BLOKCHEYN TEXNOLOGIYASINING ARXITEKTURASI VA AXBOROT XAVFSIZLIGINI TA’MINLASHDAGI O‘RNI

Chunayev Norquvvat
Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti,
e-mail: norkuvvatchunaev@gmail.com
Xabibullayev Jahongirbek Doniyorbek o‘g‘li
Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti
e-mail: j.xabibullayev@tuit.uz

Annotatsiya: *So‘nggi yillarda axborot xavfsizligini ta’minlash sohasida markazlashmagan texnologiyalarga bo‘lgan qiziqish keskin ortib bormoqda. An’anaviy markazlashgan tizimlarda mavjud bo‘lgan zaifliklar, xususan yagona nosozlik nuqtasi (Single Point of Failure), ma’lumotlarni o‘zgartirish xavfi va ishonch muammolari yangi texnologik yondashuvlarni talab qilmoqda. Ana shunday innovatsion yechimlardan biri sifatida blokcheyn texnologiyasi alohida e’tiborga loyiqdir. Shu sababli zamonaviy axborot tizimlarida blokcheyn texnologiyasining tutgan o‘rni, uning o‘ziga xos arxitekturasi va ishlash prinsiplari tahlil qilinadi. Markazlashgan tizimlardagi “yagona nosozlik nuqtasi” muammosini hal qilishda blokcheynning kriptografik algoritmlari va konsensus mexanizmlarining ahamiyati yoritilgan.*

Kalit so‘zlar: blokcheyn, arxitektura, kriptografik xesh, konsensus, markazlashmaganlik, axborot xavfsizligi, NIST.

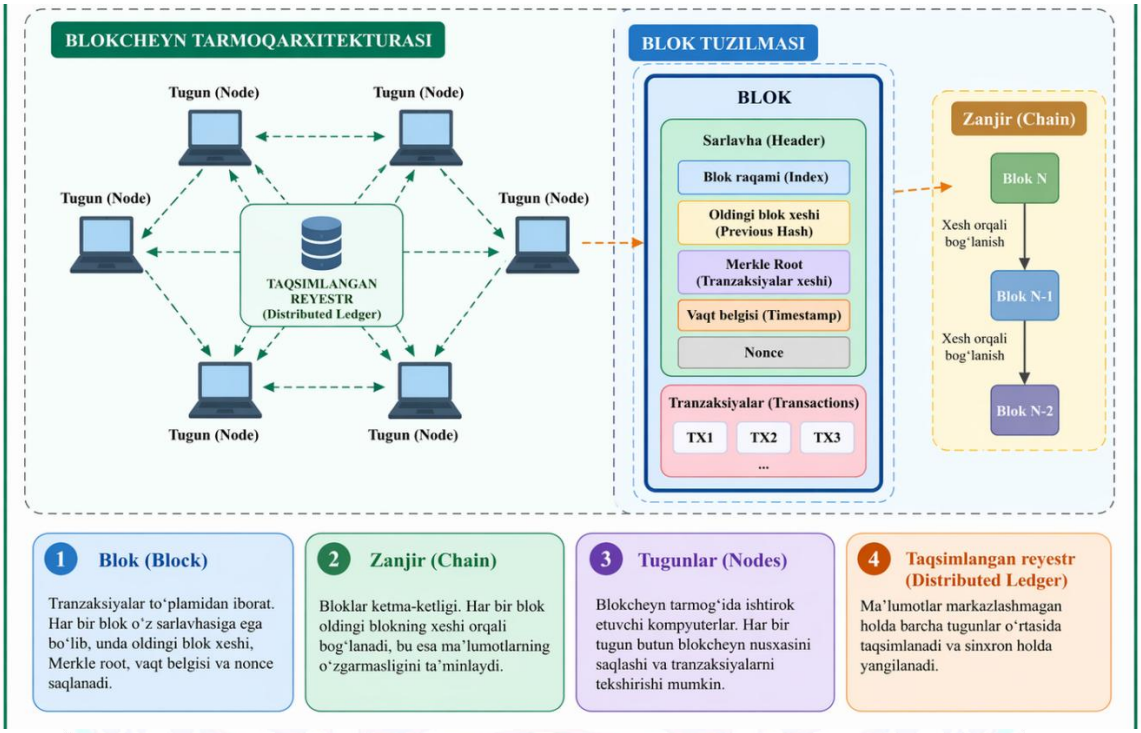
Blokcheyn texnologiyasi zamonaviy axborot tizimlari ichida eng ko‘p muhokama qilinayotgan va amaliyotga keng joriy etilayotgan yondashuvlardan biri hisoblanadi. Uning paydo bo‘lishi markazlashgan tizimlarning ayrim cheklovlari, xususan bitta markazga haddan tashqari bog‘liqlik, tranzaksiyalarni tasdiqlashda vositachilarga ehtiyoj, yozuvlarni soxtalashtirish xavfi hamda ishonchni uchinchi tomon orqali tashkil etish zarurati bilan bog‘liq edi. Blokcheyn aynan shu muammolarga javob sifatida shakllandi: u ma’lumotlarni markazlashmagan tarzda saqlash, barcha ishtirokchilar uchun yagona kelishilgan reyestr yuritish va yozuvlarning keyinchalik o‘zgartirilishini amalda juda qiyinlashtirish imkonini beradi. NIST blokcheynni markaziy repozitoriy va odatda markaziy boshqaruvsiz ishlaydigan, kriptografik bog‘langan bloklar asosida qurilgan, buzilganini ko‘rsatadigan va buzishga chidamli taqsimlangan raqamli reyestr sifatida tavsiflaydi.

Blokcheynning shakllanish tarixi birgina 2008-yildan boshlanmaydi. Uning nazariy ildizlari kriptografiya, taqsimlangan tizimlar va vaqt belgisi qo‘yish texnologiyalariga borib taqaladi. 1990-yillarda ma’lumotlarga vaqt tamg‘asi qo‘yish va hujjatlarning keyinchalik o‘zgartirilmaganini isbotlashga qaratilgan ishlanmalar paydo bo‘lgan. Keyinchalik ushbu g‘oyalar xesh-funksiyalar, raqamli imzo va zanjir ko‘rinishida bog‘langan yozuvlar konsepsiyasi bilan boyidi. Biroq blokcheynni mustaqil, yaxlit va ishlaydigan tizim ko‘rinishida dunyoga tanitgan asosiy voqea 2008-yilda Satoshi Nakamoto taxallusi ostida e’lon qilingan *Bitcoin: A Peer-to-Peer Electronic Cash System* nomli maqola bo‘ldi. Ushbu maqolada muallif internet orqali to‘g‘ridan to‘g‘ri elektron to‘lovlarni moliyaviy vositachisiz amalga oshirish g‘oyasini ilgari surdi va asosiy muammo sifatida “double-spending”, ya’ni bitta raqamli aktivni ikki marta sarflash masalasini ko‘rsatdi. Nakamoto bu muammoni peer-to-peer tarmoq, vaqt tamg‘asi serveri, xeshlash va proof-of-work yordamida hal qilishni taklif qildi.

Shu jihatdan aytish mumkinki, blokcheynni “kim ishlab chiqqan?” degan savolga ilmiy nuqtai nazardan eng to‘g‘ri javob — uni zamonaviy amaliy model sifatida *Satoshi Nakamoto* taklif qilganidir. 2008-yilda konsepsiya e’lon qilingan, 2009-yilda esa Bitcoin tarmog‘ining dastlabki ishlaydigan versiyasi ishga tushirilgan. Nakamoto maqolasida raqamli tangani “raqamli imzolar zanjiri” sifatida izohlaydi: har bir egasi avvalgi tranzaksiya xeshini va keyingi egasining ochiq kalitini imzolash orqali aktivni boshqasiga uzatadi. Biroq bu modelning markazsiz ishlashi uchun barcha ishtirokchilar tranzaksiyalar ketma-ketligining yagona tarixiga kelishib olishi kerak bo‘ladi. Aynan shu yerda blokcheynning asosiy yangiligi namoyon bo‘ladi: tranzaksiyalar ketma-ketligi bitta tashkilot bazasida emas, balki tarmoq tugunlari o‘rtasida birgalikda yuritiladi.

Blokcheyn atamasining o‘zi “bloklar zanjiri” ma’nosini anglatadi. Uning mohiyati shundaki, tarmoqdagi tranzaksiyalar alohida bloklarga jamlanadi, har bir yangi blok o‘zidan oldingi blokning xesh qiymatini o‘z ichiga oladi va shu tariqa ketma-ket zanjir hosil bo‘ladi. Agar avvalgi blokdagi biror bit o‘zgartirilsa, uning xeshi ham o‘zgaradi, demak keyingi blok bilan bog‘lanish buziladi. Natijada blokcheyn ma’lumotlar bazasi oddiy ro‘yxatdan farqli ravishda o‘zgarishlarga sezgir, iz qoldiruvchi va kriptografik jihatdan bog‘langan tuzilma hosil qiladi. NIST hujjatlarida ham blokcheynning asosiy xususiyati aynan bloklarning oldingi blok xeshi orqali ulanib borishi va shu sababli yozuvlar “tamper-evident” hamda “tamper-resistant”, ya’ni o‘zgartirilganini ko‘rsatadigan va o‘zgartirishga chidamli bo‘lishi bilan izohlanadi.

Blokcheyn qanday ishlashini tushunish uchun uning arxitekturasini ketma-ket ko‘rib chiqish kerak.



1-rasm. Blokcheyn arxitekturasi

Tarmoqda foydalanuvchi biror tranzaksiya yaratadi, masalan, ma’lum bir aktivni boshqasiga uzatadi yoki biror yozuvni reyestrga kiritadi. Bu tranzaksiya dastlab tarmoqqa yuboriladi va tugunlar orasida tarqaladi. Tugun deb blokcheyn tarmog‘ida ishtirok etuvchi kompyuter yoki serverga aytiladi. Ayrim tugunlar faqat ma’lumotni qabul qiladi va tekshiradi, ayrimlari esa yangi blok yaratish yoki konsensus jarayonida ishtirok etish vakolatiga ega bo‘ladi. NIST tavsifiga ko‘ra, foydalanuvchi tomonidan yuborilgan tranzaksiya darhol blokcheynga yozilmaydi; avval u tugunlar tomonidan qabul qilinadi, tekshiriladi va keyinchalik blokka kiritish uchun navbatda turadi. Blok e’lon qilingach, boshqa tugunlar ham undagi tranzaksiyalarning haqiqiyligi va formatini tekshiradi; agar blokda noto‘g‘ri tranzaksiyalar bo‘lsa, uni qabul qilmaydi.

Blokning ichki tuzilishi ham muhim ahamiyatga ega. Odatda blok ikki qismdan iborat bo‘ladi: sarlavha qismi va ma’lumotlar qismi. Sarlavhada blok raqami yoki balandligi, oldingi blok xeshi, blok ma’lumotlarining xeshga oid ifodasi, vaqt belgisi va ayrim tizimlarda nonce kabi maydonlar saqlanadi. Ma’lumotlar qismida esa tekshiruvdan o‘tgan tranzaksiyalar ro‘yxati joylashadi. Bitcoin oq qog‘ozida proof-of-workni hosil qilish uchun nonce qiymati o‘zgartirib borilishi, blok xeshi esa ma’lum murakkablik shartiga mos kelishi kerakligi tushuntiriladi. NIST ham ko‘plab blokcheynlarda blok sarlavhasi tarkibida oldingi blok xeshi va blok ma’lumotlarining xesh ko‘rinishi mavjudligini qayd etadi. Shu sababli blok faqat ma’lumotlar to‘plami emas, balki o‘zidan oldingi tarix bilan matematik jihatdan bog‘langan kriptografik obyekt hisoblanadi.

Blokcheynning xavfsiz ishlashida xesh-funksiyalar alohida rol o‘ynaydi. Xesh-funksiya ixtiyoriy uzunlikdagi kirish ma’lumotidan qat’iy uzunlikdagi xesh qiymatini

hosil qiladi. Uning asosiy afzalligi shundaki, kirish ma’lumotidagi juda kichik o‘zgarish ham mutlaqo boshqa xesh hosil qiladi. Shuning uchun xesh nafaqat identifikator, balki yaxlitlikni nazorat qilish vositasi hamdir. Satoshi Nakamoto tizimda SHA-256 ga o‘xshash xeshlash yondashuvidan foydalanib, bloklar va proof-of-workni tashkil etgan. NIST ham blokcheyn tarmoqlarida raqamli imzolar va kriptografik xesh funksiyalar yozuvlarning o‘zgartirilganini aniqlash va tizimni buzishga qarshi turish uchun ishlatilishini ta’kidlaydi.

Blokcheynning ishlashida yana bir hal qiluvchi element — bu *konsensus mexanizmi*. Markaziy server bo‘lmagan sharoitda tarmoq qatnashchilari qaysi blok “to‘g‘ri” ekaniga va qaysi tarix haqiqiy ekaniga kelishib olishi kerak.

Blokcheyn tizimida barcha tugunlar ma’lumotlarning to‘g‘riligiga kelishib olishlari kerak. Bu jarayon konsensus orqali amalga oshiriladi.

Asosiy konsensus algoritmlari:

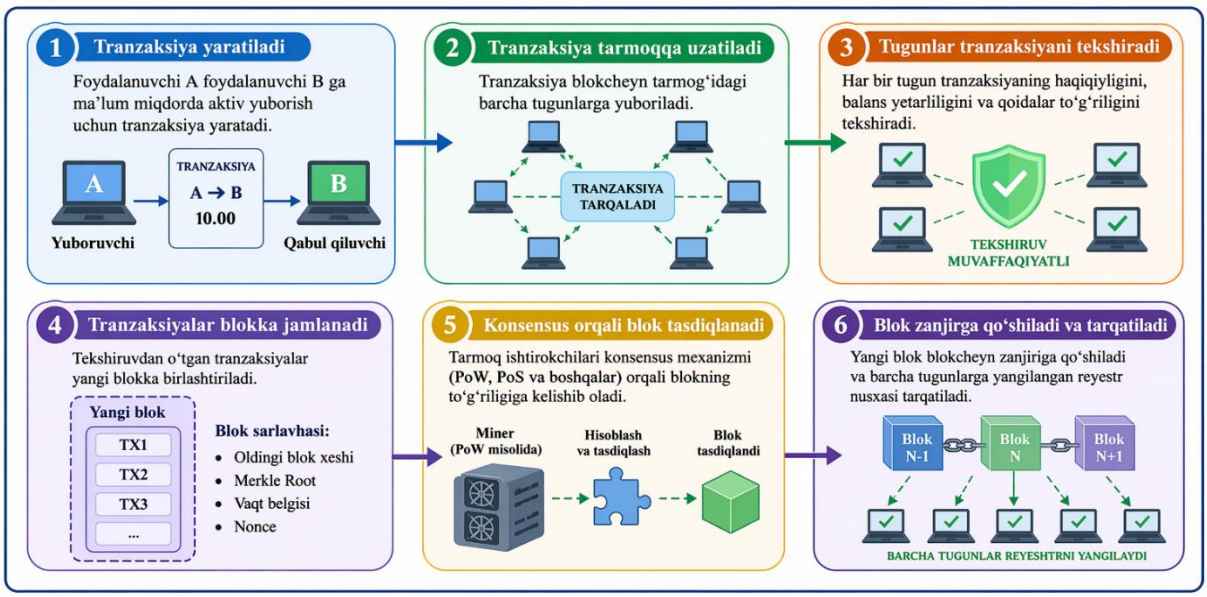
- **Proof of Work (PoW)** — hisoblash quvvatiga asoslangan (Bitcoin);
- **Proof of Stake (PoS)** — ulushga asoslangan;
- **Delegated Proof of Stake (DPoS)** — delegatsiya asosida;
- **Proof of Authority (PoA)** — ishonchli tugunlar asosida.

XUSUSIYATLAR	Proof of Work (PoW)	Proof of Stake (PoS)	Delegated Proof of Stake (DPoS)	Proof of Authority (PoA)
Asosiy g‘oya	Hisoblash quvvati orqali yangi blok yaratish	Tarmoqqa qo’yilgan ulush (stake) asosida blok yaratish huquqini tanlash	Token egalari vakillarni (delegatlar) saylaydi, ular blok yaratadi	Oldindan tasdiqlangan ishonchli tugunlar blok yaratadi
Blok yaratuvchi (validator)ni tanlash	Murakkab matematik masalani birinchi bo‘lib yechgan “miner”	Ko‘proq ulushga ega bo‘lgan validator tanlanadi (yoki tasodifiy + ulushga mos)	Saylov orqali tanlangan delegatlar navbat bilan blok yaratadi	Tizim ma’murlari tomonidan ishonchli deb belgilangan validatorlar
Tezlik va o‘tkazuvchanlik	Nisbatan past, tranzaksiya tasdiqlash vaqti uzun	Yuqori, tez tasdiqlash imkoniyati	Juda yuqori, tarmoq samaradorligi yaxshi	Yuqori, minimal kechikish bilan ishlaydi
Energiya sarfi	Juda katta energiya talab qiladi	Kam energiya sarflaydi	Kam energiya sarflaydi	Juda kam energiya sarflaydi
Xavfsizlik darajasi	Yuqori, ammo 51% hujum ehtimoli mavjud	Yuqori, iqtisodiy rag‘bat orqali xavfsizlik ta’minlanadi	Yaxshi, lekin delegatlar soni kam bo‘lsa markazlashuv xavfi ortadi	Ishonchga asoslangan, markazlashuv darajasi yuqori
Qo‘llanilish sohasi va misollar	Bitcoin, Litecoin	Ethereum 2.0, Cardano, Tezos	EOS, TRON, Lisk	VeChain, XP Network, Aion

2-rasm. Konsensus mexanizmlarining solishtirma tahlili

Bitcoin modelida bu vazifa proof-of-work orqali bajariladi. Oq qog‘ozga ko‘ra, tugunlar yangi tranzaksiyalarni blokka yig‘adi va keyin nonce qiymatini o‘zgartirib, xesh ma’lum miqdordagi nol bitlar bilan boshlanadigan variantni topishga harakat qiladi. Bunday natijani topish katta hisoblash resursi talab qiladi, lekin topilganini tekshirish nisbatan oson. Shu yo‘l bilan tarmoq “eng katta ish isboti” jamlangan eng uzun zanjirni haqiqiy deb qabul qiladi. Muallifning izohiga ko‘ra, tarixni o‘zgartirish uchun hujumchi nafaqat eski blokni, balki undan keyingi barcha bloklarni ham qayta hisoblab chiqishi va halol tugunlar zanjiridan o‘zib ketishi kerak bo‘ladi.

Amaliy nuqtai nazardan, blokcheyn tarmog‘i quyidagicha ishlaydi: yangi tranzaksiya yaratiladi va tarmoq bo‘ylab uzatiladi; tugunlar uni qabul qilib tekshiradi; ayrim tugunlar tasdiqlangan tranzaksiyalarni yangi blokka jamlaydi; blok konsensus talablariga mos keltirilgach tarmoqqa e’lon qilinadi; boshqa tugunlar blokni tekshiradi va qabul qilsa, o‘z nusxalariga qo‘shadi. Natijada butun tarmoq bo‘ylab sinxronlashtirilgan yagona reyestr vujudga keladi. Bitcoin oq qog‘ozida bu jarayon “yangi tranzaksiyalar tugunlarga uzatiladi, tugunlar ularni blokka yig‘adi, proof-of-work topadi, topilgan blokni boshqalarga yuboradi” tarzida ketma-ket ifodalangan. NIST esa bu mexanizmni yanada umumlashtirib, blokcheynda yozuvlar barcha tegishli tugunlar tomonidan tekshirilishi va noto‘g‘ri bloklarning qabul qilinmasligi bilan izohlaydi.



3-rasm. Blokcheyn ishlash jarayoni

Blokcheynning ommalashib borayotganining sababi uning faqat kriptovalyutalar bilan bog‘liq emasligidir. Dastlab u elektron pul va raqamli aktivlar uchun tanilgan bo‘lsa, keyinchalik ta’minot zanjiri, hujjat aylanishi, identifikatsiya, audit, sog‘liqni saqlash, kirishni boshqarish va davlat xizmatlari kabi ko‘plab yo‘nalishlarga tatbiq etila boshlandi. IBM blokcheynning biznes uchun asosiy afzalliklari sifatida ishonchni oshirish, xavfsizlikni kuchaytirish, shaffoflikni ta’minlash, ma’lumotlar izchilligini kuzatish va xarajatlarni kamaytirishni ko‘rsatadi. Xususan, umumiy va o‘zgarmas reyestr tashkilotlar o‘rtasidagi kelishmovchiliklarni kamaytiradi, qo‘lda solishtirish ishlarini qisqartiradi va vositachilarga bo‘lgan ehtiyojni kamaytiradi. Deloitte va PwC materiallarida esa blokcheynning enterprise muhitida qo‘llanilishi tokenizatsiya, fond o‘tkazmalari, ta’minot zanjiri kuzatuvi va raqamli aktivlar infratuzilmasi bilan bog‘liq holda ko‘rsatiladi.

Blokcheynning keng tarqalishiga ta’sir qilayotgan yana bir omil — bu an’anaviy tizimlardagi “ishonch modeli”ni qayta ko‘rib chiqish imkoniyatidir. Oddiy

markazlashgan tizimda foydalanuvchi ma’lumot to‘g‘riligini, yozuvlar to‘liq saqlanayotganini va ular keyinchalik o‘zgartirilmayotganini bitta markaziy operatorga ishonib qabul qiladi. NIST markazlashgan reyestrlarda foydalanuvchi operatsiyalar ro‘yxati to‘liq va to‘g‘ri ekaniga, tizim buzilmaganiga va server xavfsiz boshqarilayotganiga ishonishga majbur ekanini ko‘rsatadi. Blokcheynda esa qabul qilingan tranzaksiyalar taqsimlangan reyestrda saqlanadi, tugunlar noto‘g‘ri tranzaksiyalarni rad etadi, geografik tarqoq arxitektura tizimning bardoshliligini oshiradi va bitta tugundagi muammo butun tizimning ishdan chiqishiga olib kelmaydi. Shu sababli blokcheyn ko‘pincha “trustless” yoki aniqrog‘i, “trust-minimized” model sifatida talqin qilinadi: tizim ishlashi uchun alohida markaziy tashkilotga mutlaq ishonch shart bo‘lmaydi.

Ayniqsa axborot xavfsizligi nuqtai nazaridan blokcheynning jozibasi uning uchta muhim xususiyatida ko‘rinadi: o‘zgarmaslik, kuzatuvchanlik va markazlashmaganlik.

Blokcheyn texnologiyasi quyidagi xususiyatlarga ega:

- markazlashmaganlik (decentralization);
- o‘zgarmaslik (immutability);
- shaffoflik (transparency);
- xavfsizlik (security);
- ishonchlilik (trustlessness).

NISTning kirishni boshqarish bo‘yicha hujjatida blokcheyn yondashuvi ruxsat siyosatlari va loglarni o‘zgartirish ehtimolini kamaytirishi, avtorizatsiya jarayonini markazlashmagan holda tashkil etishi, bitta nosozlik nuqtasini bartaraf etishi va bloklar izchilligi orqali tizim holatini kuzatish imkonini berishi ko‘rsatilgan. Bu xususiyatlar blokcheynni faqat moliyaviy hisob-kitoblar uchun emas, balki audit talab qilinadigan, yozuvlar o‘zgarmasligi muhim bo‘lgan va bir nechta tashkilotlar o‘rtasida umumiy ishonchli reyestr kerak bo‘ladigan sohalar uchun ham moslashtiradi.

Shu bilan birga, blokcheynning ommalashuvi faqat texnik ustunliklar bilan emas, balki institutsional va iqtisodiy omillar bilan ham bog‘liq. Deloitte materiallarida korxonalar Web3 va blokcheynni raqamli biznes strategiyasining bir qismi sifatida ko‘rib chiqayotgani qayd etiladi. PwC esa blokcheyn asosidagi qo‘llanmalarni enterprise blockchain, tokenizatsiya, pul o‘tkazmalari va ta’minot zanjiri trackingi bilan bog‘laydi. Jahon iqtisodiy forumi 2026-yil boshidagi sharhida banklar va blokcheyn infratuzilmasining yaqinlashuvi, global standartlar va yanada yetuk infratuzilmaning shakllanishi bu sohani tajriba bosqichidan institutsional qo‘llash bosqichiga olib kirayotganini ta’kidlaydi. Demak, blokcheynning ommalashuvi nafaqat kriptoaktivlar trendi, balki xavfsiz, kuzatiladigan va ishonchli raqamli infratuzilmaga bo‘lgan real ehtiyoj bilan ham izohlanadi.

Biroq blokcheynni mutlaq ideal texnologiya sifatida baholash to‘g‘ri bo‘lmaydi. Uning ishlashida hisoblash resurslari sarfi, ayrim tarmoqlarda past o‘tkazuvchanlik, maxfiylik masalalari, kalitlarni boshqarish muammolari va konsensus mexanizmlariga bog‘liq cheklovlar mavjud. NIST hujjatlarida ham blokcheynning barcha holatlar uchun universal yechim emasligi, balki ma’lum talablar mavjud bo‘lgandagina maqsadga muvofiq ekani ko‘rsatiladi. Shunga qaramay, tarixiy taraqqiyoti, kriptografik asoslarga tayangan ishlash mexanizmi va turli sohalarda amaliy qiymat yaratish salohiyati sababli blokcheyn texnologiyasi bugungi kunda axborotni himoya qilish vositalari orasida muhim o‘rin egallamoqda.

Shunday qilib, blokcheyn texnologiyasi dastlab markaziy vositachisiz elektron to‘lovlar tizimini yaratish maqsadida taklif qilingan bo‘lsa-da, bugungi kunda u bundan ancha keng ma’noga ega bo‘lib qoldi. U taqsimlangan reyestr, kriptografik bog‘langan bloklar, konsensus mexanizmi va raqamli imzolar kombinatsiyasi asosida ishlaydi hamda ma’lumotlarning yaxlitligi, kuzatuvchanligi va nisbatan ishonchli almashinuvi uchun yangi imkoniyatlar yaratadi. Aynan shu sababli blokcheynni axborot xavfsizligi kontekstida faqat texnik yangilik emas, balki yangi boshqaruv va ishonch modeli sifatida ham baholash mumkin. Garchi hisoblash resurslari va o‘tkazuvchanlik kabi cheklovlari mavjud bo‘lsa-da, u axborot xavfsizligini ta’minlashda eng istiqbolli innovatsion yechim bo‘lib qolmoqda.

Foydalanilgan adabiyotlar

1. NIST. Blockchain Technology Overview. NISTIR 8202, 2018.
2. NIST. Blockchain for Access Control Systems. NISTIR 8403, 2022.
3. ENISA. Distributed Ledger Technology & Cybersecurity Report, 2021.
4. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. https://bitcoin.org/bitcoin.pdf
5. Zheng Z., Xie S., Dai H. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 2018.
6. Casino F., Dasaklis T., Patsakis C. A systematic literature review of blockchain-based applications. *Telematics and Informatics*, 2019.