ISSN 2181-3187

BLOCKCHAIN TEXNOLOGIYASI ASOSIDA AXBOROT ISHONCHLILIGI VA XAVFSIZLIGINI TA'MINLASH TAMOYILLARI

Xasanov Muxiddin Kamildjanovich,
Mardayev Nurmurod Gulmurodovich
IIV Surxondaryo akademik litsey o'qituvchilari

Annotatsiya: *Jamiyatining yashash sharoitlarini yengillashtirish vositasi sifatida qaralayotgan internet tarmog'i o'z o'rnida, intellektual mulk siyosatida yaratilgan obyektlarni muhofazasini ta'minlashda ishonchlilik nuqtai nazaridan emas, balki, ularning muhofazasini buzilishiga sababchi bo'layotganligi haqida batafsil tushuntirib beriladi.*

Kalit so'zlar: texnologiya, frod, Bincoin, Ethereum, Riple, kriptografiya, blokchain.

Axborot texnologiyalari va raqamli iqtisodiyotning rivojlanishi bilan iqtisodiyot va menejmentning turli sohalarida to'liq axborotlashtirish davri davom etmoqda. Moliyaviy tuzilmalarning bevosita pul bilan bog'liq faoliyati kiberbuzg'unchilar uchun ayniqsa, jozibador ko'rinadi. Axborot xavfsizligi sohasidagi mutaxassislar masofaviy bank xizmatlari ko'rsatishni himoyalashda katta muammolarga duch kelmoqdalar. Turli mug'ombirliklar, katta talafotlar yetkazuvchi **frod** (elektron tijoratdagi firibgarlik) bilan kurashish uchun bank sohasida ishonchli tizimlardan foydalanishga to'g'ri kelmoqda. Har bir kishi o'zining bankka taqdim qiladigan shaxsiy ma'lumotlari maxfiy bo'lib qolishidan manfaatdor.

Raqobatning kuchayishi bilan texnik maqsadlar uchun ma'lumot olishning rivojlanishi tezda operatsiyalarni yaxshilash va aktivlarning samaradorligini oshirish uchun oqilona yo'lga aylanmoqda. Iqtisodiy nazariyaga ko'ra, bank tizimi iqtisodiy o'sishni rag'batlantirish va bu eng katta o'sish potentsialiga ega bo'lgan tarmoqlar o'rtasida pul oqimlarini qayta taqsimlash uchun filtr vazifasini bajaradi. Onlayn bank, tezkor operatsiyalar, kontaktsiz to'lovlar va tezkor pul o'tkazmalarining keng tarqalishi

ISSN 2181-3187

bilan ko‘plab xakerlik usullari, shu jumladan jismoniy va statsionar qurilmalar va uskunalar orqali blockchain bugungi kunda axborot xavfsizligi va apparat tizimlarini himoya qilish masalasini yangi bosqichga olib chiqishi quyida ko‘rsatkichlarni o‘z ichiga oladi bularga:

- taqsimlangan tarmoqlarni hisoblashning xatolarga chidamliligiga,
- ma’lumotlarni saqlash va ma’lumotlarni shifrlash muammolarini ko‘rib chiqishiga,
- qarorlarni muvofiqlashtirishni soddalashtirishiga,
- tashkiliy jarayonlar xarajatlarini optimallashtirishiga,
- boshqaruv samaradorligini oshirishga,

imkon berdi. Blockchain tizimlarida tranzaksiya ma’lumotlarini himoyasi uchun xesh-funksiyalariga qo‘shimcha ravishda, yana bir muhim texnologiya - kriptografiyadan faol foydalaniladi. Kriptografiya Blockchainning eng muhim komponentidir. Shu kungacha kriptovalyutalarning maqsadi foydalanuvchilar o‘rtasidagi moliyaviy hisob-kitoblardir. Shuning uchun bloklar amalga oshirilgan tranzaktsiyalar haqidagi ma’lumotlarni saqlaydi. Agar ushbu jarayonni tushunarli tilda tasvirlashda zanjirni yaratish quyidagicha ko‘rinadi:

- Konchilar blockchainga qo‘shiladigan ma’lum miqdordagi yangi tranzaktsiyalarni tanlaydi. Eng yuqori komissiya to‘langan arizalarga ustunlik beriladi.
- Muayyan vaqtdan so‘ng tanlangan operatsiyalar yangi blokga qo‘shiladi.
- Konchilar hash hisob-kitoblarini amalga oshiradilar. Tranzaktsiyalarni tekshirish jarayoni turli foydalanuvchilarning blockchainlariga kiritilgan ma’lumotlarni taqqoslash sifatida taqdim etilishi mumkin. To‘g’ri zanjir tarmoqning boshqa ishtirokchilari bilan mos keladigan zanjirdir.
- Tranzaktsiyalar tekshirilgandan so‘ng, yangi blokga o‘zining raqamli imzosi (xesh) beriladi. Ushbu shifr unga kiritilgan izlarning haqiqiyligini aniqlaydi.

ISSN 2181-3187

Tarqalgan reestr faoliyatning turli sohalarida masalan moliya, ovoz berish, foydalanuvchilar o‘rtasida ma’lumotlar almashinuvida qo‘llanilishi mumkin. Shu munosabat bilan blockchainlarning bir nechta turlari mavjud:

Shaxsiy - Tarqalgan ma’lumotlar bazalari nafaqat to‘lov vositasi sifatida, balki boshqa sohalarda ham qo‘llaniladi. Blockchain texnologiyalari yordamida aqliy hujumlar o‘tkaziladi, fayllar uzatiladi va aqlli shartnomalar tuziladi. Ushbu maqsadlar uchun yopiq (xususiy) blockchainlar mos keladi. Ro‘yxatga olish kitobiga kirish ma’lum mijozlar uchun cheklangandir. Bunday tarmoq ichida tranzaktsiyalar barcha ishtirokchilar va bitta asosiy server tomonidan tekshiriladi. Xususiy registrlar bir qator afzalliklarga ega:

- *Maxfiylik.* Agar tarmoq qimmatli ma’lumotlarni (shaxsiy hujjatlar, yozishmalar) uzatish uchun zarur bo‘lsa, zanjirga faqat jamiyat a’zolari kirishi kerak.
- *Tranzaksiyani qayta ishlash tezligi*. O‘tkazish alohida asosiy tugun tomonidan bir zumda tasdiqlanishi mumkin.
- *Kam xarajatlar.* Agar tarmoqda xususiy konchilar bo‘lmasa, ular uchun komissiya stavkalarini belgilash shart emas.

Ommaviy - Ochiq blockchain butunlay markazlashtirilmagan tarmoq sifatida yaratilgan. Hamyon egalari teng huquqlarga ega va tranzaktsiyalarni tekshirish va yangi bloklarni qazib olishda ishtirok etishlari mumkin. Ushbu turdagi ro‘yxatga olishning bir qancha afzalliklari bor:

- Ma’muriyatning shoshilinch qarorlaridan himoya qilish. Har bir hamyon egasi ishlab chiquvchilar tomonidan taklif qilingan manba kodidagi o‘zgarishlarni qabul qilishi yoki rad etishi mumkin. Bu tarmoqning barqarorligini ta’minlaydi.
- Keng kamrovli kirish. To‘lov shlyuzlari, kripto birjalari va investitsiya loyihalari turli mamlakatlardan foydalanuvchilarni jalb qilishi va mijozlar bazasini doimiy ravishda kengaytirishi mumkin.

ISSN 2181-3187

Ommaviy blockchainning mohiyati har bir tranzaksiyaning raqamli imzosini (xesh) tekshirish qobiliyatidir. Misol uchun Bincoin, Ethereum, Riple va boshqa kripto ilovalarni keltirish mumkin. Ushbu kriptografik tushunchalarni chuqur tushunishga harakat qilamiz, chunki turli muammolar turli kriptografik echimlarni talab qilishi mumkin. Bir usul hech qachon hammaga mos kelmaydi va bu tizimdagi eng muhim xavfsizlik komponentidir. Kripto xavfsizligi yetarli emasligi sababli ko‘plab hamyonlar va birjalarga buzib kirilgan. Kriptografiya ikki ming yildan ortiq vaqtdan beri mavjud. Quyida kriptografiyadan foydalanishning boshqa usullari keltirilgan:

- maxfiylik - faqat mo‘ljallangan yoki vakolatli qabul qiluvchi xabarni tushunishi mumkin. Bu maxfiylik yoki maxfiylik deb ham ataladi;
- ma’lumotlar yaxlitligi - ma’lumotlarni tajovuzkor tomonidan yoki tasodifiy xatolar tufayli o‘zgartirib bo‘lmaydi. Ma’lumotlarning yaxlitligi ma’lumotlarning o‘zgartirilishiga to‘sqinlik qila olmasa-da, u ma’lumotlar o‘zgartirilganligini tekshirish vositasini ta’minlaydi;
- **autentifikatsiya** - jo‘natuvchining haqiqiyligi qabul qiluvchi tomonidan tekshirilishi kafolatlanadi;
- qaytarib bo‘lmaydiganlik - jo‘natuvchi, xabar yuborilgandan so‘ng, keyinchalik xabarni yuborganligini rad eta olmaydi. Bu shuni anglatadiki, jo‘natuvchi (inson yoki tizim) oldingi majburiyatlari yoki harakatlari uchun javobgarlikni rad eta olmaydi.

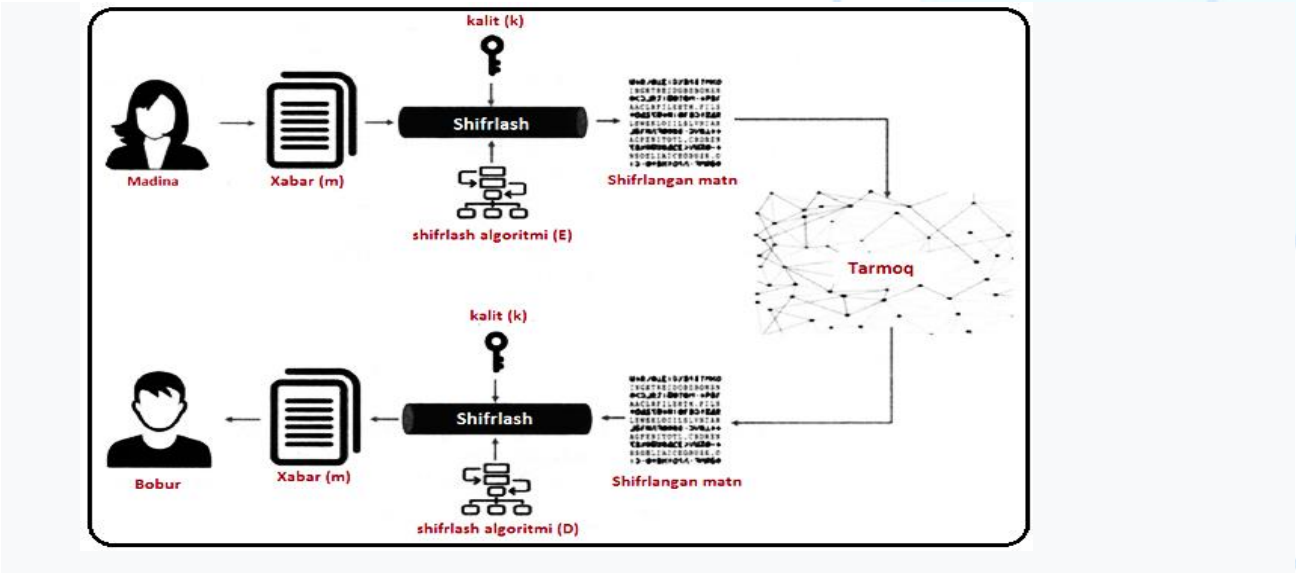
Bu ma’lumotlar matnli xabar, raqamli ma’lumotlar yoki kompyuter dasturi ko‘rinishidagi har qanday ma’lumotni oddiy matn deb atash mumkin. Kriptografiya g’oyasi ochiq matnni shifrlash algoritmi va shaxsiy matnni yaratuvchi kalit yordamida shifrlashdan iborat. Shundan so‘ng shaxsiy matn mo‘ljallangan qabul qiluvchiga uzatilishi mumkin, u oddiy matnni olish uchun shifrni ochish algoritmi va kaliti yordamida uni parolini hal qiladi[1].

[1] Б. Сингхал, Г. Дамеджа, П. С. Панда. –Блокчейн Руководство для начинающих разработчиковю Пт- 2020, 290-с.

ISSN 2181-3187

Keling, bir misolni ko‘rib chiqaylik Madina Boburga xabar (m) yubormoqchi. Agar u shunchaki xabarni xuddi shunday yuborsa, har qanday dushman, aytaylik tajavuzkor - xabarni osongina ushlab qolishi mumkin va shaxsiy hayot buziladi. Bunga e’tibor berish kerak-ki, Madina shifrlangan xabarni (shifrlangan matn) yaratish uchun (E) shifrlash algoritmi va (K) kaliti yordamida xabarni shifrlamoqchi. Xabarlarni ushlab turish uchun tajovuzkor (E) algoritmni va (K) kalitni bilishi kerak. Algoritm va kalit qanchalik kuchli bo‘lsa, dushmanga hujum qilish shunchalik qiyin bo‘ladi. Bunga e’tibor berish kerak, har doim hech bo‘lmaganda ishonchli bo‘lgan blockchain tizimlarini bashorat qilish maqsadga muvofiqdir. Bu shuni anglatadiki, tizim dushmanlar tomonidan mumkin bo‘lgan ba’zi turdagi hujumlarga qarshi turishi uchun kafolatlangan bo‘lishi kerak.

Kriptografiyaning umumiy tamoyillari sxematik tarzda 1.1-rasmda tasvirlangan. Umuman olganda kriptografiyaning ikki turi mavjud: simmetrik kalitli kriptografiya va assimetrik (ommaviy) kalitli kriptografiyadan iborat[2].



1.1-rasm. Kriptografiyaning umumiy tamoyillari

Yuqorida keltirilgan ma’lumotlarga tayangan quyidagi tushunchaga ega bo‘lamiz. Blockchain foydalanuvchilari o‘z ma’lumotlarini tarmoqdagi istalgan kompyuterdan yuborishlari va xavfsizligini ta’minlash kerak. Masalan, agar

ISSN 2181-3187

ma’lumotlar elementining egasi bo‘lmagan shaxs (masalan, tajovuzkor) blokni ataylab o‘zgartirishga qaror qilsa, u holda tizimdagi ushbu blokning barcha nusxalari tahlil qilinadi va qolgan qismdan farq qiladigan blok topiladi. Agar tizim blokning bunday versiyasini aniqlasa, uni noto‘g’ri deb tan olib, uni zanjirdan chiqarib tashlaydi. Blockchain texnologiyasidan foydalanish tuzilishi (axborot xavfsizligini ta’minlash texnologiyasi) maxsus zanjirga muvofiq tashkil etilgan, shuning uchun uni saqlash uchun mas’ul bo‘lgan yagona ma’lumot ombori yoki yagona Markaziy organ mavjud emas. Tarmoqning har bir foydalanuvchisi (blockchain tarmog’i) blokchainning barcha manbalarini yoki ularning bir qismini saqlaydi. Blockchain tarmoqlarining barcha foydalanuvchilari ma’lumotlarni tekshirish va saqlash uchun javobgardir, shuning uchun mavjud ma’lumotlarni o‘chirish va ishonchsiz ma’lumotlarni qo‘shish mumkin emas.

Foydalanilgan adabiyotlar ro‘yxati

1. Б. Сингхал, Г. Дамеджа, П. С. Панда. –Блокчейн Руководство для начинающих разработчиковю Пт- 2020, 290-с.

2. Kawasmi, Z., Gyasi, E. A. & Dadd, D. Blockchain adoption model for the global banking industry. Journal of International Technology and Information management, 28(4), 2020-y 112 – 154 p.

3. Gupta, R. Hands-on cybersecurity with blockchain : implement DDoS protection, PKI-based identity, 2FA, and DNS security using blockchain. (1st edition). Packt 2018-y.

4. Chapiro, C. Working Toward Financial Inclusion With Blockchain. 2021-Stanford Social Innovation Review. https://doi.org/10.48558/DZXJ-0Z18