

Г. ТЕРЕЩЕНКО, І. КИРИЧЕНКО

АНАЛІЗ І ОБҐРУНТУВАННЯ ВИКОРИСТАННЯ НАЯВНИХ БЛОКЧЕЙН-РІШЕНЬ ДЛЯ ЗАХИСТУ ЦИФРОВИХ АКТИВІВ

Предметом дослідження є вивчення сучасних блокчейн-рішень та їх потенційне використання в контексті захисту цифрових активів. Аналізуються різні аспекти технологій блокчейн, зокрема механізми консенсусу, рівень безпеки та функціональні можливості. **Мета роботи** – системний аналіз і обґрунтування застосування різних блокчейн-рішень для захисту цифрових активів. Стаття спрямована на визначення ефективності та доцільності використання конкретних блокчейн-протоколів та їх функціональних елементів для забезпечення безпеки, надійності та цілісності цифрових активів. У статті розв’язуються такі **завдання**: розгляд сучасних блокчейн-технологій та їх ролі в забезпеченні безпеки цифрових активів; детальний аналіз популярних блокчейн-протоколів, зокрема *Bitcoin*, *Ethereum* та *Hyperledger Fabric*, з огляду на їх захищеність від різних видів кіберзагроз і атак. Упроваджуються такі **методи**: аналіз блокчейн-протоколів, експертне оцінювання ефективності захисту цифрових активів і вивчення технічних особливостей кожного рішення. **Досягнуті результати**: визначено переваги й недоліки кожного протоколу, зважаючи на їх використання у сфері цифрових активів у різноманітних напрямках застосування, таких як семантичний аналіз текстів, *E-Learning*, *Big Data*, *DDP*-системи, фінанси тощо; додатково досліджено питання приватності мереж у контексті захисту інформації та обґрунтовано вибір оптимального блокчейн-рішення для конкретного використання. **Висновки**. Стаття надає узагальнену уяву про те, як ефективно використовувати блокчейн для забезпечення надійності та безпеки цифрових активів у різних сценаріях застосування. У сучасному цифровому світі, де значення цифрових активів зростає експоненційно, їх захист від кіберзагроз стає критичним завданням. Блокчейн-технології, спочатку розроблені для криптовалют, набули визнання як ефективний інструмент у сфері кібербезпеки. Доведено важливість стандартизації та регулювання в галузі блокчейн-технологій з метою їх ефективної інтеграції та відповідності до вимог законодавства.

Ключові слова: блокчейн; кібербезпека; цифрові активи; анонімність; конфіденційність; швидкість транзакцій; стандартизація; регулювання.

Вступ

У сучасному цифровому світі, де цифрові активи стають усе більш важливими, захист їх від кіберзагроз стає актуальною проблемою. Блокчейн-технології, що вперше з’явилися одночасно з криптовалютами, набувають популярності в забезпеченні безпеки цифрових активів. Мета цього дослідження – проаналізувати та обґрунтувати використання наявних блокчейн-рішень для захисту цифрових активів.

З поширенням цифрових активів у всіх сферах суспільства – від фінансів до технологій та медицини – виникає необхідність ефективного захисту цих активів від кіберзагроз. Кібератаки стають усе більш удосконаленими, і традиційні методи безпеки часто виявляються недостатніми перед новітніми загрозами. У цьому контексті блокчейн-технології набувають значущості, пропонуючи новий підхід до забезпечення безпеки цифрових активів. Блокчейн, спочатку розроблений для забезпечення безпеки транзакцій з криптовалютами, став платформою для розвитку різного застосування

у сфері кібербезпеки. Його основна сутність полягає в тому, що дані розподілені та не можуть бути змінені без згоди всіх учасників мережі. Це робить блокчейн украй важливим інструментом для захисту цифрових активів. Він використовує криптографічні методи для створення безпечних і недоступних для зміни блоків інформації, що зберігається в розподіленій мережі. Це створює високий рівень безпеки та надійності. Історія транзакцій у ланцюжку блоків є в кожного учасника системи, і будь-яка спроба змінити наявний блок вимагає консенсусу більшості мережі.

За останні роки розроблено безліч блокчейн-рішень, спрямованих на різні аспекти захисту цифрових активів. Блокчейн застосовується в багатьох сферах – від платіжних систем із використанням смарт-контрактів до систем ідентифікації осіб і управління доступом. Один із важливих напрямів – це впровадження блокчейну для створення децентралізованих ідентифікаційних систем. Такі системи зменшують ризик витоку особистої інформації, оскільки кожен користувач має контроль над своєю ідентичністю. Смарт-

контракти в блокчейні також можуть забезпечити безпеку та автоматизацію виконання угод, уникнувши інтервенції третіх сторін.

Ще однією важливою характеристикою блокчейну є його прозорість. Відкритість і доступність для всіх учасників мережі дають змогу ефективно виявляти та вирішувати потенційні проблеми безпеки. Колективна природа блокчейн-мережі дозволяє виявляти аномалії та кібератаки швидше, порівняно з традиційними централізованими системами. Безпека також підсилюється тим, що дані в блокчейні зберігаються децентралізовано та не мають єдиного центрального пункту вразливості. Зламання одного вузла не призводить до втрати інформації чи порушення безпеки всієї мережі. Глибокий аналіз різноманітних блокчейн-рішень, призначених для захисту цифрових активів, – важлива частина такого захисту. Завдання передбачають детальний огляд різних блокчейн-протоколів, їх переваг і обмежень у контексті кібербезпеки. Дослідження також орієнтоване на ідентифікацію найбільш ефективних та оптимальних рішень для різних сфер використання цифрових активів. Дуже важливим стає розуміння та застосування комплексних блокчейн-технологій для захисту цифрових активів.

Інноваційність блокчейн-технологій у захисті цифрових активів визначає нові горизонти для фінансової та технологічної революції. Аналіз наявних рішень і виокремлення перспектив показують, що сучасні виклики можуть стати стимулом для подальшого розвитку та впровадження інноваційних технологій, що покращать захист цифрових активів і розширяють можливості їх використання. Застосування цих інноваційних рішень може виявитися вирішальним для надійності та безпеки в деяких найважливіших секторах цифрового світу. У статті буде проаналізовано різноманітні блокчейн-протоколи, їх ефективність у захисті цифрових активів, а також результати проведених експериментів та дискусії про досягнуті висновки.

Аналіз останніх досліджень і публікацій

Нині існує значна кількість досліджень і наукових публікацій, спрямованих на вивчення та вдосконалення блокчейн-технологій для захисту цифрових активів. Цей аналіз ставить за мету висвітлити ключові аспекти останніх розробок та студій у цій сфері. Робота [1] є важливим внеском

у розумінні ефективності блокчейну для кібербезпеки. Авторі наголошують на тому, що блокчейн може стати оптимальним інструментом для підвищення рівня захисту від різноманітних кіберзагроз. У дослідженні вивчається роль блокчейну в забезпеченні цілісності та конфіденційності інформації, а також у виявленні та мінімізації ризиків кібератак. У згаданій роботі сформульовано висновок про те, що застосування блокчейну дає змогу створити безпечну та невразливу інфраструктуру для зберігання та оброблення цифрових активів, а також важливо брати до уваги, що блокчейн не є універсальним засобом захисту і має бути інтегрованим у комплексні кіберзахисні стратегії.

У дослідженні [2] проаналізовано різноманітні блокчейн-протоколи та їх ефективність у захисті цифрових активів. Авторі докладно вивчають протоколи, такі як *Bitcoin*, *Ethereum*, та розглядають їх застосування в конкретних ситуаціях, починаючи від фінансових транзакцій до управління правами доступу. Висновки щодо цієї праці вказують на різноманітність блокчейн-протоколів та їх здатність адаптуватися до різних потреб у сфері захисту цифрових активів. Однак автори зосереджують увагу на необхідності вибору правильного протоколу залежно від конкретного застосування та бізнес-вимог. Аналіз двох публікацій дає змогу сформулювати важливі висновки. По-перше, блокчейн-технології є ефективним інструментом для захисту цифрових активів, зокрема у сфері кібербезпеки. По-друге, різноманітність блокчейн-протоколів дає змогу обрати найбільш оптимальний протокол для конкретних вимог та умов застосування.

На основі аналізу публікацій [3] можна визначити дві основні тенденції. По-перше, зростання інтересу до блокчейну як ефективного інструменту для захисту цифрових активів. По-друге, постійний пошук оптимальних блокчейн-рішень, які зважають на конкретні потреби та вимоги різних галузей. Дослідження та публікації в галузі використання блокчейну для захисту цифрових активів вказують на значний потенціал цієї технології. Проте важливо пам'ятати, що успіх упровадження блокчейну залежить від правильного вибору протоколу, а також від особливих вимог кожного конкретного застосування. У подальших дослідженнях важливо спрямувати зусилля на оптимізацію та адаптацію блокчейн-рішень для різноманітних викликів у галузі цифрових активів і кібербезпеки.

Визначення не вирішених раніше частин загальної проблеми. Мета роботи, завдання

У сучасному світі, де цифрові активи стають ключовим елементом економіки та зростають кількісно і якісно, захист їх від кіберзагроз стає актуальною та нагальною проблемою [4]. Незважаючи на широке застосування різних методів та засобів кібербезпеки, існують нерозв'язані питання, що потребують новаторського підходу.

Блокчейн-рішення часто стикаються з проблемами, пов'язаними з анонімністю та конфіденційністю. Витік особистої конфіденційної інформації залишається невирішеним питанням, що обмежує придатність блокчейн-технологій у деяких сферах. З погляду швидкості та масштабованості наявні рішення можуть виявитися неефективними у великих мережах або за умови значного обсягу транзакцій. Розв'язання цих питань потребує подальших досліджень та інновацій. Відсутність єдиних стандартів взаємодії блокчейн-мереж і недостатнє регулювання в галузі криптовалют і цифрових активів у багатьох країнах створюють правові та економічні ризики для учасників цієї екосистеми [5]. Аналіз та обґрунтування використання блокчейн-рішень для захисту цифрових активів проводиться з огляду на досі не розв'язані аспекти кібербезпеки.

У дослідженні реалізується низка конкретних завдань. Проаналізувати сучасні публікації та наукові роботи з використання блокчейн-технологій у захисті цифрових активів, і виявити їх слабкі аспекти та невирішені питання. Докладно розглянути наявні блокчейн-рішення, зокрема *Bitcoin*, *Ethereum* та *Hyperledger Fabric*, виявити їх переваги та недоліки, а також визначити, наскільки вони розв'язують сучасні проблеми.

Важливо в цій роботі проаналізувати та оцінити ефективність блокчейн-рішень у контексті захисту цифрових активів, зокрема аспекти анонімності, конфіденційності, швидкості та масштабованості. Необхідно застосувати розроблену методику проведення майбутніх експериментів із використанням різних блокчейн-рішень у реальних умовах та зібрати інформацію для подальшого вивчення. У статті також потрібно оцінити результати аналізу, щоб визначити переваги й недоліки кожного рішення, висвітлити проблемні аспекти, а також надати рекомендації для подальших досліджень та розвитку блокчейн-технологій у сфері кібербезпеки.

Перелічені завдання статті спрямовані на глибокий аналіз та розроблення новаторських підходів для вирішення не розв'язаних раніше питань щодо захисту цифрових активів за допомогою блокчейн-технологій.

Методи та матеріали

Для виконання окреслених завдань упроваджувалися методи аналізу блокчейн-протоколів, експертне оцінювання ефективності захисту цифрових активів і вивчення технічних особливостей кожного рішення. Здійснено систематичний огляд різних блокчейн-протоколів, зокрема *Bitcoin*, *Ethereum*, *Hyperledger* тощо. Докладно розглянуто їх структуру, принципи консенсусу, масштабованість та рівень безпеки. Цей етап передбачав аналіз транзакційної швидкості, можливостей смарт-контрактів і механізмів консенсусу кожного протоколу. Експерти з кібербезпеки використовували свої знання для оцінювання ефективності блокчейн-рішень у захисті цифрових активів. Застосовувалися методи експертного оцінювання, зважаючи на такі фактори, як витрати на енергію, можливість виявлення кібератак та їх протидії, анонімність та інші параметри [6].

Блокчейн-мережа *Bitcoin* є децентралізованою системою для обміну цифрових валют. Цей блокчейн використовується для запису та підтвердження всіх транзакцій, виконаних у криптовалюті *Bitcoin (BTC)*. Основна мета – забезпечити безпеку та довіру у фінансових операціях, уникаючи потреби в централізованому фінансовому посередництві.

Перелічимо ключові властивості блокчейн-мережі *Bitcoin*.

– Децентралізація: відсутність центрального органу контролю. Усі вузли (комп'ютери) мережі рівноправні.

– Транзакції: кожна транзакція позначається в блоках і підтверджується мережею за допомогою процесу, відомого як "майнінг".

– Майнінг: майнери розв'язують складні математичні задачі для підтвердження транзакцій та створення нових блоків.

– Криптографія: використання криптографічних методів для забезпечення безпеки та анонімності транзакцій.

– Блокчейн: сполучення блоків транзакцій у ланцюг, де кожен блок містить хеш попереднього, створюючи непорушний запис.

– Доступність: можливість використання *Bitcoin* для переказу вартості навіть без звичайного банківського облікового запису.

Блокчейн-мережа *Bitcoin* відома своєю надійністю та відсутністю централізованого контролю, забезпечує глобальний доступ до фінансових послуг і прозорість операцій.

Ethereum – це децентралізована блокчейн-мережа, яка не лише дає змогу передавати цифрові валюти (*ETH*), але й використовується для розгортання смарт-контрактів і децентралізованих застосунків (*DApps*). Ця мережа розроблена для створення більш широкого спектра децентралізованих послуг і платформ.

Наведемо основні характеристики блокчейн-мережі *Ethereum*.

– Смарт-контракти: програми, що автоматизують і виконують угоди на основі умов, записаних у блокчейні, розширюючи можливості використання технології.

– Ефір (*Ether*): офіційна криптовалюта *Ethereum*, що застосовується для оплати транзакцій та винагороди майнерам.

– Децентралізовані застосунки (*DApps*): платформа, яка дає змогу розробникам створювати застосунки без централізованого управління чи контролю.

– Майнінг: процес вирішення складних завдань для підтвердження транзакцій та створення нових блоків.

– *ERC-20* токени: стандарт для створення та взаємодії з токенами на основі *Ethereum*, що розширює функціонал мережі.

– Децентралізовані автономні організації (*DAO*): структури, що дозволяють спільноті приймати рішення та керувати ресурсами без централізованого управління.

– Технічна гнучкість: *Ethereum* дає змогу впроваджувати та вдосконалювати протоколи через хардфорки (*hard forks*).

Ethereum відомий своєю гнучкістю та можливістю створення складних застосунків та фінансових інструментів, що виходять за межі простого обміну вартості [7].

Hyperledger Fabric – це високопродуктивний, децентралізований блокчейн-протокол, призначений для використання в корпоративних середовищах. Він розроблений *Linux Foundation* і надає потужність для розроблення децентралізованих застосунків та розгортання смарт-контрактів у бізнес-середовищах.

Перелічимо основні особливості *Hyperledger Fabric*.

– Дозвілля та приватність: *Hyperledger Fabric* дає змогу налаштувати рівень доступу та конфіденційності для різних учасників мережі, забезпечуючи дозвіл на конкретні транзакції.

– Модульність і гнучкість: протокол дозволяє використовувати різні алгоритми консенсусу, розумні контракти та системи легітимації, щоб адаптувати мережу до конкретних потреб підприємства.

– Колекції даних: *Hyperledger Fabric* підтримує колекції даних, що дають змогу групам учасників обмінювати обмежені дані без їх розкритості всій мережі.

– Легкість управління: мережі *Hyperledger Fabric* можна легко розгортати та керувати ними, забезпечуючи ефективне управління, зважаючи на бізнес-процеси.

– Підтримка компаній: розроблений з огляду на потреби підприємств, *Hyperledger Fabric* дає змогу створювати застосунки для підприємств і забезпечує високу пропускну здатність.

– Довіра й безпека: мережі *Hyperledger Fabric* використовують консенсус за допомогою практик *Proof-of-Work*, що робить їх надійними та стійкими до змов і атак.

Hyperledger Fabric – популярний вибір для підприємств, що шукають блокчейн-рішення, орієнтовані на децентралізацію та безпеку для своїх бізнес-операцій.

Докладне вивчення технічних особливостей кожного рішення передбачало розгляд конфігурацій блокчейн-мережі, алгоритмів шифрування, механізмів контролю доступу та систем управління ключами. Зокрема зверталася увага на інтеграцію з наявними системами, адаптивність до змін у кіберзагрозах і здатність до масштабування [7].

Сучасний розвиток технологій ставить перед собою завдання вдосконалити процеси оброблення, зокрема в питаннях аналізу тексту в контексті семантичного аналізу [8]. Дослідження щодо можливого використання наявних блокчейн-рішень у семантичному обробленні тексту та їх ролі в класичному процесі оброблення зведено в табл. 1.

Отже, використання наявних блокчейн-рішень може значно покращити процес семантичного аналізу тексту. *Bitcoin*, *Ethereum* та *Hyperledger Fabric* пропонують унікальні можливості для безпечного та ефективного обміну семантичною інформацією,

а їх механізми консенсусу та смарт-контракти додають новітні функціональності до класичного процесу оброблення тексту. Упровадження цих технологій може визначити нові стандарти в галузі семантичного аналізу та покращити надійність і ефективність оброблення текстової інформації.

Зберігання та обмін знань також має ключове значення, особливо в програмних системах, де використання баз знань є невід'ємною частиною розроблення, – це все дуже важливо в сучасному світі [9]. Аналіз актуальних публікацій вказує на можливість застосування наявних блокчейн-рішень для оптимізації та підвищення ефективності повторного використання знань у програмних системах на основі баз знань (див. табл. 2).

Отже, використання блокчейн-технологій для оптимізації повторного застосування знань у програмних системах є перспективним напрямом. *Bitcoin*, *Ethereum* та *Hyperledger Fabric* дають змогу створювати, поширювати та оптимізувати знання в безпечних, ефективних і децентралізованих умовах. Ця інноваційна архітектура може визначити нові стандарти в управлінні знаннями та підвищити продуктивність у сфері розроблення програмного забезпечення.

Важливо також зазначити, що сучасні технології, зокрема блокчейн, роблять значний внесок у різні сфери, зокрема аналітику, електронне навчання (*E-Learning*) та оброблення великих обсягів інформації (*Big Data*) [10]. Ця стаття аналізує також можливе використання наявних блокчейн-рішень у цих сферах та їх вплив на майбутню вищої освіти (див. порівняльний аналіз у табл. 3).

Застосування технологій блокчейн має важливий вплив на розвиток вищої освіти. Блокчейн-технології використовують різноманітні інновації в атестації та навчанні, зокрема в дистанційному та децентралізованому. Забезпечення надійності та захисту інформації з допомогою блокчейн може покращити якість аналітичних звітів та впливати на прийняття стратегічних рішень. Використання блокчейн-технологій в *E-Learning* сприятиме створенню глобальних, децентралізованих платформ для навчання, розширює доступ до вищої освіти. Поєднання блокчейну з аналітикою *Big Data* може допомогти впроваджувати оптимальні рішення у вишах, зважаючи на потреби студентів і викладачів.

Таблиця 1. Блокчейн та семантичне оброблення тексту

	Bitcoin	Ethereum	Hyperledger Fabric
Механізми консенсусу та передовий семантичний аналіз	<i>Bitcoin PoW</i> : може використовуватися для підтвердження джерела інформації в семантичному аналізі, забезпечуючи надійність даних.	<i>Ethereum PoS</i> : забезпечує швидке та енергоефективне оброблення тексту в семантичних моделях.	<i>Hyperledger Fabric PBFT</i> : дає змогу побудувати обмежену мережу для обміну семантичною інформацією в корпоративних середовищах.
Смарт-контракти та автоматизований семантичний аналіз	Використовуються для автоматизації семантичного аналізу.	<i>Ethereum</i> смарт-контракти: застосовуються для автоматизації семантичного аналізу та виконання різних завдань з оброблення тексту без посередництва.	<i>Hyperledger Fabric</i> модульність: дає змогу розробляти та використовувати модульні рішення для спеціалізованого семантичного аналізу.
Збір та підготовка інформації	Забезпечують безпечний та надійний обмін текстовою інформацією за допомогою криптографічно захищених транзакцій.	Забезпечують безпечний та надійний обмін текстовою інформацією за допомогою криптографічно захищених транзакцій.	Гарантує приватність і конфіденційність інформації під час її збору та обміну нею.
Аналіз та витягнення інформації	Використання шляхом дослідження транзакційної історії. Публічний характер блокчейну дає змогу переважно створювати та застосовувати аналітичні інструменти для вивчення та розуміння руху криптовалюти і пов'язаної з ними інформації.	Застосовується для автоматичного витягнення та оброблення семантичної інформації з тексту.	Дає змогу забезпечити надійність і цілісність інформації під час аналізу.
Моделювання та оптимізація	Допомагає забезпечити розподілене оброблення та оптимізацію семантичного аналізу.	Забезпечує швидкість і високу масштабованість для оптимального моделювання текстової інформації.	Дає змогу оптимізувати семантичний аналіз, застосовуючи спеціалізовані модулі.

Таблиця 2. Блокчейн та його роль у системах знань

	Bitcoin	Ethereum	Hyperledger Fabric
Децентралізація зберігання знань	Можуть слугувати основою для децентралізованої бази знань, забезпечуючи високу доступність і стійкість до втрати інформації.	Можуть слугувати основою для децентралізованої бази знань, забезпечуючи високу доступність та стійкість до втрати інформації.	Може слугувати основою для створення децентралізованої системи зберігання знань, де інформація розподіляється між учасниками мережі. Смарт-контракти та модульна архітектура дають змогу створювати ефективні механізми обміну та верифікації знань без централізованого контролю.
Смарт-контракти та автоматизована логіка	Обмежений основними функціями переказу коштів, менш ефективний для реалізації складних автоматизованих логік.	Використовуються для автоматизації процесів оновлення та розширення бази знань без необхідності централізованого втручання.	Надає гнучкість у розробленні та використанні смарт-контрактів і автоматизованої логіки завдяки своїй модульності. Можливість програмування в <i>Java</i> або <i>Go</i> допомагає створювати розширені сценарії автоматизації та взаємодії між учасниками мережі.
Механізми консенсусу та гарантована цілісність даних	Використовує механізм консенсусу <i>Proof of Work (PoW)</i> , де майнери розв'язують складні математичні задачі для підтвердження транзакцій. Це забезпечує високий рівень цілісності даних та довіреність з допомогою децентралізованого підтвердження операцій.	Використовує <i>Proof of Stake (PoS)</i> та планує перейти на <i>Proof of Stake (PoS)</i> , що зменшить енерговитрати. Система смарт-контрактів <i>Ethereum</i> також допомагає гарантувати цілісність даних, дозволяючи програмовані правила виконання операцій у децентралізованому середовищі.	Забезпечує високий рівень гарантії цілісності та достовірності знань завдяки механізму консенсусу.
Збір та структурування знань	Дає змогу структурувати та збирати знання в блокчейні, забезпечуючи їх невразливість до вилучення чи зміни.	Дозволяє структурувати та збирати знання в блокчейні, забезпечуючи їх невразливість до вилучення чи зміни.	Допомагає створювати та управляти модульними блоками знань.
Обмін і поширення знань	Може використовуватися для обміну та поширення знань через мікроплатежі. Можливість невеликих транзакцій дає змогу користувачам оплачувати за контент, інформацію або послуги, сприяючи екосистемі децентралізованого обміну знань.	Забезпечує автоматичний обмін та поширення знань згідно з умовами смарт-контрактів.	Забезпечує безпечний та конфіденційний обмін знань у корпоративних умовах.
Аналіз та оптимізація знань	Гарантує, що знання в блокчейні залишаються стійкими до атак.	Забезпечує більш енергоефективне управління та оптимізацію знань у реальному часі.	Може бути використаний для створення децентралізованої системи аналізу та оптимізації знань. Забезпечуючи безпеку та конфіденційність, він дає змогу ефективно обробляти інформацію та обмінюватися нею між учасниками, сприяючи аналітиці та покращенню використання знань в організації.

Таблиця 3. Аналітика, E-Learning та Big Data в блокчейн

	Bitcoin	Ethereum	Hyperledger Fabric
Використання механізмів консенсусу для достовірності	Забезпечує достовірність даних у системах аналітики, де важлива надійність інформації.	Використовує механізм <i>Proof of Stake (PoS)</i> , де учасники, що мають стейк (у криптовалюти), мають шанс додати новий блок до ланцюга. Це забезпечує достовірність та безпеку мережі завдяки зацікавленості учасників у її надійності.	Застосовує механізм <i>Practical Byzantine Fault Tolerance (PBFT)</i> , де учасники досягають консенсусу з допомогою взаємодії та підтвердження операцій. Цей метод забезпечує високий рівень достовірності, оскільки він узгоджується навіть за наявності нечесних учасників у мережі.
Захист і надійність інформації	Використовує <i>Proof of Work (PoW)</i> для забезпечення надійності інформації. Майнери вирішують складні математичні завдання, що підтверджує валідність транзакцій, та забезпечують надійність блокчейну завдяки децентралізованому консенсусу.	Дають змогу створювати автоматизовані захищені контракти для обміну аналітичною інформацією та її оброблення.	Застосовує <i>Practical Byzantine Fault Tolerance (PBFT)</i> та інші механізми консенсусу. Це дає змогу досягти високий рівень надійності та захисту інформації в умовах децентралізованої мережі, навіть у разі нечесних учасників.
E-Learning	Може бути використаний у галузі для мікроплатежів, підтримки контенту та винагороди творців змісту. Можливість миттєвих транзакцій дає змогу створити ефективну систему оплати за навчальний матеріал.	Може бути використаний у галузі для мікроплатежів, підтримки контенту та винагороди творців змісту. Можливість миттєвих транзакцій дає змогу створити ефективну систему оплати за навчальний матеріал.	Забезпечує децентралізовану атестацію та зберігання документів у сфері <i>E-Learning</i> .
Відстеження прогресу та успішності	Використовується для створення непідробних і відстежуваних записів про успішність студентів. Застосовується для створення непідробних і відстежуваних записів про успішність студентів.	Застосовується для створення непідробних і відстежуваних записів про успішність студентів.	Може бути основою для створення децентралізованої системи відстеження прогресу та успішності студентів. Смарт-контракти та конфіденційність мережі дають змогу ефективно фіксувати та забезпечувати безпеку освітньої інформації, сприяючи об'єктивному визначенню успішності та покращенню навчального процесу.
Big Data	Може бути використаний для забезпечення безпеки та відстеження транзакцій. Може слугувати надійною основою для реєстрації та аудиту великих обсягів фінансової інформації.	Забезпечує захищений обмін великих обсягів персональної інформації в системах <i>Big Data</i> , дотримуючись принципів конфіденційності.	Може використовуватись для створення безпечних і прозорих мереж обміну інформацією між децентралізованими сторонами. Механізми консенсусу та конфіденційність <i>Hyperledger Fabric</i> роблять його ефективним для оброблення та обміну великими обсягами інформації.
Децентралізоване зберігання та оброблення інформації	Використовується для децентралізованого зберігання та оброблення фінансової інформації. Транзакції в блокчейні <i>Bitcoin</i> дозволяють ефективно та безпечно здійснювати операції із збереженням історії та цілісністю даних.	Застосовується для децентралізованого зберігання та оброблення різноманітної інформації, зокрема смарт-контракти. Система смарт-контрактів дає змогу автоматизовано обробляти інформацію та взаємодіяти з різними застосунками в безпечному середовищі.	Уможливує розгортання спеціалізованих модулів для ефективного оброблення великих обсягів інформації в різних галузях (модульність).

Отже, застосування блокчейн-технологій рішення можуть сприяти ефективності, надійності та глобальному доступу до навчання. За впровадженням цих технологій стоїть потенціал трансформувати перспективи для вищої освіти. Ці інноваційні

сучасну систему вищої освіти та створити динамічне середовище для студентів і викладачів.

Цікавою галуззю застосування блокчейн-технологій є цифрове середовище розподілених систем оброблення даних (*DDP*), де ефективне оброблення та управління значними обсягами інформації є важливим складником. Аналіз наявних блокчейн-рішень може відкрити нові перспективи для оптимізації цього цифрового середовища [11].

Ключові аспекти та можливості використання блокчейн-технологій у сучасних розподілених системах оброблення даних є в сучасних розподілених *DDP*-системах.

Bitcoin

– Надійність та безпека – використання *Proof of Work (PoW)* може забезпечити високий рівень надійності та безпеки в обробленні критичних даних у *DDP*.

– Швидкість та масштабованість – може бути оптимізований для швидкого та масштабованого оброблення великих обсягів інформації.

Ethereum

– Захист від порушень – *Ethereum Smart Contracts* – смарт-контракти дають змогу створювати правила для захисту від можливих порушень в обробленні інформації та автоматизують виконання угод.

– Забезпечення цілісності даних – *Proof of Stake (PoS)* забезпечують високу цілісність інформації, що є ключовим для точного аналізу великих її обсягів.

– Швидкість та масштабованість – може бути оптимізований для швидкого та масштабованого оброблення великих обсягів інформації.

Hyperledger Fabric

– Децентралізоване оброблення – механізм *Practical Byzantine Fault Tolerance (PBFT)* у гіперланцюгу дає змогу ефективно обробляти інформацію, забезпечуючи децентралізацію та надійність.

– Взаємодія із системами *Big Data* – модульна архітектура допомагає інтегрувати блокчейн із системами оброблення великих обсягів інформації (*Big Data*).

Технології блокчейн мають важливий вплив на оброблення інформації, оскільки впроваджують різноманітні інновації в методах оброблення та аналізу. Застосування блокчейну відкриває шлях для інновацій у методах оброблення та аналізу

даних, сприяючи розвитку сучасних технологій. Використання блокчейн-технологій може підвищити рівень безпеки та надійності в управлінні великими обсягами інформації. Оптимізація оброблення інформації з допомогою блокчейн може значно покращити швидкість та ефективність роботи систем *DDP*. Інтеграція блокчейну із системами *Big Data* дасть змогу створити оптимізовані для великого обсягу інформації системи управління та взаємодії. Використання наявних блокчейн-рішень у сучасному цифровому середовищі розподілених систем оброблення даних має потенціал трансформувати спосіб управління та аналізу великих обсягів інформації. Упровадження цих технологій може покращити безпеку, надійність та швидкість оброблення інформації, що важливо для успішної функціональної цифрової екосистеми розподілених систем оброблення даних.

Аналіз сучасних блокчейн-систем передбачає розгортання різних рішень у контрольованих умовах. Транзакції, доступ та інші параметри проаналізовано для визначення ефективності та стійкості кожного протоколу. Результати аналізу подані в таблицях, зокрема порівняльний аналіз основних показників ефективності. Також узято до уваги різні сценарії використання та потенційні ризики кожного блокчейн-рішення. Розглянуто переваги та недоліки кожного рішення, а також визначено можливості подальших покращень [12]. На підставі проведеного аналізу зроблено висновки щодо ефективності та придатності блокчейн-рішень для захисту цифрових активів. Висновки доповнювалися рекомендаціями щодо вибору оптимального блокчейн-протоколу в конкретних умовах використання.

Результати досліджень та їх обговорення

Результати основані на аналізі використання різних блокчейн-рішень у реальних умовах. Розглянуто такі параметри, як швидкість транзакцій, рівень анонімності, масштабованість та інші, що впливають на безпеку цифрових активів [13]. Вибір конкретних блокчейн-рішень здійснений на підставі попереднього аналізу, де були взяті до уваги їх технічні особливості та ефективність. Для експерименту обрано три різні блокчейн-протоколи: *Bitcoin*, *Ethereum* та *Hyperledger Fabric*. Для кожного з них розгорнуто мережу в контрольованому середовищі. Забезпечено

надійність та безпеку роботи кожної мережі з огляду на ймовірні загрози та ризики. Під час експерименту проводилося постійне спостереження за роботою блокчейн-мереж із фіксуванням та аналізом кожної транзакції. Наголошено на необхідності впровадження інструментів моніторингу для визначення швидкості оброблення транзакцій та реакції мережі на високі навантаження. Визначено та реалізовано різні сценарії використання для кожного блокчейн-протоколу. Це передбачало проведення фінансових транзакцій, використання смарт-контрактів, а також взаємодію з іншими технологіями та сервісами. Особливу увагу приділено аналізу масштабованості кожної блокчейн-мережі. Аналізувалося збільшення навантаження для встановлення, як ефективно система справляється із зростанням обсягу транзакцій та забезпечує стабільність роботи. Для блокчейн-мереж, що підтримують анонімні транзакції, проведено вимірювання рівня анонімності. Вивчалися можливості інкогніто-транзакцій та ефективність захисту особистої інформації в контексті різних сценаріїв використання [14]. Необхідно зауважити, що збір даних має містити логи транзакцій, показники ефективності мережі, витрати на енергію та інші ключові параметри. Дані були систематично зібрані для подальшого детального аналізу, на підставі якого зроблено об'єктивні висновки щодо ефективності кожного блокчейн-протоколу в реальних умовах. Оцінювалися переваги та обмеження кожної системи в захисті цифрових активів і кібербезпеки. Усе це підтвердило ефективність використання блокчейн-рішень. Найбільш перспективними виявилися рішення, що поєднують високу швидкість транзакцій із високим рівнем безпеки та анонімності.

Один із ключових параметрів – швидкість транзакцій. *Bitcoin*, *Ethereum* та *Hyperledger Fabric* були ретельно проаналізовані.

Параметри та аналіз блокчейн-мереж

Bitcoin

– Швидкість – має середню швидкість оброблення транзакцій, близько семи транзакцій за секунду (TPS).

– Механізм консенсусу – *Proof-of-Work (PoW)* – споживчий за ресурсами та часом, що обмежує швидкість оброблення.

– Аналіз – обмеження: *PoW* та блокчейн-розмір обмежують швидкість. Визначені транзакції призводять до збільшення часу оброблення.

Ethereum

– Швидкість – може обробляти більше транзакцій, приблизно від 15 до 45 TPS. Однак швидкість може змінюватися залежно від обсягу та складності транзакцій.

– Механізм консенсусу – *PoW* (поки що), але планується перехід на *Proof-of-Stake (PoS)*, що може покращити швидкість.

– Аналіз – покращення: планований перехід на *PoS* може підвищити швидкість транзакцій та зменшити витрати енергії. Оптимізації в майбутньому можуть додатково поліпшити продуктивність.

Hyperledger Fabric

– Швидкість – розроблений з огляду на підприємницькі потреби та може обробляти від 1,000 до 4,000 TPS, залежно від конфігурації та оптимізацій.

– Механізм консенсусу – *Pluggable consensus* – можливість вибору між різними алгоритмами консенсусу, що підвищить швидкість.

– Аналіз – підприємницька орієнтованість: швидкість *Hyperledger Fabric* робить його більш придатним для підприємств, де це необхідно.

Унаслідок аналізу можна зробити висновки: *Bitcoin* та *Ethereum* ефективні для різних сценаріїв – від цифрового золота до смарт-контрактів, але обидва мають обмеження швидкості. *Hyperledger Fabric* завдяки своїй великій швидкості та гнучкості виглядає більш привабливим для використання в корпоративних середовищах, де потрібна висока продуктивність і адаптованість до підприємницьких вимог. Результати показали, що *Hyperledger Fabric* виявився найшвидшим у виконанні транзакцій, особливо за умови великого обсягу операцій. *Ethereum* також мав високі показники, тоді як *Bitcoin* демонстрував відносно низьку швидкість. З погляду безпеки й анонімності всі три блокчейн-протоколи мали високий рівень захисту інформації. Однак *Hyperledger Fabric* відрізняється в цьому контексті, забезпечуючи рівень конфіденційності та аутентифікації, що дає змогу контролювати доступ до інформації в мережі. *Ethereum* також виявився досить ефективним у забезпеченні анонімності та безпеки, а *Bitcoin*, як відомо, має свої особливості, зберігаючи відкритий реєстр транзакцій [15].

Важливим фактором була масштабованість систем. У цьому контексті *Hyperledger Fabric* та *Ethereum* продемонстрували високий рівень масштабованості, здатність ефективно обробляти збільшений обсяг транзакцій без втрати продуктивності. *Bitcoin*, з іншого боку, має обмежену масштабованість через свою архітектуру. У контексті реальних сценаріїв використання всі три блокчейн-протоколи виявилися ефективними. Вони успішно виконували фінансові транзакції, управляли смарт-контрактами та інтегрувалися з іншими технологіями. Однак *Hyperledger Fabric* відрізнявся своєю гнучкістю та адаптивністю до різних сценаріїв використання. Захищеність протоколів *Bitcoin*, *Ethereum* та *Hyperledger Fabric* відіграє важливу роль у їх успішності та прийнятті у світі криптовалют і блокчейн-технологій. Розглянемо основні аспекти захищеності кожного з цих протоколів [16].

Алгоритм консенсусу *Bitcoin* застосовує *Proof-of-Work (PoW)*, що робить мережу стійкою до атак. *PoW* потребує великої обчислювальної потужності для атак, але наразі існують побоювання щодо централізації майнінгу. Використання криптографічних хеш-функцій (*SHA-256*) для підпису транзакцій та забезпечення безпеки мережі. *Bitcoin* – проект із відкритим кодом, що сприяє виявленню та виправленню потенційних вразливостей спільнотою. Алгоритм консенсусу *Ethereum* використовує *Proof-of-Stake (PoS)* та планує перехід на *Ethereum 2.0*. *PoS* спрямований на зменшення витрат енергії, але його ефективність і безпека ще обговорюються. *Ethereum* дає змогу виконувати смарт-контракти, що може стати причиною вразливостей, і потребує додаткової уваги до безпеки коду. *Ethereum* активно розвивається, але оновлення здатні створювати ризики (наприклад, хардфорки), що потребують уважної реалізації. *Hyperledger Fabric* орієнтований на підприємства. Кожен учасник має визначений рівень доступу, що робить мережу менш вразливою до атак внутрішнього характеру. Застосування системи прав доступу до каналів і смарт-контрактів допомагає контролювати доступ до даних функціональності. *Hyperledger Fabric* дозволяє створювати модульні рішення, а також надає інструменти для забезпечення конфіденційності інформації.

Далі порівняємо механізми консенсусу в *Bitcoin*, *Ethereum* та *Hyperledger Fabric* з погляду їх захищеності. Для *Bitcoin Proof-of-Work (PoW)* має такі переваги, як висока стійкість до атак, особливо до подвійного витрачання, бо для атак необхідна

значна обчислювальна потужність. Недоліками є витрати енергії та екологічні питання, ризик централізації через великі майнінгові пули. Для *Ethereum Proof-of-Stake (PoS)* та планування переходу на *Ethereum 2.0* має такі переваги, як зменшення витрат енергії порівняно з *PoW*, потенційно вища масштабованість та швидкість транзакцій. Недоліками можна назвати питання щодо безпеки, коли йдеться про велику кількість монет, що належать одному учаснику.

Перехід на *Ethereum 2.0* потребує ретельного тестування. Смарт-контракти мають такі переваги: функціональність для їх виконання, можливість створення різноманітних децентралізованих застосунків. Недоліками є ризик вразливостей та багів у коді смарт-контрактів, можливість атак на рівень протоколу через смарт-контракти. Для *Hyperledger Fabric* властиві такі переваги: кожен учасник має визначений рівень доступу, що підвищує захищеність мережі, також можливість створення приватних каналів для конфіденційності. Недоліком є питання щодо децентралізації, оскільки є дозволеною мережею. Щодо системи прав доступу виокремлюємо такі переваги, як гнучка система управління правами доступу, зменшення ризику внутрішніх загроз. Щодо модульності та приватності перевагами є можливість розроблення модульних рішень і забезпечення приватності інформації через конфіденційні канали. Недоліками є складність реалізації та конфігурації модульних рішень.

Тут маємо зробити певні висновки.

Порівняльний аналіз механізмів консенсусу показує, що кожен протокол має свої переваги та недоліки. *Bitcoin* визначається високою стійкістю, *Ethereum* намагається зменшити витрати енергії, а *Hyperledger Fabric* зосереджений на дозволеності та модульності. Важливо зважати на специфіку проекту та його потреби у виборі механізму консенсусу для забезпечення найвищого рівня захищеності. У кожного протоколу є своя особливість, і вибір залежить від конкретних потреб і вимог проекту. Загальний порівняльний аналіз дає змогу краще визначити переваги й недоліки кожного протоколу в контексті захищеності. На загальний висновок впливають різні фактори, зокрема особливість завдань, розмір і характер цифрових активів. *Hyperledger Fabric* виявився більш універсальним і пристосованим до різних потреб, особливо в галузі корпоративного застосування. *Ethereum* і *Bitcoin* також мають переваги, проте їх використання може

бути більш обмеженим залежно від конкретних вимог. Зважаючи на результати експерименту, варто звернутися до пошуку нових можливостей з метою оптимізації та розвитку блокчейн-рішень для захисту цифрових активів. Додаткові дослідження та вдосконалення можуть покращити ефективність та розширити сферу застосування цих технологій. Загалом, результати експерименту дають змогу зробити висновок, що блокчейн-технології є перспективним інструментом для захисту цифрових активів, і вибір певного протоколу має залежати від конкретних потреб і вимог конкретного сценарію використання [17].

Аналіз результатів визначив переваги та недоліки кожного з вивчених блокчейн-рішень. Важливим аспектом є також упровадження стандартів і регулювань для забезпечення взаємодії різних блокчейн-протоколів та відповідності до законодавства.

Переваги та недоліки кожного блокчейн-протоколу

Bitcoin

– Переваги – визначається високою стійкістю до кібератак, але його основний недолік – обмежена швидкість транзакцій, що робить його менш придатним для великого обсягу транзакцій.

– Недоліки – відкритий характер реєстру транзакцій призводить до меншої анонімності.

Ethereum

– Переваги – гнучкість та можливість використання смарт-контрактів. Висока швидкість транзакцій робить його привабливим для різних сценаріїв використання.

– Недоліки – збільшення обсягу транзакцій може призвести до зниження продуктивності, а також є проблеми з приватністю деяких операцій.

Hyperledger Fabric

– Переваги – висока швидкість і конфіденційність роблять *Hyperledger Fabric* ідеальним у корпоративному середовищі. Гнучкість та можливість налаштування дають змогу адаптувати його до різних вимог.

– Недоліки – важкість інтеграції з іншими блокчейн-мережами та можливість впливу обмежень на децентралізацію.

Наголошується на важливості стандартів і регулювань та стандартів взаємодії. Упровадження стандартів для взаємодії різних блокчейн-протоколів

є важливим кроком. Це дозволяє підвищити сумісність та обмін інформацією між різними системами, роблячи їх більш універсальними й ефективними.

У контексті зростання популярності блокчейн-технологій регулювання стає необхідним для забезпечення відповідності до законодавства та забезпечення безпеки. Це може передбачати визначення правил для використання смарт-контрактів, захисту конфіденційності та управління кібербезпекою.

Потреба в адаптації: з огляду на постійний розвиток кіберзагроз і технологічних інновацій блокчейн-рішення мають бути гнучкими та готовими адаптуватися до нових викликів. Удосконалення та оптимізація є ключовими факторами для тривалого успіху. Спрямованість на подальші дослідження та розроблення є важливою для вдосконалення ефективності блокчейн-технологій. Подальші дослідження можуть передбачати розроблення нових протоколів, визначення кращих практик у використанні та регулюванні.

Глобальне співтовариство має взяти на себе відповідальність за розроблення стандартів і регуляцій, сприяючи взаємодії та розвитку блокчейн-технологій у гармонії із сучасними вимогами. Важливо наголосити, що такі технології мають значний потенціал для захисту цифрових активів. Однак їх успіх обумовлений правильним вибором протоколу, створенням стандартів і регулювань, а також готовністю до постійного розвитку та адаптації до змін у кіберпросторі. Глобальне співтовариство, регулятори й технологічні компанії мають співпрацювати для створення безпечного та ефективного цифрового середовища, у якому блокчейн може відігравати ключову роль [18].

Висновки й перспективи подальшого розвитку

Застосування блокчейн-технологій для захисту цифрових активів є обґрунтованим та ефективним рішенням. Дослідження підтверджує важливість подальших наукових розробок і впровадження стандартів для забезпечення безпеки цифрових активів. Результати аналізу доводять високу ефективність блокчейн-технологій у захисті. Вибір певного блокчейн-протоколу залежить від конкретних вимог і потреб користувача, проте всі розглянуті протоколи (*Bitcoin*, *Ethereum*, *Hyperledger Fabric*) продемонстрували здатність

ефективно захищати цифрові активи та управляти ними. Кожен блокчейн-протокол має свої переваги та недоліки. *Bitcoin* визначається стійкістю та першоджерельністю, але обмеженою швидкістю транзакцій. Для *Ethereum* властива гнучкість та смарт-контракти, але постає питання приватності. *Hyperledger Fabric* вирізняється конфіденційністю та гнучкістю, але може вимагати складніших інтеграцій.

Упровадження стандартів і регулювань є критичним для успішної інтеграції та розвитку блокчейн-технологій. Стандарти взаємодії дають змогу підвищити сумісність різних блокчейн-протоколів і забезпечують їх ефективну спільну роботу. Регулювання важливе для забезпечення відповідності до законодавства та безпеки цифрових активів.

Дослідження наголошує на необхідності подальших наукових розробок. Розвиток нових блокчейн-протоколів, покращення сучасних технологій та визначення кращих практик використання є важливими напрямками наступних досліджень. Активна участь у глобальній науковій спільноті сприятиме еволюції блокчейн-технологій [19].

Глобальне співтовариство відіграє ключову роль у розвитку та впровадженні блокчейн-технологій. Співпраця між державами, підприємствами та науковими установами дає змогу приймати стійкі, безпечні та ефективні блокчейн-рішення [20].

Необхідно зауважити, що цифрові активи, зокрема криптовалюти та токени, стають все більш важливим елементом сучасної фінансової системи. У світі, де цифрова трансформація набуває поширення, захист цих активів стає пріоритетом і має найближчі перспективи, наприклад надійність механізмів консенсусу, оскільки блокчейн використовує різноманітні механізми: *Proof-of-Work (PoW)*, *Proof-of-Stake (PoS)* тощо. Вони забезпечують високий рівень інформації та захищають від подвійного витрачання. Смарт-контракти, що використовують блокчейн, дають змогу автоматизувати виконання угод та управляти активами, що зменшує ризики та підвищує ефективність. Децентралізована природа блокчейну робить його менш вразливим до атак і забезпечує високий рівень захисту від цензури та маніпуляцій.

Необхідно наголосити на можливості використання блокчейну в різних галузях. Зокрема це і фінансовий сектор – упровадження блокчейну в банківські операції може підвищити ефективність та захист від шахрайств. Застосування блокчейну

в ланцюгах постачання сприятиме покращенню відстеження товарів та зменшенню підробки даних. Використання блокчейну для зберігання медичної інформації може гарантувати конфіденційність і недоступність для несанкційного доступу.

Застосування блокчейн-технологій має суттєві виклики та реальні перспективи. Масштабованість – зростання обсягу транзакцій – ставить виклик перед блокчейн-мережами. Розроблення механізмів масштабування – ключовий напрям. Регулювання та легалізація – наближення блокчейн-технологій до масового використання – потребує розроблення ефективних правових механізмів. Екологічні питання – створення енергоефективних механізмів консенсусу для зменшення екологічного впливу.

Загальний висновок

Блокчейн визнаний ефективним інструментом для захисту цифрових активів. Найближчі перспективи полягають у подальшому вдосконаленні механізмів консенсусу, розвитку масштабованості та реагуванні на виклики щодо регулювання. У дослідженні подано комплексний погляд на роль блокчейну в захисті цифрових активів та визначено шляхи розвитку цієї стратегічно важливої сфери. Застосування блокчейн-технологій для захисту цифрових активів є об'єктивно обґрунтованим і практично ефективним рішенням. Успішне впровадження та розвиток цих технологій обумовлені правильним вибором протоколу, створенням стандартів, регулюванням та активною участю глобального співтовариства. Ці фактори наголошують на важливості серйозних досліджень та співпраці для створення безпечного та надійного цифрового майбутнього. Цифрові активи стають суттєвою частиною сучасного фінансового ландшафту, вимагаючи новітніх підходів до їх захисту. Блокчейн-технології – ключовий інструмент у цьому контексті, що пропонує інноваційні рішення для забезпечення безпеки та надійності цифрових активів. Інноваційність блокчейн-технологій у захисті цифрових активів визначає нові можливості для фінансової та технологічної революції. Аналіз наявних рішень та визначення перспектив показують, що сучасні виклики можуть стати стимулом для подальшого розвитку та впровадження інноваційних технологій, які покращать захист цифрових активів і розширять можливості їх застосування.

Список літератури

1. Dwivedi Y. K. et al. Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse *Information Systems Frontiers*. 2023. Vol. 25. No. 11. P. 2071–2114. DOI: <https://doi.org/10.1007/s10796-023-10400-x>
2. Hossain M. S. What do we know about cryptocurrency? Past, present, future. *China Finance Review International*. Vol. 11. No. 4. 2021. P. 552–572. DOI: <https://doi.org/10.1108/cfri-03-2020-0026>
3. Gaba S. et al. Holochain: An Agent-Centric Distributed Hash Table Security in Smart IoT Applications *IEEE Access*. 2023. Vol. 11. P. 81205–81223. DOI: <https://doi.org/10.1109/access.2023.3300220>
4. Ratna S. et al. Digital transformation in tourism and hospitality industry: a literature review of blockchain, financial technology, and knowledge management, *EuroMed Journal of Business*. 2023. DOI: <https://doi.org/10.1108/emjb-04-2023-0118>
5. Gu X. et al. Review of Privacy Enhancement Methods for Federated Learning in Healthcare Systems, *International Journal of Environmental Research and Public Health*. 2023. Vol. 20. No. 15. Art. 6539 p. DOI: <https://doi.org/10.3390/ijerph20156539>
6. W. Du et al. Blockchain technology-based sustainable management research: the status quo and a general framework for future application, *Environmental Science and Pollution Research*. 2022. Vol. 29. No. 39. P. 58648–58663. DOI: <https://doi.org/10.1007/s11356-022-21761-2>
7. Shamsuzzoha A., Marttila J., Helo P. Blockchain-enabled traceability system for the sustainable seafood industry. *Technology Analysis and Strategic Management*. 2023. DOI: <https://doi.org/10.1080/09537325.2023.2233632>
8. Tereshchenko G., Gruzdo I. Overview and Analysis of Existing Decisions of Determining the Meaning of Text Documents. 2018 *International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*. 2018. P. 645–653, Art. No. 8632014. DOI: <https://doi.org/10.1109/INFOCOMMST.2018.8632014>
9. Shubin I., Karataiev O. Reuse of information based on the interpretation of knowledge. *Innovative technologies and scientific solutions for industries*. Vol. 2 No. 24. 2023. P. 62–71. DOI: <https://doi.org/10.30837/itsi.2023.24.062>
10. Sharonova N., Kyrychenko I., Tereshchenko G. Application of big data methods in E-learning systems. *5th International Conference on Computational Linguistics and Intelligent Systems*. 2021. (COLINS-2021), 2021. CEUR-WS, Vol. 2870. P. 1302–1311. URL: <https://ceur-ws.org/Vol-2870/>
11. Kozryiev A., Shubin I. Method of planning data processing tasks in distributed systems with limited information about available resources. *Innovative technologies and scientific solutions for industries*. 2023. No. 3 (25). P. 27–39. DOI: <https://doi.org/10.30837/ITSSI.2023.25.027>
12. Joshi P. et al. Blockchain technology for sustainable development: a systematic literature review, *Journal of Global Operations and Strategic Sourcing*. 2023. Vol. 16. No. 3. P. 683–717. DOI: <https://doi.org/10.1108/jgoss-06-2022-0054>
13. Shinde et al. Securing AI-based healthcare systems using blockchain technology: A state-of-the-art systematic literature review and future research directions, *Transactions on Emerging Telecommunications Technologies*. 2024. Vol. 35. No. 1. DOI: <https://doi.org/10.1002/ett.4884>
14. Rico-Peña J.J., Arguedas-Sanz R., López-Martin C. Models used to characterise blockchain features. *A systematic literature review and bibliometric analysis*. *Technovation*. Vol. 123. 102711 p. 2023. DOI: <https://doi.org/10.1016/j.technovation.2023.102711>
15. Zhang T., Jia F., Chen L. Blockchain adoption in supply chains: implications for sustainability. *Production Planning and Control*. 2024. DOI: <https://doi.org/10.1080/09537287.2023.2296669>
16. Wasiq M. et al. Adoption and Applications of Blockchain Technology in Marketing: A Retrospective Overview and Bibliometric Analysis. *Sustainability (Switzerland)*. 2023. Vol. 15. No. 4. 3279 p. DOI: <https://doi.org/10.3390/su15043279>
17. Sheela S. et al. Navigating the Future: Blockchain's Impact on Accounting and Auditing Practices, *Sustainability*. 2023. Vol. 15. No. 24. Art. no. 16887. DOI: <https://doi.org/10.3390/su152416887>
18. A. G. Gad et al. Emerging Trends in Blockchain Technology and Applications: A Review and Outlook, *Journal of King Saud University-Computer and Information Sciences*. 2022. Vol. 34. No. 9. P. 6719–6742. DOI: <https://doi.org/10.1016/j.jksuci.2022.03.007>
19. Plastun A. et al. Persistence in the cryptocurrency market: does size matter? *Investment Management and Financial Innovations*. 2023. Vol. 20. No. 4. P. 138–146. DOI: [https://doi.org/10.21511/imfi.20\(4\).2023.12](https://doi.org/10.21511/imfi.20(4).2023.12)
20. Suslenko V. et al. Use of cryptocurrencies bitcoin and ethereum in the field of e-commerce: case study of Ukraine. *Financial and Credit Activity Problems of Theory and Practice*. 2022. Vol. 1 No. 42. P. 62–72. DOI: <https://doi.org/10.55643/fcaptop.1.42.2022.3603>

References

1. Dwivedi, Y. K. et al. (2023), "Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse", *Information Systems Frontiers*. Vol. 25. No. 11. P. 2071–2114. DOI: <https://doi.org/10.1007/s10796-023-10400-x>
2. Hossain, M. S. (2021), "What do we know about cryptocurrency? Past, present, future". *China Finance Review International*. Vol. 11. No. 4. P. 552–572. DOI: <https://doi.org/10.1108/cfri-03-2020-0026>
3. Gaba, S. et al. (2023), "Holochain: An Agent-Centric Distributed Hash Table Security in Smart IoT Applications", *IEEE Access*. 2023. Vol. 11. P. 81205–81223. DOI: <https://doi.org/10.1109/access.2023.3300220>
4. Ratna, S. et al. (2023), "Digital transformation in tourism and hospitality industry: a literature review of blockchain, financial technology, and knowledge management", *EuroMed Journal of Business*. DOI: <https://doi.org/10.1108/emjb-04-2023-0118>
5. Gu, X. et al. (2023), "Review of Privacy Enhancement Methods for Federated Learning in Healthcare Systems", *International Journal of Environmental Research and Public Health*. Vol. 20. No. 15. Art. 6539 p. DOI: <https://doi.org/10.3390/ijerph20156539>
6. Du, W. et al. (2022), "Blockchain technology-based sustainable management research: the status quo and a general framework for future application", *Environmental Science and Pollution Research*. 2022. Vol. 29. No. 39. P. 58648–58663. DOI: <https://doi.org/10.1007/s11356-022-21761-2>
7. Shamsuzzoha, A., Marttila, J., Helo, P. (2023), "Blockchain-enabled traceability system for the sustainable seafood industry". *Technology Analysis and Strategic Management*. 2023. DOI: <https://doi.org/10.1080/09537325.2023.2233632>
8. Tereshchenko, G., Gruzdo, I. (2018), "Overview and Analysis of Existing Decisions of Determining the Meaning of Text Documents". *2018 International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*. P. 645–653, Art. No. 8632014. DOI: <https://doi.org/10.1109/INFOCOMMST.2018.8632014>
9. Shubin, I., Karataiev, O. (2023), "Reuse of information based on the interpretation of knowledge". *Innovative technologies and scientific solutions for industries*. Vol. 2 No. 24. P. 62–71. DOI: <https://doi.org/10.30837/itssi.2023.24.062>
10. Sharonova, N., Kyrtychenko, I., Tereshchenko, G. (2021), "Application of big data methods in E-learning systems". *5th International Conference on Computational Linguistics and Intelligent Systems*. 2021. (COLINS-2021), CEUR-WS. Vol. 2870. P. 1302–1311. available at: <https://ceur-ws.org/Vol-2870/>
11. Kozyriev, A., Shubin, I. (2023), "Method of planning data processing tasks in distributed systems with limited information about available resources". *Innovative technologies and scientific solutions for industries*. No. 3 (25). P. 27–39. DOI: <https://doi.org/10.30837/ITSSI.2023.25.027>
12. Joshi, P. et al. (2023), "Blockchain technology for sustainable development: a systematic literature review", *Journal of Global Operations and Strategic Sourcing*. Vol. 16. No. 3. P. 683–717. DOI: <https://doi.org/10.1108/jgoss-06-2022-0054>
13. Shinde, et al. (2024), "Securing AI-based healthcare systems using blockchain technology: A state-of-the-art systematic literature review and future research directions", *Transactions on Emerging Telecommunications Technologies*. Vol. 35. No. 1. DOI: <https://doi.org/10.1002/ett.4884>
14. Rico-Peña, J.J., Arguedas-Sanz, R., López-Martin, C. (2023), "Models used to characterise blockchain features". *A systematic literature review and bibliometric analysis. Technovation*. Vol. 123. 102711 p. DOI: <https://doi.org/10.1016/j.technovation.2023.102711>
15. Zhang, T., Jia, F., Chen, L. (2024), "Blockchain adoption in supply chains: implications for sustainability". *Production Planning and Control*. DOI: <https://doi.org/10.1080/09537287.2023.2296669>
16. Wasiq, M. et al. (2023), "Adoption and Applications of Blockchain Technology in Marketing: A Retrospective Overview and Bibliometric Analysis". *Sustainability (Switzerland)*. Vol. 15. No. 4. 3279 p. DOI: <https://doi.org/10.3390/su15043279>
17. Sheela, S. et al. (2023), "Navigating the Future: Blockchain's Impact on Accounting and Auditing Practices", *Sustainability*. Vol. 15. No. 24. Art. no. 16887. DOI: <https://doi.org/10.3390/su152416887>
18. Gad, A. G. et al. (2022), "Emerging Trends in Blockchain Technology and Applications: A Review and Outlook", *Journal of King Saud University-Computer and Information Sciences*. Vol. 34. No. 9. P. 6719–6742. DOI: <https://doi.org/10.1016/j.jksuci.2022.03.007>
19. Plastun, A. et al. (2023), "Persistence in the cryptocurrency market: does size matter?", *Investment Management and Financial Innovations*. Vol. 20. No. 4. P. 138–146. DOI: [https://doi.org/10.21511/imfi.20\(4\).2023.12](https://doi.org/10.21511/imfi.20(4).2023.12)
20. Suslenko, V. et al. (2022), "Use of cryptocurrencies bitcoin and ethereum in the field of e-commerce: case study of Ukraine". *Financial and Credit Activity Problems of Theory and Practice*. Vol. 1 No. 42. P. 62–72. DOI: <https://doi.org/10.55643/fcftp.1.42.2022.3603>

Відомості про авторів / About the Authors

Терещенко Гліб Юрійович – Харківський національний університет радіоелектроніки, старший викладач кафедри програмної інженерії, Харків, Україна; e-mail: hlib.tereshchenko@nure.ua; ORCID ID: <https://orcid.org/0000-0001-8731-2135>

Кириченко Ірина Віталіївна – кандидат технічних наук, Харківський національний університет радіоелектроніки, доцент кафедри програмної інженерії, Харків, Україна; e-mail: iryna.kyrychenko@nure.ua; ORCID ID: <https://orcid.org/0000-0002-7686-6439>

Tereshchenko Glib – Kharkiv National University of Radio Electronics, Senior Lecturer at the Department of Software Engineering, Kharkiv, Ukraine.

Kyrychenko Iryna – PhD (Engineering Sciences), Kharkiv National University of Radio Electronics, Associate Professor at the Department of Software Engineering, Kharkiv, Ukraine.

ANALYSIS AND JUSTIFICATION OF THE USE OF EXISTING BLOCKCHAIN SOLUTIONS FOR THE PROTECTION OF DIGITAL ASSETS

The **subject** of this article is consideration of modern blockchain solutions and their potential use in the context of digital asset protection. Various aspects of blockchain technology are explored, including consensus mechanisms, security levels, and functionality. The **goal** of the work is a systematic analysis and justification of the application of various blockchain solutions for the protection of digital assets. The article is aimed at determining the effectiveness and feasibility of using specific blockchain protocols and their functional elements to ensure the safety, reliability, and integrity of digital assets. The following **tasks** were solved in the article: consideration of modern blockchain technologies and consideration of their role in ensuring the security of digital assets. Conducting a detailed analysis of popular blockchain protocols, including Bitcoin, Ethereum, and Hyperledger Fabric, with a focus on their security against various types of cyber threats and attacks. The following **methods** are used: analysis of blockchain protocols, expert evaluations of the effectiveness of protection of digital assets, and study of the technical features of each solution. The following **results** were obtained: clearly defined advantages and disadvantages of each protocol were obtained, taking into account their applicability in the field of digital assets in various fields of application, such as semantic analysis of texts, E-Learning, Big Data, DDP-systems, finance, etc. In addition, the issue of network privacy in the context of information protection was investigated and justifies the choice of the optimal blockchain solution for a specific use. **Conclusions:** The article provides readers with an overview of how to effectively use blockchain to ensure the reliability and security of digital assets in a variety of usage scenarios. In today's digital world, where the value of digital assets is growing exponentially, protecting them from cyber threats becomes a critical task. Blockchain technologies, originally developed for cryptocurrencies, have gained recognition as an effective tool in the field of cyber security. The importance of standardization and regulation in the field of blockchain technologies to ensure their effective integration and compliance with the requirements of the law is put forward.

Keywords: blockchain; cyber security; digital assets; anonymity; confidentiality; speed of transactions; standardization; regulation.

Бібліографічні описи / Bibliographic descriptions

Терещенко Г. Ю., Кириченко І. В. Аналіз і обґрунтування використання наявних блокчейн-рішень для захисту цифрових активів. *Сучасний стан наукових досліджень та технологій в промисловості*. 2024. № 1 (27). С. 164–178. DOI: <https://doi.org/10.30837/ITSSI.2024.27.164>

Tereshchenko, G., Kyrychenko, I. (2024), "Analysis and justification of the use of existing blockchain solutions for the protection of digital assets", *Innovative Technologies and Scientific Solutions for Industries*, No. 1 (27), P. 164–178. DOI: <https://doi.org/10.30837/ITSSI.2024.27.164>