АКТУАЛЬНІ ПИТАННЯ ЕКОНОМІЧНИХ НАУК

Менеджмент

УДК 005.334:336.744:004.738.5:658.012.32

DOI https://doi.org/**10.5281/zenodo.15316174**

Стратегії управління ризиками в бізнес-інтеграції біткоїна: акторно-мережевий підхід

Павлов Роман Анатолійович

кандидат економічних наук, доцент, доцент кафедри економіки, підприємництва та управління підприємствами, Дніпровський національний університет імені Олеся Гончара, м. Дніпро, Україна, https://orcid.org/0000-0001-7629-2730

Павлова Тетяна Сергіївна

доктор філософських наук, професор, професор кафедри філософії, Дніпровський національний університет імені Олеся Гончара, м. Дніпро, Україна, https://orcid.org/0000-0001-7178-3573

Гринько Тетяна Валеріївна

доктор економічних наук, професор, декан факультету економіки, Дніпровський національний університет імені Олеся Гончара, м. Дніпро, Україна, https://orcid.org/0000-0002-7882-4523

Прийнято: 19.04.2025| Опубліковано: 29.04.2025

Анотація. *У роботі обґрунтовано стратегії мінімізації ризиків, що інтегрують технологічні, економічні, соціальні та культурні аспекти функціонування біткоїна в підприємницькій діяльності.* ***Мета.*** *Дослідження спрямована на теоретичне обґрунтування підходів до управління ризиками при*

інтеграції біткоїна в бізнес-процеси з використанням акторно-мережевої методології, що дозволяє розглядати криптовалютну систему як сукупність взаємодіючих гетерогенних елементів. ***Методи.*** *У роботі використано міждисциплінарний підхід, що об'єднує акторно-мережеву теорію, концепції інформаційної безпеки та інституційний аналіз криптоекономічних систем. Проведено систематизацію досліджень функціонування протоколу Біткоїн з позиції взаємодії технічних і соціальних компонентів. Застосовано компаративний аналіз архітектури безпеки традиційних фінансових систем і децентралізованих криптовалютних структур.* ***Результати.*** *Систематизовано основні категорії ризиків, пов'язаних з використанням біткоїна в бізнесі (волатильність цін, регуляторна невизначеність, кіберзагрози, операційні та репутаційні ризики), оцінено їхню специфіку з урахуванням децентралізованої природи криптовалюти. Виявлено подвійну природу транзакцій, що виступають одночасно засобом передачі вартості та об'єктом економічної конкуренції, що створює специфічне середовище ризиків. Проаналізовано практичний досвід провідних учасників криптовалютної індустрії, що демонструє ефективність багаторівневих підходів до управління ризиками. Розглянуто роль технічних особливостей протоколу Біткоїн (децентралізація, криптографічний захист, прозорість реєстру, незмінність даних) в управлінні ризиками. Обґрунтовано, що ці характеристики створюють принципово іншу архітектуру безпеки порівняно з традиційними фінансовими системами, що вимагає від бізнесу переосмислення підходів до оцінки та мінімізації ризиків.* ***Висновки.*** *Ефективне управління ризиками при використанні біткоїна в бізнесі вимагає комплексного підходу, що інтегрує технологічні рішення з фінансовими та організаційними заходами. Фундаментальні характеристики протоколу Біткоїн створюють принципово іншу архітектуру безпеки порівняно з традиційними системами, що зумовлює необхідність перегляду класичних методів оцінки та мінімізації ризиків.*

 ISSN 3041-2129

Ключові слова: *ризики, бізнес-модель, децентралізовані системи, блокчейн, протокол, криптовалютна безпека, культура управління, філософія управління.*

Risk management strategies in bitcoin business integration: an actor-network approach

Roman Pavlov

PhD in Economics, Associate Professor, Associate Professor of Department of Economics, Entrepreneurship and Enterprise Management, Oles Honchar Dnipro National University, Dnipro, Ukraine, https://orcid.org/0000-0001-7629-2730.

Tetiana Pavlova

Doctor of Philosophical Science, Professor, Professor of Department of Philosophy, Oles Honchar Dnipro National University, Dnipro, Ukraine, https://orcid.org/0000-0001-7178-3573.

Tetiana Grynko

Doctor of Sciences in Economics, Professor, Dean of the Faculty of Economics, Oles Honchar Dnipro National University, Dnipro, Ukraine, https://orcid.org/0000-0002-7882-4523.

Abstract. *As a result of the research, risk minimization strategies that integrate technological, economic, social and cultural aspects of the functioning of bitcoin in business activities have been established.* ***Purpose.*** *The research is aimed at the theoretical substantiation of approaches to risk management when integrating bitcoin into business processes using the actor -network methodology, which allows*

considering the cryptocurrency system as a set of interacting heterogeneous elements. ***Methods.*** *The work uses an interdisciplinary approach that combines actor-network theory, concepts of information security, and institutional analysis of crypto-economic systems. The systematization of studies of the functioning of the Bitcoin protocol from the standpoint of the interaction of technical and social components has been carried out. A comparative analysis of the security architecture of traditional financial systems and decentralized cryptocurrency structures is applied.* ***Results.*** *The main categories of risks associated with the use of bitcoin in business are systematized (price volatility, regulatory uncertainty, cyberthreats, operational and reputational risks), and their specifics are assessed taking into account the decentralized nature of cryptocurrency. The dual nature of transactions, which are simultaneously a means of value transfer and an object of economic competition, which creates a specific risk environment, is revealed. The practical experience of the leading participants in the cryptocurrency industry is analyzed, demonstrating the effectiveness of multi-level approaches to risk management. The role of technical features of the Bitcoin protocol (decentralization, cryptographic protection, registry transparency, data immutability) in risk management is considered. It is substantiated that these characteristics create a fundamentally different security architecture compared to traditional financial systems, which requires business to rethink approaches to risk assessment and minimization.* ***Conclusions.*** *Effective risk management when using bitcoin in business requires a comprehensive approach that integrates technological solutions with financial and organizational measures. The fundamental characteristics of the Bitcoin protocol create a fundamentally different security architecture compared to traditional systems, which makes it necessary to review the classic methods of risk assessment and minimization.*

Keywords: *risks, business model, decentralized systems, blockchain, protocol, cryptocurrency security, management culture, management philosophy.*

Постановка проблеми. Автономія Біткоїна зумовлена взаємодією, організованою протоколом. Цей протокол створює епістемологічний розрив за допомогою об'єкта «транзакція», який для користувачів виступає засобом передачі грошових коштів, а для майнерів слугує джерелом винагороди. Користувачі взаємодіють через мережу на відстані, сприймаючи її як надійний реєстр, що підтримується майнерами. Останні, у свою чергу, обмежені протоколом консенсусу, що відображає різні гіпотези про транзакційний простір Біткоїна та його учасників.

У 1980-х роках дослідники, такі як Баррі Барнс [5], Мішель Каллон [7] і Джон Ло [18], аналізували теми автономії та влади через призму делегування та дії на відстані, уникаючи використання соціальних структур як основи для пояснення колективних дій. Їхні дослідження заклали фундамент для акторно-мережевої теорії (Actor-network theory), яка вивчає зусилля з визначення суспільства через асоціації, включаючи технічні пристрої. Згідно з роботами Бруно Латура [17], Ло [20] і Фабіана Муньєси [24], люди вирішують організаційні проблеми, використовуючи стійкі об'єкти, такі як записи. Така перспектива дозволяє розглядати інновації як практику соціального конструювання та управління: розробники та промоутери технічних систем прагнуть стабілізувати певні асоціації, що проявляється в матеріальній семіотиці через зв'язування елементів у послідовний ланцюг.

Такий підхід інтерпретує поняття автономії, контролю та інтересів, пов'язаних з владою, як результати асоціацій, створюваних акторами, і спирається на ідеї Латура [16], який вважав поняття влади «гнучким і порожнім» і пропонував відмовитися від нього. Латур стверджував, що влада не є властивістю або дією актора, а виникає як результат асоціацій, які слід піддавати аналізу. Таким чином, влада стає об'єктом дослідження, що вимагає пояснення, а не концептом-причиною. На думку Латура, влада лише узагальнює наслідки колективної дії, не розкриваючи її основ. Вона представлена як композиція акторів, тимчасово об'єднаних у схеми для реалізації проєкту. Замість опори на

соціальну структуру групи людей прагнуть визначити її природу і переконати інших прийняти це визначення [16].

У контексті зростаючої інтеграції криптовалют у підприємницьку діяльність особливу актуальність набуває стратегічне управління ризиками при використанні біткоїна в бізнесі. Мережева природа протоколу Біткоїн і відсутність централізованого регулювання формують особливе середовище ризиків, що вимагає теоретичного осмислення і вироблення практичних підходів до їх мінімізації. Акторно-мережева теорія надає унікальний інструментарій для аналізу взаємодії технічних, економічних і соціальних компонентів в екосистемі біткоїна, дозволяючи концептуалізувати ризики не як автономні явища, а як результат складних асоціацій між учасниками мережі. Застосування даного підходу сприяє розробці ефективних стратегій управління ризиками, що враховують як технологічні особливості протоколу, так і поведінкові та культурні аспекти його учасників, що критично важливо для сталого розвитку бізнес-моделей, заснованих на криптовалютних транзакціях.

Аналіз останніх досліджень і публікацій. Основоположне значення для розуміння технічної архітектури та концептуальних основ протоколу Біткоїн має робота Сатоші Накамото [25], який запропонував рішення проблеми подвійних витрат через механізм «доказ роботи» (Proof of Work), що заклало фундамент для подальшого розвитку як технічних, так і економічних аспектів функціонування криптовалют. Розвиваючи технічне розуміння децентралізованих систем, Арвінд Нараяна та співавтори [26] провели комплексний аналіз технології блокчейн, деталізувавши механізми забезпечення безпеки та консенсусу в мережі Біткоїн.

У роботі Жака Фав'є та Адлі Таккал Батай [8] особлива увага приділяється трансформації сутності грошей у контексті появи біткоїна. Автори акцентують увагу на концепції «валюти-цінності», вільної від боргових відносин, що створює нову парадигму для бізнес-взаємодій. Даний аспект також досліджується в роботі Сайфедіна Аммуса [3], який розглядає біткоїн як децентралізовану альтернативу центральному банківському регулюванню.

Ризики волатильності та ринкових маніпуляцій в екосистемі криптовалют детально проаналізовані в дослідженнях Юкуна Лю та Алеха Цивінського [22], а також Ніла Гандала та співавторів [9]. Ці роботи емпірично демонструють схильність ринку криптовалют до маніпуляцій і виявляють фактори, що впливають на волатильність цін, що критично важливо для формування стратегій управління фінансовими ризиками в бізнесі.

Кібербезпека та технічні аспекти захисту криптоактивів стають фокусом досліджень Віндена Вайлда та співавторів [29], а також Абхішека Кумара та колег [14], які деталізують проблему подвійних витрат і потенційні вразливості в блокчейн-системах. Дані дослідження підкреслюють необхідність комплексного підходу до забезпечення безпеки при інтеграції криптовалют у бізнес-процеси. Стратегічні аспекти управління криптоактивами та їх інтеграції в бізнес-моделі розглядаються в роботах [21; 27], де дослідники відзначають трансформаційний вплив блокчейн-технологій на підприємницькі моделі та виділяють ключові фактори успішної інтеграції. Екологічні аспекти майнінгу біткоїна та пов’язані з ними ризики аналізуються в роботі Олівера Апеха та Ннамді Нвулу [4], які акцентують увагу на потенціалі блокчейн-технологій для управління зеленою енергетикою при одночасній наявності екологічних викликів, пов’язаних з високим енергоспоживанням.

Виділення невирішених раніше частин загальної проблеми. Водночас, незважаючи на зростаючий обсяг досліджень, застосування акторно-мережевої теорії для аналізу ризиків і стратегій управління ними в контексті Біткоїна залишається недостатньо розробленою областю. Існуючі дослідження переважно фокусуються на технічних, економічних або регуляторних аспектах, не інтегруючи їх в єдину аналітичну рамку, що зумовлює актуальність цього дослідження.

Формулювання цілей статті (постановка завдання). Метою дослідження є теоретичне обґрунтування стратегічних підходів до управління ризиками при використанні біткоїна в бізнес-середовищі через призму акторно-

мережевого підходу. Дослідження прагне розкрити автономну природу протоколу Біткоїн, механізми його функціонування та специфіку ризиків, що виникають для підприємницьких структур, які інтегрують криптовалюту в свої процеси. Особлива увага приділяється осмисленню транзакції як гібридного об'єкта та розгляду технологічних, економічних і соціальних факторів, що формують комплексне середовище ризиків при роботі з біткоїном. Дослідження орієнтоване на виявлення та обґрунтування ефективних стратегій мінімізації цих ризиків з урахуванням децентралізованої природи криптовалюти та сучасних тенденцій розвитку ринку.

Виклад основного матеріалу дослідження.

Протокол Біткоїна як децентралізований механізм реєстрового управління. Як зазначають Фав'є та Таккал Батай [8], традиційна грошова система створює ілюзію осяжності грошей, хоча банкноти є борговими зобов'язаннями. На відміну від них, біткоїн, будучи неосяжним фізично, дозволяє власнику здійснювати будь-які операції (перекази, платежі, трансфери або дарування) без участі третіх осіб завдяки комп'ютерному протоколу, що робить біткоїн «валютою-цінністю», незалежною від боргових відносин.

Для забезпечення повного контролю над активами необхідно усунути владу установ над грошима, які повинні бути «осяжними», щоб власник міг розпоряджатися ними на власний розсуд [8]. Користувачі біткоїна володіють автономією, що проявляється в можливості здійснювати перекази, платежі та дарування без участі третіх осіб. Дана ідея лежить в основі розробки Біткоїна [25] – система повинна виключати втручання третіх сторін (індивідів або організацій), здатних перешкоджати діям користувача. Такий підхід контрастує з традиційними грошима, конверсія яких залежить від фінансових інститутів, що володіють правом відмовити у виконанні операцій з юридичних або комерційних причин.

Протокол перетворює гроші в осяжний об'єкт – реєстр, доступний для зміни будь-яким користувачем. Транзакції, такі як перекази або платежі, являють

собою корекції сум біткоїнів у реєстрі на рахунках ініціатора (дебет) і отримувача (кредит). Завдяки доступності протоколу через інтернет, транзакції стають, за висловом Ло [19], «дією на відстані» щодо реєстру. Протокол забезпечує комунікацію без спотворень, що Ло пояснює як результат створення мереж, що дозволяють безпечно передавати інформацію від центру до периферії [19].

Дія користувачів на відстані щодо реєстру зумовлена пасивною роллю учасників мережі, іменованих «майнерами». Саме завдяки відсутності їх втручання в транзакції, що передаються, Біткоїн забезпечує користувачам «контроль» – транзакції зберігають параметри, встановлені користувачами, і циркулюють у середовищі без спотворень вихідних характеристик. Дослідження Ло знаходяться в руслі більш широкої наукової рефлексії середини 1980-х років про взаємозв'язок знання і влади. Ло брав участь у цих дискусіях спільно з іншими представниками соціології науки та акторно-мережевої теорії, пропонуючи досліджувати механізми обмеження автономії діючих суб'єктів [18], аж до повного підпорядкування елементів системи певним правилам. Барнс також вніс суттєвий внесок у дану дискусію. Він трансформував веберівське визначення влади як «влада плюс легітимність» у концепцію «влада мінус дискреція» [5], оскільки вона передбачає здатність формувати власні судження і приймати рішення на основі власного розсуду, на відміну від авторитету.

Протокол виступає ключовим елементом, що забезпечує автономію Біткоїна. Він являє собою сукупність правил і інструкцій, розподілених серед десятків тисяч майнерів, кожен з яких підтримує власну копію реєстру, синхронізовану з версіями інших учасників мережі. Така узгодженість дозволяє розглядати реєстр як єдине ціле, незважаючи на існування безлічі його екземплярів по всьому світу. У термінології Барнса майнери постають авторитетами, позбавленими владних повноважень, тобто можливості здійснювати дискреційні дії щодо рахунків користувачів. Ідеї Барнса [5] про

формування пасивних людських агентів знайшли відображення в дослідженнях, що заклали основи акторно-мережевої теорії. Вчені, які розвивали цю область, поширили принцип обмеження дискреції на нелюдських акторів. Каллон запропонував чітку формулювання, згідно з яким будь-яка боротьба передбачає визначення акторів і їх характеристик, а їх взаємодія здійснюється через запозичення сили в процесі, позначеному як «трансляція» [7].

Встановлений порядок, при якому єдиний реєстр підтримується на численних веб-ресурсах залежно від кількості майнерів по всьому світу, а також процес зниження їх активної ролі, не видається очевидним. Антропологічний підхід до дослідження технологій, зокрема роботи Мадлен Акріч [2], підкреслює політичне вимірювання технічних об'єктів, розглядаючи їх як акторів у гетерогенних мережах, що об'єднують людські та нелюдські елементи, що виступає особливістю сучасної культури. Ці об'єкти, на думку Акріч, не просто існують, але активно беруть участь у формуванні та стабілізації соціальних відносин, володіючи «політичною силою». Вони включені в складні ланцюжки взаємодій, що охоплюють людей, інструменти, машини та ресурси, що дозволяє їм трансформувати, натуралізувати і деполітизувати соціальні зв'язки, переносячи їх в інші форми вираження [2].

З одного боку, протокол можна розглядати як механізм залучення і притягнення, за допомогою якого виявляються характеристики, що приписуються майнерам. Дані характеристики сприяють їх об'єднанню і трансформації в мережу пасивних агентів, що функціонують в рамках заданої структури. З іншого боку, необхідно враховувати гіпотези, закладені розробниками в протокол консенсусу, що відповідає концепції «скрипту», запропонованої Акріч [1]. Згідно з даною концепцією, будь-який технічний об'єкт являє собою результат процесу, в ході якого розробники інтегрують свої уявлення про світ в його технічний зміст. Таким чином, слід переосмислити теоретичні основи протоколу, підкреслюючи його значення як інструменту організації та реалізації уявлень про світ у технічній практиці.

Консенсус в умовах недовіри: подолання «проблеми візантійських генералів». Протокол Біткоїна [25] являє собою рішення класичної задачі інформатики, відомої під метафоричним позначенням «проблема візантійських генералів». Дана задача формулюється як проблема забезпечення коректного функціонування обчислювальної системи, що складається з безлічі взаємопов'язаних компонентів, які обмінюються інформацією, незважаючи на потенційну ненадійність окремих елементів, здатних поставляти суперечливі дані. У статті, опублікованій в 1982 році, дослідники Леслі Лемпорт, Роберт Шостак і Маршалл Піз докладно описали дану проблему і запропонували можливі підходи до її вирішення, виходячи з певних припущень про природу системи та її складових [15]. Основною метою їх роботи було систематичне вивчення труднощів, що виникають внаслідок конфліктів в інформації, що передається між компонентами системи. Для наочності своїх міркувань автори зазначеної статті вдалися до евристичної метафори, уподібнивши кожен компонент системи генералу візантійської армії. Згідно з цією аналогією, генерали, обмінюючись повідомленнями через посильних, прагнуть виробити узгоджений план дій, в даному випадку – план битви. Така метафора слугує інструментом для розробки обчислювальних алгоритмів, які забезпечують стійке функціонування системи, гарантуючи успішну реалізацію узгодженого плану, незважаючи на можливі збої або навмисні спотворення інформації.

У роботі Лемпорта та співавторів [15] підкреслюється, що надійні комп'ютерні системи повинні бути здатні ефективно справлятися з наявністю несправних елементів, які можуть поставляти суперечливі відомості різним частинам системи. Для ілюстрації цієї ідеї описується абстрактний сценарій, в якому група генералів візантійської армії оточує ворожий місто і, обмінюючись інформацією виключно через посильних, повинна прийти до єдиного рішення щодо плану атаки. Однак присутність зрадників серед генералів, що прагнуть ввести інших в оману, ускладнює задачу. У зв'язку з цим виникає необхідність у розробці алгоритму, який забезпечив би досягнення консенсусу серед лояльних

учасників. Було встановлено, що в разі використання виключно усних повідомлень рішення задачі можливе лише за умови, що частка лояльних генералів перевищує дві третини від їх загального числа. При меншій кількості лояльних учасників навіть один зрадник здатний дезорієнтувати систему, перешкоджаючи досягненню згоди. Водночас, якщо застосовуються непідробні письмові повідомлення, проблема стає розв'язною незалежно від числа генералів і можливих зрадників. Такий висновок підкреслює важливість характеру комунікації в забезпеченні стійкості системи [15].

Рішення досліджуються через призму алгоритмів: який алгоритм забезпечує генералам (або компонентам системи) досягнення консенсусу (або точного обчислення)? Проблема поділяється на різні випадки в залежності від припущень про тип повідомлень, якими обмінюються генерали для узгодження. Наприклад, при використанні «усних» повідомлень – тих, що приймаються компонентом без можливості підтвердити їх достовірність від відправника, Лемпорт та співавтори [15] доводять, що не менше двох третин генералів повинні бути «лояльними» для роботи системи. Якщо ж більше третини генералів виявляються «зрадниками» (що порушують свої функції, свідомо або випадково), лояльні генерали (що працюють коректно) не зможуть прийти до згоди (точного обчислення). Термін «зрада» тут використовується як метафора, що позначає збій компонента з будь-якої причини, оскільки Лемпорт та співавтори [15] розглядають будь-яку внутрішню неполадку системи як елемент, що видає невірні дані, будь то наслідок помилки (апаратної або програмної) або результат «зловмисної поведінки».

У випадку з Біткоїном «компоненти» системи – це майнери, а їх обчислення відповідають оновленню реєстру з урахуванням транзакцій, здійснених користувачами за останні кілька хвилин. «Повідомлення», якими обмінюються майнери, являють собою транзакції, що очікують запису, зібрані в так звані «блоки». Дані блоки циркулюють між майнерами, і кожен блок – це «план битви», запропонований одним майнером іншим для «протистояння»

 ISSN 3041-2129

оновленню реєстру. Кожен майнер, як і кожен генерал, може бути чесним, тобто додавати реальні транзакції, сформовані користувачами, або недобросовісним, намагаючись порушити функціонування системи. Протокол Біткоїна розроблений таким чином, щоб одночасно задовольняти двом вимогам:

1) забезпечувати відкритість, дозволяючи будь-якій людині стати користувачем або майнером незалежно від місцезнаходження та намірів;

2) гарантувати цілісність реєстру, захищаючи його від несанкціонованих змін.

Архітектура відмовостійкості: формування надійної криптовалютної системи. Метафора візантійських генералів була корисною для Накамото [25] при початковій розробці Біткоїна, а також вона стала регулярним відсиланням у презентаціях і промо-акціях, що докладно пояснюють його технічне функціонування. Щоб проілюструвати це, можна уявити таку картину: у середньовіччі король обороняє якесь місто. Лицарі, що прагнуть захопити його, розкидані по околицях і повинні діяти узгоджено, щоб здобути перемогу. Їх успіх залежить від точної координації через повідомлення. Однак лазутчики, підіслані королем або його прихильниками, можуть спотворити ці повідомлення, щоб зірвати план. Рішення, запропоноване Біткоїном, полягає в створенні системи, де інформація передається так, що її неможливо підробити. Це, як якби лицарі обмінювалися наказами, які ніхто не може змінити, гарантуючи успіх їхньої атаки.

Згаданий вище приклад наочно демонструє, як проблема візантійських генералів втілюється в Біткоїні: лояльні майнери подібні до лицарів, що працюють заради спільної мети, а недобросовісні – до лазутчиків, що прагнуть підірвати систему. В даному контексті, основне завдання Біткоїна полягає в запобіганні поширенню хибної інформації, що порушує цілісність реєстру, наприклад, шляхом зміни історії транзакцій або підтвердження непідписаних операцій з метою викрадення коштів. Якби така спроба суто теоретично вдалася, то шахрайський блок став би частиною реєстру, що в термінах Лемпорта та

співавторів [15] означало б прийняття системою «плану битви», що веде до поразки. У нашій метафорі це виглядало б так – лазутчики, видаючи себе за лицарів, підмінюють накази, змушуючи військо відступити замість атаки, і відступ стає реальністю (табл. 1).

Таблиця 1

Порівняння моделей відмовостійкості

Інформатика (Лемпорт та співавтори) [15]		**Стратегічні аналогії**	**Біткоїн**	
Наукове уявлення	**Метафора (візантійські генерали)**		**Концепція (Накамото) [25]**	**Метафора (лицарі та лазутчики)**
Справний компонент	Лояльні генерали	Надійні виконавці	Лояльні майнери	Лицарі, що координують атаку
Несправний компонент	Зрадник	Ризики та загрози	«Нелояльні» майнери	Лазутчики, що підмінюють накази
Інформація	Повідомлення	Дані для прийняття рішень	Блок транзакцій	Інформація
Комунікація	Досягти згоди	Узгодження дій	Записати блок	Здобути перемогу
Суперечлива інформація	Заплутати лояльних генералів	Дезінформація		Перешкодити перемозі
Алгоритм	План битви	Стратегічний план	Алгоритм консенсусу	Координація для захоплення міста

Джерело: складено авторами на основі аналізу [15; 25]

У повсякденній практиці майнери не поділяються на «лояльних» і «зрадників», на відміну від теоретичної моделі авторів роботи [15] або запропонованої метафори, що пов’язує проблему та її рішення в Біткоїні. Блоки також не класифікуються як «валідні» (що ведуть до «перемоги») або «шахрайські» (що ведуть до «поразки»). Блоки повинні залишатися валідними за будь-яких умов, тобто інформація не підлягає зміні незалежно від намірів майнерів. Система спроєктована так, щоб забезпечувати цілісність реєстру.

Якщо для Лемпорта та співавторів [15] абсолютна надійність – це припущення, що вимагає особливих проєктних рішень, то в Біткоїні вона є фундаментальною установкою, що визначає підхід до вирішення проблеми.

Децентралізоване регулювання: майнери як автономні учасники мережі. У своєму дослідженні Лемпорт та співавтори [15] розглядають задачу побудови надійних комп'ютерних систем і виділяють два принципових підходи до її вирішення. Перший передбачає використання компонентів, що спочатку володіють високим ступенем надійності. В свою чергу, другий підхід, що заснований на паралельному виконанні обчислень кількома компонентами, передбачає подальше визначення остаточного результату шляхом голосування за більшістю.

Система Біткоїна реалізує другий з запропонованих підходів, заснований на голосуванні за більшістю [25]. Даний вибір зумовлений неможливістю апріорної гарантії надійності кожного майнера – учасника мережі, що формує блоки транзакцій. Після створення блоку одним з майнерів інші учасники мережі здійснюють перевірку його відповідності встановленим правилам, що фактично являє собою процес голосування за його прийняття. Однак, на відміну від моделей, розглянутих Лемпортом та співавторами [15], де склад системи фіксований, Біткоїн характеризується динамічними межами, оскільки нові майнери можуть приєднуватися до мережі, а існуючі покидати її в будь-який час. Така особливість ускладнює функціонування системи, що діє у відкритому інтернет-середовищі, де введення бар'єрів для участі неприпустимо, оскільки це суперечило б принципам децентралізації та виключало б наявність центральної керуючої інстанції.

Організація голосування передбачає необхідність однозначної ідентифікації учасників для формування легітимного складу голосуючих. В умовах відкритої системи, такої як Біткоїн, ця задача виявляється нетривіальною. Використання IP-адрес як ідентифікаторів не забезпечує надійності, оскільки учасник здатний штучно створити безліч адрес, що дозволило б йому

маніпулювати результатами голосування за принципом «один IP – один голос». Для вирішення даної проблеми Біткоїн використовує механізм, при якому вага кожного голосу визначається обчислювальною потужністю, внесеною майнером у мережу. Такий підхід, відомий як Proof of Work, був обґрунтований Накамото на основі принципу «один процесор – один голос», забезпечуючи більш надійний розподіл голосів [25].

Протокол Біткоїна ідентифікує учасників на основі їх обчислювальної потужності, яка умовно співвідноситься з кількістю процесорів, задіяних кожним майнером при створенні блоку [25]. Для вимірювання такої потужності процес формування блоку транзакцій навмисно ускладнюється, набуваючи обчислювально витратного характеру. Дана складність введена виключно для забезпечення ідентифікації учасників і запобігання маніпуляціям у процесі голосування, оскільки без цієї міри збирання транзакцій у блок було б суттєво спрощено. В рамках протоколу майнер виконує алгоритм хешування, використовуючи як вхідні дані транзакції, що очікують підтвердження, а також ідентифікатор останнього блоку, доданого до реєстру [25]. Результатом хешування повинен стати хеш, що починається із заданої кількості нулів. Якщо отриманий хеш не задовольняє такій умові, то майнер зобов'язаний повторити обчислення зі зміненими параметрами. Перший майнер, який успішно створив відповідний хеш, розповсюджує сформований блок, що включає транзакції та хеш, серед інших учасників мережі. Кожен майнер, у свою чергу, перевіряє валідність блоку і при його відповідності додає його до власної копії реєстру, оновлюючи таким чином розподілену базу даних.

Транзакційна дуальність: економічні стимули валідаційного процесу. Протокол Біткоїна [25] передбачає винагороду за енергетичні витрати, пов'язані з ідентифікацією учасників за допомогою їх обчислювальних ресурсів. Майнер, який першим сформував коректний блок, отримує відповідну винагороду, що включає два елементи: фіксовану нагороду, що являє собою заздалегідь встановлену в коді форму емісії криптовалютних одиниць, і комісії за транзакції,

що вносяться користувачами мережі. Даний механізм подвійної винагороди виступає фундаментальною основою залучення майнерів до забезпечення надійності та стійкості мережі. Відсутність подібного стимулу перетворило б процес голосування, що вимагає значних енергозатрат для виконання алгоритму хешування при додаванні кожного блоку, в діяльність, привабливу лише для ентузіастів. Протокол [25] не будує припущень про мотивації майнерів, за винятком їх орієнтації на економічну вигоду, виражену в біткоїнах. Чим більшу обчислювальну потужність учасник вкладає в мережу, тим частіше він виконує алгоритм хешування і, відповідно, тим вища його ймовірність першим визначити хеш, що задовольняє заданим умовам. Таким чином, величина винагороди знаходиться в прямій залежності від обсягу прикладених обчислювальних зусиль. Створення блоку транзакцій набуває зовсім іншого значення, ніж участь в забезпеченні безпеки реєстру – це інвестиція в комп'ютерне обладнання та електроенергію, що окупається в біткоїнах. Частина протоколу, що організовує координацію майнерів, являє собою алгоритм консенсусу, відомий як Proof of Work, де робота відповідає зусиллям з пошуку задовільного хешу [25].

Конкуренція між майнерами регулюється адаптивним механізмом протоколу, що діє в двох вимірах. По-перше, зі зростанням сукупної обчислювальної потужності мережі, що визначається кількістю активних майнерів, збільшується складність задачі хешування. Це досягається шляхом підвищення числа початкових нулів, що вимагаються в хеші, що підтримує стабільну частоту формування блоків – приблизно один блок кожні десять хвилин. Складність обчислень, таким чином, обернено пропорційна кількості майнерів, підключених до мережі. По-друге, комісії за транзакції формують конкурентний ринок їх обробки – при збільшенні попиту на валідацію майнери отримують можливість віддавати перевагу транзакціям з найбільш високими комісіями. Як зазначають автори роботи [8], подібна конкуренція стимулює майнерів нарощувати обчислювальні потужності, що сприяє посиленню безпеки мережі. Вони підкреслюють, що «доказ роботи» являє собою єдиний ефективний

спосіб запобігання шахрайству в децентралізованій системі, де консенсус досягається через підтвердження блоків учасниками, що довели свої зусилля.

Безпека мережі безпосередньо пов'язана зі зростанням енергоспоживання, що створює бар'єр для потенційних зловживань. Чим вища загальна обчислювальна потужність мережі, тим складніше недобросовісному майнеру записати підроблений блок. Для цього йому довелося б контролювати понад половину всіх обчислювальних ресурсів, що дозволило б домінувати в процесі голосування за включення блоку. Цей тип запису відомий як «атака на 51%». У контексті ідей Барнса [5] і Ло [18; 19; 20], збільшення загальної обчислювальної потужності ускладнює здійснення дискреції над системою – обмежується можливість довільного втручання у функціонування системи. Таким чином, конкуренція, структурована протоколом, обмежує потенційно негативні дії майнерів, перетворюючи їх на учасників, що діють у суворій відповідності до встановлених правил.

Протокол втілює низку припущень, необхідних для автономного функціонування розподіленого реєстру. Світ представлений відкритим простором, де індивіди об'єднані протоколом як єдиним регулятором соціального порядку. Він виступає інструментом управління відносинами влади між учасниками, що очікувано вільні у своїх діях, з метою забезпечення безпеки реєстру. Однак однієї процедури голосування недостатньо для захисту від можливого зговору, що охоплює понад половину майнерів. Свобода намірів і дій учасників закладена в основу протоколу. Його адаптивність і конкуренція спрямовані на те, щоб стимулювати майнерів слідувати їх індивідуальним економічним інтересам, що визначаються балансом витрат на обладнання та електроенергію і отримуваної винагороди, що формується як емісією біткоїнів, так і комісіями користувачів.

Механізм автономного управління, реалізований у протоколі, трансформує транзакції в гібридні об'єкти. Для користувачів вони виступають як перекази (дарування або платежі), тоді як для майнерів – предметами «роботи», що

вимагають інвестицій. Протокол чітко розмежовує процес створення транзакції, що ініціюється користувачами, і її валідацію, що здійснюється майнерами. Валідація стає для останніх діяльністю, орієнтованою на економічний розрахунок, незалежною від змісту транзакцій, але такою, що виробляє результати, значущі для всієї системи, що об'єднує майнерів і користувачів. Запис транзакцій у реєстр не залежить від їх сутності, що відображає політичну ідею розробників Біткоїна – усунути дискреційну владу банків та інших централізованих інститутів над транзакційним процесом. Така автономія, що забезпечується протоколом Біткоїна, відкриває перед бізнесом нові перспективи, дозволяючи обійти обмеження традиційних фінансових систем. Однак разом з такими можливостями сучасні підприємці стикаються з необхідністю враховувати унікальні особливості технології, які вимагають продуманого підходу до забезпечення стабільності та безпеки операцій, що приводить нас до розгляду стратегічного управління ризиками при використанні біткоїна бізнес-структурами.

Інтеграція біткоїна в бізнес-процеси: стратегічний підхід до управління ризиками. В умовах децентралізованої природи біткоїна підприємницькі структури, що інтегрують цю криптовалюту в свої процеси, стикаються з рядом специфічних викликів і можливостей. До числа перших належать різкі коливання курсу, які можуть дестабілізувати фінансове планування, а також правова нестабільність, зумовлена відмінностями в регулюванні по країнах. Крім того, зростають ризики кібератак, таких як крадіжка коштів через уразливості в інфраструктурі. З іншого боку, біткоїн надає бізнесу шанс оптимізувати витрати за рахунок вилучення посередників, розширити клієнтську базу завдяки глобальній доступності та підвищити рівень захисту даних у транзакціях. Стратегічне управління ризиками виступає тут критично важливим інструментом, який дозволяє компаніям ефективно балансувати між цими факторами, отримуючи максимальну вигоду з технології (табл. 2).

Таблиця 2

Основні ризики використання Біткоїна в бізнесі та стратегії управління ними

Ризик	Опис	Стратегія управління
Волатильність цін	Значні коливання вартості біткоїна, що впливають на фінансову стабільність	Використання деривативів (ф'ючерси, опціони) і перехід на стейблкоіни для розрахунків
Регуляторна невизначеність	Непередбачувані зміни в законодавстві різних країн	Постійний моніторинг правових змін і залучення фахівців з комплаєнсу
Кіберзагрози	Загрози злому криптовалютних гаманців і крадіжки активів через фішинг або уразливості	Впровадження мультипідписних технологій, холодне зберігання та регулярні перевірки безпеки
Операційні ризики	Труднощі з впровадженням криптовалютних систем у поточні процеси	Використання протестованих рішень і навчання співробітників, автоматизація операцій
Репутаційні ризики	Скептицизм з боку клієнтів або партнерів щодо криптовалют	Інформування стейкхолдерів і акцент на прозорості та надійності операцій
Ринкові маніпуляції	Спекулятивні дії, що спотворюють вартість біткоїна	Аналіз ринкових трендів, диверсифікація інвестиційного портфеля
Технічні збої	Помилки в програмному забезпеченні або інфраструктурі	Тестування систем, резервне копіювання та оновлення програмного забезпечення
Екологічні ризики	Високе енергоспоживання майнінгу, що викликає критику і тиск регуляторів	Застосування «зелених» технологій і підтримка екологічно відповідальних майнінг-пулів
Соціальні ризики	Можливе використання біткоїна в незаконній діяльності, що впливає на репутацію бізнесу	Дотримання KYC/AML-процедур і співпраця з регульованими платформами

Джерело: складено авторами на основі аналізу [4; 8; 9; 10; 11; 13; 14; 21; 22; 23; 27; 29; 30]

Практичне застосування стратегій управління ризиками в криптовалютному бізнесі наочно демонструє, як компанії адаптують теоретичні підходи до реальних викликів динамічного ринку. Наприклад, криптовалютна

біржа Binance, одна з найбільших у світі, активно використовує багаторівневі системи безпеки, включаючи холодне зберігання для більшої частини активів користувачів і впровадження системи моніторингу підозрілих транзакцій на основі штучного інтелекту, щоб мінімізувати ризики кібератак і шахрайства [30]. У свою чергу, біржа Coinbase забезпечує зберігання 98% активів клієнтів у холодних гаманцях офлайн, що значно підвищує рівень захисту коштів користувачів [30]. Велика криптовалютна біржа Kraken також дотримується високих стандартів безпеки, зберігаючи близько 95% активів у холодних гаманцях, розподілених по всьому світу, і застосовуючи систему двофакторної аутентифікації для захисту акаунтів користувачів [30]. У контексті фінансових ризиків компанія Grayscale Investments, що керує великим криптовалютним фондом, застосовує стратегії диверсифікації портфеля, щоб знизити вплив волатильності біткоїна на загальні результати фонду, що особливо актуально в періоди різких ринкових коливань [10].

Для підвищення обізнаності співробітників і клієнтів про ризики та можливості Біткоїна компанії можуть використовувати інноваційні освітні інструменти, такі як комікси, які, як показує дослідження Оксани Гудошник і Олександра Крупського [12], ефективні для популяризації складних наукових ідей, включаючи блокчейн-технології. Нарешті, з урахуванням екологічних ризиків, пов’язаних з енерговитратним майнінгом, компанія Hive Blockchain перейшла на використання відновлюваних джерел енергії для своїх майнінг-операцій у деяких країнах, що не тільки зменшує вуглецевий слід, але й знижує репутаційні ризики перед лицем посилення регуляторних вимог [11]. Ці кейси підкреслюють, як криптовалютні компанії інтегрують управління ризиками у свою операційну діяльність, адаптуючись до кіберзагроз, фінансової нестабільності та глобальних екологічних викликів.

Протокол Біткоїна відіграє ключову роль у зниженні ризиків завдяки своїм фундаментальним характеристикам (табл. 3). Децентралізація, криптографічний захист і механізми консенсусу створюють основу для безпечного використання

криптовалюти в бізнесі. Розуміння цих особливостей дозволяє компаніям вибудовувати стійкі моделі роботи з Біткоїном, мінімізуючи залежність від зовнішніх посередників і посилюючи контроль над активами.

Таблиця 3

Роль протоколу Біткоїна в управлінні ризиками

Характеристика протоколу	Вплив на управління ризиками	Ризики, що знижуються
Децентралізація	Усунення єдиної точки відмови та контролю з боку третіх осіб	Необґрунтоване втручання регуляторів
Proof of Work	Забезпечення безпеки мережі через високі обчислювальні витрати	Подвійне витрачання та атаки на мережу
Прозорість реєстру	Відкритий доступ до даних транзакцій для перевірки та аудиту	Помилки обліку та шахрайство
Незмінність	Захист історії транзакцій від змін	Фальсифікація даних
Криптографічний захист	Шифрування даних і ключів для запобігання витокам	Кібератаки та крадіжка активів
Відкритий код	Прозорість розробки та можливість незалежного аналізу вразливостей	Програмні помилки та приховані загрози
Обмежена емісія	Обмежений обсяг пропозиції (21 млн BTC)	Знецінення активів
Приватність (Taproot)	Покращення конфіденційності	Витік даних та відстеження операцій

Джерело: складено авторами на основі аналізу [3; 6; 8; 14; 21; 25; 26; 28; 29]

Протокол Біткоїна демонструє переваги перед традиційними системами, такими як банки, де централізація створює вразливості [8; 25]. Наприклад, впровадження Lightning Network дозволило проєктам, таким як BitPay, прискорити обробку платежів, знизивши операційні витрати, а оновлення Taproot підвищило конфіденційність, що важливо для компаній, які працюють з чутливими даними [3; 6]. Децентралізована структура виключає ризики, пов’язані із залежністю від єдиного керуючого органу, а криптографічні механізми забезпечують надійність зберігання активів. Порівняно з іншими

криптовалютами, такими як Ether, біткоїн зберігає лідерство в стійкості до атак завдяки Proof of Work, хоча і поступається в швидкості транзакцій [3; 6]. Такі особливості роблять його привабливим інструментом для бізнесу, за умови усвідомленого підходу до технічних і ринкових аспектів.

Висновки. Протокол Біткоїн являє собою гетерогенну мережу акторів (майнерів, користувачів, технічних пристроїв), взаємодія яких регулюється за допомогою закладених у нього алгоритмів консенсусу. Така архітектура формує унікальне середовище ризиків, що характеризується відсутністю централізованого контролю, що вимагає переосмислення традиційних підходів до управління ними.

Автономія біткоїна забезпечується через перетворення транзакцій у гібридні об’єкти, які для користувачів виступають засобом передачі грошових коштів, а для майнерів – джерелом винагороди. Ця дуальність створює епістемологічний розрив, який, з одного боку, забезпечує незалежність системи від зовнішнього регулювання, а з іншого – формує специфічні ризики, пов’язані зі сприйняттям і використанням криптовалюти.

Рішення «проблеми візантійських генералів» у системі Біткоїна через механізм Proof of Work створює технологічну основу для забезпечення безпеки мережі, але одночасно породжує ризики, пов’язані з можливою централізацією обчислювальних потужностей. Стратегічне управління такими ризиками повинно враховувати динаміку розвитку майнінгової індустрії та потенційні зміни в структурі розподілу обчислювальних ресурсів.

Аналіз основних категорій ризиків, пов’язаних з використанням біткоїна в бізнесі, демонструє їх взаємопов’язаний характер. Волатильність цін, регуляторна невизначеність, кіберзагрози та операційні ризики не є ізольованими феноменами, а являють собою результат складних взаємодій між різними компонентами екосистеми біткоїна.

Ефективне стратегічне управління ризиками при інтеграції біткоїна в бізнес вимагає комплексного підходу, який інтегрує технічні рішення

(використання багаторівневих систем безпеки, холодне зберігання), фінансові інструменти (деривативи, диверсифікація) та організаційні заходи (навчання персоналу, моніторинг регуляторних змін).

Практичний досвід провідних учасників криптовалютної індустрії (Binance, Coinbase, Kraken) демонструє ефективність багаторівневих підходів до управління ризиками, що поєднують технологічні рішення з організаційними практиками. Такий підхід забезпечує адаптивність до швидко мінливих умов криптовалютного ринку та регуляторного середовища.

Роль протоколу Біткоїн в управлінні ризиками проявляється через його основні характеристики: децентралізацію, криптографічний захист, прозорість реєстру та незмінність даних. Ці особливості створюють принципово іншу архітектуру безпеки порівняно з традиційними фінансовими системами, що вимагає від бізнесу переосмислення підходів до оцінки та мінімізації ризиків.

Отримані результати мають як теоретичне значення, розширюючи застосування акторно-мережевої теорії для аналізу криптовалютних екосистем, так і практичну цінність, надаючи бізнесу концептуальну основу для розробки ефективних стратегій управління ризиками при роботі з біткоїном. Подальші дослідження в даній області можуть бути спрямовані на деталізацію стратегій для конкретних галузей і бізнес-моделей, а також на аналіз трансформації ризиків у контексті еволюції регуляторного середовища та технологічного розвитку протоколу Біткоїн.

Список використаних джерел

1. Akrich M. Comment décrire les objets techniques? *Techniques & Culture*. 1987. № 9. DOI: 10.4000/tc.863.

2. Akrich M. The De-Scription of Technical Objects. Shaping Technology / Building Society: Studies in Sociotechnical Change / ed. by W. E. Bijker, W. B. Carlson, T. Pinch. Cambridge: MIT Press, 1992. P. 205-224.

3. Ammous S. The Bitcoin Standard: The Decentralized Alternative to Central Banking. Hoboken: John Wiley & Sons, Inc., 2021. 304 p.

4. Apeh O. O., Nwulu N. I. Enhancing transparency and efficiency in green energy management through blockchain: A comprehensive bibliometric analysis. *Energy Nexus*. 2025. Vol. 18. 100405. DOI: 10.1016/j.nexus.2025.100405.

5. Barnes B. On Authority and its Relationship to Power. *The Sociological Review*. 1984. Vol. 32, No. 1_suppl. P. 180-195. DOI: 10.1111/j.1467-954X.1984.tb00112.x.

6. Blandin A., Pieters G., Wu Y., Eisermann T., Dek A., Taylor S., Njoki D. 3rd Global Cryptoasset Benchmarking Study. Cambridge Centre for Alternative Finance, 2020. 71 p.

7. Callon M. Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay. *The Sociological Review*. 1984. Vol. 32, No. 1_suppl. P. 196-233. DOI: 10.1111/j.1467-954X.1984.tb00113.x.

8. Favier J., Takkal Bataille A. Bitcoin – la Monnaie Acéphale. 2e édition. Québec: Éditions du Centre National de la Recherche Scientifique, 2023. 312 p.

9. Gandal N., Hamrick J. T., Moore T., Oberman T. Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics*. 2018. Vol. 95. P. 86-96. DOI: 10.1016/j.jmoneco.2017.12.004.

10. Grayscale Research. The Role of Crypto in a Portfolio. URL: https://research.grayscale.com/reports/the-role-of-crypto-in-a-portfolio/ (дата звернення: 14.03.2025).

11. HIVE Digital Technologies Announces Plans to Build 100 MW Hydroelectric Data Center in Paraguay, Targeting to Double Revenue and Increase Hashrate to Over 12 Exahash in the Next Year. HIVE Digital Technologies Ltd. URL: https://www.hivedigitaltechnologies.com. (дата звернення: 14.03.2025).

12. Hudoshnyk O., Krupskyi O. P. Science and comics: from popularization to the discipline of Comics Studies. *History of Science and Technology*. 2022. Vol. 12, No. 2. P. 210-230. DOI: 10.32703/2415-7422-2022-12-2-210-230.

13. Iakovenko V., Pavlov R., Pavlova T., Levkovich O. Transformational Opportunities for Business Entities in the Circular Economy. Circular Business Management in Sustainability. Lecture Notes in Management and Industrial Engineering. Cham: Springer, 2023. DOI: 10.1007/978-3-031-23463-7_6.

14. Kumar A., Kumar Sah B., Mehrotra T., Rajput G. K. A review on double spending problem in blockchain. *International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)*. IEEE, 2023. P. 881-889. DOI: 10.1109/CISES58720.2023.10183579.

15. Lamport L., Shostak R., Pease M. The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*. 1982. Vol. 4, No. 3. P. 382-401. DOI: 10.1145/357172.357176.

16. Latour B. The Powers of Association. *The Sociological Review*. 1984. Vol. 32, No. 1_suppl. P. 264-280. DOI: 10.1111/j.1467-954X.1984.tb00115.x.

17. Latour B. Reassembling the Social: An Introduction to Actor-Network-Theory. Oxford: Oxford University Press, 2005. 301 p.

18. Law J. Editor's Introduction: Power/Knowledge and the Dissolution of the Sociology of Knowledge. *The Sociological Review*. 1984. Vol. 32, No. 1_suppl. P. 1-19. DOI: 10.1111/j.1467-954X.1984.tb00104.x.

19. Law J. On the Methods of Long-Distance Control: Vessels, Navigation and the Portuguese Route to India. *The Sociological Review*. 1984. Vol. 32, No. 1_suppl. P. 234-263. DOI: 10.1111/j.1467-954X.1984.tb00114.x.

20. Law J. Actor Network Theory and Material Semiotics. The New Blackwell Companion to Social Theory / ed. by B. S. Turner. Chichester, West Sussex, United Kingdom: Wiley-Blackwell, 2009. P. 141-158.

21. Liaw K. T. (ed.) The Routledge handbook of FinTech. London: Routledge, 2021. 464 p. DOI: 10.4324/9780429292903.

22. Liu Y., Tsyvinski A. Risks and returns of cryptocurrency. *The Review of Financial Studies*. 2020. Vol. 34, No. 6. P. 2689-2727. DOI: 10.1093/rfs/hhaa113.

23. Makarov I., Schoar A. Blockchain analysis of the Bitcoin market. NBER Working Paper. 2022. No. 29396. 60 p.

24. Muniesa F. Actor-Network Theory. International Encyclopedia of the Social & Behavioral Sciences. Second Edition / ed. by J. D. Wright. Oxford: Elsevier, 2015. P. 80-84. DOI: 10.1016/B978-0-08-097086-8.85001-1.

25. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. URL: https://bitcoin.org/bitcoin.pdf (дата звернення: 14.03.2025).

26. Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press, 2016. 336 p.

27. Pavlov R., Zarutska O., Pavlova T., Grynko T., Levkovich O., Hordieieva-Herasymova L. Blockchain as a management technology: Institutionalization of crypto-assets and transformation of entrepreneurial models using the example of Ethereum. *Financial and Credit Activity Problems of Theory and Practice*. 2024. Vol. 6, No. 59. P. 151-166. DOI: 10.55643/fcaptp.6.59.2024.4529.

28. Rosenquist H., Hasselquist D., Arlitt M., Carlsson N. On the Dark Side of the Coin: Characterizing Bitcoin Use for Illicit Activities. *Passive and Active Measurement: 25th International Conference*, PAM 2024, Virtual Event, March 11–13, 2024, Proceedings, Part II. Springer-Verlag, 2024. P. 37-66. DOI: 10.1007/978-3-031-56252-5_3.

29. Wylde V., Rawindaran N., Lawrence J., Balasubramanian R., Prakash E., Jayal A., Khan I., Hewage C., Platts J. Cybersecurity, data privacy and blockchain: *A review. SN Computer Science*. 2022. Vol. 3, No. 2. 127. DOI: 10.1007/s42979-022-01020-4.

30. Zeilinger D. Europe's Safest Licensed Crypto Exchanges: Expert Analysis. Blockpit. URL: https://www.blockpit.io/blog/safest-crypto-exchanges-in-europe (дата звернення: 14.03.2025).