УДК 004.056.55

В. В. Казміревський

АНАЛІЗ ДЕРЕВОПОДІБНИХ ГЕШ-ФУНКЦІЙ

Вінницький національний технічний університет

Анотація

Розглянуто та проаналізовано нециклічні та циклічні деревоподібні геш-функції, зокрема їхні структури на основі бінарних, квадро- та октодерев. Проаналізовано переваги та недоліки деревоподібних геш-функцій. Розглянуто перспективи застосування таких функцій у блокчейні. У результаті доведено, що нециклічні деревоподібні геш-функції забезпечують кращу відповідність вимогам блокчейну, тоді як циклічні структури демонструють низку обмежень у цьому контексті. Отримані результати можуть бути основою для подальшого вдосконалення криптографічних методів захисту даних у блокчейні.

Ключові слова: деревоподібні геш-функції, бінарні дерева, квадродерева, октодерева, циклічні структури, блокчейн.

Abstract

Non-cyclical and cyclical tree-like hash functions have been considered and analyzed, specifically their structures based on binary, quadtree, and octree. The advantages and disadvantages of tree-like hash functions have been discussed. The potential application of such functions in blockchain technology has been explored. As a result, it has been proven that non-cyclical tree-like hash functions better meet blockchain requirements, while cyclical structures present a number of limitations in this context. The findings may serve as a foundation for further improvement of cryptographic data protection methods in blockchain.

Keywords: Tree-like hash functions, binary trees, quadtree, octree, cyclic structures, blockchain.

Вступ

Деревоподібні геш-функції відіграють важливу роль у сучасній криптографії, забезпечуючи ефективні способи організації та перевірки даних. Їх структура базується на принципах дерев, таких як бінарні, квадро та октодерева, які пропонують різноманітні підходи до побудови та обчислення гешів. Особливий інтерес становить аналіз впливу циклічності на продуктивність деревоподібних геш-функцій у блокчейні.

Метою дослідження є удосконалення гнучкості деревоподібних геш-функцій шляхом аналізу їхніх структур. Особлива увага приділяється оцінці доцільності використання циклічних і нециклічних деревоподібних структур.

Для досягнення мети було розв’язано такі задачі:

- проведено огляд деревоподібних геш-функцій, зокрема бінарних, квадро- та октодерев, а також циклічних і нециклічних структур;
- досліджено особливості застосування деревоподібних геш-функцій у контексті блокчейну;
- оцінено обмеження циклічних деревоподібних структур у блокчейні та обґрунтовано переваги нециклічних структур для цих технологій.

Нециклічні деревоподібні геш-функції

Деревоподібні геш-функції є потужним інструментом, який дозволяє організовувати обчислення на основі ієрархічної структури. Вони можуть бути класифіковані за кількістю дочірніх вузлів та особливостями зв’язків між ними. У межах цієї класифікації розглянуто п'ять основних типів деревоподібних структур: бінарні дерева, квадродерева, октодерева, циклічні та нециклічні структури.

Бінарне дерево є структурою даних, яка організує список елементів таким чином, що початковий елемент називається коренем. Кожен елемент дерева може мати від 0 до 2 піделементів (які називаються лівою та правою гілкою). Уявлення цього процесу можна зобразити у вигляді такої структури, де кожен вузол дерева пов'язаний з підлеглими елементами, що забезпечує певну ієрархічну організацію даних (рис. 1 а). У контексті геш-функцій бінарні дерева використовуються для досягнення більш ефективного пошуку та обробки даних. Зокрема, при проектуванні бінарних деревоподібних геш-функцій елементи дерева, що мають певні значення, можуть бути розподілені за допомогою функцій гешування, що дозволяють створити оптимізовану структуру для пошуку та маніпулювання даними в

складних системах. Такий підхід є корисним для підвищення продуктивності алгоритмів пошуку, де кожен елемент дерева зберігається в залежності від значення геш-функції, що дозволяє швидко знаходити потрібні елементи, зменшуючи час обробки порівняно з іншими методами зберігання даних. Переваги цієї структури включають мінімальну складність реалізації, що робить її зручною для впровадження в різних алгоритмах. Однак, недоліками є значна глибина дерева для великих обсягів даних, що може призвести до зниження ефективності обробки та збільшення часу пошуку в разі необхідності працювати з великими наборами інформації [1].

Квадродерево є ієрархічною структурою даних, яка базується на рекурсивному розподілі 2D-області. Кожен вузол дерева представляє квадратну ділянку, а корінь дерева охоплює всю область. Квадродерево працює за принципом ділення кожної ділянки на чотири частини, що дозволяє створити чотири дочірні вузли (рис. 1 б). У контексті гешування, квадродеревоподібні структури використовуються для організації даних з урахуванням двовимірних координат. Кожен вузол містить геш-значення для певної частини області, і, завдяки такій організації, пошук і обробка даних стає значно ефективнішими. Квадродеревоподібні геш-функції є простою для реалізації структурою, яка забезпечує швидкий доступ до даних за допомогою геш-таблиць і ефективно використовує пам'ять, що важливо при обробці великих двовимірних даних. Однак вони обмежені лише двовимірними даними, що знижує їх універсальність, а при збільшенні обсягу даних глибина дерева може значно зрости, що впливає на ефективність роботи [2].

Октодерево є більш складною ієрархічною структурою, яка працює на основі рекурсивного розподілу 3D-області. Кожен вузол дерева представляє куб в 3D-просторі, а корінь дерева охоплює всю цю область. Для кожного не листового вузла його куб ділиться на 8 частин, що генерує 8 дочірніх вузлів. Данні, як правило, зберігаються в листових вузлах дерева. Серед варіантів представлення октодерева можна відзначити традиційне дерево з вказівниками, де кожен вузол має 8 вказівників на своїх дочірніх елементах (рис. 1 в). Однак, для зменшення розміру структури та покращення ефективності, вказівники можуть бути замінені на індекси в геш-таблиці, що дозволяє забезпечити доступ до будь-якого вузла дерева за сталий час. Це дозволяє зменшити кількість вказівників і забезпечити більш компактне представлення даних [3].

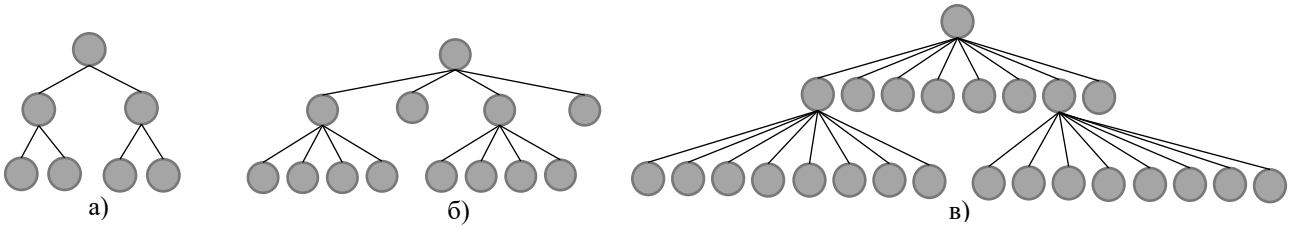

Рис. 1. а) структура бінарної деревоподібної геш-функції, б) структура квадро-деревоподібної геш-функції, в) структура окто-деревоподібної геш-функції

Циклічні деревоподібні геш-функції

Циклічне бінарне дерево є узагальненою формою класичного бінарного дерева, що допускає циклічні зв’язки між вузлами. На відміну від традиційної структури, де кожен вузол має до двох нащадків, у циклічному дереві деякі вузли можуть містити посилання назад, утворюючи цикли. Це ускладнює класичні алгоритми обходу, оскільки стандартні методи можуть потрапляти в нескінченні петлі без механізмів контролю [4]. У контексті геш-функцій такі структури моделюють повторювані залежності в даних і сприяють зменшенню колізій. Циклічні зв’язки оптимізують розподіл даних, зменшуючи дублювання та забезпечуючи швидкий доступ до повторюваних значень. Перевагами є ефективне використання пам’яті та компактність представлення. Основним недоліком є складність обходу й балансування, що обмежує застосування в задачах пошуку та обробки, роблячи такі дерева специфічними для гешування.

Циклічне октодерево є узагальненою формою стандартного октодерева, що допускає циклічні зв’язки між вузлами. На відміну від класичної структури, де кожен вузол має до восьми нащадків, у циклічному варіанті можливі зворотні посилання, які створюють цикли та ускладнюють традиційні алгоритми обходу. Такі дерева сприяють ефективному використанню пам’яті завдяки повторному використанню вузлів без дублювання даних [4]. У контексті геш-функцій вони застосовуються для адаптивного розподілу даних і зменшення конфліктів під час гешування, що є корисним у

тривимірному гешуванні та просторовому аналізі. Основними перевагами є компактне зберігання даних і гнучка організація зв’язків. Головним недоліком є складність обходу та балансування, що вимагає спеціальних алгоритмів для запобігання нескінченним ітераціям.

Циклічне квадродерево – це модифікована версія стандартного квадродерева, що допускає циклічні зв’язки між вузлами. На відміну від класичної структури, де кожен вузол має до чотирьох нащадків, у циклічному варіанті можливі зворотні посилання, що створюють цикли. Це дозволяє зменшити дублювання даних і прискорити доступ до інформації, проте ускладнює обходи дерева [4]. У контексті геш-функцій такі структури застосовуються для багаторівневого гешування, оптимізуючи розподіл і пошук даних, зокрема в задачах геопросторового аналізу, комп’ютерного зору та обробки зображень. Цикли сприяють адаптації до змінних даних і саморегуляції структури. Перевагами є компактне представлення інформації та гнучкість у розподілі даних. Головним недоліком є складність обходу та балансування, що потребує спеціальних алгоритмів. Незважаючи на це, циклічні квадродерева є перспективними для кластеризації, просторового пошуку та роботи з двовимірними структурами.

Деревоподібні геш-функції у блокчейні

Деревоподібні геш-функції відіграють ключову роль у блокчейні. Нециклічні структури забезпечують ефективну верифікацію даних, зменшуючи обсяг збереженої інформації та прискорюючи перевірку транзакцій. Вони оптимальні для класичних блокчейнів, хоча мають обмеження щодо гнучкості оновлення. Циклічні деревоподібні геш-функції, попри свою теоретичну привабливість для підвищення стійкості блокчейну, можуть спричиняти ускладнення. Додавання циклічних зв'язків між вузлами підвищує складність верифікації та може ускладнити адаптацію до змін у розподілених системах. Тому їх застосування потребує ретельного обґрунтування в залежності від специфіки блокчейн-архітектури. Оцінка обмеження циклічних та переваги нециклічних деревоподібних структур у блокчейні наведена у таблиці 1.

Таблиця 1. Оцінка застосування циклічних та не циклічних деревоподібних геш-функцій у блокчейні

Критерій	Циклічні деревоподібні структури	Нециклічні деревоподібні структури
Складність верифікації	Важча через цикли	Простіша завдяки відсутності циклів
Ефективність обробки	Знижена через додаткові обчислення	Вища через простоту обходу
Адаптивність до змін	Складна через цикли	Легша завдяки простоті структури
Масштабованість	Обмежена через додаткові обчислення	Краща завдяки простоті
Простота реалізації	Вища складність реалізації	Простіша через відсутність циклів
Використання пам'яті	Менш ефективне через збереження циклів	Більш ефективне з точки зору пам'яті

Нециклічні деревоподібні структури є більш підходящими для застосувань у блокчейні завдяки їхній ефективності, масштабованості, простоті реалізації та меншим вимогам до пам'яті. Циклічні структури створюють додаткові труднощі в управлінні та верифікації, що робить їх менш придатними для більшості блокчейн-систем, незважаючи на можливі переваги в контексті стійкості до маніпуляцій.

Визначивши, що нециклічні деревоподібні структури краще підходять для застосувань у блокчейні, варто порівняти застосування бінарних, квадро- та октодеревоподібних структур. Кожна з них має свої переваги та недоліки, що впливають на їхню придатність для специфічних задач блокчейна. Бінарне дерево є простим і ефективним варіантом для пошуку та обробки даних у блокчейні. Воно використовує логарифмічну складність пошуку за умови збалансованості, що є важливим для досягнення оптимальної продуктивності. Однак для великих обсягів даних може виникати проблема глибини дерева, що погіршує ефективність. Це дерево є найбільш універсальним та підходить для загальних задач, де не потрібна обробка багатовимірних даних. Квадродерево має перевагу в обробці двовимірних даних, таких як геопросторові координати, що можуть бути корисними у блокчейнах, що працюють з локаціями або картографічними даними. Воно дозволяє швидко організувати пошук за допомогою геш-таблиць та ефективно використовує пам'ять. Однак квадродерево обмежене лише двовимірними даними, що знижує його універсальність для більш складних задач. Октодерево, яке є більш складним для реалізації, підходить для роботи з тривимірними або багатовимірними даними. Воно здатне обробляти великі обсяги даних у тривимірних просторах, однак має високу складність реалізації та значні вимоги до пам'яті, що робить його менш придатним для загального використання в блокчейн-системах.

З огляду на простоту реалізації та ефективність для більшості блокчейн-застосунків, бінарне дерево є оптимальним вибором. Для специфічних задач, пов'язаних з двовимірними даними, такими як геопросторові обчислення, можна використовувати квадродерево, а для більш складних багатовимірних даних доцільно застосовувати октодерево, хоча його використання обмежене складністю реалізації та високими вимогами до пам'яті.

Висновки

У результаті проведеного дослідження проаналізовано особливості деревоподібних геш-функцій, включаючи бінарні, квадро- та октодеревоподібні структури, а також їхні циклічні та нециклічні варіанти. Виявлено, що нециклічні деревоподібні геш-функції є більш ефективними для застосування в блокчейні, оскільки забезпечують простіший механізм верифікації, кращу масштабованість та ефективне використання пам’яті.

Циклічні деревоподібні структури, хоча й дозволяють зменшити дублювання даних і підвищити стійкість до колізій, мають низку обмежень, пов’язаних із складністю обходу, балансування та верифікації. Це робить їх менш придатними для використання в традиційних блокчейн системах.

Також здійснено порівняння різних видів деревоподібних геш-функцій у контексті блокчейну. Встановлено, що бінарні дерева є раціональним вибором завдяки простоті реалізації та ефективності пошуку. Квадродерева мають перевагу у двовимірних задачах, тоді як октодерева забезпечують роботу з тривимірними даними, але потребують значних обчислювальних ресурсів.

Отримані результати можуть слугувати основою для подальших досліджень щодо оптимізації деревоподібних геш-функцій, зокрема шляхом розробки гібридних структур, що поєднують переваги різних підходів, а також удосконалення механізмів їхнього використання у блокчейні.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Md. Mehedi Masud, Gopal Chandra Das, Md. Anisur Rahman, Arunashis Ghose. A hashing technique using separate binary tree. Data Science Journal, Volume 5, 19 October 2006. pp. 143-161. URL: https://www.researchgate.net/publication/220390356_A_hashing_technique_using_separate_binary_tree (дата звернення: 20.01.2025).

2. Daniel Madeira, Esteban Clua, Anselmo Antunes Montenegro, Thomas Lewiner. Gpu octrees and optimized search. Cadastro de Pré–publicação : MAT. 09/09. p. 7. URL: https://www.researchgate.net/publication/265027180_Gpu_octrees_and_optimized_search (дата звернення: 20.01.2025).

3. Michael S. Warren, John Salmon. A parallel hashed Oct-Tree N-Body algorithm. Conference: Supercomputing '93. Proceedings, 1993. p. 11. URL: https://www.researchgate.net/publication/4054992_A_parallel_hashed_Oct-Tree_N-Body_algorithm (дата звернення: 20.01.2025).

4. Elena Andreeva, Rishiraj Bhattacharyya, Arnab Roy. Compactness of Hashing Modes and Efficiency Beyond Merkle Tree. Advances in Cryptology – EUROCRYPT 2021. pp. 92–123. URL: https://link.springer.com/chapter/10.1007/978-3-030-77886-6_4 (дата звернення: 20.01.2025).

Казміревський Віталій Віталійович — аспірант кафедри Захисту інформації, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: kazmirevskiy1999@gmail.com

Науковий керівник: ***Баришев Юрій Володимирович*** – к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця. email: yuriy.baryshev@vntu.edu.ua

Vitalii Kazmirevskyi — postgraduate student of Information Protection Department, Faculty for Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: kazmirevskiy1999@gmail.com

Supervisor: ***Yurii Baryshev*** – PhD (Eng), Associate Professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia. email: yuriy.baryshev@vntu.edu.ua