

**BLOKCHEYN VA KRIPTOGRAFIYA ASOSIDA TIBBIY MA'LUMOTLAR  
XAVFSIZLIGINI TA'MINLASH**

**Seidullayev M.K.**

*Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti*

**Annotatsiya:** *Ushbu tezisda blokcheyn texnologiyasidan tibbiy ma'lumotlarni xavfsiz saqlash va almashishda foydalanish imkoniyatlari tahlil qilinadi. Tibbiy ma'lumotlarning raqamlashtirilishi natijasida ularni turli tibbiyot muassasalari o'rtasida tezkor almashish zarurati ortib bormoqda. Bunda ma'lumotlarning maxfiyligi, yaxlitligi, mavjudligi va turli axborot tizimlari o'rtasidagi o'zaro moslashuvchanligini ta'minlash muhim masalalardan hisoblanadi. Tadqiqotda blokcheynning taqsimlangan reyestr, o'zgarmas yozuvlar, kriptografik himoya va smart-kontrakt kabi xususiyatlarining tibbiy ma'lumotlarni almashishdagi imkoniyatlari ko'rib chiqiladi. Shuningdek, tibbiy ma'lumotlarni himoyalashda shifrlash, kirishni boshqarish, permissioned va consortium blokcheynlar hamda off-chain saqlash yondashuvlari tahlil qilinadi. Natijada blokcheyn texnologiyasi tibbiy ma'lumotlarni ishonchli va nazorat qilinadigan tarzda almashish uchun istiqbolli texnologik yechimlardan biri ekanligi ko'rsatiladi.*

**Kalit so'zlar:** *blokcheyn, tibbiy ma'lumotlar, ma'lumotlar almashinuvi, axborot xavfsizligi, shifrlash, smart-kontrakt, elektron tibbiy karta, IoT, maxfiylik, kirishni boshqarish.*

## **KIRISH**

Raqamli texnologiyalarning tibbiyot sohasiga jadal joriy etilishi natijasida elektron tibbiy kartalar, diagnostika natijalari, laboratoriya ma'lumotlari va boshqa turdagi tibbiy axborotlarning hajmi ortib bormoqda. Ushbu ma'lumotlarni turli tibbiyot muassasalari o'rtasida almashish bemorga xizmat ko'rsatish samaradorligini oshirish imkonini beradi. Biroq tibbiy ma'lumotlarning maxfiy va yuqori darajada himoyalaniishi talab etiladigan axborot turi ekanligi sababli ularni saqlash va almashishda axborot xavfsizligi muammolari yuzaga keladi.

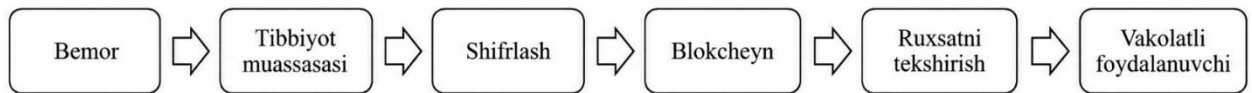
An'anaviy tibbiy axborot tizimlarida ma'lumotlar ko'pincha alohida muassasalarning xususiy ma'lumotlar bazalarida saqlanadi. Natijada bemorning turli tibbiyot muassasalarida shakllangan ma'lumotlari tarqoq holda joylashishi va ular o'rtasida ma'lumot almashinuvi murakkablashishi mumkin. Tadqiqotlarda bunday holat tibbiy axborot tizimlari o'rtasidagi interoperabellik muammolarini keltirib chiqarishi qayd etilgan.

Blokcheyn texnologiyasi esa ma'lumotlarni taqsimlangan muhitda saqlash, tranzaksiyalarni kriptografik jihatdan himoyalash va yozuvlarning yaxlitligini ta'minlash imkoniyatlari bilan tibbiy ma'lumotlarni almashish uchun yangi yondashuvni taklif qiladi. Shu sababli so'nggi yillarda blokcheyn asosida tibbiy ma'lumotlarni xavfsiz almashish bo'yicha turli arxitektura va protokollar ishlab chiqilgan.

## 2. Tibbiy ma'lumotlarni almashishda blokcheynning o'rni

Blokcheyn — ma'lumotlarni bir nechta tarmoq tugunlari o'rtasida taqsimlangan holda saqlashga imkon beruvchi texnologiya bo'lib, unda ma'lumotlar kriptografik bog'langan bloklar ko'rinishida shakllantiriladi. Har bir yangi blok oldingi blok bilan bog'lanadi va shu orqali ma'lumotlarning keyinchalik o'zgartirilganligini aniqlash imkoniyati paydo bo'ladi.

Tibbiy ma'lumotlarni almashish tizimida blokcheynni quyidagi umumiy model asosida ifodalash mumkin:



Bunda tibbiy ma'lumotlarning o'zini blokcheynda to'liq saqlash o'rniga, ayrim tadqiqotlarda ma'lumotlar shifrlangan holda tashqi yoki off-chain saqlash tizimiga joylashtirilib, blokcheynda esa ma'lumotga tegishli indeks, xesh yoki manzilni saqlash yondashuvi qo'llaniladi. Bu katta hajmdagi tibbiy ma'lumotlar bilan ishlashda blokcheyn yuklamasini kamaytirishga xizmat qilishi mumkin.

## 3. Tibbiy ma'lumotlarni himoyalashda kriptografik usullar

Tibbiy ma'lumotlarni almashish tizimlarida kriptografik himoya asosiy komponentlardan biri hisoblanadi. Ko'rib chiqilgan tadqiqotlarda Attribute-Based Encryption (ABE), Ciphertext-Policy ABE, proxy re-encryption, ECC va boshqa shifrlash mexanizmlari qo'llanilgan. Ular ma'lumotlarga faqat tegishli huquqqa ega foydalanuvchilarning kirishini ta'minlashga xizmat qiladi.

Masalan, ABE asosida foydalanuvchining lavozimi, tibbiyot muassasasi, mutaxassisligi yoki boshqa atributlari asosida ma'lumotlarga kirish huquqini belgilash mumkin.

Umumiy holda:

$$M \xrightarrow{E_K} C$$

bu yerda:

- $M$  — tibbiy ma'lumot;
- $K$  — kriptografik kalit;
- $E_K$  — shifrlash algoritmi;
- $C$  — shifrlangan ma'lumot.

Foydalanuvchi tegishli huquqqa ega bo'lgandagina:

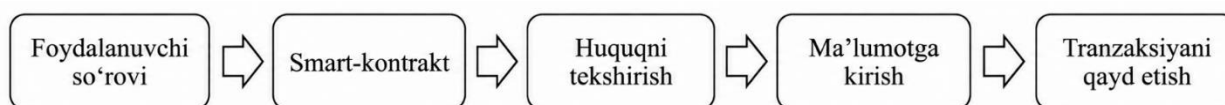
$$C \xrightarrow{D_K} M$$

orqali dastlabki ma'lumotni olishi mumkin.

## 4. Smart-kontrakt va kirishni boshqarish

Blokcheyn asosidagi tibbiy ma'lumot almashish tizimlarida smart-kontraktlar ma'lumotlarga kirish huquqlarini avtomatik boshqarish uchun ishlatilishi mumkin. Masalan, bemor o'z ma'lumotlarini ma'lum bir shifkor yoki tibbiyot muassasasiga taqdim etishga rozilik berganida, ushbu ruxsat smart-kontrakt orqali qayd etilishi mumkin.

Bunda jarayon:



ko‘rinishida tashkil qilinadi.

Bu yondashuv ma’lumotlardan kim, qachon va qanday maqsadda foydalanganligini qayd etish imkoniyatini beradi. Taherdoost tomonidan ko‘rib chiqilgan tadqiqotlarda ham kirishni boshqarish, smart-kontraktlar, ma’lumotlar yaxlitligi va kuzatuvchanlik blokcheyn asosidagi tibbiy ma’lumot almashishning muhim yo‘nalishlari sifatida ko‘rsatilgan.

### **5. Blokcheyn turlarining tibbiy ma’lumot almashishdagi qo‘llanilishi**

1-jadval. Blokcheyn turlarining tibbiy ma’lumot almashishdagi qo‘llanilishi

| <b>Blokcheyn turi</b>        | <b>Asosiy xususiyati</b>                       | <b>Tibbiyotda qo‘llanishi</b>                                       |
|------------------------------|------------------------------------------------|---------------------------------------------------------------------|
| <b>Public blockchain</b>     | Ochiq va keng ishtirokchilar tarmog‘i          | Ochiq verifikatsiya, tranzaksiyalarni tekshirish                    |
| <b>Private blockchain</b>    | Bitta tashkilot tomonidan boshqariladi         | Kasalxona ichidagi ma’lumotlarni boshqarish                         |
| <b>Consortium blockchain</b> | Bir nechta tashkilotlar tomonidan boshqariladi | Kasalxonalar va tibbiyot tashkilotlari o‘rtasida ma’lumot almashish |
| <b>Hybrid blockchain</b>     | Ochiq va yopiq elementlarni birlashtiradi      | Maxfiy ma’lumotlar va umumiy verifikatsiyani birgalikda boshqarish  |

Tibbiy ma’lumotlar maxfiyligi yuqori bo‘lganligi sababli tadqiqotlarda private va consortium blockchain yondashuvlari ko‘p uchraydi. Bunday tizimlarda tarmoqqa kimlarning qo‘shilishi va ma’lumotlardan foydalanish huquqlari nazorat qilinadi.

### **6. Xulosa**

Blokcheyn texnologiyasi tibbiy ma’lumotlarni xavfsiz almashish uchun istiqbolli texnologiyalardan biri hisoblanadi. Uning taqsimlangan arxitekturasi, kriptografik himoya, ma’lumotlar yaxlitligi va tranzaksiyalarni kuzatish imkoniyatlari tibbiy axborot tizimlarida qo‘llash uchun muhim xususiyatlarni taqdim etadi. Tahlil qilingan tadqiqotlarda shifrlash, smart-kontrakt, kirishni boshqarish, permissioned/consortium blockchain va off-chain saqlash kabi yondashuvlardan foydalanilayotgani ko‘rsatilgan.

Shu bilan birga, blokcheynni tibbiyot sohasiga keng joriy etish uchun masshtablanuvchanlik, ma’lumotlar maxfiyligi, interoperabellik, ishlash tezligi va me’yoriy talablar bilan bog‘liq masalalarni hal qilish zarur. Shuning uchun kelgusidagi tadqiqotlarda blokcheynni IoT, bulutli hisoblash, edge computing va zamonaviy kriptografik mexanizmlar bilan integratsiyalash istiqbolli yo‘nalishlardan biri sifatida qaralishi mumkin.

**FOYDALANILGAN ADABIYOTLAR:**

Taherdoost H. The Role of Blockchain in Medical Data Sharing // Cryptography. – 2023. – Vol. 7, No. 3. – Art. 36. – DOI: 10.3390/cryptography7030036.

16. Agbo C. C., Mahmoud Q. H., Eklund J. M. Blockchain Technology in Healthcare: A Systematic Review // Healthcare. – 2019. – Vol. 7, No. 2. – Art. 56. – DOI: 10.3390/healthcare7020056.

17. Dimitrov D. V. Blockchain Applications for Healthcare Data Management // Healthcare Informatics Research. – 2019. – Vol. 25, No. 1. – P. 51–56. – DOI: 10.4258/hir.2019.25.1.51.

18. Yaqoob I., Salah K., Jayaraman R., Al-Hammadi Y. Blockchain for Healthcare Data Management: Opportunities, Challenges, and Future Recommendations // Neural Computing and Applications. – 2022. – Vol. 34, No. 14. – P. 11475–11490. – DOI: 10.1007/s00521-020-05519-w.

19. Merlo V., Pio G., Giusto F., Bilancia M. On the Exploitation of the Blockchain Technology in the Healthcare Sector: A Systematic Review // Expert Systems with Applications. – 2023. – Vol. 213. – Art. 118897. – DOI: 10.1016/j.eswa.2022.118897.

20. Saeed H., Malik H., Bashir U., et al. Blockchain Technology in Healthcare: A Systematic Review // PLOS ONE. – 2022. – Vol. 17, No. 4. – e0266462. – DOI: 10.1371/journal.pone.0266462.

21. Meenavolu S. B. K., Kasyapa C. V. Blockchain Integration in Healthcare: A Comprehensive Investigation of Use Cases, Performance Issues, and Mitigation Strategies // Frontiers in Digital Health. – 2024. – Vol. 6. – DOI: 10.3389/fdgth.2024.1359858.

22. Secure Medical Data Storage with Blockchain Technology // Procedia Computer Science. – 2023. – Vol. 225. – P. 961–968. – DOI: 10.1016/j.procs.2023.10.083.