BLOKCHAIN TEXNOLOGIYASI ASOSIDA TARMOQ XAVFSIZLIGINI TA'MINLASH

IBRAGIMOV SH.M., TILLAVOLDIYEVA S.X.
FarDU dotsenti, shavkat70@bk.ru,
FarDU talabasi, gulsoraxonyorbekova@gmail.com

Annotatsiya. Ushbu maqolada blokchain texnologiyasining zamonaviy kompyuter tarmoqlarida axborot xavfsizligini ta'minlashdagi roli va istiqbollari tahlil qilinadi. Blokchaynning markazlashmagan tuzilmasi, o'zgartirib bo'lmaydigan registr va konsensus mexanizmlari asosida tarmoq xavfsizligini ta'minlashdagi afzalliklari ko'rib chiqiladi. Shuningdek, texnologiyaning DDoS hujumlariga qarshi kurash, identifikatsiyani boshqarish va ma'lumotlar yaxlitligini saqlashdagi ahamiyati yoritiladi. Maqolada blokchain asosidagi xavfsizlik tizimlarining korporativ tarmoqlar, IoT va davlat axborot infratuzilmasida qo'llanilishi haqida ilmiy xulosalar berilgan.

Kalit so'zlar: Blokchain, tarmoq xavfsizligi, markazlashmagan tizim, konsensus mexanizmi, smart kontrakt, DDoS himoya, IoT xavfsizligi, axborot yaxlitligi, kriptografik xesh, PKI.

KIRISH. Raqamli texnologiyalarning tez sur'atlar bilan rivojlanishi va tarmoqqa ulangan qurilmalar sonining ortib borishi bilan birga, axborot xavfsizligi tahdidlari ham yangi darajaga ko'tarilmoqda. 2023-yil statistikasiga ko'ra, dunyo bo'ylab har kuni 2 000 dan ortiq kiberhujum qayd etiladi, yillik iqtisodiy zarari 8 trillion dollardan oshadi. Klassik markazlashgan xavfsizlik tizimlari esa yagona nosozlik nuqtasi (Single Point of Failure) muammosidan xoli emas. Blokchain texnologiyasi bu muammoga tubdan yangi — markazlashmagan, kriptografik jihatdan ishonchli va o'zgartirib bo'lmaydigan — yechim taklif qiladi.

Blokchain — bu ma'lumotlarni bir-biriga kriptografik zanjir orqali bog'langan bloklarda saqlaydigan, taqsimlangan va markazlashmagan registr texnologiyasidir. 2008-yilda Satoshi Nakamoto tomonidan Bitcoin kriptovalyutasi asosida taqdim etilgan ushbu texnologiya, keyinchalik axborot xavfsizligi, logistika, tibbiyot va davlat boshqaruvi sohalarida keng qo'llanila boshladi. Har bir blok oldingi blokning kriptografik xeshi (SHA-256), vaqt tamg'asi (timestamp) va tranzaksiya ma'lumotlarini o'z ichiga oladi. Bu tuzilma har qanday o'zgartirishni darhol fosh qiladi.

Dunyo miqyosida Ethereum, Hyperledger Fabric va IOTA kabi blokchain platformalari tarmoq xavfsizligi tizimlarida faol sinab ko'rilmoqda. AQShning

DARPA tashkiloti 2022-yilda blokchain asosidagi harbiy aloqa tarmoqi prototipini muvaffaqiyatli sinovdan o‘tkazdi. Xitoyda esa davlat axborot infratuzilmasini blokchayn yordamida himoyalash milliy strategiya sifatida belgilangan. O‘zbekistonda ham raqamli iqtisodiyot dasturlari doirasida blokchain texnologiyalarini joriy etish bo‘yicha bir qator loyihalar amalga oshirilmoqda.

Ushbu maqolaning asosiy maqsadi — blokchain texnologiyasining kompyuter tarmoqlari xavfsizligini ta’minlashdagi imkoniyatlarini tahlil qilish, uning afzalliklari va amaliy tatbiqlarini ko‘rganishdan iborat. Shuningdek, maqolada blokchain asosidagi xavfsizlik tizimlarining O‘zbekiston raqamli infratuzilmasidagi o‘rni va istiqbollari haqida fikr yuritiladi.

ASOSIY QISM. Blokchain texnologiyasining tuzilmasi va ishlash tamoyili: Blokchain tizimi uchta asosiy komponentdan tashkil topadi: bloklar zanjiri, taqsimlangan tugunlar tarmog‘i va konsensus mexanizmi. Har bir blok quyidagi ma’lumotlarni o‘z ichiga oladi: oldingi blokning SHA-256 xeshi, Unix-format vaqt tamg‘asi, Merkle daraxtida joylashtirilgan tranzaksiyalar va nonce (isbot ishlari uchun tasodifiy son). Biror blokdagi ma’lumotni o‘zgartirish uchun zanjirdagi barcha keyingi bloklarni qayta hisoblash kerak bo‘ladi - bu esa amalda imkonsiz hisoblanadi. Aynan shu xususiyat blokchain asosli tizimlarni ma’lumotlar yaxlitligini ta’minlashda eng ishonchli vosita qiladi.

Konsensus mexanizmlari - blokchain tizimining yuragi hisoblanadi. Eng keng tarqalgan mexanizmlar: Proof of Work (PoW) - hisoblash kuchi asosida blok yaratish (Bitcoin); Proof of Stake (PoS) - aktivlar ulushiga ko‘ra validatsiya (Ethereum 2.0); Practical Byzantine Fault Tolerance (PBFT) - korporativ blokchaynlarda tezkor konsensus (Hyperledger Fabric). Tarmoq xavfsizligi uchun PBFT va uning variantlari ayniqsa muhim, chunki ular tarmoqdagi tugunlarning 1/3 qismi buzilgan bo‘lsa ham to‘g‘ri ishlashda davom etadi.

Blokchain asosida tarmoq xavfsizligini ta’minlash usullari: Blokchayn tarmoq xavfsizligini ta’minlashning bir necha muhim yo‘nalishlarida qo‘llaniladi. Birinchidan, identifikatsiyani boshqarish (Identity Management): an’anaviy markazlashgan PKI

(Public Key Infrastructure) tizimida sertifikat markazi buzilsa, butun tizim xavf ostida qoladi. Blokchain asosidagi PKI esa sertifikatlarni taqsimlangan registrda saqlaydi, bu esa Man-in-the-Middle hujumlarini oldini oladi. MIT tadqiqotiga ko‘ra, blokchain-PKI an’anaviy tizimga nisbatan 60% samaraliroq hujumlarni aniqlaydi.

Blokchain tarmoq xavfsizligida quyidagi asosiy vazifalarni bajaradi:

- DDoS hujumlariga qarshi himoya: taqsimlangan tuzilma yagona hujum nuqtasini yo‘q qiladi;
- ma’lumotlar yaxlitligi: o‘zgartirishlar darhol aniqlanadi, audit izi saqlanadi;
- foydalanuvchi autentifikatsiyasi: markazlashmagan identifikatsiya tizimi;
- smart kontraktlar orqali avtomatik xavfsizlik qoidalarini qo‘llash;
- tarmoq jurnallarini (log) o‘zgartirib bo‘lmaydigan shaklda saqlash;
- IoT qurilmalar identifikatsiyasini boshqarish va ruxsatnomalarni nazorat qilish.

Mazkur imkoniyatlar sababli blokchain texnologiyasi zamonaviy SDN (Software-Defined Networking) va NFV (Network Functions Virtualization) tizimlari bilan ham samarali integratsiyalanmoqda.

DDoS hujumlariga qarshi blokchain asosidagi himoya: DDoS (Distributed Denial of Service) hujumlari zamonaviy tarmoqlarga eng katta tahdidlardan biri hisoblanadi. 2023-yilda qayd etilgan eng kuchli DDoS hujumi 3,47 Tbps tezlikda amalga oshirildi. An’anaviy himoya tizimlari markazlashgan filtr serverlariga tayanadi, bu esa ularning o‘zini hujum nishoniga aylantirib qo‘yadi. Blokchain asosidagi himoya tizimida esa har bir tarmoq tugunida mustaqil filtr ishlaydi: shubhali trafik bloklarda qayd etiladi, konsensus mexanizmi orqali tasdiqlanadi va butun tarmoq bo‘ylab ulashiladi.

Amaliy misol: Cloudflare kompaniyasi 2022-yilda blokchain asosidagi IPFS (InterPlanetary File System) texnologiyasidan foydalanib, DDoS hujumlariga chidamli veb-xizmat modelini muvaffaqiyatli sinab ko‘rdi. Cisco tadqiqotiga ko‘ra, blokchain asosidagi IoT xavfsizlik tizimlari an’anaviy usulga nisbatan hujumlarni aniqlashda 40% tezroq va 35% arzonroq ishlaydi.

Xavfsizlik va ishonchlilik: Smart kontraktlar - bu blokchain tarmog‘ida avtomatik bajariladigan dasturiy kodlar bo‘lib, tarmoq xavfsizligi qoidalarini odam aralashuviga ehtiyoj sezmasdan qo‘llash imkonini beradi. Masalan, tarmoq qurilmasi ruxsatsiz kirish urinishini aniqlaganda, smart kontrakt avtomatik ravishda: hujum manbaini bloklaydi; voqeani o‘zgartirib bo‘lmaydigan jurnalga yozadi; tarmoq administratorlariga xabar yuboradi; zaxira marshrutni faollashtiradi. Hyperledger Fabric platformasida amalga oshirilgan bunday tizimlar korporativ tarmoqlarda xavfsizlik hodisalariga munosabat vaqtini 70% gacha qisqartirgan.

Blokchain asosida IoT tarmoq xavfsizligi: Internet of Things (IoT) qurilmalari soni 2025-yilda 75 milliardga yetishi prognoz qilinmoqda. Bu qurilmalarning aksariyati cheklangan hisoblash resurslari va zaif kriptografik himoyaga ega. Blokchain texnologiyasi IoT xavfsizligida quyidagi muammolarni hal etadi: qurilma autentifikatsiyasi - har bir IoT qurilma o‘zining kriptografik identifikatoriga ega bo‘ladi; ma’lumotlar yaxlitligi - sensor ma’lumotlari blokchaynga yozilgach, o‘zgartirib bo‘lmaydi; ruxsatlarni boshqarish - smart kontraktlar qurilmalar o‘rtasidagi muloqotni nazorat qiladi. Samsung va IBM birgalikda ishlab chiqqan ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry) platformasi ushbu yondashuvning tijorat tatbiqiga yorqin misoldir.

Sog‘liqni saqlash sohasida blokchain bemor ma’lumotlarini himoyalash va tibbiy qurilmalar tarmoq xavfsizligini ta’minlashda qo‘llanilmoqda. MedRec platformasi (MIT ishlanmasi) blokchain yordamida tibbiy yozuvlar ulashishni xavfsiz va audit izli qiladi. Moliya sohasida SWIFT tarmog‘i blokchain texnologiyasini tranzaksiyalar xavfsizligini kuchaytirish uchun sinovdan o‘tkazmoqda. O‘zbekistonda esa O‘zbekiston Respublikasi Markaziy banki va UZINFOCOM blokchain asosidagi xavfsizlik tizimlarini davlat reyestrlari va moliyaviy tarmoqlarida qo‘llash bo‘yicha dastlabki loyihalarni amalga oshirmoqda.

XULOSA. Bugungi kunda kibertahdidlarning murakkablashib borishi tarmoq xavfsizligida yangi va ishonchli texnologiyalarni qo‘llash zaruratini yuzaga keltirmoqda. Blokchain texnologiyasi ana shunday zamonaviy yechimlardan biri

bo‘lib, u markazlashmagan tuzilmasi, kriptografik xesh zanjiri va smart kontraktlar orqali tarmoq xavfsizligini tubdan yangi darajaga ko‘tarish imkonini beradi.

Maqola davomida blokchain tuzilmasi va konsensus mexanizmlari, DDoS hujumlariga qarshi himoya usullari, smart kontraktlar orqali xavfsizlikni avtomatlashtirish, IoT tarmoq himoyasi va amaliy tatbiq holatlari tahlil qilindi. Tadqiqot natijalariga ko‘ra, blokchain asosidagi xavfsizlik tizimlari an’anaviy usullarga nisbatan hujumlarni aniqlashda sezilarli darajada samarali va ma’lumotlar yaxlitligini ta’minlashda ishonchlidir.

Shuningdek, blokchain texnologiyasi SDN va NFV tizimlari bilan integratsiyalanib, zamonaviy raqamli infratuzilmalarning xavfsizligini ta’minlashda muhim o‘rin tutadi. Ayniqsa IoT, moliya va sog‘liqni saqlash sohalarida blokchain asosidagi himoya tizimlari yuqori samaradorlikni ta’minlamoqda. O‘zbekiston uchun esa raqamli transformatsiya jarayonida blokchain texnologiyasini milliy tarmoq xavfsizligi tizimiga integratsiyalash dolzarb va istiqbolli yo‘nalish hisoblanadi.

FOYDALANILGAN ADABIYOTLAR

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. - URL: https://bitcoin.org/bitcoin.pdf
2. Buterin V. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2013. URL: https://ethereum.org/whitepaper
3. Dorri A., Kanhere S., Jurdak R. Blockchain in Internet of Things: Challenges and Solutions. IEEE Access. 2017. Vol. 5. P. 44257-44268.
4. Hyperledger Foundation. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. RFC 3031, IETF, 2001.
5. Meng W., Li W., Kwok L. F. Enhancing the Security of Blockchain-Based Software Defined Networking. Cisco Press, 2015.
6. IEEE Access. - 2018. - Vol. 6. - P. 10659-10672. O‘Reilly Media, 2017.
7. Novo O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. IEEE Internet of Things Journal. - 2018. - Vol. 5. - No. 2. - P. 1184-1195.
8. Ali M.S. et al. Applications of Blockchains in the Internet of Things: A Comprehensive Survey. IEEE Communications Surveys Tutorials. - 2019. -Vol. 21. - No. 2. - P. 1676-1717.
9. Cisco Annual Internet Report 2020-2025. Cisco Systems, Inc. - 2020. Pearson, 5th Edition, 2011.
10. O‘zbekiston Respublikasi Prezidentining 2020-yil 28-apreldagi “Raqamli O‘zbekiston - 2030” Strategiyasi haqidagi farmoni. Cisco Press, 2021.