

**BLOKCHEYN TEXNOLOGIYALARI NEGIZIDA HIMOYALASH
MEXANIZMLARINI YARATISH****RAXMATXO‘JAYEV RASHIDXON RIXSITILLA O‘G‘LI***Toshkent davlat iqtisodiyot universiteti**“Raqamli iqtisodiyot” kafedrasida mustaqil izlanuvchisi**rashidkhon@icloud.com*

Blockchain texnologiyalari so‘nggi yillarda kiberxavfsizlik sohasida inqilobiy yechim sifatida e‘tirof etilmoqda. An‘anaviy markazlashtirilgan tizimlarda ma‘lumotlar markaziy serverlarda saqlanadi va boshqariladi, bu esa ularni kiberhujumlar, ma‘lumotlarni buzish va ruxsatsiz kirishlarga nisbatan zaif qiladi. Blockchain esa tarqatilgan va markazlashmagan ma‘lumotlar bazasini yaratish orqali ushbu zaifliklarni kamaytiradi. Har bir tranzaksiya yoki ma‘lumot birligi tarmoqdagi ko‘plab tugunlar tomonidan tasdiqlanadi va blok zanjiriga qo‘shiladi. Bu yondashuv ma‘lumotlarning o‘zgartirilmazligini, shaffofligini va xavfsizligini ta‘minlaydi, chunki har qanday nohaq o‘zgartirish darhol aniqlanadi va rad etiladi.

Blockchain asosidagi tizimlar foydalanuvchi identifikatsiyasini va autentifikatsiyani ham mustahkamlashga yordam beradi. Masalan, identifikatsiya va kirish ma‘lumotlarini blok zanjiriga yozish orqali ruxsatsiz kirishlar oldini olish mumkin. Har bir foydalanuvchi tranzaksiyasi shifrlangan va autentifikatsiyalangan bo‘lib, uning tarixini o‘zgartirish imkoni yo‘q. Shu tariqa, tizim foydalanuvchilarni kuzatish, autentifikatsiya qilish va xavfsizlikni oshirish imkoniyatiga ega bo‘ladi.

Kiberxavfsizlik sohasida Blockchainning yana bir muhim qo‘llanilishi ma‘lumotlarni uzatishda xavfsizlikni ta‘minlashdir. An‘anaviy tizimlarda ma‘lumotlar serverlar orqali uzatiladi va ular buzilish yoki o‘g‘irlashga moyil bo‘ladi. Blockchain esa ma‘lumotlarni kriptografik tarzda shifrlash va tarqatish orqali uzatishni xavfsiz qiladi. Masalan, IoT qurilmalari yoki moliyaviy tranzaksiyalarni amalga oshiruvchi tizimlarda blockchain integratsiyasi ma‘lumotlarni manipulyatsiya qilish xavfini sezilarli darajada kamaytiradi.

Blockchain texnologiyalari kiberxavfsizlikni avtomatlashtirish va shaffoflikni oshirish imkonini beradi. Smart-kontraktlar orqali tizim ichidagi shartlar avtomatik ravishda bajariladi va har qanday nohaq harakat darhol blokirovka qilinadi. Bu esa inson omilidan kelib chiqadigan xatolik va xakerlik xavfini kamaytiradi. Smart-kontraktlar moliya, sug‘urta, ta‘lim va boshqa sohalarda xavfsiz, avtomatlashtirilgan operatsiyalarni ta‘minlaydi. Blockchainning audit va shaffoflik imkoniyatlari ham kiberxavfsizlik uchun muhimdir. Har bir tranzaksiya tarixini tarmoqdagi barcha tugunlar tekshiradi, bu esa tizimda shaffoflikni yaratadi va firibgarlikni oldini oladi. Korxonalar va davlat organlari blockchain asosidagi tizimlar orqali barcha

operatsiyalarni real vaqt rejimida kuzatishi va nazorat qilishi mumkin. Bu tizimning kiberxavfsizlik darajasini oshiradi va noxush holatlarning oldini oladi. Shuningdek, blockchain tizimlari ma'lumotlarning uzluksizligini va tiklanishini ta'minlashga yordam beradi. Tarqatilgan tuzilma tufayli, agar biror tugun yoki server ishlamasa ham, tizim ishlashda davom etadi. Bu esa kiberhujumlar yoki texnik nosozliklar natijasida yuzaga keladigan operatsion uzilishlarni kamaytiradi.

Hozirgi vaqtda ko'plab kompaniyalar va moliyaviy institutlar kiberxavfsizlikni oshirish maqsadida blockchainni qo'llamoqda. Masalan, moliyaviy tranzaksiyalarni xavfsiz amalga oshirish, yetkazib berish zanjirida mahsulotlar haqidagi ma'lumotlarni o'zgarmas tarzda saqlash, shuningdek, raqamli identifikatsiya tizimlarini mustahkamlashda blockchain muhim rol o'ynaydi. Shu bilan birga, blockchain kiberxavfsizlikni oshirish bilan birga, jarayonlarni tezlashtiradi va xarajatlarni kamaytiradi. Biroq, blockchain texnologiyasini kiberxavfsizlikda qo'llashda ayrim cheklovlar va muammolar mavjud. Masalan, tranzaksiyalarni tasdiqlash jarayoni ba'zan sekinlashishi mumkin, bu esa yuqori tezlikdagi tizimlar uchun muammo tug'diradi. Shuningdek, blockchainning o'ziga xos murakkabligi va dasturiy ta'minot talablarining yuqoriligi tizimni joriy qilish va boshqarishni qiyinlashtiradi. Shu sababli, blockchainni kiberxavfsizlikda qo'llashda texnologik, operatsion va moliyaviy jihatlarni hisobga olish zarur.

Kelajakda blockchainning kiberxavfsizlikdagi roli yanada oshadi, chunki texnologiya doimiy rivojlanmoqda va yangi protokollar, yuqori samaradorlik va moslashuvchanlikni ta'minlovchi yechimlar paydo bo'lmoqda. Sun'iy intellekt va mashina o'rganish bilan integratsiya qilinadigan blockchain tizimlari aniq tahdidlarni aniqlash, real vaqt rejimida javob berish va kiberhujumlarning iqtisodiy oqibatlarini minimallashtirish imkonini beradi. Shu tariqa, blockchain texnologiyalari kiberxavfsizlik sohasida nafaqat himoya mexanizmi, balki operatsion barqarorlikni oshiruvchi strategik vosita sifatida xizmat qilmoqda.

Blockchain texnologiyalariga asoslangan kiberxavfsizlik mexanizmlari markazlashtirilmagan tuzilma, shifrlash, smart-kontraktlar, real vaqt monitoringi, shaffoflik va ma'lumotlarning o'zgarmasligini ta'minlaydi. Bu yondashuv kiberhujumlar, ma'lumotlarni manipulyatsiya qilish va ruxsatsiz kirishlar kabi tahdidlarga qarshi samarali himoya yaratadi. Shu bilan birga, blockchain tizimlari operatsion uzluksizlikni kamaytiradi, jarayonlarni optimallashtiradi va moliyaviy hamda texnologik barqarorlikni oshiradi. Ushbu texnologiyani to'g'ri joriy etish va boshqarish orqali tashkilotlar kiberxavfsizlik sohasida yuqori darajadagi ishonchlilik va himoyaga erisha oladi.

Blockchainning kiberxavfsizlikdagi yana bir afzalligi ma'lumotlarning o'zgarmasligini ta'minlash. Masalan, sog'liqni saqlash tizimlarida bemorlar ma'lumotlarini blockchain orqali saqlash mumkin. Har bir kirish va yangilanish

tranzaksiyasi blok zanjiriga yoziladi, shuning uchun tarixni o'zgartirish yoki ma'lumotlarni soxtalashtirish imkonsiz bo'ladi. Bu nafaqat kiberxavfsizlikni oshiradi, balki audit va nazoratni ham soddalashtiradi. blockchain tizimlari global va interfaol kiberxavfsizlik ekotizimini yaratishda ham qo'llaniladi. Turli mamlakatlar va tashkilotlar blockchain orqali xavf-xatar ma'lumotlarini tezkor va shaffof tarzda almashish imkoniga ega bo'ladi. Bu esa kiberhujumlar tarqalishini kamaytiradi va jahon miqyosida tizimlar barqarorligini oshiradi.

Xulosa. So'nggi yillarda blockchain texnologiyalari kiberxavfsizlik sohasida inqilobiy vosita sifatida shakllanib bormoqda. An'anaviy markazlashgan tizimlarda mavjud bo'lgan zaifliklar kiberhujumlar, ruxsatsiz kirish va ma'lumotlarni buzish blockchainning tarqatilgan va markazlashmagan tuzilmasi orqali samarali kamaytiriladi. Har bir tranzaksiya blok zanjirida shifrlangan va tasdiqlangan holda saqlanadi, bu esa ma'lumotlarning o'zgarmasligi, shaffofligi va xavfsizligini kafolatlaydi. Smart-kontraktlar va avtomatlashtirilgan mexanizmlar inson omilidan kelib chiqadigan xatolik va xakerlik xavfini sezilarli darajada kamaytiradi.

Blockchain shuningdek ma'lumotlarni uzatishda xavfsizlikni ta'minlaydi, real vaqt monitoringini amalga oshiradi, operatsion uzluksizlikni kamaytiradi va audit imkoniyatlarini oshiradi. Tarqatilgan tuzilma tufayli tizimlar kiberhujumlar yoki texnik nosozliklar natijasida ishlashni davom ettira oladi. Shu bilan birga, blockchain integratsiyasi moliyaviy, operatsion va identifikatsiya jarayonlarini optimallashtiradi, jarayonlarni tezlashtiradi va xarajatlarni kamaytiradi. Kelajakda blockchainning kiberxavfsizlikdagi roli yanada ortadi. Sun'iy intellekt va mashina o'rganish bilan birlashtirilgan blockchain tizimlari aniq tahdidlarni aniqlash, real vaqt rejimida javob berish va iqtisodiy oqibatlarni minimallashtirish imkonini beradi. Shu tariqa, blockchain texnologiyalari nafaqat himoya mexanizmi, balki operatsion barqarorlikni oshiruvchi strategik vosita sifatida xizmat qilmoqda.

Blockchain asosidagi kiberxavfsizlik mexanizmlari ma'lumotlarni o'zgarmas saqlash, shaffoflik, autentifikatsiya, avtomatlashtirilgan javob mexanizmlari va operatsion uzluksizlikni ta'minlaydi. To'g'ri joriy etilgan blockchain tizimlari tashkilotlarga yuqori darajadagi kiberxavfsizlik, ishonchlilik va global miqyosda barqarorlikni taqdim etadi.

Foydalanilgan adabiyotlar

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>
2. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation Review*, 2, 6–10.
3. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. *PLOS ONE*, 11(10), e0163477. <https://doi.org/10.1371/journal.pone.0163477>

4. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. Proceedings of the IEEE International Congress on Big Data (BigData Congress), 557–564.
5. Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media.
6. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292–2303. <https://doi.org/10.1109/ACCESS.2016.2566339>
7. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55–81.
8. Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? Journal of Governance and Regulation, 6(1), 45–62.