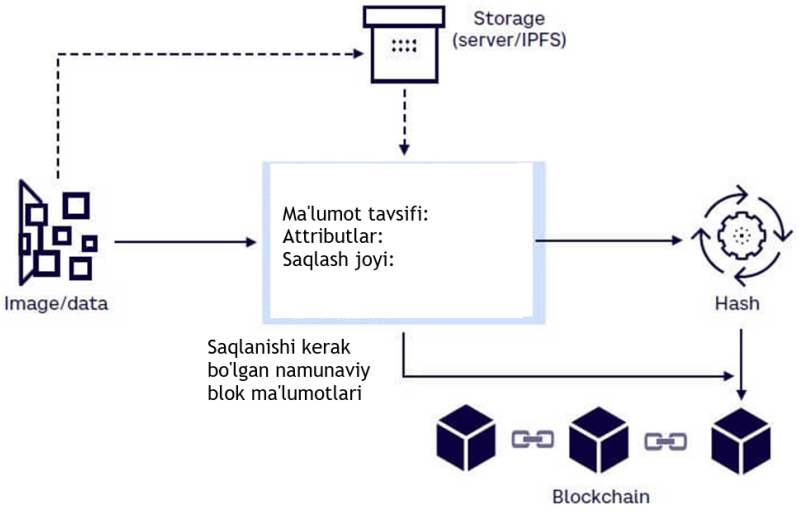
BLOCKCHEYNDA MA’LUMOTLARGA ISHLOV BERISH JARAYONINI TASHKIL ETISH

Xasan Ergashev[1], Baxtiyor Akmuradov[2]
[1] University of Management and Future Technologies universiteti magistranti;
xasane059@gmail.com
(93) 420 22 23
[2] University of Management and Future Technologies universiteti dotsenti;
b.u.akmuradov@gmail.com
(97)890 47 57

Annotatsiya: Mazkur ishda blokcheyn texnologiyasining asosiy tamoyillari, ma’lumotlarni xavfsiz saqlash va boshqarish mexanizmlari hamda blokcheynning strukturaviy komponentlari chuqur tahlil qilingan. Xususan, ma’lumotlarning hash funksiyalari yordamida yaxlitligi ta’minlanishi, tugunlar orqali tarmoqda sinxron ishlov berish, konsensus mexanizmlari va bloklar orasidagi bog‘lanish prinsiplari yoritilgan. Blokcheynning turlari va ularning afzallik hamda kamchiliklari tahlil qilingan.
Kalit so‘zlar: Blokcheyn, Hash funksiyasi, taqsimlangan reyestr, tugun, tranzaksiya, blok, zanjir, minerlar, konsensus mexanizmi, ruxsat berilgan blokcheyn, ruxsatsiz blokcheyn.

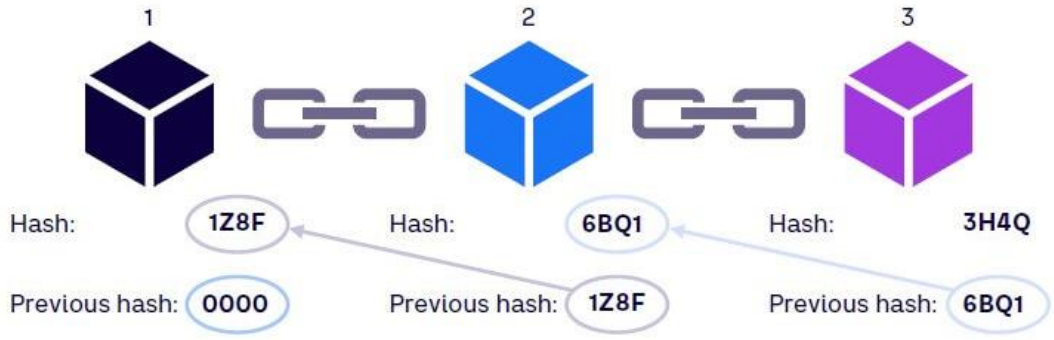
Ma’lumotlar odatda xavfsizlik sababli shifrlanadi yoki blokning o‘lcham cheklovlariga mos keladigan o‘lchamga qadar hashlanadi, asl ma’lumot esa tashqi serverlarda yoki IPFS (InterPlanetary File System) kabi taqsimlangan fayl tizimlarida saqlanadi.



1-rasm. Blockcheynda ma’lumotlarga ishlov berish jarayoni

Hash blokcheynda saqlangan ma’lumotlarning yaxlitligi va o‘zgartirib bo‘lmasligini himoya qilish uchun keng qo‘llaniladi. Ushbu funksiya har qanday o‘lchamdagi kirish ma’lumotlarini qabul qilib, ularda hisoblashlar amalga oshiradi va o‘lchami belgilangan chiqish hosil qiladi. Hash funksiyasi ikki kirish ma’lumotining bir xil chiqishni yaratmasligini ta’minlashi kerak. Hash funksiyalari DLT ning o‘zgartirib bo‘lmasligini himoya qilishda muhim ahamiyatga ega. Blokcheynda hash ishlatilishi tufayli, har bir

qo‘shilgan blok oldingi hashni oladi, va yangi yaratilgan hash barcha tugunlar bilan bo‘lishiladi. Har bir tugun o‘zining nusxasini saqlaydi; biror blokni o‘zgartirmoqchi bo‘lgan har kim barcha tugunlarda ma’lumotlarni yangilashga majbur bo‘ladi, bu esa tugunlar soni oshgani sayin ancha qiyinlashadi.



2-rasm. Blokcheyn hosil qilishda bloklarning bog‘lanishi

Taqsimlangan tizimlar - shuning uchun blokcheynlar tranzaksiyani blokcheynga qo‘shishdan oldin uni tasdiqlash uchun tarmoqning tugunlari orasida sinxronizatsiya va kelishuvga erishish mexanizmini talab qiladi. Turli blokcheynlar turli konsensus mexanizmlaridan foydalanadi va ularning ko‘pchiligi quyidagi bir yoki bir nechta, lekin barcha talablarni optimallashtirgan: tranzaksiyalar tezligi/uzatish sig‘imi, energiya sarfi, markazlashmaganlik, xavfsizlik yoki kengaytiriluvchanlik[3].

Blokcheynning ikki asosiy kategoriyasi mavjud: ruxsat berilmagan va ruxsat berilgan. Ushbu ikki kategoriya ichida to‘rtta variant joylashgan bo‘lib, ba’zi o‘zaro xususiyatlarga ega: jamoat, shaxsiy, konsorsium va gibrid.

Bunda: blokcheyn 2 turga ajratiladi:ruxsatsiz va ruxsat berilgan.

Ommaviy (hech qanday signal beruvchi obyekt tomonidan boshqarilmaydi);

Gibrid (ba’zi bir jamoatchilik nazorati bilan bitta obyekt tomonidan boshqariladi);

Xususiy (bitta obyekt tomonidan boshqariladi);

Konsortsium (obyektlar guruhi tomonidan boshqariladi).

Ommaviy blokcheynlar. Jamoat blokcheynlari to‘liq markazlashmagan va ruxsat berilmagan bo‘lib, har qanday kishi ishtirok etishi mumkin. Ushbu asosda, jamoat blokcheynlari teng huquqlarni taqdim etadi va har kim yangi bloklar yaratish va/yoki ma’lumot bloklarini tasdiqlash huquqiga ega. DLT-ni qo‘llab-quvvatlash uchun zarur bo‘lgan katta energiya iste’moli va to‘liq maxfiylik va anonimlikning yo‘qligi jamoat blokcheynining asosiy kamchiliklari hisoblanadi. Har kim jamoat blokcheyniga qo‘shilishi mumkin bo‘lgani uchun, zararli faoliyatlar, masalan, xakerlik, tokenlarni o‘g‘irlash va tarmoqni to‘xtatish ehtimoli mavjud.

Xususiy blokcheynlar. Shaxsiy blokcheynlar ruxsat berilgan blokcheynlar bo‘lib, egasi tarmog‘iga kirish darajasini belgilaydi. Qoidalar belgilanadi va administrator tomonidan o‘zgartirilishi mumkin. Boshqaruv ushbu tizimni shaxsiy blokcheynlarni istagan kompaniya yoki tashkilotlar uchun juda yaxshi ishlash holatiga olib keladi. Shaxsiy blokcheynlar odatda tezroq va xavfsizroq bo‘ladi, chunki egasi/administrator tugunlarni boshqaradi, bu esa konsensusga tezroq erishish imkonini beradi.

Konsorsium blokcheynlari. Konsorsium blokcheynlari ham ruxsat berilgan blokcheynlar bo‘lib, shaxsiy blokcheynlardan farqli o‘laroq, ular bir guruh tashkilotlar tomonidan boshqariladi. Ruxsat berilgan blokcheyn sifatida konsorsium blokcheynining foydalari boshqaruv, xavfsizlik, tezlik va kengaytirilishdir. Asosiy kamchilik shundaki, yangilanishlarni amalga oshirish uchun barcha ishtirokchilarning kelishuvini talab qiladi. Konsorsium blokcheynlarining foydalari shaxsiy blokcheynlar bilan o‘xshash, chunki kirish nazorat qilinadi. Konsorsium blokcheynlari shaxsiy blokcheynlarga qaraganda ko‘proq markazlashmagan bo‘lib, yuqori darajadagi xavfsizlikni ta’minlaydi.

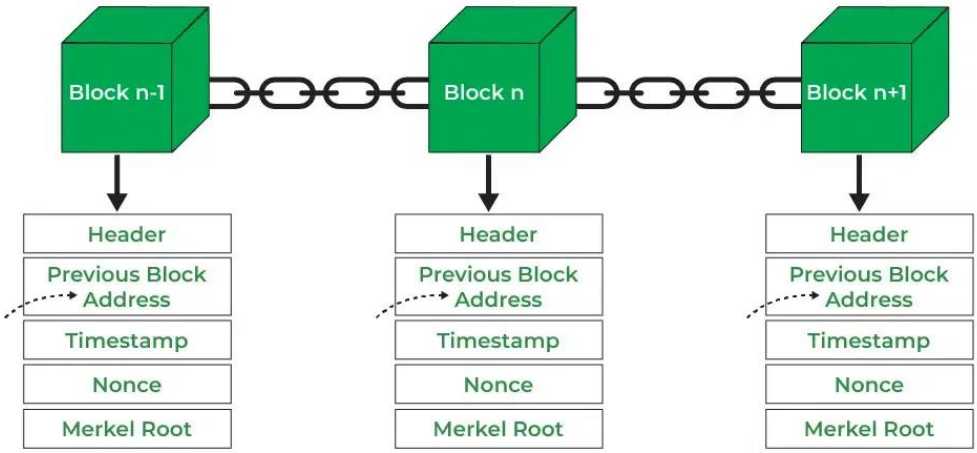
Gibrid blokcheynlar. Gibrid blokcheynlari nomidan ham ma’lumki, jamoat va shaxsiy blokcheynlarning foydalarini birlashtiradi. Ular tarmog‘iga kirishni nazorat qiladigan yagona tashkilot tomonidan boshqariladi, ammo shuningdek, jamoat blokcheynining xususiyatlarini, masalan, yaxlitlik, shaffoflik va xavfsizlikni taklif qiladi, bu esa shaxsiy va jamoat blokcheynlari yechimlarining eng yaxshi tomonlarini taqdim etadi. Bu tashkilotlarga texnologik cheklovlarga asoslanib rejalarni moslashtirish o‘rniga, istagan narsalarini amalga oshirishda yaxshiroq nazoratni taqdim etadi.

Blockchainning asosiy komponentlari

- *Tugun (Node):* Tugunlar tarmoq ishtirokchilari bo‘lib, ularning qurilmalari ularga taqsimlangan reyestrni kuzatib borishga va turli tarmoq vazifalarida aloqa markazlari sifatida xizmat qilishga imkon beradi. Bir miner yangi blokni tranzaksiyalar bilan blokcheynga qo‘shmoqchi bo‘lganda, blok barcha tarmoq tugunlariga tarqatiladi.
- *Tranzaksiya:* Tranzaksiya shartnoma yoki kelishuvni anglatadi va tomonlar o‘rtasida aktivlar (odatda naqd pul yoki mulk) transferlarini bildiradi. Blockchain tarmog‘idagi kompyuterlar tranzaksiya ma’lumotlarini raqamli reyestr deb ataladigan saqlashda nusxasini saqlaydi.
- *Blok:* Blok blockchain tarmog‘ida zanjirda bir bog‘lanishga o‘xshaydi. Kriptovalyuta sohasida bloklar tranzaksiyalarni saqlovchi yozuvlar kabi bo‘lib, ular hash daraxtiga shifrlanadi. Har kuni dunyoda katta miqdorda tranzaksiyalar sodir bo‘ladi. Foydalanuvchilar bu tranzaksiyalarni blok tuzilmasi yordamida kuzatib boradilar.
- *Zanjir (Chain):* Zanjir - bu barcha bloklarning butun blockchain strukturasida bir zanjir yordamida bog‘lanishini anglatadi. Ushbu bloklar oldingi blokning hash’i yordamida bog‘lanadi, bu esa zanjirli tuzilishni ifodalaydi.
- *Minerlar:* Blockchain qazib olish - bu tranzaksiyalardagi har bir qadamni tasdiqlash jarayoni bo‘lib, barcha kriptovalyutalar bilan ishlashda muhim o‘rin tutadi. Ushbu qazib olish jarayonida qatnashgan odamlar minerlar deb ataladi. Blockchain qazib olish - tranzaksiyalardagi har bir qadamni tasdiqlash jarayonidir.
- *Konsensus:* Konsensus - bu kompyuter va blockchain tizimlarida tarmoqning yagona holati bo‘yicha zarur kelishuvga erishish uchun ishlatiladigan xato xotiraga chidamli mexanizmdir. Bu multi-agent tizimlari yoki taqsimlangan jarayonlar kabi cryptocurrency tizimlarida foydalidir. Bu, shuningdek, rekordlarni saqlash va boshqa ishlarni amalga oshirishda ham foydalidir.

Ma’lumotlarni saqlash va boshqarish:

- *Bosh (Header):* Bu butun blockchain ichidagi ma’lum bir blokni aniqlash uchun ishlatiladi. U blockchaindagi barcha bloklarni boshqaradi. Blok boshligi minerlar tomonidan odatdagi qazib olish faoliyati doirasida nonce qiymatini o‘zgartirish orqali vaqti-vaqti bilan xeshlanadi. Blok boshida uchta blok metama’lumotlar to‘plami mavjud.
- *Oldingi Blok Manzili/Hash:* Bu i+1-chi blokni i-chi blok bilan xesh yordamida bog‘lash uchun ishlatiladi. Qisqacha aytganda, bu zanjirdagi avvalgi (ota-ona) blokning xeshiga havola bo‘ladi.
- *Vaqtni Belgilash (Timestamp):* Bu tizim blokdagi ma’lumotlarni tasdiqlaydi va raqamli hujjatlarning yaratilgan vaqtini yoki sanasini belgilaydi. Vaqtni belgilash - bu hujjat yoki voqeaning noyob ravishda aniqlash uchun ishlatiladigan belgilar qatoridir va uning yaratilgan vaqtini ko‘rsatadi.
- *Nonce:* Bu faqat bir marta ishlatiladigan son. U blokdagi ishni tasdiqlashning asosiy qismidir. Nonce, joriy maqsadga teng yoki kichik bo‘lsa, yashirin maqsad bilan solishtiriladi. Minerlar ko‘plab Nonce’ni har soniyada sinab ko‘rishadi va ularning qaysi biri haqiqiy Nonce ekanligini topishadi.
- *Merkel Root:* Bu ma’lumotlar bloklarining turli tuzilmalarini tashkil etuvchi ma’lumotlar strukturasi. Merkel daraxti, butun tranzaksiyaning raqamli izini ishlab chiqarib, blokdagi barcha tranzaksiyalarni saqlaydi. Bu foydalanuvchilarga tranzaksiya blokga kiritilishi mumkinmi yoki yo‘qligini tasdiqlash imkonini beradi.



3-rasm. Blockcheyn strukturasi

Blockchain texnologiyasi, ma’lumotlarni xavfsiz va shaffof tarzda yozib olishning kuchli usulini taklif etadi, bu uning markazlashmagan, o‘zgarmas daftarchasi orqali amalga oshiriladi. Ma’lumotlarni bloklarga tashkil qilib, zanjirda bog‘lash orqali blockchain, bir marta ma’lumot qo‘shilganidan so‘ng, uning o‘zgartirilishi yoki o‘chirilishi mumkin emasligini ta’minlaydi. Ushbu tuzilma, turli ilovalar, jumladan kriptovalyutalar va ta’minot zanjirlarini boshqarish kabi sohalarda xavfsizlik, ishonch va yaxlitlikni kuchaytiradi. Blockchain texnologiyasi rivojlanishda davom etar ekan, uning markazlashmaganlik, shaffoflik va kriptografik xavfsizlik kabi asosiy tamoyillari uning samaradorligi va ishonchliligini ta’minlashda muhim ahamiyatga ega bo‘ladi.

ADABIYOTLAR:

1. Mohanta B.K.; Dehury M.K.; Kalidindi S.V. Управление идентификацией в IoT с использованием блокчейна // В трудах 13-й Международной конференции по вычислительным, коммуникационным и сетевым технологиям (ICCCNT), Харагпур, Индия, 3–5 октября 2022.; стр.1–6.
2. Siris V.A.; Dimopoulos D.; Fotiou N.; Voulgaris S.; Polyzos G.C. Blockchain для авторизации в ограниченных средах IoT // Всемирного форума IEEE 2019 года по Интернету вещей (WF-IoT'19), Лимерик, Ирландия, 15–18 апреля 2019 г.; стр. 364–367.
3. Тонг Ф., Чен С., Хуан С., Чжан И., Шен С. Безопасная внутридоменная и междоменная авторизация и аутентификация с использованием блокчейна для Интернета вещей // IEEE Internet Things J. 2022, 10 , 7761–7773.