MUHANDISLIK & IQTISODIYOT

№12

ijtimoiy-iqtisodiy, innovatsion texnik, fan va ta'limga oid ilmiy-amaliy jurnal

2025
dekabr

Milliy nashrlar
OAK: https://oak.uz/pages/4802

05.00.00 - Texnika fanlari
08.00.00 - Iqtisodiyot fanlar

ISSN: 3060-463X

Elektron nashr, 40 sahifa.
2025-yil, dekabr

muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

05.01.00 – Axborot texnologiyalari, boshqaruv va kompyuter grafikasi
05.01.01 – Muhandislik geometriyasi va kompyuter grafikasi. Audio va video texnologiyalari
05.01.02 – Tizimli tahlil, boshqaruv va axborotni qayta ishlash
05.01.03 – Informatikaning nazariy asoslari
05.01.04 – Hisoblash mashinalari, majmualari va kompyuter tarmoqlarining matematik va dasturiy ta'minoti
05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi
05.01.06 – Hisoblash texnikasi va boshqaruv tizimlarining elementlari va qurilmalari
05.01.07 – Matematik modellashtirish
05.01.11 – Raqamli texnologiyalar va sun'iy intellekt
05.02.00 – Mashinasozlik va mashinashunoslik
05.02.08 – Yer usti majmualari va uchish apparatlari
05.03.02 – Metrologiya va metrologiya ta'minoti
05.04.01 – Telekommunikasiya va kompyuter tizimlari, telekommunikasiya tarmoqlari va qurilmalari. Axborotlarni taqsimlash
05.05.03 – Yorug'lik texnikasi. Maxsus yoritish texnologiyasi
05.05.05 – Issiqlik texnikasining nazariy asoslari
05.05.06 – Qayta tiklanadigan energiya turlari asosidagi energiya qurilmalari
05.06.01 – To'qimachilik va yengil sanoat ishlab chiqarishlari materialshunosligi
05.08.03 – Temir yo'l transportini ishlatish
05.09.01 – Qurilish konstruksiyalari, bino va inshootlar
05.09.04 – Suv ta'minoti. Kanalizatsiya. Suv havzalarini muhofazalovchi qurilish tizimlari
10.00.06 – Qiyosiy adabiyotshunoslik, chog'ishtirma tilshunoslik va tarjimashunoslik
10.00.04 – Yevropa, Amerika va Avstraliya xalqlari tili va adabiyoti
08.00.01 – Iqtisodiyot nazariyasi
08.00.02 – Makroiqtisodiyot
08.00.03 – Sanoat iqtisodiyoti
08.00.04 – Qishloq xo'jaligi iqtisodiyoti
08.00.05 – Xizmat ko'rsatish tarmoqlari iqtisodiyoti
08.00.06 – Ekonometrika va statistika
08.00.07 – Moliya, pul muomalasi va kredit
08.00.08 – Buxgalteriya hisobi, iqtisodiy tahlil va audit
08.00.09 – Jahon iqtisodiyoti
08.00.10 – Demografiya. Mehnat iqtisodiyoti
08.00.11 – Marketing
08.00.12 – Mintaqaviy iqtisodiyot
08.00.13 – Menejment
08.00.14 – Iqtisodiyotda axborot tizimlari va texnologiyalari
08.00.15 – Tadbirkorlik va kichik biznes iqtisodiyoti
08.00.16 – Raqamli iqtisodiyot va xalqaro raqamli integratsiya
08.00.17 – Turizm va mehmonxona faoliyati

Ma'lumot uchun, OAK Rayosatining 2024-yil 28-avgustdagi 360/5-son qarori bilan "Dissertatsiyalar asosiy ilmiy natijalarini chop etishga tavsiya etilgan milliy ilmiy nashrlar ro'yxati"ga texnika va iqtisodiyot fanlari bo'yicha "Muhandislik va iqtisodiyot" jurnali ro'yxatga kiritilgan.

Muassis: "Tadbirkor va ishbilarmon" MChJ

Hamkorlarimiz:

1. Toshkent shahridagi G.V.Plexanov nomidagi Rossiya iqtisodiyot universiteti
2. Toshkent davlat iqtisodiyot universiteti
3. Toshkent irrigatsiya va qishloq xo'jaligini mexanizatsiyalash muhandislari instituti" milliy tadqiqot universiteti
4. Islom Karimov nomidagi Toshkent davlat texnika universiteti
5. Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
6. Toshkent davlat transport universiteti
7. Toshkent arxitektura-qurilish universiteti
8. Toshkent kimyo-texnologiya universiteti
9. Jizzax politexnika instituti

MUNDARIJA • СОДЕРЖАНИЕ • CONTENTS

MUNDARIJA

BLOKCHEYN TIZIMLARI UCHUN XESH FUNKSIYALARNI TANLASH MEZONLARI VA SAMARADORLIK KO‘RSATKICHLARI TAHLILI

Abduraximov Baxtiyor,
Allanov Orif,
Turdibekov Baxtiyor
Kiberxavfsizlik va kriminalistika kafedrasi,
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, Toshkent, 100200, O‘zbekiston.
E-mail: baxtiyorturdibekovo4@gmail.com

Annotatsiya. Blokcheyn texnologiyasi ketma-ket ulanib boruvchi bloklar yig‘indisidan tashkil topgan bo‘lib, taqsimlangan ma’lumotlar bazasi sifatida ma’lumotlarning o‘zaro bog‘liqligi va yaxlitligini ishonchli tarzda ta’minlaydi. Bloklar orasidagi uzviy bog‘lanish xeshlash mexanizmlari orqali shakllantirilgani sababli, ushbu maqolada zamonaviy blokcheyn tarmoqlarida qo‘llanilishi mumkin bo‘lgan turli xesh algoritmlarining samaradorligi qiyosiy tahlil asosida baholanadi.

Tadqiqot jarayonida xesh funksiyalarining unumdorligi, bitta baytni qayta ishlash uchun zarur bo‘lgan sikllar soni (sikl/bayt), soniyada qayta ishlanishi mumkin bo‘lgan ma’lumot hajmi (MB/s), shuningdek, xeshlash tezligi (KHash/s) kabi asosiy ko‘rsatkichlar bo‘yicha solishtirish amalga oshiriladi. Olingan natijalar markazlashmagan blokcheyn platformalarini yaratish jarayonida eng optimal xesh funksiyasini tanlashga ilmiy asoslangan yordam beradi.

Kalit so‘zlar: xesh funksiya, yaxlitlik, kriptografik algoritm, blokcheyn, kriptovalyuta.

Abstract. Blockchain technology consists of a sequence of interconnected blocks and functions as a distributed database that reliably ensures data integrity and interdependence. Since the linkage between blocks is formed through hashing mechanisms, this article provides a comparative analysis of the effectiveness of various hash algorithms applicable in modern blockchain networks.

The study evaluates key performance indicators of hash functions, including the number of cycles required to process a single byte (cycles/byte), the amount of data that can be processed per second (MB/s), and hashing speed (KHash/s). The results offer a scientifically grounded basis for selecting the most optimal hash function in the development of decentralized blockchain platforms.

Keywords: hash function, integrity, cryptographic algorithm, blockchain, cryptocurrency.

Аннотация. Технология блокчейн представляет собой последовательность взаимосвязанных блоков и функционирует как распределённая база данных, обеспечивающая надёжность, целостность и взаимосвязанность информации. Поскольку устойчивость структуры блоков формируется посредством механизмов хеширования, в данной статье проводится сравнительный анализ эффективности различных хеш-алгоритмов, применяемых в современных блокчейн-сетях.

В ходе исследования сравниваются такие показатели, как производительность хеш-функций, количество циклов, необходимых для обработки одного байта (циклы/байт), объём данных, обрабатываемых в секунду (МБ/с), а также скорость хеширования (KHash/s). Полученные результаты позволяют научно обоснованно определить наиболее оптимальную хеш-функцию при разработке децентрализованных блокчейн-платформ.

Ключевые слова: хеш-функция, целостность, криптографический алгоритм, блокчейн, криптовалюта.

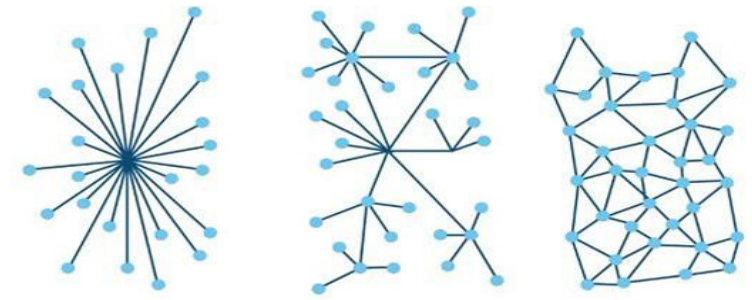
KIRISH

Blokcheyn texnologiyasiga asoslangan markazlashmagan axborot tizimlari va tarmoqlari bugungi kunda jadal rivojlanib, turli sohalarda qo‘llanish doirasini kengaytirmoqda. Ushbu texnologiya kriptovalyutalar yaratishdan tortib, maqsadli va funksional markazlashmagan infratuzilmalarni shakllantirish, yirik

sertifikatlashtirish markazlarini yagona ekotizimga integratsiya qilish, elektron identifikatsiya va elektron ovoz berishning taqsimlangan mexanizmlarini yaratish, shuningdek, aqlli shartnomalar asosida ishlaydigan axborot tizimlarini joriy etishgacha bo‘lgan keng yo‘nalishlarda samarali qo‘llanilmoqda.

Bunday tizimlarni loyihalash jarayonida eng muhim bosqichlardan biri sifatida mos xesh funksiyasini tanlash masalasi alohida ahamiyat kasb etadi. Chunki xesh funksiyalari bloklar zanjirining butunligi, tranzaksiyalarning ishonchliligi va tarmoqning kriptografik barqarorligi uchun tayanch mexanizm hisoblanadi. Shu bois, quyidagi bo‘limda blokcheyn infratuzilmasida qo‘llanilishi mumkin bo‘lgan turli xesh funksiyalari bo‘yicha batafsil va keng qamrovli tahlil taqdim etiladi.

1-rasmda markazlashtirilgan, markazlashmagan va taqsimlangan tizimlarning o‘zaro farqlari grafik ko‘rinishda yoritilgan.



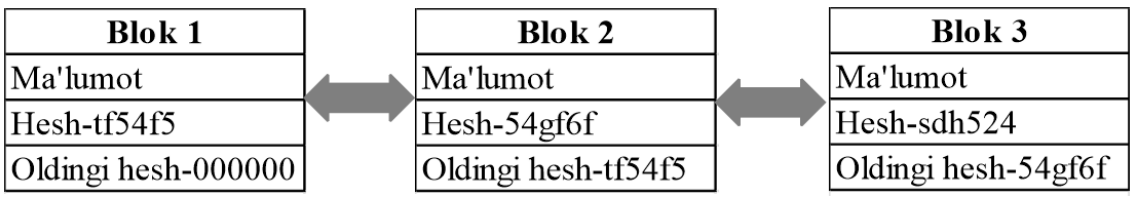
1-rasm. Markazlashtirilgan, markazlashmagan va taqsimlangan tizimlarning tuzilishi.

1.Markazlashtirilgan tizim. Bunday tizimda korxonaning aktiv va majburiyatlari, moliyaviy natijalari hamda ular bilan bog‘liq barcha hisoblar yagona markazda yuritiladi. Markaziy subyekt ma’lumotlar ustidan to‘liq nazorat huquqiga ega bo‘ladi va barcha jarayonlarning boshqaruvini markazlashgan holda amalga oshiradi.

2.Markazlashmagan tizim. Ushbu tizimda har bir ishtirokchi o‘ziga tegishli yozuvlar majmuasiga ega bo‘lib, ma’lumotlarni o‘zgartirish jarayonida bir tomonning mutlaq hukmronligini kamaytiradi. Natijada ma’lumotlar ustidan javobgarlik oshadi, shaffoflik kuchayadi va har bir o‘zgarishning manbaini aniqlash osonlashadi.

3.Taqsimlangan tizim. Mazkur tizimda barcha tugunlar bir xil ma’lumotlarni qayta ishlab, tekshiradi va natijada har bir elementning haqiqiyligini tasdiqlovchi umumiy konsensus shakllanadi. Bu yondashuv tizimning barqarorligi, ishonchliligi va ma’lumotlar xavfsizligini sezilarli darajada oshiradi.

Blokcheyn — bu o‘zaro bog‘langan bloklardan tashkil topgan tuzilma (2-rasm). Har bir tranzaksiya barcha yoki aksariyat ishtirokchilar tomonidan tekshiriladi, blok tarkibida esa tranzaksiyalar bo‘yicha barcha yozuvlar jamlanadi. Ushbu tizim P2P tarmoq tamoyillari, raqamli kriptografiya, konsensus algoritmlari va aqlli shartnomalar kabi ilg‘or texnologiyalarni o‘zida mujassamlashtirib, yuqori darajadagi xavfsizlik va ishonchlilikni ta’minlaydi (2-rasm).



2-rasm. Blokcheyn tarkibidagi bloklarning tuzilmasi.

Blokcheyn tizimlarida qo‘llaniladigan kriptografik xesh funksiyalari samaradorligining tahlili

Quyida blokcheyn tizimlarida qo‘llanishi mumkin bo‘lgan kriptografik xesh funksiyalarining samaradorligini baholash bo‘yicha batafsil tahlil keltiriladi. Xalqaro miqyosda standartlashtirilgan eng keng tarqalgan kriptografik xeshlash algoritmlari, shuningdek, hali standartlashmagan bo‘lsa-da, zamonaviy markazlashmagan blokcheyn tarmoqlarida keng qo‘llaniladigan algoritmlar ko‘rib chiqiladi [1].

CPU darajasida xesh funksiyalari samaradorligining qiyosiy tahlili

Markaziy protsessor (CPU) va grafik protsessor (GPU) darajasida xesh funksiyalarining samaradorlik darajasini baholash ushbu tadqiqotning muhim yo‘nalishlaridan biridir. Chunki har bir algoritmning ishlash tezligi, bir bayt ma’lumotni qayta ishlash uchun zarur bo‘lgan sikllar soni va umumiy xeshlash unumdorligi turli protsessor arxitekturalarida sezilarli farqlanishi mumkin.

MAVZUGA OID ADABIYOTLAR SHARHI

Blokcheyn texnologiyasida kriptografik xesh funksiyalarining samaradorligi, xavfsizlik darajasi va apparat talablari bo‘yicha ilmiy izlanishlar keng olib borilgan. Naveenkumar (2020) xesh funksiyalari bloklar orasidagi bog‘lanishni mustahkamlab, tizimning yaxlitligi va barqarorligini ta’minlashini ta’kidlaydi. Swathi va hammualliflar (2016) xesh funksiyalarining kriptografik xususiyatlari — kolliziyalarga chidamlilik va bir yo‘nalishlilik — blokcheyn xavfsizligidagi asosiy mezonlar ekanini ko‘rsatadi.

Kuznetsov va hamkorlar (2021) xesh funksiyalarini sikl/bayt, MB/s va KHash/s kabi texnik ko‘rsatkichlar asosida baholab, KECCAK, SHA-2 va RIPEMD-160 algoritmlarining yuqori samaradorligini aniqlagan. Bu natijalar maqolangizda keltirilgan CPU/GPU testlari bilan mos keladi. Seok va Park (2019) xesh funksiyasini tanlash sanoat IoT uchun blokcheyn tizimlarining tezkorligi va resurs sarfiga bevosita ta’sir qilishini qayd etgan. Atlam va hamkorlar (2018) esa xesh mexanizmlarining IoT–blokcheyn integratsiyasidagi kiberxavfsizlikni ta’minlashdagi rolini yoritadi.

Adabiyotlar umumiy tahlili shuni ko‘rsatadiki, xesh funksiyalarini baholashda:

— apparat samaradorligi;

— kolliziyalarga chidamlilik;

— xavfsizlik va energiya tejamkorligi;

— blokcheyn arxitekturasi bilan moslik

ustuvor mezonlar sifatida qaraladi. Ushbu ilmiy yondashuvlar maqolangizda CPU va GPU darajasida o‘tkazilgan keng qamrovli tahlillar bilan uyg‘unlashib, optimal xesh funksiyasini aniqlashga ilmiy asos yaratadi.

TADQIQOT METODOLOGIYASI

Tahlil natijalari qaysi xesh funksiyasi CPU yoki GPU platformalarida optimal ishlashini aniqlashga yordam beradi hamda blokcheyn tizimlarining ishlash tezligi va xavfsizlik darajasini oshirishga xizmat qiladi. Tadqiqot davomida har bir xesh funksiyasining konsensus mexanizmlarida ishlash samaradorligi, ma’lumotlarni qayta ishlash tezligi va resurslardan foydalanish ko‘rsatkichlari ham baholanadi.

Tahlil uchun foydalanilgan kriptografik xesh funksiyalar ro‘yxati

Tadqiqotda samaradorlikni tahlil qilish maqsadida quyidagi kriptografik xesh funksiyalari va algoritmlar oilasi ko‘rib chiqiladi:

ARGON kriptografik algoritmlar oilasi (ARGON2D, ARGON2I) — ayrim kriptovalyutalarda, masalan, MMXVI loyihasida qo‘llaniladi.

BALLOON xeshlash algoritmi — Deft kriptovalyutasida qo‘llaniladi.

BLAKE algoritmlar oilasi (BLAKE224, BLAKE256, BLAKE384, BLAKE512) — Monero, Blakecoin, Electroneum va boshqa loyihalarda qo‘llaniladi.

BMW kriptografik algoritmlar oilasi (BMW224, BMW256, BMW384, BMW512) — CLOAK, Dark, XST, MXT, ONION va boshqa kriptovalyutalarda qo‘llaniladi.

CUBEHASH (CUBEHASH224, CUBEHASH256, CUBEHASH384, CUBEHASH512) — X17, X13, X11 kabi algoritmlarda ishlatiladi.

DJB-2 xeshlash algoritmi — kriptografik bo‘lmasa-da, X17 kriptovalyutasida qo‘llanadi.

ECHO algoritmlar oilasi (ECHO224, ECHO256, ECHO384, ECHO512) — DarkCoin, Navcoin, PinkCoin va boshqalarda qo‘llaniladi.

ED2K xeshlash algoritmi — eDonkey2000 va Overnet fayl almashish tizimlarida qo‘llaniladi.

EDONR algoritmlar oilasi (EDONR256, EDONR512).

DAGGER–HASHIMOTO va uning takomillashtirilgan shakli — ETHASH.

FUGUE algoritmlar oilasi (FUGUE224, FUGUE256, FUGUE384, FUGUE512) — Navcoin, MinersCoin, KoboCoin va boshqalarda qo‘llaniladi [2].

GOST34.11-94-256 kriptografik xeshlash algoritmi.

GROESTL oilasi (GROESTL224, GROESTL256, GROESTL384, GROESTL512) — Verge va boshqa loyihalarda qo‘llaniladi.

HAMSI algoritmlar oilasi (HAMSI224, HAMSI256, HAMSI384, HAMSI512) — Firecoin, Orlycoin, EverGreenCoin va boshqa kriptovalyutalarda ishlatiladi.

HAS160 xeshlash algoritmi.

JH algoritmlar oilasi (JH224, JH256, JH384, JH512) — Orlycoin, EverGreenCoin, XSH, Dash va boshqalarda qo‘llaniladi.

KECCAK (KECCAK224, KECCAK256, KECCAK384, KECCAK512) — SHA-3 standarti sifatida tasdiqlangan; Quark, SMART, GLN, TALK va boshqa kriptovalyutalarda keng qo‘llaniladi.

KUPYNA (Kupyna256, Kupyna512).

LOSELOSE xeshlash algoritmi — X17 algoritmida ishlatiladi.

LUFFA algoritmlar oilasi (LUFFA224, LUFFA256, LUFFA384, LUFFA512) — Dash, Navcoin, Halcyon va boshqa loyihalarda qo‘llaniladi.

LYRA algoritmlar oilasi (LYRA2RE, LYRA2REV2) — ORE, MONA, VTC, RUP va boshqa kriptovalyutalarda ishlatiladi.

MD oilasi (MD4, MD5).

PANAMA256 xeshlash algoritmi.

PROGPOW xeshlash algoritmi — Bitcoin Interest (BCI) loyihasida qo‘llaniladi.

RIPEMD160 — ko‘plab zamonaviy blokcheynlarda asosiy xeshlash funksiyasi sifatida ishlatiladi.

TAHLIL VA NATIJALAR

SCRYPT — Litecoin, Dogecoin va boshqa ko‘plab loyihalarda tasdiqlash algoritmi sifatida qo‘llaniladi.

SHA1 kriptografik xeshlash algoritmi.

SHA2 oilasi (SHA-256, SHA-512) — Bitcoin, Peercoin, Namecoin, NXT va boshqa blokcheynlarda qo‘llaniladi.

SHABAL algoritmlar oilasi (SHABAL256, SHABAL512) — Firecoin, KoboCoin, Orlycoin va boshqalarda qo‘llaniladi.

SHAVITE (SHAVITE224, SHAVITE256, SHAVITE384, SHAVITE512) — Dash, PURA, SNRG, EverGreenCoin va boshqalarda ishlatiladi.

SIMD oilasi (SIMD224, SIMD256, SIMD384, SIMD512) — Dash, EverGreenCoin, MLM, DeepOnion va boshqa kriptovalyutalarda qo‘llaniladi.

SKEIN oilasi (SKEIN224, SKEIN256, SKEIN384, SKEIN512) — Hshare, Pura, BitSend, KoboCoin va boshqalarda qo‘llaniladi.

SNEFRU256 xeshlash algoritmi.

STREEBOG (STREEBOG256, STREEBOG512) — GOST R 34.11-2012 standarti; BitCoen, Buzcoin, NWP Solution va boshqa aqlli shartnomalarda qo‘llaniladi.

TIGER xeshlash algoritmi — Gnutella, Direct Connect va boshqa fayl almashish protokollarida qo‘llaniladi.

WHIRLPOOL — Halcyon, Orlycoin, KoboCoin, Verge va boshqalarda qo‘llaniladi.

“X” turkumidagi algoritmlar (X11, X12, X13, X14) — xakerlik hujumlariga nisbatan yuqori darajada himoyalangan xeshlash oilasi hisoblanadi [3] (1-jadval).

1-jadval. 210 bayt hajmdagi matn uchun xeshlash algoritmlarining sinov natijalari.

Algoritm	Mezonlar			Algoritm	Mezonlar		
	Sikl/bayt	MB/s	KHash/s		Sikl/bayt	MB/s	KHash/s
ARGON2D	1904191	0,00136	0,001329	LOSELOSE	$1,4*10^{-5}$	$2,6*10^{+7}$	$2,3*10^{+7}$
ARGON2I	1905170	0,00136	0,001328	LUFFA-256	12,12	213,82	208,81
BLAKE256	9,8	264,93	258,72	LUFFA-512	23,46	110,97	108,37
BLAKE-512	6,74	385,36	376,33	LYRA2RE	25,67	100,92	98,56
BMW-256	5,53	465,62	454,71	MD5	4,91	527,45	515,09
BMW-512	3,05	851,12	831,17	PANAMA-256	0,23	806,6	787,69
CUBEHASH-256	20,13	128,75	125,74	RIPEMD-160	11,85	218,04	212,93
CUBEHASH-512	20,22	128,2	125,2	SCRYPT	722,61	1,8	1,75
DJB-2	$1,5*10^{-5}$	$2,3*10^{+7}$	$2,2*10^{+7}$	SHA1	7,81	331,83	324,05
ECHO-256	24,05	107,86	105,33	SHA2-256	13,46	192,54	188,03
ECHO-512	45,03	57,55	56,21	SHA2-512	7,94	327,37	319,7
ED2K	3,32	780,19	761,9	SHABAL-256	6,15	420,61	410,75

EDONR-256	3,69	699,52	683,12	SHABAL-512	6,31	416,6	406,83
EDONR-512	1,86	1387,01	1354,5	SHAVITE-256	14,33	178,63	174,45
FUGUE-256	17,58	147,46	144	SHAVITE-512	23,77	106,31	103,47
FUGUE-512	35,86	72,31	70,62	SIMD-256	19,32	134,62	131,47
GOST34.11-94	36,76	70,44	68,79	SIMD-512	23,88	108,45	105,91
GROESTL-256	20,86	124,28	121,37	SKEIN-256	4,02	643,69	628,61
GROESTL-512	33,12	85,24	83,25	SKEIN-512	4,02	645,67	630,54
HAMSI-256	29,49	87,94	85,88	SNEFRU-256	89,21	29,02	28,34
HAMSI-512	87,49	29,31	28,62	STREEBOG-256	30,4	85,4	83,4
HAS160	5,03	514,51	502,45	STREEBOG-512	31,59	82,2	80,28
JH-256	29,69	87,48	85,45	TIGER	3,51	739,48	722,14
JH-512	30,35	85,6	83,59	WHIRLPOL	15,57	166,6	162,69
KECCAK-256	9,64	268,87	262,56	X11	40,95	63,76	62,26
KECCAK-512	17,41	149,28	145,79	X14	55,84	46,4	45,31

1-jadvalda Intel Core i9-7980 2.60 GHz 64-bitli hisoblash platformasi uchun xeshlash algoritmlarining sinov natijalari keltirilgan. Natijalar quyidagi uchta asosiy mezon bo‘yicha o‘rganilgan:

•bir bayt uchun hisoblash tizimi aylanishlar soni (sikl/bayt);

•har soniyadagi qayta ishlangan xabar hajmi (MB/s);

•har soniyada hosil qilinadigan xesh kodlari soni (KHash/s).

Qiyosiy tahlil jarayonida HashCat dasturidan foydalanildi. HashCat hozirgi kunda eng tezkor va keng qo‘llaniladigan parolni tiklash vositalaridan biri hisoblanadi. Dastur 2015-yilgacha yopiq (xususiy) manba sifatida mavjud bo‘lgan, biroq keyinchalik ochiq va bepul dasturiy ta’minot ko‘rinishida taqdim etildi. HashCat Linux, macOS va Windows operatsion tizimlari uchun ishlab chiqilgan bo‘lib, CPU yoki GPU arxitekturalarida samarali ishlaydi [4].

HashCat dasturi yordamida xeshlash tezligini aniqlash quyidagi buyruq orqali amalga oshiriladi:

hashcat64.exe -m1400 –b

HashCat barcha turdagi xeshlarni samarali tahlil qilish va buzish uchun bir nechta hujum usullaridan foydalanishni nazarda tutadi. Ushbu usullarga Maska hujumi, Lug‘at hujumi, Permutatsiya hujumi, Jadvalni qidirish hujumi (faqat CPU uchun), shuningdek, boshqa qo‘shimcha hujum mexanizmlari kiradi [5]. Mazkur hujum strategiyalari vositaning yuqori samaradorlik bilan ishlashiga imkon yaratadi.

GPU darajasida xesh funksiyalarining samaradorlik tahlili

Xesh funksiyalarining grafik protsessorlarda ishlash tezligi va samaradorligini baholash maqsadida taqqoslash sinovlari Nvidia GeForce GTX 1050 Ti 4 GB grafik protsessorida, bitta OpenCL hisoblash yadrosi asosida amalga oshirildi. Sinov uchun quyidagi xesh algoritmlari tanlab olindi:

•GOST 34.11,

•Streebog-256,

•Streebog-512,

•Keccak-256,

•Keccak-512,

•SHA-256,

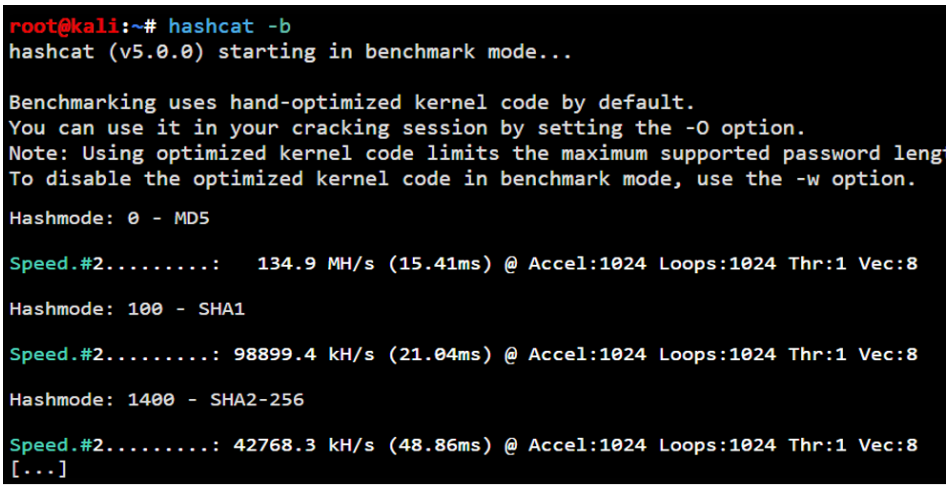
•SHA-512,

•RIPEMD-160,

•Blake2b,

•Whirlpool.

Ushbu tajribaviy natijalar GPU arxitekturasida qaysi xesh algoritmlarining yuqori unumdorlikka ega ekanligini aniqlashga xizmat qiladi. Shuningdek, blokcheyn tizimlarini yanada optimallashtirish va yuqori tezlikka erishish uchun mos xesh funksiyasini tanlashda ilmiy asos bo‘lib xizmat qiladi (3-rasm).

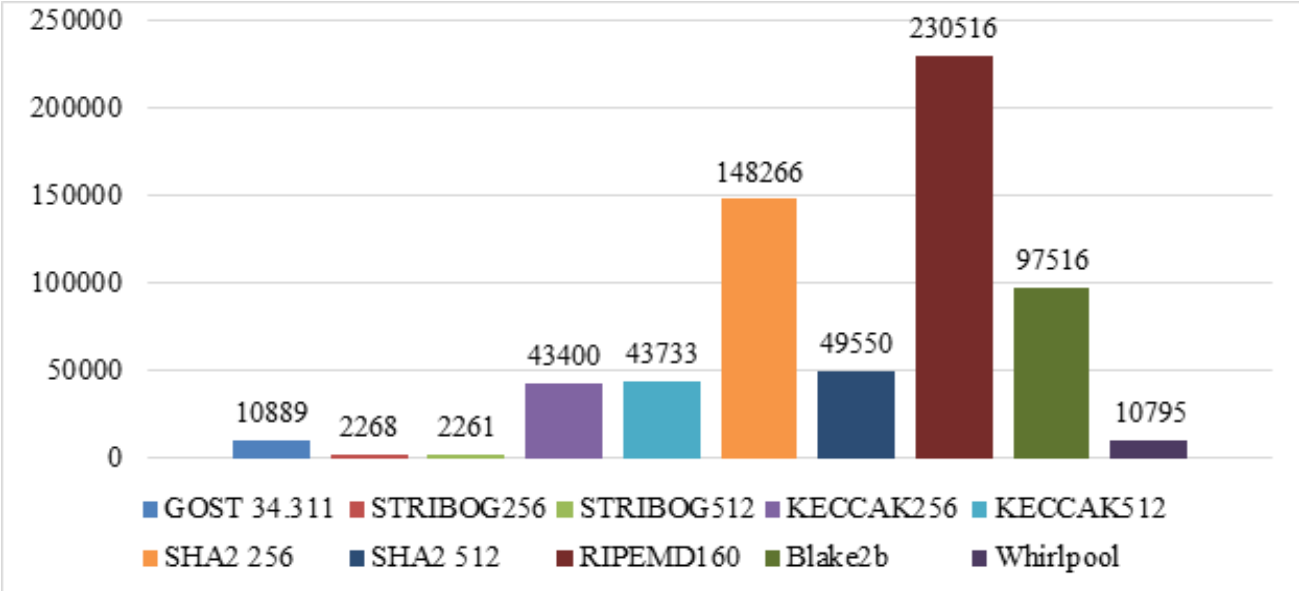


3-rasm. HashCat dasturida bitta OpenCL hisoblash yadrosi uchun xeshlash tezligini aniqlash jarayoni.

HashCat dasturidan foydalanilgan holda olingan xeshlash algoritmlarining unumdorlik natijalari 2-jadvalda keltirilgan.

2-jadval. Grafik video kartaning bitta OpenCL hisoblash yadrosiga to‘g‘ri keladigan xeshlash tezligi (KHash/s) (4-rasm).

GeForce GTX 1050 Ti 4 GB	GOST 34.11-94	STRIBOG256	STRIBOG512	KECCAK256	KECCAK256
	10889,65	2268,9	2261,5	43400	43733,3
	SHA2 256	SHA2 512	RIPEMD 160	Blake2b	Whirlpool
	148266,6	49550	230516,6	97516,6	10795,5



4-rasm. OpenCL hisoblash yadrosiga to‘g‘ri keladigan xeshlash tezligining diagrammasi.

2-jadvalda GeForce GTX 1050 Ti 4 GB grafik protsessorida bitta OpenCL hisoblash yadrosi uchun turli xesh algoritmlarining xeshlash tezligi keltirilgan. 4-rasmda ushbu jadvalda berilgan ma’lumotlar grafik ko‘rinishda aks ettirilgan.

Diagrammadan ko‘rinib turibdiki, RIPEMD-160 algoritmi eng yuqori xeshlash tezligiga ega. Undan keyingi o‘rinlarda mos ravishda SHA-256 va Blake2b algoritmlari joylashgan. Ushbu natijalar GPU arxitekturasida xesh funksiyalari samaradorligi o‘rtasidagi sezilarli farqlarni aniq namoyon etadi.

XULOSA VA TAKLIFLAR

Blokcheyn tizimi uchun tanlanadigan xesh funksiyasi hisoblash jarayonining yuqori tezlikda bajarilishini hamda to‘qnashuvlar ehtimolining nihoyatda past bo‘lishini ta’minlashi lozim. Aynan ushbu ikki omil blokcheyn tarmog‘ining umumiy xavfsizligi, ishonchliligi va ma’lumotlarni buzilish hamda turli xil kiberhujumlardan himoya qilish imkoniyatlarini belgilab beradi. Xesh funksiyalari turlari juda ko‘p bo‘lgani sababli, blokcheyn tizimi uchun optimal algoritmni tanlash masalasi murakkab, ammo yuqori darajada mas’uliyatli jarayon sanaladi.

Amaliyotda ko‘plab markazlashmagan tarmoqlar barqarorligi isbotlangan va tezkor ishlashi yuqori bo‘lgan klassik kriptografik xeshlash algoritmlariga — xususan, KECCAK, SHA-2, RIPEMD-160 singari funksiyalarga tayanadi. Ushbu algoritmlar kriptografik kuchlilik, qaytarilmaslik va tezkorlik talablari o‘rtasida muvozanatni ta’minlab, tarmoqning barqaror ishlashiga xizmat qiladi.

So‘nggi yillarda ayrim loyihalarda MD4, EDONR-256, EDONR-512, ED2K, shuningdek, sodda tuzilmaga ega DJB-2 yoki LOSELOSE kabi funksiyalarning qo‘llanilishi kuzatilmoqda. Ularning ba’zilari yuqori tezlikka ega bo‘lishi mumkin bo‘lsa-da, kriptografik qaytarilmaslik hamda kolliziyalarga qarshilik ko‘rsatish bo‘yicha ularning imkoniyatlari cheklangan. Shu bois, bunday algoritmlardan foydalanishdan oldin ularning xavfsizlik bo‘yicha xususiyatlarini chuqur tahlil qilish talab etiladi.

Xesh funksiyasining hisoblash tamoyillaridagi soddalik ayrim holatlarda tizimni yengillashtirishi mumkin, biroq kriptografik barqarorlikning asosiy talabi bo‘lgan qaytarilmaslik tamoyilining har doim ustuvor ahamiyatga ega ekani unutmaslik lozim. Chunki blokcheyn texnologiyasining eng katta afzalligi ham aynan ushbu tamoyilga tayangan holda ma’lumotlar yaxlitligi va ishonchliligini ta’minlash imkoniyatiga ega bo‘lishidadir.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Naveenkumar, R. (2020-yil noyabr). *The Persistence of Blockchain Technology using Digital Signature and Hash Functions*. International Journal of All Research Education and Scientific Methods (IJARESM), 8(11). ISSN: 2455-6211.
2. Swathi, E., Vivek, G., & Rani, G. S. (2016). *Role of Hash Function in Cryptography*. National Conference on Computer Security, Image Processing, Graphics, Mobility and Analytics, Hindiston, 10–13-betlar.
3. Kuznetsov, A., Oleshko, I., Tymchenko, V., Lisitsky, K., Rodinko, M., & Kolhatin, A. (2021). *Performance Analysis of Cryptographic Hash Functions Suitable for Use in Blockchain*. International Journal of Computer Network and Information Security (IJCNIS), 13(2), 1–15. https://doi.org/10.5815/ijcnis.2021.02.01
4. Seok, B., Park, J., & Park, J. H. (2019). *A Lightweight Hash-Based Blockchain Architecture for Industrial IoT*. Applied Sciences, 9(18), 3740. https://doi.org/10.3390/app9183740
5. Atlam, H. F., Alenezi, A., Alassafi, M. O., & Wills, G. B. (2018). *Blockchain with Internet of Things: Benefits, Challenges, and Future Directions*. International Journal of Intelligent Systems and Applications, 10(6), 40–48.

muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

Ingliz tili muharriri: Feruz Hakimov

Musahhih: Zokir Alibekov

Sahifalovchi va dizayner: Iskandar Islomov

2025. № 12

"Muhandislik va iqtisodiyot" jurnali 26.06.2023-yildan
O'zbekiston Respublikasi Prezidenti Adminstratsiyasi huzuridagi
Axborot va ommaviy kommunikatsiyalar agentligi tomonidan
№S–5669245 reyestr raqami tartibi bo'yicha ro'yxatdan o'tkazilgan.
Litsenziya raqami: №095310.

Manzilimiz: Toshkent shahri Yunusobod tumani 15-mavze 19-uy

+998 93 718 40 07 https://muhandislik-iqtisodiyot.uz/index.php/journal t.me/yait_2100