UDK 681.3.06

Axatov A.R., Nazarov F.M.

Cheklangan va kechikish sharoitlardagi tizimlarda taqsimlangan reestr (blokcheyn) texnologiyalari asosida ma’lumotlar ishonchliligini ta’minlash

Annotatsiya. Ma’lumotlar oqimini keskin ortishi va ularni tezkor qayta ishlash muammosi hozirgi kunda ma’sul soha vakillari uchun asosiy vazifa bo’lib qolmoqda. Shundan kelib chiqib kompyuter tarmoqlaridagi ma’lumotlarni saqlash va qayta ishlash jarayonini optimallashtirish maqsadida taqsimlangan reestr texnologiyalarni qo’llash va blokcheyn texnologiyasi asosida ishlov beriladigan ma’lumotlarni kriptografik maxfiylashtirish qarab o’tilgan. Blokcheyn texnologiyasi asosida cheklovlar va kechikish sharoitlaridagi jarayonlarni aks etadigan tizimlar ma’lumotlarini qayta ishlash va ularning ishonchliligini oshirish usul va algoritmlari ishlab chiqilgan.

***Kalitli so’zlar*:** kompyuter tarmoqlari, blokcheyn, ma’lumotlar ishonchliligi, cheklovlar va kechikish, shifr funksiya, kriptografik shifrlash.

Mavzuning dolzarbligi va masalaning qo’yilishi. Hozirgi vaqtda axborot tizimlari va texnologiyalarini takomillashtirish hamda ularni himoyalash usul va algoritmlarini ishlab chiqishga, ularni takomillashtirishga alohida e’tibor qaratilmoqda. Respublikamizda axborot texnologiyalarni rivojlantirish va ularni ishlab chiqarish, fan, ta’lim va sport sohalariga joriy etish bo’yicha yetakchi rivojlangan mamlakatlar tajribasiga tayangan holda taqsimlangan reestr ya’ni blokcheyn texnologiyalari yordamida hal etish bu sohani bir muncha sifat darajasini oshirishga xizmat qiladi. Hozirda axborot oqimi va hajmining keskin ortishi bilan bu axborotlarning qayta ishlash va ularning xavfsizligini ta’minlash muammosi ham yetarli darajada ortib bormoqda. Bunday muommolarni hal etishda korxona va tashkilotlarning cheklangan holatdagi sharoitga ega hujjat almashinuv tizimlarining ma’lumotlar bazasi va ish jarayonini blokcheyn texnologiyasini qo’llash asosida hal etish mumkin. Bu texnologiyalarni qo’llash asosida ma’lumotlarni qayta ishlashni optimallashtirishning yangicha yondashuv asosida ma’lumotlarni yig’ish, uzatish, saqlash va qayta ishlash usullarini ishlab chiqish, tanlangan ilmiy tadqiqot ishining dolzarb va istiqbolli yo’nalishlaridan biri hisoblanadi.

Tizimdagi cheklovlar va kechikishlar – bu tarmoq tizimlarida topshiriqlar va vazifalarni bajarish jarayonida qa’tiy muddatlar belgilanadi, ammo ijro etilish vaqtida muddatlarning kechikish holatlari hamda parametrlari mavjud bo’lgan jarayonlar tushuniladi. Bunday jarayonli tizimlarga ta’lim shartnoma to’lov holatini monitoring qilish, kommunal to’lovlarni monitoring qilish va boshqalar kirishi mumkin. Shu munosabat bilan, tashkilotlarning ma’lumotlar aylanish tizimlari - belgilangan vaqt ichida vazifalarni bajarmaslik hamda kechikishlar bilan ishlov berish jarayonini cheklovlar va kechikish sharoitlaridagi tizimlar deb ataymiz (CHKT) [4].

Cheklangan va kechikish sharoitlaridagi tizimlarda qayta ishlanadigan ma’lumotlar hajmining ortib borishi, ularning tarmoq tizimlarida qayta ishlash va xavfsizligini oshirish uchun zamonaviy blokli shifrlash algoritmlari asosida taqsimlangan reestr texnologiyalarini qo’llash masalasi qarab o’tiladi.

Uzining texnologik mohiyatiga ko’ra blokcheyn texnologiyasidan foydalanish turli sub’ektlarni huquqiy qobilyati yoki maqomini tasdiqlovchi u yoki bu registrlarga yuridik ishonchli yozuvlarni kiritishdan iborat bo’lgan davlat ma’muriy proseduralarini avtomatlashtirish sohasida keng istiqbolli bo’lib xizmat qiladi [1,2]. Blokcheyn texnologiyasining ommaviyligini oshishi ma’lumotlar bazasining himoyasi uchun markazlashmagan texnologiyalardan foydalanishga yo’naltirilishi, xavfsizlik masalalari bilan bog’liq bajarilayotgan amallarning o’zgaruvchanligi va bajarilishining kamayishini ta’minlash bilan ham belgilanadi. Blokcheyn texnologiyalari va prinsiplari, ularni amalga oshirishda tez o’zgarayotgan «raqamli dunyo» sharoitlarida qo’llashning maksimal ochiqligi va ko’p variantliligiga erishishga imkon beradi.

Shu qatorda tarmoq texnologiyasi asosida ishlaydigan axborot tizimlarida ma’lumotlar ishonchliligini ta’minlashda taqsimlangan reestr texnologiyalaridan foydalanish axborot ishonchliligini ta’minlashning yangicha yondashuvi hisoblanadi. Bu yondashuvning ishlash jarayoni va mexanizmlarining algoritmlarini ishlab chiqish esa dolzarb tadqiqot mavzusini kasb etmoqda.

Blokcheyn texnologiyasi qo’llanilishida bloklar internet tarmog’ida taqsimlanishiga qaramay, aslida har bir ma’lumot tarmoqning ixtiyoriy joyida blok tarkibiga kirish uchun shifrlanishi va shu tufayli kirish ma’lumotlarini xavfsiz saqlanishiga imkonlar mavjud bo’ladi [4]. Bu yerda kriptografiyaning eng samarali shifrlash metodlaridan foydalaniladi. Masalan, shifrlashning yopiq kaliti dinamik ravishda blok zanjirining tugunlariga bog’liq holda tanlanganda, ma’lumotlar bazasiga ruxsat etilmagan shaxslar hujum qilsa bunda zanjir tarkibidagi ma’lumotni ochish uchun zanjirning har bir tugunini ochib chiqishiga to’g’ri keladi. Bu jarayon esa albatta juda ko’p vaqtni ta’lab etadi va bu vaqtda qo’lga kiritishi lozim bo’lgan ma’lumot foydasiz hisoblanadi. Natijada bloklar zanjiri o’zining har qanday internet foydalanuvchilariga erkin tartibda ma’lumotlarni xavfsiz uzatishni ta’minlashi mumkin.

Blokcheyn texnologiyasidan foydalanish xavfsizligining asosiy xususiyati - tizim tarkibidagi ma’lumotlar markazlashtirilmagan holda saqlanishidir. Agar bitta foydalanuvchi serverida joylashgan ma’lumotlar bazasi nazariy jihatdan buzilsa, faqat ushbu foydalanuvchi ma’lumotlariga ta’sir qiladi, bundan kelib chiqadiki bu texnologiyaning xavfli tuynuklari mavjud bo’lmaydi. [2]. Bunda faqat shaxsiy foydalanuvchilarning shaxsiy kalitlarini o’g’irlashga urinish imkoniyati qoladi bu esa yetarli darajada katta foyda keltirmaydi. Texnik jihatdan bunday blokli uzatish to’liq xavfsiz hisoblanadi. Ushbu jarayonda ko’plab kompyuterlar ishtirok etishi mumkin va ularning har birida blokning ruxsat etilgan nusxasi mavjud bo’ladi. Bosqichlardan biri muvaffaqiyatsiz bo’lsa, zararlangan qismni uzib, blokni yana uzatish kifoya bo’lib qoladi. Blok tarkibidagi har bir ma’lumot shifr funksiya yordamida maxfiylashtiriladi, har bir shifr noyob hisoblanadi, keyingi operatsiyani hisoblashda avvalgisiga hech qanday aloqasi bo’lmagan boshqa bir parametr yaratiladi. Shifr funksiyada boshlang’ich parametrni tiklash mumkin emas yangi shifr kalitning chastotasi formulalar darajasida o’rnatiladi, faqat ma’lum bir tizim yaratuvchisi uni o’zgartirishi mumkin bo’ladi.

Blokcheyn texnologiyasini rivojlanish istiqbollarining imtiyozlaridan biri foydalanuvchining foydalanish ro’yxatini e’tiborsiz qoldirishga yo’l qo’yilmasligi va bu texnologiyani global darajada joriy etishda, porloq istiqbollarni yuzaga

keltiradi. Blokcheyn bir vaqtning o'zida quyidagi bir nechta muammolarni hal qilishga imkon beradi:

- Kuchli serverlarga, maxsus ma'lumotlarni saqlash komplekslariga ehtiyoj yo'qligi sababli moddiy xarajatlarni kamaytirish;
- Moliyaviy tartib-qoidalar uchun vaqtni sezilarli darajada pasaytirish;
- Respublikadagi barcha ijtimoiy jarayonlarni yagona xavfsiz tarmoqga biriktirgan holda ma'lumotlar bazasini yaratish.

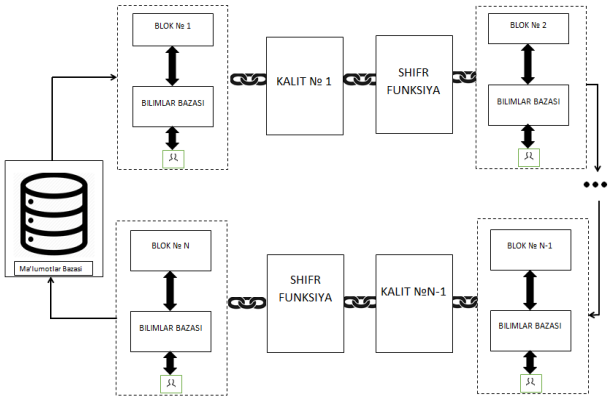
Shundan kelib chiqadiki ma'lumotlar bazasining xavfsiz holda yaratish uchun bu texnologiya tizimdagi barcha foydalanuvchilarni qonunga rioya qilishga majbur qiladi, chunki har qanday operatsiyalar ochiq tarzda amalga oshiriladi [3].

Tarmoq tizimidagi ma'lumotlarga blokcheyn texnologiyasini qo'llash algoritmini ishlab chiqish

Blokcheyn texnologiyasi ma'lumotlarni markazlashmagan va kriptografik bloklangan tarmoqda saqlashga mo'ljallangan. Bu texnologiya asosan shu vaqtgacha amaliyotda raqamli iqtisodiyotning rivojlantirishga xizmat qilib kelgan, unda har bir amalga oshirilgan tranzaksiyadan uning egasi manfaatdor hisoblangan. Tarmoq tizimlarida bu texnologiya ma'lumotlar almashinuvida ularning xavfsizligini barqarorlashtirishga xizmat qiladi. Yuqorida keltirilgan tamoillar va mexanizmlardan kelib chiqib axborot tizimlarining ma'lumotlar bazasini blokcheynda yaratish algoritmini ishlab chiqamiz. Ma'lumotlarni bloklarda saqlash asosida ularning xavfsizligini barqarorlashtirish mexanizmi 1-rasm ko'rinishida amalga oshirilishi mumkin.

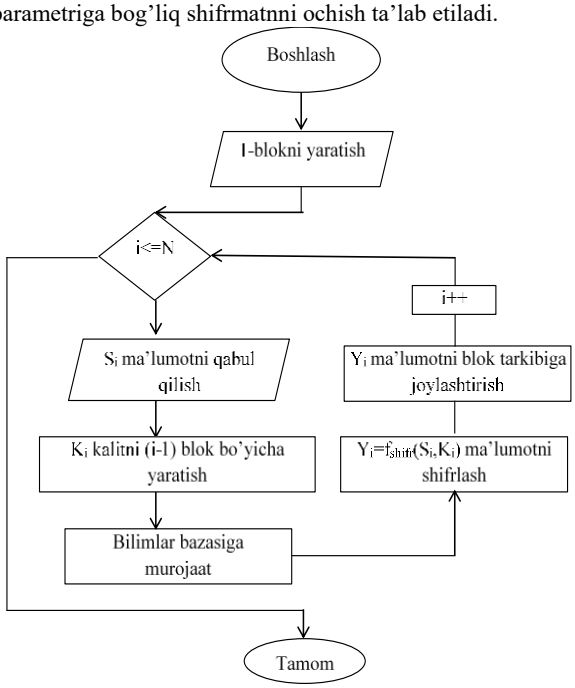
Yuqoridagi 1-rasmda tasvirlangan jarayon ma'lumotlarni zanjir shaklida dinamik kalitli kriptografik usul bilan saqlashni tashkil qiladi. Bunda har bir blok tarkibida saqlangan ma'lumot uzidan oldingi blok tarkibidagi ma'lumotning parametri bo'yicha maxfiylashtirilgan hisoblanadi [4]. Bilimlar bazasi tarkibida blok yaratilishi va maxfiylashtirilishi uchun xizmat qiladigan usul hamda algoritmlar mavjud bo'ladi. Tarmoqdagi axborot tizimlarining ma'lumotlar bazasi blokcheyn texnologiyasi asosida quyidagi algoritm bo'yicha yaratiladi:

1) dastlabki blok yaratilgan hisoblanadi;
2) har bir *n* – blok kaliti (*n-1)* – blok tarkibidagi ma'lumotning parametri bo'yicha yaratiladi;
3) har blok tarkibiga saqlanadigan ma'lumot yaratilgan kalit bo'yicha kriptografik usullar yordamida maxfiylashtiriladi;
4) shifrlangan ma'lumot blok tarkibiga joylashtiriladi.



1 – rasm. Kriptografik metodli blokcheyn texnologiyasi asosida ma'lumotlar bazasini shakllantirish

Ishlab chiqilgan algoritm bo'yicha yaratilgan ma'lumotlar bazasi tarkibidagi ma'lumotning xavfsizligi yuqori darajada ishonchli hisoblanadi. Ma'lumotlar bazasini tashkil qilish jarayonida bilimlar bazasiga murojaat asosida kriptografik usul tanlanishi quyidagi blok sxemali algoritm kurinishida tashkil qilinadi. Ruxsat etilmagan foydalanuvchi yoki tizimlar tomonidan ma'lumotlar bazasiga buzib kirilgan vaqtda bu ma'lumotlardan foydalanish imkoni bo'lmaydi, chunki ma'lum bir *n*-blok ma'lumotiga ega bo'lishi uchun *n-1* - blok parametriga bog'liq shifrmatnni ochish ta'lab etiladi.



Algoritmda keltirilgan *N* ma'lumotlar bazasining shu momentdagi oxirgi foydalanuvchisi hisoblanadi. Ishlab chiqilgan algoritm asosida axborot tizimlarining butun ma'lumotlar bazasini blokcheyn asosida yartish imkoniyatini beradi. Yaratilgan algoritm asosida ma'lumotlar bazasini shakllantirish, ma'lumotlar bazasi xavfsizligini ta'minlashga xizmat qiladi.

Blokcheyndagi ma'lumotlarni kriptografik shifrlashning matematik modeli

Tarmoq tizimlaridagi ma'lumotlar bazasini blokcheyn texnologiyasi asosida ishlab chiqishning asosiy mohiyati bu ma'lumotlar xavfsizligini oshirish hisoblanadi. Tadqiqotlar natijasida blokcheyn texnologiyasi tarkibiga yuqorida ishlab chiqilgan algoritm bo'yicha kriptografik shifrlash funksiyasi zamonaviy blokli shifrlash usuli asosida yaratildi. Zamonaviy blokli shifrlash usuli hisoblangan AES (Rijndael) usuli kalit uzunligi 128, 192 yoki 256 bit va blok o'lchami 128 bitdan iborat bo'lgan bazaviy blokli shifrlashga asoslangan [5,6]. Bu usul tarkibidagi shifrlash kalitini dinamiklashtirish asosida dinamik blokli algoritm ishlab chiqildi.

Dinamik blokli algoritm tarkibidagi shifrlash bayt bilan ya'ni 0 dan 255 gacha raqamlar yoki 8 bitli ikkilik raqamlar bilan ishlaydi. Shifrlash algoritmidagi barcha baytlar $F(2^8)$ oxirgi maydonning elementlari sifatida qaraladi. *F* - bu maydonning cheklangan sonli ixtiyoriy elementlar to'plamidan iborat. Maydondagi har bir elementlar uchun ikkita ikkilik operatsiyalar belgilanadi, ya'ni ikkita maydon elementlarini qo'shish va ikkita maydon elementlarini ko'paytirish natijada maydon elementlari yaratiladi. Maydondagi elementlar orasida 0 element mavjud bo'lsa, unga har qanday element qo'shilishi natijasida bir xil elementni va ko'paytirish orqali har qanday element 0 elementni beradi. Maydondagi elementlar orasida birlik element mavjud bo'lib, natijada har qanday element o'sha elementning o'zini qaytaradi. Maydonning har bir elementi uchun multiplikativ ravishda teskari element mavjud bo'lib, uning natijasi birlik elementga olib keladi [6, 8].

Dinamik blokli algoritmida baytlar ustida amallar bajariladi, unda $F(2^8)$ maydonning elementlari ko'phad sifatida ifodalanishi mumkin, bunda ko'phadning darajasi 7 dan katta bo'lmaslik lozim.

Baytlar

$$A=\{a_7,a_6,a_5,a_4,a_3,a_2,a_1,a_0\}, a_i \in \{0,1\}, i=\overline{0...7}$$

ko'rinishida tasvirlansa, u holda maydon elementlaridan tashkil topgan ko'phad (1) formula ko'rinishida yoziladi.

$$a(x)=a_7x^7+a_6x^6+a_5x^5+a_4x^4+a_3x^3+a_2x^2+a_1x^1+a_0x^0, (1)$$

Agar $a_i=\{11010101\ \}$ ko'rinishda bo'lsa, u holda ko'phad $x^7+x^6+x^4+x^2+1$ ko'rinishda bo'ladi. $F(2^8)$ maydonning elementlari uchun qo'shish va ko'paytirish amallari aniqlangan hamda ular additivlik va multiplikativlik xossalarga ega [7].

Dinamik blokli algoritm bajarilishida ko'phadlarni qo'shish ($\oplus$) XOR amali orqali amalga oshiriladi. Bu amalni ikkilik hamda o'n oltilik sanoq sistemalarida quyidagicha amalga oshirish mumkin:

$$AB_{16} \oplus D6_{16} = 7D_{16},\ \{11101011\ \} \oplus \{11010110\ \} = \{00111101\ \}_2$$

Chekli maydonda ixtiyoriy nolga teng bo'lmagan *a* element uchun unga teskari bo'lgan *–a* element mavjudligidan *a+(-a)=0* tenglik o'rinli bo'ladi, bu erda nol element sifatida *{00}*$_{16}$ qaraladi va $a \oplus a = 0$ tenglik $F(2^8)$ maydonda o'rinli deb hisoblanadi.

Shifrlash algoritmi tarkibida ko'phadlarni ko'paytirish quyidagi ko'rinishda bajariladi:

a) Ko'phad o'nlik sanoq sistemasida ko'paytiriladi;

b) Darajasi katta bo'lgan ko'phadlar (yettinchi darajadan) sakkizinchi darajali ko'phadga bo'lganda yetti va undan past darajali ko'phad paydo bo'ladi, unda bo'lish jarayonidagi ayirish amali ikkilik sanoq sistemasida $\oplus$ amali asosida amalga oshiriladi.

Ko'paytirish amalini $\bullet$ bilan ifodalanib yuqoridagi ko'paytirish algoritmi asosida ko'phad $a_6x^7+\ldots+a_2x^1+a_1x^0$ ko'rinishga keltiriladi. Bunda *x time ( )* funksiya yuqorida takidlangan ko'paytirish amaliga nisbatan berilgan ko'phadni *x* ga ko'paytirishni ifodalaydi. Bu funksiyani *n* marta qo'llab x^n ga ko'paytirish amali bajariladi. {57}$\bullet${13} = {fe}. Bunda {57}$\bullet${13}={57}$\bullet$({01} $\oplus$ {02} $\oplus$ {10})={57} $\oplus$ {ae} $\oplus$ {07}={fe} orqali amalga oshiriladi.

Yuqorida keltirilgan algoritm to'rt baytli so'zlar bilan quyidagicha amalga oshiriladi. To'rt baytli so'zlarni koefisentlari *F(2^8)* chekli maydondan olingan, darajasi uchdan katta bo'lmagan ko'phad (2) ko'rinishida ifodalash mumkin:

$$a_3x^3+a_2x^2+a_1x^1+a_0x^0 \qquad (2)$$

Ikkita ko'phadlarni qo'shish jarayoni o'xshash hadlar oldidagi koeffisientlarni $\oplus$ amali orqali bajariladi, ya'ni:

$$a(x)+b(x)=(a_3\oplus b_3)x^3+(a_2\oplus b_2)x^2+(a_1\oplus b_1)x^1+(a_0\oplus b_0) \quad (3)$$

Ko'paytirish amali natijasi to'rt baytli so'zdan iborat bo'lishi uchun, uchinchi darajadan katta bo'lgan har qanday ko'phad uchun $x^i \bmod (x^4+1)=x^{i \bmod 4}$ formula o'rinli bo'ladi. Natijada, *a(x)*va *b(x)* ko'phadlarni $\oplus$ kupaytmasini ifodalovchi

$$d(x)=a(x)\oplus b(x)=d_3x^3+d_2x^2+d_1x^1+d_0 \quad (4)$$

formulaga ega bo'lamiz [9,10].

Yuqorida takidlanlgan amallar quyidagi (5) matrisa ko'rinishida tasvirlanadi:

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \bullet \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} \qquad (5)$$

Kvadrat arxitekturaga ega kriptografik usul blokli shifrlash algoritmi o'zgaruvchan uzunlikdagi kalitlar orqali shifrlanadi. Kalit va blok uzunliklari bir-biriga bog'liq bo'lmagan holda 128, 192 yoki 256 bit bo'ladi.

Maxfiylashtiriladigan ya'ni shifrlash uchun kiritilayotgan ma'lumot baytlari $S_{i,j}(i,j=0..3)$ ko'rinishida belgilanadi, ya'ni:

1-jadval

Tranzaksiya ma'lumotlar jadvali

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

Shifr kalit ham shunday kvadrat shaklda $k_{i,j}(i,j=0..3)$ ko'rinishida tasvirlanadi. Ular 128 bit = 16 bayt = 4 so'z (to'rtta 32 bitlik blok)dan iborat:

2-jadval

Shifrlash kaliti jadvali

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$

Kriptografik shifrlash algoritmi tarkibidagi raundlar soni n_r, kirish bloklar o'lchami n_b hamda kalit uzunligi n_k larga bog'liq ravishda quyidagi jadvalga mos holda qo'llaniladi.

3-jadval

Shifrlash parametrlari jadvali

n_r	n_b=4, 128 bit	n_b=6, 192 bit	n_b=8, 256 bit
n_k=4, 128 bit	10	12	14
n_k=6, 192 bit	12	12	14
n_k=8, 256 bit	14	14	14

Har bir raund shifrlash jarayonlari quyida keltirilgan algoritm asosidagi akslantirishlardan foydalanilgan holda amalga oshiriladi:

1) SubBytes – algoritmda qayd etilgan 16x16 o'lchamli jadval asosida baytlarni almashtirish, ya'ni S -blok akslantirishlarini amalga oshirish;

2) ShiftRows – algoritmda berilgan jadvalga ko'ra holat baytlarini siklik surish;

3) MixColumns – ustun elementlarini aralashtirish, ya'ni algoritmda berilgan matrisa bo'yicha akslantirishni amalga oshirish;

4) AddRoundKey – raund kalitlarini qo'shish, ya'ni bloklar mos bitlarni XOR amali bilan qo'shish.

Ishlab chiqilgan shifrlash algoritm asosida shifrlash funksiyasi yaratiladi va bu funksiya har bir amalga oshiriladigan tranzaksiyani maxfiylashtirishga xizmat qiladi. Maxfiylashtirilgan ma'lumotlarning shifr kaliti zanjir tartibida dinamik o'zgarib boradi, bu esa o'z o'zidan kalitni oshkorlashtirish imkoniyati yo'qligini ko'rsatadi.

Eksprement natijasi. Tadqiqot ishining amaliy qo'llanilishi bo'yicha eksperimentlar tashkil etildi va natijalar

tahlili bajarildi. Eksperiment ishida, tarmoq tizimlaridagi ma'lumotlar bazasini kriptografik usul bilan blokcheyn texnologiyasi yordamida shakllantirish hamda serverlar tarkibidagi mavjud usul yordamida shakllantirish jarayonlari taqqoslanib o'tilgan. Axborot tizimi sifatida oliy ta'lim shartnoma to'lov jarayonini monitoring qilish tizimi va elektron xujjat almashinuv tizimi tanlab olindi.

Axborot tizimining ishlash jarayonida kun, oy va yil mobaynida amalga oshiriladigan tranzaksiyalar hajmidan kelib chiqib har bir sekund bo'yicha yuqoridagi ishlab chiqilgan algoritmlar yordamida amalga oshiriladigan tranzaksiyalar va ularning samaradorligi aniqlandi.

4-jadval

Tadqiqot eksprementi jadvali

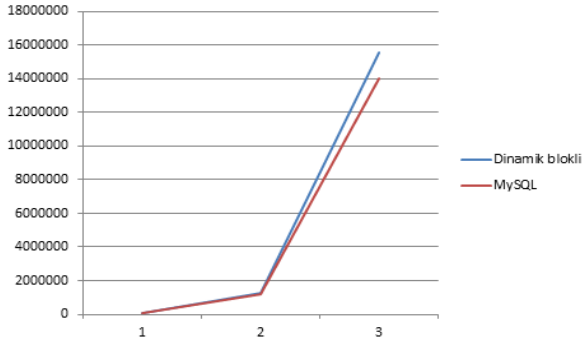
Muddat	Sekund	x_i	$\overline{x}_i$	$\overline{y}_i$
Kun	*86400*	*43200*	*38880*	*0,1*
Oy(30 kun)	*2592000*	*1296000*	*1166400*	*0,1*
Yil	*31104000*	*15552000*	*13996800*	*0,1*

Serverlar ya'ni MySQL tarkibidagi mavjud xavfsizlik usuli yordamida amalga oshiriladigan tranzaksiyalar x_i va kriptografik usul yordamida amalga oshiriladigan tranzaksiyalar $\overline{x}_i = 0{,}9x_i$ parametrlar orqali ifodalanadi. Bunda o'rtacha har ikki sekundda bitta tranzaksiya amalga oshirilishi nazarda tutilgan bo'lib tranzaksiyalarning samaradorligi (6) orqali aniqlanadi.

$$\overline{y}_i = \frac{|x_i - \overline{x}_i|}{x_i} \qquad (6)$$

Ishlab chiqilgan blokcheynga asoslangan kriptografik usul va server tarkibidagi mavjud usul yordamida amalga oshiriladigan tranzaksiyalar qiyosiy tahlil natijalari 2-rasmda grafiklar bilan tasvirlangan.

Kriptografik metodli blokcheyn texnologiyasi asosida ishlab chiqilgan usul bilan ma'lumotlar bazasini shakllantirishda, serverlar tarkibidagi xavfsizlikni ta'minlash uchun mavjud usullarga nisbatan yuqori darajali kompyuterlar ta'lab etiladi. Ishlab chiqilgan usul yordamida tranzaksiyalar hajmi vaqtga nisbatan kamroq amalga oshirilishi mumkin, ammo ishlab chiqilgan algoritm asosida amalga oshirilgan tranzaksiyalarning xavfsizlik darajasi ancha mukammal hisoblanadi.



2-rasm. Tranzaksiyalarning amalga oshirilishi

Xulosa. Bajarilgan tadqiqot ishida kriptografik metodli blokcheyn texnologiyasini tarmoq texnologiyalaridagi tizimlarning ma'lumotlar bazasini shakllantirish va tizim tarkibidagi ma'lumotlar xavfsizligini oshirishga xizmat qiladi. Zamonaviy kriptografik usullar yordamida ishlab chiqilgan algoritm asosidagi blokcheyn texnologiyasi, tarmoq tizimidagi ma'lumotlar xavsizligini ta'minlash uchun asosiy vosita hisoblanadi. Blokcheyn texnologiyasi asosida ma'lumotlarni saqlash ularni kriptografik shifrlash jarayonida vaqt rejimidan yutqazmaslik uchun amaliyotda yuqori darajali serverlar va super kompyuterlar bo'lishi ta'lab etiladi.

Foydalanilgan adabiyotlar

1. Wang L., Shen X., Li J., Shao J., Yang Y. Cryptographic primitives in blokcheyns. Journal of Network and Computer Applications, vol. 127, pp. 43 – 58, 2019.

2. Duffield E., Schinzel H., Gutierrez F., Transaction locking and masternode consensus: A mechanism for mitigating double spending attacks. CryptoPapers.info, 2014, [Online; accessed 3-Jun-2019].

3. Pedro Franco. The Blokcheyn. Understanding Bitcoin: Cryptography, Engineering and Economics. John Wiley & Sons, 2014. 288 p.

4. Ахатов А.Р., Назаров Ф. М. Методы реализации технологии блокчейн на основе криптографической защиты для системы обработки данных с ограничением и запаздыванием в электронном документообороте. Вестник компьютерных и информационных технологий. Международный научный журнал. № 10, 2019

5. Винтова Т. А. Интернет-технологии предоставления услуг по автоматизации процессов управления предприятиями. Славянский форум. 2017. № 1(15).С. 263 – 273.

6. Dam K.W., Lin H. S. Cryptography's Role in Securing the Information Society. National Academy Press. Washington, D.C. 1996.

7. Коблиц. Н. Курс теории чисел и криптографии - М., Научное издателство ТВП, 2001 г., 260 стр.

8. Масленников. Практическая криптография БҲВ – СПб 2003

9. Шнаер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке С. Триумф. 2002.

10. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком. 2002.

A.R.Axatov. Samarqand davlat universiteti t.f.d, professor.

F.M.Nazarov, Samarqand davlat universiteti tayanch doktorant

Ensuring the reliability of information based on the distributed register technologies (blockchain) in systems with the conditions of restrictions and delay

Abstract: Sharp increase of the data flow and the problem of their processing today remains one of the main tasks solved by specialists of information technology. In this regard, the issues of using distributed registry technology are considered to optimize the storage and processing of information in computer networks, as well as methods of cryptographic encryption of information processed by blockchain technology. Methods and algorithms have been developed for processing and increasing the reliability of systems information that reflect processes in the conditions of restrictions and delays based on blockchain technology.

Key words: computer networks, blockchain technology, information reliability, restriction and delay, encryption function, cryptographic encryption.