BLOKCHEYN TIZIMIDA «51% HUJUM» XAVFI VA UNI BARTARAF ETISH CHORA-TADBIRLARI

Umarov Sh.A.

FarDTU dotsenti, sh.umarov81@mail.ru

Annotatsiya. Ushbu maqolada blokcheyn texnologiyasida yuzaga kelishi mumkin bo‘lgan 51% hujumlar va ularning bir nechta turi tahlil qilingan. Shuningdek, maqolada 51% hujumning mohiyati, uning amalga oshirilish mexanizmi va blokcheyn tizimlari uchun xavfi hamda bunga qarshi kurash usullari yoritilgan. Hujumlarning iqtisodiy va texnologik oqibatlari, matematik modellari, hamda ilg‘or himoya choralari bayon qilingan.

Kalit so‘zlar: 51% hujum, blokcheyn, kriptovalyuta, xavfsizlik, konsensus, PoW, double spending.

KIRISH

Blokcheyn bu raqamli ma’lumotlarni tarmoqdagi barcha ishtirokchilar o‘rtasida taqsimlangan, o‘zgarmas va kriptografik jihatdan himoyalangan reestr bo‘lib, ma’lumotlar “bloklar” shaklida izchil ravishda saqlanadi va har bir blok oldingi blokga bog‘langan holda tashkil etiladi [1]. Blokcheyn – ma’lumotlarni tarqoq tarzda saqlash va o‘zgartirmasdan qayd etishga mo‘ljallangan tizimdir. U markazlashmaganligi, shaffofligi va xavfsizligi bilan ajralib turadi. Blokcheynning ishlash asosi – konsensus algoritmi bo‘lib, u orqali tarmoq ishtirokchilari qanday blok haqiqiy ekanligini belgilaydi [2].

Blokcheynning asosiy xususiyatlari quyidagilar:

– ma’lumotlar xesh (hash) funksiyalari orqali shifrlanadi.

– markaziy server mavjud emas, har bir foydalanuvchida to‘liq yozuvlar nusxasi mavjud bo‘ladi.

– bir marta kiritilgan ma’lumotni keyinchalik o‘zgartirish yoki o‘chirish mumkin emas, ya’ni immutability.

– barcha ishtirokchilar ma’lumotlar tranzaksiyalarini tekshirishi mumkin.

Demak, blokcheyn axborot xavfsizligini ta’minlashda yangi bosqich bo‘lib, yaxlitlik, ishonch, oshkoralik va tahdidlarga bardoshlilikni ta’minlaydi. U axborotning soxtalashtirilishini, o‘chirilishini va noqonuniy o‘zgartirishni imkonsiz qiladi [3].

MATERIALLAR VA USULLAR

Tranzaksiyalarni amalga oshirishda eng keng tarqalgan konsensus usuli (Proof-of-Work) bo‘lib, maynerlar murakkab matematik masalalarni yechish orqali yangi blok yaratish huquqini oladi. Biroq, agar bir guruh yoki shaxs tarmoq xesh-quvvatining 50% dan ortig‘iga ega bo‘lsa, ular butun tarmoqni manipulyatsiya qilishi mumkin. Bu holat 51% hujum deb nomlanadi [4]. 51% hujum bu blokcheyn tarmog‘idagi hisoblash resurslarining 51% yoki undan ortig‘iga egalik qilish orqali tranzaksiyalarni noqonuniy o‘zgartirish, ikki marta xarajat qilish (double spending), yangilanishlarni bloklash yoki to‘sish imkonini beruvchi xatarli kiberhujum turidir [5]. 51% hujum blokcheyn tizimlarining mustaqillik va ishonchlilik tamoyillariga bevosita tahdid soladi. Bu turdagi hujumlar natijasida blokcheyn foydalanuvchilari o‘z mablag‘larini yo‘qotishi yoki tizimga ishonchni yo‘qotishi mumkin. Shu bois, kriptovalyuta tizimlarini loyihalashda va himoya qilishda bu xavf turini hisobga olish talab qilinadi. Tarmoqning xavfsizligi foydalanuvchilar o‘rtasidagi tarqoqlik va xesh quvvatning ko‘pchilik tomondan boshqarilishiga bog‘liq. Proof-of-Work tizimida har bir mayner blok yaratish imkoniyatiga o‘z xesh-quvvatiga mutanosib ravishda ega bo‘ladi. Agar maynerlardan biri yoki pul birlashmasi 50%+1 xesh quvvatga ega bo‘lsa, u haqiqiy tranzaksiyalarni bekor qilishi, o‘zining kriptovalyutasini ikki marta almashishi, boshqa maynerlarni bloklashi mumkin [6].

Agar hujumchi hisoblash quvvatining haqiqiy tarmoq quvvatidagi ulushiga ega bo‘lsa, u holda uning hujumda muvaffaqiyat qozonish ehtimoli quyidagicha hisoblanadi:

$$p = 1 - q\ ,$$

bu yerda p - hujumchining xesh quvvati.

Hujum muvaffaqiyatli bo‘lish ehtimoli

$$P = \begin{cases} 1, & agar\ \ q > p, \\ \left(\frac{q}{p}\right)^k, & agar\ \ q < p \end{cases}$$

ifoda bilan hisoblanadi, bu yerda k -o‘tkazib yuborilgan bloklar soni.

MUHOKAMA VA NATIJALAR

51% hujum natijasida Double Spending xavfi paydo bo‘ladi, ya’ni bir kriptovalyuta ikki marta xarajat qilinadi. Double Spending jarayonida bir xil kriptovalyutani yoki raqamli aktivni ikki yoki undan ortiq tranzaksiyada, go‘yoki u har safar alohida boshqa puldek, bir nechta qabul qiluvchilarga bir vaqtda yuborishga urinish yuzaga keladi. Ikki marta xarajat qilishda sotuvchi mahsulotni jo‘natadi, lekin haqiqiy to‘lov amalga oshmagan bo‘ladi. Bu esa kriptovalyuta tizimi va uning barqarorligiga nisbatan ishonchni pasaytiradi. Asosiy blokcheyndan chetlashish orqali butun tarmoqda nizo kelib chiqishi mumkin [8]. Shu sababli kriptovalyuta tizimida quyidagi himoya choralarini ko‘rish tavsiya qilinadi**:**

1. Ko‘plab tasdiqlar orqali to‘lovni qabul qilish, masalan, kamida 6 blok tasdig‘i maqsadga muvofiq.
2. Tezda tranzaksiyani qabul qilmaslik, tezkor to‘lovlarni ehtiyotkorlik bilan tekshirib chiqish.
3. Kuchli konsensus algoritmlaridan foydalanish, ya’ni PoW, PoS va ularning gibridlari.
4. Tarmoqdagi hisoblash quvvatini markazlashmagan holda taqsimlash.

Shuning Selfish Mining hujum turi paydo bo‘lishi ham mumkin bo‘ladi. Selfish Mining - shaxs yoki maynerlar guruhi tomonidan amalga oshiriladigan hujum turi bo‘lib, ular yangi bloklarni darhol tarmoqqa e’lon qilmasdan, yashirin holda saqlash orqali boshqa maynerlarni aldab, o‘z bloklarini ustun qilib qiladilar va shu orqali tarmoqdagi kriptovalyuta mukofotlarini ko‘proq olishadi. Selfish Mining blokcheyn tarmog‘idagi adolat, ishonch va samaradorlik prinsiplariga zid bo‘lib, kriptovalyuta tizimining xavfsizligiga, ishonchliligiga va barqarorligiga jiddiy zarar yetkazishi mumkin. Shu sababli, kichik maynerlarni qo‘llab-quvvatlash va ularni markazlashmagan holda ishlashiga sharoit yaratish, Yangi konsensus algoritmlarini joriy qilish, masalan, GHOST (Greedy Heaviest Observed Subtree) algoritmi, tarmoqdagi maynerlar faoliyatini kuzatib va tahlil qilib borish, shubhali faol maynerlarni aniqlash kerak bo‘ladi.

51% hujumda Censorship hujum ham paydo bo‘ladi. Censorship - blokcheyn tarmog‘ida maynerlar tomonidan aniq bir manzil yoki tranzaksiyani qasddan qabul qilmaslik, ya’ni tarmoqqa kiritmaslik amaliyotidir. Bunda boshqa maynerlar ham ushbu tranzaksiyani shubhali deb, uni blokka qo‘shishdan bosh tortadi. Natijada tranzaksiya "cheklanadi", ya’ni tarmoqdan o‘tishi mumkin emas. Katta maynerlar istalgan manzilni to‘sishi orqali nazoratni qo‘lga olishi mumkin. Oxir-oqibat senzuralangan tranzaksiyalar uzoq vaqt tarmoqda “ochiq” holda qoladi. Censorship blokcheynning ochiqlik, senzurasizlik va to‘liq ishtirok tamoyillariga xilof holat bo‘lib, bu xavf blokcheynning ishonchli va adolatli tizim sifatida faoliyat yuritishiga salbiy ta’sir qiladi. Shu sababli, ba’zi choralarni ko‘rish tavsiya qilinadi:

- Miner Extractable Value (MEV) nazorati;
- Tranzaksiyalarni qayta uzatish (rebroadcasting);
- Privacy-kriptografiya, masalan ZK-texnologiyadan foydalanish.

Yana shuningdek, 51% hujumda Chain Reorganization hujum paydo bo‘ladi. Chain Reorganization blokcheyn tarmog‘ida avvaldan mavjud bo‘lgan bloklar zanjirini ma’lum miqdorda bekor qilib, uni yangi, uzunroq va yaroqli zanjir bilan almashtirish jarayonidir. Ya’ni tarmoqda ikki xil blokcheyn zanjiri vujudga keladi, masalan hujumchi yashirincha o‘z blokcheyn zanjirini quradi. Hujumchining blokcheyn zanjiri uzunroq bo‘lsa, tarmoq uni asosiy deb qabul qiladi. Ilgarigi asosiy bo‘lgan blokcheyn zanjiridagi bloklar va tranzaksiyalar bekor qilinadi. Demak, tarmoqda ikki marta xarajat qilish (Double Spending) imkoni paydo bo‘ladi. Oldin amalga oshirilgan to‘lovlar “yo‘q” deb hisoblanadi.

Bunda ham Double Spending hujumidagi himoya choralarini ko‘rish tavsiya qilinadi. Bu jarayon oddiy holatlarda ham texnik jihatdan ro‘y berishi mumkin, lekin qasddan amalga oshirilsa, u holda bu kiberhujum sifatida baholanadi .

Eng muhimi, 51% hujumda hujumchi quyidagilarni qila olmaydi:

- Ular tarmoq qoidalarini o‘zgartira olmaydi yoki boshqalarning xususiy kalitlariga kira olmaydi, mablag‘larini o‘g‘irlay olmaydi.

- Ular blokcheyn protokolini o‘zgartira olmaydi va belgilangan umumiy tangalar sonidan tashqari yangilarini yarata olmaydi.
- Ular blokcheynga oldindan qo‘shilgan juda eski bloklarni o‘zgartira olmaydi, chunki bu juda ko‘p hisoblash quvvatini talab qiladi va avvalgi tranzaksiya tarixini qayta yozish juda qiyin masala hisoblanadi.

Umuman olganda 51% hujumdan himoyalanish uchun PoW o‘rniga PoS va hybrid konsensus joriy etish, xesh quvvatini markazlashtirmaslik, Chain finalityni joriy etish, Fork-deteksiya algoritmlaridan foydalanish, tarmoqni to‘liq monitoringi va real-time alert tizimlarini qo‘llash tavsiya qilinadi.

51% hujum ehtimolini hisoblashda Markov zanjiri modeli qo‘llaniladi. Agar hujumchi xesh quvvatining p qismga ega bo‘lsa, u n blok orqali ishonchli zanjirni orqaga qaytarishi ehtimoli:

$$P = 1 - \sum_{k=0}^{n} \frac{\lambda^k \cdot e^{-\lambda}}{k!}, \quad \lambda = n \cdot \frac{q}{p}, \quad p > q,$$

bu yerda p - hujumchining xesh quvvati, q - tarmoq qoldig‘i. $p > 0{,}5$ bo‘lsa, ehtimol katta bo‘ladi.

XULOSA

51% hujumlar faqat texnik muammo emas, balki iqtisodiy va huquqiy xavf hamdir. Shu sababli, foydalanuvchilar xavf to‘g‘risida xabardor qilinishi, hukumatlar tomonidan standartlar joriy etilishi, detsentralizovan tarmoqlar uchun turli qonunlar ishlab chiqilishi lozim. 51% hujum blokcheyn tizimlari uchun jiddiy tahdid bo‘lib, ayniqsa PoW asosida ishlovchi kriptovalyutalar uchun xavflidir. Bunday hujumlardan himoyalanish uchun tizimlar konsensus mexanizmlarini diversifikatsiya qilishi, monitoring va tahlil instrumentlarini joriy etishi zarur. Hybrid va energy-efficient algoritmlarni qo‘llash 51% hujum xavfini kamaytirishi sababli kelajakda ulardan foydalanish maqsadga muvofiqdir.

FOYDALANILGAN ADABIYOTLAR

1. Петренко, А. (2023). Квантово-устойчивый блокчейн. Питер.

2. Вилаков, Н. В., & Бочаров, М. И. (2025). Способы защиты криптовалютных блокчейн систем и систематизация угроз. Системная инженерия и информационные технологии, 7(2 (21)), 143-154.

3. Lin, Z. (2024). Comparative Analysis of Blockchain Consensus. In Proceedings of the 2024 2nd International Conference on Image, Algorithms and Artificial Intelligence (Vol. 115, p. 264). Springer Nature.

4. Титжинський, А. А. (2024). Порівняльний аналіз консенсусних алгоритмів у контекстіїхньої стійкості до атак. Матеріали XII науково-технічної конференції „Інформаційні моделі, системи та технології“, 96-96.

5. Babur, S. M., Khan, S. U. R., Yang, J., Chen, Y. L., Ku, C. S., & Por, L. Y. (2024). Preventing 51% Attack by Using Consecutive Block Limits in Bitcoin. IEEE Access.

6. Azizjonovich, U. S. (2023). KRIPTOBARDOSHLI KRIPTOGRAFIK TIZIMLAR VA ULARNING KLASSIFIKATSIYASI. Al-Farg'oniy avlodlari, 1(4), 15-21.

7. Santhosh, A., & Subramanian, N. (2024, April). Classify Attacks Based on Blockchain Components. In 2024 12th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.

8. Umarov, S. A., & Umarova, M. I. (2025). THE NEED AND IMPORTANCE OF USING ANTIVIRAL DEFENSE SYSTEMS BASED ON ARTIFICIAL IMMUNE SYSTEMS. Miasto Przyszłości, 61, 543-548.