УДК 004.9
А. А. Титжинський
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЗАХИСТ БЛОКЧЕЙНУ ВІД КВАНТОВИХ ОБЧИСЛЕНЬ

UDC 004.9
A. A. Tytzhynskyi

PROTECTION OF BLOCKCHAIN FROM QUANTUM COMPUTING

Блокчейн-технологія забезпечує прозорість і захищеність даних у багатьох сферах, таких як фінанси, логістика та охорона здоров'я. Однак із розвитком квантових обчислень постає загроза для існуючих криптографічних механізмів, які є основою безпеки блокчейну. Дослідження спрямоване на аналіз методів захисту блокчейну від квантових обчислень.

Квантові комп'ютери здатні значно прискорити виконання задач, які вважаються складними для класичних комп'ютерів. Алгоритм Шора дозволяє розв'язувати задачі факторизації та обчислення дискретного логарифма за поліноміальний час, що ставить під загрозу криптографічні алгоритми, такі як RSA та ECC, які широко використовуються в блокчейні. Для вирішення цих проблем досліджуються квантово-стійкі алгоритми, що включають криптографію на основі граток, хешів, кодів та багаточленів. Ці алгоритми забезпечують новий рівень захисту від атак квантових комп'ютерів[1].

Окрім криптографічних змін, модернізація механізмів консенсусу є важливим напрямом для посилення безпеки. Існуючі механізми, такі як Proof of Work, можуть бути замінені або модифіковані із врахуванням можливостей квантових обчислень. Досліджуються альтернативи, включаючи Proof of Stake з додатковим захистом і механізми Byzantine Fault Tolerance, що дозволяють підвищити стійкість системи до квантових атак. Гібридні системи, які поєднують класичні та квантово-стійкі алгоритми, забезпечують перехідний етап до більш безпечних стандартів [2].

Було проведено дослідження впливу квантових обчислень на найбільш поширені алгоритми блокчейну, такі як SHA-256 та ECDSA. Встановлено, що квантові комп'ютери можуть значно скоротити час підбору хешів або приватних ключів, що підвищує ймовірність атак на блокчейн-мережі. Це робить актуальним розробку нових стандартів і протоколів, які враховують можливості квантових технологій [3].

Для збереження безпеки блокчейну в умовах розвитку квантових обчислень необхідно впроваджувати квантово-стійкі криптографічні методи, адаптувати існуючі протоколи та підвищувати рівень досліджень у цій сфері. Стандартизація нових криптографічних алгоритмів та їх інтеграція в існуючі блокчейн-системи є пріоритетними завданнями для забезпечення довготривалої безпеки даних. Масштабованість і швидкодія нових рішень також повинні бути враховані при розробці цих систем, щоб вони могли відповідати сучасним вимогам [4].

Таким чином, розвиток квантових обчислень вимагає переосмислення основ безпеки блокчейну. Лише активні дослідження та інноваційні підходи дозволять зберегти довіру до технологій розподіленого реєстру в умовах квантової ери.

Література

1. Procedia Computer Science. Vol. 177, pp. 183-191. ArXiv. URL: https://arxiv.org/abs/2011.03460.
2. Allende M., López León D., Cerón S., Leal A., Pareja A., Da Silva M., Pardo A., Jones D., Worrall D., Merriman B., Gilmore J., Kitchener N., Venegas-Andraca S. E., 2021. Quantum-resistance in blockchain networks. International Journal of Quantum Information. Vol. 19, No. 7, pp. 1-15. ArXiv. URL: https://arxiv.org/abs/2106.06640.
3. Gate.io Research Team, 2023. Post-Quantum Cryptography in Blockchain Security. Blockchain Technology Research Journal. No. 12, pp. 45-52. Gate.io. URL: https://www.gate.io/uk/learn/articles/post-quantum-cryptography-in-blockchain-security/1061.
4. Cryptomus Editorial Team, 2022. Quantum Computers and Cryptocurrencies: Impact and Solutions. Journal of Blockchain Applications. Vol. 8, No. 3, pp. 27-34. Cryptomus. URL: https://cryptomus.com/uk/blog/quantum-computers-and-cryptocurrencies.