О. В.Сілагін

Д. Е. Марков

# АНАЛІЗ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ЗБЕРІГАННЯ І УПРАВЛІННЯ КРИПТОВАЛЮТНИМИ АКТИВАМИ

Вінницький національний технічний університет, місто Вінниця

Анотація. Робота присвячена аналізу апаратних та програмних засобів для зберігання і управління криптовалютними активами. Досліджується інформаційна технологія зберігання і управління криптовалютними активами як альтернатива використання фіатніх коштів. Проаналізовано природа та економічна сутність віртуальних грошей. Описано основні засади функціонування криптовалюти, особливості її емісії та придбання. З'ясовано основні проблемні місця правового регулювання криптовалютних коштів, можливі ризики використання підконтрольних третім особам систем. Перевірено захист коштів, який надається кожним з рішень. Обрано найкращі рішення в залежності від мети використання криптовалютними активами. На базі проведеного дослідження розроблено рекомендації до системи, що захистить криптовалютні активи користувачів від можливості їх втрати через дії третьої сторони.

**Ключові слова: блокчейн, криптовалюти, криптовалютні активи, криптовалютний гаманець, біржа, регулювання криптовалют..**

Abstract. The work is devoted to the analysis of hardware and software for storage and management of cryptocurrency assets. Information technology of storage and management of cryptocurrency assets as an alternative to the use of Fiat funds is investigated. The nature and essence of virtual money are analyzed. The basic principles of cryptocurrency functioning, peculiarities of its issue and acquisition are described. The main problem areas of legal regulation of cryptocurrency funds are clarified, the risks of using systems controlled by third parties are possible. The protection of funds provided by each of the solutions has been verified. The best solutions are chosen depending on the purpose of using cryptocurrency assets. On the basis of the study, recommendations for the system have been developed that will protect users ' cryptocurrency assets from the possibility of their loss due to the actions of a third party.

**Key words: blockchain, cryptocurrency, crypto-currency assets, cryptocurrency wallet, the exchange, the regulation of cryptocurrencies.**

## Вступ

Сьогодні в умовах глобалізації фінансові системи окремих країн, як й інші сторони економіки, удосконалюються і прогресують, відбувається поширення ІТ- технологій та загальної комп'ютеризації. Це сприяє появі нових фінансових інститутів, інструментів та форм взаємодії між індивідами. Звідси з'являється новий аналог традиційних валют – криптовалюта та її найпоширеніша грошова одиниця – «біткоін».

В сучасних умовах глобалізації особливо актуальним та складним завданням для вітчизняної економіки виступає дослідження динаміки розвитку українського ринку електронних грошей, оскільки це дозволить з'ясувати певні особливості сучасного фінансового сектору та пов'язані з цим й інші соціально-економічні показники.

Система грошового обігу продемонструвала гостру нестабільність в період світової фінансової кризи 2008-2009 років. Саме в цей час довіра до американського долара послабшала і в суспільстві з'явилися ідеї щодо створення нових валют, зокрема регіональних [1]. Саме тоді й формується пірингова платіжна система «Bitcoin», розроблена Сатоші Накамото, та вперше застосовується термін «криптовалюта».

Саме біткоін (Bitcoin) став найпоширенішою і найдорожчою криптовалютою. Ця віртуальна валюта є децентралізованою, всі операції з її участю анонімні, а центр емісії відсутній. Торгові угоди проводяться тільки в електронному форматі, а операції купівлі-продажу цієї валюти можна здійснити через онлайнбіржі (наприклад BTC-E). За допомогою спеціальних обмінних пунктів в онлайн-мережах (WebMoney) або через брокера Форексу (FXOpen) криптовалюту можна обміняти на основні валюти світу. Також біткоіни можна отримати в результаті прийняття оплати за надані товари та послуги або через купівлю безпосередньо у іншого власника. Останній варіант вважається найвигіднішим, оскільки не передбачає комісійної маржі брокера. Ще одним способом отримання цифрової валюти є майнінг. Його зміст полягає в тому, що на комп'ютери користувачів, які знаходяться в різних точках планети, встановлюють спеціальне програмне забезпечення за допомогою якого в результаті вирішення певних математичних завдань генеруються біткоіни. В даному випадку процес їх створення і розповсюдження не контролюється єдиним емісійним центром, а розгалуженість забезпечує безпеку [2]. Біткоін подібний до електронних грошей, але саме принципи повної анонімності, відсутності контролю і обмеженого випуску відрізняють його від роботи електронних платіжних систем.

Вважається, що ця валюта захищена від інфляції, оскільки процедура емісії запрограмована на зменшення кількості віртуальних грошей в обороті. Всього заплановано до 2033 генерувати 21 млн. одиниць цієї криптовалюти.

Біткоіни діляться на дробові частини, мінімальна з яких складає 0,00000001 біткоіна. Мінімальну одиницю біткоін часто називають Сатоші – на честь її засновника. Таким чином, 1 біткоін = 100 млн Сатоші. У 2011 році американська компанія випустила готівкові біткоіни у вигляді монет декількох номіналів і позолочених злитків, які стали предметом колекціонування і сьогодні мають велику інвестиційну цінність [3].

Мережа біткоін заснована на «блокчейн» (ланцюжку блоків) і є публічним регістром, який зберігає дані про всі транзакції системи. Блокчейн - це тип розподіленої бази даних, яка зберігає записи цифрових транзакцій. Замість того, щоб мати центрального адміністратора, як традиційні бази даних (банки, уряд і бухгалтерія), вона має мережу тиражованих баз даних, синхронізовану через Інтернет і яку видно всім користувачам в мережі[6].

Коли цифрова угода здійснюються 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[4].

Існує два види ланцюжка:

- Публічний Blockchain - відкрита, доповнювальна база даних. Такий вид блокчейна використовується в криптовалютіBitcoin. Кожен учасник може записувати і читати дані.
- Приватний блокчейн має обмеження по запису / читання даних. Можуть встановлюватися пріоритетні вузли. Підвид PrivateBlockchain - ексклюзивний блокчейн. В такому ланцюжку встановлюється група осіб, що займається обробкою транзакцій.

Підбиваючи попередні підсумки, перерахуємо ключові особливості Blockchain:

- Децентралізація - в ланцюжку немає сервера. Кожен учасник - це і є сервер. Він підтримує роботу всього блокчейна;
- Прозорість - інформація про транзакції, контрактах і так далі зберігається у відкритому доступі. При цьому ці дані неможливо змінити;
- Теоретична необмеженість - теоретично блокчейн можна доповнювати записами до нескінченності. Тому його часто порівнюють з суперкомп'ютером;
- Надійність - для запису нових даних необхідний консенсус вузлів блокчейна Це дозволяє фільтрувати операції і записувати тільки легітимні транзакції. Здійснити підміну хеша майже нереально.

Конструкція усієї системи – це послідовність блоків(ланцюжок), а не замкнуте коло чи щось інше. Кожен з блоків містить масив певних даних і всі блоки пов'язані між собою. Тобто, новий «масив» може бути створений тільки після того, як закритий старий масив.

Блок транзакцій - спеціальна структура для запису групи транзакцій в блокчейні. Транзакція вважається завершеною і достовірної ( «підтвердженої»), коли перевірені її формат і підписи, і коли сама транзакція об'єднана в групу з декількома іншими і записана в спеціальну структуру - блок. Вміст блоків може бути перевірено, так як кожен блок містить інформацію про попередньому блоці. Всі блоки збудовані в один ланцюжок, який містить інформацію про всі вчинені коли-небудь операції в базі. Найперший блок в ланцюжку - первинний блок (англ. Genesisblock) - розглядається як окремий випадок, так як у нього відсутній батьківський блок.

Блок складається з заголовка і списку транзакцій. Заголовок блоку включає в себе свій хеш, хеш попереднього блоку, хеші транзакцій і додаткову службову інформацію. В системі Bitcoin першою транзакцією в блоці завжди вказується отримання комісії, яка стане нагородою користувачеві за створений блок. Далі йде список транзакцій, сформований з черги транзакцій, ще не записаних в попередні блоки. Критерій відбору з черги задає майнер самостійно. Це не обов'язково повинна бути хронологія за часом[5].

**Актуальність**

У звичайному світі люди звикли зберігати гроші в гаманці, і якщо провести аналогію між паперовими грошима і криптовалютами, то у них виявиться багато спільного. Це означає, що і криптовалюта теж повинна зберігається в гаманці. Однак, якщо звичайний гаманець може мати лише кілька параметрів і призначений тільки для зберігання грошей, то ось в криптовалютних гаманцях все дещо складніше. За типом зберіганнякриптовалюти їх можна розділити на «гарячі» і «холодні»; за типом зберігання приватних ключів - на «кастодіальні» і «не кастодіальні», а за типом інсталяції - на локальні, мобільні, апаратні, браузерні і паперові (так-так, саме паперові).

У 2014 році кількість кріптокошельков дорівнювало приблизно 2 млн, зараз ця цифра прагне до 23 млн, тобто середнє зростання приблизно в 2,5 рази на рік.

На сьогоднішній день тільки в MyEtherWallet (один з популярних продуктів по зберіганню кріптовалюти) вже зареєстровано понад 15 млн акаунтів, на яких зберігається приблизно 62 млрд доларів. Ці цифри говорять про те, що активне зростання числа користувачів триватиме.

Криптовалютний гаманець - це 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.

## Мета

Мета дослідження є аналіз апаратних та програмних засобів для зберігання і управління криптовалютними активами. Досліджується інформаційна технологія зберігання і управління криптовалютними активами як альтернатива використання фіатніх коштів. Аналіз повинен принести ясність у причини використання будь-якого з типів гаманців, означити їх переваги і недоліки, висвітлити небезпечні місця через які можуть бути викрадені кошти. Та розробити рекомендації до системи, яка позбавить користувача втратити кошти через втручання інших структур.

## Задачі

Для досягнення поставленої мети потрібно вирішити слідуючі задачі:

1. Аналіз і порівняння усіх існуючих типів інформаційних технологій для зберігання і управління криптовалютними активами.
2. Визначення оптимального типу або обрання найважливіших характеристик, які повинні дотримуватись.
3. Створення рекомендацій до системи, яка уникне найнебезпечніших проблем та захистить кошти користувача.

## Розв’язання задач

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 ж застосовуються для "холодного зберігання" криптовалюти, тому вони більш безпечні.

Суть кастодіальних гаманців в тому, що вони НЕ дають доступу до свого приватному ключу, 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 дуже популярним подією.

Некастодіальні електронні гаманці працюють навпаки - 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, так як, якщо seed-фразабуде втрачена, то доступ до гаманця вже ніяк не вийде 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 блокчейні. Десктопні електронні гаманці можна розділити на 2 вида:

- Товстий гаманець –в даному випадку, мається на увазі завантаження на комп'ютер повної копіїблокчейна. 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, що блокчейнтого ж 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, але зате набагато зручніше у використанні.

Апаратний гаманець криптовалют це окремий пристрій, що на вигляд нагадує «флешку». 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 апаратні гаманці займають майже лідируючі позиції.

Web-гаманці або браузерні– це досить простий тип гаманців для використання, він не вимагає від користувача якихось 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 вільного дискового простору;

- У більшості, подібні сервіси пропонують своїм користувачам додаткові зручності, такі як відсутність комісії на перекази між користувачами, відправка монет іншим його користувачам на адресу електронної пошти або номер телефону;

Однак, ви повинні пам'ятати, що такі гаманці мають «кастодіальних» 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 гаманці криптовалют, що можна встановити на мобільні пристрої (смартфони, планшети). 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).

Після проведеного аналізу і ознайомлення з перевагами і недоліками існуючих структурних рішень для зберігання і управління криптовалют наведемо найважливіші рекомендації для обрання найкращого гаманця:

- Некастодіальність;
- Анонімність;
- Додатковий захист(PIN code і інші);
- Мобільність;
- Легкість.

## Висновки

В результаті проведених досліджень було проаналізовано усі відомі типи криптовалютних гаманців, шо існують на сьогоднішній день, а також надано рекомендації для системи , що захистить криптовалютні активи користувачів від можливості їх втрати через дії третьої сторони. Було запропоновано уникати надання третій стороні(таким як біржі і т.д.) можливостей проявляти вплив на кошти користувача, що обумовлено потребою захисту коштів. З цим допоможе некастодіальний підхід, який вже реалізований у деяких технічних рішеннях.

## Список літератури


1. Ashton K. That Internet of Things / K. Ashton // Thing. RFID Journal, 22 July 2009. [Electronic resource]. – Mode of access http://www.rfidjournal.com/articles/view?4986.
2. Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015. [Electronic resource]. – Mode of access http://www.gartner.com/newsroom/id/3165317.
3. Shancang Li. The internet of things: a survey / Li Shancang, Li Da Xu, and Shanshan Zhao // Information Systems Frontiers 2015, 17.2. – Pp. 243-259.
4. Whitmore Andrew. The Internet of Things – A survey of topics and trends / Whitmore Andrew, Anurag Agarwal, and Li Da Xu // Information Systems Frontiers 17.2, 2015. – Pp. 261-274.
5. Dorri, Ali. Kanhere, and Raja Jurdak / Ali Dorri, S. Salil // Blockchain in internet of things: Challenges and Solutions" arXiv preprint arXiv:1608.05187, 2016.
6. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. [Electronic resource]. – Mode of access https://bitcoin.org/bitcoin.pdf.


## Відомості про авторів


Сілагін Олексій Віталійович – к.т.н., доцент, доцент кафедри КН ВНТУ, e-mail: avsilagin@gmail.com, 21016, м.Вінниця

Марков Дмитро Едуардович – магістрант кафедри КН ВНТУ, e-mail: dimamarkovvin@gmail.com, 21000, м.Вінниця

Silagin Alexey Vitalievich – Ph.D., Assistant Professor of the Computer Science Chair, Vinnytsia National Technical University, e-mail: avsilagin@gmail.com, 21016, Vinnytsia

Markov Dmitry Eduardovich – magistrant Vinnytsia National Technical University, e-mail: dimamarkovvin@gmail.com, 21000, Vinnytsia