BLOKCHEYN ASOSIDA MA'LUMOTLAR XAVFSIZLIGINI TA'MINLASH USULLARI

Abdupattayev Xondamirjon Elyorjon o'g'li
University of management and future technologies
1-kurs magistranti
https://doi.org/10.5281/zenodo.20594906

Annotatsiya. Mazkur maqolada blokcheyn texnologiyasining ma'lumotlar xavfsizligini ta'minlashdagi o'rni va ahamiyati tahlil qilingan. Blokcheynning ishlash tamoyillari, kriptografik himoya mexanizmlari, konsensus algoritmlari, aqlli shartnomalar hamda markazlashtirilmagan ma'lumotlar bazalarining xavfsizlik afzalliklari yoritilgan. Shuningdek, blokcheyn texnologiyasining moliya, sog'liqni saqlash, elektron hukumat, bulutli hisoblash va Internet of Things tizimlarida qo'llanilishi hamda ma'lumotlarning maxfiyligi, yaxlitligi va ishonchliligini ta'minlashdagi imkoniyatlari ko'rib chiqilgan.
Kalit so'zlar: blokcheyn, kiberxavfsizlik, kriptografiya, xeshlash, autentifikatsiya, konsensus, maxfiylik, reyestr, tranzaksiya, shifrlash, xavfsizlik, bulut, IoT, identifikatsiya.

KIRISH

Zamonaviy jamiyatda axborot va raqamli texnologiyalar hayotning barcha sohalariga chuqur kirib bormoqda. Davlat boshqaruvi, iqtisodiyot, ta'lim, sog'liqni saqlash, sanoat va xizmat ko'rsatish tarmoqlarida turli axborot tizimlari va raqamli platformalardan keng foydalanilmoqda. Raqamlashtirish jarayonlarining jadallashuvi natijasida ma'lumotlar hajmi ortib borayotganligi, ularni saqlash, qayta ishlash va uzatish bilan bog'liq masalalarga bo'lgan e'tiborni kuchaytirmoqda. Shu bilan birga, axborot resurslarini turli tahdidlar va noqonuniy ta'sirlardan himoya qilish dolzarb vazifalardan biriga aylanmoqda.

Bugungi kunda axborot xavfsizligini ta'minlash masalasi nafaqat texnik, balki iqtisodiy va ijtimoiy ahamiyatga ham ega. Ma'lumotlarning yo'qolishi, o'zgartirilishi yoki ruxsatsiz tarqalishi tashkilotlar faoliyatiga salbiy ta'sir ko'rsatishi, moddiy zararlar keltirib chiqarishi hamda foydalanuvchilar ishonchining pasayishiga sabab bo'lishi mumkin. Shu bois ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta'minlay oladigan zamonaviy texnologiyalarni ishlab chiqish va amaliyotga joriy etish muhim ahamiyat kasb etmoqda.

So'nggi yillarda axborot xavfsizligini ta'minlashga qaratilgan innovatsion yondashuvlar va texnologiyalar faol rivojlanmoqda. Ular orasida markazlashtirilmagan ma'lumotlar bazalari, kriptografik himoya vositalari hamda taqsimlangan axborot tizimlari alohida o'rin tutadi. Bunday texnologiyalar ma'lumotlarning ishonchliligini oshirish, ularni noqonuniy o'zgartirishdan himoya qilish hamda axborot almashinuvi jarayonlarining xavfsizligini ta'minlash imkonini beradi. Axborot texnologiyalarining rivojlanishi bilan bir qatorda ma'lumotlarni himoyalashga bo'lgan talab ham ortib bormoqda. Shu sababli zamonaviy xavfsizlik mexanizmlarini o'rganish, ularning afzalliklari va amaliy imkoniyatlarini tahlil qilish ilmiy tadqiqotlarning muhim yo'nalishlaridan biri hisoblanadi.

ASOSIY QISM

Blokcheyn texnologiyasi ma'lumotlarni saqlash va uzatishning zamonaviy usullaridan biri bo'lib, u markazlashtirilmagan boshqaruv tamoyiliga asoslanadi. Mazkur texnologiyada ma'lumotlar ketma-ket joylashtirilgan bloklar ko'rinishida saqlanadi va har bir yangi blok avvalgi blok bilan kriptografik bog'lanadi. Natijada bloklar zanjiri hosil bo'ladi. Ushbu tuzilma ma'lumotlarning yaxlitligini ta'minlashda muhim ahamiyat kasb etadi, chunki zanjirdagi biror blokdagi ma'lumotni o'zgartirish uchun undan keyingi barcha bloklarni ham qayta hisoblash talab etiladi. Bu esa amaliy jihatdan juda murakkab jarayon bo'lib, ma'lumotlarni qalbakilashtirish imkoniyatini keskin kamaytiradi.

Blokcheyn asosida ma'lumotlar xavfsizligini ta'minlashning eng muhim usullaridan biri kriptografik himoya mexanizmlaridan foydalanish hisoblanadi. Tizimda har bir tranzaksiya yoki ma'lumotlar yozuvi maxsus matematik algoritmlar yordamida shifrlanadi. Xesh-funksiyalar ma'lumotlarning o'zgarmasligini nazorat qilishda asosiy vosita bo'lib xizmat qiladi. Har bir blok

o‘zining noyob xesh qiymatiga ega bo‘ladi va ushbu qiymat blok tarkibidagi ma’lumotlarga bog‘liq ravishda shakllanadi. Agar blokdagi biror belgi o‘zgartirilsa ham xesh qiymati to‘liq o‘zgaradi. Shu sababli tarmoq ishtirokchilari ma’lumotlarning buzilganligini tezda aniqlash imkoniyatiga ega bo‘ladi. Kriptografik himoya mexanizmlari blokcheyn tizimining asosiy xavfsizlik qatlamini tashkil etib, ma’lumotlarni ruxsatsiz o‘zgartirish va qalbakilashtirishdan himoya qiladi.

Blokcheyn texnologiyasida ochiq va yopiq kalitlar asosidagi raqamli imzo tizimi ham keng qo‘llaniladi. Har bir foydalanuvchi o‘zining shaxsiy kaliti va ommaviy kalitiga ega bo‘ladi. Tranzaksiyalar shaxsiy kalit yordamida imzolanadi va boshqa ishtirokchilar ommaviy kalit orqali ushbu tranzaksiyaning haqiqiyligini tekshiradi. Mazkur yondashuv ma’lumotlar manbasini aniq identifikatsiya qilish, foydalanuvchi autentifikatsiyasini ta’minlash va tranzaksiyalarni inkor etish holatlarining oldini olish imkonini beradi. Natijada tizimda yuqori darajadagi ishonchlilik va shaffoflik shakllanadi.

Ma’lumotlar xavfsizligini ta’minlashda konsensus algoritmlarining o‘rni ham katta hisoblanadi. Konsensus mexanizmi tarmoqdagi barcha tugunlarning ma’lumotlar bo‘yicha yagona qarorga kelishini ta’minlaydi. Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Authority (PoA) kabi algoritmlar blokcheyn tizimlarida keng qo‘llaniladi. Ushbu mexanizmlar yordamida tarmoqdagi yangi bloklar tekshiriladi va tasdiqlanadi. Konsensus algoritmlarining asosiy vazifasi noto‘g‘ri yoki soxta ma’lumotlarning blokcheynga kiritilishining oldini olishdan iborat. Shu sababli blokcheyn tizimlarida markaziy nazorat organisiz ham ma’lumotlarning ishonchliligini saqlash mumkin bo‘ladi.

Blokcheyn asosidagi xavfsizlikning yana bir muhim jihati ma’lumotlarning taqsimlangan holda saqlanishidir. An’anaviy ma’lumotlar bazalarida barcha ma’lumotlar bitta markaziy serverda joylashgan bo‘lsa, blokcheynda ma’lumotlarning nusxalari tarmoqdagi ko‘plab tugunlarda saqlanadi. Agar tarmoqning bir qismi ishdan chiqsa yoki kiberhujumga uchrasa ham qolgan tugunlar ma’lumotlarning saqlanishini va tizim faoliyatining davom etishini ta’minlaydi. Bu xususiyat blokcheynni xizmat ko‘rsatishni rad etish (DDoS) hujumlari, apparat nosozliklari va ma’lumotlarning yo‘qolishi kabi xavflarga nisbatan barqarorroq qiladi.

Zamonaviy axborot tizimlarida aqlli shartnomalar (Smart contracts) ham ma’lumotlar xavfsizligini ta’minlashda muhim vosita sifatida qo‘llanilmoqda. Aqlli shartnomalar oldindan belgilangan qoidalar asosida avtomatik ravishda bajariladigan dasturiy kodlardan iborat. Ular vositachilarsiz ishlaydi va barcha operatsiyalar blokcheyn tarmog‘ida qayd etiladi. Bu esa inson omili bilan bog‘liq xatolarni kamaytiradi hamda firibgarlik xavfini pasaytiradi. Ayniqsa moliyaviy operatsiyalar, elektron hujjat aylanishi va elektron savdo tizimlarida aqlli shartnomalarning qo‘llanilishi xavfsizlik darajasini sezilarli ravishda oshirmoqda.

Sog‘liqni saqlash tizimlarida blokcheyn texnologiyasi bemorlarning tibbiy ma’lumotlarini himoya qilishda keng istiqbollarga ega. Tibbiy ma’lumotlar yuqori darajada maxfiy hisoblanganligi sababli ularni himoyalash katta ahamiyatga ega. Blokcheyn yordamida bemor ma’lumotlari shifrlangan holda saqlanadi va ulardan foydalanish huquqi faqat ruxsat berilgan shaxslargagina taqdim etiladi. Shu bilan birga, ma’lumotlarga kim, qachon va qanday murojaat qilganligi to‘g‘risidagi ma’lumotlar ham blokcheynda qayd etiladi. Bu esa ma’lumotlar ustidan nazoratni kuchaytiradi va noqonuniy foydalanish holatlarini kamaytiradi.

Moliyaviy sektor blokcheyn texnologiyasidan eng faol foydalanayotgan sohalardan biri hisoblanadi. Banklar va to‘lov tizimlari blokcheyn asosida xavfsiz tranzaksiyalarni amalga oshirish, firibgarlik holatlarini aniqlash va operatsion xarajatlarni qisqartirish imkoniyatiga ega bo‘lmoqda. Tranzaksiyalarni tasdiqlash jarayonining markazlashtirilmaganligi tufayli ma’lumotlarni soxtalashtirish yoki noqonuniy o‘zgartirish deyarli imkonsiz holga keladi. Natijada moliyaviy operatsiyalarning xavfsizligi va shaffofligi sezilarli darajada ortadi. Shuningdek, blokcheyn texnologiyasi Internet of Things (IoT) qurilmalari xavfsizligini ta’minlashda ham samarali vosita sifatida qaralmoqda. IoT muhitida millionlab qurilmalar o‘zaro ma’lumot almashadi va bu jarayon xavfsizlik bilan bog‘liq muammolarni yuzaga keltiradi. Blokcheyn yordamida qurilmalar autentifikatsiyasi, ma’lumotlar almashinuvi va kirishni boshqarish jarayonlari ishonchli tarzda tashkil etilishi mumkin. Natijada qurilmalar o‘rtasidagi aloqalar xavfsizligi oshadi va kiberhujumlar ehtimoli kamayadi. Shu bilan birga, blokcheyn texnologiyasining ayrim cheklovlari ham mavjud. Xususan, ayrim konsensus algoritmlarining yuqori energiya sarfi,

tranzaksiyalarni qayta ishlash tezligining cheklanganligi va katta hajmdagi ma’lumotlarni saqlash bilan bog‘liq muammolar tadqiqotchilar tomonidan faol o‘rganilmoqda. Biroq yangi avlod blokcheyn platformalari ushbu kamchiliklarni bartaraf etishga qaratilgan innovatsion yechimlarni taklif qilmoqda. Shuning uchun blokcheyn texnologiyasi kelajakda ma’lumotlar xavfsizligini ta’minlashning eng istiqbolli vositalaridan biri sifatida o‘z ahamiyatini yanada oshirishi kutilmoqda.

Blokcheyn asosida ma’lumotlar xavfsizligini ta’minlashda ruxsat darajalarini boshqarish mexanizmlari alohida ahamiyat kasb etadi. Ochiq blokcheyn tarmoqlarida istalgan foydalanuvchi tarmoqqa ulanishi va ma’lumotlarni ko‘rishi mumkin bo‘lsa, korporativ va davlat axborot tizimlarida ko‘pincha ruxsat etilgan (Permissioned Blockchain) blokcheynlardan foydalaniladi. Bunday tizimlarda tarmoq ishtirokchilari oldindan ro‘yxatdan o‘tkaziladi va ularga aniq vakolatlar beriladi. Natijada ma’lumotlardan foydalanish, yozuvlarni kiritish yoki tasdiqlash jarayonlari qat’iy nazorat ostida amalga oshiriladi. Bu yondashuv ayniqsa bank sektori, davlat reyestrlari, soliq tizimlari va korporativ ma’lumotlar bazalarida yuqori samaradorlikni ta’minlaydi.

Ma’lumotlarning kuzatiluvchanligi (traceability) blokcheyn texnologiyasining yana bir muhim afzalliklaridan hisoblanadi. Tizimga kiritilgan har bir yozuv vaqt belgisi bilan birga saqlanadi va uning butun tarixini kuzatish mumkin bo‘ladi. Ushbu xususiyat ma’lumotlarning kelib chiqish manbasini aniqlash, o‘zgarishlar tarixini tekshirish va audit jarayonlarini soddalashtirish imkonini beradi. Korxona va tashkilotlarda ma’lumotlarning qachon yaratilgani, kim tomonidan o‘zgartirilgani yoki qaysi foydalanuvchi tomonidan foydalanilgani haqidagi ma’lumotlar avtomatik tarzda qayd etiladi. Natijada ichki nazorat tizimlari samaradorligi ortadi va noqonuniy harakatlarni aniqlash imkoniyati kengayadi.

Blokcheyn texnologiyasi elektron hujjat aylanish tizimlarida ham ma’lumotlar xavfsizligini ta’minlashning samarali vositasi sifatida qo‘llanilmoqda. An’anaviy hujjat almashinuvida hujjatlarning yo‘qolishi, o‘zgartirilishi yoki qalbakilashtirilishi xavfi mavjud bo‘lsa, blokcheyn asosidagi tizimlarda hujjatning raqamli izi yaratiladi va u bloklar zanjirida saqlanadi. Hujjatning asl nusxasi o‘zgartirilgan taqdirda ham uning dastlabki holati va o‘zgarishlar tarixi saqlanib qoladi. Bu esa davlat xizmatlari, sud-huquq tizimi, notarial xizmatlar va korporativ boshqaruvda hujjatlar ishonchliligini sezilarli darajada oshiradi.

Kiberxavfsizlik nuqtai nazaridan blokcheyn texnologiyasi markazlashgan autentifikatsiya tizimlariga muqobil yechim sifatida ham qaralmoqda. Hozirgi kunda ko‘plab axborot tizimlari foydalanuvchi identifikatsiyasini markaziy serverlar orqali amalga oshiradi. Ushbu serverlarning buzilishi yoki ishdan chiqishi katta hajmdagi foydalanuvchi ma’lumotlarining sizib chiqishiga olib kelishi mumkin. Markazlashtirilmagan identifikatsiya (Decentralized Identity) konsepsiyasida esa foydalanuvchilar o‘z raqamli identifikatorlarini mustaqil boshqaradilar. Shaxsiy ma’lumotlar yagona serverda emas, balki blokcheyn asosidagi xavfsiz muhitda saqlanadi. Natijada identifikatsiya ma’lumotlarini o‘g‘irlash va noqonuniy foydalanish xavfi kamayadi.

Blokcheynning ma’lumotlar xavfsizligidagi istiqbolli yo‘nalishlaridan biri ko‘p tomonlama ma’lumot almashish jarayonlarini himoyalash hisoblanadi. Zamonaviy tashkilotlar faoliyatida ma’lumotlar turli idoralar, kompaniyalar va foydalanuvchilar o‘rtasida uzluksiz almashinib turadi. Bunday jarayonlarda ma’lumotlarning haqiqiyligini tekshirish va ishonchli uzatilishini ta’minlash murakkab vazifa hisoblanadi. Blokcheyn tarmog‘i barcha ishtirokchilarga yagona va o‘zgarmas ma’lumotlar manbasini taqdim etishi orqali ushbu muammoni hal qiladi. Natijada ma’lumotlarning turli versiyalari paydo bo‘lishi yoki ular ustida noqonuniy o‘zgartirishlar kiritilishi ehtimoli kamayadi.

Bulutli hisoblash muhitida blokcheyn texnologiyasidan foydalanish ham so‘nggi yillarda keng rivojlanmoqda. Bulutli xizmatlar katta hajmdagi ma’lumotlarni saqlash va qayta ishlash imkoniyatini bersa-da, foydalanuvchilar ko‘pincha ma’lumotlar xavfsizligi va maxfiyligidan xavotir bildiradilar. Blokcheyn yordamida bulutli muhitda saqlanayotgan ma’lumotlarning yaxlitligini nazorat qilish, kirish huquqlarini boshqarish va audit yozuvlarini yuritish mumkin. Bu esa bulutli platformalarga bo‘lgan ishonchni oshiradi hamda ma’lumotlarning noqonuniy o‘zgartirilishiga qarshi qo‘shimcha himoya qatlamini yaratadi.

So‘nggi yillarda blokcheyn va sun’iy intellekt texnologiyalarining integratsiyasi ham ma’lumotlar xavfsizligini ta’minlashda yangi imkoniyatlarni yuzaga keltirmoqda. Sun’iy intellekt tizimlari katta hajmdagi ma’lumotlarni tahlil qilish va xavfsizlik tahdidlarini aniqlash imkoniyatiga ega bo‘lsa,

blokcheyn ushbu ma’lumotlarning ishonchliligini va o‘zgarmasligini ta’minlaydi. Natijada xavfsizlik hodisalarini aniqlash, firibgarlik harakatlarini bashorat qilish va avtomatik himoya mexanizmlarini ishga tushirish samaradorligi ortadi. Ushbu ikki texnologiyaning uyg‘unlashuvi kelajakda yanada xavfsiz va aqlli axborot tizimlarini yaratishga xizmat qiladi.

Davlat boshqaruvi tizimlarida blokcheyn texnologiyasidan foydalanish fuqarolar ma’lumotlarini himoyalash va davlat xizmatlari shaffofligini oshirish imkonini bermoqda. Yer kadastri, mulk huquqi, aholi reyestri va boshqa muhim ma’lumotlar blokcheyn asosida yuritilganda ularning noqonuniy o‘zgartirilishi yoki yo‘q qilinishi ehtimoli sezilarli darajada kamayadi. Bundan tashqari, davlat organlari o‘rtasidagi ma’lumot almashinuvi jarayoni tezlashadi va ma’lumotlarning ishonchlilik darajasi ortadi. Shu sababli ko‘plab mamlakatlar blokcheyn texnologiyasini elektron hukumat tizimlariga bosqichma-bosqich joriy etish ustida ish olib bormoqda.

XULOSA

Xulosa qilib aytganda, zamonaviy axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi ma’lumotlar xavfsizligini ta’minlash masalasining ahamiyatini yanada oshirmoqda. Raqamli ma’lumotlar hajmining ortib borishi, axborot almashinuvi jarayonlarining kengayishi hamda kiberxavflarning murakkablashuvi mavjud himoya mexanizmlarini takomillashtirish zaruratini yuzaga keltirmoqda. Shu sababli ma’lumotlarni saqlash, uzatish va qayta ishlash jarayonlarida xavfsizlikni ta’minlay oladigan zamonaviy texnologiyalardan samarali foydalanish muhim vazifalardan biri hisoblanadi.

Tadqiqot natijalari shuni ko‘rsatadiki, yangi avlod axborot texnologiyalari ma’lumotlarning yaxlitligi, ishonchliligi va himoyalanganlik darajasini oshirishda muhim ahamiyat kasb etadi. Ularning amaliyotga joriy etilishi axborot tizimlari faoliyatining barqarorligini ta’minlash, ma’lumotlar bilan bog‘liq xavflarni kamaytirish hamda foydalanuvchilar o‘rtasidagi ishonchni mustahkamlash imkonini beradi. Ayniqsa, raqamli transformatsiya sharoitida axborot resurslarini samarali boshqarish va himoyalash masalalari dolzarb ilmiy-amaliy yo‘nalishlardan biri bo‘lib qolmoqda. Shu bilan birga, zamonaviy texnologiyalarni joriy etish jarayonida texnik, tashkiliy va huquqiy muammolar ham mavjud bo‘lib, ularni bartaraf etish bo‘yicha ilmiy izlanishlarni davom ettirish zarur. Axborot xavfsizligi sohasida innovatsion yondashuvlarni rivojlantirish, ilg‘or texnologiyalarni amaliyotga tatbiq etish hamda kiberxavfsizlik madaniyatini yuksaltirish kelgusida yanada ishonchli va barqaror axborot muhitini shakllantirishga xizmat qiladi. Umuman olganda, axborot xavfsizligini ta’minlash zamonaviy jamiyat taraqqiyotining muhim omillaridan biri bo‘lib, ushbu yo‘nalishda olib borilayotgan ilmiy tadqiqotlar va amaliy ishlanmalar raqamli iqtisodiyotning barqaror rivojlanishiga, axborot resurslarining himoyalanganligini ta’minlashga hamda raqamli texnologiyalardan samarali foydalanishga keng imkoniyatlar yaratadi.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi Prezidenti. “Raqamli O‘zbekiston – 2030” strategiyasi to‘g‘risida. – Toshkent, 2020.
2. Abduqodirov A. A., Hayitov O. R. Axborot xavfsizligi asoslari. – Toshkent: O‘zbekiston Respublikasi IIV Akademiyasi, 2021. – 312 b.
3. Aripov M. M., Muhammadiyev J. O. Axborot texnologiyalari va tizimlari. – Toshkent: Fan va texnologiya, 2020. – 384 b.
4. Maraximov A. R., To‘rayev X. Axborot xavfsizligi. – Toshkent: Aloqachi, 2019. – 288 b.
5. Sodiqov A. S. Kiberxavfsizlik asoslari va amaliyoti. – Toshkent: Innovatsion rivojlanish nashriyoti, 2022. – 276 b.
6. Umarov B. A., Yuldashev N. T. Raqamli iqtisodiyot va zamonaviy axborot texnologiyalari. – Toshkent: Iqtisodiyot, 2021. – 340 b.
7. Aripov M. M. Informatika, axborot texnologiyalari. – Toshkent: O‘qituvchi, 2019. – 432 b.
8. Xolmatov D. Sh. Ma’lumotlarni himoyalashning zamonaviy usullari. – Toshkent: Tafakkur, 2021. – 248 b.