Міністерство освіти і науки України
Кам’янець-Подільський національний університет імені Івана Огієнка
Фізико-математичний факультет
Кафедра комп’ютерних наук

Кваліфікаційна робота магістра
з теми: «**Вдосконалення методів підвищення конфіденційності та цілісності даних в криптовалютних блокчейнах**»

Виконав: здобувач вищої освіти групи KN1-M23 спеціальності 122 Комп’ютерні науки
Задорожний Володимир Володимирович
Керівник: Смалько Олена Аркадіївна, доцент, кандидат педагогічних наук
Рецензент: Сорич Віктор Андрійович, доцент, кандидат фізико -математичних наук

м. Кам’янець-Подільський – 2024 р.

АНОТАЦІЯ

Магістерська робота присвячена дослідженню методів забезпечення конфіденційності та цілісності даних у блокчейн-системах. У роботі розглянуто основні криптографічні методи, такі як хешування та шифрування, а також їхню роль у блокчейн-технологіях. Особливу увагу приділено вдосконаленню існуючих методів шифрування та хешування для підвищення продуктивності та надійності систем. Описано алгоритми оптимізації процесів шифрування та представлені фрагменти реалізації відповідних рішень. Практичне значення роботи полягає у можливості застосування отриманих результатів для покращення захисту даних у криптовалютних блокчейнах та інших децентралізованих системах.

Ключові слова: блокчейн, хешування, криптографія, алгоритми шифрування, конфіденційність, цілісність даних.

ANNOTATION

The master's thesis focuses on the study of methods for ensuring data confidentiality and integrity in blockchain systems. The work examines key cryptographic methods, such as hashing and encryption, and their role in blockchain technologies. Particular attention is given to improving existing encryption and hashing methods to enhance system performance and reliability. Algorithms for optimizing encryption processes are described, along with illustrative code implementations of the proposed solutions. The practical significance of the study lies in the applicability of the obtained results to improve data protection in cryptocurrency blockchains and other decentralized systems.

Keywords: blockchain, hashing, cryptography, encryption algorithms, confidentiality, data integrity.

ЗМІСТ

ВСТУП

Сучасний розвиток цифрових технологій значно збільшує обсяги даних, що зберігаються та передаються у мережах. Блокчейн-технології стали фундаментом для багатьох галузей, включаючи фінанси, логістику, охорону здоров’я, але зі зростанням їх популярності виникають численні виклики щодо забезпечення конфіденційності та цілісності даних. Незважаючи на використання надійних криптографічних алгоритмів, такі аспекти, як відстеження транзакцій, ризики компрометації даних та кібератаки, потребують пошуку нових підходів для підвищення рівня безпеки.

У контексті криптовалютних блокчейнів проблема конфіденційності стає особливо актуальною через прозорість мережі, де будь-який користувач має доступ до історії транзакцій. Водночас забезпечення цілісності даних є критичним для довіри до децентралізованих систем. Таким чином, дослідження методів, які вдосконалюють ці аспекти, має велике значення для подальшого розвитку галузі блокчейн-технологій.

Зі зростанням потужності обчислювальних систем та розвитком технологій аналізу даних виникають нові виклики для криптографічних алгоритмів, що лежать в основі блокчейнів. Хоча квантові комп'ютери поки що залишаються теоретичним інструментом, зростає ймовірність їхньої появи у майбутньому, що може поставити під загрозу безпеку існуючих алгоритмів, таких як RSA та ECC, які використовуються для шифрування й підпису даних. Водночас традиційні виклики блокчейн-технологій включають масштабування мережі через значний обсяг транзакцій, потребу в підвищеній швидкості обробки та оптимізації зберігання даних. Розвиток технологій аналізу, зокрема машинного навчання та штучного інтелекту, підсилює загрози анонімності користувачів, оскільки нові методи дозволяють ідентифікувати транзакційні зв'язки та потенційно розкривати учасників мережі. Тому дослідження нових алгоритмів шифрування, методів забезпечення конфіденційності та підвищення

ефективності систем є критично важливим для стійкого розвитку блокчейн-технологій.

Об’єктом дослідження є механізми забезпечення конфіденційності та цілісності даних у криптовалютних блокчейнах.

Предметом дослідження є вдосконалення методів криптографічного захисту даних у блокчейн-системах для підвищення їхньої конфіденційності, цілісності та ефективності обробки.

Метою дослідження є вдосконалення методів і алгоритмів криптографічного захисту даних у блокчейн-системах для підвищення їхньої конфіденційності, цілісності та ефективності обробки, враховуючи сучасні технології й процеси обробки інформації.

Завдання дослідження:

1. Дослідити сучасні моделі, методи та алгоритми криптографічного захисту даних, що використовуються у блокчейн-системах.
2. Виявити ключові загрози для конфіденційності, цілісності та ефективності обробки даних у блокчейн-мережах.
3. Описати та реалізувати алгоритми вдосконалених методів хешування та шифрування, що покращують конфіденційність та забезпечують цілісність даних у блокчейні.

Методи дослідження. Для досягнення поставленої мети використано методи теоретичного аналізу, моделювання криптографічних алгоритмів, експериментального дослідження їх продуктивності та порівняльного аналізу для оцінки ефективності запропонованих рішень.

Практичне значення роботи. Результати дослідження можуть бути використані для підвищення безпеки та ефективності криптографічного захисту даних у блокчейн-системах, зокрема у криптовалютних платформах, децентралізованих фінансових застосунках та інших інформаційних системах.

Апробація результатів досліджень проводилась упродовж двох міжнародних конференцій, зокрема під час 10-ї Міжнародної наукової

конференції «Сучасні проблеми математичного моделювання, прогнозування та оптимізації» пам’яті почесного професора Кам’янець-Подільського національного університету імені Івана Огієнка, д.т.н., професора, почесного академіка НАПНУ Анатолія Федоровича ВЕРЛАНЯ (м. Кам’янець-Подільський), а також Міжнародної науково-методичної Інтернет-конференції «Проблеми вищої математичної освіти: виклики сучасності» (м. Вінниця). За результатами роботи конференцій опубліковано тези: «Модель криптоблокчейну з посиленим захистом конфіденційності» [3], «Перспективні математичні концепції та технології для забезпечення цілісності даних у криптоблокчейнах» [4].

Структура роботи. Робота складається з трьох розділів. У першому розділі розглядаються основи шифрування в блокчейні та його роль у забезпеченні конфіденційності й цілісності. Другий розділ присвячено аналізу поширених методів захисту криптоблокчейнів та опису способів вдосконалення методів забезпечення конфіденційності та цілісності у розподілених базах даних. У третьому розділі описуються алгоритми вдосконалення деяких методів хешування та шифрування, що використовуються в блокчейнах. У чотирьох додатках наводяться коди програмних модулів з результатами їхньої роботи. Загальний обсяг роботи складає N сторінок. У списку використаних джерел міститься 32 інформаційних джерела.

ВИСНОВКИ

У результаті виконання дослідження було досягнуто поставленої мети, а саме вдосконалення методів і алгоритмів криптографічного захисту даних у блокчейн-системах для підвищення їхньої конфіденційності, цілісності та ефективності обробки з урахуванням сучасних технологій і процесів обробки інформації. Усі завдання, визначені на початку дослідження, були успішно виконані.

Зокрема:

1. **Досліджено сучасні моделі, методи та алгоритми криптографічного захисту даних, що застосовуються у блокчейн-системах.** Було проаналізовано основні криптографічні підходи, включно з хеш-функціями та алгоритмами симетричного й асиметричного шифрування, а також їхню роль у забезпеченні безпеки даних.

2. **Виявлено ключові загрози для конфіденційності, цілісності та ефективності обробки даних у блокчейн-мережах.** До основних викликів віднесено ризики відстеження транзакцій у публічних блокчейнах, компрометації криптографічних ключів, а також потребу у підвищенні швидкодії та масштабованості криптографічних алгоритмів для обробки великих обсягів даних.

3. **Описано та реалізовано алгоритми вдосконалених методів хешування та шифрування.** В роботі надано детальний опис принципів роботи розглянутих алгоритмів і фрагменти коду, що демонструють їх функціонування у контексті блокчейн-систем для підвищення конфіденційності та забезпечення цілісності даних.

Отримані матеріали можуть бути корисними для розробників блокчейн-платформ, дослідників у галузі криптографії та інформаційної безпеки, а також фахівців, що займаються впровадженням децентралізованих систем у різних сферах діяльності, таких як фінанси, охорона здоров'я, логістика та інші.

Практичне значення роботи полягає в можливості застосування отриманих результатів для вдосконалення існуючих методів криптографічного

захисту даних у блокчейн-системах. Запропоновані алгоритми та їхні реалізації можуть слугувати основою для підвищення рівня конфіденційності користувачів, оптимізації швидкодії процесів хешування та шифрування, а також забезпечення надійної цілісності даних у розподілених мережах. Зокрема, отримані результати можуть бути впроваджені у криптовалютних платформах, децентралізованих фінансових застосунках (DeFi), системах електронного документообігу та інших інформаційних технологіях, що потребують високого рівня безпеки та продуктивності.

Таким чином, виконана робота є важливим кроком у напрямку вдосконалення криптографічного захисту блокчейн-систем та створює підґрунтя для подальших досліджень у сфері безпеки даних у децентралізованих мережах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антоненко С. А. Криптографічні основи застосування електронного цифрового підпису в Україні. Правова інформатика. 2013. № 4 (40). С.19-28.

2. Бойко Д. І. Методи та засоби підвищення цілісності даних у системному аналізі за допомогою технології блокчейн: магістер. диплом. робота : спеціальність 124 «Системний аналіз». КНЕУ ім. Вадима Гетьмана. Київ, 2024. 94 с.

3. Бевз О. М., Квєтний Р. Н. Шифрування даних на основі високонелінійних булевих функцій та кодів з максимальною відстанню: монографія. Вінниця: ВНТУ, 2010. 96 с.

4. Задорожний В. В., Смалько О. А. Модель криптоблокчейну з посиленим захистом конфіденційності. Сучасні проблеми математичного моделювання, прогнозування та оптимізації: тези доповідей 10-ї Міжнародної наукової конференції. Пам'яті почесного професора Кам'янець-Подільського національного університету імені Івана Огієнка, д.т.н., професора, почесного академіка НАПНУ Анатолія Федоровича ВЕРЛАНЯ. Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2024. С.88-89. URL: http://surl.li/zjimmz (дата звернення: 25.11.2024).

5. Задорожний В. В., Смалько О. А. Перспективні математичні концепції та технології для забезпечення цілісності даних у криптоблокчейнах. Матеріали Міжнародної науково-методичної Інтернет-конференції «Проблеми вищої математичної освіти: виклики сучасності». Вінниця, 2024. С.91-93. URL: http://surl.li/rbwuwm (дата звернення: 25.11.2024).

6. Каткова Т. І. Забезпечення криптографічного захисту державних інформаційних ресурсів. Наукові нотатки. Луцьк, 2022. № 73. С. 54–58.

7. Ковальчук А. М. Бінарні лінійні перетворення в модифікаціях алгоритму RSA шифрування зображень. Український журнал інформаційних технологій. 2020, т. 2, № 1. С. 37–42.

8. Кузнецова С., Писаковський А. Децентралізовані фінанси в сучасній фінансовій системі: розвиток та ризики. Цифрова економіка та економічна безпека: науково-практичний журнал. 2024. № 4 (13). С.154–158.

9. Кузнецов О., Кіян А. Новий підхід до побудови пост-квантової схеми. Безпека інформаційних систем і технологій. 2020. №1(2). С.23-30.

10. Терещенко Г., Кириченко І. Аналіз та обґрунтування використання існуючих блокчейн-рішень для захисту цифрових активів. Інноваційні технології та наукові рішення для промисловості. 2024. №1 (27). С.164-178.

11. Фесенко А. Порівняння постквантових стандартів у розрізі впровадження у класичні алгоритми електронного підпису. Безпека інформаційних систем і технологій. 2024. Т. 1, № 7. С.31-38. DOI: 10.17721/ISTS.2024.7.31-38.

12. Adeniyi E. A., Falola P. B., Maashi M. S., Aljebreen M., Bharany S. Secure Sensitive Data Sharing Using RSA and ElGamal Cryptographic Algorithms with Hash Functions. Information 2022, 13, 442. DOI: 10.3390/info13100442

13. Benhamouda F., Camenisch J., Krenn S., Lyubashevsky V., Neven G. (2014). Better zero-knowledge proofs for lattice encryption and their application to group signatures. In Sarkar, P., & Iwata, T. (Eds.), *Advances in cryptology – ASIACRYPT 2014. Lecture Notes in Computer Science*, vol. 8873, pp. 551–572. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-662-45611-8_29.

14. Bhargavan K., et al. *Formal Verification of PQXDH: A Hybrid Post-Quantum Key Exchange Protocol*. Proceedings of the USENIX Security Symposium, 2023. URL: http://surl.li/pmghlh. (дата звернення: 25.11.2024).

15. Chen Y., Li S. A High-Throughput Hardware Implementation of SHA-256 Algorithm. 2020 IEEE International Symposium on Circuits and Systems (ISCAS), Seville, Spain, 2020, pp. 1-4, DOI: 10.1109/ISCAS45731.2020.9181065.

16. Chandel A., Aggarwal A., Mittal A., Choudhury T. Comparative Analysis of AES & RSA Cryptographic Techniques, International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, 2019, pp. 410-414, DOI: 10.1109/ICCIKE47802.2019.9004338.

17. Fan X., Niu B. (2021). Multi-core and SIMD Architecture Based Implementation on SHA-256 of Blockchain. *Xu K., Zhu J., Song X., Lu, Z. (eds) Blockchain Technology and Application*. CBCC 2020. Communications in Computer and Information Science, vol. 1305. Springer, Singapore. DOI: 10.1007/978-981-33-6478-3_4.

18. Franck L. D., Ginja G. A., Carmo J. P., Afonso J. A., Luppe M. Custom ASIC Design for SHA-256 Using Open-Source Tools. Computers 2024, 13, 9. DOI: 10.3390/computers13010009.

19. Fatima S, Rehman T, Fatima M, Khan S, Ali MA. Comparative Analysis of AES and RSA Algorithms for Data Security in Cloud Computing. Engineering Proceedings. 2022; 20(1):14. DOI: 10.3390/engproc2022020014.

20. Rawal B. S., Kumar L. S., Maganti S., Godha V. Comparative Study of Sha-256 Optimization Techniques. *2022 IEEE World AI IoT Congress (AIIoT)*, Seattle, WA, USA, 2022, pp. 387-392, DOI: 10.1109/AIIoT54504.2022.9817185.

21. Heo J. W. Decentralised blockchain storage solution scalable and secure optimisation scheme for efficient data management. Dissertation for the degree of Doctor of Philosophy. School of Computer Science. Faculty of Science. Queensland University of Technology, 2024. 188 p.

22. Helix Research Group. *The Cryptographic Hash Function SHA-256*. URL: https://helix.stormhub.org/papers/SHA-256.pdf (дата звернення: 25.11.2024).

23. Kontham S., Kumar P. Exploring the role of blockchain technology in ensuring data integrity and security in cloud computing. Journal of Nonlinear Analysis and Optimization. 2024. Vol. 15, Issue. 1, No.15. URL: https://griml.com/84CyE (дата звернення: 25.11.2024).

24. Liu J., Fan C., Tian X., Ding Q. Optimization of AES and RSA Algorithm and Its Mixed Encryption System. In: Pan, JS., Tsai, PW., Watada, J., Jain, L. (eds) Advances in Intelligent Information Hiding and Multimedia Signal Processing. IIH-MSP 2017. Smart Innovation, Systems and Technologies, vol. 82. Springer, Cham. DOI: 10.1007/978-3-319-63859-1_48.

25. Meng X. Exploring the role of blockchain technology in enhancing data integrity and privacy protection. Applied and Computational Engineering. 2024. Vol.87(1). DOI: 10.54254/2755-2721/87/20241508.

26. Morhaim L. Blockchain and cryptocurrencies technologies and network structures: applications, implications and beyond. 2019. URL: https://hal.science/hal-02280279v1 (дата звернення: 25.11.2024).

27. Parikh P, Patel N., Patel D., Modi P., Kaur H. Ciphering the Modern World: A Comprehensive Analysis of DES, AES, RSA and DHKE, 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2024, pp. 838-842, DOI: 10.23919/INDIACom61295.2024.10498330.

28. Radanliev P. The rise and fall of cryptocurrencies: defining the economic and social values of blockchain technologies, assessing the opportunities, and defining the financial and cybersecurity risks of the Metaverse. *Financial Innovation*. 2024. Vol. 10, Issue 1. DOI:10.1186/s40854-023-00537-8.

29. Satheesha S. Evaluating privacy technologies in blockchains for financial systems. Degree project in information and communication technology, second cycle. Stockholm, 2021. URL: http://surl.li/hznnub (дата звернення: 25.11.2024).

30. Weingärtner T., Fasser F., Reis Sá da Costa P., Farkas W. Deciphering DeFi: A Comprehensive Analysis and Visualization of Risks in Decentralized Finance. *Journal of Risk and Financial Management*. 2023. Vol. 16, Issue 10. DOI: 10.3390/jrfm16100454.

31. Zou L., Ni M., Huang Y., Shi W., Li X. (2020). Hybrid Encryption Algorithm Based on AES and RSA in File Encryption. *Hung, J., Yen, N., Chang, JW. (eds) Frontier Computing*. 2019. Lecture Notes in Electrical Engineering, vol. 551. Springer, Singapore. DOI: 10.1007/978-981-15-3250-4_68.

32. Muth R., Tschorsch F. SmartDHX: Diffie-Hellman Key Exchange with Smart Contracts, 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), Oxford, UK, 2020, pp. 164-168. DOI: 10.1109/DAPPS49028.2020.00022.