УДК 004.056.5

А. В. Грицак
А. В. Марущак

РОЗРОБКА АЛГОРИТМУ ЗАХИЩЕНОЇ ДЕЦЕНТРАЛІЗОВАНОЇ СИСТЕМИ РЕЗЕРВНОГО КОПІЮВАННЯ НА ОСНОВІ IPFS, БЛОКЧЕЙНУ ТА СМАРТ-КОНТРАКТІВ

Вінницький національний технічний університет

Анотація
У сучасному інформаційному суспільстві вагоме значення має забезпечення конфіденційності, доступності та довготривалого зберігання даних. У даній роботі запропоновано розробку алгоритму захищеної системи резервного копіювання, що базується на децентралізованому зберіганні даних з використанням IPFS, шифрування та смарт-контрактів у блокчейн-середовищі. Проаналізовано переваги такого підходу над централізованими рішеннями: усунення єдиної точки відмови, підвищення конфіденційності, прозорість доступу та масштабованість. Запропоновано комплексний алгоритм функціонування системи, що охоплює шифрування, фрагментацію, хешування, реплікацію, розподіл по вузлах, контроль доступу, моніторинг, логування та відновлення даних.
Ключові слова: *резервне копіювання; децентралізоване зберігання; блокчейн; смарт-контракти; інформаційна безпека; контроль доступу.*

Abstract
In today's information society, ensuring confidentiality, accessibility, and long-term storage of data is of great importance.This paper proposes the development of an algorithm for a secure backup system based on decentralized data storage using IPFS, encryption and smart contracts in a blockchain environment. The advantages of this approach over centralized solutions are analyzed, including the elimination of a single point of failure, enhanced confidentiality, access transparency, and scalability. A comprehensive algorithm for the system's operation is proposed, covering encryption, fragmentation, hashing, replication, node distribution, access control, monitoring, logging, and data recovery.
Keywords: *backup; decentralized storage; blockchain; smart contracts; information security; access control.*

Вступ

Сучасна цифрова епоха висуває високі вимоги до безпеки, доступності та довготривалого зберігання даних. Традиційні централізовані рішення для резервного копіювання втрачають актуальність через низку недоліків – централізацію, вразливість до атак та залежність від провайдерів. Це зумовлює необхідність впровадження нових підходів. Одним із перспективних рішень є використання децентралізованих сховищ у поєднанні з технологіями блокчейну та смарт-контрактів, що забезпечують не лише надійне зберігання даних, а й прозорий контроль за їх використанням.

Результати дослідження

У сучасному світі, де обсяги даних стрімко зростають, а вимоги до їхньої безпеки та доступності стають дедалі суворішими, дедалі більше уваги приділяється децентралізованим рішенням для зберігання інформації. Децентралізоване сховище файлів (DFS) – це спосіб зберігання даних на кількох

серверах або місцях, а не в централізованому сховищі даних. Це рішення має на меті покращити доступ до даних і керування ними, зробивши дані доступними в будь-який час і в будь-якому місці [1].

Використання децентралізованого зберігання у резервному копіюванні забезпечує високу надійність, оскільки усуває єдину точку відмови: навіть при виході з ладу окремих вузлів доступ до даних зберігається. Завдяки шифруванню користувач може безпечно зберігати конфіденційну інформацію, не покладаючись на довіру до сторонніх сервісів. Смарт-контракти у блокчейн-середовищі дозволяють автоматизувати контроль доступу до резервних копій, визначаючи, хто, коли і за яких умов може звертатися до даних. Вони фіксують усі події, забезпечують прозорість і незмінність журналів доступу, що важливо для аудиту та безпеки. Крім того, можлива реалізація складних механізмів доступу – з урахуванням геолокації, часу, пристрою тощо.

Проєктування захищеної системи резервного копіювання на основі децентралізованого зберігання даних є важливим етапом забезпечення цілісності та безпеки в умовах зростання загроз інформаційній безпеці. Традиційні централізовані рішення стикаються з ризиками зловмисного доступу, кібератак та залежності від єдиного постачальника. Натомість децентралізовані системи пропонують стійкість до збоїв, надійність і захист завдяки шифруванню та блокчейн-технологіям.

Мета такої системи – створити безпечне, надійне та масштабоване середовище для зберігання резервних копій із дотриманням конфіденційності, цілісності та доступності даних. Ключовими елементами є фрагментація та розподіл даних, шифрування, ідентифікація за хешами та використання протоколів, як-от IPFS.

IPFS (InterPlanetary File System) – це розподілена файлова система, що працює між вузлами та прагне з’єднати всі обчислювальні пристрої з однією системою файлів [2]. Після успішного завантаження даних IPFS генерує унікальний ідентифікатор вмісту (CID) для кожного фрагмента, що дозволяє отримувати файли на основі їхнього вмісту [5].

Принцип роботи IPFS полягає у такому:

1. Файл розбивається на частини, хешується, і кожна версія отримує унікальний ідентифікатор – CID (Content Identifier).

2. Інші вузли мережі шукають файл за CID і, завантаживши його, зберігають копію, стаючи його постачальниками.

3. Вузли можуть закріпити файл, щоб зберігати його назавжди, або автоматично видаляти, щоб економити місце.

4. Кожна нова версія файлу має новий CID, тому старі версії не перезаписуються і файли захищені від змін.

5. IPNS і DNSLink допомагають прив’язати довгі CID до зручних для користувача назв.

6. Якщо браузер не підтримує IPFS напряму, можна отримати доступ через шлюзи, наприклад ipfs.io [3].

CID – це мітка, яка використовується для вказівки на матеріал в IPFS. Вона не вказує, де зберігається контент, але формує свого роду адресу на основі самого контенту [4].

Блокчейн забезпечує фіксацію транзакцій та контроль доступу через смарт-контракти. Вони автоматизують надання доступу, фіксують звернення до копій і забезпечують захист від несанкціонованих дій.

Шифрування реалізується на всіх етапах – передача, зберігання, відновлення – із контролем ключів користувачем. Рекомендується гібридне шифрування: симетричне для обсягів даних і асиметричне – для захисту ключів.

Відновлення даних здійснюється через ідентифікацію фрагментів, перевірку хешів і об'єднання у цілісну структуру. Для підвищення доступності застосовують реплікацію фрагментів на кількох вузлах. Масштабованість системи забезпечує її адаптивність до зростання обсягів і нових технологій.

Децентралізовані рішення для резервного копіювання дозволяють усунути ці проблеми, розподіляючи дані по численних географічно розподілених вузлах мережі. Це підвищує надійність збереження інформації, а також забезпечує її конфіденційність.

Основою роботи такої системи є комплексний алгоритм, який включає кілька важливих етапів:

1. Ідентифікація даних для резервного копіювання. На початку визначаються файли, каталоги чи системи, що потребують захисту. Важливо класифікувати інформацію за рівнем її чутливості, щоб застосувати адекватні заходи безпеки.

2. Шифрування даних. Перед передачею у мережу дані піддаються надійному шифруванню, що гарантує їх захист навіть у випадку компрометації.

3. Фрагментація. Зашифровані дані розбиваються на окремі фрагменти, які зберігатимуться на різних вузлах. Такий підхід ускладнює доступ до повної інформації для потенційних зловмисників.

4. Генерація унікальних хешів для кожного фрагмента. Хешування дозволяє перевіряти цілісність фрагментів під час їх відновлення.

5. Вибір вузлів для зберігання. Вузли підбираються на основі критеріїв надійності, географічного розташування та доступного простору.

6. Безпечна передача фрагментів. Дані передаються через захищені канали, що виключає ризик перехоплення.

7. Запис фрагментів на вузли. Кожен вузол зберігає лише частину загального обсягу інформації, що забезпечує стійкість до втрати даних.

8. Фіксація інформації про місця зберігання. Відомості про розташування фрагментів заносяться у захищену базу даних або блокчейн, що полегшує подальше відновлення.

9. Перевірка цілісності даних. Після збереження здійснюється контроль за допомогою хешів для виключення пошкоджень.

10. Визначення політик доступу. Регламентуються права користувачів на роботу з резервними копіями за ролями, часом або іншими параметрами.

11. Реалізація смарт-контрактів для контролю доступу. Смарт-контракти автоматизують управління доступом, забезпечуючи прозорість та незмінність правил.

12. Моніторинг та сповіщення. Система в режимі реального часу відслідковує спроби доступу і оповіщає адміністратора про підозрілі дії.

13. Відновлення даних за запитом. Після перевірки прав користувача система збирає фрагменти з різних вузлів та відновлює цілісні дані.

14. Шифрування відновлених даних. Для безпеки інформація шифрується повторно перед передачею користувачу.

15. Логування операцій. Усі дії щодо резервного копіювання та відновлення фіксуються для аудиту та підвищення рівня безпеки.

Традиційні методи контролю доступу мають вразливості, що можуть бути використані зловмисниками. Смарт-контракти на блокчейн-платформах надають можливість автоматизувати управління доступом, забезпечуючи прозорість, надійний аудит та незмінність записів.

Основні етапи алгоритму моніторингу доступу:

1. Ідентифікація користувача. Перед доступом відбувається аутентифікація через смарт-контракт із верифікацією у блокчейні.

2. Визначення прав доступу. Смарт-контракт оцінює роль користувача і визначає його можливості щодо конкретних даних.

3. Перевірка відповідності політикам безпеки. Контроль відповідності прав користувача діючим політикам.

4. Аналіз типу операції. Визначення, чи дозволена операція (перегляд, зміна, видалення).

5. Аудит спроб доступу. Запис усіх спроб доступу для подальшого аналізу.

6. Моніторинг часу і місця доступу. Виявлення аномальних або несанкціонованих дій.

7. Двоетапна аутентифікація. Посилення безпеки за рахунок додаткових перевірок.

Поєднання децентралізованого зберігання на базі IPFS, блокчейн-технологій і сучасних методів шифрування формує надійний механізм для захищеного резервного копіювання даних. Автоматизація контролю доступу через смарт-контракти не лише підвищує прозорість і аудит, а й мінімізує ризики несанкціонованих дій, роблячи систему більш стійкою до внутрішніх та зовнішніх загроз.

Висновки

Децентралізована система резервного копіювання, що базується на IPFS, шифруванні та смарт-контрактах, забезпечує високий рівень конфіденційності, доступності та цілісності даних. Вона усуває єдину точку відмови, дозволяє гнучко керувати доступом, автоматизує аудит операцій і є стійкою до збоїв і атак. Завдяки гібридному шифруванню, реплікації, логуванню та масштабованій архітектурі така система може ефективно застосовуватись у критичних IT-середовищах, які потребують найвищого рівня захисту резервних копій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке децентралізоване сховище файлів?. Gate.io. [Електронний ресурс]. Режим доступу: https://www.gate.io/uk/learn/articles/what-is-distributed-file-storage/939 (дата звернення: 21.04.2025).

2. Benet J. IPFS - Content Addressed, Versioned, P2P File System. 2014. 29 липня. 27 с. [Електронний ресурс]. Режим доступу: https://doi.org/10.48550/arXiv.1407.3561 (дата звернення: 24.04.2025).

3. Introduction to IPFS | Symphony. Software development and design for the world's most innovative brands | Symphony. [Електронний ресурс]. Режим доступу: https://symphony.is/about-us/blog/introduction-to-ipfs (дата звернення: 26.04.2025).

4. Content Identifiers (CIDs) | IPFS Docs. [Електронний ресурс]. Режим доступу: https://docs.ipfs.tech/concepts/content-addressing/ (дата звернення: 30.04.2025).

5. Chintal B. P. Secure Decentralized Storage System Using Blockchain and IPFS // SSRN. 2025. 18 лютого. 7 с. [Електронний ресурс]. Режим доступу: https://doi.org/10.2139/ssrn.5142864 (дата звернення: 30.04.2025).

Марущак Анастасія Віталіївна **–** студентка групи 2КІТС-21б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: anamar349@gmail.com

Науковий керівник: ***Грицак Анатолій Васильович*** – доцент каф. Менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: grytsak.a.v@gmail.com

Marushchak Anastasiia Vitalyivna – student of group 2CITS-21b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: anamar349@gmail.com

Supervisor: ***Hrytsak Anatolii Vasyliovych*** – docent of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: grytsak.a.v@gmail.com