**Vol. 6, No. 2, 2024**

DOI: https://doi.org/10.23939/csn2024.02.082

**УДК 004.75**

# АНАЛІЗ ОСОБЛИВОСТЕЙ БЕЗПЕЧНОЇ ОБРОБКИ ДАНИХ В ТЕХНОЛОГІЇ БЛОКЧЕЙНУ НА ОСНОВІ ЕКСПЕРИМЕНТАЛЬНОЇ МЕРЕЖІ ОБМІНУ ТРАНЗАКЦІЯМИ

**О. О. Іванюк, Н. С. Денисенко**

Національний університет "Львівська політехніка",
кафедра комп'ютеризованих систем автоматики
*E-mail: oleh.o.ivaniuk@lpnu.ua, Nikita.Denysenko.mKNUO.2022@lpnu.ua*



**У статті зроблено акцент на дослідженні роботи технології блокчейну на рівні даних, а саме проаналізовано механізми безпечного обміну транзакціями. Розглянуто розподілену структуру блокчейн-мережі, побудовану на основі послідовності блоків, котрі містять дані транзакцій. Описано фундаментальні особливості роботи технології блокчейну, а також 6-компонентну багатошарову архітектуру блокчейну. Показано важливість застосування криптографічних хеш-функцій для забезпечення безпеки і цілісності даних у блокчейн-мережі.**

**З метою симуляції процесу обміну транзакціями між користувачами мережі створено експериментальну блокчейн-аплікацію. Це дало змогу наочно показати особливості використання таких криптоінструментів, як публічний і приватний ключі та цифровий підпис для вирішення проблеми несанкціонованих транзакцій. Проведено аналіз продуктивності експериментальної блокчейн-мережі при різних значеннях складності видобування блока.**

**Ключові слова: блокчейн, блок, рівень даних, захист даних, хеш-функція, транзакція, публічний ключ, приватний ключ, цифровий підпис.**

## Вступ

Технологія блокчейну, що функціонує на базі розподіленої системи цифрових реєстрів, стала ключовим інноваційним рішенням у світі фінансів, перетворюючи та удосконалюючи традиційні методи обробки фінансових операцій. Цей новітній напрямок розвитку цифрових технологій роботи з даними став об'єктом інтенсивного вивчення та досліджень, оскільки його потенціал відкриває широкі перспективи для покращення ефективності, безпеки та прозорості у багатьох сферах, зокрема у фінансовому секторі.

Існує думка, що технологія блокчейну, завдяки своїй внутрішній структурі, є практично нечутливою до загроз безпеки. Хоча така точка зору, звісно, є надто оптимістичною, водночас блокчейн володіє рядом потужних властивостей безпеки. Ключовим для забезпечення безпеки технології блокчейну є застосування криптографічних засобів, які гарантують цілісність та конфіденційність даних транзакцій. Такі інструменти, як криптографічні ключі використовують для шифрування та дешифрування даних, забезпечуючи безпеку транзакцій в мережі. Ця стаття фокусуватиметься на дослідженні особливостей роботи саме цих засобів безпеки. Ще одним важливим безпековим механізмом для блокчейну є алгоритми консенсусу Proof of Work (PoW) і Proof of Stake (PoS), що забезпечують згоду всіх вузлів мережі щодо стану блокчейну. Ці алгоритми

вводять набори правил, які регламентують процес додавання блоку в ланцюг мережі й унеможливлюють маніпуляції зловмисників реєстром. На відміну від централізованих систем, які є вразливими через збій у точці управління мережею, блокчейн-мережі – децентралізовані. Така структура розподіляє дані між вузлами мережі, що суттєво зменшує ризик критичного збою в одній конкретній точці, адже навіть у випадку, якщо буде скомпроментовано кілька вузлів, мережа продовжить працювати коректно.

Також варто зазначити, що для нетехнічних людей архітектура технології блокчейну може бути досить складною для розуміння, що може ускладнювати її широке впровадження. Ця робота ставить на меті на прикладі дослідження роботи експериментальної блокчейн-мережі наочно пояснити, як на основі криптографії досягається надійність та безпека транзакцій.

## Огляд літературних джерел

У роботі [1] досліджується питання забезпечення безпеки даних і захисту конфіденційності під час транзакцій блокчейну, одночасно підвищуючи ефективність транзакцій і надійність. Пропонується метод захисту конфіденційності для транзакцій блокчейну на основі полегшеного гомоморфного шифрування. Побудовано інфраструктуру блокчейну і, ґрунтуючись на її структурних характеристиках, прийнято технологію доказу з нульовим розголошенням для перевірки легітимності даних, гарантуючи справжність і точність транзакцій.

У роботі [2] запропоновано комплексний метод застосування технології блокчейну для забезпечення безпеки в мережі та протидії постійним загрозам, а також зростанню кіберзлочинності та кібератакам. На цій основі авторами розроблено захищену систему журналів, яка надаватиме безпечні та надійні журнали слідчим для хмарної криміналістики. Секретність та конфіденційність користувачів хмари забезпечуються за допомогою методу шифрування з можливістю пошуку.

У літературному джерелі [3] досліджується питання включення технології блокчейну в безпечний життєвий цикл розробки (SDLC) для посилення заходів безпеки протягом усього процесу розробки програмного забезпечення. Блокчейн, який характеризується своєю децентралізованою, прозорою та незмінною природою, пропонує надійну структуру для пом'якшення ризиків, пов'язаних із вразливістю програмного забезпечення, витоком даних і неавторизованим доступом. Дослідження заглиблюється в те, як блокчейн можна легко інтегрувати в кожну фазу SDLC – аналіз вимог, проєктування, впровадження, тестування, розгортання та обслуговування. Вбудовуючи протоколи блокчейну в ці етапи, SDLC може досягти більш високого рівня гарантії безпеки.

У роботі [4] розглянуто можливість інтеграції технології блокчейну і багатофакторної автентифікації (БФА) як додаткових рішень для підвищення безпеки транзакцій і забезпечення цілісності даних на платформах електронної комерції. Окрім безпекових переваг, які надає блокчейн, зазначається, що БФА додає додатковий рівень безпеки, вимагаючи кількох форм перевірки перед наданням доступу до конфіденційної інформації або завершення транзакцій. Інтеграція блокчейну та MFA у системи електронної комерції забезпечує комплексне рішення безпеки, яке стосується як цілісності даних, так і контролю доступу.

У роботі [5] запропонована система переважно зосереджена на забезпеченні безпеки системи блокчейну за допомогою різних механізмів. Розроблена модель складається із системи на основі фінансових транзакцій, яка працює на основі технології RFID. Доступ до даних, отриманих із системи, можуть мати лише авторизовані клієнти, що забезпечує перший рівень безпеки шляхом автентифікації дійсного клієнта за допомогою автентифікації M2M. Після аутентифікації користувача він може отримати доступ до системи транзакцій. Дані транзакцій, які зберігаються в локальній системі, захищаються за допомогою технології блокчейну на основі хешування. Згенерований хеш знову захищається шляхом поділу та зберігання хешу в двох різних місцях.

Автори роботи [6], розглядаючи важливу проблему забезпечення цілісності даних у децентралізованих системах, проводили дослідження ймовірності фальсифікації даних у рамках дерев Меркла, які є ключовими в технологіях блокчейну та Інтернету речей (IoT). Результати показали

зменшення ймовірності фальсифікації зі збільшенням довжини хешу та зворотний зв'язок із довшими шляхами Меркла. Ця робота пропонує важливу інформацію про оптимізацію структур дерев Меркла для посилення безпеки в блокчейні та системах Інтернету речей, досягнення балансу між обчислювальною ефективністю та цілісністю даних.

## Постановка завдання

На прикладі експериментальної блокчейн-мережі проаналізувати особливості процесу безпечного обміну даними, зокрема, дослідити, як за допомогою застосування криптографічних механізмів вирішується проблема несанкціонованих транзакцій**.** Виконати дослідження продуктивності експериментальної блокчейн-мережі при різних значеннях складності видобування блока.

## Особливості технології блокчейну

Блокчейн – це децентралізована база даних, організована в пов'язаний послідовний список блоків. Блоки, як основний компонент блокчейну, зберігають набір дійсних транзакцій, захищених криптографією [4]. Дані транзакцій записуються глобальною розподіленою мережею спеціальних комп'ютерів, які називаються вузлами. У системі блокчейну кожен вузол може ініціювати обмін інформацією та передавати її всім іншим вузлам в мережі.

Вузли мережі використовують минулі транзакції для перевірки поточної транзакції, після успішної перевірки транзакцію додають до поточного блокчейну. Кількість транзакцій агрегується та вставляється в блокчейн-блок залежно від часового вікна. Блок, до прикладу біткойна, може включати в себе в середньому понад 500 транзакцій. Максимальний розмір блока становить приблизно 1 МБ, верхній ліміт, запропонований Сатоші Накамото в 2010 році, був навмисно обмежений в цілях безпеки.

Завдяки використанню криптографічних методів та алгоритмів консенсусу технологія блокчейну гарантує цілісність даних, неможливість перезапису внесеної раніше інформації.

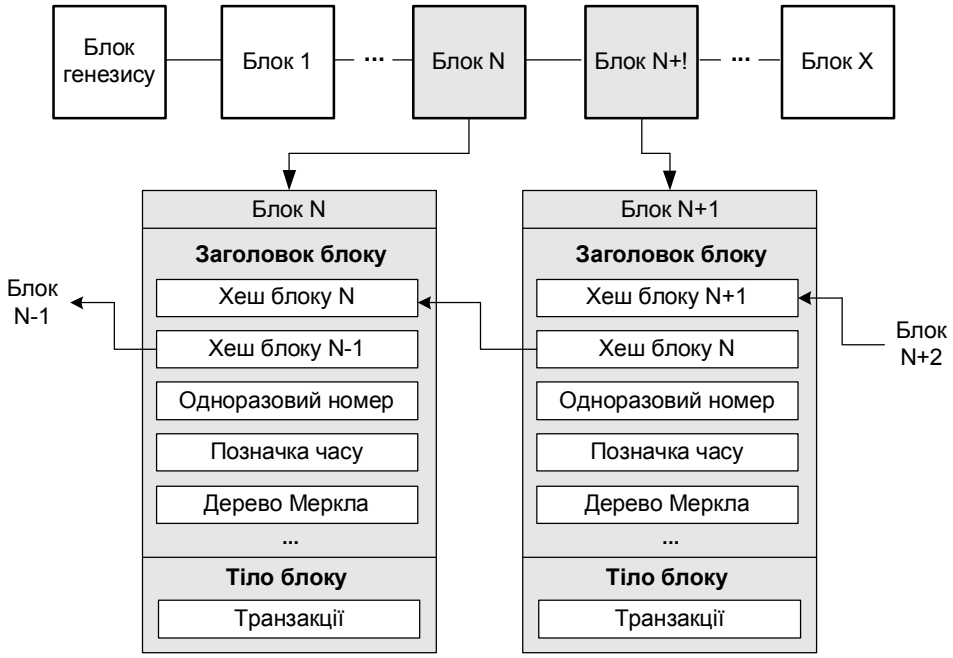


*Рис. 1. Загальна структура блоків у блокчейн-мережі*

Розглянемо більш детально ланцюг блокчейн-мережі із представленням типової структури блоків (рис. 1). Першим блоком у блокчейні є генезис-блок, який ще також називають блоком 0, він є батьківським для всіх наступних блоків у мережі. У структурі блоку виділяють заголовок і тіло.

Заголовок блоку застосовують з метою ідентифікації відповідного блоку в мережі блокчейн. Він складається із таких компонентів:

- хеш блоку – власний унікальний хеш блоку;
- хеш попереднього блоку – це посилання на хеш попереднього в ланцюжку, батьківського блоку;
- одноразовий номер (*nonce*) – це випадкове значення, яке розраховується методом проб і помилок, щоб спробувати різні перестановки для досягнення необхідного рівня складності при генерації блоку;
- позначка часу – фіксує час створення блоку, щоб впорядкувати його в хронологічному порядку;
- дерево (корінь) Меркла – 256-бітовий криптографічний хеш усіх транзакцій, включених до даного блоку, на основі нього користувачі перевіряють можливість включення нової транзакції до блоку.

Тіло блоку містить дані про всі перевірені і додані до блоку транзакції. Зокрема, у транзакціях зберігається інформація про адреси відправника і отримувача криптовалюти, а також суму переказу.

Варто зазначити, що залежно від того чи іншого блокчейну, структура блоку може дещо відрізнятися від наведеної на рис. 1.

Блоки сполучаються один з одним в ланцюг у хронологічній послідовності, на основі включення хешу попереднього заголовка блоку (як показано на рис. 1). Це забезпечує незмінність та стійкість ланцюга мережі до втручання, адже для того, щоб внести зміни в один блок, необхідно виконати оновлення кожного наступного блоку.

Технологія блокчейну характеризується фундаментальними **особливостями децентралізації, прозорості**, **автентичності** та **аудиту**. На відміну від централізованих систем, блокчейн характеризується децентралізацією. Це означає, що мережа розосереджена на багатьох вузлах і жоден вузол не може самостійно контролювати всю мережу. Такий підхід дає змогу побудувати більш стійку і безпечну систему, через відсутність єдиної, центральної точки контролю або відмови. Прозорий та зашифрований дизайн ланцюга блокчейну дає змогу всім вузлам спостерігати за обміном даними між численними блоками мережі. Це забезпечує членам мережі можливість простішого відстеження і перевірки транзакцій. На початку кожної нової транзакції кожна компетентна база даних співпрацює з усіма іншими базами даних для створення нового блоку з необхідними характеристиками. База даних, яка успішно вирішує математичне кодування і створює блок, перемагає. Цей блок перевіряється та автентифікується іншими блоками. Після того, як всі блоки підтвердять транзакцію, дані шифруються, але прозоро зберігаються в базі даних. Для кожного блоку автентифікація та аудит запускаються автоматично і працюють у фоновому режимі. Завдяки тому, що кожен блок зберігає хеш попереднього, блоки об'єднуються у відповідну хронологічну, лінійну послідовність. Історія транзакцій залишається доступною в інших блоках навіть у разі несанкціонованого видалення або вторгнення в початковий блок транзакцій.

**Архітектура блокчейну** включає шість значущих компонентів, інтегрованих в багатошарову структуру блокчейну.

**Апаратний рівень** є верхнім рівнем блокчейну, що функціонує за клієнт-серверною моделлю. В центрі обробки даних на сервері зберігаються дані блокчейну, а клієнти (вузли) під час використання вебдодатків надсилають відповідні запити на сервер, наприклад, для отримання даних. Також апаратний рівень включає віртуальні машини, які працюють як операційні системи та розміщують смарт-контракти.

**Рівень даних** включає в себе пов'язані дані транзакцій блоків та техніки, що супроводжують їх, такі як хеш-алгоритми (наприклад, SHA256), технології відміток часу, асиметричне шифрування (наприклад, алгоритм цифрового підпису еліптичної кривої (ECDSA) та дерева Меркла [6]. Кожен вузол використовує різні стратегії для інкапсуляції транзакцій та отриманих кодів в нові блоки,

включаючи хеш-функцію та дерево Меркла. Кожному блоку присвоюється часова відмітка, яка вказує на час його створення. Після цього новий блок приєднується до ланцюга, підключаючись до початкового блоку [7].

**Рівень мережі.** Мережевий або одноранговий (P2P) рівень відповідає за міжвузлову комунікацію. Він контролює поширення і виявлення блоків та обробку транзакцій. Враховуючи те, що блокчейн-мережа є відкритою системою, кожен вузол має мати достовірні дані про транзакції, які перевіряються іншими вузлами. Мережевий рівень полегшує цю комунікацію.

**Рівень консенсусу** життєво необхідний для існування блокчейн-мережі. Він забезпечує перевірку блоків, їх розміщення у коректній послідовності та гарантує, що між всіма вузлами мережі досягнуто згоди щодо валідності кожної транзакції. Реєстрація нових транзакції можлива лише за згодою більшості вузлів мережі. Цей рівень застосовує кілька алгоритмів консенсусу (таких як PoS та PoW) для забезпечення сталості даних та відмовостійкості в розподілених мережах.

**Рівень стимулювання** дозволяє зміцнити перевірку безпеки блокчейну, пропонуючи конкретні стимули вузлам, що співпрацюють у валідації безпеки. Цей рівень включає економічні винагороди в блокчейні, систему розподілу валюти та механізм випуску валюти, щоб гарантувати, що особи, які допомагають генерувати наступний блок, отримують можливу вигоду [7]. В архітектурі блокчейну рівень стимулювання реалізується не завжди, це залежить від застосованого алгоритму консенсусу.

**Прикладний рівень** є рівнем, де здійснюється розробка та розгортання додатків блокчейну, таких як смарт-контракти, ланцюжковий код і децентралізовані програми (DApps). Розробники мають змогу створювати нові сервіси та програми, які базуються на прозорості та безпеці технології блокчейну. Спектр таких програмних рішень може бути доволі широкий: застосунки для соціальних мереж, браузери, гаманці, застосунки Defi та платформи NFT. Незважаючи на те, що користувацький інтерфейс таких програм зазвичай подібний до інтерфейсу будь-якої іншої стандартної програми, серверне зберігання даних цих програм децентралізоване.

## Криптографічні хеш-функції

Використання криптографічних хеш-функцій є важливою складовою технології блокчейну. Для багатьох операцій хешування є методом застосування криптографічної хеш-функції до даних, що обчислює відносно унікальний вихід (називається контрольною сумою) фіксованої довжини для вхідних даних практично будь-якого розміру (наприклад, файлу, тексту чи зображення). Це дозволяє учасникам незалежно взяти вхідні дані, захешувати ці дані та одержати той самий результат, доводячи, що в даних не було змін. Навіть найменша зміна у вхідних даних (наприклад, зміна одного біта) призведе до повністю відмінної вихідної контрольної суми.

Криптографічні хеш-функції мають такі важливі **властивості безпеки.**

**Стійкість до знаходження попереднього образу**. Це здатність хеш-функції не розкривати жодної інформації про вхідні дані. Математично це означає, що криптографічні хеш-функції є односторонніми; обчислення правильного значення входу, виходячи з певного вихідного значення (попереднього образу), є обчислювально неможливим (наприклад, задано контрольну суму, знайти *x* таке, що *hash (x)* = контрольна_сума).

**Стійкість до знаходження другого попереднього образу**. Це означає, що неможливо знайти вхід, який хешується у конкретний вихід. Зокрема, криптографічні хеш-функції розроблені так, щоб за допомогою конкретного введення було обчислювально неможливо знайти друге введення, яке виробляє той самий вихід (наприклад, задано *x*, знайти у таке, що *hash (x) = hash (y)*. Єдиний підхід – це виснажливий пошук простору введення, але це обчислювально неможливо зробити з якимнебудь шансом на успіх.

**Стійкість до колізій**. Це означає, що неможливо знайти два входи, які хешуються в однаковий вихід. Зокрема, обчислювально неможливо знайти два входи, які виробляють однаковий хеш (наприклад, знайти *x* і *y* такі, що *hash (x) = hash (y)*.

Конкретною криптографічною хеш-функцією, яку використовують у багатьох реалізаціях блокчейну, є безпечний хеш-алгоритм (Secure Hash Algorithm, SHA) з розміром вихідних даних 256 бітів (SHA-256). Багато комп'ютерів підтримують цей алгоритм апаратно, що робить його швидким для обчислення. Алгоритм SHA-256 має вихідний розмір 32 байти (32 байти = 256 бітів) і, як правило, відображається як 64-знаковий шістнадцятковий рядок (табл. 1). Це означає, що існує 2^256, що приблизно дорівнює 10^77, або 115,792,089,237,316,195,423,570,985,008,687,907,853, 269,984,665,640,564,039,457,584,007,913,129,639,936 можливих значень контрольної суми. Алгоритм для SHA-256, а також інших, визначений у Федеральному стандарті обробки інформації (Federal Information Processing Standard, FIPS) 180-4 [8]. На вебсайті безпечного хешування Національного інституту стандартів і технологій (National Institute of Standards and Technology, NIST) містяться специфікації FIPS для всіх схвалених NIST хеш-алгоритмів.

*Таблиця 1*

**Зразки вхідних даних та відповідних вихідних значень контрольної суми SHA-256**

| Вхідні дані | Вихідні дані (SHA-256) |
|---|---|
| Transaction data | 9a61299ef2bbfc27cabba3f6dca0311618e9f72721a60dc1e2ba2bc50bfe970a |
| Transaction data | 9a61299ef2bbfc27cabba3f6dca0311618e9f72721a60dc1e2ba2bc50bfe970a |
| transaction data | 86d9050926fde112924e2f71ea8d17b88d90068f39c9907bb3932c2df3c46dfc |
| data | 3a6eb0790f39ac87c94f3856b2dd2c5d110e6811602261a9a923d3bb23adc8b7 |

У табл. 1 наведено приклад вхідних даних, оброблених хеш-алгоритмом SHA-256. Можна побачити, що одним і тим самим вхідним даним завжди будуть відповідати ті самі вихідні дані. Проста зміна регістру літер вхідних даних призводить до цілком інших вихідних даних. Для вхідних даних різної довжини завжди буде генеруватися вихід однакової довжини. Важливо наголосити, що хеш-функції є лише односторонніми: на основі результату хешування неможливо відновити вхідні дані.

**Результати дослідження**

Для тестової блокчейн-аплікації використовується вебдодаток, написаний мовою JavaScript, який надає інструментарій для симуляції процесу обміну транзакціями між користувачами [9]. Запропоновано відповідні скрипти для реалізації хеш-функцій та виведенням результатів на HTML сторінку.

Використана для дослідження бібліотека CryptoJS [10] пропонує колекцію безпечних криптографічних алгоритмів. Зокрема, надається ряд актуальних алгоритмів хешування, таких як MD5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, KECCAK (SHA-3). У межах цього дослідження використовували алгоритм хешування SHA-256, який добре зарекомендував себе в блокчейні біткойна.

Розгорнута експериментальна аплікація надає інструменти для тестування роботи блокчейн-мережі з різними параметрами заголовка блоку. Передбачено налаштовування складності видобування (майнінгу) блока мережі шляхом завдання необхідної кількості нулів на початку його хешу. Також надається можливість встановлювати значення одноразового номеру (*maximumNonce*) для обмеження часу тривалості майнінгу блоку. У ході цього дослідження, при заданому параметрі складності *difficultyMajor* = 4, було згенеровано хеш, який починається з 0000, а значення параметру одноразового номера *maximumNonce* становить 8·16^4 = 524288. Встановлено, що збільшення на порядок значення одноразового номера призводить до відповідного суттєвого зростання часу тривалості видобування блоку.

Наведена на рис. 2 програма реалізована за допомогою бібліотеки CryptoJS, яка надає необхідні інструменти для роботи з хеш-функціями. Зокрема, функція *sha256()* на основі алгоритму SHA256 виконує обчислення хешу вмісту конкретного блоку у вказаному ланцюгу. Такий підхід

гарантує унікальний цифровий відбиток для кожного блоку, що є необхідним для забезпечення незмінності блокчейну. Функції *updateState(), updateHash()* та *updateChain()* відповідають за візуальне оновлення стану карти блоку, оновлення значення хешу та синхронізацію блокчейну відповідно. Це включає в себе визначення успішності чи помилки блоку на основі умов, заданих хешу, а також перевірку та оновлення попередніх хешів для всіх блоків у ланцюгу.

```
function sha256(block, chain) {
  // calculate a SHA256 hash of the contents of the block
  return CryptoJS.SHA256(getText(block, chain));
}

function updateState(block, chain) : void  {
  // set the card background red or green for this block
  if ($('#block'+block+'chain'+chain+'hash').val().substr( from: 0, difficulty) === pattern) {
    $('#block'+block+'chain'+chain+'card').removeClass( a: 'card-error').addClass( a: 'card-success');
  }
  else {
    $('#block'+block+'chain'+chain+'card').removeClass( a: 'card-success').addClass( a: 'card-error');
  }
}

function updateHash(block, chain) : void  {
  // update the SHA256 hash value for this block
  $('#block'+block+'chain'+chain+'hash').val(sha256(block, chain));
  updateState(block, chain);
}

function updateChain(block, chain, txCount) : void  {
  // update all blocks walking the chain from this block to the end
  for (var x = block; x <= 5; x++) {
    if (x > 1) {
      $('#block'+x+'chain'+chain+'previous').val($('#block'+(x-1).toString()+'chain'+chain+'hash').val());
    }
    updateHash(x, chain);
    if (txCount)
      for (var y : number =0; y<txCount; y++)
        verifySignature(block, chain, y);
  }
```

*Рис. 2. Скрипт, що відповідає за роботу хеш-функцій*

При роботі з блокчейном виникає проблема несанкціонованих транзакцій, коли, наприклад, хтось захотів би додати транзакцію, яка надсилає собі чиїсь кошти. Для вирішення цього питання був розроблений механізм, який запобігає створенню будь-ким несанкціонованих транзакцій. Для цього використовується криптографічний примітив, який називається пара публічних /приватних ключів (Public / Private Keys), які використовують для підпису (рис. 3). Приватний ключ є конфіденційним, відомим тільки його власнику, не повідомляється стороннім особам і використовується для підписування даних, забезпечуючи конфіденційність та автентифікацію власника. Публічний ключ генерується відповідно до приватного ключа і не є конфіденційним, розповсюджується відкрито між іншими особами. Будь-який учасник мережі з публічним ключем може перевірити підписувача транзакції, яка була підписана за допомогою приватного ключа.

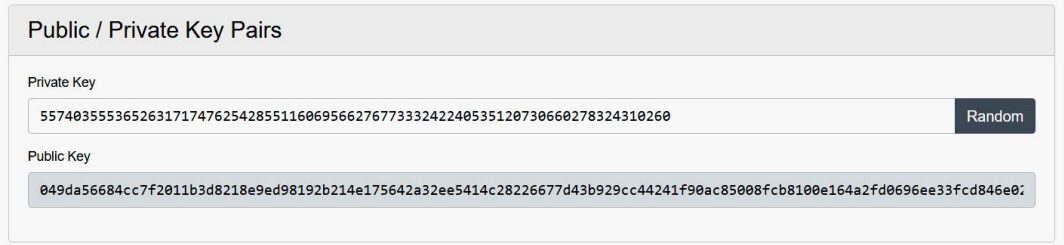


*Рис. 3. Результат генерації публічного і приватного ключів*


*Рис. 4. Підпис транзакції приватним ключем*

На рис. 4 показано, як відбувається процес підпису повідомлення *Message* (наприклад, фінансової транзакції) приватним ключем *Private Key*, в результаті чого формується підпис повідомлення *Message Signature*. Цей підпис повідомлення може бути наданий іншому учаснику мережі для перевірки (опція *Verify*) повідомлення *Message*. Так особа, яка має відкритий, публічний ключ відправника та підпис повідомлення, може верифікувати, чи *Message* є валідним. Кожна проведена транзакція супроводжується цифровим підписом, який підтверджує контроль валідного приватного ключа, не розкриваючи його, забезпечуючи таким чином безпеку.

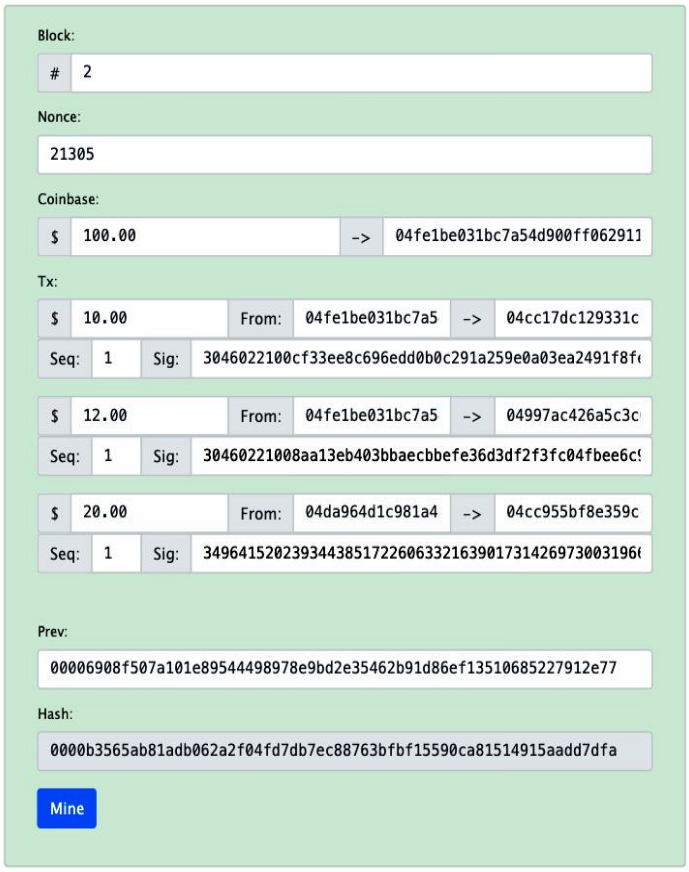


*Рис. 5. Блок з даними транзакцій*
*в експериментальній блокчейн-мережі*

На рис. 5 представлено створений, з вище зазначеними налаштуваннями, 2-й блок мережі, який містить дані транзакцій експериментальної блокчейн-аплікації. Повідомленням в цьому випадку є значення суми переказу в доларах США (поля *Coinbase* і *Tx*), яке надсилається від відправника з публічним ключем *From* до отримувача з публічним ключем ->. Коли відправник підтверджує транзакцію, відбувається її підписання приватним ключем відправника і створюється *Підпис повідомлення Sig*. Отримувач, володіючи публічним ключем відправника і *Підписом повідомлення,* виконує верифікацію транзакції і валідність приватного ключа відправника. В полі підпис *Sig* міститься цифровий підпис, який підтверджує валідність відповідної транзакції. У випадку, коли хтось спробує змінити суму, наприклад, першої транзакції з 10 на 100 $, то це призведе до руйнування блоку (в даній аплікації колір фону блоку набуде червоного кольору), а також до невалідності підпису *Sig*. Більше того, зміни в одному блоці роблять всі наступні за ним блоки невалідними. У цьому випадку було успішно створено блок та додано до нього відповідні дані транзакцій.

Створена за описаним підходом, хронологічна послідовність блоків утворює блокчейн-мережу.

Такий підхід дає можливість створювати захищені блокчейн-системи, де учасникам для обміну транзакціями достатньо згенерувати унікальний публічний і приватний ключ, без необхідності звернення до централізованих органів влади.

**Аналіз продуктивності експериментальної блокчейн-мережі.** Для оцінки продуктивності експериментальної блокчейн-мережі було обрано такі метрики, як транзакції в секунду, час виконання і час блоку. **Транзакції в секунду TPS** (Transactions Per Second) – це показник, який вимірює кількість транзакцій, які упаковуються та зберігаються в блоці мережі за одиницю часу. **Час виконання** – це загальна кількість часу в секундах, протягом якого блокчейн-платформі вдалося виконати та підтвердити всі транзакції в наборі даних. **Час блоку** – час, необхідний для створення одного блоку мережі.

Апаратно-програмна платформа, на якій проводилися експерименти: 8-ядерний процесор Intel Core i7-13700H 5 GHz, 32 ГБ оперативної пам’яті, жорсткий диск SSD на 1000 ГБ, під керуванням Windows 11. Аналіз продуктивності виконувався для різних значень параметра складності видобування блока мережі з використанням алгоритму хешування SHA-256. Тестування часу виконання здійснювалося в сценарії проведення coinbase-транзакцій.

*Таблиця 2*

**Оцінка продуктивності експериментальної блокчейн-мережі**

| Складність видобування блока | Транзакцій в секунду TPS | Час виконання, с | Час блока, с |
|---|---|---|---|
| 2 | 5,95 | 2,35 | 0,26857 |
| 3 | 4,34 | 3,22 | 0,5725 |
| 4 | 1,53 | 10,43 | 1,29375 |
| 5 | 0,26 | 53,23 | 12,58 |

У табл. 2 наведені середні для серії експериментів значення показників продуктивності тестової мережі. Час виконання і час блоку зростають при збільшенні параметра складності мережі. Водночас при цьому кількість транзакцій в секунду TPS зменшується. Значне зменшення значення TPS спостерігається при рівні складності мережі 5 і вище. Дослідження показали, що на рівні складності 6 тестована аплікація може втрачати стабільність і процес видобування блоку може виходити з-під контролю. Із зростанням складності видобування блоків відбувається збільшення значення одноразового номера nonce. Наприклад, якщо на 4-му рівні складності мережі першим спрацьовуючим nonce є 72608, на 5-му рівні – 134816, то на 6-й складності значення одноразовго номера вже становить 8719932.

## Висновки

З метою аналізу процесу безпечної обробки даних в технології блокчейну проведено програмну симуляцію блокчейн-мережі для обміну транзакціями. Розгорнута з використанням бібліотеки CryptoJS експериментальна аплікація дає можливості для тестування основних етапів створення блоку мережі з різними параметрами його заголовка. Розглянуто особливості створення і роботи в блокчейні таких криптографічних інструментів, як хеш-функції, публічні та приватні ключі, цифровий підпис. Показано, що для коректної ідентифікації транзакцій в блокчейні застосовуються криптографічні хеш-функції. З огляду на високу надійність і широку апаратну підтримку, доцільним є використання для хешування вхідних даних 256-бітового алгоритму SHA-256. Розглянуто ключові криптографічні засоби протидії несанкціонованим транзакціям в мережі. Показано, як публічний і приватний ключі забезпечують створення цифрового підпису кожної транзакції, який гарантує автентичність інформації, яка передається мережею. Спільне застосування зазначених інструментів дає змогу забезпечити високу конфіденційність, цілісність та безпеку даних транзакцій, що зберігаються в блокчейні. Проведено аналіз продуктивності експериментальної блокчейн-мережі, який показав, що при зростанні значення складності видобування блока знижується кількість транзакцій в секунду, а час виконання і блока збільшуються. Експериментальна аплікація є простою в розгортанні і може бути використана для інтерактивного ознайомлення та тестування ключових концепцій блокчейну. Позитивною стороною є можливість аналізу різних механізмів і сценаріїв функціонування блокчейну, починаючи від особливостей застосування криптографічних інструментів до процесу проведення coinbase-транзакцій.

## Список літератури

*1. Wang G., Li C., Dai B., Zhang S. (2024). Privacy-Protection Method for Blockchain Transactions Based on Lightweight Homomorphic Encryption. Information 2024, 15, 438. DOI: https://doi.org/10.3390/ info15080438*

*2. Farhana A., Nisha A, Harikrishnan S. (2024). Adoption of Blockchain in Cyber Security. International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume 4, Issue 2, p. 353–360, August 2024, DOI: http://dx.doi.org/10.48175/IJARSCT-19429*

*3. Gajbhiye B., Jain S., Chhapola A. (2024). Secure SDLC: Incorporating Blockchain for Enhanced Security. Scientific Journal of Metaverse and Blockchain Technologies, 2(2), p. 97–110. DOI: https://doi.org/10.36676/ sjmbt.v2.i2.40*

*4. Zishan M., Russell S. (2024). Data Privacy and Security in E-commerce: Utilizing Blockchain and Multi-Factor Authentication to Safeguard Transactions. ResearchGate, August 2024, DOI: http://dx.doi.org/10.13140/RG. 2.2.16554.63682*

*5. Kumari S, Farheen S. (2024) Blockchain based data security for financial transaction system. 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2020, p. 829–833. DOI: 10.1109/ICICCS48265.2020.9121108*

*6. Kuznetsov O., Rusnak A., Yezhov A., Kuznetsova K., Kanonik D. and Domin O. (2024) Evaluating the Security of Merkle Trees: An Analysis of Data Falsification Probabilities, Cryptography, vol. 8, no. 3, Art. no. 3, Sep. 2024, DOI: 10.3390/cryptography8030033.*

*7. Salimitari M., Chatterjee M., and Fallah Y.(2020). A survey on consensus methods in Blockchain for resource-constrained IoT networks, Internet of Things, vol. 11, p. 1–23, 2020. DOI:10.36227/techrxiv.12152142*

*8. National Institute of Standards and Technology, "Secure Hash Standard (SHS)", Federal Information Processing Standards (FIPS) Publication 180-4, August 2015. DOI: https://doi.org/10.6028/NIST.FIPS.180-4*

*9. Blockchain Demo. A web-based demonstration of blockchain concepts. [Electronic resource]. Available at: https://github.com/anders94/blockchain-demo/ (Accessed: 05.10.2024)*

*10. Crypto JS. JavaScript library of crypto standards [Electronic resource]. Available at::. https://www.npmjs.com/package/crypto-js (Accessed: 05.10.2024)*

# ANALYSIS OF THE FEATURES OF SECURE DATA PROCESSING IN BLOCKCHAIN TECHNOLOGY BASED ON AN EXPERIMENTAL TRANSACTION EXCHANGE NETWORK

**O. Ivaniuk, N. Denysenko**

Lviv Polytechnic National University,
Department of computerized automation systems
*E-mail: oleh.o.ivaniuk@lpnu.ua, Nikita.Denysenko.mKNUO.2022@lpnu.ua*



**The article focuses on the study of blockchain technology at the data layer, namely, the mechanisms for secure exchange of transactions are analyzed. The distributed structure of the blockchain network, built on the basis of a sequence of blocks containing transaction data, is considered. The fundamental features of the blockchain technology are described, as well as the 6-component multilayer blockchain architecture. The importance of using cryptographic hash functions to ensure the security and integrity of data in a blockchain network is shown.**

**In order to simulate the process of exchanging transactions between network users, an experimental blockchain application was created. This made it possible to clearly demonstrate the features of using such crypto-tools as public and private keys and digital signature to solve the problem of unauthorized transactions. The performance of the experimental blockchain network is analyzed at different values of block mining complexity.**

**Keywords: blockchain, block, data level, data protection, hash function, transaction, public key, private key, digital signature.**