

BLOKCHEYN TIZIMIDA FAYLLARNI SAQLASH USULLARI

Qurbonova Kabira Erkinovna

TDTU Katta oqituvchi

Ahmadov Ulug'bek Said o'g'li

*Muxammad al – Xorazmiy nomidagi TATU “Kiberxavfsizlik va kriminalistika”
kafedrası stajyor o'qituvchisi*

Oripov Asilbek Baxtiyor o'g'li

Xayriddinov Shaxboz Shavkatovich

Muxammad al – Xorazmiy nomidagi TATU talabalari

Annotatsiya: Ushbu maqolada blokcheyn tizimida fayllarni saqlash usullari, ularning arxitekturaviy xususiyatlari hamda afzallik va kamchiliklari tahlil qilinadi. Blokcheyn – bu taqsimlangan reyestr (distributed ledger) texnologiyasi bo'lib, ma'lumotlarning o'zgarmasligi (immutability), shaffofligi va xavfsizligini ta'minlaydi. Biroq katta hajmdagi fayllarni bevosita blokcheynda saqlash texnik va iqtisodiy jihatdan samarasiz bo'lishi mumkin.

Kalt so'zlar: Blokcheyn, taqsimlangan reyestr, on-chain, off-chain, IPFS, Filecoin, Storj, markazlashmagan saqlash, kriptografik xesh, ma'lumotlar xavfsizligi.

Ma'lumotlar xavfsizligini ta'minlash barcha tizimlar uchun juda muhimdir. An'anaga ko'ra, ma'lumotlar relyatsion ma'lumotlar bazasi tizimlarida yoki NoSQL ma'lumotlar do'konlarida saqlanadi. Afsuski, ushbu an'anaviy saqlash usullari nafaqat ma'lumotlarni o'g'irlashga, balki ruxsatsiz o'zgartirishlarga ham himoyasiz qiladi. Ma'lumotlarni o'g'irlash aniq xavfsizlik buzilishini ko'rsatsada, markazlashtirilgan ma'lumotlarni saqlash texnologiyalari bilan bog'liq yana bir muhim muammo - bu bitta nosozlik nuqtalarining mavjudligi.

Biroq, blokcheyn texnologiyasi o'zgarmaslik va markazsizlashtirish kabi atributlarni taklif qiluvchi ma'lumotlarni saqlashga yangi yondashuvni taqdim etadi. Blockchain yordamida ma'lumotlarni saqlashning asosan ikkita usuli mavjud. Bir yondashuv ma'lumotlarni tranzaksiyaning bir qismi sifatida to'g'ridan-to'g'ri saqlashni o'z ichiga oladi, bu ko'pchilik ommaviy blokcheyn tizimlari uchun mumkin. Boshqa usul aqlli shartnoma orqali ma'lumotlarni saqlashni o'z ichiga oladi.

Shunga qaramay, joriy blokcheyn saqlash yechimlari o'z cheklovlariga ega. Birinchidan, yuqori darajada foydalaniladigan blokcheynlarda buni qilish narxi haddan tashqari qimmat bo'lishi mumkin. Bundan tashqari, blokcheynlarda saqlanadigan ma'lumotlar ko'pincha statik va dasturlashtirilmaydi. DeFi, NFT va GameFi kabi markazlashtirilmagan ilovalarning tobora ommalashib borishi xavfsizroq, markazlashmagan va tejamkor dinamik saqlash tizimlariga talab ortib borayotganini ta'kidlaydi.

EthStorage innovatsion, tejamkor va dinamik saqlash yechimiga yo'l ochmoqda, u mavjud saqlash imkoniyatlari duch keladigan cheklovlarni bartaraf etish imkoniyatiga ega.

Joriy blokcheyn saqlash yechimlari. So'nggi paytlarda markazlashtirilmagan saqlash mashhurlikning o'sishiga guvoh bo'ldi va bozorda turli xil variantlar paydo bo'ldi. Quyida hozirda mavjud bo'lgan markazlashtirilmagan ma'lumotlarni saqlash mahsulotlarining ayrimlari keltirilgan.

Arweave: Ba'zi markazlashtirilmagan ma'lumotlarni saqlash yechimlari maxfiylikka ustuvor ahamiyat bersa yoki senzura va monitoringdan qochishga qaratilgan bo'lsada, Arweave ma'lumotlarning doimiylikiga e'tibor qaratish orqali o'zini ajratib turadi. Arweave blokcheyn texnologiyasiga o'xshashliklari bilan peer-to-peer (P2P) saqlash protokoli sifatida ishlaydi. U Arweave mijozlari sifatida xizmat qiluvchi shaxsiy kompyuterlarning qo'shimcha saqlash imkoniyatlaridan foydalanadi. Tizim ma'lumotlarni saqlash va boshqa funksiyalarni osonlashtiradigan permaweb deb nomlanuvchi dastur orqali ishlaydi.

Permaweb ichida veb-sahifalarni va har xil turdagi ma'lumotlarni, shu jumladan statik fayllarni saqlash uchun o'zgarmas muhit yaratiladi. Ushbu saqlash xizmatidan foydalanish uchun foydalanuvchilar AR tokenlaridan foydalangan holda bir martalik to'lovni amalga oshirishlari talab qilinadi, buni ko'pchilik kriptovalyuta birjalaridan olish mumkin. Shunisi e'tiborga loyiqki, Arweave 100% hamjamiyat tomonidan boshqariladigan platforma sifatida ishlaydi va saqlash opsiyalari turi boshqa saqlash protokollariga qaraganda moslashuvchan bo'lmasligi mumkin.

Filecoin: Filecoin 2017-yilda 257 million dollar yig'ib, tarixdagi eng yirik tanga takliflaridan birini o'tkazgani uchun keng tan olingan.

Tranzaktsiyalarni amalga oshirish uchun foydalanuvchilar o'zlarining fayllarini saqlash uchun FIL dan foydalanadilar, "konchilar" yoki saqlash tugunlari esa ushbu fayllarni saqlash uchun FIL oladi. Blokcheyn daftarchasi ushbu tranzaktsiyalarni qayd qiladi va fayllar to'g'ri saqlanganligini tasdiqlovchi dalil bo'lib xizmat qiladi. Filecoin IPFS asosida qurilgan, P2P gipermedia protokoli, taqsimlangan saqlash uchun HTTP-dan foydalanish cheklovlarini hal qilish uchun mo'ljallangan.

Narxlar nuqtai nazaridan, Filecoin har kimning ishtirok etishiga imkon beruvchi ochiq bozor sifatida ishlaydi. Garchi ushbu sozlash ko'proq moslashuvchanlikni taqdim etsa-da, bu maxsus saqlash byudjetiga ega bo'lgan tashkilotlar uchun, ayniqsa xabarlar tomonidan iste'mol qilinadigan resurslar uchun to'lovlarni talab qiladigan "gaz to'lovlari" ni hisoblashda qiyinchiliklar tug'dirishi mumkin.

Filecoin loyihasi ochiq manba asosida ishlaydi va saqlash provayderlari, iste'molchilar va ishlab chiquvchilarni fayl tizimidan foydalangan holda ilovalar yaratishga undaydi. Ammo shuni ta'kidlash kerakki, Filecoin tomonidan qo'llaniladigan Lotus tugunlari hozirda faqat Linux va MacOS-da qo'llab-quvvatlanadi, Windows-da esa o'lchovni cheklash hali qo'llab-quvvatlanmaydi.

Siakoin: Filecoin-ga o'xshab, Sia global P2P tarmog'ida fayllarni shifrlaydigan va tarqatadigan markazlashtirilmagan ma'lumotlarni saqlash platformasini taklif qilish uchun blokcheyn texnologiyasidan foydalanadi. Sia mijoz dasturi Windows, Linux va macOS bilan mos keladi va har bir faylni 30 ta segmentga ajratadi va ularni turli xostlarga tarqatadi.

Ortiqchalikni ta'minlash va atigi 10 ta segmentdan fayllarni tiklashni ta'minlash uchun dastur Reed-Solomon o'chirish kodlashidan foydalanadi. Bundan tashqari, u segmentlarni saqlash xostlariga uzatishdan oldin ularni shifrlash uchun ochiq manbali Threefish algoritmidan foydalanadi. Siacoin ijarachilar tomonidan saqlash sotib olish uchun ishlatiladi, xostlar esa fayllarni saqlash uchun garov sifatida foydalanadi.

Sia dasturiy ta'minoti butunlay ochiq manba bo'lib, dasturchilar ilovalarni yaratishda foydalana oladigan API ni o'z ichiga oladi. Sia-ni ijarachi yoki uy egasi sifatida sozlash jarayoni yaxshi hujjatlashtirilgan va sodda bo'lib, uni raqobatchilardan ajratib turadi.

Sia markazlashtirilmagan saqlash bozorini taklif etadi, bu erda saqlash provayderlari biznes uchun raqobatlashadi, bu esa kamroq taxmin qilinadigan narxlarni keltirib chiqaradi. Sia ma'lumotlariga ko'ra, 1 TB saqlash oyiga 2 dollardan kam bo'lishi kerak (Siacoin bilan to'lanadi), lekin ijarachilar shartnoma tuzish to'lovlari va faylni yuklash va yuklab olish uchun tarmoqli kengligi to'lovlari kabi qo'shimcha xarajatlarni ham hisobga olishlari kerak.

Storj va Tardigrad: Storj Sia-ning asosiy raqiblaridan biri bo'lib, blokcheynga asoslangan saqlash bilan o'xshash xizmatlarni taklif qiladi. Storj Labs ikkita alohida biznes sohasini o'z ichiga oladi: ta'minot tomoniga e'tibor qaratadigan Storj va talab tomonini hal qiluvchi Tardigrad. Storj tarmog'i ta'minot tomonida saqlashni ta'minlovchi tugun operatorlari va xostlarini o'z ichiga oladi, Tardigrade mijozlari esa talab tomonida tardigrade.io veb-sayti orqali saqlashni sotib oladi. Aslida, Storj tugun operatorlari Tardigrade foydalanuvchilariga markazlashtirilmagan saqlashni taklif qiladi.

Storj xotirasi S3-ga mos keladi, ma'lumotlarni kichikroq segmentlarga ajratish va ularni xuddi Sia kabi global tarmoqda saqlash uchun AES-256-GCM simmetrik shifrlashdan foydalanadi. Biroq, Storj faylni 80 ta segmentga ajratadi, shundan 30 ta segment butun faylni qayta tiklash uchun etarli. Storj Labs ma'lumotlariga ko'ra, Tardigrade saqlash zaxira nusxalari, arxivlar, media-kontent, gibrid bulutli saqlash xizmatlari, katta hajmdagi fayllarni uzatish, 4 KB dan ortiq jurnal fayllari va ma'lumotlar bazasi oniy tasvirlari uchun juda mos keladi. Tardigrade, shuningdek, ishlab chiquvchilar uchun markazlashtirilmagan bulutli saqlash sifatida sotiladi.

Boshqa xizmatlardan farqli o'laroq, Tardigrade qat'iy narxlarni taklif qiladi, bu esa saqlash xarajatlarini byudjetlashtirishni osonlashtiradi. Narxlar tashkilot tomonidan saqlangan va yuklab olingan ma'lumotlar miqdoriga bog'liq. Masalan, bepul reja foydalanuvchilarga oyiga 150 Gb saqlash va 150 Gb gacha (har bir loyiha

uchun 50 Gb) o'tkazish qobiliyatini taqdim etadi, pro reja esa har bir terabayt saqlash uchun 4 dollar va o'tkazish qobiliyati har bir terabayt uchun 7 dollar oladi.

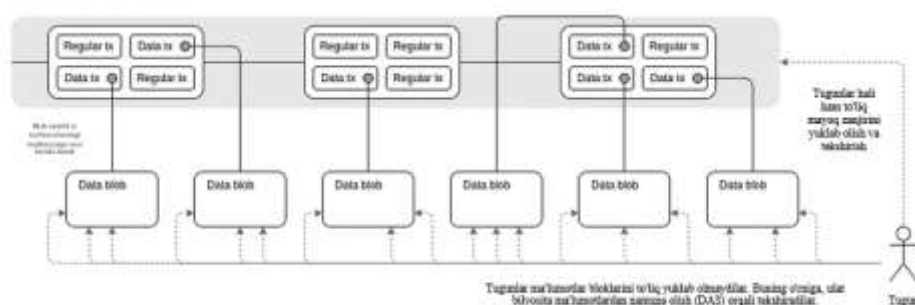
Hozirgi vaqtda bozorda ko'plab blokcheyn ma'lumotlarini saqlash yechimlari mavjud, ammo bu yechimlar duch keladigan umumiy muammo saqlangan ma'lumotlarda dinamiklik va dasturlash qobiliyatining yo'qligi. Bundan tashqari, ushbu saqlash opsiyalarining aksariyati EVM-ga mos kelmaydi, bu esa Web 3 ekotizimining aksariyat qismini tashkil etuvchi EVM blokcheynlari bilan ishlashda ulardan foydalanish holatlarini cheklaydi. Natijada, saqlash tizimlari Web 3 ekotizimidagi o'zgarishlarga mos kelishini ta'minlash uchun innovatsion yechimlar talab qilinadi.

Hozirgi vaqtda bozorda blokcheyn ma'lumotlarini saqlash uchun bir nechta yechimlar mavjud bo'lsa-da, ushbu yechimlar duch keladigan umumiy muammo shundaki, saqlangan ma'lumotlar turi dinamik yoki dasturlashtirilmaydi. Bundan tashqari, yuqorida sanab o'tilgan saqlash yechimlarining aksariyati EVM-ga mos kelmaydi, bu esa Web 3 ekotizimining ko'p qismini tashkil etuvchi EVM blokcheynlari bilan o'zaro aloqada bo'lganda ulardan foydalanishning cheklangan holatlariga ega. Shu sababli, saqlash yechimlari Web 3 ekotizimidagi o'zgarishlarga mos kelishini ta'minlash uchun yangi innovatsiyalarni yaratish kerak.

EIP-4844: Taklif etilayotgan Ethereumni yaxshilash taklifi 4844 (EIP-4844), shuningdek, Kankunni yangilash deb ham ataladi, Ethereum tarmog'ida tranzaksiya to'lovlarini kamaytirishga qaratilgan. Ushbu yangilanish gaz narxini pasaytirish uchun mo'ljallangan, blob-tashuvchi tranzaksiya deb ataladigan yangi turdagi tranzaksiyani taqdim etadi.

EIP-4844 proto-danksharding deb ham ataladi, chunki u yangi tranzaksiya formatlari va tekshirish qoidalarini o'z ichiga olgan danksharding asosi va mantiqini amalga oshiradi. Maqsad Ethereum tarmog'ining samaradorligini oshirish va ushbu yaxshilanishlar orqali umumiy tranzaksiya to'lovlarini kamaytirishdir.

Proto-Danksharding: Danksharding Ethereum uchun yangi sharding arxitekturasini taqdim etadi, u masshtablilikni oshirish uchun bloblar deb ataladigan katta hajmdagi ma'lumotlar birliklaridan foydalanadi. 2-qavat protokollari yig'malarga qaratilgan ushbu qo'shimcha ma'lumotlar bo'shliqlaridan tarmoq tiqilib qolishini yumshatish uchun foydalanadi va natijada tranzaksiya to'lovlarining kamayishiga olib keladi.



1.1-rasm. Ethereum ishlashi

Biroq, Ethereum-da to'liq dankshardingni amalga oshirish birdaniga sodir bo'lmaydi. Bu EIP-4844 yoki proto-danksharding kabi bir qator tayyorgarlik yangilanishlarini talab qiladi. Ethereum asoschilaridan biri Vitalik Buterin ta'riflaganidek, proto-danksharding dankshardingning "mantiqi va iskalasining ko'p qismini" o'z ichiga oladi, lekin haqiqiy shardingni o'z ichiga olmaydi.

Proto-Dankshardingni saqlash yechimlari: Proto-danksharding ko'p o'lchovli EIP-1559 to'lov bozori orqali gaz narxlari inqirozini hal qiladi. Proto-dankshardingdan oldin, EIP-4488 yuqori gaz to'lovi muammosini hal qilishni maqsad qilgan.

EIP-4488 ikkita qoidani o'z ichiga oladi: Qo'ng'iroq ma'lumotlari gaz narxi bayt uchun 16 gaz birligidan bayt uchun 3 gaz birligiga tushirildi.

Har bir blok uchun 1 MB cheklov amalga oshirildi, har bir tranzaksiya uchun qo'shimcha 300 bayt, natijada nazariy maksimal taxminan 1,4 MB.

Qattiq chegaraga ega bo'lish o'rtacha yuk ko'tarilishining eng yomon holatda yuk ko'tarilishiga olib kelmasligini ta'minlaydi. Bu, shuningdek, eng yomon blok hajmi joriy hajmdan pastroq bo'lishini kafolatlaydi, 1,8 MB bilan solishtirganda 1,4 MB.

XULOSA

Xulosa qilib aytganda, blokcheyn tizimida fayllarni saqlash bevosita (on-chain) yoki bilvosita (off-chain) amalga oshirilishi mumkin. Katta hajmdagi ma'lumotlar uchun to'liq on-chain saqlash iqtisodiy va texnik jihatdan maqsadga muvofiq emas. Shu sababli zamonaviy tizimlarda ko'proq gibrad yondashuv qo'llaniladi.

Markazlashmagan saqlash platformalari IPFS, Filecoin va Storj blokcheyn bilan integratsiyalashgan holda ma'lumotlarning yaxlitligi va xavfsizligini ta'minlaydi. Kelajakda blokcheyn asosidagi saqlash tizimlari bulutli texnologiyalar bilan birgalikda yanada rivojlanishi va keng qo'llanilishi kutilmoqda.

ADABIYOTLAR RO'YXATI:

1. Mastering Blockchain. – Packt Publishing, 2017.
2. Ethereum Foundation. Ethereum Smart Contract Documentation.
3. IPFS. IPFS Technical Documentation.
4. Filecoin Foundation. Filecoin Whitepaper.
5. IEEE. Blockchain-based Data Storage Research Articles.