

СЕКЦІЯ XIII. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ

DOI 10.62731/mcnd-15.03.2024.003

АНАЛІЗ ТИПІВ БЛОКЧЕЙНІВ ТА ЇХ ПРИДАТНОСТІ ДЛЯ СХОВИЩ ЗОБРАЖЕНЬ

Терещенко Гліб Юрійович

ORCID ID: 0000-0001-8731-2135

Старший викладач кафедри програмної інженерії
Харківський національний університет радіоелектроніки, Україна

Крупеня Олександр Володимирович

здобувач вищої освіти факультету комп'ютерних наук
Харківський національний університет радіоелектроніки, Україна

Сьогодні ми живемо в час Big Data [1], коли інформацію про нас безперервно накопичують та аналізують корпорації та державні установи, які використовують ці дані для надання послуг, удосконалення процесів прийняття рішень, прогнозування майбутніх тенденцій та досягнення різноманітних інших цілей. Безсумнівно, дані є цінним активом в економіці, що сприяє інноваціям та зростанню.

Незважаючи на переваги суспільства, заснованого на даних, зростає загальна тривога щодо приватності користувачів. Централізовані сутності, будь то публічні чи приватні, накопичують великі обсяги особистих та чутливих даних. Користувачі не мають майже ніякого контролю над інформацією, яка збирається про них та її подальшим використанням.

Користувачі не повинні довіряти чутливу інформацію, а також особисті дані взагалі, в руки третіх сторін, бо це створює ризики можливих атак та зловживань. Замість цього, користувачам слід володіти своїми даними та контролювати їх самостійно, забезпечуючи безпеку без обмеження можливостей компаній та влади надавати персоналізовані послуги. Ця мета може бути досягнута шляхом поєднання блокчейну, перепризначеного як посередник управління доступом, з рішенням зберігання даних поза ланцюжком блокчейну [2].

Постійно зростаючий обсяг цифрових зображень, включаючи особисті фотографії, медичні відомості та конфіденційна бізнес-інформація, також вимагає надійних і безпечних рішень для зберігання даних та захисту авторських прав. Традиційні методи, часто централізовані за своєю природою, хоча і приваблюють користувачів своєю простотою та доступністю, викликають занепокоєння щодо витоку даних, порушення конфіденційності та відсутності стороннього контролю. Технологія блокчейн із властивою їй децентралізацією, незмінністю та прозорістю представляє потенційний підхід до вирішення цих проблем [3].

Мета цього дослідження полягає в тому, щоб дослідити доцільність і ефективність використання технології блокчейн для зберігання зображень, зосередившись на розумінні того, як різні типи блокчейнів можуть впливати на такі фактори, як безпека, масштабованість і доступність.

Для реалізації цієї мети необхідно розв'язати такі завдання: класифікувати та проаналізувати різні типи архітектур блокчейну, включаючи відкриті, приватні та консорціальні блокчейни; оцінити продуктивність обраних типів блокчейну з

урахуванням таких чинників, як безпека даних, масштабованість та вартість використання для зберігання зображень.

Це дослідження допоможе розкрити потенційні переваги та обмеження використання блокчейну у даному контексті, що сприятиме глибшому розумінню його можливого застосування у реальних сценаріях.

Схожі праці

Автори в статті [4] пропонують звернути увагу на криптографічну структуру на базі блокчейну для цифрових зображень Imagechain, що забезпечує безпеку та цілісність та відповідає потребі у безпечному керуванні зображеннями в різних галузях. Imagechain поєднує блокчейн та криптографічне вбудовування, забезпечуючи безпеку зображень за допомогою хешування. Вона підтримує різні формати файлів та методи вбудовування для зручності користування. Результати дослідження доводять ефективність Imagechain у захисті та запобіганні підробки цифрових зображень. Її унікальні особливості забезпечують надійність.

Загалом, Imagechain пропонує перспективне рішення для безпечного керування цифровими зображеннями за допомогою блокчейну та криптографії. Її універсальність та безпека роблять її цінною для різних сфер застосування.

В [5] пропонується новий метод безпечного обміну зображеннями з використанням технології блокчейну, криптографії та децентралізованого зберігання, вирішуючи важливі потреби у керуванні даними.

Дослідники пропонують систему, що поєднує блокчейн для безпечного зберігання даних, шифрування AES для конфіденційності і IPFS для децентралізованого зберігання. Смарт-контракти керують транзакціями та доступом.

Система демонструє ефективність у забезпеченні безпеки обміну зображеннями, запобігаючи несанкціонованому доступу та забезпечуючи цілісність даних. Масштабованість IPFS підвищує надійність.

Дослідження пропонує перспективний метод безпечного обміну зображеннями за рахунок використання технології блокчейну, криптографії та IPFS [6] та адресує важливі виклики безпеки у керуванні цифровими зображеннями.

У підсумку, автори "Share and Retrieve Images Securely Using Blockchain Technology" [5] надають цінні уявлення щодо застосування блокчейну у керуванні зображеннями, пропонуючи надійний метод безпечного обміну та отримання цифрових зображень.

"Аналіз досліджень у галузі блокчейну: Зосередження на зберіганні даних, масштабованості та доступності" [7] - це дослідження, яке розглядає ключові аспекти технології блокчейну, акцентуючи увагу на зберіганні даних, масштабованості та доступності. Воно спрямоване на покращення розуміння та розвиток безпечних рішень для зберігання даних у блокчейні. Методологією є бібліометричний аналіз, з використанням CiteSpace та VOSviewer для виявлення тенденцій та прогалів у дослідженнях блокчейну. Результати демонструють зростаючий інтерес у науковій літературі до зберігання даних, та вирішення питань масштабованості та доступності про блокчейн, підкреслюючи попит на безпеку у цій галузі.

Загалом, [7] надає цінні знання для науковців, практиків та політиків, які цікавляться майбутнім технології блокчейн та її потенційними застосуваннями у різних секторах.

Стаття [8] звертається до проблеми безпеки даних у сфері охорони здоров'я, зосереджуючись на обміні медичними зображеннями. Вона комбінує незмінність блокчейну, принципи "zero trust" та IPFS для зберігання даних поза блокчейном. Дослідники пропонують децентралізовану систему, яка поєднує блокчейн для забезпечення цілісності даних та принципи "zero trust" для шифрування та аутентифікації. Оцінка результатів показує покращену безпеку та ефективність системи з використанням блокчейну, та вищезгаданих принципів, що запобігають

несанкціонованому доступу та забезпечують масштабованість.

Запропонована система значно підвищує безпеку медичних даних, вирішуючи кіберзагрози та сприяючи забезпеченню конфіденційності даних.

Як можна побачити, незважаючи на великий інтерес дослідників до теми зберігання даних за допомогою блокчейну, досі не було проведено аналіз різних видів блокчейну саме у контексті зберігання зображень. Інші роботи або мають лише дотичну тему, або одразу заглиблюються у реалізацію однієї ідеї. Це дослідження має на меті це виправити.

Для досягнення мети дослідження, яка полягає у вивченні доцільності та ефективності використання технології блокчейн для зберігання зображень та визначенні впливу різних типів блокчейнів на такі фактори, як безпека, масштабованість та доступність, можна використовувати наступні методи дослідження:

1. Літературний огляд: Проведення аналізу наявної літератури щодо використання технології блокчейн для зберігання зображень, включаючи наукові статті, книги, конференційні доповіді та інші джерела.

2. Класифікація блокчейнів: Проведення класифікації типів архітектур блокчейну, систематизація різних підходів та розуміння їхніх відмінностей та особливостей.

3. Порівняльний аналіз: Порівняння результатів отриманих досліджень та аналізу з метою визначення найбільш підходящого типу блокчейну для зберігання зображень з урахуванням їхніх переваг та недоліків.

Таблиця 1

Матеріали дослідження

Джерело	Тип роботи	Рік	Тема	Висновки
[9]	Опитування	2022	Технологія блокчейн та її безпека	Повний огляд технології блокчейн, що охоплює її різні компоненти, програми та аспекти безпеки
[10]	Дослідження	2022	Гібрид із протоколом розподіленого об'єднання блокчейнів для зберігання зображень	Розроблено протокол з низькими вимогами до пам'яті на основі блокчейну під назвою DISP
[11]	Дослідження	2019	Децентралізований обмін зображеннями та захист авторських прав за допомогою блокчейну та перцептивних хешів	Поєднання технології блокчейн та IPFS має великі перспективи для майбутнього обміну файлами
[12]	Дослідження	2022	Якісне порівняння реєстрів мереж передачі даних нового покоління	IPFS ефективна та стійка, але відсутні економічні стимули, що робить його непрактичним для довгострокового використання, особливо для приватних і корпоративних даних
[13]	Дослідження	2019	Порівняльний аналіз блокчейн-платформ – Bitcoin та Ethereum.	Bitcoin - криптовалюта, тоді як Ethereum прагне стати платформою для dApps і смарт-контрактів. Перехід Ethereum на PoS і такі ініціативи, як шардинг, спрямовані на вирішення проблем масштабованості та стійкості, відрізняючи його від Bitcoin з точки зору енергоефективності та перспективності.
[14]	Дослідження	2022	Порівняння Hyperledger Fabric і Ethereum Blockchain	Публічність Ethereum і підтримка IoT роблять його більш придатним для середовищ з широким спектром пристроїв. Приватність Hyperledger Fabric і менше навантаження на систему роблять його привабливим варіантом для сценаріїв, які потребують більш контрольованого та безпечного мережевого середовища.

Продовження табл. 1

Матеріали дослідження

Джерело	Тип роботи	Рік	Тема	Висновки
[15]	Дослідження	2022	Захищене зберігання даних у децентралізованій хмарі від Blockchain Ethereum	У цьому дослідженні запропоновано модель захищеного зберігання даних через децентралізовану хмару блокчейном Ethereum
[16]	Дослідження	2018	Система обміну медичними зображеннями на основі блокчейну та смарт-контракту кредитних балів	Через блокчейн, заснований на розподіленій надійній базі даних процесу обміну записаними зображеннями, ми реалізовано міжорганізаційну, надійну та контрольовану систему обміну медичними зображеннями з встановлення смарт-контрактами на основі кредитних балів пацієнтів і медичних установ.
[17]	Дослідження	2021	Створення моделі децентралізованого зберігання на основі IPFS і блокчейну для медичних зображень	Запропоновано структуру для забезпечення моделі децентралізованого зберігання для обміну медичними зображеннями через IPFS і технологію блокчейн, що усуває перешкоду залежності від сторонніх розробників.
[18]	Дослідження	2023	Однорангова система зберігання та обміну файлами на основі блокчейну консорціуму	Запропоновано нову однорангову архітектуру обміну даними на основі блокчейну консорціуму. Можливо зберігати дані автентифікації та авторизації файлів у блокчейні, що зробить авторизацію більш надійною. Запроваджено механізм доступу до ідентифікаційної інформації, сумісний із блокчейном консорціуму.
[19]	Дослідження	2024	Безпечний та ефективний обмін секретними зображеннями на основі блокчейну за допомогою аутсорсингу обчислень у бездротових мережах	Схема безпечного та ефективного обміну секретними зображеннями на основі блокчейну (BC-SEIS) може досягти бажаної безпеки зв'язку та високої обчислювальної ефективності в бездротових мережах.
[20]	Дослідження	2024	Децентралізований обмін зображеннями через блокчейн і IPFS	Об'єднання блокчейну та IPFS пропонує рішення, яке посилює принципи конфіденційності користувачів і права власності на дані в цифровому середовищі.

Блокчейн-платформи можна класифікувати за трьома основними типами архітектури:

Централізовані блокчейни: мають один центральний орган, який контролює мережу та валідує транзакції. Прикладами є Ripple, Hyperledger Fabric (з приватною мережею). До переваг відносяться висока швидкість транзакцій, простота налаштування. Недоліки - низький рівень децентралізації, ризик цензури, залежність від центрального органу.

Децентралізовані блокчейни: не мають центрального органу, всі учасники мережі рівні. Валідація транзакцій відбувається за допомогою консенсус-алгоритмів, таких як Proof-of-Work (PoW) або Proof-of-Stake (PoS). Приклади: Bitcoin, Ethereum, Litecoin. Переваги: високий рівень децентралізації, безпека, стійкість до цензури. Недоліки: низька швидкість транзакцій, високі комісії, складність налаштування.

Гібридні блокчейни: поєднують елементи централізованих і децентралізованих блокчейнів. Можуть мати центральний орган, який відповідає за певну частину мережі, а інші частини децентралізовані. Приклади: EOS, Tron. Переваги: баланс між

децентралізацією, масштабованістю та швидкістю. Недоліки: складність архітектури, ризик централізації.

Окрім трьох основних типів, існують й інші підходи до класифікації блокчейнів за архітектурою:

- За кількістю шарів:

- Одношарові (single-layer): Це блокчейни, які складаються з одного основного шару, наприклад, Bitcoin.

- Багатошарові (multi-layer): Ці блокчейни мають більш складну архітектуру з кількома рівнями абстракції. Прикладом може бути Ethereum, яка має окремий рівень для смарт-контрактів та різноманітні додатки.

- За типом консенсус-алгоритму:

- Proof-of-Work (PoW): Цей алгоритм використовується для підтвердження транзакцій та створення нових блоків шляхом вирішення складних обчислювальних завдань.

- Proof-of-Stake (PoS): У цьому типі алгоритму відбувається вибір нових блоків на основі володіння монетами або токенами криптовалюти.

- Delegated Proof-of-Stake (DPoS): У DPoS власники tokenів делегують свої голоси представникам, які мають право голосувати за транзакції.

- Proof-of-Authority (PoA): В цьому алгоритмі блоки створюються авторитетними учасниками мережі, а не на основі обчислювальної роботи або володіння токенами.

- За типом ланцюга:

- Публічні (public): Це блокчейни, до яких може приєднатися будь-хто і бачити всі транзакції та блоки, наприклад, Bitcoin та Ethereum.

- Приватні (private): Вони обмежені доступом і використовуються, головним чином, в організаціях або корпоративних середовищах.

- Консорціумні (consortium): Це блокчейни, які використовуються кількома організаціями або сторонами з визначеними правами доступу.

- За типом зберігання даних:

- On-chain (на ланцюжку): Деякі дані зберігаються безпосередньо на ланцюжку блокчейну. Це може бути корисно для створення додатків, які потребують високої стійкості та неперевершеної безпеки.

- Off-chain (поза ланцюжком): Деякі дані можуть бути збережені поза блокчейном, забезпечуючи при цьому швидкість та масштабованість. Проте, цей підхід може збільшити ризик безпеки та централізації.

Саме блокчейни зі зберіганням даних поза ланцюжком найкраще підходять для систем зберігання зображень за рахунок зменшення навантаження на блокчейн, оскільки великі обсяги даних зберігаються поза ним, при цьому забезпечуючи високу доступність та надійність. Це дозволяє блокчейнам бути більш масштабованими та ефективними.

Дослідження показало, що блокчейн рішення, такі як Ethereum та IPFS, можуть бути ефективними сховищами для зображень, проте вони мають свої особливості та обмеження. Час завантаження на блокчейн Ethereum трохи перевищує час для IPFS, але обидва значно повільніші, ніж Dropbox. Проте, вони продемонстрували прийнятну пропускну здатність, що свідчить про їхню здатність обробляти великі обсяги даних. Вартість зберігання на блокчейні IPFS виявилася більш вигідним з економічної точки зору, ніж централізовані системи зберігання. У той же час блокчейн рішення продемонстрували високий рівень безпеки, оскільки дані шифруються та розподіляються по мережі.

Аналіз різних типів блокчейнів показує, що їх придатність для зберігання зображень залежить від детального балансування між їхніми внутрішніми характеристиками та специфічними потребами застосування.

Певні аспекти структури блокчейну, такі як розмір та склад блоків, безпосередньо впливають на його ефективність у роботі з даними зображень. Блокчейни з надійними алгоритмами хешування та ефективними механізмами управління даними можуть забезпечити високий рівень цілісності та безпеки даних. Однак, більші розміри блоків, хоча й вміщують більше даних, можуть призвести до проблем з масштабованістю та збільшенням потреб у зберіганні. Це вимагає досягнення делікатного балансу між обсягом даних та продуктивністю блокчейну.

Окрім технічних атрибутів, вибір блокчейну для зберігання зображень повинен керуватися специфічними вимогами застосування. Такі фактори, як бажаний рівень децентралізації, безпеки та масштабованості, відіграють вирішальну роль. Хоча публічні блокчейни, такі як Ethereum, можуть похвалитися високими функціями безпеки та широким використанням, їх висока вартість транзакцій та ресурсомісткі процеси майнінгу можуть зробити їх менш придатними для зберігання великих обсягів даних зображень. І навпаки, приватні або консорціумні блокчейни, такі як Hyperledger Fabric, пропонують більший контроль над мережею, потенційно забезпечуючи більш економічно ефективне рішення для конкретних випадків використання, включаючи зберігання зображень у межах визначеної групи учасників.

IPFS (InterPlanetary File System) може виступати як доповнення до блокчейну, пропонуючи децентралізоване та економічно вигідне рішення для зберігання самих зображень. IPFS використовує систему хешування для зв'язку даних, роблячи їх доступними через мережу P2P. Це може допомогти зменшити навантаження на блокчейн, зберігаючи лише метадані зображень, такі як хеш-суми та посилання на IPFS.

Зрештою, придатність блокчейну та IPFS для зберігання зображень залежить від ретельного аналізу потреб та пріоритетів конкретного застосування. Розробники та організації повинні ретельно оцінити фактори, такі як масштабованість, безпека, економічна ефективність, та доступність, щоб зробити кращий вибір.

Висновки. Дослідження різноманітних типів блокчейнів та аналіз їх придатності для сховищ зображень пролило світло на потенційні можливості та обмеження використання цих технологій. Виявлені переваги та недоліки кожного типу блокчейну, а також їхні можливі сценарії застосування, можуть послужити важливим керівними принципами для розробників сховищ зображень.

Подальші дослідження можуть зосередитися на покращенні методів зберігання даних, розробці більш ефективних алгоритмів консенсусу та розширенні можливостей розподіленого сховища зображень. Враховуючи швидкий розвиток технологій блокчейну, відкривається безмежний потенціал для інновацій у сфері сховищ даних, включаючи зображення.

Список використаних джерел:

1. Kyrychenko I., Tereshchenko G., Chetverykov G. Overview of image storage models in Big Data conditions. Комп'ютерна математика в науці, інженерії та освіті CMSEE-2020: матеріали Всеукр. наук. конф., Полтава, 20 November 2020. Полтава, 2020. Р. 18–20.
2. Zyskind, Guy et al. "Decentralizing Privacy: Using Blockchain to Protect Personal Data." 2015 IEEE Security and Privacy Workshops (2015): 180-184.

3. Kyrychenko I., Bilous N., Tereshchenko G. Copyright protection using blockchain. Бионика интеллекта. Информация, язык, интеллект. 2019. Vol. 1, no. 92. P. 52–58.
4. Koptyra K, Ogiela MR. Imagechain-Application of Blockchain Technology for Images. Sensors (Basel). 2020 Dec 25;21(1):82. doi: 10.3390/s21010082. PMID: 33375606; PMCID: PMC7796195.
5. Alshareef, Ahmed & Yannawar, Pravin & Abdul-Qawy, Antar. (2022). Share and Retrieve Images Securely Using Blockchain Technology. 14. 207-2011.
6. Benet, J. (2014). IPFS - Content Addressed, Versioned, P2P File System. ArXiv, abs/1407.3561.
7. Kandpal M, Goswami V, Priyadarshini R, Barik RK. Towards Data Storage, Scalability, and Availability in Blockchain Systems: A Bibliometric Analysis. Data. 2023; 8(10):148. <https://doi.org/10.3390/data8100148>.
8. Sultana, M., Hossain, A., Laila, F. et al. Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. BMC Med Inform Decis Mak 20, 256 (2020). <https://doi.org/10.1186/s12911-020-01275-y>.
9. Huaqun Guo, Xingjie Yu, A survey on blockchain technology and its security, Blockchain: Research and Applications, Volume 3, Issue 2, 2022, 100067, ISSN 2096-7209, <https://doi.org/10.1016/j.bcr.2022.100067>.
10. Liu, F., Yang, Cy., Yang, J. et al. A hybrid with distributed pooling blockchain protocol for image storage. Sci Rep 12, 3457 (2022).
11. R. Mehta, N. Kapoor, S. Sourav and R. Shorey, "Decentralised Image Sharing and Copyright Protection using Blockchain and Perceptual Hashes," 2019 11th International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, India, 2019, pp. 1-6, doi: 10.1109/COMSNETS.2019.8711440.
12. E. Daniel and F. Tschorsch, "IPFS and Friends: A Qualitative Comparison of Next Generation Peer-to-Peer Data Networks," in IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 31-52, Firstquarter 2022, doi: 10.1109/COMST.2022.3143147.
13. Rankhambe, B.P., & Kaur Khanuja, H. (2019). A Comparative Analysis of Blockchain Platforms – Bitcoin and Ethereum. 2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA), 1-7.
14. Zhao, Z. (2022). Comparison of Hyperledger Fabric and Ethereum Blockchain. 2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC), 584-587.
15. Khan N, Aljoaey H, Tabassum M, Farzamniah A, Sharma T, Tung YH. Proposed Model for Secured Data Storage in Decentralized Cloud by Blockchain Ethereum. Electronics. 2022; 11(22):3686. <https://doi.org/10.3390/electronics11223686>.
16. H. Tang, N. Tong and J. Ouyang, "Medical Images Sharing System Based on Blockchain and Smart Contract of Credit Scores," 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 2018, pp. 240-241, doi: 10.1109/HOTICN.2018.8605956.
17. Kumar, Randhir & Tripathi, Rakesh. (2021). Building an IPFS and Blockchain-Based Decentralized Storage Model for Medical Imaging. 10.4018/978-1-7998-2795-5.ch002.
18. Shaoliang Peng, Wenxuan Bao, Hao Liu, Xia Xiao, Jiandong Shang, Lin Han, Shan Wang, Xiaolan Xie, Yang Xu, A peer-to-peer file storage and sharing system based on consortium blockchain, Future Generation Computer Systems, Volume 141, 2023, Pages 197-204, ISSN 0167-739X, <https://doi.org/10.1016/j.future.2022.11.010>.
19. Z. Zhou et al., "Blockchain-Based Secure and Efficient Secret Image Sharing With Outsourcing Computation in Wireless Networks," in IEEE Transactions on Wireless Communications, vol. 23, no. 1, pp. 423-435, Jan. 2024, doi: 10.1109/TWC.2023.3278108.
20. Vayadande, Kuldeep, et al. "Empowering Data Sovereignty: Decentralized Image Sharing through Blockchain and Interplanetary File System". International Journal of Intelligent Systems and Applications in Engineering 12 (14s):223-35.