BLOCKCHAIN TEXNOLOGIYASI VA UNING KIBERXAVFSIZLIKDAGI O'RNI

Hasanova Ozodaxon Yuldosh qizi
Qarshi davlat universiteti talabasi
E-mail:khasanovaozoda213@gmail.com

Annotatsiya: *Ushbu maqolada blockchain texnologiyasining kiberxavfsizlik sohasidagi roli va imkoniyatlari ilmiy jihatdan tahlil qilinadi. Markazlashmagan tuzilma, kriptografik himoya va o'zgarmaslik xususiyatlariga ega bo'lgan blockchain texnologiyasining an'anaviy xavfsizlik tizimlaridan ustunliklari ko'rsatiladi. Ma'lumotlar yaxlitligini ta'minlash, shaxsiy identifikatsiyani himoyalash, IoT qurilmalar xavfsizligi va kibervoqealar jurnalini yuritish kabi muhim yo'nalishlarda blockchain qo'llanishining samaradorligi asoslab beriladi. Shuningdek, texnologiyaning hozirgi cheklovlari va kelajak istiqbollari ham ko'rib chiqiladi.*

Kalit so'zlar: *blockchain texnologiyasi, kiberxavfsizlik, taqsimlangan reyestr, kriptografik himoya, markazlashmagan identifikatsiya, ma'lumotlar yaxlitligi, IoT xavfsizligi, axborot xavfsizligi, distributed ledger technology, cybersecurity.*

Abstract: *This article provides a scientific analysis of the role and potential of blockchain technology in the field of cybersecurity. It highlights the advantages of blockchain technology–characterized by its decentralized structure, cryptographic protection, and immutability–over traditional security systems. The effectiveness of blockchain application is substantiated in key areas such as ensuring data integrity, protecting personal identification, securing IoT devices, and maintaining cyber-event logs. Additionally, the current limitations and future prospects of the technology are examined.*

Keywords: *blockchain technology, cybersecurity, distributed ledger, cryptographic protection, decentralized identification, data integrity, IoT security, information security, distributed ledger technology (DLT)*

Аннотация: *В данной статье научно анализируется роль и возможности технологии блокчейн в сфере кибербезопасности. Рассматриваются преимущества технологии блокчейн, обладающей такими характеристиками, как децентрализованная структура, криптографическая защита и неизменяемость, перед традиционными системами безопасности. Обосновывается эффективность использования блокчейна в таких критических направлениях, как обеспечение целостности данных, защита персональной идентификации, безопасность устройств IoT и ведение журналов киберсобытий. Также рассматриваются текущие ограничения и будущие перспективы технологии.*

Ключевые слова: *технология блокчейн, кибербезопасность, распределенный реестр, криптографическая защита, децентрализованная идентификация, целостность данных, безопасность IoT, информационная безопасность, технология распределенного реестра (DLT).*

Kirish. Zamonaviy raqamli dunyoda axborot xavfsizligi tobora muhim ahamiyat kasb etmoqda. Kiberhujumlar, ma’lumotlar sizib chiqishi va raqamli firibgarlik kabi tahdidlar tashkilotlar, davlatlar va oddiy foydalanuvchilar uchun jiddiy muammo bo’lib qolmoqda. 2023-yilgi global kiberxavfsizlik hisobotlariga ko’ra, yiliga 8 trillion AQSh dollaridan ortiq zarar ko’rilmoqda. Aynan shu vaziyatda blockchain texnologiyasi yangi va ishonchli yechim sifatida e’tiborni tortmoqda.

Blockchain – dastlab 2008-yilda Satoshi Nakamoto tomonidan Bitcoin kriptovalyutasi uchun yaratilgan texnologiya. Biroq keyingi o’n yillikda u moliya, sog’liqni saqlash, davlat boshqaruvi va kiberxavfsizlik kabi sohalarda inqilobiy o’zgarishlar olib kelmoqda . Ushbu maqolaning maqsadi blockchain texnologiyasining kiberxavfsizlikdagi o’rnini ilmiy jihatdan tahlil etish va uning amaliy imkoniyatlarini asoslab berishdan iborat.

Blockchain – bu ma’lumotlarni bloklarga yozib, ularni kriptografik zanjir shaklida bog’laydigan taqsimlangan reyestr texnologiyasidir (Distributed Ledger Technology – DLT). Har bir blok quyidagi elementlardan tashkil topadi :

– Ma’lumotlar (Data) – tranzaksiyalar yoki boshqa yozuvlar;

– Xesh (Hash) – blokning kriptografik identifikatori (SHA-256 algoritmi);

– Oldingi blokning xeshi –zanjirni bog’lovchi muhim element;

– Vaqt tamg’asi (Timestamp) – blok yaratilgan vaqt.

Texnologiyaning asosiy xususiyatlari quyidagilardan iborat:

– Markazlashmagan tuzilma – ma’lumotlar bitta serverda emas, minglab tugunlarda saqlanadi;

– O’zgarmaslik (Immutability) – yozilgan ma’lumotni o’zgartirish yoki o’chirish imkonsiz;

– Shaffoflik – tarmoqdagi barcha ishtirokchilar operatsiyalarni ko’rishi mumkin;

– Konsensus mexanizmi – tarmoq a’zolari kelishuvi asosida ishlaydi (PoW, PoS va boshqalar).

Bugungi kunda kiberxavfsizlik sohasida bir qator dolzarb muammolar mavjud bo’lib, ular tashkilotlar va davlatlar uchun jiddiy xavf tug’dirmoqda. Asosiy tahdidlar quyidagilardan iborat :

1. DDoS hujumlari – serverlarni ortiqcha so’rovlar bilan ishdan chiqarish;
2. Ma’lumotlar sizib chiqishi – shaxsiy va korporativ ma’lumotlarning o’g’irlanishi;
3. Identifikatsiya soxtalashtirish – foydalanuvchi kimligini qalbakilashtirish;
4. Zanjir ta’minoti hujumlari (Supply Chain Attacks) – dasturiy ta’minot orqali kirib olish;
5. Markazlashgan tizimlarning zaif nuqtalari – bitta server buzilsa, butun tizim xavf ostida.

An’anaviy tizimda foydalanuvchi ma’lumotlari bitta markaziy bazada saqlanadi va bu esa xakerlar uchun maqsadli nishon bo’ladi. Blockchain asosidagi o’z-o’zini boshqaruvchi identifikatsiya (Self-Sovereign Identity – SSI) tizimida foydalanuvchi o’z shaxsiy ma’lumotlarini o’zi nazorat qiladi. Markaziy server mavjud bo’lmagani uchun, uni buzish ham imkonsizlashadi. Microsoft va Sovrin Foundation kabi tashkilotlar SSI tizimlarini muvaffaqiyatli sinab ko’rgan.

Blockchainда har bir ma’lumot bloki oldingi blokning kriptografik xeshini o’z ichiga oladi. Agar kimdir ma’lumotni o’zgartirishga urinsa, butun zanjir o’zgaradi va bu darhol aniqlanadi. Bu xususiyat ayniqsa tibbiyot, moliya va davlat arxivlari uchun juda muhim hisoblanadi. Tadqiqotlarga ko’ra, blockchain asosidagi tizimlar ma’lumotlar buzilishini aniqlashda 99,9% aniqlikka erishmoqda.

An’anaviy ochiq kalit infratuzilmasida (PKI) sertifikat markazlari (Certificate Authority – CA) buzilsa, minglab foydalanuvchilar xavf ostiga tushadi. Blockchain asosidagi PKI esa sertifikatlarni taqsimlangan tarzda saqlaydi va bu yagona zaif nuqtani yo’q qiladi. MIT tadqiqotchilari tomonidan ishlab chiqilgan Certcoin tizimi blockchain orqali PKI muammosini hal etishning samarali namunasidir .

2025-yilga kelib dunyo bo’ylab 75 milliarddan ortiq IoT qurilmasi ishlamoqda. Markaziy server orqali boshqariladigan bunday qurilmalar katta xavf tug’diradi. Blockchain esa qurilmalar o’rtasida to’g’ridan-to’g’ri, ishonchli va himoyalangan aloqa o’rnatishga imkon beradi. Samsung ARTIK va IBM Watson IoT kabi yirik platformalar bu yondashuvni amalda qo’llaydi.

Blockchain’ning o’zgarmaslik xususiyati uni audit log (xavfsizlik jurnali) sifatida ideallashtiradi. Kiberhujum sodir bo’lganda, tergov jarayonida blockchain’dagi yozuvlar buzilmagan holda saqlanishi tekshiruvchilar uchun ishonchli dalil bo’la oladi. Bu xususiyat ayniqsa raqamli jinoyatchilikka qarshi kurashda muhim ahamiyatga ega .

1-jadval. Blockchain yondashuvlarining kiberxavfsizlikdagi taqqoslanishi

Yondashuv	Xususiyatlari	Afzalliklari	Kamchiliklari
Markazlashmagan identifikatsiya (SSI)	Foydalanuvchi o'z ma'lumotlarini nazorat qiladi	Markaziy zaif nuqta yo'q, xakerlik qiyin	Kalitni yo'qotish xavfi
Ma'lumotlar yaxlitligi	Kriptografik xesh bilan himoya	O'zgartirishlarni darhol aniqlash	Katta hajmda sekinlashish
PKI (Ochiq kalit infratuzilmasi)	Sertifikatlar taqsimlangan tarzda saqlanadi	Yagona markaziy nuqta bartaraf etiladi	Murakkab boshqaruv
IoT xavfsizligi	Qurilmalar orasida to'g'ridan-to'g'ri aloqa	Real vaqt monitoring, kuchaytirish oson	Qurilma resurslari cheklangan
Kibervoqea jurnali	O'zgarmas audit log	Sud dalili sifatida ishlatish mumkin	Saqlash hajmi katta

Blockchain kiberxavfsizlik uchun kuchli vosita bo'lsa-da, uning ba'zi cheklovlari ham mavjud bo'lib, ularni hisobga olmaslik noto'g'ri xulosalarga olib keladi :

– Masshtablilik muammosi – katta hajmdagi ma'lumotlarni qayta ishlashda sekinlashish kuzatiladi (Bitcoin tarmog'i sekundiga atigi 7 tranzaksiyani qayta ishlaydi);

– 51% hujumi – agar biror tashkilot tarmoqning 51% nazoratini qo'lga kiritsa, ma'lumotlarni o'zgartirishi mumkin;

– Xususiy kalitni yo'qotish – foydalanuvchi o'z kalitini yo'qotsa, ma'lumotlarga kirish butunlay mumkin bo'lmay qoladi;

– Energiya sarfi – Proof-of-Work konsensus mexanizmi juda ko'p energiya sarflaydi;

– Qonuniy tartibga solish – ko’pgina mamlakatlarda blockchain asosidagi tizimlarning huquqiy maqomi hali aniq emas.

Mutaxassislar blockchain va kiberxavfsizlik integratsiyasining kelajagi yorqin ekanligini ta’kidlamoqda. Bir qator istiqbolli yo’nalishlar mavjud :

– Zero-Knowledge Proof (ZKP) – foydalanuvchi ma’lumotlarini oshkor qilmasdan autentifikatsiya imkonini beruvchi texnologiya;

– Kvant kriptografiyasi bilan integratsiya – kvant kompyuterlariga chidamli blockchain tizimlari yaratish;

– Web3 va desentralizatsiyalashgan internet – foydalanuvchilar uchun to’liq ma’lumot huquqi;

– Smart kontraktlar orqali avtomatlashtirilgan xavfsizlik protokollari;

– Davlat boshqaruvida blockchain asosidagi elektron ovoz berish tizimlari.

O’zbekiston Respublikasida ham raqamli iqtisodiyotni rivojlantirish strategiyasi doirasida blockchain texnologiyalarini qo’llash bo’yicha bir qator tashabbuslarda qadamlar qo’yilmoqda. Bu esa mamlakatimizdagi axborot xavfsizligini yangi darajaga olib chiqish imkonini beradi.

Xulosa. Ushbu maqolada blockchain texnologiyasining kiberxavfsizlik sohasidagi roli va imkoniyatlari ilmiy jihatdan tahlil qilindi. Olib borilgan tadqiqot natijasida quyidagi xulosalarga kelindi:

Blockchain texnologiyasi markazlashmagan tuzilmasi, kriptografik himoyasi va o’zgarmaslik xususiyatlari tufayli an’anaviy xavfsizlik tizimlaridan tubdan farq qiladi;

Markazlashmagan identifikatsiya, PKI xavfsizligi, IoT himoyasi va audit log kabi sohalarda blockchain samarali vosita bo’la oladi;

Masshtablilik, energiya sarfi va 51% hujumi kabi muammolar hal etilishi lozim;

Kvant kriptografiyasi va ZKP bilan integratsiya texnologiyaning kelajakdagi rivojlanish yo’nalishlarini belgilab beradi.

Xulosa qilib aytganda, to’g’ri qo’llanilganda blockchain texnologiyasi raqamli dunyoning xavfsizligini yangi darajaga olib chiqishi shubhasiz. Kelgusi tadqiqotlarda amaliy tizimlar ishlab chiqish va O’zbekiston sharoitida qo’llash imkoniyatlarini o’rganish maqsadga muvofiqdir.

FOYDALANILGAN ADABIYOTLAR

1. Cybersecurity Ventures. (2023). Cybercrime Report 2023. Cybersecurity Ventures Publishing. – 48 b.
2. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. – 9 b.
3. Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution. Penguin Random House. – 324 b.
4. ENISA. (2022). Threat Landscape Report. European Union Agency for Cybersecurity. – 112 b.
5. IBM Security. (2022). Cost of a Data Breach Report 2022. IBM Corporation. – 56 b.
6. Allen, C. et al. (2016). The Path to Self-Sovereign Identity. Life with Alacrity Blog. – 12 b.
7. Azaria, A., et al. (2016). MedRec: Using Blockchain for Medical Data Access. IEEE DSNW. – 6 b.
8. Saidova D. Teaching Programming Collaboratively Through Google Colab AND Github Integration //Green Economy and Development. – Т. 3. – №. 11. – С. 667884.
9. Saidova D. E. Analysis of the problems of the teaching object-oriented programming to students //International Journal of Social Science Research and Review. – 2022. – Т. 5. – №. 6. – С. 229-234.