DOI: https://doi.org/10.36910/6775-2524-0560-2026-64-31
УДК: 004.4
Федчун Кирило Юрійович, здобувач освіти
Гришанович Тетяна Олександрівна, к.ф.-м.н., доцент
https://orcid.org/0000-0002-3595-6964
Волинський національний університет імені Лесі Українки, м. Луцьк, Україна

БЛОКЧЕЙН-АЛГОРИТМ РОЗПОДІЛЕНОЇ ВАЛІДАЦІЇ ДЛЯ ЗАХИЩЕНОГО ЗБЕРЕЖЕННЯ ТА ПЕРЕДАЧІ ДАНИХ

Федчун К. Ю., Гришанович Т. О. Блокчейн-алгоритм розподіленої валідації для захищеного збереження та передавання даних. У статті розглянуто проблему безпечного збереження та передачі даних у розподілених інформаційних системах. Обґрунтовано актуальність використання технології блокчейн як основи для побудови децентралізованих систем, здатних гарантувати цілісність, достовірність і незмінність інформації без застосування централізованих органів керування. Метою роботи є розроблення блокчейн-алгоритму для побудови надійної системи онлайн-збереження та передачі даних із використанням механізмів розподіленої валідації та алгоритму консенсусу. Запропонований алгоритм базується на багаторівневій процедурі обробки інформаційних транзакцій, що включає локальну перевірку, розподілену валідацію, колективне підтвердження транзакцій, формування нового блоку за алгоритмом Proof of Work та синхронізацію вузлів мережі. Особливістю алгоритму є реалізація дворівневого механізму підтвердження транзакцій до запуску процедури консенсусу, що дозволяє підвищити достовірність даних, зменшити навантаження на механізм майнінгу та підвищити продуктивність системи. Практичну реалізацію алгоритму виконано у вигляді програмного комплексу з відкритою архітектурою на основі Python, Flask, REST API та WebSocket. Для апробації розробленого рішення створено експериментальну платформу електронного онлайн-голосування, яка підтвердила працездатність запропонованого алгоритму. Отримані результати демонструють можливість використання розробленого алгоритму як універсальної основи для побудови захищених розподілених інформаційних систем різного призначення, що потребують високого рівня безпеки, цілісності та надійності збереження і передачі даних.
Ключові слова: блокчейн, розподілена система, децентралізована архітектура, алгоритм консенсусу, інформаційні транзакції, валідація транзакцій, захищене збереження даних, передавання даних, інформаційна безпека.

Fedchun K., Hryshanovych T. A Blockchain-Based Distributed Validation Algorithm for Secure Data Storage and Transmission. The paper addresses the problem of secure data storage and transmission in distributed information systems. The relevance of blockchain technology as a foundation for developing decentralized systems capable of ensuring data integrity, authenticity, and immutability without relying on a centralized authority is substantiated. The aim of this research is to develop a blockchain-based algorithm for building a reliable online data storage and transmission system using distributed validation mechanisms and a consensus algorithm. The proposed algorithm is based on a multi-stage information transaction processing procedure that includes local verification, distributed validation, collective transaction confirmation, new block generation using the Proof of Work consensus algorithm, and network node synchronization. A distinctive feature of the proposed approach is the implementation of a two-stage transaction confirmation mechanism performed prior to the consensus procedure. This enables improved data reliability, reduced computational workload associated with the mining process, and enhanced overall system performance. The algorithm has been implemented as an open-architecture software solution based on Python, Flask, REST API, and WebSocket technologies. To validate the proposed approach, an experimental electronic online voting platform was developed and used as a case study to demonstrate the functionality and effectiveness of the algorithm. The obtained results confirm that the proposed algorithm can serve as a universal foundation for the development of secure distributed information systems requiring a high level of security, data integrity, and reliability in data storage and transmission.
Keywords: blockchain, distributed system, decentralized architecture, consensus algorithm, information transactions, transaction validation, secure data storage, data transmission, information security.

Постановка проблеми. У цифровому суспільстві стрімко зростає потреба у створенні надійних систем збереження та передачі даних, здатних гарантувати високий рівень безпеки, цілісності та доступності інформації. Традиційні централізовані системи керування даними мають низку суттєвих недоліків, серед яких наявність єдиної точки відмови, ризик несанкціонованого доступу, залежність від центрального адміністратора та вразливість до кібератак. У зв'язку з цим особливої актуальності набувають децентралізовані технології, зокрема блокчейн, які дозволяють створювати розподілені системи без необхідності використання централізованого органу керування.

Технологія блокчейн є одним із найбільш перспективних напрямів розвитку сучасних децентралізованих інформаційних систем. Її головною особливістю є використання розподіленого реєстру, у якому дані зберігаються у вигляді послідовного ланцюга блоків, захищених криптографічними методами. Такий підхід забезпечує незмінність інформації, високу стійкість до модифікації даних, прозорість операцій та надійний механізм перевірки транзакцій. Завдяки цьому блокчейн активно використовується у фінансовій сфері, логістиці, системах електронного документообігу, медицині, IoT та електронному голосуванні.

Особливого значення блокчейн-технології набувають у системах онлайн-збереження та передачі даних, де критично важливими є захист інформації, забезпечення конфіденційності користувачів та гарантована цілісність переданих даних. Використання алгоритмів консенсусу, криптографічного хешування, цифрових підписів та механізмів розподіленої валідації дозволяє створити ефективне середовище для безпечної взаємодії між вузлами мережі.

Метою роботи є створення блокчейн-алгоритму для побудови надійної та захищеної системи онлайн-збереження і передачі даних. Основне призначення такого алгоритму полягатиме у забезпеченні цілісності, безпеки та достовірності інформації у розподіленому середовищі.

Основні вимоги до алгоритму:

- алгоритм має базуватись на децентралізованій архітектурі, що забезпечує стабільність функціонування системи та усуває залежність від єдиного центру управління;
- система повинна гарантувати прозорість і відкритість усіх процесів обробки та передавання даних;
- алгоритм має забезпечувати високу продуктивність і швидкодію для обробки значної кількості транзакцій без затримок;
- програмна реалізація повинна мати відкритий вихідний код, що сприятиме вдосконаленню системи спільнотою розробників та своєчасному виявленню можливих вразливостей;
- система повинна ефективно функціонувати на різних типах пристроїв і забезпечувати раціональне використання обчислювальних ресурсів користувачів.

Для практичної демонстрації роботи розробленого алгоритму передбачається створення платформи електронного онлайн-голосування.

Аналіз останніх досліджень і публікацій. Проблематика безпечного збереження та передачі даних у розподілених мережах є одним із ключових напрямів сучасних досліджень у галузі інформаційних технологій. Значна кількість наукових праць останніх років присвячена застосуванню блокчейн-технологій для створення децентралізованих систем, здатних забезпечити цілісність, надійність та захист інформації без використання централізованих органів керування.

У статті [7] автори розглядають сучасні принципи побудови блокчейн-систем, алгоритми консенсусу та механізми криптографічного захисту даних. Особлива увага приділяється використанню розподілених реєстрів у системах обміну інформацією та захисту цифрових транзакцій, підкреслюється, що застосування блокчейн-технологій дозволяє значно підвищити стійкість систем до несанкціонованих змін та кібератак. Також проблематика безпеки персональних даних у розподілених мережах розглядається у роботі [9]. Автори пропонують механізм захисту персональної інформації із застосуванням розподілених хеш-таблиць та криптографічних алгоритмів. У дослідженні доведено, що блокчейн дозволяє значно підвищити рівень контролю користувача над власними даними та мінімізувати ризики витоку інформації. Перспективним напрямом є також застосування блокчейну у медичних інформаційних системах. У [3] запропоновано модель безпечного збереження та обміну медичними даними з використанням асиметричного шифрування та блокчейн-технологій. Автори підтверджують, що запропонована модель гарантує високі показники безпеки, швидке завантаження та передачу даних, а також надійний контроль доступу до інформації.

У праці [4] досліджено алгоритм обміну даними на основі блокчейн у розподілених мережах. Автори запропонували механізм децентралізованої передачі інформації, який забезпечує високий рівень захисту даних та підвищує продуктивність системи. Результати дослідження демонструють, що використання блокчейну дозволяє зменшити ризики втрати інформації та забезпечити цілісність даних у процесі передавання.

Проблему безпечного контролю доступу до даних розглянуто у роботі [6]. Автори запропонували модель поєднання блокчейн-мережі з off-chain-сховищами для зменшення навантаження на мережу та підвищення ефективності роботи системи. У дослідженні доведено, що використання смарт-контрактів та криптографічних ключів дозволяє забезпечити конфіденційність і цілісність інформації навіть у розподіленому середовищі.

У статті [2] проаналізовано інтеграцію блокчейн із системою IPFS для створення безпечного середовища збереження та передачі даних. Автори зазначають, що поєднання IPFS і блокчейн забезпечує високу доступність інформації, ефективне розподілене збереження файлів та криптографічний контроль цілісності даних.

Дослідження [11] присвячене побудові моделі захисту транзакційних даних у великих приватних мережах. У роботі використано алгоритми консенсусу та криптографічного хешування для забезпечення достовірності інформації та захисту мережі від несанкціонованого втручання. Автори підкреслюють ефективність децентралізованого підходу для забезпечення стабільності та безпеки обробки транзакцій.

Важливим напрямом сучасних досліджень є використання блокчейн-технологій у хмарних сервісах. У статті [8] описано механізм управління ключами безпеки у хмарних системах з використанням блокчейн та цифрових двійників. Результати дослідження демонструють, що блокчейн дозволяє забезпечити незмінність записів, прозорість операцій та безпечний обмін інформацією між вузлами мережі.

Проблематика масштабованості блокчейн-систем досліджується у статті [5], де запропоновано механізм шардованого блокчейну для промислових IoT-систем. Автори доводять, що використання шардінгу дозволяє підвищити продуктивність мережі, зменшити затримки обробки транзакцій та оптимізувати використання ресурсів системи.

У книзі [1] автор розглядає сучасні архітектури блокчейн-систем, принципи роботи алгоритмів консенсусу, смарт-контрактів та механізмів забезпечення безпеки розподілених мереж. Значну увагу приділено питанням масштабованості, продуктивності та захисту даних у блокчейн-мережах нового покоління.

У [10] запропоновано підхід фрагментації файлів та їх розподіленого збереження у блокчейн-середовищі. Автори доводять, що поділ даних на окремі частини та їх збереження у розподіленій мережі дозволяє підвищити доступність інформації та знизити ризики втрати даних.

Таким чином, аналіз сучасних наукових праць свідчить про значний інтерес до використання блокчейн-технологій для побудови безпечних систем онлайн-збереження та передачі даних. Основними перевагами блокчейн є децентралізація, криптографічний захист, прозорість операцій, незмінність записів та стійкість до атак. Водночас актуальними залишаються питання масштабованості, оптимізації продуктивності та ефективного управління ресурсами мережі, що обумовлює доцільність подальших досліджень у напрямі розроблення нових блокчейн-алгоритмів для розподілених систем збереження і передачі інформації.

Викладення основного матеріалу і обґрунтування отриманих результатів.

Запропонований у роботі алгоритм призначений для побудови розподілених інформаційних систем, у яких необхідно забезпечити цілісність, достовірність та незмінність даних без використання централізованого органу керування. Основою алгоритму є децентралізована архітектура Blockchain, відповідно до якої кожний вузол мережі виконує однаковий набір функцій щодо приймання, перевірки, підтвердження, зберігання та синхронізації інформаційних транзакцій.

На відміну від традиційних централізованих систем збереження даних, де перевірка достовірності інформації покладається на центральний сервер, запропонований алгоритм реалізує механізм колективного прийняття рішень усіма активними вузлами мережі. Такий підхід забезпечує відсутність єдиної точки відмови, підвищує стійкість до зовнішніх атак та дозволяє підтримувати працездатність системи навіть за часткового виходу окремих вузлів із ладу.

Архітектура алгоритму складається з п'яти взаємопов'язаних функціональних модулів: приймання транзакцій, розподіленої валідації, колективного підтвердження, алгоритму консенсусу Proof of Work та синхронізації мережі. Послідовна взаємодія зазначених модулів забезпечує повний цикл обробки інформації — від моменту надходження нових даних до їх остаточного включення у блокчейн.

Будь-яке повідомлення, що надходить до системи, представляється у вигляді інформаційної транзакції (рис. 1). До її складу входять службовий ідентифікатор, корисні дані, часові мітки та службова інформація, необхідна для подальшої перевірки. Такий підхід забезпечує універсальність алгоритму та дозволяє використовувати його незалежно від предметної області.

Першим етапом обробки є локальна валідація транзакції. На цьому етапі виконується перевірка її коректності, аналіз наявності аналогічних записів у локальному блокчейні та серед транзакцій, що вже перебувають у процесі перевірки. Одночасно контролюється унікальність службового ідентифікатора, що унеможливлює повторне опрацювання однакових повідомлень.

Особливістю запропонованого алгоритму є виконання повної процедури валідації ще до запуску алгоритму консенсусу. Завдяки цьому до процесу майнінгу допускаються лише перевірені

транзакції, що дозволяє істотно скоротити кількість зайвих обчислень та підвищити продуктивність системи.

```
def __init__(self):
    self.current_transactions = []
    self.chain = []
    self.nodes = set()
    self.nodes_in_validation = []
    self.deleted_nodes = [{
        'deleted_nodes': [],
        'senders': set(),
    }]
    self.added_nodes = [{
        'added_nodes': [],
        'senders': set(),
    }]
    self.transaction_resolver = []
    self.mining_list = []
    self.mining_resolver = []


    self.host='0.0.0.0'
    self.port=1000


    self.new_block(previous_hash=1, proof=100)
```

Рис. 1. Внутрішні дані вузла

Після завершення локальної перевірки інформація автоматично розповсюджується між усіма активними вузлами мережі. Кожний вузол незалежно повторює процедуру валідації та передає результати іншим учасникам мережі. Таким чином реалізується механізм незалежної перевірки інформації без використання центрального координатора.

Для синхронізації процесу розподіленої перевірки використовується проміжне сховище результатів валідації, у якому накопичуються відомості про всі інформаційні транзакції, що перебувають у процесі перевірки. Для кожної транзакції зберігаються результати перевірки, вузол-ініціатор та часові параметри її обробки. Це дозволяє уникнути дублювання службових повідомлень, мінімізувати мережевий трафік та забезпечити узгодженість роботи всіх учасників розподіленої системи.

Після завершення процедури валідації виконується колективне підтвердження транзакції. Для цього аналізуються результати перевірки, отримані від усіх активних вузлів мережі. Якщо кількість позитивних підтверджень перевищує встановлений поріг, транзакція переходить до наступного етапу обробки та може бути використана для формування нового блока.

На відміну від більшості існуючих реалізацій Blockchain, де перевірка транзакцій фактично завершується під час майнінгу, запропонований алгоритм використовує дворівневий механізм підтвердження. Спочатку здійснюється незалежна розподілена валідація транзакції, після чого виконується її колективне підтвердження, і лише після цього запускається алгоритм консенсусу. Така організація процесу дозволяє підвищити достовірність інформації, скоротити кількість конфліктних ситуацій та зменшити навантаження на систему консенсусу.

Після завершення процедури розподіленої валідації та колективного підтвердження інформаційних транзакцій система переходить до етапу формування нового блока. На цьому етапі до подальшої обробки допускаються лише транзакції, які успішно пройшли всі попередні перевірки та отримали достатню кількість підтверджень від активних вузлів мережі. Такий підхід дозволяє мінімізувати ймовірність включення до блокчейна недостовірних або конфліктних даних і підвищує ефективність роботи механізму консенсусу.

Для забезпечення узгодженості стану розподіленої мережі використано алгоритм консенсусу Proof of Work (PoW) (рис. 2). Його використання забезпечує криптографічний захист ланцюга блоків та унеможливлює модифікацію вже підтверджених даних без повторного виконання значного обсягу обчислень. Оскільки кожний блок містить хеш попереднього блока, будь-яка зміна інформації призводить до порушення цілісності всього ланцюга. Таким чином забезпечується незмінність даних після їх підтвердження мережею.

```python
def valid_proof(self, last_proof, proof):
    guess = f'{last_proof}{proof}'.encode()
    guess_hash = hashlib.sha256(guess).hexdigest()
    if guess_hash[:4] == "0000":
        print('proof:', proof)
        print('lastproof:', last_proof)
    return guess_hash[:4] == "0000"
```

Рис. 2. Алгоритм Proof of Work

Особливістю нашого алгоритму є додатковий етап розподіленого підтвердження результатів Proof of Work. У більшості існуючих блокчейн-систем вузол, який першим знаходить допустиме значення *proof*, одразу формує новий блок та передає його іншим учасникам мережі. Запропонований алгоритм доповнює цей процес процедурою незалежної перевірки знайденого рішення всіма активними вузлами. Після отримання результату кожний вузол повторно виконує перевірку правильності обчислення та підтверджує або відхиляє запропоноване рішення.

Для координації процесу підтвердження використовується спеціалізована структура даних, у якій накопичуються результати перевірки, отримані від усіх вузлів мережі. Для кожного кандидата на створення нового блока зберігаються ідентифікатор вузла, знайдене значення *proof*, часові мітки створення повідомлення та результати перевірки іншими учасниками. Такий підхід забезпечує узгоджене прийняття рішення щодо формування нового блока та виключає можливість його одноосібного створення.

Окрему увагу приділено ситуації одночасного знаходження допустимого рішення кількома вузлами мережі. У запропонованому алгоритмі така ситуація вирішується шляхом аналізу часових міток отриманих повідомлень. Перевага надається вузлу, який першим завершив обчислення та передав підтверджене рішення іншим учасникам мережі. Це дозволяє уникнути утворення паралельних гілок блокчейна та забезпечує єдиний узгоджений стан ланцюга даних у всіх вузлах.

Після завершення процедури підтвердження формується новий блок, який містить порядковий номер, часову мітку створення, список підтверджених транзакцій, значення *proof* та криптографічний хеш попереднього блока. Збереження хешу попереднього блока формує безперервний ланцюг взаємопов'язаних записів, що гарантує цілісність усієї історії збережених даних.

Для підтримання працездатності розподіленої мережі алгоритм містить механізм автоматичного контролю активності вузлів. У процесі обміну службовими повідомленнями контролюється доступність кожного учасника мережі. Якщо вузол не відповідає протягом визначеного інтервалу часу, він тимчасово виключається із процесу консенсусу. Після відновлення зв'язку вузол автоматично синхронізує локальну копію блокчейна із мережею та поновлює участь у підтвердженні транзакцій і формуванні нових блоків. Такий механізм забезпечує високу відмовостійкість системи та дозволяє підтримувати її працездатність навіть за часткової втрати окремих вузлів.

Практичну реалізацію запропонованого алгоритму виконано у вигляді програмного комплексу з відкритою архітектурою. Серверна частина реалізована мовою Python із використанням фреймворку Flask, який забезпечує взаємодію між вузлами через REST API. Передбачено окремі програмні інтерфейси для реєстрації вузлів, передавання інформаційних транзакцій, виконання розподіленої валідації, обміну результатами консенсусу та синхронізації блокчейна. Модульна структура програмної реалізації дозволяє інтегрувати запропонований алгоритм до різних інформаційних систем без зміни його базових механізмів.

Для забезпечення оперативного обміну інформацією між серверною та клієнтською частинами застосовано технологію WebSocket, яка забезпечує двосторонній зв'язок у режимі реального часу (рис. 3). Завдяки цьому всі зміни стану мережі, результати підтвердження транзакцій та процес формування нових блоків миттєво відображаються користувачам без необхідності періодичного опитування сервера. Такий підхід зменшує мережеве навантаження та підвищує швидкодію системи.

```python
@app.route('/transactions/new', methods=['POST'])
def new_transaction():
    values = request.get_json()
    transaction = values.get('transaction')
    sender = values.get('sender')


    required = ['sender', 'recipient', 'amount']
    if not all(k in transaction for k in required):
        return 'Missing values', 400


    print("транзакція залетіла", values)
    response = blockchain.transaction_validator(transaction['sender'], transaction['recipient'], transaction['amount'])

    call_data({
        "nodes": list(blockchain.nodes),
        "chain": list(blockchain.chain),
        "call_info": {
            "node_sender": sender,
            "node_recipient": self_node_adress,
            },
        "voting_results": list(blockchain.voteCalculator())
        })

    return jsonify(response), 201
```

Рис. 3. Маршрут transaction/new

Для перевірки працездатності запропонованого алгоритму розроблено експериментальну платформу електронного онлайн-голосування, яка використовує всі описані механізми розподіленої валідації, колективного підтвердження транзакцій, алгоритму Proof of Work та синхронізації вузлів. У межах цієї платформи транзакція містить інформацію про вибір користувача, однак запропонований алгоритм не залежить від типу даних, що передаються. Завдяки цьому він може бути використаний як універсальна основа для побудови різноманітних розподілених інформаційних систем, у яких необхідно забезпечити захищене збереження, передавання та підтвердження достовірності даних.

Висновки та перспективи подальших досліджень. У роботі представлено розроблений блокчейн-алгоритм, призначений для побудови розподілених систем захищеного збереження та передавання даних без використання централізованого органу керування. Запропонований алгоритм базується на децентралізованій архітектурі та поєднує механізми розподіленої валідації інформаційних транзакцій, їх колективного підтвердження, алгоритму консенсусу Proof of Work і синхронізації вузлів мережі.

На відміну від традиційних підходів, алгоритм реалізує багатоетапну процедуру підтвердження транзакцій, за якої перед запуском алгоритму консенсусу здійснюється незалежна розподілена валідація та колективне підтвердження інформаційних транзакцій. Це дозволяє зменшити навантаження на механізм консенсусу, підвищити достовірність оброблюваних даних і мінімізувати ймовірність включення некоректних транзакцій до блокчейна. Запропонований підхід забезпечує цілісність, незмінність і прозорість процесів обробки інформації, а також підвищує відмовостійкість системи завдяки відсутності єдиного центру керування та використанню механізму автоматичної синхронізації вузлів. Практичну працездатність алгоритму підтверджено шляхом його реалізації у вигляді програмного комплексу з відкритою архітектурою та апробації на експериментальній платформі електронного онлайн-голосування. Отримані результати свідчать про можливість використання запропонованого алгоритму як універсальної основи для побудови широкого класу розподілених інформаційних систем, у яких критично важливими є захист, достовірність і цілісність даних.

Подальші дослідження доцільно спрямувати на підвищення масштабованості та продуктивності запропонованого алгоритму під час функціонування у великих розподілених мережах. Перспективними напрямами є оптимізація механізму консенсусу шляхом використання альтернативних алгоритмів (наприклад, Proof of Stake або Practical Byzantine Fault Tolerance), дослідження адаптивного керування складністю підтвердження транзакцій залежно від поточного навантаження мережі, а також інтеграція алгоритму зі смарт-контрактами та розподіленими файловими системами. Окремий інтерес становить експериментальне оцінювання продуктивності, відмовостійкості та рівня інформаційної безпеки запропонованого алгоритму для різних предметних областей, зокрема систем електронного документообігу, хмарних сервісів, Інтернету речей та медичних інформаційних систем.

Список літератури

1. Bashir I. Mastering Blockchain. Distributed ledger technology, decentralization, and smart contracts explained. 2nd ed. BIRMINGHAM-MUMBAI : Packt Publishing Ltd, 2018. 910 p.
2. Bin Saif M., Migliorini S., Spoto F. Efficient and Secure Distributed Data Storage and Retrieval Using Interplanetary File System and Blockchain. Future Internet. 2024. Vol. 16, no. 3. P. 98. URL: https://doi.org/10.3390/fi16030098 (date of access: 25.05.2026).
3. Construction of a secure storage and sharing model for medical data under computer network technology / P. Yin et al. Applied Mathematics and Nonlinear Sciences. 2023. URL: https://doi.org/10.2478/amns.2023.2.00888 (date of access: 25.05.2026).
4. Cui S., Wang H. Blockchain-based data sharing algorithm in distributed network data storage. Journal of Computational Methods in Sciences and Engineering. 2024. Vol. 24, no. 1. P. 427–444. URL: https://doi.org/10.3233/jcm-237038 (date of access: 25.05.2026).
5. Data storage mechanism of industrial IoT based on LRC sharding blockchain / Y. Ren et al. Scientific Reports. 2023. Vol. 13, no. 1. URL: https://doi.org/10.1038/s41598-023-29917-x (date of access: 25.05.2026).
6. Goint M., Bertelle C., Duvallet C. Secure Access Control to Data in Off-Chain Storage in Blockchain-Based Consent Systems. Mathematics. 2023. Vol. 11, no. 7. P. 1592. URL: https://doi.org/10.3390/math11071592 (date of access: 25.05.2026).
7. Gupta P. K., Shellamurthu S. "BLOCKCHAIN AND DECENTRALIZED TECHNOLOGIES", Int. J. Sci. Inno. Eng., vol. 2, no. 9, pp. 601–608, Sep. 2025, doi: 10.70849/IJSCI.
8. Huang J., Yi J. The key security management scheme of cloud storage based on blockchain and digital twins. Journal of Cloud Computing. 2024. Vol. 13, no. 1. URL: https://doi.org/10.1186/s13677-023-00587-4 (date of access: 25.05.2026).
9. Investigation of personal data protection mechanism based on blockchain technology / R. Zhu et al. Scientific Reports. 2023. Vol. 13, no. 1. URL: https://doi.org/10.1038/s41598-023-48661-w (date of access: 25.05.2026).
10. Tmeizeh M., Rodríguez-Domínguez C., Hurtado-Torres M. V. File chunking towards on-chain storage: a blockchain-based data preservation framework. Cluster Computing. 2024. URL: https://doi.org/10.1007/s10586-024-04646-6 (date of access: 25.05.2026).
11. Yakubu B. M., Sabi'u J., Bhattarakosol P. Blockchain-based privacy and security model for transactional data in large private networks. Scientific Reports. 2023. Vol. 13, no. 1. URL: https://doi.org/10.1038/s41598-023-44101-x (date of access: 25.05.2026).

References

1. Bashir I. Mastering Blockchain. Distributed ledger technology, decentralization, and smart contracts explained. 2nd ed. BIRMINGHAM-MUMBAI : Packt Publishing Ltd, 2018. 910 p.
2. Bin Saif M., Migliorini S., Spoto F. Efficient and Secure Distributed Data Storage and Retrieval Using Interplanetary File System and Blockchain. Future Internet. 2024. Vol. 16, no. 3. P. 98. URL: https://doi.org/10.3390/fi16030098 (date of access: 25.05.2026).
3. Construction of a secure storage and sharing model for medical data under computer network technology / P. Yin et al. Applied Mathematics and Nonlinear Sciences. 2023. URL: https://doi.org/10.2478/amns.2023.2.00888 (date of access: 25.05.2026).
4. Cui S., Wang H. Blockchain-based data sharing algorithm in distributed network data storage. Journal of Computational Methods in Sciences and Engineering. 2024. Vol. 24, no. 1. P. 427–444. URL: https://doi.org/10.3233/jcm-237038 (date of access: 25.05.2026).
5. Data storage mechanism of industrial IoT based on LRC sharding blockchain / Y. Ren et al. Scientific Reports. 2023. Vol. 13, no. 1. URL: https://doi.org/10.1038/s41598-023-29917-x (date of access: 25.05.2026).
6. Goint M., Bertelle C., Duvallet C. Secure Access Control to Data in Off-Chain Storage in Blockchain-Based Consent Systems. Mathematics. 2023. Vol. 11, no. 7. P. 1592. URL: https://doi.org/10.3390/math11071592 (date of access: 25.05.2026).
7. Gupta P. K., Shellamurthu S. "BLOCKCHAIN AND DECENTRALIZED TECHNOLOGIES", Int. J. Sci. Inno. Eng., vol. 2, no. 9, pp. 601–608, Sep. 2025, doi: 10.70849/IJSCI.
8. Huang J., Yi J. The key security management scheme of cloud storage based on blockchain and digital twins. Journal of Cloud Computing. 2024. Vol. 13, no. 1. URL: https://doi.org/10.1186/s13677-023-00587-4 (date of access: 25.05.2026).
9. Investigation of personal data protection mechanism based on blockchain technology / R. Zhu et al. Scientific Reports. 2023. Vol. 13, no. 1. URL: https://doi.org/10.1038/s41598-023-48661-w (date of access: 25.05.2026).
10. Tmeizeh M., Rodríguez-Domínguez C., Hurtado-Torres M. V. File chunking towards on-chain storage: a blockchain-based data preservation framework. Cluster Computing. 2024. URL: https://doi.org/10.1007/s10586-024-04646-6 (date of access: 25.05.2026).
11. Yakubu B. M., Sabi'u J., Bhattarakosol P. Blockchain-based privacy and security model for transactional data in large private networks. Scientific Reports. 2023. Vol. 13, no. 1. URL: https://doi.org/10.1038/s41598-023-44101-x (date of access: 25.05.2026).

Історія статті:
Отримано: 27.05.2026 Доопрацьовано: 12.09.2026 Прийнято до друку: 23.09.2026 Опубліковано: 29.09.2026