ФІНАНСОВО–КРЕДИТНА І ГРОШОВА ПОЛІТИКА

УДК 336.744.1 **DOI: 10.37332/2309-1533.2022.1.13**
JEL Classification: E49

Гонак І.М.
канд. екон. наук,
кафедра міжнародної економіки,
Бабій С.В.
старший викладач,
кафедра економічної кібернетики та інформатики,
Західноукраїнський національний університет,
м. Тернопіль

ВИДИ КРИПТОВАЛЮТНИХ ГАМАНЦІВ

Honak I.M.,
cand.sc.(econ.),
department of international economics,
Babii S.V.
senior lecturer of economic cybernetics and Informatics
West Ukrainian National University,Ternopil

TYPES OF CRYPTOCURRENCY WALLETS

Постановка проблеми. Основою ефективності будь-якого бізнесу є безпечне зберігання активів суб'єктом господарювання. Не є винятком здійснення криптовалютного бізнесу, під час здійснення якого активи зберігаються на криптовалютному гаманці. Криптовалютний гаманець необхідно відкривати при здійсненні будь-якого криптовалютного бізнесу – майнінгу криптовалют, торгівлі криптовалютою на біржі, обміну фіатних валют на криптовалютні монети чи обміну одних криптомонет на інші криптомонети, інвестування у криптовалюти. Тому, є нагальна необхідність у вивченні суті роботи криптовалютного гаманця та видів криптогаманців, особливостей функціонування та забезпечення безпеки криптогаманців в умовах зростання активності кібернетичних правопорушників.

Аналіз останніх досліджень і публікацій. Проблематика розвитку та функціонування криптовалют протягом тривалого часу перебувала в полі зору таких вітчизняних і зарубіжних науковців та дослідників, як П. Вінья, З. Двуліт, М. Дученко, А. Макурін, В. Мандрик, М. Миколишин, Т. Момонт, Т. Павленко, К. Павлова, М. Ребрик, М. Свон, В. Скрипник, Н. Танклевська, А. Тапскотт, Д. Тапскотт, С. Хабер, І. Шнабель, К. Штепенко та ін.

Однак, теоретичне обґрунтування криптовалютного бізнесу та його складової – криптовалютних гаманців – перебуває на етапі концептуального оформлення, оскільки більшість аспектів їхньої роботи до цих пір не обґрунтовані. Необхідність цих досліджень обумовлюється швидким розвитком ринку криптовалют, спробою напрацювання правового поля їхнього функціонування.

Постановка завдання. Мета статті полягає у вивченні видів криптовалютних гаманців, їх особливостей та переваг.

Виклад основного матеріалу дослідження. При здійсненні криптовалютного бізнесу у будь-якій формі (майнінг, торгівля, інвестування) для отримання чи відправки криптовалютних монет необхідною є реєстрація криптовалютного гаманця.

Криптовалютний гаманець є інструментом, який можна використовувати для взаємодії з blockchain-мережею. Тобто, криптогаманці не зберігають цифрових активів, а надають інструменти, що є необхідними для взаємодії з блокчейном. Криптогаманці мають можливість генерувати потрібну

для надсилання та отримання криптовалютних монет інформацію через blockchain-транзакції. Ця інформація може складатись із однієї чи кількох пар публічних та приватних ключів [1].

Криптогаманець має адресу, що є буквено-цифровим ідентифікатором, створеним на основі публічного і приватного ключів. Така адреса є, фактично, «місцем» у blockchain, куди є можливість відправляти криптомонети. Отже, криптокористувач може ділитися своєю адресою з третіми особами для одержання криптовалют, проте, необхідно оберігати від розголосу приватний ключ (адресу криптогаманця можна порівняти із номером картки, на яку треті особи можуть перекидувати гроші, проте, PIN–код та CVV2–код нікому передавати не можна).

Аналіз розподілу власників адрес та криптомонет Bitcoin проведемо за даними табл. 1.

Таблиця 1

Розподіл власників адрес та монет Bitcoin

Баланс, BTC	Адреси	% адрес (всього)	Монети	доларів США	% монет (всього)
(0 - 0,00001)	3146979	7,75% (100%)	14,90 BTC	620934	0% (100%)
[0,00001 - 0,0001)	7626300	18,78% (92,25%)	333,57 BTC	13901431	0% (100%)
[0,0001 - 0,001)	10265570	25,28% (73,47%)	3976 BTC	165688550	0,02% (100%)
[0,001 - 0,01)	10101224	24,87% (48,19%)	38144 BTC	1589650221	0,2% (99,98%)
[0,01 - 0,1)	6163246	15,18% (23,32%)	199115 BTC	8298061129	1,05% (99,78%)
[0,1 - 1)	2496446	6,15% (8,14%)	774447 BTC	32274804908	4,09% (98,72%)
[1 - 10)	664822	1,64% (2%)	1691666 BTC	70499566160	8,93% (94,64%)
[10 - 100)	129783	0,32% (0,36%)	4248705 BTC	177063274053	22,42% (85,71%)
[100 - 1000)	13572	0,03% (0,04%)	3894555 BTC	162304182491	20,56% (63,28%)
[1000 - 10000)	2036	0,01% (0,01%)	5261553 BTC	219273348713	27,77% (42,73%)
[10000 - 100000)	81	0% (0%)	2169991 BTC	90433600050	11,45% (14,96%)
[100000 - 1000000)	4	0% (0%)	664320 BTC	27685296858	3,51% (3,51%)

Джерело: сформовано на основі [2]

Проаналізувавши дані табл. 1, можемо зробити висновок, що тільки 2% Bitcoin-адрес здійснюють контроль над 94,64% криптомонет Bitcoin. Необхідно зважити на те, що Bitcoin-адреса – це не «рахунок», а один криптокористувач має можливість володіти багатьма адресами, тому монополія обмеженого кола криптокористувачів на володіння криптомонетами Bitcoin може бути ще більш глибокою, ніж проілюстровано даними табл. 1.

На основі розрахованих даних подамо графічне представлення кривої Лоренца (рис. 1).

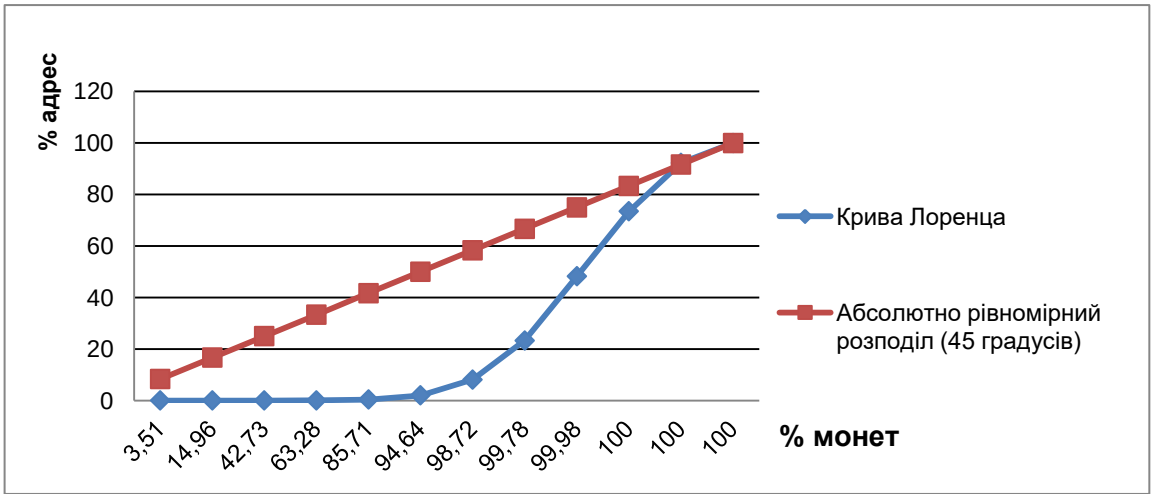

Рис. 1. Графічне представлення кривої Лоренца розподілу монет Bitcoin між адресами, %

Джерело: сформовано на основі даних табл. 1

Необхідно зауважити, що значення коефіцієнта Джині для ринку криптомонет Bitcoin станом на 05.02.2022 року є значно вищим, ніж у КНДР, де керівництво країни здійснює контроль над більшістю ресурсів країни.

У табл. 2 здійснимо аналіз розподілу адрес за вартістю монет Bitcoin.

Таблиця 2

Розподіл адрес за вартістю криптовалютних монет Bitcoin

Наявність на криптовалютній адресі криптомонет, вартістю:	Кількість адрес	Частка адрес у їх загальній кількості, %
більше $1	35039590	59,260
більше $100	15345212	25,952
більше $1000	6313579	10,678
більше $10000	1963548	3,321
більше $100000	373193	0,631
більше $1000000	85885	0,145
більше $10000000	7472	0,013
Разом	59128479	100

Джерело: сформовано на основі [3]

Отже, після аналізу даних табл. 2 робимо висновок, що понад 95,89% адрес містять криптовалютні монети Bitcoin на суму менше десяти тисяч доларів і тільки 4,11% – більше, ніж на суму десять тисяч доларів. Дана ситуація добре проілюстрована на рис. 2.

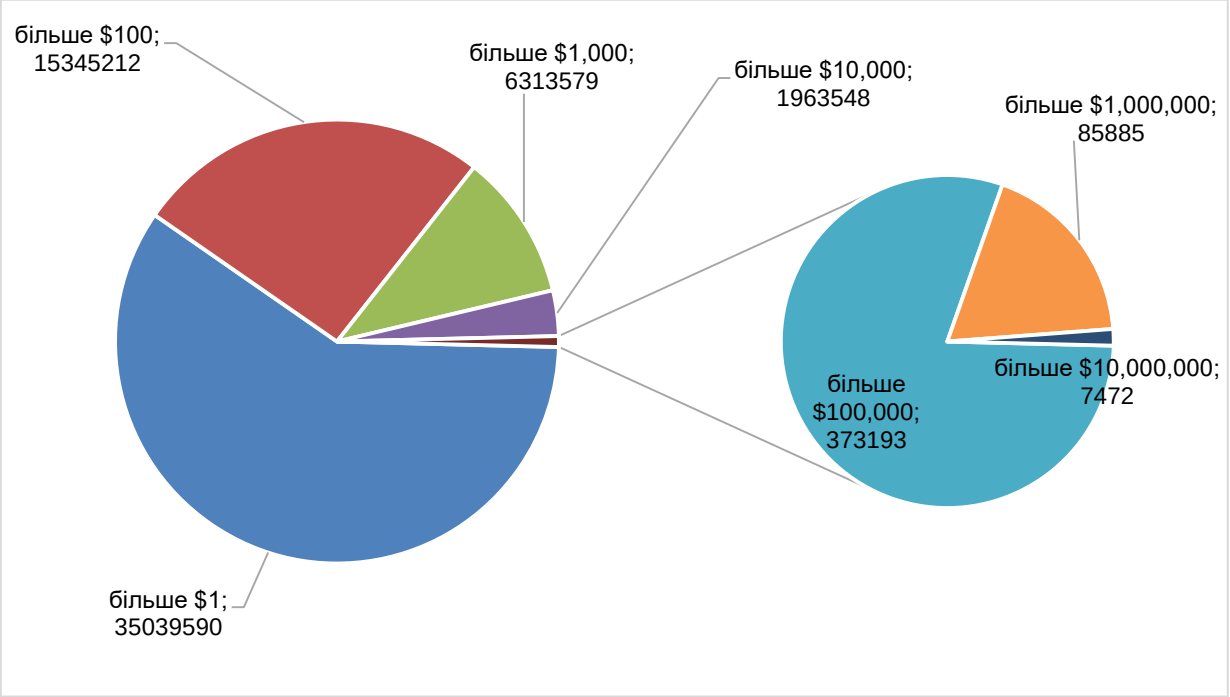

Рис. 2. Розподіл адрес за вартістю криптовалютних монет Bitcoin

Джерело: сформовано на основі даних табл. 2

Приватний ключ надає доступ до криптовалютних монет криптокористувача незважаючи на те, який криптогаманець використовує криптокористувач. Отже, якщо персональний комп'ютер чи комунікатор пошкодиться або його зламають, власник криптогаманця зможе одержати доступ до своїх криптовалютних активів через інший пристрій за умови наявності приватного ключа чи seed-вислову. Необхідно зважати, що криптомонети ніколи не покидають blockchain, переказуються із однієї адреси на іншу.

Залежно від механізму роботи, гаманці поділяються на холодні та гарячі.

Гарячий криптогаманець є гаманцем, підключеним до Інтернету. За умови, що криптокористувач створив акаунт на криптовалютній біржі і відправляє кошти на криптовалютний гаманець, то у цей момент здійснюється депозит на гарячий криптогаманець. Гарячі гаманці не складно налаштувати і криптокористувачі отримують до своїх активів легкий доступ, що є зручним для трейдерів та інших криптокористувачів.

Холодні криптовалютні гаманці є, фактично, пакетом інструментів на USB-носії для зберігання інформації, що необхідна для доступу до криптовалютних монет та не вимагають безперебійного Інтернет-з'єднання [4]. Холодні криптогаманці є значно безпечнішою альтернативою «зберігання» криптовалютних монет, ніж гарячі. Цей метод називається холодним зберіганням і є підходящим для інвесторів та «Ходлерів» (HODL є терміном, що використовується щодо інвесторів у криптовалюти, які відмовляються продавати наявну у них криптовалюту незалежно від зростаючої чи спадаючої динаміки вартості криптомонет [5]).

На криптовалютному ринку є велика кількість різноманітних гаманців, які можна розділити на п'ять груп:

I) ***електронні гаманці (веб-гаманці)*** створюються на криптовалютних біржах чи онлайн обмінниках. Алгоритм реєстрації криптовалютного електронного гаманця простий, займає близько десяти хвилин, подібний до реєстрації електронної пошти. Реєстрація електронного гаманця не вимагає встановлення спеціальної програми на персональний комп'ютер.

У криптокористувача є можливість скористатися веб-гаманцем з метою доступу до блокчейнів через інтерфейс браузера без потреби у завантаженні чи установленні програми. До електронних криптогаманців (веб-гаманців) можна віднести як біржові криптовалютні гаманці, так і інші криптогаманці на базі браузера. У значній кількості випадків криптокористувач має можливість створити новий криптогаманець і встановити власний пароль для доступу до криптогаманця. Проте, деякі постачальники послуг мають можливість зберігати та управляти приватними ключами від імені криптокористувача і це може бути прийнятним варіантом для криптокористувачів-початківців, але це є невиправдано ризикованим рішенням.

Якщо у криптокористувача відсутні приватні ключі, то криптовалютний користувач довіряє наявні у нього криптомонети третій особі. Для вирішення цієї проблеми, значна кількість електронних криптогаманців (веб-гаманців) на даний час дають змогу криптокористувачам здійснювати управління своїми ключами чи повністю, чи через спільний контроль (мультипідпис). Тому необхідно перевіряти технічний підхід до кожного криптогаманця перед тим, як обрати той, що є прийнятним для криптокористувача.

Найбільш популярними та надійними електронними гаманцями є Hive, Cryptopay, StrongCoin, Xapo, GreenAddress, BitGo, Coinkite, Coinbase, Bitcoin Core, Matbea [6].

Слід зазначити, що електронні гаманці є слабкозахищеними перед хакерськими атаками кіберправопорушників через те, що ці криптогаманці реєструються віддалено, а дані про нього зберігаються на сервері, до якого є постійний доступ за умови наявності Інтернету.

Хакерські атаки на криптогаманці є значною проблемою для економічних суб'єктів криптовалютного бізнесу. Наприклад, атака кіберправопорушників привела до поділу ETH на дві гілки: ethereum та ethereum classic. Також значним є викрадення криптовалют хакерами.

У 2021 році капіталізація ринку криптовалют досягнула трьох мільярдів доларів США [7], що зумовило зростання активності кіберправопорушників на ринку. Дії хакерів здійснювали на ринок настільки значний вплив, що деякі криптобіржі внаслідок цих дій збанкрутували (зокрема, у 2014 році збанкрутували біржа Mt. Gox, з рахунків якої кіберправопорушники викрали 460 мільйонів доларів США). Про зростання уваги кіберправопорушників до криптовалютного ринку свідчить те, що із 2017 року по 2020 рік, тобто за чотири роки, правопорушники викрали криптовалютних монет на суму майже десять мільярдів доларів, у 2020 році (за один рік) правопорушники провели 122 атаки і викрали 3,8 мільярдів доларів США [8, с. 15] (тобто, за один рік викрадено суму, що складає майже сорок відсотків суми, викраденої протягом чотирьох років). У часовому проміжку із 2012 по 2020 роки сума викрадених криптовалют склала 13,6 мільярди доларів США і, при цьому, було здійснено близько 330 зломів криптобірж, криптогаманців і децентралізованих застосунків, тобто, за чотири роки із 2017 по 2020 рік викрадено понад сімдесят відсотків загальної за дев'ять років суми, а тільки за 2020 рік здійснено третину всіх зломів і викрадено майже тридцять відсотків загальної суми із періоду 2012–2020 років [9]. Найбільші атаки на криптовалютні біржі та суми викрадених криптомонет подано у табл. 3.

Із даних табл. 3 можемо зробити висновок, що із року у рік частота кіберправопорушень на криптовалютному ринку зростає і зростають суми викрадених коштів. Ця тенденція продовжилась і у 2021 році – тільки за третій квартал хакери викрали 1,1 мільярди доларів [7].

II) ***Десктопні криптогаманці*** є програмою, що завантажується і запускається локально на персональному комп'ютері. Цю програму можна завантажити із загальнодоступних сайтів. Ці програми вважають значно надійнішими і зручнішими для роботи, ніж електронний криптовалютний гаманець через те, що надають криптокористувачу повний контроль над приватними ключами і власними коштами. При створенні нового десктопного гаманця файл із назвою «wallet.dat» зберігатиметься локально на персональному комп'ютері. Файл «wallet.dat» міститиме інформацію про приватні ключі криптокористувача, яким криптокористувач користатиметься з метою доступу до власних адрес криптовалютних монет, тому власнику криптогаманця необхідно зашифрувати файл персональним паролем.

Таблиця 3

Найбільші кіберправопорушення та суми викрадених коштів

Назва криптобіржі	Дата кіберправо-порушення	Суми викрадених коштів, млн дол США	Викрадені суми у криптовалютних монетах
Mt. Gox	Лютий 2014	450-460	850000 Bitcoin
Bitfinex	Серпень 2016	72	120000 Bitcoin
NiceHash	Грудень 2017	64	4736 Bitcoin
Coincheck	Січень 2018	533	523000000 NEM
Bitgrain	Лютий 2018	170	17000000 NANO
CoinBene	Березень 2019	105	110 видів криптовалют
Binance	Травень 2019	40	7000 Bitcoin
Upbit	Листопад 2019	49	342000 Etherum
KuCoin	Вересень 2020	275	6 видів криптовалют, у тому числі 1008 Bitcoin, 11543 Etherum
Poly Network	Серпень 2021	604	2858 Etherum (267 млн доларів США), 6610 Binance Coin (більше 252 млн доларів США), Tether (приблизно 85 млн доларів США)

Джерело: сформовано на основі [10]

При шифруванні десктопного гаманця, власнику криптогаманця необхідно вводити пароль щоразу, коли запускається програмне забезпечення, щоб програма змогла прочитати файл wallet.dat. При втраті цього файлу чи паролю, власник криптогаманця може втратити доступ до своїх активів.

Отже, криптокористувачу необхідно робити резервні копії файлу wallet.dat і берегти їх у надійних місцях. Також, є можливість експортувати приватний ключ або seed-вислів і отримувати доступ до криптокоштів через інші пристрої в разі неможливості доступу до особистого персонального комп'ютера.

Десктопні гаманці є безпечнішими, ніж інші веб-версії криптогаманців, проте, криптокористувачу необхідно пересвідчитися, що на персональному комп'ютері криптокористувача відсутні віруси та шкідливі програми перед тим, як здійснювати налаштовування та використовувати криптогаманець.

Десктопні гаманці є двох видів: «тонкі» та «товсті». «Тонкі» криптогаманці надають можливість криптокористувачу оперативно здійснювати транзакції, проте мають обмежений обсяг опцій. На противагу їм, «товсті» десктопні криптогаманці представляють собою повноцінну програму із значним обсягом функцій (зокрема, із можливістю майнінгу). Проте, для «товстого» гаманця необхідна наявність значного обсягу вільного місця на комп'ютерному диску (біля двохсот гігабайт) та проведення транзакцій займає більше часу, ніж на «тонкому» криптовалютному гаманці.

Найбезпечнішими десктопними вважаються криптогаманці від розробників криптовалют, зокрема, Ethereum Wallet (Mist) чи Bitcoin Core, що підтримують тільки власну криптовалюту. Але ці криптогаманці менш функціональні у порівнянні із мультивалютними (універсальними). Найбільш популярними мультивалютними універсальними десктопними криптогаманцями є Jaxx, Coinomi та Exodus.

III) Більшість широковживаних криптогаманців мають версії не тільки для персональних комп'ютерів, а і ***версії для смартфонів (мобільні гаманці)*** через те, що значна кількість користувачів комунікаторів не працюють із персональними комп'ютерами або працюють мало. Версії для смартфонів мають переваги та недоліки, аналогічні десктопним криптогаманцям. Завантажити версії для смартфонів є можливість із GooglePlay чи AppStore.

Мобільні гаманці допускають здійснення транзакцій криптовалютних монет за допомогою QR-кодів і підходять для здійснення поточних транзакцій. Trust Wallet є прикладом мобільного криптовалютного гаманця.

Мобільні пристрої також можуть заразитись шкідливим додатком чи заразитись шкідливою програмою, через що необхідно здійснити шифрування мобільного гаманця паролем та зробити резервні копії приватних ключів та seed-вислову на випадок втрати доступу до смартфону.

Веб-гаманці, десктопні та мобільні гаманці можна, умовно, назвати ***програмними криптогаманцями*** через те, що переважна більшість із них так чи інакше є підключеними до мережі Інтернет, тобто є гарячими криптогаманцями.

IV) ***Апаратні криптовалютні гаманці*** є фізичним електронним пристроєм, застосовують генератор випадкових чисел (RNG) з метою генерації публічних чи приватних ключів. Потім ключі можуть зберігатись у самому пристрої, не під'єднаному до мережі Інтернет. Тому апаратне сховище є різновидом холодного криптогаманця та визнається, практично, найбезпечнішим криптогаманцем.

Апаратні криптогаманці пропонують максимально високий рівень захисту криптовалютних монет від атак у мережі, але якщо прошивка гаманця не буде здійснена належно, то працюватиме криптогаманець невірно. Також слід зазначити, що для щоденного користування апаратні гаманці незручні через ускладнений доступ до коштів. Для полегшення доступу до коштів можна використовувати спеціальні програми (наприклад, Binance DEX використовують з метою підключення комп'ютерних пристроїв до торгової платформи). Використання спеціальних програм надає можливість безпечного доступу до криптовалют на гаманці через те, що приватний ключ ніколи не покидає пристрій криптокористувача (ключі доступу до апаратного гаманця генеруються локально і зберігаються на спеціальній флешці – токені). Криптокористувачу доцільно використовувати апаратний гаманець для довгострокового зберігання криптовалют чи за наявності сум криптомонет.

Для захисту апаратного криптовалютного гаманця від шкідливих програм (вірусів) та Інтернет-правопорушників (хакерів) використовуються PIN-коди для підтвердження транзакцій і захищені чіпи, а для відновлення доступу до апаратних криптогаманців використовується мнемофаза. Криптогаманці не є безкоштовними і вартують від п'ятдесяти до ста доларів і їх реалізують на ринку фірми-виробники – KeepKey, Digital Box, Trezor, Ledger та Cool Wallet. Цей вид гаманця прийнято називати «холодним».

Недоліком апаратного криптогаманця є потреба у переведенні криптоактивів із нього на електронний гаманець при здійсненні поточних транзакцій, тому апаратний гаманець доцільно використовувати для транзакцій із значними сумами та для довгострокового інвестування у криптовалюти. Необхідно уважно зберігати seed-вислів (комбінацію символів, необхідну для відновлення апаратного криптогаманця) окремо від токена через те, що спільна втрата токена та seed-вислову може призвести до безповоротної втрати криптовалютних монет.

Згідно даних станом на 19 листопада 2020 року, сума криптомонет Bitcoin, що зберігалися у неліквідних криптовалютних гаманцях (це значить, що монети із криптогаманця і сам криптогаманець не змінювали своєї поточної адреси протягом п'яти років та довше), складали 77% від 14,8 мільйона «добутих» (намайнених) на той час монет Bitcoin. Більшість із цих криптогаманців були апаратними і тільки 3,4 мільйони криптовалютних монет Bitcoin [11], що були легкодоступними для покупців, тобто знаходились, в основному, не на апаратних криптогаманцях, а на електронних та десктопних гаманцях.

V) Одним із найбільш надійних способів зберігання криптовалют є ***криптогаманці на паперовому носії***. На паперовому носії розміром як банкнота розміщений приватний ключ у вигляді QR-коду та публічний ключ доступу (криптоадреса). Для здійснення транзакцій з криптовалютними монетами необхідно ці коди сканувати.

Деякі веб-сайти із паперовими криптогаманцями дають можливість завантажувати їх код з метою генерування нових адрес та ключів в офлайні. Тому паперові криптогаманці володіють значною стійкістю до хакерських онлайн атак і їх вважають надійним замінником холодного сховища.

Проте, криптогаманці на паперовому носії є незручними через те, що криптомонети з нього пересилаються всі (весь наявний баланс), а не частинами (тобто, якщо у криптокористувача на криптогаманці на паперовому носії є п'ять монет Ethereum, то неможливо потратити три монети, а необхідно всі п'ять монет перекинути на гарячий гаманець, витратити передбачені три монети, а дві монети, що залишились, необхідно повернути на новостворений паперовий гаманець).

При імпортуванні приватного ключа паперового криптогаманця у гарячий криптовалютний гаманець і витрачанні тільки частки наявних монет, криптомонети, що лишилися, можуть бути надіслані на «іншу адресу», що автоматично генерується Bitcoin протоколом і якщо криптокористувач не встановить цю адресу вручну, є вірогідність втрати монет. Сучасні програмні криптогаманці, у своїй більшості, робитимуть це за криптокористувача, відсилаючи залишок криптомонет на адресу, що є однією із адрес криптокористувача. Слід зауважити, що паперовий криптогаманець після надсилання першого грошового переказу буде пустим незалежно від обсягу переказу, тому скористатись ним повторно неможливо.

Частка криптомонет Bitcoin на ринку криптовалют станом на 17 листопада 2021 року складала 43,63%, а частка криптомонети Ethereum – 19,33% [7]. Операції із цими криптовалютами займають понад половину ринку, тому розглянемо особливості криптогаманців для цих та інших криптовалют із найбільшою капіталізацією.

Криптовалютними гаманцями для криптомонети Bitcoin є:

Airbitz – є версія для персонального комп'ютера та для смартфона Android;

ArcBit – є версія для персонального комп'ютера, для смартфонів Android та iOS;

Armory – є версія для персонального комп'ютера;

Bitcoin Core – є версія для персонального комп'ютера та для смартфона Android;

Bitcoin Knots – є версія для персонального комп'ютера;

BitGo – є електронні гаманці та версія для персонального комп'ютера;

Bither – є версія для персонального комп'ютера, для смартфонів Android та iOS;

Coin Space – є електронний гаманець, версія для смартфонів Android та iOS;

Coinbase – є електронний гаманець;

Copay – є версія для персонального комп'ютера, для смартфонів Android та iOS;

Electrum – є версія для персонального комп'ютера та для смартфона Android;

GreenBits – є версія для смартфона Android;

mSIGNA – є версія для персонального комп'ютера;

Mycelium – є версія для смартфона Android;

Xapo – є електронний гаманець.

Найбільш зручними, розповсюдженими та надійними гаманцями для криптомонети Ethereum є ETHAdress, Mist, JAXX, MyEtherWallet, Exodus, MetaMask та Coinbase.

Для криптовалютної монети ripple розроблені такі криптогаманці, як BitGo, Toast Wallet, CoinPayments та Exarpy.

Криптогаманцями, які підтримують роботу криптомонети Bitcoin Cash, є: Copay Guarda Wallet, Bitcoin Cash Wallet, StrongCoin, Electron Cash, Coin space, Exodus, BTC.com, WebMoney, CoinBase, Jaxx, Unit Wallet, Stash Wallet, Coinomi, Mobi та Edge.

Роботу із криптовалютою Litecoin підтримують криптогаманці Jaxx, Rahakott, Exedus, Cryptonator, Electrum-LTC, LiteVault та Block.io.

Криптогаманцями, що підтримують роботу із криптовалютою Binance Coin, є гаманці Mist, MyEtherWallet, ImToken та MetaMask.

Для криптовалюти Dash використовують криптогаманці Coinomi, Rahakott, Jaxx, Dash Core, Dash Wallet та Dash Electrum.

Криптогаманці, які підтримують роботу криптовалюти EOS, є наступними: електронні криптогаманці – Scatter, MetaMask та MyEtherWallet; десктопні криптогаманці – SimplEOS, Altcoin.io та Exodus; для смартфонів розроблений криптогаманець Infinito Wallet; найкращий апаратний гаманець Ledger Nano S.

Криптогаманцями для криптовалюти Bitcoin SV є Pixel Wallet, Atomic Wallet, NextCash, Bitaddress, Guarda, CashPay Wallet та CashPay.

Криптогаманці, що підтримують роботи криптовалюти Monero, є Monero Wallet GUI, MyMonero та Monerujo.

Основні вимоги щодо забезпечення оптимальної безпеки економічного суб'єкта у роботі із криптовалютними гаманцями:

1. Для здійснення безпечного доступу до криптовалютного гаманця необхідно застосовувати двофакторну google-аутентифікацію (2FA) без використання SMS. Google аутентифікатор убезпечує доступ до криптовалютного гаманця від правопорушників, які використовують для шахрайства обмін SIM-карт. Додаток слід встановлювати уважно, щоб замість google-аутентифікатора 2FA, не встановити SMS 2FA, тому що SMS 2FA можна перехопити [12].

2. Якщо є можливість, то використовувати код захисту від фішингу – функцію безпеки, яку пропонують криптовалютні біржі (наприклад, Binance). Код захисту від фішингу надає можливість криптокористувачам отримати допоміжний рівень безпеки для власного облікового запису. Після увімкнення антифішингового коду, код буде присутнім на всіх електронних листах, надісланих із криптовалютної біржі. Антифішинговий код підтвердить справжність листа і цим справжній лист відрізнятиметься від фішингового [13].

3. Доцільним є управління адресою зняття коштів. Наприклад, на криптобіржі Binance формується білий список адрес для виведення коштів.

Білий список адрес для виведення коштів є ще однією функцією безпеки. Якщо функція білого списку вимкнена, обліковий запис криптокористувача може виводити кошти на будь-яку адресу. Проте, якщо білий список ввімкнути, криптокористувач матиме можливість здійснити виведення коштів лише на внесені до білого списку адреси.

Отже, кошти із криптовалютної біржі можна буде отримати лише за адресами, які криптокористувач внесе в білий список. Це є доцільним через те, що якщо криптокористувач станете жертвою фішингу і криптоправопорушник отримає доступ до рахунку криптокористувача, хакер не зможе заволодіти грошима криптокористувача [14].

4. Необхідно забезпечити ефективний захист приватних ключів доступу до криптовалютного гаманця. Для захисту приватних ключів необхідно використати наступний алгоритм:

I) для захисту криптовалютних активів, що розміщені на криптогаманці, необхідно тримати у безпеці приватні ключі та тримати криптоактиви у довірених сторонніх кастодіанів (наприклад, на біржі, де їх придбали);

II) необхідно тримати приватні ключі в офлайні і переконатись, що вони не знаходитимуться на пристроях, підключених до мережі Інтернет, щоб до них не змогли одержати доступ криптоправопорушники;

III) потрібно захистити приватні ключі від руйнування чи втрати через утворення декількох безпечних резервних копій (наприклад, на декількох флешках).

5. Не використовувати логіни та паролі для доступу до криптовалютного гаманця такі ж, як і для майнінг-пулу, поштової скриньки чи ін., для того, щоб правопорушник, який зумів отримати доступ до одного акаунта, не зміг використати дані доступу до нього з метою доступу до криптогаманця економічного суб'єкта криптовалютного ринку.

6. Втрата доступу до криптовалютних гаманців є можливою. Тому необхідно здійснювати періодичне резервне копіювання файлів wallet.dat чи seed-висловів – seed-вислів працює як root ключ, що генерує та надає доступ до ключів та адрес у криптогаманці. Резервну копію необхідно робити і при шифруванні пароля.

7. При здійсненні поточних транзакцій із невеликим обсягом криптовалютних активів доречно скористатися мобільним чи вебдодатком або тонким гарячим криптогаманцем. При цьому, значну частку наявних у криптокористувача активів необхідно тримати на холодних криптогаманцях. Щоб отримати доступ до холодного апаратного криптовалютного гаманц,я криптоправопорушнику необхідно використати метод брутфорс із фізичним доступом до пристрою (перебрати всі можливі варіанти приватних ключів чи мнемонічних фраз-паролів, а це займатиме непередбачено велику кількість часу).

8. Застосовувати для криптобізнесу гаманці із відкритим вихідним кодом і для зберігання різних криптомонет користуватися різними криптовалютними гаманцями.

При недотриманні правил безпеки можуть виникнути проблеми із доступом до криптогаманця і відновити безперешкодний доступ до електронного гаманця буде проблематично через вкрай міцний захист криптовалютних гаманців від кіберправопорушників та відсутність збережених копій даних доступу до гаманця. Для відновлення доступу необхідно скористатися бібліотеками Pyethrecovery чи Pyethereum або спеціальною програмою Python. За умови випадкового видалення цифрового приватного ключа або ушкодження жорсткого диску чи токена необхідно скористатись копією файлу на іншому носії чи звернутись до служби підтримки криптогаманця чи криптовалюти.

Висновки з проведеного дослідження. Таким чином, за результатами проведеного дослідження можемо зробити наступні висновки:

1. Відкриття криптовалютного гаманця є необхідним при здійсненні будь-якого виду криптовалютного бізнесу – майнінгу, торгівлі чи інвестування. Криптогаманці є важливим елементом інфраструктури, що дають можливість переказувати кошти через blockchain-мережу.

2. Існує п’ять типів криптогаманців – електронний гаманець, десктопний гаманець, додаток для комунікатора, апаратний криптогаманець та електронний гаманець на паперовому носії. Кожен із типів криптогаманців володіє певним обсягом переваг та недоліків, тому необхідно ґрунтовно розібратись у алгоритмі їх роботи перед тим, як розміщувати на них свої криптоактиви.

3. Для активних операцій варто користуватись тонким гарячим криптогаманцем, мобільним чи вебдодатком, проте тримати там незначну суму операційних коштів, а для збереження основної суми криптовалютних активів варто користуватись холодним апаратним криптогаманцем через те, що холодні криптогаманці не підключені до мережі Інтернет і тому є безпечнішими та стійкішими до онлайн фішингових атак чи криптовалютного шахрайства.

4. Для захисту акаунта економічного суб’єкта криптовалютного ринку необхідно користуватись двофакторною google-аутентифікацію на всіх криптогаманцях – у цьому випадку криптовалюта криптокористувача буде надійно зберігатись.

5. Для здійснення криптовалютного бізнесу варто обрати криптовалютні гаманці з відкритим вихідним кодом та для кожної криптовалютної одиниці варто заводити окремі криптогаманці.

6. Відновити втрачений доступ до електронного криптогаманця є надзвичайно складним (інколи – майже неможливим) завданням, тому зберігати приватні ключі доступу слід надзвичайно обережно.

Література

1. Що таке криптовалютний гаманець? *BINANCE-ACADEMY*. 18 січня 2019. URL: https://academy.binance.com/uk/articles/crypto-wallet-types-explained (дата звернення: 01.11.2021).

2. Bitcoin Rich List. Bitcoin distribution. *BitInfoCharts.* URL: https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html (дата звернення: 05.02.2022).

3. Bitcoin Rich List. Addresses richer than. *BitInfoCharts.* URL: https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html (дата звернення: 06.02.2022).

4. Що таке “холодний” крипто-гаманець та як захистити його від зламу? Поради. *Cybercalm*. 12.06.2020. URL: https://cybercalm.org/novyny/shho-take-holodnyj-krypto-gamanets-ta-yak-zahystyty-jogo-vid-zlamu-porady/ (дата звернення: 01.11.2021).

5. HODL. *BINANCE-ACADEMY*. URL: https://academy.binance.com/en/glossary/hodl (дата звернення: 06.02.2022).

6. Як вибрати електронний гаманець для криптовалюти. *BANKCHART.UA.* URL: https://bankchart.com.ua/finansoviy_gid/investitsiyi/statti/yak_vibrati_elektronniy_gamanets_dlya_kriptovalyuti (дата звернення: 01.11.2021).

7. Недєлков К., Цяцьоркін М., Примак К. Хакери вкрали $1,1 млрд у криптовалюті лише за третій квартал 2021-го. Як зберегти криптокошти та анонімність рахунків. *Forbes.* 17 листопада 2021. URL: https://forbes.ua/money/khakeri-vkrali-11-mlrd-u-kriptovalyuti-lishe-za-tretiy-kvartal-2021-yak-zberegti-kriptokoshti-ta-anonimnist-rakhunkiv-17112021-2796 (дата звернення: 17.11.2022).

8. Ребрик М. А. Криптоактиви: міфи vs факти та потенційний вплив на монетарну сферу. URL: https://bank.gov.ua/admin_uploads/article/Rebryk_2021-29-05.pdf?v=4 (дата звернення: 06.02.2022).

9. Куницький О. Хакер начал возвращать украденную криптовалюту более чем на $600 млн в Poly Network. Что произошло. *Forbes.* 12 августа 2021. URL: https://forbes.ua/ru/news/khaker-pochav-povertati-vkradenu-kriptovalyutu-na-ponad-600-mln-u-poly-network-shcho-stalosya-12082021-2257 (дата звернення: 01.11.2021).

10. Гонак І. М. Ризики функціонування криптовалютного бізнесу. *Науковий вісник Херсонського державного університету*. *Серія «Економічні науки»*. 2021. № 44. С. 81-86.

11. Why Bitcoin is Surging and How This Rally Is Different from 2017 (Hint: It's Who's Buying). *Chainalysis.* 2020, November, 19. URL: https://blog.chainalysis.com/reports/bitcoin-price-surge-explained-2020/ (дата звернення: 01.11.2021).

12. Сонг Дж., Лопп Дж., Бентон О. #StaySAFU: 5 порад безпеки від професіоналів. *BINANCE.* 29.06.2020. URL: https://www.binance.com/uk-UA/blog/all/staysafu-5-%D0%BF%D0%BE%D1%80%D0%B0%D0%B4-%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8-%D0%B2%D1%96%D0%B4-%D0%BF%D1%80%D0%BE%D1%84%D0%B5%D1%81%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%96%D0%B2-421499824684900668 (дата звернення: 01.11.2021).

13. Binance Anti-Phishing Code Guide. *BINANCE. ACADEMY*. 2018, December, 10. URL: https://academy.binance.com/uk/articles/anti-phishing-code (дата звернення: 01.11.2021).

14. How to whitelist a withdrawal address on Binance. *BINANCE. ACADEMY.* 2018, December, 09. URL: https://academy.binance.com/uk/articles/withdrawal-address-whitelist (дата звернення: 01.11.2021).

References

1. "BINANCE-ACADEMY (2019), "What is a cryptocurrency wallet?", available at: https://academy.binance.com/uk/articles/crypto-wallet-types-explained (access date November 01, 2021).

2. Bitcoin Rich List. Bitcoin distribution, *BitInfoCharts,* available at: https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html (access date November 01, 2021).

3. Bitcoin Rich List. Addresses richer than, *BitInfoCharts,* available at: https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html (access date November 01, 2021).

4. Cybercalm (2020), "What is a "cold" crypto-wallet and how to protect it from burglary? Advice", available at: https://cybercalm.org/novyny/shho-take-holodnyj-krypto-gamanets-ta-yak-zahystyty-jogo-vid-zlamu-porady/ (access date November 01, 2021).

5. HODL, *BINANCE-ACADEMY*, available at: https://academy.binance.com/en/glossary/hodl (access date November 01, 2021).

6. "How to choose an electronic wallet for cryptocurrency", *BANKCHART.UA,* available at: https://bankchart.com.ua/finansoviy_gid/investitsiyi/statti/yak_vibrati_elektronniy_gamanets_dlya_kriptovalyuti (access date November 01, 2021).

7. Nedielkov, K., Tsiatsorkin, M. and Prymak, K. (2021), "Hackers stole $ 1.1 billion in cryptocurrency in the third quarter of 2021 alone. How to keep cryptocurrencies and anonymity accounts", *Forbes*, available at: https://forbes.ua/money/khakeri-vkrali-11-mlrd-u-kriptovalyuti-lishe-za-tretiy-kvartal-2021-yak-zberegti-kriptokoshti-ta-anonimnist-rakhunkiv-17112021-2796 (access date November 17, 2021).

8. Rebryk, M.A. (2021), "Crypto assets: myths vs facts and potential impact on the monetary sphere", available at: https://bank.gov.ua/admin_uploads/article/Rebryk_2021-29-05.pdf?v=4 (access date November 01, 2021).

9. Kunytskyi, O. (2021), "The hacker began to return the stolen cryptocurrency for more than $600 million in Poly Network. What happened", *Forbes*, available at: https://forbes.ua/ru/news/khaker-pochav-povertati-vkradenu-kriptovalyutu-na-ponad-600-mln-u-poly-network-shcho-stalosya-12082021-2257 (access date November 01, 2021).

10. Honak, I.M. (2021), "The risks of operating a cryptocurrency business", *Naukovyi visnyk Khersonskoho derzhavnoho universytetu. Seriia «Ekonomichni nauky»*, no. 44, pp. 81-86.

11. Chainalysis (2020), Why Bitcoin is Surging and How This Rally Is Different from 2017 (Hint: It's Who's Buying), available at: https://blog.chainalysis.com/reports/bitcoin-price-surge-explained-2020/ (access date November 01, 2021).

12. Song, J., Lopp, J. and Benton, O. (2020), "#StaySAFU: 5 safety tips from professionals, *BINANCE*, available at: https://www.binance.com/uk-UA/blog/all/staysafu-5-%D0%BF%D0%BE%D1%80%D0%B0%D0%B4-%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8-%D0%B2%D1%96%D0%B4%D0%BF%D1%80%D0%BE%D1%84%D0%B5%D1%81%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%96%D0%B2-421499824684900668 (access date November 01, 2021).

13. BINANCE. ACADEMY (2018), Binance Anti-Phishing Code Guide, available at: https://academy.binance.com/uk/articles/anti-phishing-code (access date November 01, 2021).

14. BINANCE. ACADEMY (2018), How to whitelist a withdrawal address on Binance, available at: https://academy.binance.com/uk/articles/withdrawal-address-whitelist (access date November 01, 2021).