UNIVERSAL JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
ISSN 2992 – 8788
https://sr-journals.org/index.php/UJMTCS

BLOKCHEYN TIZIMLARINING ARXITEKTURASI VA ULARNING ISHLASH PRINSIPI

G'oyibnazarova Aziza Abdullo qizi
Muhammad Al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti magistranti
E-mail: goyibnazarovaaziza@gmail.com

Annotatsiya. Ushbu maqola blokcheyn texnologiyasining nazariy asoslari, blokcheyn texnologiyasining arxitekturasi tahlili, blokcheyn tizimlarining ishlash prinsipi, blokcheyn texnologiyasining qo'llanilish sohalari, konsensus algoritmlari yoritadi.

Kalit so'zlar. Blokcheyn texnologiyasi, blokcheyn trilemmasi, konsensus algoritmlari, merkle daraxti, xesh funksiyalar

Аннотация. В данной статье рассматриваются теоретические основы технологии блокчейн, анализ архитектуры технологии блокчейн, принцип работы блокчейн-систем, области применения технологии блокчейн, алгоритмы консенсуса.

Ключевые слова. Технология блокчейн, трилемма блокчейн, алгоритмы консенсуса, дерево Меркла, хеш-функции.

Abstract. This article covers the theoretical foundations of blockchain technology, analysis of the architecture of blockchain technology, the principle of operation of blockchain systems, areas of application of blockchain technology, consensus algorithms.

Keywords. Blockchain technology, blockchain trilemma, consensus algorithms, merkle tree, hash functions

Kirish. Hozirda blokcheyn texnologiyasi asosida ishlovchi tizimlar butun dunyoda turli xildagi sohalarda keng qo'llanilib kelinmoqda. Dastlab blokcheyn texnologiyasi kriptovalyutalarni yaratish, ularni markazlashmagan holda boshqarish va xavfsizligini ta'minlash uchun qo'llanilgan bo'lsa, bugungi kunga kelib blokcheyn texnologiyasini sog'liqni saqlash sohasida, bank va moliya sohasida (DeFi), ovoz berishda, ko'chmas mulk va mulkni boshqarish sohasida (NFTs), logistika sohasida, media sohalarida(NFTs), sug'urtada va yana bir qancha sohalarda qo'llash imkoniyatini bermoqda[1].

Blokcheyn texnologiyasini hozirga kelib ommalashganining sababi uning markazlashmaganlik, xavfsizlik va ma'lumotlarning deyarli o'zgartirishning imkoniyati mavjud emasligidadir. Ushbu texnologiya asosida ishlaydigan tizimlarda nazorat qiluvchi markaziy o'rganing yo'q ekanligi, ya'ni inson faktori yo'q ekanligi va boshqaruvning kriptologik primitivlar asosida bo'lishi tizim xavfsizligini yanada oshiradi. Lekin shunga qaramay blokcheyn tizimlarining arxitekturasi va ishlash mexanizmi murakkab bo'lib, ularni o'rganib chiqish ilmiy hamda amaliy tomondan muhim jarayon hisoblanadi.

Ushbu tadqiqotning maqsadi blokcheyn tizimlarining arxitekturasi va ularning ishlash prinsipini tahlil qilishdan iborat bo'lib, unda asosan Bitcoin hamda Etherium tizimlari organiladi.

1. Blokcheyn texnologiyasining tavsifi

Blokcheyn tizimlari P2P tarmog'i asosida ishlovchi, kriptografik jihatdan himoyalangan, ma'lumotlarni faqatgina qo'shib borish mumkin bo'lgan hamda shu ma'lumotlarni o'zgartirishning deyarli imkoni bo'lmagan va foydalanuvchilar o'rtasida faqatgina konsensus orqali yagona kelishuvga erishiladigan taqsimlangan tizimdir[2].

Blokcheyning texnologiyasi umumiy holatda o'zining markazlashmaganlik, ma'lumot o'zgarmasligi, shaffoflik va xavfsizlik xususiyatlari bilan ajralib turadi. Ammo shuni aytib o'tish kerakki, blokcheyn texnologiyasi asosida ishlaydigan tizimga qarab, yuqorida keltirib o'tilgan xususiyatlar holat qisman o'zgarishi mumkin. Masalan [2] ga ko'ra, blokcheyndagi ma'lumotlarni

o’zgartirish Yevropa Ittifoqining “unutish huquqi” yoki “o’chirish huquqi”ni holatlarda o’rinli sanaladi[3][4].

Ko’plab klassik adabiyotlarda blokcheyn tizimlari ommaviy, xususiy va konsorsium turlarga bo’linadi. (Ayrim adabiyotlarda gibrit tur ham mavjud bo’lib, u qisman konsorsiumga tenglashtiriladi).

Ommaviy blokcheynlar ruxsatsiz blokcheynlar turkumiga kirib, tizimdan ixtiyoriy foydalanuvchi foydalanish imkoniyatiga ega. Bunday blokcheynlarga Bitcoin, Namecoin va Etheriumlarni misol qilish mumkin.

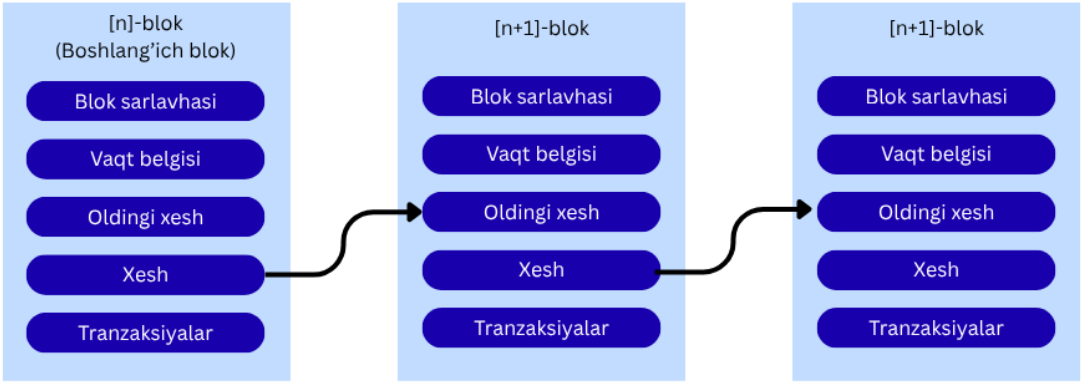
Xususiy blokcheynlar ruxsatli blokcheynlar turkumiga kirib, bunday turdagi blokcheynlar asosan tashkilotlarda ma’lumotlarni almashish uchun foydalaniladi. Bunda nazorat oldindan belgilan foydalanuvchlar tomonidan olib borilgani uchun blokcheyning markazlashmaganlik xususiyati qisman yoqoladi. Bunday blokcheynlarga Hyperledger Fabric va Quoriumlarni misol qilish mumkin.

Konsorsium turidagi blokcheynlar bir nechta tashkilotlar o’rtasida ma’lumot almashinish uchun ishlatiladi. Ular ommaviy va xususiy blokcheynlarning gibrid versiyasi hisoblanadi.

2. Blokcheyn tizimlarining arxitekturasi

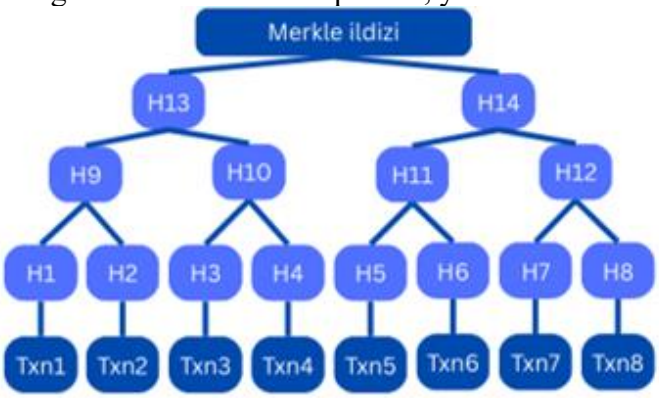
Blokcheyn texnologiyasi asosida ishlaydigan tizimlar tuzilishiga ko’ra bir -biridan farq qiladi. Chunki ushbu tizimdagi ma’lumotlarni taqsimlangan, xavfsiz va o’zgarmas holda saqlash uchun arxitektura bir nechta qatlamdan iborat bo’lishi kerak. Umumiy holatda blokcheyn arxitekturasi to’rtta asosiy qatlamdan iborat deb qaraladi:

1. Ma’lumotlar qatlami - tranzaksiyalar va bloklardan iborat bo’lib, unda blokcheyn tizimlarida yaratilgan barcha tranzaksiyalar to’plami bloklarda ma’lum bir qonuniyatlar asosida saqlanadi. Bunda bloklar bir-biri bilan o’zaro bog’lanadi va bloklar zanjirinin hosil qiladi. Blok o’zidan oldingi blokning xesh qiymati bilan quyidagicha bog’lanadi:



1-rasm. Bloklarning bog’lanishi

1-rasmda umumiy holatda blokning tuzilishi berilgan. Lekin, [3] ga ko’ra, blokning o’zi ham ikki qismdan blok sarlavhasi hamda blok tanasidan iborat. Blok tanasida, blok qabul qilgan barcha tranzaksiyalarning ma’lumotlari ya’ni xesh qiymatlari joylashadi va xesh qiymatlar juftlashib yana xesh qiymat hosil qiladi va bu jarayon bitta Merkle ildizi qiymatini hosil qilmaguncha davom etadi. Bu jarayon Merkle daraxti algoritmi asosida hosil qilinadi, ya’ni:



2-rasm. Merkle ildizi hosil bo’lishi

Hosil bo'lgan Merkel ildizi blok sarlavhasidan joy oladi. [7] ga ko'ra blok sarlavhasida bir martalik son (nonces) ham qatnashib, u mayning hisoblashda eng muhim vazifani bajaradi. Shuni ham ta'kidlash kerakki, Bitcoin tizimidagi dastlabki blokning oldingi xesh qiymati 64 ta 0 dan iborat bo'lib, u faqatgina bitta ya'ni mukofot tranzaksiyasidan tashkil topgan haqidagi ma'lumotlar The Times jurnalida 2009-yilning 3 yanvarida e'lon qilingan.

2. Tarmoq qatlami – blokcheyn tizimlarida ma'lumotlarni tugunlarga uzatish, tekshirish va ma'lumot qatlamidagi barcha ma'lumotlarni audit qilish vazifasini o'z ichiga oladi [5]. Ushbu qatlamning eng asosiy vazifalaridan bir bu tugunlarga tranzaksiyalarni va bloklani uzatish hamda jarayonlarni sinxronlashdan iborat.
3. Konsensus qatlami - bu blokcheyn tarmog'idagi hamma tugunlar qaysi blok to'g'ri ekanligi va blokning joriy holati to'g'risida yagona yechimga keladigan qatlam hisoblanadi. Turli blokcheyn tizimlarida turli xil konsensus mexanizmlaridan foydalaniladi. Umumiy holatda konsensus mexanizmlarining 2 xil turga isbotga asoslangan konsensus mexanizmlari (PoW, PoS, DPoS, PoA) va vizantiya xatoligiga bardoshli konsensus mexanizmlariga bo'lish mumkin (PBFT, Ripple, dBFT).
4. Ilova qatlami – bu blokcheyning barcha qatlamlarini ustida ishlovchi qatlam bo'lib, u foydalanuvchiga ko'rinadigan va haqiqiy biznes jarayonlarni amalga oshiradigan dasturiy ekotizim hisoblanadi. Ilovalar qatlami smart kontraktlar, markazlashmagan ilovalar va avtonom agentlardan tashkil topgan bo'lib, blokcheynda ishlaydigan turli xil foydalanuvchi darajasidagi agentlar va dasturlarni o'z ichiga oladi[2].

Blokcheyn arxitekturasi asosan shu yuqorida keltirilib o'tilgan qatlamlardan tashkil topgan bo'lib, turli xil adabiyotlarda tizim turiga qarab bunda tashqari yana tarmoq topologiyasi qatlami va shartnoma qatlamlari ham mavjud bo'lishi mumkin.

Blokcheyn tizimlarining ishlash prinsipi.

Blokcheyn tizimlarining ishlash prinsipi asosan quyidagi vazifalarni bajarishga asoslangan:

1. Tranzaksiyalarni bloklarda taqsimlangan holda saqlash;
2. Hosil bo'lgan bloklarni xeshlash va dastlabki blok xeshi bilan bog'lash;
3. O'zgarmas ro'yxatni shakllantirish;
4. Bloklarni qabul qilish va joriy holatini tekshirish uchun konsensus mexanizmlarini qo'llash.

Kengroq qilib tushuntiriladigan bo'lsa tugun foydalanuvchisi tranzaksiyani amalga oshirishi uchun tranzaksiya yaratadi va unda qabul qiluvchining adressi va tranzaksiya miqdori kiritiladi. So'ngra o'zining maxfiy imzosi bilan imzolab tranzaksiyani tarmoqqa yuboradi. P2P protokollida ushbu tranzaksiya eng yaqin tugun tomonidan qabul qilinadi va boshqa tugunlarga tarqatiladi. Tugunlar tranzaksiyaning, imzoni haqiqiyligi va ikki martalik sarf yo'qligini tekshirishadi va jarayon muvaffaqiyatli yakkunlangach tranzaksiya tarmoqdagi kutish zonasiga yuboriladi (mempoolga). [6] ga ko'ra har 10 minut ichida Bitcoin tizimlarida bitta blok hosil bo'ladi. Bunda blok hosil bo'lishi uchun tizimdagi maynerlar bir martalik qiymat (nonces) ni shunday tanlashligi kerakki natija tarmoq tomonidan har 2016 ta blokda avtomatik hosil bo'ladigan target qiymatdan kichik bo'lishi kerak:

$$H(blok) < target$$

Yuqorida keltirilgan H(blok) blok sarlavhasidagi barcha ma'lumotlarni ketma-ket yozib, ularning umumiy xesh qiymatini olish orqali hisoblanadi:

$$H(blok) = H(oldin_blok_xeshi\,||merkle_ildizi||vaqt_belgisi||versiya||bir\ martalik\ son)$$

Agar mayner bir martalik qiymatni talab darajasida 1-bo'lib topsa uning blokki zanjirga qo'shiladi va mayner bitcoin bilan mukofotlanadi [7]. Bu jarayon PoW(ish isboti) consensus algoritmi bo'lib, u asosan bitcoin asosida ishlaydigan tizimlarda qo'llaniladi. Bunda mayner bitcoin mukofotini olish energiya sarf qiladi.

Blok samarali tarzda umumiy zanjirga qo'shilgach, tranzaksiya bajarilgan hisoblanadi va yuboruvchi yuborga qiymat qabul qiluvchiga yetib boradi.

Xulosa.

Blokcheyn texnologiyasi asosida ishlaydigan tizimlar murakkab arxitekturaga ega bo'lib, ularning tuzilishi tizim turiga bog'liq, ammo umumiy holda blokcheyn texnologiyasining arxitekturasi ma'lumotlar qatlami, tarmoq qatlami, konsensus va ilovalar qatlamidan iborat.

Blokcheyn tizimlarining ishlash prinsipi asosan tranzaksiyalarni hosil qilish ularni bloklarda taqsimlangan holda saqlash, bu bloklarni xeshlash va dastlabki blok xesh qiymati bilan bog'lash, tizimda ma'lumot yaxlitligini ta'minlash hamda blokni zanjirga qo'shish uchun mos konsensus mexanizmlaridan foydalanishdan iborat.

Foydalanilgan adabiyotlar

1. J. Soriano, "helalabs," 25 08 2024. [Online]. Available: https://helalabs.com/blog/12-best-real-world-applications-of-blockchain-technology-in-2024/. [Accessed 22 12 2025].
2. Imran B, Mastering Blockchain, 4th ed. Packt Publishing, 2023 [Online]. Available: https://www.perlego.com/book/3884620. [Accessed: 12-Apr-2026]
3. European Parliament and Council of the European Union. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [Elektron resurs] // Official Journal of the European Union. — 2016. — L 119. — URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (murojaat qilingan sana: 14.02.2026).
4. European Parliament and Council of the European Union. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) : Art. 17 — Right to erasure [Elektron resurs]. — 2016. — URL: https://gdpr-info.eu/art-17-gdpr (murojaat qilingan sana: 12.02.2026).
5. Khodaiemehr H., Bagheri K., Feng C. Navigating the quantum computing threat landscape for blockchains: A comprehensive survey // Computer Science Review. — 2026. — Vol. 59. — Art. 100846.
6. Buterin V. Ethereum whitepaper [Elektron resurs]. – Kirish rejimi: https://ethereum.org/whitepaper/ (murojaat sanasi: 11.04.2026).
7. **Nakamoto S.** Bitcoin: A Peer-to-Peer Electronic Cash System [Elektron resurs]. — 2008. — URL: https://bitcoin.org/bitcoin.pdf (murojaat qilingan sana: 12.02.2026).