DOI: 10.34185/1991-7848.itmm.2025.01.087

ДОСЛІДЖЕННЯ АЛГОРИТМІВ УПРАВЛІННЯ КОНКУРЕНТНИМ ДОСТУПОМ ТА УНИКНЕННЯ КОЛІЗІЙ У БЛОКЧЕЙН-МЕРЕЖАХ

Швачич Г.Г.[1], Битько А.М.[2]

[1]НТУ «Дніпровська політехніка», д.т.н., професор, Україна

[2]НТУ «Дніпровська політехніка», Україна

Анотація. *У роботі представлено системний аналіз технології блокчейн та особливості її застосування, розглянута внутрішня логіка (шифрування, консенсус). Розглядається дослідження конкурентного доступу та уникнення колізій при функціонуванні технології блокчейн. Зазначене суттєво впливає на її продуктивність, масштабованість та надійність, що є ключовими факторами для успішного впровадження цієї технології в різних сферах. Аналізується одна з основних проблем блокчейна щодо забезпечення достовірності даних, яка вимагає використання ефективних алгоритмів шифрування. Ці алгоритми повинні забезпечувати високу криптографічну стійкість інформації в мережі, підтримувати реалізацію цифрового підпису та гарантувати безпеку транзакцій. Також розглянуто спеціальні алгоритми управління конкурентним доступом і уникнення колізій у блокчейн-мережах, що сприяють підвищенню ефективності їх роботи.*

Ключові слова: *колізії, доступ, блокчейн-мережі, хеш, достовірність даних, шифрування, дешифрування, алгоритми, мережа.*

Вступ. Як і будь-яка інноваційна технологія, блокчейн має низку задач, які необхідно розв’язати для його повномасштабного впровадження. Однією з найважливіших є проблема децентралізованого зберігання даних. Якщо в кожному вузлів мережі зберігати повний реєстр даних, то можна відновити мережу навіть після видалення останнього вузла. Однак, слід враховувати, що мережа постійно зростає, що призводить до неконтрольованих обсягів даних. Крім того, для приєднання нового учасника до мережі необхідно синхронізувати величезну кількість даних [1, 2]. Це пов'язано з необхідністю завантаження всієї історії транзакцій, щоб новий вузол міг повністю інтегруватися в мережу і забезпечити її цілісність. Як варіант вирішення цієї проблеми, можна використовувати стандартну базу даних (БД), де зберігаються реальні дані в зашифрованому вигляді, а в блокчейн заносяться лише їхні хеші.

Застарілі блоки при цьому архівуються. Це може бути локальним рішенням зазначеної проблеми.

З огляду на зазначене, можна припустити, що для розв'язування цих задач можна використовувати методи з таких технологій, як Big Data [3, 4]. Вона також орієнтована на роботу з великими обсягами зберігання та обробки даних. Крім того, цей підхід вже відпрацьований у різних архітектурах: Map Reduce, Shared Memory, Shared Nothing, Shared Disk, тощо. Основною перешкодою для інтеграції інструментів Big Data у блокчейн є тип системи: блокчейн є децентралізованою, розподіленою системою, що означає, що обчислення розподіляються між кількома вузлами і відсутні вузли, які керують роботою інших вузлів мережі. Однак тут можна розглянути інший підхід. При цьому слід враховувати, що технічно блокчейн є простою базою даних з істотною масштабованістю і відсутністю мов запитів. Проте децентралізованість, незмінність, прозорість і можливість універсального обміну даними компенсують ці недоліки. У зв'язку з цим нині ведуться розробки технологій BigchainDB і IPDB, які можуть стати базами даних глобального масштабу з децентралізованим управлінням.

Ще однією важливою задачею є забезпечення довіри до системи, яка має бути одночасно анонімною і прозорою для її учасників. Користувачі хочуть бачити рух даних у мережі, але при цьому інші користувачі не повинні знати, чим займаються вони. Для цього було вирішено застосувати алгоритми асиметричного шифрування, завдяки чому кожен користувач має пару ключів: приватний і публічний. Приватний ключ використовується для підпису блоків, що відправляються користувачем, а адреса користувача в мережі відображається за допомогою публічного ключа.

Однією з головних проблем блокчейну є достовірність даних, що визначає необхідність застосування ефективних алгоритмів шифрування. Вони повинні гарантувати достатню криптографічну стійкість інформації в мережі, а також дозволяти реалізувати цифровий підпис [5]. У зв'язку з цим розглянемо спеціальні алгоритми конкурентного доступу та вирішення колізій у мережі.

Основний матеріал досліджень. Спеціальні алгоритми конкурентного доступу та вирішення колізій в мережах блокчейн спрямовані на забезпечення ефективного обміну даними між блоками, які спільно використовують один канал передачі. Конкурентний доступ означає, що декілька пристроїв можуть одночасно намагатися передавати дані, що може призвести до конфліктів або колізій. Для мінімізації таких проблем використовуються різні алгоритми.

Нині застосовуються наступні спеціальні алгоритми конкурентного доступу і дозволу колізій в мережі:

– PBFT – запит на додавання блоку розсилається усім учасникам, і усі роблять обчислення хэша наступного блоку, після чого розсилають своє рішення іншим учасникам. У результаті кожен учасник отримує масив відповідей і приймає відповідь із загальною довірчою ймовірністю 0,5. Недолік алгоритму – час виконання транзакції збільшується залежно від розміру мережі.

– PoW – вузли мережі (майнери) розв'язують задачу з обчислення хешу наступного блоку з певною умовою. При цьому хто швидше порахує хеш, того блок і буде наступним. Недолік алгоритму – енергоємність через складності обчислень і присутність деякої централізації – майнерів.

– PoS – альтернатива PoW, алгоритм не вимагає великих обчислювальних потужностей: учасники мережі мають внутрішньо системну валюту, і хто багатіший, той має пріоритет для формування блоку.

– Деякі додаткові ресурсу (Burn, Space, Bandwidth) – є різновидами PoW і PoS.

Ці алгоритми використовуються в залежності від типу мережі, вимог до швидкості передачі даних, надійності та масштабованості.

Аналіз логічної моделі «достовірності» технології блокчейн на основі асиметричного алгоритму шифрування RSA. Розглянемо алгоритм роботи асиметричного шифрування RSA [6].

На першому етапі обираються два прості числа p і q. Далі на основі співвідношень:

$$n = q \cdot p, \tag{1}$$

$$\varphi(n) = \varphi(pq) = (p-1)(q-1) \tag{2}$$

знаходять модуль для відкритого та закритого ключа і функцію Ейлера від модуля (2). Потім обирається ціле число *e* (відкрита експонента) від 1 до $\varphi(n)$ (взаємно просте з $\varphi(n)$). Зазвичай в якості *e* беруть прості числа, що містять невелику кількість одиничних біт в двійковому записі, але не занадто малі, для швидкого піднесення до ступеня.

Далі знаходиться число *d*, що відповідає формулі (3) :

$$d \cdot e \, mod \varphi(n) = 1. \tag{3}$$

Таким чином формується приватний ключ {*d, n*} і публічний ключ {*e, n*}, за допомогою яких робиться шифрування:

$$c = m^e \cdot mod \, n, \tag{4}$$

і дешифрування

$$m = c^d \cdot mod \, n = c = m^{ed} \cdot mod \, n = m \cdot mod \, n = m, \tag{5}$$

даних.

При цьому m < n, c – шифровані дані, m – нешифровані дані, $mod \varphi(n)$ – множина значень (чим більше, тим краще).

При спробі ж зламати (підібрати) закритий ключ доведеться перебрати 2^N комбінацій, де *N* – довжина ключа. Наприклад, при довжині ключа в 256 біт і швидкості підбору паролів 1024 в секунду знадобиться 1,23e + 67 років, що дуже і дуже багато, та і інформація на той час буде вже не актуальна.

Також можна використовувати і прогресивніші алгоритми, такі як Elliptic Curve Digital Signa – ture Algorithm (ECDSA), які працюють схожим чином, але мають свої особливості.

Висновки. Перехід від екстенсивного до інтенсивного розвитку призводить до зменшення кількості вільних ніш, що, у свою чергу, вимагає співпраці серед багатьох раніше незалежних людей і організацій. Кожна з них має свою базу даних та інфраструктуру, що часто спричиняє неточності та невідповідність інформації. У світі, де ціна помилки перевищує вартість системи, необхідні технології, здатні управляти витратами, знижувати їх, забезпечувати ефективний обмін даними і мінімізувати помилки, що значною мірою досягається завдяки технології блокчейн.

У роботі представлено системний аналіз технології блокчейн та особливості її застосування, розглянута внутрішня логіка (шифрування, консенсус).

Перспективи впровадження блокчейн-технології є значними. Вона застосовується не тільки для реалізації традиційних розподілених фінансово-економічних систем, але й у рамках корпоративних інформаційних систем, що супроводжують життєвий цикл виробів, зокрема при впровадженні синхронних технологій проектування як розподіленої облікової книги записів. Такий підхід дозволяє забезпечити синхронізацію проектних дій між розподіленими командами розробників та виробничими процесами.

ЛІТЕРАТУРА

1. Agbo C. C., Mahmoud Q. H., Eklund, J. M. Blockchain technology in healthcare: a systematic review. Healthcare. 2020. 7(2), 56.
2. Attaran, M. Blockchain technology in healthcare: Challenges and opportunities. International Journal of Healthcare Management. 2022. 15(1). P. 70 – 83.
3. Zgurovsky M.Z., Zaychenko Y.P. Big Data: Conceptual Analysis and Applications. Springer, 2020. – 298 p.
4. Thomas Erl. Big Data Fundamentals. Concepts, Drivers & Techniques. — Prentice Hall, 2016. – 235 p.
5. Гринович А.А., Пухальська Г.В. Електронний цифровий підпис: особливості застосування, переваги та проблеми. – [Електронний ресурс]. – Режим доступу до ресурсу: http://journals.khnu.km.ua/vestnik/pdf/ekon/2009_2/zmist.files/05.pdf
6. Алгоритм шифрування RSA, види атак на нього. Реалізація мовою Python. – [Електронний ресурс]. – Режим доступу до ресурсу: https://dou.ua/forums/topic/43026/?utm_source=chatgpt.com

RESEARCH ON ALGORITHMS FOR MANAGING COMPETITIVE ACCESS AND AVOIDING COLLISIONS IN BLOCKCHAIN NETWORKS

Hennadi Shvachych, Andrii Bytko

Abstract. *The paper presents a systematic analysis of blockchain technology and its application features, examining the internal logic (encryption, consensus). The research focuses on competitive access and collision avoidance in the operation of blockchain technology. These aspects significantly influence its performance, scalability, and reliability, which are critical factors for the successful adoption of this technology in various fields. The study addresses one of the main issues of blockchain—ensuring data integrity, which requires the use of efficient encryption algorithms. These algorithms must provide high cryptographic security of information within the network, support digital signature implementation, and ensure transaction security. Additionally, the paper explores specialized algorithms for managing competitive access and avoiding collisions in blockchain networks, contributing to their operational efficiency.*

Keywords: *collisions, access, blockchain networks, hash, data integrity, encryption, decryption, algorithms, network.*

REFERENCE

1. Agbo C. C., Mahmoud Q. H., Eklund, J. M. Blockchain technology in healthcare: a systematic review. Healthcare. 2020. 7(2), 56.
2. Attaran, M. Blockchain technology in healthcare: Challenges and opportunities. International Journal of Healthcare Management. 2022. 15(1). P. 70 – 83.
3. Zgurovsky M.Z., Zaychenko Y.P. Big Data: Conceptual Analysis and Applications. Springer, 2020. – 298 p.
4. Thomas Erl. Big Data Fundamentals. Concepts, Drivers & Techniques. — Prentice Hall, 2016. – 235 p.
5. Hrynovych A.A., Pukhalska H.V. Elektronnyi tsyfrovyi pidpys: osoblyvosti zastosuvannia, perevahy ta problemy. – [Elektronnyi resurs]. – Rezhym dostupu do resursu: http://journals.khnu.km.ua/vestnik/pdf/ekon/2009_2/zmist.files/05.pdf
6. Alhorytm shyfruvannia RSA, vydy atak na noho. Realizatsiia movoiu Python. – [Elektronnyi resurs]. – Rezhym dostupu do resursu: https://dou.ua/forums/topic/43026/?utm_source=chatgpt.com