угодами, які відбулися в останні декілька хвилин і розсилається по всій мережі. Підтверджений блок транзакцій потім датується і додається до ланцюга в лінійному, хронологічному порядку. Нові блоки перевірених транзакцій пов'язані з більш старими блоками, утворюють ланцюжок блоків, які показують кожну транзакцію, досягнуту в історії цього блокчейну [1]. Увійшовши в блокчейн-мережу, користувач підключається до інших комп'ютерів мережі для того, щоб обмінюватися з ними даними: блоками і записами. Отримавши нові дані, кожен користувач перевіряє їх коректність, і, переконавшись у достовірності, зберігає їх у себе, а також передає коректні дані далі по мережі. Найбільшого поширення блокчейн технології набули в сфері створення віртуальних грошей – криптовалют, а це в, свою чергу, дало поштовх для створення нового класу веб-додатків для управління криптовалютними активами, що одержали назву «криптовалютних гаманців». Отже криптовалютний гаманець - це додаток, за допомогою якого можна управляти криптовалютою або криптовалютами певного користувача. Основними функціями гаманця є зберігання, а також можливість відправляти і отримувати криптовалюти від інших користувачів. Але на відміну від класичних банківських електронних кабінетів, криптовалютний гаманець має свою специфіку, пов'язану з використаннями блокчейн технологій. На сьогоднішній день відчувається дефіцит зручних, надійних і широкофункціональних сервісів по обслуговуванню криптовалют, тому тему дослідження вважаю актуальною.

Постановка задачі

Хоча з моменту появи першої криптовалюти минуло тільки 10 років, вже склалася певна класифікація криптовалютних гаманців [2,3,4]. Так,за ступінню універсальності, вони можуть бути одновалютними та мультивалютними, за типом зберігання криптовалюти їх можна розділити на «гарячі» і «холодні»; за типом зберігання приватних ключів - на «кастодіальні» і «не кастодіальні», а за типом інсталяції - на локальні, мобільні, серверні, апаратні, браузерні. В найпростішому варіанті - це просто дані, які

забезпечують доступ до свого рахунку. Розглянемо найбільш популярні існуючі рішення криптовалютних гаманців.

Аналіз методології створення криптовалютних гаманців

Криптовалютний гаманець – це, по суті, додаток, за допомогою якого можна зберігати криптовалюту. Хоча і фізично він ніде не зберігається - користувачам просто дають дані, які забезпечують доступ до свого рахунку. Ці дані, в залежності від типу гаманця, можуть являти собою стандартну пару «емейл + пароль», приватний ключ або seed-фразу. Основним завданням гаманця є зберігання, а також можливість відправляти і отримувати криптовалюти від інших людей.

Відмінність між гарячим і холодним гаманцем полягає в тому, що гарячий гаманець працює при підключенні до інтернету, а холодний може працювати і без. Гарячі електронні гаманці менш захищені, так як існує ризик крадіжки ваших персональних даних через інтернет, проте, при цьому вони більш затребувані серед користувачів. Холодні електронні гаманці застосовуються для "холодного зберігання" криптовалюти, тому вони більш безпечні.

Суть кастодіальних гаманців в тому, що вони не дають доступу до свого приватного ключа, а просто зберігають його на своєму централізованому сервері. Найчастіше таке рішення надають криптовалютні біржі. Плюс такого рішення в тому, що можна відновити доступ до облікового запису через пошту, якщо пароль був загублений. Мінус – обліковий запис може бути заморожений в разі якогось втручання, а для розморожування користувача можуть попросити пройти процедуру KYC. Також користувач може втратити гроші під час хакерських атак, що останнім часом є досить частим явищем.

Некастодіальні електронні гаманці працюють інакше - вони надають повний контроль над своїми приватними ключами, не використовуючи сервер. Величезним плюсом такого рішення є те, що кошти належать тільки користувачу. Ніхто інший не зможе ними заволодіти без його seed-фрази. Однак, в цьому полягає і мінус такого гаманця, адже, якщо seed-фраза буде втрачена, то доступ до гаманця вже ніяк не повернути.

Локальний (десктопний) гаманець - це програма, яка встановлюється на стаціонарний комп'ютер або ноутбук. Даний вид гаманців є одним з найскладніших для користувачів, але при цьому володіє найкращими показниками з безпеки і анонімності. Потрібно відзначити, що найчастіше їх використовують досвідченні користувачі або компанії, які проводять розробки на блокчейн-технологіях. Десктопні електронні гаманці можна розділити на 2 види:

- Товстий гаманець – в даному випадку передбачається завантаження на комп'ютер повної копії блокчейна. За фактом, товстий гаманець криптовалют - це повна нода мережі, яка не тільки дозволяє вам керувати своїм рахунком, але і підтримує роботу блокчейна. З огляду на те, що об'єм блокчейн-біткоїна займає вже близько 250Гб, то для роботи гаманця відповідно потрібно високопродуктивне «залізо»;
- Тонкий гаманець ,на відміну від товстого гаманця, займає на комп'ютері всього кілька мегабайт пам'яті і встановлюється за пару хвилин. Це програма-клієнт, для роботи якої не потрібно завантажувати на комп'ютер увесь блокчейн. Він дозволяє створювати адреси криптовалют і виконувати транзакції. З блокчейном тонкий гаманець взаємодіє не безпосередньо, як товсті гаманці, а через сервер розробників програми. Тому вони вважаються менш захищеними, проте набагато зручніше у використанні.

Апаратний гаманець криптовалют це окремий пристрій, що на вигляд нагадує «флешку» [5]. Такий блокчейн-гаманець служить для «холодного» зберігання криптовалют і підключається до інтернету тільки тоді, коли потрібно зробити транзакцію. Апаратні гаманці надають зручний доступ до блокчейну з високим ступенем

захисту, так як приватні ключі зберігаються тільки в пам'яті самого пристрою. Незважаючи на їх вартість, від 60 до 100 доларів, вони дозволяють здійснювати транзакції таким чином, що хакери не можуть до них дістатися. При втраті такого гаманця ніхто крім вас не зможе нічого зробити із засобами, при цьому ви з легкістю зможете відновити до них доступ через seed-фразу на новий пристрій. Тому по співвідношенню надійності і зручності використання лідирують апаратні гаманці.

Web-гаманці або браузерні – ще один, досить простий тип гаманців для використання, він не вимагає від користувача особливих знань в криптовалютах. Більш того, має низку переваг:

- користуватися гаманцем можна на різних пристроях, незалежно від вашого місця знаходження, головне, щоб був вільний доступ до Інтернету;
- немає необхідності в скачуванні всіх блоків мережі, що економить багато часу і дисковий простір;

У більшості, подібні сервіси пропонують своїм користувачам додаткові зручності, такі як відсутність комісії за перекази між користувачами, відправка монет іншим його користувачам на адресу електронної пошти або номер телефону. Однак, потрібно пам'ятати, що такі гаманці мають «кастодіальне» рішення. При використанні Web-гаманця доступ до коштів має і сторонній сервіс. Тому їх збереження залежить вже не тільки від самого користувача. При «зломі» такого ресурсу монети користувачів найімовірніше будуть вкрадені.

Мобільні гаманці криптовалют – це додатки, які можна встановити на мобільні пристрої (смартфони, планшети)[6]. Потрібно відзначити, що вони увібрали в себе всі кращі якості від перерахованих вище видів гаманців. Адже вони можуть бути «не кастодіальними», досить анонімними і при цьому надають доступ до криптовалют в будь-якій точці світу, де є Інтернет. Так як це окремий додаток, то найчастіше розробники наділяють його ще й корисними додатковими функціями. Що стосується безпеки, то мобільні гаманці займають «золоту середину», так як крім звичайного PIN-коду можуть мати прив'язку до відбитку пальця або FACE ID (зазвичай налаштовується користувачем за бажанням).

Висновки

В результаті проведеного аналізу можна зробити висновок, що за критерієм оптимального співвідношення зручності і безпеки на сьогоднішній день найбільш перспективними є мобільні гаманці з прив'язкою до відбитку пальця або FACE ID.

Список використаних джерел

1.Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. [Electronic resource]. – Mode of access https://bitcoin.org/bitcoin.pdf.

2.Christidis Konstantinos, Michael Devetsikiotis. Blockchains and Smart Contracts for the Internet of Things. [Electronic resource]. – Mode of access http://ieeexplore.ieee.org/iel7/6287639/6514899/07467408.pdf?arnumber=7467408.

3.Boohyung Lee. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment / Lee Boohyung, Lee Jong-Hyouk. The Journal of Supercomputing, 2016. – Pp.1-16.

4.Ferrer E.C. The blockchain: a new framework for robotic swarm systems. arXiv preprint arXiv:1608.00695, 2016.

5.Bahga Arshdeep. Blockchain Platform for Industrial Internet of Things / Bahga Arshdeep, Vijay K. Madisetti // Journal of Software Engineering and Applications. – 2016. – № 9. – Pp. 533-546.

6.Andreas M. Antonopoulos. Mastering Bitcoin: unlocking digital cryptocurrencies. "O'Reilly Media, Inc.", 2014. – 298 p.