BLOKCHEYN TIZIMLARIDA MUAMMOLAR 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.20390452

Annotatsiya: Mazkur ilmiy tezisda blokcheyn texnologiyasining xavfsizlik jihatlari, ayniqsa markazlashmagan tarmoqlarda yuzaga keladigan asosiy tahdidlar va ularni bartaraf etish usullari tahlil qilinadi. Tadqiqot davomida 51% hujumi, Sybil hujumi, Double Spending, smart-kontrakt zaifliklari, kriptografik kalitlar bilan bog‘liq muammolar hamda DDoS hujumlarining blokcheyn infratuzilmasiga ta’siri o‘rganildi. Shuningdek, Proof-of-Work, Proof-of-Stake, Multi-signature, shifrlash algoritmlari va audit mexanizmlarining xavfsizlikni ta’minlashdagi roli ilmiy manbalar asosida tahlil qilindi. Tadqiqot natijalari blokcheyn texnologiyasining yuqori darajadagi himoya imkoniyatlariga ega ekanligini ko‘rsatsa-da, inson omili va dasturiy zaifliklar sababli xavfsizlikka tahdidlar saqlanib qolayotganini ko‘rsatadi.

Kalit so‘zlar: Blokcheyn, axborot xavfsizligi, smart-kontrakt, kriptografiya, Sybil hujumi, 51% attack, Double Spending, Proof-of-Work, Proof-of-Stake, decentralizatsiya, kiberxavfsizlik.

Аннотация: В данном научном тезисе анализируются аспекты безопасности технологии блокчейн, в частности основные угрозы, возникающие в децентрализованных сетях, а также методы их предотвращения. В ходе исследования были изучены влияние атак 51%, атак Сибиллы (Sybil attack), Double Spending, уязвимостей смарт-контрактов, проблем, связанных с криптографическими ключами, а также DDoS-атак на инфраструктуру блокчейна. Кроме того, на основе научных источников проанализирована роль механизмов Proof-of-Work, Proof-of-Stake, Multi-signature, алгоритмов шифрования и механизмов аудита в обеспечении безопасности. Результаты исследования показывают, что, несмотря на высокий уровень защитных возможностей технологии блокчейн, угрозы безопасности сохраняются из-за человеческого фактора и программных уязвимостей.

Ключевые слова: Блокчейн, информационная безопасность, смарт-контракт, криптография, атака Сибиллы, атака 51%, Double Spending, Proof-of-Work, Proof-of-Stake, децентрализация, кибербезопасность.

Abstract: This scientific thesis analyzes the security aspects of blockchain technology, particularly the major threats arising in decentralized networks and the methods for mitigating them. During the research, the impacts of 51% attacks, Sybil attacks, Double Spending, smart contract vulnerabilities, issues related to cryptographic keys, and DDoS attacks on blockchain infrastructure were examined. In addition, the role of Proof-of-Work, Proof-of-Stake, Multi-signature mechanisms, encryption algorithms, and audit mechanisms in ensuring security was analyzed based on scientific sources. The research results demonstrate that although blockchain technology possesses a high level of security capabilities, threats to security still remain due to human factors and software vulnerabilities.

Keywords: Blockchain, information security, smart contract, cryptography, Sybil attack, 51% attack, Double Spending, Proof-of-Work, Proof-of-Stake, decentralization, cybersecurity.

Kirish

So‘nggi yillarda blokcheyn texnologiyasi moliya, logistika, sog‘liqni saqlash, elektron hukumat va raqamli identifikatsiya tizimlarida keng qo‘llanila boshladi. Blokcheynning asosiy afzalligi ma’lumotlarning markazlashmagan holda saqlanishi va kriptografik himoya orqali o‘zgarmasligini ta’minlashdan iborat [1]. 2008-yilda Satoshi Nakamoto tomonidan taklif etilgan Bitcoin tizimi blokcheyn texnologiyasining amaliy qo‘llanishiga asos soldi [2].

Blokcheyn texnologiyasi markazlashmagan arxitekturaga ega bo‘lib, tranzaksiyalarni bir nechta tugunlar orqali tekshirish mexanizmini qo‘llaydi. Ushbu mexanizm ma’lumotlarning soxtalashtirilishini kamaytiradi va tizimga bo‘lgan ishonchni oshiradi [3]. Shu bilan birga, texnologiyaning rivojlanishi bilan xavfsizlik muammolari ham murakkablashib bormoqda.

Tadqiqotlarga ko‘ra, blokcheyn tizimlaridagi asosiy xavflar 51% hujumlari, smart-kontraktlardagi xatoliklar, Sybil hujumlari, maxfiy kalitlarning yo‘qolishi hamda phishing hujumlari bilan bog‘liq [4]. Masalan, 2016-yilda Ethereum tarmog‘idagi DAO platformasiga qilingan hujum natijasida 50 million AQSh dollaridan ortiq mablag‘ yo‘qotilgan [5]. Bu hodisa smart-kontrakt xavfsizligi masalasining naqadar muhim ekanligini ko‘rsatdi.

Shu sababli blokcheyn texnologiyasida xavfsizlikni ta’minlash, zamonaviy tahdidlarni aniqlash va ularni bartaraf etish usullarini ishlab chiqish dolzarb ilmiy masalalardan biri hisoblanadi.

Metodologiya

Mazkur tadqiqotda ilmiy kuzatuv, taqqoslash, tizimli tahlil va statistik ma’lumotlarni o‘rganish metodlaridan foydalanildi. Tadqiqot uchun IEEE, Springer, Elsevier va ACM bazalarida chop etilgan ilmiy maqolalar hamda xalqaro tashkilotlarning hisobotlari asos qilib olindi.

Blokcheyn xavfsizligi bilan bog‘liq tahdidlar quyidagi mezonlar asosida tahlil qilindi:

- hujum turi;
- tizimga ta’siri;
- iqtisodiy zarar darajasi;
- texnik himoya mexanizmlari;
- amaliy bartaraf etish usullari.

Shuningdek, Bitcoin va Ethereum tarmoqlarida yuzaga kelgan real xavfsizlik hodisalari o‘rganildi hamda Proof-of-Work va Proof-of-Stake konsensus algoritmlarining xavfsizlik samaradorligi taqqoslandi [6].

Natijalar

Tadqiqot davomida blokcheyn tizimlaridagi asosiy xavfsizlik tahdidlari aniqlanib, ularning texnologik xususiyatlari o‘rganildi.

51% hujumi

51% hujumida tarmoq hisoblash quvvatining katta qismi bir guruh tomonidan nazorat qilinadi. Bu holatda hujumchi tranzaksiyalarni bekor qilishi yoki ikki marta sarflash imkoniyatiga ega bo‘ladi [7]. Bitcoin Gold tarmog‘ida 2018-yilda sodir bo‘lgan 51% hujumi natijasida taxminan 18 million dollarlik zarar qayd etilgan [8].

Double Spending muammosi

Double Spending bir xil kriptovalyutani ikki marta ishlatish holatini anglatadi. Nakamoto tomonidan ishlab chiqilgan Proof-of-Work mexanizmi ushbu muammoni kamaytirish uchun qo‘llanilgan [2]. Biroq kichik blokcheyn tarmoqlarida ushbu xavf saqlanib qolmoqda.

Sybil hujumi

Sybil hujumida bir foydalanuvchi bir nechta soxta identifikatorlar orqali tarmoqni nazorat qilishga harakat qiladi [9]. Bu ayniqsa kichik va yangi blokcheyn tarmoqlarida yuqori xavf tug‘diradi.

Smart-kontrakt zaifliklari

Ethereum platformasida smart-kontraktlardan foydalanish keng tarqalgan bo‘lsa-da, koddagi xatoliklar katta moliyaviy zararlarni keltirib chiqarishi mumkin [10]. DAO hujumi bunga eng mashhur misollardan biridir.

Kriptografik kalitlar xavfsizligi

Blokcheyn tizimlarida maxfiy kalitlarni yo‘qotish foydalanuvchining aktivlarga kirishini butunlay yo‘qotishiga olib keladi. Chainalysis ma’lumotlariga ko‘ra, Bitcoin’larning taxminan 20 foizi foydalanib bo‘lmaydigan holatga kelgan [11].

DDoS va tarmoq hujumlari

DDoS hujumlari tugunlarning normal ishlashiga to‘sqinlik qiladi va tranzaksiyalarni qayta ishlash tezligini pasaytiradi [12]

Tahlil va muhokama

Blokcheyn texnologiyasi zamonaviy axborot tizimlari ichida eng yuqori xavfsizlik darajasiga ega bo‘lgan texnologik yechimlardan biri sifatida e’tirof etiladi. Ushbu texnologiyaning asosiy ustunligi markazlashmagan arxitektura, kriptografik himoya va konsensus algoritmlarining birgalikdagi ishlashiga asoslanadi [1]. An’anaviy ma’lumotlar bazalarida barcha axborot bitta markaziy serverda saqlanadi va ushbu serverga hujum uyushtirilganda tizimning butun xavfsizligi izdan chiqishi mumkin. Blokcheyn tizimida esa ma’lumotlar tarmoqdagi minglab tugunlar o‘rtasida taqsimlangan bo‘lib, bu holat ma’lumotlarni o‘zgartirish yoki yo‘q qilishni ancha murakkablashtiradi [2].

Shunga qaramasdan, blokcheyn texnologiyasi mutlaq xavfsizlikni kafolatlamaydi. So‘nggi yillarda turli blokcheyn platformalarida sodir bo‘lgan kiberhujumlar mavjud zaifliklarni ko‘rsatib berdi. Ayniqsa, Proof-of-Work konsensus mexanizmidan foydalanadigan tarmoqlarda 51% hujumi eng xavfli tahdidlardan biri sifatida qayd etiladi [7]. Ushbu hujumda tarmoq hisoblash quvvatining katta qismi bir subyekt nazoratiga o‘tadi va bu tranzaksiyalarni bekor qilish yoki bir xil aktivni ikki marta ishlatish imkonini beradi. Bitcoin Gold tarmog‘ida kuzatilgan hujum natijasida millionlab dollar zarar yetgani blokcheyn xavfsizligi bilan bog‘liq jiddiy muammolar mavjudligini ko‘rsatdi [8].

Katta blokcheyn tarmoqlarida bunday hujumni amalga oshirish uchun juda katta moliyaviy va texnik resurs talab qilinadi. Masalan, Bitcoin tarmog‘ida global hashrate hajmi nihoyatda yuqori bo‘lgani sababli 51% hujum iqtisodiy jihatdan samarasiz hisoblanadi [6]. Biroq kichik va yangi tashkil etilgan blokcheyn tarmoqlarida ushbu tahdid yuqori darajada saqlanib qolmoqda. Bu esa blokcheyn xavfsizligi tarmoq hajmi va ishtirokchilar soniga ham bevosita bog‘liqligini ko‘rsatadi.

Proof-of-Work algoritmi xavfsizlikni ta’minlashda samarali mexanizm bo‘lsa-da, energiya sarfi bilan bog‘liq muammolarni yuzaga keltirmoqda. Cambridge Centre for Alternative Finance ma’lumotlariga ko‘ra, Bitcoin tarmog‘ining yillik elektr energiyasi iste’moli ayrim rivojlangan davlatlar energiya iste’moliga tenglashgan [6]. Bu holat ekologik va iqtisodiy muammolarni keltirib chiqarishi sababli yangi konsensus mexanizmlarini ishlab chiqishga ehtiyoj tug‘ildi.

Shu sababli Proof-of-Stake konsensus algoritmi muqobil yechim sifatida keng rivojlanmoqda. Ushbu tizimda tranzaksiyalarni tasdiqlash foydalanuvchilarning hisoblash quvvatiga emas, balki tarmoqdagi ulushiga bog‘liq bo‘ladi [13]. Ethereum platformasining 2022-yilda Proof-of-Work tizimidan Proof-of-Stake tizimiga o‘tishi energiya sarfini keskin kamaytirdi [14]. Ethereum

Foundation ma’lumotlariga ko‘ra, yangi tizim energiya iste’molini 99 foizdan ortiq qisqartirgan [14]. Bu natija blokcheyn texnologiyasining ekologik barqarorligini oshirishda muhim qadam bo‘ldi.

Biroq Proof-of-Stake tizimi ham barcha muammolarni to‘liq hal qilmaydi. Ayrim tadqiqotchilar ushbu tizimda katta miqdordagi tokenlarga ega bo‘lgan foydalanuvchilar tarmoq ustidan nazoratni kuchaytirishi mumkinligini ta’kidlaydi [13]. Bu esa markazlashuv xavfini yuzaga keltiradi. Demak, konsensus algoritmlarini tanlashda nafaqat texnik xavfsizlik, balki iqtisodiy va boshqaruv omillari ham muhim ahamiyat kasb etadi.

Blokcheyn tizimlaridagi eng katta xavflardan biri smart-kontraktlar bilan bog‘liqdir. Smart-kontraktlar avtomatik bajariladigan dasturiy kod bo‘lib, ular inson aralashuvisiz tranzaksiyalarni amalga oshiradi [10]. Ethereum platformasida smart-kontraktlardan keng foydalanilishi DeFi va NFT loyihalarining rivojlanishiga katta turtki berdi. Shu bilan birga, koddagi xatoliklar millionlab dollar mablag‘ yo‘qotilishiga sabab bo‘lmoqda.

2016-yilda DAO platformasiga uyushtirilgan hujum smart-kontrakt xavfsizligi bo‘yicha eng yirik hodisalardan biri hisoblanadi [5]. Hujumchilar smart-kontrakt kodidagi rekursiv chaqiruv zaifligidan foydalangan holda katta miqdordagi Ethereum mablag‘larini o‘zlashtirgan. Ushbu hodisa Ethereum tarmog‘ining hard fork amalga oshirishiga olib kelgan [5]. DAO hodisasi blokcheyn tizimlarida dasturiy xavfsizlikni ta’minlash naqadar muhimligini yaqqol ko‘rsatdi.

Smart-kontrakt xavfsizligini oshirish uchun formal verifikatsiya va audit metodlaridan foydalanish muhim hisoblanadi [15]. Formal verifikatsiya yordamida dastur kodi matematik modellar orqali tekshiriladi va mantiqiy xatolar aniqlanadi. OpenZeppelin, ConsenSys va CertiK kabi kompaniyalar smart-kontrakt auditlarini professional tarzda amalga oshirib kelmoqda [15]. Tadqiqotlar shuni ko‘rsatadiki, auditdan o‘tgan smart-kontraktlarda xavfsizlik bilan bog‘liq muammolar sezilarli darajada kam uchraydi.

Blokcheyn xavfsizligida kriptografik kalitlarni himoya qilish ham asosiy masalalardan biri hisoblanadi. Blokcheyn tizimlarida foydalanuvchilar aktivlarga egalik qilish uchun maxfiy kalitlardan foydalanadi [16]. Agar ushbu kalit yo‘qolsa yoki uchinchi shaxs qo‘liga tushsa, foydalanuvchi o‘z aktivlarini qayta tiklay olmaydi. Chainalysis hisobotlariga ko‘ra, mavjud Bitcoin aktivlarining taxminan 20 foizi yo‘qolgan kalitlar sababli foydalanilmaydigan holatda qolmoqda [11].

Mazkur muammoni kamaytirish uchun Multi-signature texnologiyasidan foydalanish samarali vosita sifatida qaralmoqda [16]. Ushbu usulda tranzaksiyani amalga oshirish uchun bir nechta maxfiy kalit talab qilinadi. Natijada bitta kalit o‘g‘irlangan taqdirda ham aktivlarni noqonuniy o‘zlashtirish qiyinlashadi. Ayniqsa korporativ blokcheyn tizimlarida Multi-signature xavfsizlikni oshirishning muhim vositasiga aylangan.

Blokcheyn tarmoqlarida Sybil hujumlari ham jiddiy xavf tug‘diradi. Sybil hujumida bitta foydalanuvchi ko‘plab soxta identifikatorlar orqali tarmoqni nazorat qilishga urinadi [9]. Bu holat ayniqsa kichik va kam ishtirokchili blokcheyn tarmoqlarida xavfli hisoblanadi. Sybil hujumlari konsensus mexanizmlarining noto‘g‘ri ishlashiga va tranzaksiyalarni manipulyatsiya qilishga olib kelishi mumkin. Tadqiqotlar shuni ko‘rsatadiki, Proof-of-Work va Proof-of-Stake mexanizmlari Sybil hujumlariga qarshi qisman himoya yaratadi, chunki hujumchi katta iqtisodiy resurs sarflashga majbur bo‘ladi [13].

DDoS hujumlari ham blokcheyn infratuzilmasining barqaror ishlashiga tahdid soladi [12]. Bunday hujumlarda tugunlarga juda katta miqdorda so‘rov yuborilib, tizim ishlashi sekinlashtiriladi yoki to‘xtatiladi. Ayniqsa markazlashgan kriptovalyuta birjalari DDoS hujumlariga ko‘proq duch kelmoqda. Chunki blokcheynning o‘zi markazlashmagan bo‘lsa-da, ayrim xizmatlar

markazlashgan serverlarga bog‘liq holda ishlaydi. Shu sababli CDN texnologiyalari, tarmoq filtrlari va trafik monitoring tizimlaridan foydalanish muhim hisoblanadi.

Blokcheyn xavfsizligida inson omili eng zaif bo‘g‘inlardan biri sifatida baholanadi. Verizon Data Breach Investigations Report ma’lumotlariga ko‘ra, kiberhujumlarning katta qismi inson xatolari yoki ijtimoiy muhandislik usullari bilan bog‘liq [17]. Phishing hujumlari orqali foydalanuvchilarning maxfiy kalitlari va login ma’lumotlari qo‘lga kiritilishi mumkin. Ayniqsa kriptovalyuta hamyonlari va birjalariga oid soxta veb-saytlar foydalanuvchilar uchun katta xavf tug‘dirmoqda.

Mazkur muammoni kamaytirish uchun foydalanuvchilarning kiberxavfsizlik savodxonligini oshirish zarur. Ikki faktorli autentifikatsiya, hardware wallet qurilmalari va biometrik autentifikatsiya usullaridan foydalanish foydalanuvchi xavfsizligini sezilarli darajada oshiradi [16]. Ayniqsa hardware wallet qurilmalari maxfiy kalitlarni internetdan ajratilgan holda saqlashi sababli eng xavfsiz vositalardan biri hisoblanadi.

Blokcheyn texnologiyasining kelajakdagi xavflaridan biri kvant kompyuterlari bilan bog‘liqdir. Hozirgi blokcheyn tizimlarida RSA va elliptik egri chiziqli kriptografiya algoritmlaridan foydalaniladi [18]. Kvant kompyuterlari rivojlanishi natijasida ushbu algoritmlarni buzish ehtimoli mavjudligi ta’kidlanmoqda. Aggarwal va boshqa tadqiqotchilar kvant hisoblash texnologiyalari blokcheyn xavfsizligiga jiddiy xavf tug‘dirishini qayd etgan [18].

Shu sababli post-kvant kriptografiya yo‘nalishi faol rivojlanmoqda. Post-kvant algoritmlar kvant kompyuterlariga bardoshli kriptografik himoya yaratishga qaratilgan [18]. AQShning NIST tashkiloti tomonidan post-kvant kriptografiya standartlarini ishlab chiqish bo‘yicha tadqiqotlar olib borilmoqda. Kelajakda blokcheyn tizimlari ushbu algoritmlarni integratsiya qilishi ehtimoli yuqori.

Tahlillar shuni ko‘rsatadiki, blokcheyn xavfsizligi faqat texnik himoya vositalari bilan cheklanmaydi. Tizimning iqtisodiy modeli, foydalanuvchilarning savodxonligi, dasturiy ta’minot sifati va boshqaruv mexanizmlari ham umumiy xavfsizlik darajasiga ta’sir ko‘rsatadi. Shu sababli blokcheyn xavfsizligini ta’minlash kompleks yondashuvni talab qiladi.

Bugungi kunda davlat organlari va yirik korporatsiyalar blokcheyn texnologiyasidan foydalanishga qiziqish bildirmoqda. Moliya, logistika, tibbiyot va davlat xizmatlarida blokcheynning joriy etilishi xavfsizlikka bo‘lgan talabni yanada oshirmoqda. Ayniqsa markaziy banklarning raqamli valyutalari loyihalarida blokcheyn xavfsizligi strategik ahamiyat kasb etmoqda.

Xulosa

Blokcheyn texnologiyasi axborot xavfsizligini ta’minlashda muhim innovatsion yechimlardan biri hisoblanadi. Markazlashmagan arxitektura va kriptografik himoya tizimlari ma’lumotlarning yaxlitligini ta’minlaydi. Biroq 51% hujumi, smart-kontrakt zaifliklari, Sybil hujumlari va inson omili bilan bog‘liq tahdidlar blokcheyn tizimlari uchun jiddiy xavf bo‘lib qolmoqda.

Tadqiqot natijalari shuni ko‘rsatdiki, xavfsizlikni ta’minlashda konsensus algoritmlarini takomillashtirish, audit tizimlarini rivojlantirish va foydalanuvchilar savodxonligini oshirish muhim ahamiyatga ega. Kelajakda post-kvant kriptografiya texnologiyalarini joriy qilish blokcheyn tizimlarining barqaror xavfsizligini ta’minlashda muhim rol o‘ynaydi.

Adabiyotlar, References, Литературы:

1.Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. *Bitcoin and Cryptocurrency Technologies*. Princeton University Press, 2016. – pp. 15–28.
2. Nakamoto S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. – pp. 1–9.
3. Swan M. *Blockchain: Blueprint for a New Economy*. O’Reilly Media, 2015. – pp. 7–20.
4. Zheng Z., Xie S., Dai H., Chen X., Wang H. “Blockchain Challenges and Opportunities: A Survey”. *International Journal of Web and Grid Services*, 2018. – Vol.14, No.4. – pp. 352–375.
5. Siegel D. *Understanding The DAO Attack*. CoinDesk Research Report, 2016. – pp. 2–6.
6. Cambridge Centre for Alternative Finance. *Cambridge Bitcoin Electricity Consumption Index Report*. 2023. – pp. 10–18.
7. Rosenfeld M. “Analysis of Hashrate-Based Double Spending”. *arXiv Journal*, 2014. – pp. 1–13.
8. Kharif O. “Hackers Attack Bitcoin Gold”. *Bloomberg Technology Report*, 2018. – pp. 3–5.
9. Douceur J. “The Sybil Attack”. *Peer-to-Peer Systems Conference Proceedings*. Springer, 2002. – pp. 251–260.
10. Atzei N., Bartoletti M., Cimoli T. “A Survey of Attacks on Ethereum Smart Contracts”. *International Conference on Principles of Security and Trust*, 2017. – pp. 164–186.
11. Chainalysis Report. *The Lost Bitcoins Research*. 2020. – pp. 5–11.
12. Conti M., Kumar E., Lal C., Ruj S. “A Survey on Security and Privacy Issues of Bitcoin”. *IEEE Communications Surveys & Tutorials*, 2018. – Vol.20, No.4. – pp. 3416–3452.
13. Saleh F. “Blockchain Without Waste: Proof-of-Stake”. *The Review of Financial Studies*, 2021. – Vol.34, No.3. – pp. 1156–1190.
14. Ethereum Foundation. *Ethereum Merge Report*. 2022. – pp. 4–9.
15. Torres C., Schütte J., State R. “Osiris: Hunting for Integer Bugs in Ethereum Smart Contracts”. *ACSAC Conference Proceedings*, 2018. – pp. 664–676.
16. Antonopoulos A. *Mastering Bitcoin*. O’Reilly Media, 2017. – pp. 210–225.
17. Verizon. *Data Breach Investigations Report*. 2023. – pp. 12–27.
18. Aggarwal D., Brennen G., Lee T., Santha M., Tomamichel M. “Quantum Attacks on Bitcoin”. *Ledger Journal*, 2018. – Vol.3. – pp. 68–90.