BLOKCHEYNDA MA'LUMOTLARNI XESHLASH MEXANIZMLARI: NAZARIY ASOSLAR, ALGORITMLAR ARXITEKTURASI VA XAVFSIZLIK TAHLILI

Raimov Ulug'bek Yorqinbek o'g'li
Teacher at Andijan State Technical Institute
E-mail: uraimov0111@gmail.com
ORCID: 0009-0009-9304-5980

Annotatsiya. Ushbu tadqiqot blokcheyn texnologiyasining fundamental komponenti bo'lgan ma'lumotlarni xeshlash mexanizmlarining nazariy asoslari, texnik arxitekturasi va xavfsizlik jihatlarini chuqur ilmiy tahlil qilishga bag'ishlanadi. Maqolada kriptografik xesh funksiyalarining pre-image resistance, second pre-image resistance, collision resistance va avalanche effect kabi mustahkamlik talablari asosida shakllangan matematik modeli o'rganiladi. Shuningdek, hashingning blokcheyn arxitekturasida bajaradigan vazifalari — blok header tuzilmasida oldingi blok xeshiga tayangan holda zanjirning o'zgarmasligini ta'minlash, transaksiyalarni Merkle daraxtlari orqali ixchamlashtirish va verifikatsiya jarayonlarini optimallashtirish — ilmiy asoslangan holda yoritiladi. Tadqiqotda zamonaviy hashing algoritmlari, jumladan SHA-256, Keccak-256 (SHA-3), Blake2/3 va ASIC-resistant algoritmlar (Equihash, Scrypt, RandomX) texnik samaradorlik, xavfsizlik darajasi, energiya iste'moli va konsensus mexanizmlari bilan integratsiyasi nuqtai nazaridan taqqoslanadi. Shuningdek, Proof of Work va Proof of Stake mexanizmlarida hashingning roli, shuningdek, Zero-Knowledge protokollarida (Pedersen, Poseidon) isbot generatsiyasi uchun qo'llanishi tahlil qilinadi. Tadqiqot natijalari hashing algoritmlari blokcheyn tizimlarining ishonchliligi, barqarorligi va kelajakdagi quantum computing tahdidlariga nisbatan chidamliligini belgilashda strategik ahamiyatga egaligini ko'rsatadi. Kalit xulosalar blokcheyn xavfsizligi konsepsiyasida hashingni takomillashtirish bo'yicha ilmiy takliflarni o'z ichiga oladi.

Kalit so'zlar: Blockchain, Kriptografik xesh funksiyalari, SHA-256, Keccak-256, Merkle daraxti, Konsensus algoritmlari.

Ushbu annotatsiya va kalit so'zlarning akademik talablarga mos keladigan rus va ingliz tillaridagi tarjimasi:

Аннотация. Данное исследование посвящено глубокому научному анализу теоретических основ, технической архитектуры и аспектов безопасности механизмов хеширования данных, являющихся фундаментальным компонентом технологии блокчейн. В статье исследуется математическая модель криптографических хеш-функций, сформированная на основе таких требований устойчивости, как стойкость к поиску прообраза (pre-image resistance), стойкость к поиску второго прообраза (second pre-image

ISSN 3030-3907

resistance), коллизионная стойкость (collision resistance) и эффект лавины (avalanche effect). Также научно обосновываются функции хеширования в архитектуре блокчейна: обеспечение неизменности цепи путем опоры на хеш предыдущего блока в структуре заголовка, компактное представление транзакций через деревья Меркла и оптимизация процессов верификации. В исследовании проводится сравнительный анализ современных алгоритмов хеширования, включая SHA-256, Keccak-256 (SHA-3), Blake2/3 и ASIC-устойчивые алгоритмы (Equihash, Scrypt, RandomX), с точки зрения технической эффективности, уровня безопасности, энергопотребления и интеграции с механизмами консенсуса. Анализируется роль хеширования в механизмах Proof of Work и Proof of Stake, а также его применение для генерации доказательств в протоколах с нулевым разглашением (Zero-Knowledge: Pedersen, Poseidon). Результаты исследования показывают, что алгоритмы хеширования имеют стратегическое значение в определении надежности, стабильности и устойчивости блокчейн-систем к будущим угрозам квантовых вычислений. Ключевые выводы включают научные предложения по совершенствованию хеширования в концепции безопасности блокчейна.

Ключевые слова: Блокчейн, криптографические хеш-функции, SHA-256, Keccak-256, дерево Меркла, алгоритмы консенсуса.

Abstract. This research is devoted to an in-depth scientific analysis of the theoretical foundations, technical architecture, and security aspects of data hashing mechanisms, which constitute a fundamental component of blockchain technology. The article examines the mathematical model of cryptographic hash functions formed on the basis of robustness requirements such as pre-image resistance, second pre-image resistance, collision resistance, and the avalanche effect. Furthermore, the functions of hashing within the blockchain architecture are scientifically elucidated: ensuring chain immutability by referencing the previous block hash in the block header structure, compacting transactions through Merkle trees, and optimizing verification processes. The study compares modern hashing algorithms, including SHA-256, Keccak-256 (SHA-3), Blake2/3, and ASIC-resistant algorithms (Equihash, Scrypt, RandomX), in terms of technical efficiency, security level, energy consumption, and integration with consensus mechanisms. The role of hashing in Proof of Work and Proof of Stake mechanisms, as well as its application for proof generation in Zero-Knowledge protocols (Pedersen, Poseidon), is also analyzed. The research results demonstrate that hashing algorithms hold strategic importance in determining the reliability, stability, and resilience of blockchain systems against future quantum computing threats. Key

ISSN 3030-3907

findings include scientific proposals for enhancing hashing within the framework of blockchain security.

Keywords: Blockchain, Cryptographic hash functions, SHA-256, Keccak-256, Merkle tree, Consensus algorithms.

Kirish.

Blokcheyn texnologiyasi zamonaviy raqamli infratuzilmaning asosiy kriptografik tayanchlaridan biri bo‘lib, uning ishonchliligi ma’lumotlarni xeshlash mexanizmlariga bevosita bog‘liqdir. Xesh funksiyalari har qanday turdagi ma’lumotni qat’iy belgilangan uzunlikdagi raqamli “barmoq izi”ga aylantirishi, deterministik natija berishi, pseudotasodifiy va kolliziyalarga chidamli bo‘lishi bilan blokcheynning xavfsizlik modelini shakllantiradi. Drescher (2017) tomonidan ta’kidlanganidek, xesh funksiyalari blokcheynda nafaqat ma’lumotni identifikatsiya qilish, balki tarmoqdagi transaksiyalarni tezkor solishtirish, verifikatsiya jarayonlarini ixchamlashtirish va ma’lumot butunligini kafolatlash uchun ham zarurdir.

Blokcheynning taqsimlangan peer-to-peer muhiti katta hajmdagi transaksiyalar bilan ishlaydi va ularni noyob tarzda aniqlash zarurati paydo bo‘ladi. Shuning uchun xesh funksiyalarini “raqamli barmoq izi” sifatida talqin qilish to‘g‘ri metafora bo‘lib, ular yordamida har bir transaksiyaning noyob identifikatori yaratiladi. Xesh funksiyalarini qo‘llash naqshlari — mustaqil xeshlash, birlashtirilgan xeshlash, takroriy xeshlash, ketma-ket va ierarxik xeshlash — blokcheyn arxitekturasining strukturalash jarayonini belgilaydi. Aynan ierarxik xeshlash tamoyili Merkle daraxtlarining asosiy mexanizmini tashkil etib, katta hajmdagi ma’lumotlar bo‘yicha ixcham Merkle root orqali butun blokning o‘zgarmasligini matematik tarzda tasdiqlaydi[1].

Kriptografik xesh funksiyalarining nazariy asoslari Rogaway va Shrimpton (2004), shuningdek Wiley va MDPI platformalarida chop etilgan so‘nggi tadqiqotlarda chuqur o‘rganilgan bo‘lib, xesh funksiyalarining pre-image resistance, second pre-image resistance va collision resistance talablari ularning barqarorligini belgilaydi. Zamonaviy blokcheynlarda SHA-256, Keccak-256, Blake2/3 kabi algoritmlarning qo‘llanilishi ma’lumotlar yaxlitligi, konsensus mexanizmlarining samaradorligi va kelajakdagi post-quantum tahdidlariga chidamlilikni mustahkamlashda muhim omil sifatida baholanadi.

Kriptografik xesh funksiyalari blokcheyn texnologiyasining matematik asosini tashkil etib, ma’lumotlarni qisqa, qat’iy uzunlikdagi raqamli qiymatga aylantiruvchi mexanizmdir. Ular blokcheynning ma’lumot butunligini saqlash, transaksiyalarni identifikatsiya qilish, bloklar orasidagi bog‘liqlikni yaratish hamda tarmoqdagi har bir tugun tomonidan ma’lumotning bir xil talqin qilinishini ta’minlashda muhim rol o‘ynaydi. Xesh funksiyalarining ishlash tamoyili Drescher

ISSN 3030-3907

(2017) tomonidan “raqamli barmoq izi” metaforasi bilan ta’riflangan bo‘lib, qanday qilib barmoq izi har bir individni noyob aniqlasa, xesh qiymati ham har bir ma’lumotni noyob tarzda belgilaydi[2].

Xesh funksiyasining matematik ta’rifi quyidagicha ifodalanadi:

$$H:M\rightarrow\{0,1\}n$$

Bu yerda M – har qanday uzunlikdagi ma’lumotlar to‘plami, nnn esa belgilangan bit uzunligi (masalan, SHA-256 uchun 256 bit). Bu xususiyat blokcheyn tarmog‘idagi barcha ma’lumotlar, ularning hajmidan qat’i nazar, bir xil uzunlikdagi identifikator orqali taqqoslanishini ta’minlaydi.

Xesh funksiyalari deterministik bo‘lishi shart, ya’ni har safar bir xil kirish ma’lumotiga bir xil natija qaytadi. Bunda tarmoqdagi barcha tugunlar identik natija oladi. Aks holda, blokcheynning konsensus mexanizmi izdan chiqadi.

Xesh funksiyalarining eng muhim tamoyillaridan biri — bir tomonlama bo‘lishdir. Matematik nuqtayi nazardan, bu shunday ifodalanadi:

$$H(x)=\text{ybo‘lsa ham,}y\rightarrow x\text{ amalda imkonsiz.}$$

Bu xususiyat blokcheynning maxfiylik va butunlik tamoyillarini kafolatlaydi. Ma’lumot xeshlanganidan so‘ng uni qayta tiklab bo‘lmaydi, bu esa transaksiyalar mazmunining oshkor bo‘lib qolishini cheklaydi va tizim xavfsizligini oshiradi.

Collision resistance – xesh funksiyasining eng muhim kriptografik kafolatlaridan biridir. Ya’ni turli ma’lumotlarning bir xil xesh qiymatiga ega bo‘lish ehtimoli juda kichik bo‘lishi kerak. Kolliziya ehtimoli nazariy jihatdan quyidagicha baholanadi:

$$P(\text{collision})\approx 2^{-n/2}$$

Masalan, SHA-256 algoritmida n=256n=256n=256 bo‘lgani uchun amaliy kolliziya ehtimoli deyarli nolga teng. Rogaway va Shrimpton (2004) ushbu tamoyilni xesh funksiyalarining eng asosiy xavfsizlik mezonlaridan biri sifatida talqin qiladi.

Xesh funksiyalarida pseudotasodifiylik ham muhim o‘rin tutadi. Kirish ma’lumotidagi juda kichik o‘zgarish (hatto bitta bit) chiqishdagi natijaning keskin o‘zgarishiga olib kelishi kerak. Bu hodisa “avalanche effect” deb yuritiladi va blokcheyn uchun juda muhimdir. Chunki ma’lumotdagi minimal manipulyatsiya ham darhol seziladi va xesh qiymatlaridagi farq orqali aniqlanadi.

Drescher tomonidan tushuntirilgan xeshlash naqshlari kriptografik jarayonlarning amaliy qo‘llanilishini chuqurroq tushunish imkonini beradi. Mustaqil xeshlash har bir ma’lumotni alohida qayta ishlaydi, birlashtirilgan xeshlash esa ko‘plab ma’lumotlarni bitta satrga jamlab, umumiy xesh hosil qiladi. Takroriy xeshlash xesh natijasini yana qayta xeshlashdan iborat bo‘lib, Bitcoin blok sarlavhasida qo‘llanadigan “double SHA-256” buning yorqin misolidir.

ISSN 3030-3907

Ketma-ket xeshlash oqim ma’lumotlar bilan ishlovchi tizimlarda qo‘llanadi va har bir yangi ma’lumot avvalgi xesh qiymati bilan birlashtiriladi.

Eng muhim naqsh — bu ierarxik xeshlash, ya’ni Merkle daraxtlari mexanizmi. Merkle daraxti blok ichidagi barcha transaksiyalarning kriptografik izini umumlashtirib, yagona Merkle rootni hosil qiladi. Bu root blok headerida saqlanadi va blokning butun mazmuni o‘zgarmaganini isbotlash uchun xizmat qiladi. Agar bitta transaksiyada o‘zgarish yuz bersa, daraxt bo‘yicha barcha yuqoridagi xeshlar o‘zgaradi va natijada butun blokning haqiqiyligi buziladi.

Zamonaviy ilmiy tadqiqotlarda (MDPI, Wiley, IOS Press) xesh funksiyalarining blokcheyn xavfsizligidagi roli, ularning samaradorligi va yangi arxitekturalar bo‘yicha muhim xulosalar keltiriladi. Ayniqsa Keccak (SHA-3) ning sponge konstruktsiyasi, Blake2/Blake3 algoritmlarining yuqori tezligi va SHA-256 ning barqarorligi blokcheynning kelajakdagi texnologik rivojlanish yo‘nalishlarini belgilaydi. Shu bois, xesh funksiyalarining matematik asoslarini chuqur o‘rganish blokcheyn texnologiyasining xavfsizlik, samaradorlik va barqarorlik darajasini baholashda muhim ilmiy omil hisoblanadi[3][4].

Blokcheyn arxitekturasining o‘ziga xosligini belgilovchi eng muhim omillardan biri bu kriptografik xesh funksiyalarining tizim ichidagi o‘rni va ular bajaradigan vazifalardir. Xesh funksiyalari blokcheynning barcha asosiy jarayonlarini — bloklarning bog‘lanishi, transaksiyalarning identifikatsiyasi, ma’lumotning o‘zgarmasligi, verifikatsiya mexanizmlari, konsensus jarayonlari va yengil tugunlar faoliyatini — kriptografik darajada mustahkamlaydi. Xesh funksiyasi istalgan uzunlikdagi ma’lumotni qat’iy uzunlikdagi qiymatga o'tkazishga mo‘ljallangan bo‘lib, matematik tarzda quyidagi ko‘rinishda ifodalanadi:

$$H{:}M\rightarrow\{0,1\}^n$$

Bu yerda MMM — kirish ma’lumotlari to‘plami, nnn — xesh uzunligi (masalan, SHA-256 uchun 256 bit). Xesh funksiyasining deterministic bo‘lishi, ya’ni har bir bir xil kiritma uchun doimo bir xil natija berishi, blokcheyn tarmog‘ining barcha tugunlari o‘rtasida konsensusning shakllanishi uchun zarurdir. Shu sababli har bir blok yaratilganda uning sarlavhasi xeshlanadi va natija blokning noyob identifikatori sifatida saqlanadi.

Blokcheynning zanjirsimon tuzilmasi xesh pointerlar orqali yaratiladi. Har bir blok o‘zidan oldingi blokning xesh qiymatini o‘zida saqlaydi. Agar BiB_iBi blokning mazmuni o‘zgaradigan bo‘lsa, uning xesh qiymati ham o‘zgaradi:

$$H(B_i)\neq H(B_i')$$

Bu o‘zgarish zanjirning keyingi barcha bloklaridagi xesh pointerlarni buzadi va natijada butun blokcheyn strukturasi mos kelmay qoladi. Xuddi shuning uchun blokcheynning o‘zgarmaslik tamoyili matematik jihatdan mustahkam va amalda

ISSN 3030-3907

buzib bo‘lmaydigan mexanizmga ega. Zanjirning o‘rtasidagi bitta bitning o‘zgarishi ham barcha keyingi bloklarning noto‘g‘ri bo‘lishiga olib keladi, shuning uchun tasdiqlangan bloklarni o‘zgartirish deyarli imkonsiz hisoblanadi.

Transaksiyalarni xeshlash blokcheynning eng muhim amaliy jarayonlaridan biridir. Har bir transaksiyaga xesh funksiyasi qo‘llanadi va shu orqali noyob identifikator hosil qilinadi. Xesh funksiyasining pseudotasodifiy xususiyati tufayli:

$$x \to x', ||x - x'|| = 1 \Rightarrow H(x) \text{ va } H(x') \text{ butunlay farqli bo‘ladi.}$$

Bu “avalanche effect” deb yuritiladi va transaksiyalarni soxtalashtirishni mutlaqo imkonsiz qiladi. Transaksiyalar xesh orqali tanib olinadi, solishtiriladi va blok ichidagi tartibi aniqlanadi. Xeshlar identifikator sifatida barqaror bo‘lgani uchun tugunlar transaksiyalarni juda tez qayta ishlay oladi, bu tarmoqning optimalligini sezilarli oshiradi.

Merkle daraxtlari blokcheyn arxitekturasidagi eng muhim ierarxik xeshlash tuzilmasidir. Har bir transaksiyaning xeshi daraxt barglariga joylashtiriladi, keyin ular juft-juft birlashtirilib yana xeshlanadi. Bu jarayon yuqoriga ko‘tarilgan sari davom etadi va yakunida Merkle root hosil bo‘ladi. Merkle root quyidagi tarzda ishlaydi:

$$h_{i,j} = H(h_{i-1,2j} \| h_{i-1,2j+1})$$

Bu yagona root blokdagi barcha transaksiyalarning kriptografik izini ifodalaydi. Blokning ichidagi istalgan transaksiyadagi o‘zgarish daraxtning bir bo‘lagini, so‘ngra yuqoridagi barcha xeshlarni, oxirida Merkle rootni ham o‘zgartiradi. Shu sababli Merkle root blok sarlavhasiga kiritilgan eng muhim kriptografik indikator hisoblanadi. Bu mexanizm yengil tugunlarda (SPV nodes) bloklarni to‘liq yuklamasdan turib, faqat Merkle yo‘li orqali transaksiyani tekshirish imkonini yaratadi.

Konsensus algoritmlarida xeshlash yana ham siyosiy ahamiyat kasb etadi. Proof-of-Work tizimlarida maynerlar blok sarlavhasiga nonce qo‘shib yana qayta-qayta xesh hisoblaydi va ma’lum murakkablik darajasiga mos keladigan xesh qiymatini topishi kerak:

$$H(Header) < Target$$

Bu jarayon tarmoqni hisoblash jihatdan murakkab qiladi va xavfsizlik darajasini oshiradi. Proof-of-Stake tizimlarida esa xeshlash validator tanlashda, bloklarning tasodifiyligini belgilashda va tasdiqlash jarayonlarida qo‘llanadi. Har ikki mexanizmda xeshlash tizimning ishonchliligini saqlashda beqiyos ahamiyatga ega[5][6].

Umuman olganda, xesh funksiyalari blokcheynning o‘zgarmaslik, aniqlik, samarali verifikatsiya, zanjir barqarorligi va xavfsizlik tamoyillari uchun tayanch kriptografik mexanizm bo‘lib xizmat qiladi. Xeshlashni olib tashlash blokcheynning butun arxitekturasini mazmunsiz qilib qo‘ygan bo‘lardi.

ISSN 3030-3907

1-jadval.

Xeshlashning arxitekturaviy ahamiyati

Arxitektura tamoyili	Xeshlashning roli	Izoh
O‘zgarmaslik (Immutability)	Xesh pointerlar orqali bloklarning bog‘lanishi	Bitta bit o‘zgarishi ham butun zanjirni buzadi, bu o‘zgarmaslikni ta’minlaydi.
Aniqlik (Integrity)	Transaksiyalar va bloklarning xesh identifikatori	Har bir obyektning noyobligi kafolatlanadi va soxtalashtirish imkoni yo‘q.
Sinxronlik (Consistency)	Deterministik xeshlash	Barcha tugunlar bir xil natija oladi, konsensusning asosini tashkil etadi.
Verifikatsiya samaradorligi	Merkle daraxtlari orqali ixcham tekshiruv	SPV tugunlar tez va kam resurs bilan transaksiyani isbotlashi mumkin.
Zanjir barqarorligi	Blok sarlavhasi xeshlanishi	Bloklar orasidagi kriptografik bog‘liqlik buzilmaydi.
Xavfsizlik (Security)	Kolliziyaga chidamlik, bir tomonlama funksiyalar	Transaksiyalarni o‘zgartirish, qayta tiklash yoki soxtalashtirish amalda imkonsiz.

Blokcheyn texnologiyasida hashing algoritmlarining o‘rni beqiyos bo‘lib, ular tizimning xavfsizligini, barqarorligini va ishonchliligini ta’minlovchi asosiy kriptografik mexanizmdir. Hashing algoritmlarining samaradorligi blokcheynning umumiy ishlash mexanizmlariga, ayniqsa konsensus protokollariga bevosita ta’sir qiladi. Shu sababli turli blokcheyn platformalari o‘zining maqsadiga qarab farqli hashing algoritmlaridan foydalanadi. Ularning barchasi kriptografik mustahkamlik, kolliziyalarga chidamlilik, qaytarilmaslik, deterministiklik va pseudotasodifiylik tamoyillariga asoslanadi.

Zamonaviy blokcheynlarning aksariyatida hashingning eng mashhur varianti SHA-256 algoritmidir. U Bitcoin tarmog‘ining asosiy tayanchi bo‘lib, transaksiyalarni identifikatsiya qilishdan tortib blok sarlavhalarini generatsiya qilishgacha bo‘lgan barcha kriptografik jarayonlarda qo‘llaniladi. SHA-256 algoritmi o‘zining yuqori barqarorligi, kolliziyalarga qarshi chidamliligi va ko‘p

ISSN 3030-3907

yillik amaliy tajriba bilan tasdiqlangan ishonchliligi tufayli dunyodagi eng keng qo‘llaniladigan hashing standartlaridan biri hisoblanadi. Bitcoin arxitekturasi aynan shu algoritmning ishonchliligiga tayanadi, chunki PoW jarayonida milliardlab xesh hisob-kitoblari bajariladi va har bir natijaning aniq deterministik bo‘lishi zarur.

Ethereum esa SHA-256 o‘rniga Keccak-256 algoritmidan foydalanadi. Keccakning arxitekturasi SHA oilasidan farq qiladi va u ma’lumotlarni qayta ishlashda yanada moslashuvchan tizimga ega. Ethereumning Keccakni tanlashi uning faqat mayningga emas, balki aqlli kontraktlar, hisoblash amallari va ma’lumotlarni qayta ishlaydigan murakkab funksiyalarni ham qo‘llab-quvvatlashi bilan bog‘liq. Keccak-256 algoritmi xavfsizlik darajasining yuqoriligi bilan ajralib turadi va ko‘plab ilmiy tadqiqotlarda uning kolliziya ehtimoli amaliy jihatdan juda past ekani e’tirof etilgan.

Blake2 va Blake3 kabi yangi avlod hashing algoritmlari tezlik va samaradorlik bo‘yicha sezilarli ustunlikka ega. Blake2 SHA-256ga qaraganda tezroq ishlaydi, hisoblash resurslari kamroq sarflaydi va shu bilan birga kriptografik mustahkamlik darajasi yuqori. Blake3 esa zamonaviy ko‘p yadroli tizimlar uchun optimallashtirilgan bo‘lib, ma’lumotlarni parallel qayta ishlash imkonini beradi. Bu algoritmlar ayniqsa katta hajmdagi ma’lumotlarni qayta ishlaydigan blokcheyn platformalarida yoki yuqori darajadagi tranzaksiya oqimini talab qiladigan tizimlarda foydalidir. Ba’zi blokcheynlar, masalan Zcash, Litecoin yoki Monero, ASIC qurilmalarining ustunlikka ega bo‘lishini oldini olish uchun maxsus hashing algoritmlaridan foydalanadi. Zcash Equihash algoritmini qo‘llaydi, u xotira talabchanligi tufayli ASIClar bilan samarali ishlash imkonini bermaydi va GPU asosidagi mayningni qo‘llab-quvvatlaydi. Litecoinning Scrypt algoritmi esa xotira markazli yondashuvga ega bo‘lib, SHA-256ga nisbatan boshqacha xususiyatlarga ega. Moneroda esa RandomX algoritmi qo‘llaniladi, u CPU markazli bo‘lishi sababli tarmoqning markazlashuvdan holi bo‘lishini ta’minlaydi. Bu algoritmlar turli hujum vektorlariga qarshi blokcheynning himoya darajasini oshirishga qaratilgan[8].

Hashing algoritmlarining konsensus mexanizmlaridagi o‘rni yanada muhimdir. Proof-of-Work (PoW) modelida hashing isbot mexanizmining asosini tashkil etadi. Maynerlar blok sarlavhasiga turli qiymatlarni qo‘shib, uni qayta-qayta xeshlaydilar va faqat ma’lum shartlarga mos tushadigan qiymat topilganda blok haqiqiy deb qabul qilinadi. Ushbu jarayon tarmoqning himoyasi uchun zarur bo‘lgan hisoblash murakkabligini yaratadi. Xeshlash bu yerda “ish isboti” sifatida qo‘llanadi va kim ko‘proq hisoblash quvvatiga ega bo‘lsa, o‘sha blok yaratish imkoniyatiga ega bo‘ladi. Bu jarayon tarmoqni turli hujumlardan, jumladan “double spending” kabi muammolardan himoya qiladi.

ISSN 3030-3907

Proof-of-Stake (PoS) tizimida hashing PoWdagi kabi markaziy o‘rinni egallamasa-da, baribir konsensusning bir nechta bosqichlarida zarur element sifatida ishlatiladi. PoS tizimida validatorlarni tanlash jarayonida xeshlash deterministik va tasodifiy komponentlar o‘rtasida muvozanat yaratadi. Validatorlar orasida adolatli tanlov amalga oshirilishi uchun xesh funksiyalari qo‘llaniladi. Shuningdek, PoS tizimlari blokning haqiqiyligini tasdiqlashda, hujjatlashtirish jarayonlarida va bloklar orasidagi kriptografik bog‘lanishni saqlashda ham xeshlashga tayanadi.

Zero-Knowledge texnologiyalarida hashingning o‘rni yanada murakkab va kengaytirilgan ko‘rinishga ega. Masalan, zk-SNARK yoki zk-STARK texnologiyalarida hashing matematik isbotlarni yashirin shaklda yaratishga yordam beradi. Pedersen hashing, Poseidon hashing kabi algoritmlar zero-knowledge isbotlarining tezkor va xavfsiz ishlashiga imkon yaratadi. Bu texnologiyalar maxfiylikni saqlashga qaratilgan Web3 ekotizimlarida tobora keng qo‘llanmoqda.

Umuman olganda, hashing algoritmlari blokcheynning barcha jarayonlarida uzluksiz ishlaydigan, tizimning butun kriptografik poydevorini tashkil qiladigan mexanizmdir. Har bir blokcheyn o‘zining ehtiyojlari, xavfsizlik talablari, konsensus modeli va maqsadlariga qarab alohida hashing algoritmini tanlaydi. Bu tanlov tarmoqning barqarorligi, tezligi, energiya sarfi va hujumlarga chidamliligi bilan bevosita bog‘liqdir. Shu sababli hashing algoritmlari blokcheyn texnologiyalarida strategik ahamiyatga ega bo‘lib qoladi.

Ushbu tadqiqot blokcheyn texnologiyasining asosiy kriptografik elementi bo‘lgan xeshlash jarayonining nazariy va amaliy jihatlarini chuqur o‘rganishga bag‘ishlandi. Hashing blokcheyn arxitekturasining barcha qatlamlarida ishlaydigan, transaksiyalarning identifikatsiyasidan tortib konsensus mexanizmlarining barqarorligigacha bo‘lgan jarayonlarni himoyalovchi tayanch mexanizm sifatida namoyon bo‘ladi. Tadqiqot davomida xesh funksiyalarining deterministikligi, qaytarilmasligi, pseudotasodifiyligi va kolliziyaga chidamliligi blokcheynning o‘zgarmaslik tamoyilini qanday ta’minlashi keng tahlil qilindi. Ayniqsa, xesh pointerlar yordamida bloklarning zanjirsimon bog‘lanishi blokcheynning fundamental ishonch asosini shakllantirishi ilmiy asoslangan tarzda bayon etildi.

Merkle daraxtlari orqali ierarxik xeshlash mexanizmining qo‘llanilishi bloklardagi transaksiyalarni ixcham, tezkor va aniq tarzda tekshirish imkonini berishi muhim xulosa sifatida qayd etildi. Ushbu mexanizm tufayli yengil (SPV) tugunlar butun blokni yuklamasdan turib, faqat Merkle yo‘li orqali transaksiyaning haqiqiyligini isbotlay oladi. Bu blokcheyn tarmoqlarining keng ko‘lamda ishlay olishi, mobil va resurs cheklangan qurilmalar tomonidan qabul qilinishi uchun strategik afzallik yaratadi.

ISSN 3030-3907

Hashing algoritmlarining funksional farqlari ham tadqiqotning muhim jihatlaridan biri bo‘ldi. SHA-256, Keccak-256, Blake2/3, Scrypt, Equihash, RandomX kabi algoritmlarning turli blokcheyn platformalarida qo‘llanilishi ularning xavfsizlik talablari, konsensus modeli, hisoblash resurslari va markazlashuv darajasiga qarab qanday tanlanishini ko‘rsatdi. Ayniqsa, Proof-of-Work va Proof-of-Stake konsensus mexanizmlarida hashingning tutgan o‘rni turlicha bo‘lishiga qaramay, ular har ikkala tizimda ham ishonchlilik, tasodifiylik, kriptografik barqarorlik va isbotlash jarayonlarining asosiy tayanchi sifatida xizmat qilishi aniqlashtirildi[9].

Umuman olganda, xeshlash mexanizmi blokcheynning ishlash falsafasini belgilovchi, ularning o‘zgarmas va markazlashmagan tabiatini ta’minlovchi eng asosiy kriptografik tamoyildir. Tahlillar shuni ko‘rsatdiki, hashing algoritmlarisiz blokcheyn tizimi amalda mavjud bo‘la olmaydi. U ma’lumotlarning yaxlitligini saqlash, tarmoq ishtirokchilari o‘rtasida ishonch yaratish, konsensus algoritmlarini amalga oshirish va tizim barqarorligini kafolatlashda hal qiluvchi o‘rin tutadi. Shu bois hashing kelajakdagi Web3 va decentralizatsiya ekotizimlarining ham markaziy elementi bo‘lib qoladi.

FOYDALANILGAN ADABIYOTLAR

1. *Wiley Online Library.* (2020). **Blockchain-based Data Integrity using Cryptographic Hashing Techniques.** https://onlinelibrary.wiley.com/doi/full/10.1155/2020/8876317

2. *IOS Press Ebooks.* (2019). **Blockchain Hash Functions and Integrity Preservation in Distributed Systems.** https://ebooks.iospress.nl/volumearticle/50851

3. *MDPI Materials Journal.* (2019). **Application of Hashing Methods in Blockchain-Based Systems.** https://www.mdpi.com/2571-8800/2/3/21

4. *MDPI Symmetry Journal.* (2024). **Cryptographic Structures and Hash Algorithms in Decentralized Architectures.** https://www.mdpi.com/2073-8994/16/1/62

5. Drescher, D. (2017). **Blockchain Basics: A Non-Technical Introduction in 25 Steps.** Springer, Berlin. (Xususan, *Step 10: Hashing Data* bo‘limidan foydalanildi.)

6. Rogaway, P., & Shrimpton, T. (2004). **Cryptographic Hash-Function Basics: Definitions, Implications and Separations for Preimage Resistance, Second Preimage Resistance and Collision Resistance.** In *Fast Software Encryption – FSE 2004*, Springer LNCS Vol. 3017.

7. Merkle, R. (1987). **A Digital Signature Based on a Conventional Encryption Function.** In *Advances in Cryptology — CRYPTO ’87*. Springer.

ISSN 3030-3907

8. Nakamoto, S. (2008). **Bitcoin: A Peer-to-Peer Electronic Cash System.** https://bitcoin.org/bitcoin.pdf

9. Bertoni, G., Daemen, J., Peeters, M., & Van Assche, G. (2013). **Keccak Sponge Function Family.** NIST SHA-3 Standard Documentation.

ISSN 3030-3907