KIBERXAVFSIZLIKNI TA’MINLASHDA BLOCKCHAIN TEXNOLOGIYASINING AHAMIYATI

Chunayev Norquvvat Eshquvat o‘g‘li
Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti,
e-mail: norkuvvatchunaev@gmail.com

Annotatsiya: Bugungi kunda axborot xavfsizligini ta’minlash dolzarb masalalardan biriga aylanmoqda. Blockchain texnologiyasi moliya sektorida kriptovalyutalar orqali keng qo‘llanilmoqda. Biroq, ushbu texnologiya kiberxavfsizlik uchun ham foydalidir. Ushbu maqolada turli tadqiqotchilar tomonidan kiberxavfsizlik sektori uchun taklif etilgan blockchain usullari ko‘rib chiqiladi. Tadqiqot natijalari shuni ko‘rsatdiki, aksariyat olimlar blockchain texnologiyasidan Internet narsalariga (IoT) tegishli qurilmalar, tarmoqlar va ma’lumotlarni himoya qilishda foydalanishga e’tibor qaratgan. Ushbu ishda blockchain yordamida axborot texnologiyalarining uchta muammoli yo‘nalishini himoya qilish bo‘yicha ilgari o‘tkazilgan tadqiqot strategiyalari tahlil qilingan. Tadqiqotning asosiy xulosasi shundan iboratki, kelajakdagi tadqiqotchilar kiberxavfsizlik ilovalari yaratishda yagona blockchain tizimini ishlab chiqishga e’tibor qaratishlari uchun integratsiya va yechimlarning bir xillashtirilishini ta’minlash zarur.

Kalit so‘zlar: Blockchain, Internet narsalar (IoT), kiberxavfsizlik, kompyuter xavfsizligi.

2008-yilda Satoshi Nakamoto tomonidan nashr etilgan rasmiy hisobot – *“Bitcoin: tengdoshlarga asoslangan elektron to‘lov tizimi”* blockchain texnologiyasi ommaga birinchi bor tanishtirilgan holat bo‘ldi. Ushbu hujjatda an’anaviy moliyaviy institutlarni chetlab o‘tuvchi, internet orqali to‘lovlarni amalga oshirishning to‘liq tengdoshlarga asoslangan usuli tasvirlangan. Muallif ushbu tizim blockchain asosida ishlashini tushuntiradi. Bu so‘nggi o‘n yil ichida paydo bo‘lgan innovatsion texnologiya bo‘lib, nafaqat bank sektoriga, balki ishlab chiqarish, ta’lim va kiberxavfsizlik kabi boshqa sohalarga ham ta’sir ko‘rsatishi mumkin [1].

Blockchain tushunchasini tushuntirish uchun uni *reyestr* bilan taqqoslash mumkin. Blockchain mohiyatan tranzaksiya yozuvlari to‘plamidan iborat bo‘lib, har bir yozuv ikki tomon o‘rtasidagi kelishuvni ifodalaydi. Biroq, ushbu tizimning asosiy xususiyati shundaki, ma’lumotlar butun tarmoq bo‘ylab taqsimlanadi, lekin nusxalanmaydi. Markazlashgan server yoki muayyan tashkilot mavjud emas, ya’ni tarmoqdagi barcha ishtirokchilar ma’lumotlarning yagona to‘g‘ri versiyasini tanlash huquqiga ega emaslar.

An’anaviy global veb-tarmoq me’morchiligida *klient-server yondashuvi* qo‘llanilib, barcha kerakli ma’lumotlarni o‘z ichiga olgan markaziy server ishlatiladi. Bunday tuzilma ma’lumotlarni yangilash va barcha ulangan qurilmalarga o‘zgarishlarni yetkazib berishni osonlashtirish uchun mo‘ljallangan. Biroq, blockchain texnologiyasi markazlashmagan bo‘lib, tarmoqdagi har bir kompyuter yozuvlarning to‘g‘riligi va tartibini ta’minlash uchun javobgardir. Ma’lumotlarni o‘zgartirish uchun butun tarmoq ushbu o‘zgarishning haqiqiyligini tasdiqlashi kerak. Bunda ushbu o‘zgarish blockchain tarkibidagi keyingi bloklarning xususiyatlarida aks ettiriladi.

Blockchain tizimida saqlanadigan ma’lumotlar ishonchli bo‘lib, manipulyatsiyaga sezilarli darajada kamroq moyil, chunki u *konsensus protokoli* (yangi ma’lumotlarni tekshirish qoidalarining umumiy to‘plami) va *moliyaviy rag‘batlantirish* (to‘g‘ri tekshirishni amalga oshirgan foydalanuvchilarga mukofot berish) kabi mexanizmlarga asoslanadi [2].

Blockchain tranzaksiyalarini tushunish va ularning kiberxavfsizlik sohasidagi ilovalarini anglash uchun quyidagi asosiy komponentlarni hisobga olish kerak:

Uzel (node) – tengdoshlarga asoslangan tarmoqdagi bitta kompyuter. Har bir uzel blockchain reyestrining to‘liq nusxasiga ega.

Tranzaksiya (transaction) – blockchain zanjiridagi eng kichik element bo‘lib, muayyan ma’lumotlarni yozib boradi.

Blok (block) – bir nechta tranzaksiyalarni o‘z ichiga olgan ma’lumotlar tuzilmasi bo‘lib, u barcha tarmoq uzellari orasida taqsimlanadi.

Zanjir (chain) – blockchainning aniq belgilangan bloklar ketma-ketligi.

Maynerlar (miners) – bloklarni tekshirish va ularni blockchain tuzilmasiga qo‘shish bilan shug‘ullanuvchi uzellarning kichik guruhi. Ushbu tekshiruv natijasida maynerlar moliyaviy mukofot olishlari mumkin. Mayner tomonidan tasdiqlangan blok barcha tarmoq ishtirokchilariga uzatiladi.

Konsensus (consensus protocol) – blockchain bilan bog‘liq operatsiyalarni bajarishda rioya qilinishi kerak bo‘lgan qoidalar to‘plami.

Blockchain – bu kompyuter texnologiyalari kelajagiga ijobiy ta’sir ko‘rsatishi va turli sohalarni rivojlantirishi mumkin bo‘lgan innovatsion texnologiya bo‘lib, u shaffof va ilg‘or yechimlar taqdim etadi. Bu ochiq, o‘zgartirib bo‘lmaydigan va taqsimlangan zanjirlar tizimi bo‘lib, ko‘plab sohalarda amaliy qo‘llanilishi mumkin. Kriptovalyutalarning o‘sishi ushbu texnologiyaning mashhurligini oshirdi, garchi blockchain faqat moliyaviy soha bilan cheklanmaydi.

Blockchain kriptografik bog‘langan bloklar ketma-ketligi sifatida tavsiflanadi. Har bir blok uchta asosiy qismdan iborat: oldingi blokning xesh ma’lumotlari, joriy ma’lumotlarning xeshi va oldingi xesh. Bu bloklar o‘rtasida o‘zaro bog‘liqlikni yaratib, butun zanjir yaxlitligini tekshirish imkonini beradi. Agar bloklardan birining ma’lumotlari o‘zgartirilsa, uning xeshi ham o‘zgaradi, bu esa butun zanjir bo‘ylab

keyingi bloklarning xeshlarini yaroqsiz holga keltiruvchi zanjirli reaksiyaga sabab bo‘ladi. Shu sababli, blockchain tranzaksiyalarini o‘zgartirish imkonsizdir.

Ushbu infratuzilma kiberxavfsizlik muammolariga yechim taklif qilishda juda foydali bo‘lishi mumkin, xususan, *Internet narsalari (IoT) qurilmalari, tarmoqlar, shuningdek, ma’lumotlarni saqlash va uzatish sohalarida* qo‘llanishi mumkin.

Blockchain texnologiyasini tadqiq qilish metodologiyasi

Blockchain – bu taqsimlangan yozuv yuritish modeli bo‘lib, tarmoqdagi tugunlar (uzellar) barcha ma’lumotlarni saqlashi mumkin. Ko‘plab tugunlar buni konsensus yoki ma’lumotlarga murojaat qilish zarurati tufayli amalga oshiradi. Bu markazlashgan ma’lumotlar omboriga bo‘lgan ehtiyojni bartaraf etadi. Har qanday tajovuzkor blockchain’ni buzmoqchi bo‘lsa, u tarmoqdagi aksariyat tugunlarni buzishi kerak bo‘ladi, chunki tarmoq taqsimlangan joylarda saqlanayotgan ma’lumotlar bloklarini tekshirib, farqlanadiganlarini aniqlaydi. Ko‘pincha aksariyat bloklarda to‘g‘ri yoki o‘zgarmagan ma’lumotlar saqlanadi. Blockchain’ning ilg‘or funksiyalari uni zamonaviy xavfsizlik standartlariga mos qiladi.

Ushbu tadqiqotda blockchain texnologiyasining kiberxavfsizlik sanoatida qo‘llanilishini baholash uchun *ikkinchi darajali sifat tahlili* qo‘llanilgan. Tadqiqot blockchain’ning kiberxavfsizlikdagi roliga bag‘ishlangan ilmiy ishlarga asoslanadi. Ishning e’tibor markazi ikkita asosiy jihatdan iborat: birinchidan, blockchain texnologiyasining kiberxavfsizlikda eng so‘nggi qo‘llanilish holatlari ko‘rib chiqiladi; ikkinchidan, blockchain asosida kiberxavfsizlik yechimlarini joriy etish yondashuvlari tahlil qilinadi. Ko‘rib chiqilgan tadqiqotlarning asosiy natijalari va tavsiyalari muhokama qilinib, *blockchain zamonaviy IT-muhitlarda xavfsizlikni qanday ta’minlashi* ko‘rsatib beriladi.

Tadqiqot natijalari

Ko‘plab tadqiqotlar shuni ko‘rsatdiki, blockchain texnologiyasi IoT qurilmalari, tarmoq xavfsizligi va ma’lumotlarni saqlash tizimlarida yanada samaraliroq ishlaydi. Quyidagi jadvalda blockchain xavfsizlik yechimlarining eng so‘nggi amalga oshirilish sohalari ko‘rsatilgan bo‘lib, ularga IoT, tarmoq, ma’lumotlar, ochiq kalit infratuzilmasi (PKI) va ma’lumotlar maxfiyligi kiradi.

Bugungi kunda 9 milliarddan ortiq IoT qurilmalari mavjudligi sababli, blockchain texnologiyasining IoT qurilmalarini himoya qilishga qaratilganligi tushunarli. Chunki ushbu qurilmalar yetarli xavfsizlik konfiguratsiyasiga ega emas, natijada ko‘pchiligi buzilib, botnet tarmoqlariga qo‘shilib ketmoqda. Masalan, Mirai botneti IoT qurilmalaridan tashkil topgan bo‘lib, u Dyn DNS kompaniyasiga qarshi muvaffaqiyatli hujum uyushtirgan. Dyn DNS — bu internetdagi eng yirik domen nomlarini hal qilish firmalaridan biri hisoblanadi [5].

Shuning uchun ko‘plab xavfsizlik tadqiqotchilari blockchain texnologiyasi yordamida IoT qurilmalarini himoya qilish usullarini o‘rganmoqdalar.

1-jadval

Blockchain texnologiyasini amalga oshiradigan qurilmalarda xavfsizlikni samarali amalga oshirish bo‘yicha tavsiyalar

Muammo	– Yechimlar/Tavsiyalar
Maxfiylik	– Markazsizlashtirish va avtorizatsiya o‘rtasidagi muvozanatni saqlash
	– Aralashtirish usullari (xususiy va ochiq platformalar)
	– MimbleWimble usuli
Yaxlitlik	– Ierarxik blokcheyn dizayni
	– Xabarlarni identifikatsiya qilish va autentifikatsiya qilish
Mavjudlik	– Qarshi choralarni muntazam tekshirish
	– Ma’lumotlarni saqlash usullarini takomillashtirish
Autentifikatsiya	– Aqlli shartnomalarni yengil shifrlash usullari bilan birlashtirish
	– SSI va DID usullari
	– Xabarlarni identifikatsiya qilish va autentifikatsiya qilish
Zaifliklar	– Elliptik egri asosidagi shifrlash, atributga asoslangan imzolar, raqamli sertifikatlar, noyoblikni ta’minlash uchun vaqt belgilaridan foydalanish, kriptografik kalitlarning o‘lchamini oshirish
	– Xavfsiz kanallar, tranzaktsiyalarni ajratish, yangi foydalanuvchilar uchun past imtiyozli yondashuv
	– Blokcheyn ierarxik zanjirida bir nechta chaincode orqali kirishni boshqarish
Ishonch	– Global kelishilgan reputatsiya baholash modeli
	– Blokcheynni raqamlashtirish

Blokcheyn kiberxavfsizlik tadqiqotlarining ikkinchi eng keng tarqalgan yo‘nalishi ma’lumotlarni saqlash bilan bog‘liq. Bu ko‘p sonli ma’lumotlar o‘g‘irliklari bilan izohlanadi, chunki xakerlar milliardlab odamlarning ma’lumotlarini o‘z ichiga olgan kompaniyalarga hujum qila olgan. Masalan, 2014-yilda Yahoo buzilishi natijasida uch milliard mijozning ma’lumotlari o‘g‘irlangan, 2021-yil oktabrida esa Instagram buzilishi 1,5 milliard foydalanuvchining ma’lumotlarining sizib chiqishiga olib kelgan. Shu sababli, xavfsizlik bo‘yicha tadqiqotchilar bulut platformalari kabi ma’lumot saqlash joylari uchun blokcheyn xavfsizlik yechimlarini ishlab chiqishga qiziqish bildirmoqda.

Bundan tashqari, tadqiqotchilar blokcheyn texnologiyasining tarmoq xavfsizligida qo‘llanilishini ham o‘rganmoqda. Bu sohadagi tadqiqotlarning aksariyati

autentifikatsiya masalasiga qaratilgan, chunki hozirgi tarmoq xavfsizligi usullari, masalan, WPA shifrlash tizimi, buzilishi va tajovuzkorlar tomonidan foydalanilishi mumkin.

Blokcheynning kiberxavfsizlikdagi yana bir qo‘llanilishi firibgarlik va shaxsiy ma’lumotlarni o‘g‘irlashning oldini olishdir. Foydalanuvchilar doimiy ravishda ruxsatsiz kirish va ma’lumotlarni o‘zgartirish tahdidiga duch kelishadi. Bu ko‘plab foydalanuvchilarning markazlashtirilgan ma’lumot omborlaridan foydalanishi bilan bog‘liq. Masofaviy hujum orqali zaif komponentlarga kirib, tajovuzkorlar ushbu ma’lumot omborlarini buzishi va ma’lumotlarga ruxsatsiz kirishi yoki ularni o‘zgartirishi mumkin. Biroq, blokcheyn asosidagi tarqatilgan ma’lumot omborlari bunday tahdidlarga qarshi himoya qiladi. Masalan, saylov natijalari kabi maxfiy ma’lumotlar minglab kompyuterlarda saqlanishi mumkin, va har bir kompyuter ushbu ma’lumotlarning nusxasiga ega bo‘ladi. Agar xaker barcha nusxalar mavjud bo‘lgan tizimlarga yetarlicha kira olmasa, faqat bir nechta tizimlarni buzish butun tarmoq ma’lumotlariga ta’sir qilmaydi.

Shuningdek, blokcheyn texnologiyasining maxfiylikni ta’minlashdagi xavfsizlik yechimlariga katta qiziqish mavjud. Ko‘plab tadqiqotlar shaxsiy ma’lumotlarni blokcheyn asosida universal autentifikatsiya sxemasi yordamida himoya qilish yo‘llarini o‘rganmoqda. Bu foydalanuvchilarga o‘z ma’lumotlarini turli tashkilotlarga taqdim etish zaruratidan xalos qiladi, chunki blokcheyn ularning shaxsini tasdiqlash uchun ishlatiladi.

Shunday savol tug‘iladi: blokcheyn texnologiyasi qanday qilib kiberxavfsizlikni oshirishga yordam berishi mumkin? Zamonaviy xavfsizlik tizimlari yuqori darajadagi himoyani ta’minlaydi, ammo ularning ham zaif tomonlari bor. Buning sababi shundaki, aksariyat xavfsizlik mahsulotlari IT-resurslarni himoya qilishda mustaqil ishlashga mo‘ljallangan. Masalan, DDoS hujumlari (taqsimlangan xizmatdan voz kechish hujumi) davomida xakerlar xavfsizlik tizimining faqat bitta komponentiga hujum qilib, uni ishdan chiqarishi va keyin himoyasiz qolgan IT-resursga hujum uyushtirishi mumkin.

Blokcheyn texnologiyasining xavfsizlikni oshirish imkoniyatlarini o‘rganuvchi tadqiqotchilar ushbu texnologiyaning taqsimlangan xavfsizlik vositalari orqali mustahkamroq himoya ta’minlashi mumkinligiga ishora qiladi. Tadqiqot natijalari shuni ko‘rsatadiki, blokcheyn qurilmalar, ma’lumotlar va Internet-of-Things (IoT) tarmoqlarining xavfsizligini ta’minlashda muhim rol o‘ynashi mumkin. IoT tarmoqlarida ruxsatsiz kirish va qurilmalarni boshqarish eng jiddiy xavfsizlik zaifligidir.

Blokcheyn asosidagi xavfsizlik yechimlari barcha IoT qurilmalar uchun kirishni boshqarish va ma’lumotlar almashinuvini yaxshiroq nazorat qilish imkonini beradi.

Blokcheyn orqali foydalanuvchilarni aniq identifikatsiya qilish, autentifikatsiya qilish va ma’lumotlar uzatish jarayonlarini xavfsiz amalga oshirish mumkin. Ruxsatsiz kirishning oldini olish uchun blokcheyn ishonchli ulanishlar va sessiyalar tarixini taqsimlangan shaklda saqlash orqali ishlaydi. Yangi ulanishlar faqat oldingi ishonchli ulanishlarning ko‘pchiligi yangi foydalanuvchini tasdiqlagan taqdirdagina amalga oshirilishi mumkin. Masalan, IoT qurilmasi sifatida IP-kamera faqat ishonchli uy qurilmalariga kirish imkonini beradi. Agar xaker kamera tizimiga kirishga harakat qilsa, blokcheyn asosidagi xavfsizlik yechimi unga kirish huquqini taqiqlaydi, agar ishonchli qurilmalar ko‘pchilik ovozi bilan uni tasdiqlamasa.

Tadqiqotchilar ma’lumotlar xavfsizligidagi eng katta zaifliklardan biri yagona nuqtali ishdan chiqish yoki buzilish ekanligini aniqlagan. Bunday zaiflik natijasida ma’lumotlarning o‘g‘irlanishi, o‘zgartirilishi yoki butunlay yo‘qolishi mumkin.

Blokcheyn texnologiyasi rivojlanib, zamonaviy dunyoda tobora ko‘proq qo‘llanmoqda. Kiberxavfsizlik ushbu texnologiya o‘rganilgan va amalga oshirilgan istiqbolli sohalardan biri hisoblanadi. Blokcheyn infratuzilmasi IoT qurilmalari, tarmoqlar, ma’lumotlarni saqlash va uzatish kabi sohalarda mavjud xavfsizlik muammolarini hal qilish imkonini beradi. Ushbu ishda zamonaviy olimlar tadqiqotlarida blokcheyn texnologiyasining qo‘llanilishi tahlil qilinadi. Tadqiqotlar shuni ko‘rsatdiki, blokcheyn xavfsizligi bo‘yicha ko‘pgina tadqiqotchilar IoT qurilmalari uchun xavfsizlik mexanizmlarini joriy etishga katta e’tibor qaratmoqdalar. Tarmoqlar va ma’lumotlar ham blokcheyn xavfsizligining muhim jihatlaridan biri hisoblanadi. Blokcheyn texnologiyalarining boshqa qo‘llanilish sohalari ham o‘rganilgan bo‘lsa-da, xavfsizlik zamonaviy raqamli texnologiyalar dunyosida eng muhim omil hisoblanadi. Ushbu tadqiqot blokcheyn an’anaviy xavfsizlik texnologiyalarining doirasidan tashqariga chiqadigan jiddiy xavfsizlik kamchiliklarini bartaraf etishga qodir ekanligini ko‘rsatadi.

Foydalanilgan adabiyotlar

1. Xabibullayev J.D., DDoS-hujumlarning oldini olishda blockchain texnologiyasining imkoniyatlarini tahlili // Лучшие интеллектуальные исследования, 2025-yil 26-fevral. Vol. 39, №-3. –b 121-131.
2. Chunayev N.E., Xabibullayev J.D., Application of blockchain technology to ensuring reliability and data security in the internet of things, “Moliya-kredit tizimini strategik rivojlantirishning muammolari va ustuvor yo‘nalishlari” mavzusida xalqaro ilmiy-amaliy konferensiya 2024-yil 25-aprel. –b. 27-29.
3. Базанов С. Биткоин: Одноранговая электронная денежная система // Medium.com, 2019, URL: medium.com/bitcoin-review/биткоин-одноранговая-электронная-денежная-система-c66b254385d2

4. Алтынов Д.С., Пиневич Е.В., Годунов А.Е., Шенявский Н.И. Blockchain в системе обеспечения транспортной безопасности // Инженерный вестник Дона, 2022, №1. URL: ivdon.ru/ru/magazine/archive/n1y2022/7422
5. Пескова О.Ю., Половко И.Ю., Захарченко А.Д. Применение блокчейн-технологий в системах электронного документооборота: анализ и программная реализация // Инженерный вестник Дона, 2019, №3. URL: ivdon.ru/ru/magazine/archive/N3y2019/5801
6. Ibrahim R.F., Abu Al-Haija Q., Ahmad A. DDoS Attack Prevention for Internet of Thing Devices Using Ethereum Blockchain Technology. Sensors 2022. 22(6806). pp. 1-21.
7. Radivilova T., Hassan H.A. Test for penetration in Wi-Fi network: attacks on WPA2-PSK and WPA2-Enterprise. 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo). 2017. pp. 1-4.