

BLOKCHEYN TEXNOLOGIYASI XAVFSIZLIGI

B.Sh.Aytmuratov - t.f.n.

S.B. Abdullayev – magistrant

Ushbu maqolada Blockchain texnologiyasining xavfsizligi muhokama qilinadi. Blockchain texnologiyasi, texnologiyaning ijobiy va salbiy tomonlarini

Kalit so'zlar: Blokcheyn texnologiyasi, Bitcoin, xavfsizlik.

Blockchain - bu bir-biriga bog'langan bloklarga o'xshash ma'lumotlar bazasi. Bunday ma'lumotlar bazasining xususiyati shundaki, ma'lumotlarni saqlash qurilmasi umumiy serverga ulanmagan. Shu bilan birga, ma'lumotlar miqdori va shuning uchun bloklar soni doimiy ravishda o'sib bormoqda. Har bir yozuvda vaqt belgisi va oldingi yozuvga (blok) havola mavjud. Xavfsizlikni ta'minlash uchun ma'lumotlar shifrlangan. Muayyan blokga kirish faqat blokning shaxsiy kalitiga ega bo'lgan foydalanuvchi tomonidan olinadi, bu holda faylga yozish mumkin emas.

Blockchain texnologiyasi Bitcoinning asosi ekanligi bilan mashhur, ammo kriptovalyutalar haqida o'ylamasdan Blockchain-dan foydalanishning boshqa usullari mavjud. Ushbu texnologiyani tadbirning har bir ishtirokchisida mavjud bo'lgan, yangilangan kitob sifatida tasavvur qilish mumkin. Ushbu kitobda har qanday voqea qayd etilishi mumkin - moliyaviy operatsiyalardan tortib kvartiralarini sotish yozuvlarigacha. Blokcheyn eng tez rivojlanayotgan texnologiyalardan biridir. Bu raqamli axborot tranzaksiyalari bilan bog'liq ikkita eng katta muammolarni hal qiladi: nazorat qilish va takrorlash.

Blockchain elliptik egri chiziqdagi raqamlarni topishga asoslangan ochiq kalit tizimi bo'lgan Elliptic Curve Cryptography (ECC) dan foydalanadi. Ma'lumotlar xavfsizligi ularni bitta mahalliy serverda emas, balki butun dunyo bo'ylab kompyuterlar tarmog'ida taqsimlangan saqlash (ko'paytirish) bilan kafolatlanadi. Buxgalteriya kitobiga kiritilgan barcha yozuvlarni o'zgartirib bo'lmaydi - tranzaksiyalar ishtirokchilari o'rtasida konsensusga erishilmasa, hatto ma'lumotlar bazasi operatorlari ham buni qila olmaydi.

Blockchain xronologik yoki tranzaksiya tartibida bog'langan har qanday shifrlangan hujjatlar blokini himoya qilishi mumkin. Shuningdek, Blockchain reestriga ko'chmas mulk, konchilik huquqlari, transport vositalari, san'at asarlari, zargarlik buyumlari va boshqa ob'ektlarga bo'lgan huquqlar kiritilishi mumkin.

Har bir blok kriptografik himoyalangan bo'lsa ham, umumiy tarmoq hali ham xavf ostida bo'lishi mumkin. Mutaxassislarining ta'kidlashicha, "buzilish" sodir bo'lgan taqdirda tajovuzkorlar ko'p sonli bloklarga kirish huquqiga ega bo'lishadi. Nazariy jihatdan, agar siz Blockchain tarmog'ining tasdiqlovchi resurslarining yarmidan ko'pini

olsangiz, buni amalga oshirish mumkin. Bunday holda, alohida bloklar zanjiri yaratiladi, bu asosiy bo'lib qoladi va eski bloklarning operatsiyalarini bekor qiladi. Ushbu muammoni hal qilish ko'p darajali xavfsizlik tizimi bo'lishi mumkin, ammo bu yondashuv yagona markaz va tartibga soluvchi organlarga ega bo'lmagan ishonchli makon bo'lgan Blockchainning asosiy printsipiga zid keladi. Bunday mulohazalar fonida Blockchain texnologiyasi zaruratga o'xshamaydi. U faqat ko'p sonli operatsiyalar va aktyorlar bilan sxemalarni amalga oshirish uchun ishlatilishi kerak. Agar tashkilot kichik ma'lumotlar bazasiga ega bo'lsa, Blockchainni qo'llashning hojati yo'q.

Blockchain texnologiyasining eng yaqqol va yaqqol ustunligi har qanday operatsiya yoki tranzaksiyalarni amalga oshirishda ko'plab "vositachilar"dan xalos bo'lishdir. Bu nafaqat jarayonni soddalashtirishi, balki uni arzonlashtirishi ham mumkin. Shu bilan birga, texnologiya alohida bloklar uchun ham, tarmoqning o'zi uchun ham etarli darajada xavfsizlikni ta'minlaydi, chunki u yagona markazga ega emas va tashqaridan boshqarilmaydi[3-4]. Kriptografik himoyaga ega bo'lgan har bir blokni faqat shaxsiy kalit taqdim etgandan keyin o'zgartirish mumkin, bu aslida moliyaviy qiymatdir. Blockchain-ning kamchiliklari orasida uni qonuniy aralashuv bilan bevosita bog'liq bo'lgan operatsiyalarda qo'llashning mumkin emasligini ta'kidlash mumkin. Bundan tashqari, hozirda Blockchain rivojlangan to'lov tizimlarining tranzaksiyalari sonini ta'minlay olmaydi.

Blockchain texnologiyasining asosiy xususiyatlari quyidagicha:

- **Tizim markazlashtirilmagan** - bunda hech qanday markaziy tashkilot tizimni boshqarmaydi va tizim ishlashi uchun u mavjud bo'lishi shart emas;

- **Tizimda ma'lumotlar shaffofligi** ta'minlangan va auditni amalga oshirish imkoniyati mavjud - tizimda u yaratilgandan buyon amalga oshirilgan har bir bitimning (tranzaksiyaning) to'liq nusxasi bloklar ketma-ketligi ko'rinishida saqlanadi va tizimning barcha ishtirokchilari uchun ochiq bo'ladi;

- **Tizimda ma'lumotlar taqsimlangan holatda saqlanadi** – tarmoqning har bir tugunida blockchain nusxasi saqlanadi bu esa ma'lumotlarga yagona tashkilotning egalik etishining oldini oladi;

- **Tizimda markazlashtirilmagan konsensus mavjud** - bitimlar markaziy tashkilot tomonidan emas, balki tarmoqning barcha tugunlari tomonidan tekshiriladi. Bu markazlashtirilgan konsensus paradigmasiga qaraganda ancha xavfsiz;

- **Tizim xavfsiz** – blockchain buzg'unchilardan himoyalangan va kiber jinoyatchilarning tizimni buzish imkoniyati deyarli nolga teng.

Blockchain dastlab moliyaviy operatsiyalarni ro'yxatga olish uchun ishlatilgandi, bunda barcha tranzaksiyalar shifrlanadi va barcha ishtirokchilar tomonidan saqlanadi (masalan, Bitcoin va boshqa kriptovalyuta tizimlarida). Shunday qilib, barcha operatsiyalar shaffof va har qanday o'zgartirishlarni osongina kuzatish va aniqlash

mumkin.

Blockchainning afzalliklari bu tranzaksiyalarning shaffofligi, shuningdek ko'plab tugunlarda bloklarning nusxalarining saqlashidadir, bu jarayonning barcha ishtirokchilariga sheriklarning harakatlari to'g'risida ma'lumot olish imkoniyatini beradi va tizimni ishonchli qiladi. Blockchainning bu imkoniyatlaridan bir-biriga ishonmaydigan tamonlar o'rtasida ishonchli tizimlarni yaratishda foydalanish mumkin[1].

Blockchain nafaqat biznesning barcha sohalariga, balki ta'lim sohasiga ham asta-sekin kiritilmoqda, chunki biznes va fan o'rtasidagi o'zaro ta'sir innovatsion mahsulotlar ishlab chiqarishga katta hissa qo'shadi. Raqamli iqtisodiyotning rivojlanishi bilimlar iqtisodiyotining rivojlanishi bilan uzviy bog'liqdir. Bilimlar iqtisodiyoti nomoddiy ishlab chiqarishga asoslanadi va o'sish bilim va bu bilimlarga ega bo'lgan odamlar tomonidan boshqariladi.

Biz blokcheynni qo'llashning mumkin bo'lgan sohalaridan faqat bittasini, ya'ni o'quv jarayonida foydalanishni ko'rib chiqamiz. Ushbu sohada ikkita o'zaro bog'liq vazifani taklif qilish mumkin[2-3]:

1. Ta'lim jarayonining ayrim tarkibiy qismlarining ishlashini avtomatlashtirish yoki samaradorligini oshirish uchun blokcheyn texnologiyasidan foydalanish.

2. Blokcheyn texnologiyasiga bag'ishlangan o'quv fanlari o'quv jarayoniga kirish.

Adabiyotlar ro'yxati:

1. Raval S. Detsentralizovannie prilozheniya. Texnologiya Blockchain v deystvii. – SPb.: Piter, 2017. – 240 s.
2. F.Zakirova va boshq. Elektron o'quv-metodik majmualar va ta'lim resurslarini yaratish metodikasi. Metodik qo'llanma, T.: OUMTV, 2010. - 57b
3. Blokcheyn nima (blokcheyn)va u nima uchun kerak? [Elektron resurs]
URL:<http://www.provest.com/2017/07/chtot-aloe-blockchain>
4. Blokcheyn texnologiyasi xavfsizligi: afsonalar va haqiqat [Elektron resurs]
<https://www.iemag.ru/analytics/detail.php?ID=38358>