DOI: 10.20998/2079-0023.2024.01.17
УДК 004.82

Г. Ю. ТЕРЕЩЕНКО, старший викладач кафедри програмної інженерії, Харківський національний університет радіоелектроніки; м. Харків, Україна; e-mail: hlib.tereshchenko@nure.ua; ORCID: https://orcid.org/0000-0001-8731-2135
Є. М. ПИСАРЕНКО, Харківський національний університет радіоелектроніки, бакалавр кафедри програмної інженерії; м. Харків, Україна, e-mail: yelyzaveta.pysarenko@nure.ua; ORCID ID: https://orcid.org/0009-0009-6534-2558

АНАЛІЗ ТИПІВ БЛОКЧЕЙНІВ ТА ЇХ ПРИДАТНОСТІ ДЛЯ СХОВИЩ ЗОБРАЖЕНЬ

Досліджено різні типи блокчейнів та їх можливе використання для створення сховища зображень. Метою дослідження було оцінити переваги та обмеження різних типів блокчейнів з точки зору зберігання зображень. Застосовано методи обробки даних для аналізу технічних характеристик різних типів блокчейнів та порівняльного аналізу параметрів ефективності та надійності. Отримано результати, які дозволили сформулювати принципи вибору типу блокчейну для створення сховища зображень та ідентифікувати переваги та обмеження кожного типу з точки зору зберігання зображень у залежності від пріоритетів програмного продукту. Висновок полягає в тому, що використання блокчейну забезпечує високий рівень безпеки та цілісності зображень, деякі типи блокчейнів проявляють високу швидкість та масштабованість. Проте, важливо розуміти, що процес збереження може залишатися централізованим, тому потрібно проводити додаткові дослідження для оптимального використання та розвитку цих технологій. Майбутні дослідження можуть включати аналіз можливостей забезпечення конфіденційності учасників та розвитку стандартів для обміну мультимедійним контентом через блокчейн. Важливо враховувати, що використання блокчейну може сприяти підвищенню прозорості та довіри у процесі зберігання та обміну мультимедійним контентом, що є важливим для розвитку цифрової економіки. Однак для досягнення повного потенціалу блокчейну у сфері мультимедіа, необхідно розробляти ефективні стратегії для вирішення проблем конфіденційності, масштабованості та централізації, що виникають при впровадженні цих технологій. Такий комплексний підхід дозволить забезпечити стабільну та ефективну інфраструктуру для управління мультимедійним контентом у цифровому середовищі.

Ключові слова: блокчейн, сховище, зображення, транзакції, водяні знаки, DRM, конфіденційність.

Вступ. У сучасному цифровому світі, де обсяги даних стрімко зростають, а конфіденційність та безпека є критичними аспектами, дослідження та розробка ефективних методів захисту цифрових активів набувають особливого значення. Одним з ключових аспектів цього процесу є збереження зображень, які мають велике значення в таких галузях, як медицина, наука, промисловість та мистецтво.

З огляду на постійний розвиток цифрової технології та зростаючі вимоги до захисту конфіденційності та цілісності даних, вивчення можливостей блокчейну для збереження зображень є актуальною і перспективною областю досліджень. Надійне збереження цифрових зображень, зокрема, вимагає не лише ефективного забезпечення конфіденційності та безпеки, але й гарантії невідхильності та незмінності відображення оригінальної інформації [12].

Актуальність проблеми полягає в тому, що зображення зазнають ризику порушення конфіденційності та несанкціонованого доступу через підключення до відкритих мереж та вразливості наявних систем зберігання. Тому розробка надійних інструментів для збереження та захисту зображень має велике практичне значення.

У останні роки блокчейн-технології набули широкого застосування в різних галузях, включаючи фінанси, логістику, медицину та мистецтво. Однак до цього часу дослідження, спрямовані на аналіз придатності різних типів блокчейнів для сховищ зображень, є обмеженими.

Існуючі методи розв'язання задачі: Сьогодні розповсюдження контенту стає все більш актуальною та складною задачею. Традиційні методи доставки мультимедійного контенту, які базувалися на фізичних носіях, застарівають, а нові технології Інтернету вимагають нових підходів до розповсюдження контенту [9]. Однією з поточних проблем є забезпечення безпеки та цілісності мультимедійного контенту під час його розповсюдження через мережу Інтернет.

Для захисту авторських прав і цілісності збережених даних важливо мати систему, яка може ефективно відстежувати та підтверджувати походження контенту. Деякі існуючі методи захисту авторських прав, такі як шифрування, управління цифровими правами (DRM) та водяні знаки, вже застосовуються для цієї мети. Однак, існують проблеми, пов'язані з цими методами, такі як складність у реалізації, неодноразовість атак та залежність від централізованих структур [9].

Технологія блокчейн, відома своєю децентралізованістю та надійністю, може вирішити деякі з цих проблем. Блокчейн є розподіленим цифровим реєстром, який забезпечує незмінність та перевірку транзакцій. Він може бути використаний для створення системи, яка забезпечує надійність та невідкладність відстеження авторства мультимедійного контенту.

Ця стаття має на меті доповнити цілісний огляд застосування технології блокчейн для захисту авторських прав у сфері мультимедіа.

Аналіз. Останнім часом як промисловість, так і наукові кола, почали розглядати можливість збереження прав інтелектуальної власності з використанням технологій блокчейну. У статті представлений стислий огляд наявних систем захисту контенту на основі блокчейну із зазначенням їх основних атрибутів і деталей реалізації.

У дослідженні [1] запропоновано створення структури на основі блокчейна, що забезпечує

виконання авторських прав на мультимедійні об'єкти через смарт-контракти. Система використовує автономне централізоване рішення для зберігання даних, озеро даних, для реєстрації транзакцій всіх даних, що додані до блокчейну. Інформація у озері даних зашифрована та підписана цифровим підписом, що забезпечує конфіденційність та достовірність. Доступ до збережених даних можуть отримати лише авторизовані користувачі після перевірки їх цифрових підписів та прав доступу з погодженням більшості вузлів.

У роботі Пена та ін. [2] пропонується система управління цифровими авторськими правами на базі Ethereum, що дозволяє власникам контенту та клієнтам працювати безпосередньо, без централізованого посередника. У системі використовуються цифрові водяні знаки, криптосистема Ель-Гамаля, перцептивна хеш-функція, смарт-контракт та IPFS. Однак ця схема потребує великих витрат пам'яті та часу ЦП через використання шифрування Ель-Гамаля для шифрування всього мультимедійного контенту.

У дослідженні [3] пропонується схема DRM на основі блокчейна для захисту авторських прав на проєктні роботи. Система включає два методи: захист авторських прав і торгівлю. Метод захисту авторських прав реєструє права, запитує інформацію та перевіряє кореляцію, тоді як процес торгівлі включає захист дизайнерського контенту та підтвердження доставки для забезпечення справедливої торгівлі. Зареєстрований покупець може придбати зареєстровані роботи у постачальників контенту (продавців) за допомогою смарт-контрактів. Під час доставки контент шифрується відкритим ключем покупця, а потім доставляється через додаток. Перед отриманням контенту покупець повинен ввести свій секретний ключ у додаток, який розшифровує дані та надає доступ. Однак запропонована схема не гарантує безпеку секретного ключа користувача, який передається до додатка для підпису та розшифрування контенту.

У статті [4] пропонується мультимедійна блокчейн-платформа на основі водяних знаків, захищена від втручання, яка забезпечує безпеку та цілісність розповсюдженого зображення. Запропонована модель блокчейну базується на алгоритмі самовбудовування водяних знаків на основі стисненого зондування (CS), у якому унікальна інформація водяного знака складається з криптографічного хешу та хешу зображення. Криптографічний хеш складається з історії транзакцій для отримання метаданих мультимедійного вмісту з мультимедійного блокчейну, тоді як хеш зображення використовується для збереження оригінального мультимедійного вмісту, який можна отримати.

Криптографічний хеш можна використовувати для отримання інформації мультимедійного вмісту (наприклад, права власності або історії модифікацій), яка зберігається в мультимедійному блокчейні, а хеш зображення можна використовувати для ідентифікації підроблених областей. Зразки CS можуть бути використані для реконструкції оригінального зображення та визначення місцезнаходження пошкоджених областей. У блокчейні транзакція складається з інформації про транзакцію зображення, що містить ідентифікатор транзакції та інформації зразків CS. Після схвалення транзакції вузлами перевірки зображення розповсюджується, а потім зберігається на сервері медіабази даних. Хоча зберігання інформації про перевірку зображення в блокчейні є вигідною стратегією, зображення все одно зберігається централізовано або зберігається власником, що впливає на доступність керування зображеннями.

У [5] технологія блокчейну використовується для безпечного зберігання водяних знаків та забезпечення автентифікації за часовою міткою для кількох водяних знаків. Запропонована система використовує перцептивну хеш-функцію для обчислення хеш-значення зображення, технологію блокчейну для запису метаданих, пов'язаних із інформацією про авторські права, QR-код для створення водяного знака, алгоритм цифрових водяних знаків для вбудовування інформації про авторські права, криптографічну хеш-функцію для обчислення хеш-значень як вихідних зображень, так і зображень з водяними знаками, а також мережу IPFS для зберігання, керування та поширення зображень з водяними знаками та пов'язаною інформацією про авторські права. Однак запропонована схема забезпечує перевірку концепції керування авторськими правами лише на цифрові зображення.

Ву та ін. [6] запропонував систему торгівлі даними на основі блокчейну та смарт-контрактів із функціями відстеження даних і виявлення незаконної поведінки. Він забезпечує два торгові сценарії із захистом конфіденційності від будь-якої неавторизованої сторони, включаючи торгову платформу. Ефективний метод відбитків пальців призначений для виявлення зміненого зображення, таким чином захищаючи авторські права на дані. Генератор відбитків даних призначений для створення відбитків пальців шляхом об'єднання кількох векторів ознак, отриманих із даних. Виявивши незаконно розповсюджену копію, генератор відбитків даних витягує ідентифікований вектор, який потім порівнюється з відбитками, записаними в усіх чинних контрактах. Згенерований відбиток пальця стійкий до незначних змін даних, таких як кадрування, додавання шуму та зміна яскравості. Однак система не задовольняє параметри конфіденційності та безпеки анонімного протоколу зняття відбитків пальців у децентралізованому середовищі.

У посиланні [7] автори пропонують систему розподілу контенту P2P, що базується на технології блокчейн. Запропонована система використовує стійку до змови дактилоскопію (для забезпечення стійкості до змови), гомоморфні та симетричні схеми шифрування (для захисту контенту та конфіденційності даних), перцептивну хеш-функцію (для автентифікації контенту), смарт-контракт на основі Ethereum (для виконання атомарних платежів та підтвердження доставки) та мережу IPFS (для зберігання мультимедійного контенту). Хоча запропонована система враховує властивості конфіденційності та безпеки анонімного протоколу зняття відбитків пальців у розподіленому середовищі, це лише доказ концепції, яка не була реалізована та оцінена у реальному світі.

У посиланні [8] Лі пропонує нову схему хаотичного шифрування зображень, засновану на блокчейні, пов'язану з відбитками пальців, яка забезпечує автентифікацію, відстежування та стійкість до атак безпеки (наприклад, атаки з використанням вибраного відкритого тексту або підробки). У цій схемі відбитки пальців розповсюджувачів контенту, вбудовані в зашифровані зображення, кодуються стійкими до змови кодами Тардоса для запису декількох відбитків пальців з фіксованою довжиною даних та забезпечення можливості відстежування. Перед розповсюдженням контенту в вихідне зображення вбудовується підпис відправника та відбитки пальців всіх розповсюджувачів системи з використанням оборотної схеми водяних знаків та хаотичної карти. Потім це зображення з відбитками пальців шифрується з використанням структури Фрідріха, яка складається з заміни, перестановки та дифузії. Відбиток пальця, ключ приховування даних та ключ шифрування записуються в блокчейн. На стороні отримувача при розшифруванні отримується зображення відбитка пальця, що містить підпис відправника та всі відбитки пальців вищих розповсюджувачів (об'єднаний відбиток пальця), які можна видобути індивідуально, а потім порівняти з записаною інформацією в блокчейні для перевірки. Хоча система забезпечує стійкість до змови, цілісність даних та захист авторських прав, вона не задовольняє всім властивостям конфіденційності та безпеки анонімного протоколу зняття відбитків пальців у децентралізованому середовищі.

У табл. 1 представлено порівняння схем щодо типів блокчейну, типів транзакцій, автоматизації даних, криптовалюти, протоколів консенсусу та методів захисту вмісту. Таблиця 1 пронумерована відповідно до списку використаної літератури.

Одна з вибраних схем використовує приватний блокчейн, що передбачає контрольний рівень поверх блокчейну, яким керує довірений орган, який відповідає за дозвіл на виконання дій дозволеними системними об'єктами. Кілька інших схем використовують блокчейн консорціуму, як розподілену книгу для збереження контролю та конфіденційності, одночасно скорочуючи витрати та збільшуючи швидкість транзакцій.

Більшість схем використовують гібридні транзакції, які передбачають запис даних у ланцюжку в приватній або загальнодоступній службі блокчейну, наприклад як метадані вмісту, інформація про власників авторських прав або користувачів, водяний знак або відбиток пальця користувача (у зашифрованому вигляді), ліцензія DRM і зобов'язання щодо вмісту, серед іншого, а також механізми поза мережею, такі як створення та зберігання захищеного авторським правом вмісту, вилучення інформації про авторські права з вмісту або протоколу відстеження. Транзакції в ланцюжку виконуються для досягнення прозорості, безпеки, незмінності та можливості перевірки, і вважаються найкращими для переказів криптовалюти в повністю децентралізований спосіб. Механізми поза мережею дозволяють владі заощадити витрати на мережу, оскільки вони не мають комісії за транзакцію. Крім того, ці механізми досить швидкі, оскільки вони не пов'язані обмеженнями швидкості транзакцій, пов'язаними з транзакціями в ланцюжку.

Більшість схем гарантують захист вмісту за допомогою використання цифрових водяних знаків як окремого механізму або в поєднанні з DRM або шифруванням [9].

Можна помітити, що більшість систем забезпечують цілісність даних і захист від комунікаційних атак. З погляду захисту від несанкціонованого доступу ми можемо спостерігати, що багато систем гарантують захист від несанкціонованого доступу. Це цілком очікувано, оскільки ця властивість забезпечується технологією блокчейн. Можна помітити, що менше схем стосуються конфіденційності даних, відстеження, автентичності та умовного доступу. З точки зору захисту від атак, лише кілька схем стійкі до загальної обробки сигналів і атак змови/коаліції. З огляду на толерантність якості, ми помітили, що прозорість захищеного авторським правом вмісту (з водяними знаками/відбитками пальців) оцінюється значно меншою кількістю схем.

Дискусії. Зашифрований контент безпечний настільки, наскільки безпечним є ключ, використаний для його шифрування. Таким чином, криптографічними ключами необхідно ретельно керувати (наприклад,

Таблиця 1 – Порівняння схем захисту авторських прав на основі блокчейну з посиланням на таксономію [9]

Номер	Типи контенту	Типи блокчейну	Типи транзакцій	Автоматизація даних	Криптовалюта	Методи захисту контенту
1	Зображення	Публічний	Гібридний	dApp	Ефіріум	Шифрування
2	Зображення	Публічний	Гібридний	dApp	Ефіріум	Шифрування і водяний знак
3	Зображення	Консорціум	Ончейн	dApp	Ефіріум	DRM
4	Зображення	Консорціум	Ончейн	Смарт-контракт	Ефіріум	Водяний знак
5	Зображення	Приватний	Гібридний	dApp	Не вказана	Водяний знак
6	Зображення	Гібридний	Гібридний	dApp	Не вказана	Відбитки пальців
7	Зображення, аудіо, відео	Публічний	Гібридний	Смарт-контракт	Ефіріум	Відбитки пальців
8	Зображення	Консорціум	Ончейн	Смарт-контракт	Не вказана	Шифрування і відбитки пальців

передавати, зберігати або оновлювати), щоб гарантувати, що дані залишаються захищеними, але при необхідності доступними для декількох користувачів системи.

Методи шифрування не можуть запобігти несанкціонованому використанню та незаконному розповсюдженню контенту користувачем після розшифрування отриманого контенту.

Споживачі можуть шукати альтернативні варіанти отримання контенту, такі як програми для обміну файлами P2P. Проте, щоб забезпечити сумісність систем DRM, постачальникам контенту або виробникам мультимедійних програвачів, необхідно знати конфіденційну інформацію, пов'язану зі схемою захисту DRM, що збільшує ризик витоку. У такому разі один витік (або «злом») може поставити під загрозу не лише один із кількох каналів розповсюдження, а й розповсюдження всього сумісного контенту з DRM.

Системи DRM можуть викликати низку юридичних проблем, якщо їх неправильно використовувати, наприклад, використання інструментів моніторингу, навмисне і ненавмисне, для звітності та збору даних щодо звичок та переваг їх споживачів (наприклад, типу контенту, який вони використовують). Це може призвести до серйозних наслідків конфіденційності, наприклад, використання цих даних з метою їх продажу третім особам.

З боку фахівця з впровадження у схемі цифрових водяних знаків підтримання відповідного балансу між властивостями надійності, ємності та непомітності є складним завданням, оскільки ці властивості суперечать одна одній, тобто. якщо одне збільшується, інше зменшується.

Чим складніша схема нанесення водяних знаків, тим вищі витрати, пов'язані з процесами впровадження та виявлення. Витрати, пов'язані з використанням та виявленням водяних знаків, повинні бути мінімальними, щоб відповідати вимогам реального часу.

У схемах цифрового зняття відбитків пальців, заснованих на кодах, стійких до змови, існує компроміс [10] між розміром бази користувача N і стійкістю до змови, $c0$ і довжиною кодового слова m. Зі збільшенням N або $c0$, довжина m збільшується і навпаки. Цей компроміс може зробити код, що відстежується, непрактичним, оскільки багатьом додаткам потрібна велика база користувачів і стійкість до змови. Однак ці вимоги призведуть до створення довгих кодів, що відстежуються.

Більшість досліджень, пов'язаних з протоколами анонімного зняття відбитків пальців, припускають наявність довіреної третьої сторони, яка відповідає за створення відбитків пальців та відстеження порушників авторських прав. Ця довіра передбачає впевненість користувача в тому, що довірений об'єкт поводитиметься очікуваним чином, щоб забезпечити безпеку та анонімність. У деяких інших схемах, у яких уникає використання такої сторони, обчислювальні та комунікаційні витрати досить високі через використання принаймні однієї з таких вимогливих технологій: гомоморфне шифрування, фіксація бітів або безпечні багатосторонні обчислення.

Блокчейн страждає від проблеми масштабованості через обмежений розмір блоку, наприклад, Біткойн може досягати 7 транзакцій в секунду через те, що протокол Біткойн обмежує розмір блоку до 1 МБ. Можливим вирішенням цієї проблеми є збільшення розміру блоку, але це створює навантаження на безпеку через те, що збільшення ймовірності появи втрачених блоків явно вплине на пропускну здатність та витрати на перевірку. Чим вище межа розміру блоку, тим більше транзакційне навантаження, перевантаження блокчейна та затримки транзакцій. Отже, зниження комісії за транзакцію призведе до зниження безпеки. Таким чином, компроміс між безпекою, масштабованістю та децентралізацією є проблемою при розробці блокчейну.

Блокчейни без дозволів встановлюють, що записані дані доступні, і таким чином забезпечують публічний доступ до них усім учасникам. Однак це може поставити під загрозу конфіденційність даних. Більше того, якщо конфіденційні дані були помилково завантажені в публічний блокчейн, виправити шкоду неможливо.

Коди смарт-контрактів схильні до помилок через людську помилку або неповну інформацію. Більш того, самовиконуваний характер смарт-контрактів має на увазі меншу гнучкість для реалізації фактичних намірів сторін.

Мова програмування для реалізації смарт-контрактів – це постійна сфера досліджень. У даний час найбільш використовуваною об'єктно-орієнтованою мовою високого рівня для реалізації складних смарт-контрактів у Ethereum є Solidity, яка все ще розвивається та має ряд обмежень, таких як відсутність бібліотек загального призначення, перевірка типів та підтримка багатопотоковості, між іншим. Інші популярні мови програмування (Python, C++, Java) також використовують для написання смарт-контрактів. Однак зробити програми читабельними у кожній формі залишається непростим завданням. У випадку з Біткойном мова сценаріїв для написання простого коду не є повною за Тьюрингом і не підтримує всі можливі структури програмування, зокрема цикли.

Блокчейн може постраждати від атак, коли деякі вузли можуть отримати більшість у мережі та зловживати ним, наприклад, вони можуть скасувати транзакції, щоб виконати подвійне витрачання та перешкоджати іншим майнерам підтвердити блоки.

Конфіденційність користувача може бути порушена всередині блокчейна, наприклад, можна відстежити реальну IP-адресу користувача, історію транзакцій можна пов'язати, щоб розкрити його справжню особистість або можливість зв'язку через його підключений набір вузлів.

Блокчейну не вистачає сумісності через відсутність універсальних стандартів. Існуючі мережі блокчейнів мають власні параметри, такі як моделі консенсусу, схеми транзакцій, криптовалюта і функціональність смарт-контрактів. Більше того, невизначеність та спекулятивний характер криптовалюти, як і раніше, перешкоджають її широкому поширенню.

Усі типи атак – внутрішні та зовнішні – мають бути прийняті до уваги, щоб оцінити безпеку та надійність нових чи наявних схем нанесення водяних знаків та зняття відбитків пальців.

Багато програм захисту авторських прав на основі блокчейна фокусуються виключно на перевагах технології, залишаючи осторонь деталі їх реалізації. Тому важливо розробити практичну структуру на основі блокчейну, яка повинна враховувати як технічні деталі, так і деталі впровадження, такі як оцінка переваг і недоліків систем із дозволами та без дозволів перед вибором одного з цих рішень, вибір відповідного механізму консенсусу залежить від вимог (наприклад, пропускна спроможність транзакцій, затримка, мінімальна комісія за транзакції, централізація/децентралізація та безпека) та оцінка ефективності за допомогою впровадження структури для розрахунку обчислювальної вартості та загального часу відповіді.

Визнані технологічні стандарти встановлюють специфікації та процедури, які є вигідними з точки зору забезпечення ефективності, надійності та підвищеної безпеки. Завдяки цій статті можна зробити висновок, що існує потреба в універсальному стандарті, якому могли б дотримуватися постачальники мультимедійного контенту, виробники та компанії, що беруть участь, щоб ділитися новими рішеннями щодо захисту авторських прав на основі блокчейну, а також інтегрувати їх з існуючими. системи. Аналогічним чином, цей стандарт повинен дозволяти автоматичну конвертацію між різними криптовалютами для поліпшення досвіду користувача.

Майбутні дослідження повинні вивчити можливі рішення з урахуванням конфіденційності, які могли б захистити конфіденційність суб'єктів (власника контенту, покупця тощо), які беруть участь у транзакціях додатків для захисту контенту на основі блокчейну. Вимоги конфіденційності та безпеки повинні бути визначені на початковому етапі цих схем, оскільки дані (наприклад, інформація, що стосується власника контенту, відкриті ключі учасників, псевдоніми та інформація про авторські права, серед іншого) видно всі в мережі [11].

Усі можливі атаки на безпеку та конфіденційність (наприклад, підслуховування, DDoS-атака або видача себе за іншу особу) на смарт-контракт мають аналізувати за допомогою формального аналізу безпеки. До того, транзакції смарт-контрактів мають бути технічно оборотними, щоб довести їхню довгострокову ефективність. Крім того, щоб змінити або скасувати смарт-контракт, у коді має бути передбачена подія, що ініціює модифікацію та її припинення/розширення. Таким чином, проблема боротьби з атаками на безпеку та конфіденційність смарт-контракту потребує подальшого вивчення [12].

Висновки. Після аналізу типів блокчейнів та їх придатності для сховищ зображень на основі наданої інформації, можна зробити наступні висновки та зазначити перспективи дослідження.

Розглянута широка гама технологій блокчейну, що використовуються для захисту мультимедійного контенту, свідчить про їхню різноманітність у перевагах та обмеженнях. Вибір конкретного типу блокчейну може залежати від потреб та вимог конкретної системи. Використання блокчейну, особливо з водяними знаками та криптографічними хешами, забезпечує високий рівень безпеки та цілісності зображень. Механізми ідентифікації та відновлення контенту покращують відстежування та виявлення фальсифікацій. Деякі типи блокчейнів проявляють високу швидкість транзакцій та масштабованість, що робить їх привабливими для розгляду як рішення для сховищ зображень. Важливо розуміти, що, незважаючи на безпеку та недоступність для модифікації даних, процес збереження зображень може залишатися централізованим, що впливає на доступність та контроль над контентом.

Перспективи дослідження: Можливості дослідження включають оцінку ефективності та пропускної здатності різних схем блокчейну, розробку нових методів виявлення фальсифікацій та вдосконалення процесів збереження та обміну мультимедійним контентом через блокчейн.

Загалом, дослідження підтверджує потенціал блокчейну як ефективного інструменту для захисту та управління мультимедійним контентом. Однак потрібно проводити додаткові дослідження для розуміння оптимальних стратегій використання та розвитку цих технологій для сховищ зображень.

Список використаної літератури

1. Vishwa A., Hussain F. K. *A Blockchain based approach for multimedia privacy protection and provenance*. URL: http://doi.org/doi.org/10.1109/ssci.2018.8628636 (access date: 16.02.2024).
2. Peng W. et al. *Secure and Traceable Copyright Management System Based on Blockchain*. URL: http://doi.org/doi.org/10.1109/iccc47050.2019.9064101 (access date: 16.02.2024).
3. Lu Z. et al. *Blockchain for Digital Rights Management of Design Works*. URL: http://doi.org/doi.org/10.1109/icsess47205.2019.9040744 (access date: 16.02.2024).
4. Bhowmik D., Feng T. *The multimedia blockchain: A distributed and tamper-proof media transaction framework*. URL: http://doi.org/doi.org/10.1109/icdsp.2017.8096051 (access date: 16.02.2024).
5. Meng Z. et al. *Design Scheme of Copyright Management System Based on Digital Watermarking and Blockchain*. URL: http://doi.org/doi.org/10.1109/compsac.2018.10258 (access date: 16.02.2024).
6. Wu Z. et al. *Privacy-Friendly Blockchain Based Data Trading and Tracking*. URL: http://doi.org/doi.org/10.1109/bigcom.2019.00040 (access date: 16.02.2024).
7. Qureshi A., Megias D. *Blockchain-based P2P multimedia content distribution using collusion-resistant fingerprinting*. URL: http://doi.org/doi.org/10.1109/apsipaasc47483.2019.9023054 (access date: 16.02.2024).
8. Li R. *Fingerprint-related chaotic image encryption scheme based on blockchain framework*. URL: http://doi.org/doi.org/10.1007/s11042-020-08802-z (access date: 16.02.2024).
9. Qureshi A., Megías Jiménez D. *Blockchain-Based Multimedia Content Protection: Review and Open Challenges*. URL: http://doi.org/doi.org/10.3390/app11010001 (access date: 16.02.2024).
10. Qureshi A., Megías D., Rifà-Pous H. *Framework for preserving security and privacy in peer-to-peer content distribution systems*. URL: http://doi.org/doi.org/10.1016/j.eswa.2014.08.053 (access date: 07.03.2024).
11. Kyrychenko I., Tereshchenko G. *Using blockchain technology in international business relationships*. URL: https://nure.ua/wp-

content/uploads/workshop/konferentsiia-aktualni-problemy-ekonomichnoi-kibernetyky-ta-ekonomichnoi-bezpeky-.pdf (access date: 07.03.2024).
12. Tereshchenko G. Y., Kyrychenko I. V., Bilous N. V. *Copyright protection using Blockchain*. URL: http://doi.org/10.30837/bi.2019.1(92).09 (access date: 16.02.2024).

References (transliterated)

1. Vishwa A., Hussain F. K. *A Blockchain based approach for multimedia privacy protection and provenance*. Available at: http://doi.org/doi.org/10.1109/ssci.2018.8628636 (accessed 16.02.2024).
2. Peng W. et al. *Secure and Traceable Copyright Management System Based on Blockchain*. Available at: http://doi.org/doi.org/10.1109/iccc47050.2019.9064101 (accessed 16.02.2024).
3. Lu Z. et al. *Blockchain for Digital Rights Management of Design Works*. Available at: http://doi.org/doi.org/10.1109/icsess47205.2019.9040744 (accessed 16.02.2024).
4. Bhowmik D., Feng T. *The multimedia blockchain: A distributed and tamper-proof media transaction framework*. Available at: http://doi.org/doi.org/10.1109/icdsp.2017.8096051 (accessed 16.02.2024).
5. Meng Z. et al. *Design Scheme of Copyright Management System Based on Digital Watermarking and Blockchain*. Available at: http://doi.org/doi.org/10.1109/compsac.2018.10258 (accessed 16.02.2024).
6. Wu Z. et al. *Privacy-Friendly Blockchain Based Data Trading and Tracking*. Available at: http://doi.org/doi.org/10.1109/bigcom.2019.00040 (accessed 16.02.2024).
7. Qureshi A., Megias D. *Blockchain-based P2P multimedia content distribution using collusion-resistant fingerprinting*. Available at: http://doi.org/doi.org/10.1109/apsipaasc47483.2019.9023054 (accessed 16.02.2024).
8. Li R. *Fingerprint-related chaotic image encryption scheme based on blockchain framework*. Available at: http://doi.org/doi.org/10.1007/s11042-020-08802-z (accessed 16.02.2024).
9. Qureshi A., Megías Jiménez D. *Blockchain-Based Multimedia Content Protection: Review and Open Challenges*. Available at: http://doi.org/doi.org/10.3390/app11010001 (accessed 16.02.2024).
10. Qureshi A., Megías D., Rifà-Pous H. *Framework for preserving security and privacy in peer-to-peer content distribution systems*. Available at: http://doi.org/doi.org/10.1016/j.eswa.2014.08.053 (accessed 07.03.2024).
11. Kyrychenko I., Tereshchenko G. *Using blockchain technology in international business relationships*. Available at: https://nure.ua/wp-content/uploads/workshop/konferentsiia-aktualni-problemy-ekonomichnoi-kibernetyky-ta-ekonomichnoi-bezpeky-.pdf (accessed 07.03.2024).
12. Tereshchenko G. Y., Kyrychenko I. V., Bilous N. V. *Copyright protection using Blockchain*. Available at: http://doi.org/10.30837/bi.2019.1(92).09 (accessed 16.02.2024).

Надійшла (received) 17.05.2024

UDC 004.82

H. Y. TERESHCHENKO, Senior Lecturer of the Department of Software Engineering, Kharkiv National University of Radio Electronics; Kharkiv, Ukraine; e-mail: hlib.tereshchenko@nure.ua; ORCID: https://orcid.org/0000-0001-8731-2135
E. M. PYSARENKO, Kharkiv National University of Radio Electronics, Bachelor of Software Engineering Department; Kharkiv, Ukraine; e-mail: yelyzaveta.pysarenko@nure.ua; ORCID ID: https://orcid.org/0009-0009-6534-2558

ANALYSIS OF BLOCKCHAIN TYPES AND THEIR SUITABILITY FOR IMAGE STORAGE

There different types of blockchains and their possible use for creating an image repository are investigated. The purpose of the study was to evaluate the advantages and limitations of different types of blockchains in terms of image storage. Data processing methods were applied to analyze the technical characteristics of various types of blockchains and comparative analysis of efficiency and reliability parameters. The results were obtained, which made it possible to formulate the principles of choosing the type of blockchain for creating image storage and to identify the advantages and limitations of each type from the point of view of image storage, depending on the priorities of the software product. The conclusion is that the use of blockchain provides a high level of security and integrity of images, some types of blockchains exhibit high speed and scalability. However, it is important to understand that the preservation process may remain centralized, so more research is needed to optimally use and develop these technologies. Future research may include an analysis of the possibilities of ensuring the privacy of participants and the development of standards for the sharing of multimedia content via blockchain. It is important to consider that the use of blockchain can contribute to increasing transparency and trust in the process of storing and sharing multimedia content, which is important for the development of the digital economy. However, in order to achieve the full potential of blockchain in the field of multimedia, it is necessary to develop effective strategies to solve the problems of privacy, scalability and centralization that arise when implementing these technologies. Such a comprehensive approach will provide a stable and effective infrastructure for managing multimedia content in the digital environment.

Keywords: blockchain, storage, images, transactions, watermarks, DRM, privacy.

Повні імена авторів / Author's full names

Автор 1 / Author 1: Терещенко Гліб Юрійович / Tereshchenko Glib
Автор 2 / Author 2: Писаренко Єлизавета Михайлівна / Pysarenko Yelyzaveta

ЗМІСТ