KVANT SHAROITIDA BLOKCHEYN TIZIMLARIDA XAVFSIZLIK MUAMMOLARI TAHLILI

G'oyibnazarova Aziza Abdullo qizi
Muhammad al-Xorazmiy nomidagi
Toshkent Axborot texnologiyalari universiteti, magistr
E-mail: goyibnazarovaaziza@gmail.com
https://doi.org/10.5281/zenodo.20421780

Annotatsiya: Mazkur ilmiy tezisda kvant hisoblash texnologiyalarining rivojlanishi fonida blokcheyn tizimlarida yuzaga kelayotgan xavfsizlik muammolari tahlil qilinadi. Tadqiqot davomida kvant kompyuterlarining klassik kriptografik algoritmlarga, xususan RSA va Elliptic Curve Cryptography (ECC) tizimlariga koʻrsatadigan tahdidlari oʻrganilgan. Blokcheyn tizimlarida tranzaksiyalarni himoyalash, raqamli imzolarni tekshirish va konsensus mexanizmlarining barqarorligi kvant texnologiyalari nuqtai nazaridan baholangan. Shuningdek, post-kvant kriptografiyasi, lattice-based, hash-based va multivariate kriptografik algoritmlarning blokcheyn tizimlarida qoʻllanilishi tahlil etilgan. Tadqiqot natijalari kvant kompyuterlarining rivojlanishi mavjud blokcheyn infratuzilmalariga sezilarli xavf tugʻdirishini koʻrsatadi hamda post-kvant xavfsizlik standartlarini joriy etish zarurligini asoslaydi.

Kalit soʻzlar: Blokcheyn, kvant kompyuteri, post-kvant kriptografiyasi, ECC, RSA, Shor algoritmi, Grover algoritmi, xavfsizlik, raqamli imzo, konsensus mexanizmi.

Аннотация: В данном научном тезисе анализируются проблемы безопасности, возникающие в блокчейн-системах на фоне развития технологий квантовых вычислений. В ходе исследования были изучены угрозы, которые квантовые компьютеры представляют для классических криптографических алгоритмов, в частности для систем RSA и Elliptic Curve Cryptography (ECC). С точки зрения квантовых технологий была оценена устойчивость механизмов защиты транзакций, проверки цифровых подписей и консенсусных механизмов в блокчейн-системах. Кроме того, проанализировано применение постквантовой криптографии, а также lattice-based, hash-based и multivariate криптографических алгоритмов в блокчейн-системах. Результаты исследования показывают, что развитие квантовых компьютеров представляет значительную угрозу существующим блокчейн-инфраструктурам и обосновывает необходимость внедрения стандартов постквантовой безопасности.

Ключевые слова: Блокчейн, квантовый компьютер, постквантовая криптография, ECC, RSA, алгоритм Шора, алгоритм Гровера, безопасность, цифровая подпись, механизм консенсуса.

Abstract: This scientific thesis analyzes the security issues emerging in blockchain systems in the context of the development of quantum computing technologies. The study examines the threats posed by quantum computers to classical cryptographic algorithms, particularly RSA and Elliptic Curve Cryptography (ECC) systems. The stability of transaction protection, digital signature verification, and consensus mechanisms in blockchain systems is evaluated from the perspective of quantum technologies. In addition, the application of post-quantum cryptography, including lattice-based, hash-based, and multivariate cryptographic algorithms in blockchain systems, is analyzed. The research results indicate that the development of quantum computers poses a significant threat to existing blockchain infrastructures and highlights the necessity of implementing post-quantum security standards.

Keywords: Blockchain, quantum computer, post-quantum cryptography, ECC, RSA, Shor's algorithm, Grover's algorithm, security, digital signature, consensus mechanism.

Kirish

So‘nggi yillarda blokcheyn texnologiyasi moliyaviy tizimlar, elektron hukumat, sog‘liqni saqlash va logistika kabi ko‘plab sohalarda keng qo‘llanila boshladi. Blokcheynning asosiy afzalligi markazlashmagan tuzilma va kriptografik himoya mexanizmlariga asoslangan xavfsizlik tizimidir [1]. Bitcoin va Ethereum kabi blokcheyn platformalari tranzaksiyalarni himoyalash uchun Elliptic Curve Digital Signature Algorithm (ECDSA) va SHA-256 xesh algoritmlaridan foydalanadi [2].

Biroq kvant hisoblash texnologiyalarining rivojlanishi mavjud kriptografik tizimlarning barqarorligiga jiddiy tahdid tug‘dirmoqda. 1994-yilda Peter Shor tomonidan ishlab chiqilgan Shor algoritmi katta sonlarni faktorlash va diskret logarifm masalalarini polinomial vaqt ichida yechish imkonini berishi isbotlangan [3]. Mazkur algoritm RSA va ECC asosidagi xavfsizlik tizimlarini zaiflashtiradi. Shu sababli kvant kompyuterlarining rivojlanishi blokcheyn xavfsizligi uchun muhim muammoga aylangan.

Google kompaniyasi 2019-yilda “Sycamore” kvant protsessori orqali kvant ustunligiga erishganini e’lon qildi [4]. IBM, Intel va D-Wave kompaniyalari ham yuqori quvvatli kvant tizimlarini ishlab chiqmoqda. Tadqiqotchilar tomonidan

kvant kompyuterlari yaqin kelajakda amaliy kriptografik tizimlarni buzish imkoniyatiga ega bo‘lishi mumkinligi qayd etilgan [5].

Blokcheyn tizimlarida xavfsizlikning asosiy elementi bo‘lgan raqamli imzolar kvant kompyuterlarining rivojlanishi natijasida zaiflashadi. ECC asosidagi tizimlar kvant hujumlariga nisbatan ayniqsa sezgir hisoblanadi [6]. Shu sababli post-kvant kriptografiyasi konsepsiyasi ishlab chiqilgan bo‘lib, u kvant kompyuterlariga bardosh bera oladigan algoritmlarni yaratishga qaratilgan.

Metodologiya

Mazkur tadqiqotda ilmiy tahlil, komparativ tahlil, kriptografik algoritmlarni baholash va xalqaro standartlarni o‘rganish metodlaridan foydalanildi. Tadqiqot jarayonida NIST tomonidan tavsiya etilgan post-kvant kriptografik standartlar, IEEE va ACM bazalaridagi ilmiy maqolalar hamda blokcheyn xavfsizligiga oid zamonaviy tadqiqotlar tahlil qilindi [7].

Kvant hisoblash texnologiyalarining blokcheyn tizimlariga ta’siri quyidagi yo‘nalishlarda o‘rganildi:

- Raqamli imzo algoritmlarining zaifligi;
- Konsensus mexanizmlariga kvant hujumlari;
- Hash algoritmlarining barqarorligi;
- Post-kvant kriptografik algoritmlar samaradorligi.

Shuningdek, Bitcoin va Ethereum platformalarida qo‘llanilayotgan ECDSA algoritmlarining kvant kompyuterlariga nisbatan zaifligi ilmiy manbalar asosida tahlil qilindi [8].

Natijalar

Tadqiqot natijalari kvant kompyuterlarining blokcheyn xavfsizligiga sezilarli xavf tug‘dirishini ko‘rsatdi. Xususan, Shor algoritmi yordamida ECC asosidagi ochiq kalitlardan maxfiy kalitlarni tiklash mumkinligi aniqlandi [3]. Bitcoin tizimida ochiq kalit tranzaksiya vaqtida tarmoqqa uzatiladi. Agar yetarli quvvatga ega kvant kompyuteri mavjud bo‘lsa, tajovuzkor maxfiy kalitni hisoblab topishi va tranzaksiyani soxtalashtirishi mumkin [9].

Grover algoritmi esa xesh funksiyalarining xavfsizligini pasaytiradi. SHA-256 algoritmida klassik tizimda 2^256 murakkablik talab qilinsa, Grover algoritmi yordamida bu murakkablik 2^128 ga kamayadi [10]. Bu esa hash funksiyalarining xavfsizlik darajasini sezilarli kamaytiradi.

Ethereum blokcheynida ham ECDSA algoritmi qo‘llaniladi. Tadqiqotlarda qayd etilishicha, kvant kompyuterlarining rivojlanishi Ethereum hamyonlarining xavfsizligiga tahdid tug‘diradi [11]. Mutaxassislar tomonidan mavjud blokcheyn tizimlarini post-kvant algoritmlariga migratsiya qilish zarurligi ta’kidlangan.

NIST tomonidan CRYSTALS-Kyber va CRYSTALS-Dilithium algoritmlari post-kvant standartlari sifatida tanlangan [12]. Ushbu algoritmlar lattice-based kriptografiyaga asoslanadi va kvant kompyuterlariga nisbatan barqaror hisoblanadi. Tadqiqotlarda Dilithium algoritmi raqamli imzolar uchun yuqori xavfsizlik va samaradorlikni ta’minlashi ko‘rsatilgan [12].

Hash-based imzo tizimlari, xususan XMSS va SPHINCS+ algoritmlari ham kvant xavfsiz tizimlar sifatida baholanmoqda [13]. Biroq ushbu algoritmlarda imzo hajmi katta bo‘lishi blokcheyn tarmoqlari uchun qo‘shimcha yuklama keltirib chiqaradi.

Tahlil va muhokama

Blokcheyn texnologiyasining xavfsizligi asosan kriptografik algoritmlarga bog‘liq. Hozirgi blokcheyn tizimlarida ochiq kalitli kriptografiya asosiy himoya mexanizmi sifatida ishlatiladi. Bitcoin tizimida ECDSA algoritmi orqali foydalanuvchilarning tranzaksiyalari autentifikatsiya qilinadi [2]. ECC algoritmi diskret logarifm muammosining murakkabligiga asoslangan bo‘lib, klassik kompyuterlarda uni yechish amaliy jihatdan imkonsiz hisoblanadi.

Shor algoritmi paydo bo‘lishi bilan ushbu xavfsizlik paradigmasi o‘zgardi. Peter Shorning tadqiqotlariga ko‘ra, kvant kompyuterlari diskret logarifm va faktorlash masalalarini samarali yecha oladi [3]. Bu esa blokcheyn tizimlarining asosiy xavfsizlik qatlamini zaiflashtiradi.

Bitcoin tarmog‘ida tranzaksiya amalga oshirilganda foydalanuvchining ochiq kaliti blokcheynga uzatiladi. Kvant hujumchisi ushbu ochiq kalit asosida maxfiy kalitni hisoblab topishi mumkin [9]. Natijada foydalanuvchining mablag‘lari o‘g‘irlanishi ehtimoli yuzaga keladi. Tadqiqotchilar tomonidan millionlab Bitcoin manzillari kvant hujumlariga potensial ravishda zaif ekanligi qayd etilgan [14].

Grover algoritmi hash funksiyalarining murakkabligini kamaytiradi. SHA-256 algoritmi hozirgi blokcheyn tizimlarida keng qo‘llaniladi. Klassik tizimlarda brute-force hujumi juda katta hisoblash resurslarini talab qiladi. Ammo Grover algoritmi yordamida qidiruv tezlashadi [10]. Shu sababli kelajakda SHA-512 kabi uzunroq hash algoritmlaridan foydalanish zarurati paydo bo‘lishi mumkin.

Kvant xavfsizligini ta’minlash maqsadida post-kvant kriptografiyasi rivojlantirilmoqda. NIST tomonidan 2016-yildan boshlab post-kvant standartlashtirish dasturi amalga oshirildi [12]. Ushbu jarayonda lattice-based, code-based, hash-based va multivariate algoritmlar o‘rganildi. 2022-yilda CRYSTALS-Kyber va Dilithium algoritmlari standart sifatida tanlandi.

Lattice-based algoritmlar Learning With Errors (LWE) muammosiga asoslanadi. Tadqiqotlarga ko‘ra, kvant kompyuterlari ushbu muammoni samarali yecha olmaydi [15]. Shu sababli Kyber algoritmi kalit almashish tizimlari uchun istiqbolli variant sifatida baholanmoqda.

Blokcheyn tizimlariga post-kvant algoritmlarini integratsiya qilish murakkab jarayon hisoblanadi. Birinchidan, yangi algoritmlar katta hajmdagi kalit va imzolarni talab qiladi [13]. Bu esa blok hajmining ortishiga va tranzaksiya tezligining pasayishiga olib kelishi mumkin. Ikkinchidan, mavjud blokcheyn infratuzilmasini yangilash katta iqtisodiy xarajatlarni talab qiladi.

Ethereum hamjamiyati tomonidan post-kvant migratsiyasi bo‘yicha tadqiqotlar olib borilmoqda [11]. Vitalik Buterin kvant xavfsizligini Ethereum ekotizimining uzoq muddatli barqarorligi uchun muhim omil sifatida baholagan. Ayrim tadqiqotchilar hybrid kriptografik tizimlarni joriy etishni taklif qilmoqda, bunda klassik va post-kvant algoritmlari birgalikda qo‘llaniladi [16].

Kvant kompyuterlarining rivojlanish sur’ati ham muhim omil hisoblanadi. IBM kompaniyasi 2023-yilda ming kubitdan ortiq protsessorlarni ishlab chiqish rejasini e’lon qilgan [17]. Mutaxassislar tomonidan amaliy kvant hujumlari uchun millionlab fizik kubitlar talab qilinishi ta’kidlangan bo‘lsa-da, texnologik rivojlanish tezlashmoqda.

Blokcheyn xavfsizligi faqat kriptografiya bilan cheklanmaydi. Konsensus mexanizmlariga ham kvant tahdidlari mavjud. Proof-of-Work tizimlarida kvant kompyuterlari mining jarayonini tezlashtirishi mumkin [18]. Bu esa tarmoqdagi markazlashuv xavfini oshiradi. Tadqiqotchilar tomonidan kvantga bardoshli konsensus mexanizmlarini ishlab chiqish bo‘yicha izlanishlar olib borilmoqda.

Hash-based imzo tizimlari kvant xavfsiz variant sifatida ko‘rib chiqiladi. XMSS va SPHINCS+ algoritmlari davlat standartlari darajasida tavsiya etilgan [13]. Biroq ularning asosiy kamchiligi katta hajmdagi imzolardir. Bu blokcheyn tarmoqlarida saqlash xarajatlarini oshiradi.

Code-based kriptografiya, xususan McEliece algoritmi ham post-kvant xavfsizlikni ta’minlaydi [19]. Ammo katta hajmdagi ochiq kalitlar amaliy qo‘llashni murakkablashtiradi. Multivariate algoritmlar esa samarali ishlashiga qaramay, ayrim xavfsizlik muammolari sababli keng qo‘llanilmayapti.

Xalqaro standartlashtirish tashkilotlari post-kvant xavfsizligiga katta e’tibor qaratmoqda. ETSI, ISO va NIST tomonidan post-kvant algoritmlarini joriy etish bo‘yicha tavsiyalar ishlab chiqilgan [12]. Bank tizimlari, davlat ma’lumotlar bazalari va blokcheyn platformalari ushbu standartlarga bosqichma-bosqich o‘tishi zarurligi ta’kidlanmoqda.

Xulosa

Tadqiqot natijalari kvant kompyuterlarining rivojlanishi blokcheyn tizimlari xavfsizligiga jiddiy tahdid tug‘dirishini ko‘rsatdi. Xususan, Shor algoritmi ECC va RSA asosidagi tizimlarni zaiflashtiradi, Grover algoritmi esa hash funksiyalarining xavfsizlik darajasini kamaytiradi. Bitcoin va Ethereum kabi zamonaviy blokcheyn platformalari kvant hujumlariga nisbatan sezgir hisoblanadi.

Post-kvant kriptografiyasi ushbu muammolarning asosiy yechimi sifatida shakllanmoqda. NIST tomonidan standartlashtirilgan Kyber va Dilithium algoritmlari istiqbolli variantlar sifatida baholanmoqda. Biroq post-kvant algoritmlarini blokcheyn tizimlariga integratsiya qilish texnik va iqtisodiy muammolarni yuzaga keltiradi.

Kelajakda blokcheyn platformalarida hybrid kriptografik tizimlarni joriy etish, kvant xavfsiz konsensus mexanizmlarini ishlab chiqish hamda xalqaro standartlarga mos post-kvant migratsiyasini amalga oshirish muhim ahamiyat kasb etadi.

Foydalangan adabiyotlar ro‘yxati

1.Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. – pp. 1–9.
2.Antonopoulos A. M. Mastering Bitcoin. O’Reilly Media, 2017. – pp. 45–78.
3.Shor P. W. “Algorithms for Quantum Computation: Discrete Logarithms and Factoring”. Proceedings of FOCS, 1994. – pp. 124–134.
4.Arute F. et al. “Quantum Supremacy Using a Programmable Superconducting Processor”. Nature, 2019. – pp. 505–510.
5.Bernhardt C. Quantum Computing for Everyone. MIT Press, 2019. – pp. 112–145.
6.Aggarwal D., Brennen G., Lee T. et al. “Quantum Attacks on Bitcoin”. Ledger Journal, 2018. – pp. 15–32.
7.Chen L. et al. Report on Post-Quantum Cryptography. NIST, 2016. – pp. 5–41.
8.Bonneau J. et al. “SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies”. IEEE Symposium, 2015. – pp. 104–121.
9.Proos J., Zalka C. “Shor’s Discrete Logarithm Quantum Algorithm for Elliptic Curves”. Quantum Information & Computation, 2003. – pp. 317–344.
10.Grover L. K. “A Fast Quantum Mechanical Algorithm for Database Search”. ACM Symposium, 1996. – pp. 212–219.
11.Buterin V. Ethereum White Paper. 2014. – pp. 1–36.
12.Alagic G. et al. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. NIST, 2022. – pp. 10–55.

13.Hülsing A. et al. “SPHINCS+: Submission to the NIST Post-Quantum Project”. 2020. – pp. 3–48.
14.Fernández-Caramés T. M., Fraga-Lamas P. “Towards Post-Quantum Blockchain”. IEEE Access, 2020. – pp. 21091–21116.
15.Regev O. “On Lattices, Learning with Errors, Random Linear Codes, and Cryptography”. STOC, 2005. – pp. 84–93.
16.Bindel N. et al. “Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange”. IACR Cryptology, 2019. – pp. 1–29.
17.IBM Quantum Roadmap Report. IBM Research, 2023. – pp. 2–18.
18.Kiktenko E. et al. “Quantum-secured Blockchain”. Quantum Science and Technology, 2018. – pp. 1–12.
19.Bernstein D. J., Lange T. Post-Quantum Cryptography. Springer, 2009. – pp. 5–17.