A.A. Saidov, J.T.Usmonov

ELEKTRON HUKUMAT TIZIMLARIDA BLOKCHEYN TEXNOLOGIYALARINI QO‘LLASH ASOSLARI

O‘ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI
MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

A.A. Saidov, J.T.Usmonov

ELEKTRON HUKUMAT TIZIMLARIDA BLOKCHEYN TEXNOLOGIYALARINI QO‘LLASH ASOSLARI

O‘quv qo‘llanma

O‘zbekiston Respublikasi Oliy va o‘rta-maxsus ta’lim vazirligi huzuridagi Muvofiqlashtiruvchi kengash tomonidan 5A330502 – “Elektron hukumat tizimini boshqarish” magistratura ta’lim yo‘nalishida tahsil olayotgan talabalar uchun o‘quv qo‘llanma sifatida tavsiya etilgan.

O‘zbekiston Respublikasi Oliy va o‘rta maxsus ta’lim vazirligining Muvofiqlashtiruvchi kengashi tomonidan o‘quv qo‘llanma sifatida tavsiya etilgan

«Mahalla va oila nashriyoti»
Toshkent 2021

UO'K: 004:339.543(075.8)
BBK: 32.81
S 21

A.A. Saidov, J.T. Usmonov. Elektron hukumat tizimlarida blokcheyn texnologiyalarini qo'llash asoslari // Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti. –T., 2021. -142 b.

O'quv qo'llanma blokcheyn texnologiyasi tarafdorlari va uning muxoliflari fikrlarini inobatga olgan holda elektron hukumat tizimida blokcheyn texnologiyalarini qo'llash imkoniyatlarini o'rganishning dastlabki qadamlariga bag'ishlangan. Blokcheyn tizimlarida tranzaksiyalarning ishonchliligini nazorat qilish usullari, blokcheyn texnologiyasi elementlarini amaliyotga joriy etish va bojxona idoralari misolida axborot tizimlar orqali foydalanuvchilar o'rtasida axborot almashish, elektron raqamli imzoni ikki karra qo'llash algoritmlarini ishlab chiqish bo`yicha ko`nikma hosil qilishga qaratilgan.

O'quv qo'llanma 5A330502 – "Elektron hukumat tizmini boshqarish" mutaxassisligida tahsil olayotgan magistratura talabalari uchun mo'ljallangan.

Taqrizchilar:

Jumanov J.X. - t.f.d., professor. Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti, "Kompyuter tizimlari" kafedrasi mudiri.

Ubaydullaeva Sh.R. - t.f.n., Toshkent irrigatsiya va qishloq xo'jaligini mexanizatsiyalash muhandislari instituti, "TJAIChAB" kafedrasi dotsenti.

ISBN 978-9943-7778-4-2

Mundarija

Kirish

Bugungi kunda axborotni birinchi manbaidan to so'ngi manziligacha ishonchli himoyasini ta'minlash texnologiyalaridan biri "Blokcheyn tizimlari" texnologiyasi hisoblanadi. Blokcheyn texnologiyasi (Blockchain yoki tranzaksiya bloklari zanjiri) paydo bo'lgan kunidan boshlab darhol maxsus va ommaviy axborot vositalaridagi keng ko'lamli muhokamalarda o'ziga katta e'tibor tortdi. Ba'zi uning muxlislari hatto blokcheynni Internet paydo bo'lganidan buyon paydo bo'lgan eng katta ixtiro deb e'lon qilishdi. Shu sababli, keyingi bir necha yil ichida blokcheyn haqida ko'plab kitoblar va maqolalar yozildi.

Hozirda "blokcheyn" deb nomlanadigan texnologiya 2008-yilda Satoshi Nakamoto (Satoshi Nakamoto) taxallusi ostida faoliyat yuritgan muallif tomonidan taklif qilingan.

Garchi Satoshi Nakamoto "bitkoin" kriptovalyutasi kodini e'lon qilgan va u har 1000 bitkoin uchun 0,003 dollar kurs bilan savdo qilingan bo'lsada, 2017-yil o'rtalariga kelib uning kursi har 1 "bitkoin" uchun 1800 dollardan ortdi va bir necha yuz ming martaga ko'paydi.

Biroq, blokcheyn tushunchasi va uning qo'llanilish sohasi ko'lami kriptovalyutanikiga nisbatan ancha kengroq. Taqsimlangan ro'yxatga olish (reyestr) texnologiyasining xususiyatlari, uni ko'pgina sohalarda - fayllarni uzatish tizimlaridan tortib mualliflik huquqlarini yana-da ishonchliroq himoya qilishgacha, masalan, san'at asarlari mualliflik huquqlarini himoya qilish, demokratik saylovlar tashkil etishdi foydalanishga imkon beradi.

Tabiiyki, blokcheyn texnologiyasi dastlab bank sektori e'tiborini tortgan. Agar ba'zi markaziy banklar blokcheyn asosidagi kriptovalyutaning erkin muomalasiga shubha bilan qarashayotgan bo'lsalarda, ularda blokcheyn texnologiyasining o'zi katta qiziqish uyg'otadi. Rivojlangan (AQSH, Buyuk Britaniya, YevroIttifoq) va rivojlanayotgan mamlakatlarning markaziy banklari (Xitoy, Rossiya va boshqalar) tijorat banklari bilan birgalikda blokcheynni o'rganish bo'yicha ishchi guruhlar tuzganlar.

Shu bilan birga, Yevropaning yirik banklari, *Hongkong and Shanghai Banking Corporation* (HSBC - Gonkong va Shanxay bank korporatsiyasi) boshchiligida, o'zaro ichki amaliyotda qo'llash uchun

blokcheyn asosidagi platformani ishlab chiqish bo‘yicha konsorsium tashkil etilishini e’lon qilishgan; Bank of America esa Microsoft kompaniyasi bilan birgalikda onlayn blokcheyn-platformasini yaratish bo‘yicha ish olib bormoqda. Rossiyada yirik tijorat banklari - “Sberbank”, “Tinkoff”, “Alfa” va boshqalar “marketcheyn” tizimini yaratishda ishtirok etdilar.

Blokcheynning asosiy tarafdorlari blokcheynning afzalliklari – uning benuqsonligi, ishonchliligi va bajariladigan amallarning to‘liq shaffofligi deb hisoblaydilar. Ko‘pincha mazkur texnologiyani oddiy bitimlar uchun ishlatish taklif etiladi. Smart-kontraktlar yoki aqlli shartnomalar esa bitimni amalga oshirish kafolatini beradi: shartnoma bo‘yicha amalga oshirilgan tranzaksiya yozuvlari blokcheynning markazlashtirilmagan reyestrida joylashadi va bitimning barcha ishtirokchilari undagi har qanday o‘zgarishlarni ko‘rib turadilar.

Boshqalar, blokcheynning muhim kamchiliklaridan biri “xato aniqlangan taqdirda, tuzilgan shartnomalarni tuzatish imkoniyatining yo‘qligi, bu shartnoma shartlarining noto‘g‘ri bajarilishiga yoki yuridik ahamiyatga molik harakatlarning keyingi barcha zanjirini bekor qilishga olib kelishi mumkin” deb hisoblashadi. Bunday holda muammoni barcha tomonlarning oldindan roziligi bilan, yangi shartnomani tuzish va ehtimol, eski shartnomani bekor qilish yo‘li bilan hal qilish mumkin bo‘ladi xolos. Bu esa blokcheyn texnologiyasi tarafdorlari e’lon qiladigan asosiy afzalliklardan biri – blokcheyn vaqt va moddiy xarajatlarini kamaytiradi degan da’volarini yo‘qqa chiqaradi.

Mazkur o‘quv qo‘llanma, blokcheyn texnologiyasi tarafdorlarining ham, uning muxoliflarining ham fikrlarini inobatga olgan holda, Elektron hukumat va elektron tijorat tizimlarida blokcheyn texnologiyalarini qo‘llash imkoniyatlarini o‘rganishning dastlabki qadamlariga bag‘ishlangan.

O‘quv qo‘llanmasini takomillashtirish yuzasidan bo‘lgan taklif va mulohazalarni mualliflar mamnuniyat bilan qabul qiladilar va oldindan minnatdorchilik bildiradilar.

1-BOB. BLOKCHEYN TIZIMLARI TUSHUNCHASI VA TEXNOLOGIK SXEMASI

Bugungi kunda Blokcheyn tizimlari tushunchasi juda fragmental, uzuq-yuluq - uning keng imkoniyatlari, uning atrofidagi media shov-shuvlar, uni amalga oshirishning texnik murakkabligi, ushbu texnologiyaning ilmiy asoslarini unga yopishgan asossiz eyforiyadan ajratib olishni qiyinlashtiradi.

Shunga qaramay, yirik biznes tomonidan Blokcheyn tizimlari texnologiyasini tadqiq qilishni keng miqyosda moliyalashtirish o‘z samarasini bermoqda: kundan-kunga Blokcheyn tizimlari tushunchasi va uning qo‘llanilish sohasi keng tushunilib, aniqlanib bormoqda.

Tarjimada blokcheyn (blockchain) so‘zlari bir-biri bilan bog‘langan bloklar zanjirini anglatadi, ushbu holatda esa u tranzaksiya bloklari zanjiri sifatida tushuniladi. Blokcheyn - bu to‘liq taqsimlangan hisobga olish jurnallarining (reyestrlarning) bir qatlamli tizimi bo‘lib, u tizimning yaxlitligini ta’minlash va saqlab qolish uchun, kriptografik va axborotlarni himoya qilishning keng miqyosli texnologiyalaridan foydalangan holda tartibga solingan, o‘zaro bog‘liq ma’lumotlar bloklari axborotini qayta ishlashga mo‘ljallangan algoritmlarni amalga oshiradigan *dasturiy modul* hisoblanadi.

Ushbu texnologiya, har bir amalga oshirilgan tranzaksiya qayd qilinadigan va tarmoqning barcha qatnashchilariga ma’lum bo‘ladigan, axborotning ommaviy depozitariysi, ya’ni taqsimlangan, markazlashtirilmagan, shifr bilan himoyalangan ma’lumotlar bazasi sifatida tavsiflanadi. Reyestrdagi har qanday tranzaksiya faqat tarmoq qatnashchilarining yarmidan ko‘pi tomonidan ma’qullangan taqdirdagina haqiqiy deb tan olinadi. Bu shuni anglatadiki, tizimning biron bir ishtirokchisi yoki tashqi agent ushbu tizim foydalanuvchilarning barchasi roziligini olmasdan qonuniy operatsiyani amalga oshira olmaydi [9].

Blokcheyn texnologiyasining keltirilgan ta’riflari “bir qatlamli tizim”, “dasturiy modul”, “o‘zaro bog‘liq tranzaksiyalar bloklari”, “kriptografik texnologiyalar”, “tizimning yaxlitligi”, “ommaviy depozitariy”, “ma’lumotlar bazasini shifrlash ”, “tarmoq ishtirokchilari” va boshqalar kabi bir nechta muhim so‘zlarni o‘z ichiga oladiki, bir qarashda ular blokcheyn tushunchani murakkablashtirib ko‘rsatadi.

Blokcheyn tizimlar faoliyatining texnologik sxemasini tushunish uchun avval ushbu texnologiya yordamida hal qilinishi mumkin bo‘lgan biror masalani ko‘rib chiqish foydali bo‘ladi.

“Mulkni boshqarish” masalasini keng ma’noda ko‘rib chiqish bunga misol bo‘lishi mumkin. Bu yerda ma’lum qiymatlarga ega bo‘lgan mulk sifatida - pul, mulk, ko‘chmas mulk, intellektual mulk obyektlari, axborot yoki boshqa obyektlar bo‘lishi mumkin. Mulkni boshqarish haqida gap ketganda, subyektdan subyektga o‘tuvchi mulkka bo‘lgan huquqning hayotiy sikli nazarda tutiladi. Shu bilan birga, mulk huquqini qabul qilish va topshirish bo‘yicha barcha amallar ishonchliligi va mustahkam asosga egalik darajasi noma’lum bo‘lgan elektron tizim asosida amalga oshiriladi deb qaraladi.

Blokcheynning asosiy vazifasi – shu ishonchliligi va mustahkam asosga egalik darajasi noma’lum, noma’lum miqdordagi ishtirokchilardan iborat bo‘lgan to‘liq taqsimlangan bir qatlamli tizimda yaxlitlikni ta’minlash va saqlashdan iborat.

1.1. Bir qatlamli axborot tizimlari va ularning amaliy ahamiyati

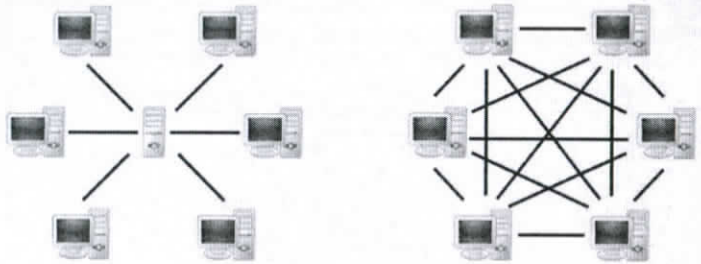
Bir qatlamli tarmoqlar - bu taqsimlangan tizimlarning muayyan turi hisoblanadi. Ular “tugun ”deb nomlangan alohida kompyuterlardan iborat bo‘lib, ularning hisoblash resurslariga ushbu tarmoqning barcha boshqa tugunlari hech qanday markaziy muvofiqlashtirish punktisiz kirishlari mumkin. Bunday tarmoqning barcha tugunlari tizimda teng huquqlarga va bir xil rollarga ega. Bundan tashqari, ularning barchasi ham resurslarni yetkazib beruvchilar hamda iste’molchilar hisoblanadilar.

Bir qatlamli tizimlar uchun fayllardan birgalikda foydalanish, kontentni tarqatish va shaxsiy maxfiy ma’lumotlarni himoya qilish kabi juda foydali qo‘llanish sohalari mavjud. Ushbu dasturiy ilovalarning aksariyati oddiy, ammo kuchli g‘oyadan, ya’ni har bir oddiy foydalanuvchi kompyuterini yagona taqsimlangan tizimni tashkil etadigan tugunlarga aylantirish g‘oyasidan foydalanadi. Natijada, bunday dasturiy muhitdan foydalanuvchilar yoki mijozlar qancha ko‘p bo‘lsa, tizim shunchalik yirik va kuchli bo‘ladi.

Bir qatlamli tizimlarning dasturiy ta’minoti ularning arxitekturasiga juda bog‘liq. Dasturiy tizimlarni amalga oshirishning ko‘plab usullari mavjud. Ammo tizimni amalga oshirish jarayonida

asosiy qarorlardan biri uning arxitekturasini, ya’ni uning tarkibiy qismlarini va ular o‘rtasidagi munosabatlarni tashkil qilish sxemalarini aniqlash bo‘lib hisoblanadi.

Dasturiy tizim arxitekturasining ikkita - markazlashtirilgan va taqsimlangan asosiy turlari mavjud (1.1-rasm). Markazlashtirilgan dasturiy tizimlarda, muayyan periferik komponentlar bilan ulanadigan bitta markaziy komponent ajralib turadi. Bunday sxemadan farqli o‘laroq, taqsimlangan tizimlarning tarkibiy qismlari, muvofiqlashtirish va boshqarish funksiyalariga ega bo‘lgan biron bir markaziy elementni ajratmasdan, o‘zaro bog‘liq elementlar tarmog‘ini hosil qiladi.



1.1-rasm. Taqsimlangan (o‘ngda) va markazlashtirilgan (chapda) tizimlar arxitekturalari

Alohida olingan kompyuterlarga nisbatan taqsimlangan tizimning asosiy afzalliklari quyidagilardan iborat:

- yuqori hisoblash quvvati;
- boshqaruv va boshqa qo‘shimcha xarajatlar kamayishi;
- yuqori ishonchlilik;
- tabiiy taraqqiyot imkoniyati.

Alohida kompyuterlarga qaraganda taqsimlangan tizimlarning kamchiliklari quyidagilar bo‘lib hisoblanadi:

- ishlarni muvofiqlashtirish xarajatlari ortishi;
- axborot almashishni tashkil etish xarajatlari;
- tarmoq muhitiga bog‘liqlik;
- dasturiy ta’minot murakkabligining yuqoriligi;
- xavfsizlik muammolari.

Bir qator ilmiy tadqiqotlarda, jumladan butun bir sanoat sohasini o‘zgartirib yuborgan bir qatlamli tizimga misol keltirilgan. U ham

bo‘lsa, musiqa sanoati. Ko‘p yillar davomida musiqa sanoati quyidagi sxema bo‘yicha ish olib borgan: musiqachilar, qo‘shiqlarni yozib oladigan, yozuvlarni turli xil tashuvchilarga - vinil, magnit lenta yoki kompakt disklarga ko‘chiradigan va ularga tovar ko‘rinishini beradigan studiyalar bilan shartnoma tuzardilar, keyin tashuvchilarning tovar nusxalari iste’molchilarga turli xil kanallar orqali, shu jumladan universal savdo markazlari va ixtisoslashtirilgan musiqa do‘konlari orqali sotilardi.

Aslida, ovoz yozish studiyalari musiqachilar va musiqa ixlosmandlari o‘rtasida vositachilik qilishgan. Ovoz yozish studiyalari prodyusserlikda, marketingda va musiqiy yozuvlarni tarqatish bo‘yicha muayyan bilimlari va amaliy tajribasi tufayli vositachilar sifatida ishtirok etishga qodir edilar.

Ammo XXI asrning birinchi o‘n yilligida ovoz yozish studiyalari ishlaydigan muhit tubdan o‘zgardi. Musiqiy yozuvlarni raqamlashtirish, arzon narxlarda yozib olish uskunalari paydo bo‘lishi, personal kompyuterlar sonining jadal o‘sishi, Internetning paydo bo‘lishi va jadal rivojlanishi - bularning barchasi ovoz yozish studiyalari endi musiqa sanoatining majburiy tarkibiy qismi bo‘lolmay qolishiga olib keldi.Endilikda studiyalarning uchta asosiy vazifasi - prodyusserlash, marketing, tarqatishni musiqachilar va iste’molchilarning o‘zlari bajarishi mumkin bo‘lib qoldi.Endi butun dunyo bo‘ylab ayrim musiqa fayllarini odamlar tomonidan hech qanday kompakt-disklarni sotib olmasdan birgalikda foydalanish imkoniyati tug‘ildi. Bir qatlamli tarmoq uslubi, aslida, iste’molchilarga har qachongidan ham kengroq assortimentdagi musiqalarni tinglash imkoniyatini beradigan, media-fayllar uchun ommabop, raqamli, ulkan savdo maydoniga aylandi. Shu bilan birga, ovoz yozish studiyalari ma’lum darajada bu ishdan chetlanib qoldi.

Shuni ta’kidlash kerakki, bu yerda musiqachilarning kompakt-disklarni donalab sotishdan ko‘ra ommaviy tanilishga bo‘lgan qiziqishlari muhim rol o‘ynadi. Ular, musiqiy yozuvlarni sotilishi natijasida ularga ovoz yozish studiyalari to‘lagan puldan ko‘ra ommaviy tanilishdan ko‘proq daromad ola boshladi.

Musiqiy industriyani shu qadar zaiflashtirgan va bir qatlamli tizimlarning tarqalishiga yordam beradigan asosiy xususiyatlari - musiqaning nomoddiy tabiati va ma’lumotlarni nusxalash va uzatish uchun kam xarajat sarflanishi edi.

Bir qatlamli tizimlarning imkoniyatlari musiqa sohasi bilan cheklanmaydi. Asosan nomoddiy yoki raqamli mahsulotlar yoki xizmatlarni ishlab chiqaruvchilar va iste’molchilar o‘rtasida vositachi rolini o‘ynaydigan har qanday faoliyat sohasini istalgan vaqtda bir qatlamli tizimga almashtirish mumkin.

Masalan, bizning bank hisob raqamimiz yoki kredit kartamizda nima saqlanadi? Haqiqiy pulmi? Yo‘q. Biz qo‘limizda ushlab turgan pullarimiz allaqachon nomoddiy bitlarga va baytlarga aylangan. Hozirda pul mablag‘larining oz qismigina jismoniy banknotlar va tangalar shaklida mavjud. Jahon pul mablag‘lari va aktivlarining juda katta qismi bitlar va baytlar shaklida, moliya industriyasining markazlashgan axborot tizimlarida ko‘zga ko‘rinmas shaklga aylangan.

Shu ma’noda olganda, ba’zi asarlar mualliflari, masalan, bir oz oldinga ketib, jahon moliya industriyasi faoliyatini istalgan vaqtda bir qatlamli tizimga almashtirish mumkin, banklar va boshqa ko‘plab moliyaviy soha namoyondalarini, hozir bizning pulimiz va farovonligimizni aks ettiradigan bitlar va baytlarning ishlab chiqaruvchilari va iste’molchilari o‘rtasidagi oddiy vositachilar deb baholashadi.

Biroq, bir narsani unutmaslik kerakki, banklar va boshqa moliyaviy soha muassasalari, yoki ko‘chmas mulkni yoki moddiy boyliklarni ro‘yxatga olish bilan bog‘liq bo‘lgan muassasalar musiqa industriyasi subyektlarining yuqoridagi misolda bo‘lgani kabi, faqatgina vositachilarigina emas. Vositachilik xizmatlaridan tashqari, ular yana bitta - ehtimol eng muhim xizmatni amalga oshiradilar – bu, taklif qilinayotgan mulk haqiqatan ham sotuvchiga, moliyaviy manba esa xaridorga tegishli ekanligini tasdiqlaydi va kafolatlaydi. Bu, hozirgi kunda oddiy bir qatlamli tizimlar hal qila olmaydigan moliyaviy amallarning juda muhim tarkibiy qismi hisoblanadi.

Biroq, bir qatlamli tizimlarning markazlashtirilgan tizimlarga nisbatan ustunligi, vositachilar orqali bilvosita o‘zaro aloqa qilish o‘rniga, shartnoma bilan bog‘langan hamkorlar o‘rtasida to‘g‘ridan-to‘g‘ri munosabat o‘rnatish imkoniyati, demak, axborotga ishlov berish vaqtlari qisqarishi va qo‘shimcha xarajatlarning kamligi bo‘lib qolaveradi.

1.2. Blokcheyn texnologiyalari – banklar transformatsiyasining innovatsion yechimi

So‘nggi yillarda zamonaviy axborot texnologiyalari hosilasi bo‘lgan blokcheyn va sun’iy intellekt imkoniyatlarining jahon taraqqiyotida tutgan o‘rni va ahamiyati ortib bormoqda.

Jumladan, raqamli iqtisodiyotni rivojlantirish yo‘nalishlaridan biri bo‘lgan “Blokcheyn” texnologiyasi davlat boshqaruvi tizimiga va boshqa jamoatchilik munosabatlariga ham asta-sekin joriy etilmoqda.

O‘zbekiston Respublikasi Prezidenti huzuridagi Loyiha boshqaruvi milliy agentligi tomonidan ishlab chiqilgan “Kripto-birjalar faoliyatini litsenziyalash tartibi to‘g‘risidagi Nizom”da blokcheynga quyidagicha ta’rif berilgan:

Blokcheyn – barcha ma’lumotlar ketma-ket qayd qilinadigan va bloklar bo‘yicha joylashtiriladigan taqsimlangan ma’lumotlar reestri, bunda har bir yangi blok oldingi blokka kriptografik imzo orqali bog‘lanadi.

Blokcheyn jamoatchilik o‘rtasida kriptovalyuta texnologiyasi sifatida tanilgan bo‘lsada, aslida blokcheyn turli maqsadlarda masalan: raqamli identifikatsiyalash, egalik va mulkiy huquqlar himoyasi va to‘lov tizimi sifatida ishlatilishi mumkin.

Shuningdek, blokcheyn texnologiyasining afzallik jihati operatsiyalar va tranzaksiyalarni amalga oshirish jarayonida shaffoflik, ishonchlilik, tezlik va barqarorlikni ta’minlash, tomonlarning hech qanday vositachisiz bitimlarni xavfsiz va ishonchli amalga oshirish imkonini berishidir.

Ta’kidlash lozimki, bugungi kunda blokcheyn texnologiyasini bank sohasida qo‘llash natijasida pul o‘tkazmalarini arzonlashtirish va tezlashtirish, ish samaradorligini oshirish, bank va mijozlarning maxfiy ma’lumotlarini himoya qilish va moliyaviy hamkorlikning yangi modellarini yaratish kabi imkoniyatlarni yaratish mumkin.

Banklarda blokcheyn texnologiyasini joriy etish bo‘yicha jahon tajribasi o‘rganilganda, ma’lum bo‘ldiki dastlab 2016 yilda Amerika qo‘shma shtatlari tomonidan moliyaviy operatsiyalarning xavfsizligini oshirish va xarajatlarini kamaytirish maqsadida foydalanilgan. Shu bilan birga, AQShning “JPMorgan Chase” investitsion banki “Aqlli shartnomalar”ni shartli saqlash orqali mulkiy huquq va qimmatbaho

aktivlarni tokenizatsiya qilish xususiyatiga ega “EthLab Quorum” xususiy blokcheyni ishga tushirgan.

Xususan, JPMorgan investitsion banki 2017 yilning oktyabrida 75 dan ortiq banklar bilan “Quorum” blokcheyniga asoslangan, bozorning barcha ishtirokchilari uchun bank operatsiyalarining maksimal darajada shaffofligini ta’minlaydigan “Banklararo Axborot Tarmog‘i”ni (IIN-Interbank Information Network) sinovdan o‘tkazgan.

AQShdagi Bank of America 2018 yilning aprel oyida shaxsiy ma’lumotlarni qayd etish va aniqlash, ma’lumotlar ba’zasiga kirgan har bir kishining hisobini yuritish, faqatgina vakolatli shaxslarga kirish imkonini beruvchi blokcheyn texnologiyasi asosida ishlovchi yangi tizim uchun AQSh Patent va savdo belgisi Byurosiga talabnoma topshirgan.

Blokcheyn texnologiyasini banklarda joriy qilish nafaqat AQShda balki Rossiyada so‘nggi yillarda ommalashib bormoqda. Bunga misol tariqasida Sberbank tomonidan ko‘chmas mulk bozoriga kiritilgan “DomKlik” onlayn xizmati keltirish mumkin.

O‘zbekistonda raqamli iqtisodiyotni rivojlantirish, investitsiyalar uchun qulay shart-sharoitlarni yaratish, kripto-aktivlar aylanmasi va blokcheyn texnologiyasini joriy etish bo‘yicha qator islohotlar amalga oshirilmoqda. Xususan O‘zbekiston Respublikasi Prezidentining 2018 yil 3 iyuldagi “O‘zbekiston Respublikasida raqamli iqtisodiyotni rivojlantirish chora-tadbirlari to‘g‘risida” PQ-3832-son hamda 2018 yil 2 sentyabrdagi “O‘zbekiston Respublikasida kripto-birjalar faoliyatini tashkil etish chora-tadbirlari to‘g‘risida”gi PQ-3926-son qarorlari qabul qilingan.

Qaror ijrosini ta’minlash maqsadida 2020 yilning 20 yanvar kuni O‘zbekiston Respublikasi Prezidenti huzuridagi Loyiha boshqaruvi milliy agentligi (keyingi o‘rinlarda-Agentlik) Koreyaning “Kobea Group” texnologik kompaniyasi bilan hamkorlikda Markaziy Osiyodagi ilk “UzNEX” kripto-birjasi ishga tushirildi.

O‘rganilgan xorij tajribasiga muvofiq, O‘zbekistonda tijorat banklarida quyidagi maqsadlar va xizmatlarda blokcheyn texnologiyasidan foydalanish mumkin.

Transchegaraviy to‘lovlar va pul o‘tkazmalarida. Banklar pul o‘tkazmalarining xarajatlarini kamaytirish va tranzaksiyalar tezligini oshirish uchun blokcheyn texnologiyasidan foydalanishlari mumkin.

Shaffoflikni oshirishda. Banklarda blokcheyn texnologiyasidan foydalanish shaffoflikni oshirishda qator qulayliklar yaratadi. Xususan, noaniqlik yoki xatolar tufayli noto‘g‘ri kirilgan ma’lumotlarni tezda tuzatish orqali hujjatlar aylanmasi va auditorlik tekshiruvlar sonini kamaytiradi. Shuningdek, noto‘g‘ri ma’lumotlar bo‘yicha to‘lovlarni amalga oshirish ehtimolini, firibgarlik va shaxsiy ma’lumotlarning o‘g‘irlanish faktlarini kamaytiradi.

Aqlli shartnomalar tatbiq etish va yuridik xarajatlar kamaytirishda. An’anaviy shartnomalar o‘rniga aqlli shartnomalardan foydalanish bitimning barcha ishtirokchilarini himoya qiladi, chunki pul yoki boshqa qimmatliklar shartnoma bajarilish vaqtida shartli ravishda kompyuter algoritmida saqlanadi va faqatgina barcha shartlar bajarilgandan so‘nggina tomonlarga egalik qilish huquqini beradi.

Aqlli shartnomalar hujjatlarni to‘ldirish va tasdiqlash bilan bog‘liq barcha narsani avtomatlashtiradi, jarayon samaradorligini oshiradi, vaqt va pul xarajatlarini kamaytiradi.

Hamkorlikda ma’lumotlarni almashish va saqlashda. “Deloitte” xalqaro auditorlik kompaniyasining hisob kitoblariga ko‘ra, blokcheyn texnologiyalari banklar tomonidan ma’lumotlarni qayta ishlash va saqlash uchun sarflanadigan sarf-xarajatlarni 25 foizga kamaytirish imkonini beradi. Bundan tashqari, bu saqlanadigan ma’lumotlarning xavfsizligini va ishonchliligini oshiradi.

Raqamli identifikatsiyani tasdiqlashda. Banklarda amalga oshiriladigan to‘lov tizimi bilan bog‘liq aksar moliyaviy operatsiyalar mijoz identifikatsiyasini talab qiladi va har bir operatsiya uchun mazkur amaliyotni takrorlashga to‘g‘ri keladi.

Blokcheyn texnologiyasida yaratilgan identifikatsion kartada tasdiqlash amaliyotidan faqatgina bir marta o‘tiladi va uni keyingi identifikatsiya, avtorizatsiya, va verifikatsiya jarayonlarida ishlatish mumkin.

Normativ hisobot. O‘zgarmas va ishonchli raqamlarga ega blokcheynga asoslangan buxgalteriya kitobi hisobotlarni ishonchli almashish imkonini beradi.

Xorijiy tajribaga muvofiq va bugungi kunda mamlakatimizdagi moliyaviy salohiyati, holatidan kelib chiqib, blokcheyn texnologiyalarini O‘zbekistondagi tijorat banklarida joriy etish mijozlar uchun yanada qulay sharoitlarni yaratish, bank faoliyatini

yanada tezkorligini ta’minlash va sifatli xizmat ko‘rsatishni takomillashtirishga xizmat qilishi mumkin.

Ko‘chmas mulkni sotib olish va sotish jarayoni misolini ko‘rib chiqaylik. Aytaylik, *A* shaxs uyini *B* shaxsga ko‘chmas mulkni sotyapti. Bunday holda, *B* shaxs oldida hech bo‘lmaganda quyidagi savollar tug‘iladi.

- sotiladigan uy haqiqatan ham *A* shaxsga tegishlimi?
- sotilayotgan mulk ilgari boshqa shaxsga sotilmaganmi yoki u boshqa moliyaviy amallar uchun garov sifatida berilmaganmi?
- xarid bo‘yicha huquqiy hujjatlarni rasmiylashtirgandan so‘ng ko‘chmas mulkni sotib olish uchun to‘lovni amalga oshirishga *A* shaxs rozi bo‘ladimi?
-agar oldindan to‘lash zarur bo‘lsa, sotib olish va sotishni qonuniylashtirish jarayonini kechiktirib, *A* shaxs firibgarlik qilmaydimi?

Shu bilan birga, *A* shaxs oldida hech bo‘lmaganda quyidagi savollar tug‘iladi:

- *B* shaxs sotuv uchun huquqiy hujjatlar rasmiylashtirilgunga qadar mulk uchun oldindan to‘lashga rozi bo‘ladimi?
- agar *B* shaxs oldindan to‘lov qilishga rozi bo‘lmasa, u sotib olishni qonuniylashtirish jarayonidan keyin to‘lovni kechiktirib aldamaydimi?

Yuzaga keladigan muammolarni hal qilish uchun tomonlarga kamida bittadan advokat va yana bir riyeltor degani kerak bo‘ladi. Agar advokatlar ko‘chmas mulkni sotib olish va sotish bo‘yicha hujjatlarni, shu jumladan kadastr hujjatlarini tayyorlash bo‘yicha xizmatlarni ko‘rsatsa, riyeltor kafil vazifasini bajaradi. Bundan tashqari, riyeltor sotuvchi va xaridor bir-birini topishga yordam beradigan vositachi rolini ham o‘ynaydi.

Bundan tashqari, ko‘chmas mulkni sotib olish va sotishni rasmiylashtirish uchun notarius xizmatlari, shuningdek ko‘chmas mulk kitoblariga o‘zgartirishlar kiritish uchun davlat kadastr idoralari xizmati talab qilinadi.

Tabiiyki, barcha vositachilar bepul ishlamaydi va bunday vositachilar qancha ko‘p bo‘lsa, oldi-sotti uchun zarur vaqt ham, moliyaviy xarajatlar ham shuncha ko‘p bo‘ladi.

Bitkoin blokcheyni. Bitkoin blokcheyni taxminan bir vaqtda amalga oshiriladigan tranzaksiyalar guruhi yoki bloklar uzun zanjirini

ifodalaydi. Bu zanjir ko'lami cheksiz uzoq bo'ladi – tizimning o'zi qancha ko'p faoliyat ko'rsatsa, blokning uzunligi shunchalikko'p o'sadi. Bunday xronologik tuzilma juda muhimdir, chunki unda barcha, shu jumladan, eng ilk tranzaksiyalarning ham qonuniyligi kafolatlanadi. Asl maqsadida ko'ra, foydalanuvchining bitkoinlarni kimgadir takroriy o'tkazishga yo'naltirilgan keyingi harakatlari noqonuniy deb topiladi. Har bir operatsiyaning vaqti qayd qilingan bo'lgani uchun bitkoinlarni olish va o'tkazmalarni amalga oshirish nazorat qilinadi. Bitkoin blokcheyni o'z iqtisodiyotining istalgan qatnashchisi uchun ochiq bo'lgan ketma-ketlikni yaratgan holda, tizim istalgan vaqt har bir qatnashchining hisobraqami holatini nazorat qiladi, shuningdek, har bir bitkoin blokcheynning bir qismiga «biriktirib qo'yilgan»ni uchun, u qaerda yaratilgani, sarflangani yoki olingani haqidagi axborotni identifikatsiya qila oladi. Agar masalan, Anvar New-Yorkda bir stakan Nescafeqahvasi xarid qilish uchun o'z smartfoniga o'rnatilgan elektron hamyondan foydalanadigan bo'lsa, bunda tarmoq uning elektron hamyonidan kafe elektron hamyoniga qandaydir kattalikda bitkoin o'tkazish so'rovi haqida axborot oladi. Bu paytda tranzaksiya - tasdiqlashni kutib turgan «to'xtatib turilgan operatsiya» deb hisoblanadi. Lekinmaynerlar yangi tranzaksiyalar blokini shakllantirish uchun zarur bo'lgan jarayonlarni amalga oshirib va uni blokcheynga kiritib bo'lgach, haridor tranzaksiyasixuddi o'sha 10 daqiqada amalga oshirilgan boshqa tranzaksiyalar bilan birga, bosh jurnalda doimiy qayd qilib qo'yiladi. Mos ravishda, uning bitkoinga kofe xarid qilishi autentik va ortqa qaytarilmas operatsiya deb hisoblanadi. Blokcheyn bitkoin bazaviy dasturiy protokoli boshqaruvi ostida bo'ladi. Satoshi Nakamotodan boshlab, bitkoin tarmog'ining har bir foydalanuvchisi kompyuter yoki smartfonga tarmoqdagi boshqa kompyuterlar bilan o'zaro aloqa qilish qoidalarini xabar qiladigan dasturiy yo'riqnomalar to'plamini u yoki bu tarzda yuklaydi. Blokcheyn bitta kompyuterda yoki serverda mavjud bo'lishi mumkin emas. Tarmoq registratorlari bilan bog'liq vaziyatdagi kabi, blokcheyndagi ma'lumotlar tarmoq uzellari yoki kompyuterlar egalari hamjamiyatida taqsimlangan ko'rinishda mavjud bo'ladi. Bu tugunlarga elektron hamyonlar o'rnatilgan, ya'ni ular yordamida bitkoiyn hisobraqamlaridagi qoldiqni u belgilab qo'yilgan blokcheynning chegaralangan qismida o'zgartirgan holda to'lov tashabbusi bilan chiqishmumkin bo'ladi. Tugunlar shaxsiy

kompyuterlar – yoki, zamonaviy tushunishda, ixtisoslashgan mayning markazlarini ham o'z ichiga oladi – ular yordamida maynerlar blokcheynni shakllantiradi va buning uchun yangi bitkoinlar ko'rinishida mukofot oladi. Oldindan belgilangan tartibda birgalikda ishlagan holda, bu tarmoq uzellarnong ishonchliligijamoaviy ravishda bosh jurnal (grossbook) vositasida kafolatlaydi.Tabiiyki, bitkoin kriptovalyutasi blokcheynsiz mavjud bo'la olmaydi. Amaldagi doimiy o'zgarib turadigan kirim va chiqimlarni hisobga olish kriptovalyutani ifodalaydi. Bitkoinlar o'z holicha mavjud bo'la olmaydi va siz qaysidir elektron qurilmaga kirib, bir nechta bitkointanga olishingiz mumkin bo'lmaydi. Tasdiqlangan tranzaktsiyalar ko'rinishidagi doimiy ravishda uzayib boradigan blokcheynning yana bir muhim jihati – uning hamma uchun ochiqligidir. Bu esa bitkoinni yopiq elektron valyuta tizimlaridan farqlaydi. Maxsus dasturiy ta'minot sifatida ko'pincha Londonning Blockchain kompaniyasi tomonidan ishlab chiqilgan bepul dasturdan foydalaniladi.

Ochiq kalitli shifrlash tizimi internetda va moliyaviy ilovalarda, shu jumladan, onlayn-banking va elektron pochtada keng miqyosda foydalaniladi. U begonalarning maxfiy axborotga ulanishiga imkon bermagan holda, insonlarga belgilangan ma'lumotlar almashinishga imkon beradi va o'ta maxfiy parol maxfiy bo'lmagan foydalanuvchi nomi bilan kombinatsiyalanadigan bank hisobraqamiga internetdan ulanish tizimini eslatib yuboradi. Bu tizimning muhim xususiyati shundaki, hozirgi zamon kompyuter texnologiyalaridan foydalangan holda, teskari matematik hisob-kitoblar usuli bilan shaxsiy kalitni amalda topib bo'lmaydi. Xeshlashtirishsh algoritmio'ziga xos «xesh»lar ierarxiyasi tuzishga imkon beradi va bu juda foydali hisoblanadi, chunkimaynerlar tomonidan bir vaqtning o'zida bajariladigan tranzatsiyalarni guruhlashi mumkin bo'lgan tuzilma yaratiladi. Bu quyidagi tartibda ro'y beradi. Mayner kompyuteridagi dasturiy ta'minot yordamida birinchi tranzaksiya xeshini – undagi mavjud axborot bilan birga – keyingi xeshlanmagan va qayta ishlanmagan axboroti bilan yangi xesh yaratish uchun birlashtiradi. Endi ikkala tranzatsiya haqidagi axborot to'liq xeshlangan bo'lib qoladi. Bu jarayonmaynerning kompyuteri orqali qayta ishlash uchun qabul qiladigan galdagi tranzaksiya bilan takrorlanadi. Ikkita tranzaksiya haqidagi axborot asosida tashkil qilingan xesh, uchinchi tranzaksiya haqidagi axborot bilan birlashtiriladi va yana bitta,

uchinchi xesh yaratiladi. Bu jarayoni yangi tranzaksiyalar qayta ishlashga kelib tushishi bilan har safar takrorlanavaradi. Birlashtirilgan xesh tarkibidagi axborotni xeshlar zanjiri bo‘ylab, ortga qarab harakatlangan holda oson tekshirish mumkin bo‘ladi. Aynan shu tariqa tranzaksiyalar blokcheyn uchun qurilish bloklariga birlashtiriladi va mos ravishda bloklar deb ataladi.Kompyuterlar o’zaro musobaqaga kirishib, bir vaqtda va tezda kodlashtirish hamda maksimal hajmdagi ma’lumotlarni yangi, to‘liq butlangan bloklarga birlashtirish va kelgusida avvalgi blok ortidan blokcheynga qo‘shish uchun xeshlar taklif qiladi. Bu musobaqada bazaviy bitkoin algoritmi tomonidan yutuqli deb tan olingan maxsus raqam egasi g‘olib chiqadi. Bu raqamni olishuv juda qiyin, shu sababli, kompyuterlar yutuqli nomer hosil bo‘lmagunga qadar – takror va takror xeshlardan iborat bo‘lgan bloklar yaratishda davom etadi. Kompyuter tomonidan yaratiladigan yangi xesh-bloklarning har biri undagi alohida ma’lumotlarga tasodifiy tarzda hosil qilingan (bir martalik kod deb ataladigan) unikal raqam qo‘shish yo‘li bilan yaratiladi. Yuqorida aytib o‘tilganidek, ular qatoriga so‘nggi tranzaksiya haqida xeshlangan ma’lumotlar, shuningdek, avvalgi xesh-blok haqidagi ma’lumotlar kiritiladi. Yangi bir martalik kod qo‘shib, biz yakuniy xesh-blokni to‘liq o‘zgartiramiz. Ta’kidlash joizki, bir martalik kod atamasi Lyuis Kerrolldan olingan bo‘lib, u frabjous (ajoyib) so‘zidan foydalangan va bu so‘znifaqat bitta holatga nisbatan qo‘llanadigan va kelgusida qo‘llash uchun yaroqli bo‘lmagan «bir martalik so‘z» sifatida tavsiflagan. Mayningga jalb qilingan kuchli kompyuter tugunlari tomonidan yutuqli kod topish jarayonida ishlab chiqilgan va chiqarib tashlangan milliardlab «bir martalik so‘z»lar taqdiri mana shunday. Bu virtual raqamlar o‘rmonida virtual parol ovini eslatib yuboradi.Mohiyatan, agarhisoblab chiqilgan tizim resursidoimiy bo‘lib qolaveradigan bo‘lsa, raqamlarni tasodifiy tanlab olish matematik qonuniyatlari shundayki, yetarli darajada uzoq vaqt davomida alohida olingan tugunbu tizimda jalb qilgan hisoblash resursiga proporsional ravishda bitkoinlar miqdorini ishlab topishi lozim. Muammo shundaki, tizimda ishlayotgan yakuniy hisoblash tugunlari miqdori va ularning harakatlariga to‘lov sifatida ishtirok etadigan bitkoin bloklari miqdorida kuchsiz kompyuter yutuqli kod hosil qilishi va mukofot uchun 25 bitkoin tanga olishiga qadar juda katta vaqt o‘tadi. Aynan shu sababli, eng yirik maynerlardan tashqari,

hamma hozirgi paytda birgalikda ishlab topilgan bitkoinlarni barcha qatnashchi tugunlar o‘rtasida ularning hisoblash resursiga proporsional ravishda taqsimlab beradigan «mayning pullari»ga birlashadi. Bunda kuchsizroq tugunlar, qoidaga ko‘ra, oziga bitkoin ulushini ishlab topadi, xolos.Bu matematik hisob-kitoblar maynerlarga ikki sababga ko‘ra topshiriladi. Birinchidan, ular mayning harajatlarini shakllantiradi, chunki ular uchun talab qilinadigan hisoblash resurslari ancha qimmat: uning tannarxi texnika amortizatsiyasi va elektr energiyasi qiymatidan iborat. Bu mayning jarayonini tartibga solish hamda bitkoinlar emissiyasi va ularni olish uchun zarur bo‘lgan ishlar o‘rtasida o‘zaro aloqa bog‘lashga imkon beradi. Ikkinchidan, bu g‘olibga tranzaksiyani tasdiqlash uchun zarur bo‘lgan ishni bajarishga rag‘batlantiradigan mukofot to‘lagan holda raqobat muhitini yaratadi.Masala hal etilgach, g‘olib-kompyuterda ishlaydigan bitkoin dasturi tranzaksiyalarning yangi blokini xesh bilan «muhrlaydi» va unga doimiy o‘sib boradigan blokcheyn zanjirida o‘sha paytdagi oxirgi blokdan keyin keladigan blokning raqamini beradi.

Tranzaksiyalarning yangi bloki yaratilgan va blokcheynga ulangandan keyin yana bitta muhim masala qoladi: boshqa maynerlarning tarkibidagi tranzaksiyalar ishonchli ekanligini tasdiqlashi lozim. Bunday tasdiqlashsiz qaysi operatsiyalar real ekanligini, qaysilari esa real emasligini aniqlashning imkoni yo‘q. Shunday qilib, qaysidir nopok mayner blokka qalbaki tranzaksiyalar kiritmaganligini bexato bilib bo‘lmaydi. Ehtimol, ular tasarruf qilish huquqiga ega bo‘lgan bitkoinlarni kimgadir o‘tkazish – boshqacha qilib aytganda, firibgarlik tranzaksiyasini amalga oshirish bilan bog‘liq bo‘lishi mumkin. Shundagina tizim bu tranzaksiyani qonuniy sifatida qabul qiladi. Demak, boshqa maynerlarraqobatda g‘olib chiqqan mayner ishini tasdiqlash nomi ostida ma’lum bo‘lgan holatni tasdiqlashlari lozim. Ular blokda kodlashtirilgan tranzaksiyalar bo‘yicha ma’lumotlarni blokcheyndagi operatsiyalar butun zanjirini tahlil qilish asosida ularning ishonchliligini tekshirish uchun xuddi shu blokdagi xeshlangan ma’lumotlar bilan taqqoslaydi. Bir qarashda bu masala chegaradan oshirib yuborilgan masala bo‘lib ko‘rinadi, lekin uni bajarish bilan kuchli kompyuterlar shug‘ullanadi. Demak, bu jarayon bir martalik kodlar ishlab chiqish kabi sermashaqqat emas va nisbatan tez hamda oson bajarilishi mumkin. Boshqa maynerlar

tasdiqlashi haqidagi informatsiya tarmoqqa va elektron hamyonlar egalariga yuboriladi.

Noma'lum qolgan bitkoin yaratuvchisi erkin bozorda raqobat tamoyiliga murojaat qilgan holda, taqsimot adolatliligi muammosini hal qiladi. Bu xabardor bo'lmaganlar uchun maqsadsiz bo'lib ko'rinishi mumkin bo'lgan jarayon – xeshlar to'xtovsiz raqobatining maqsadlaridan biri deb hisoblanadi. Maynerlarmatematik masalalarni yagona maqsad bilan – poygada g'olib chiqish va mukofotga bitkoin olish uchun yechadilar, qo'shimcha natija esa shundan iboratki, ular tranzaksiyalarni tasdiqlaydilar va blokcheynni dolzarb holatda saqlaydilar. Shundan kelib chiqib, bitkoin protokoli kim mukofot olishga loyiq ekanligini hal qiladi. Yangi bitkoinlarga ega bo'lish – maynerlar harakatlarini kompensatsiya qilishning yagona usuli emas. Bazaviy dasturiy ta'minot hamjunatuvchidan tranzaksiyalar uchun komission to'lovlar undirish funksiyasidan iborat bo'ladi. Hozirda atigi bir necha xil tranzaksiya turi o'tkazganlik uchun kichik majburiy komission to'lovlar undiriladi. Ular qatoriga «chang» tranzaksiyalari – juda kichik miqdorlardagipul o'tkazmalari kiradi. Bular ko'p sonli ma'nosiz so'rovlar yoki tranzaksiyalar, shuningdek, ortiqcha axborot hajmiga ega bo'lgan tranzaksiyalar (axborot hajmi 10 kilobaytdan ortiq bo'lgan tranzaksiyalar shunday hisoblanadi) jo'natgan holda tarmoqni «qulatish»ga urinadigan nopok dasturchilar tomonidan tarmoqqa hujumlarning oldini olish uchun zarurdir. Foydalanuvchilar shu tariqa yakuniy tasdiqlashni kutishga ketadigan vaqtni qisqartirgan holda, maynerlarga birinchi galda qayta ishlash va ularni blokka kiritish ehtimolini oshirishga urinib, o'z tranzaksiyasi summasiga kichik komission to'lovlarni kiritishi mumkin.

Raqamli iqtisodiyot yaratgan jasmoniy va raqamli voqelik o'rtasida asosiy ko'priklardan biri - buyumlar Internetiyoki «hamma buyumlar Interneti» hisoblanadi. Eng oddiy shaklda u buyumlar (mahsulot, hizmat, joy va boshqalar) va odamlar o'rtasidagi turli o'zaro bog'liq bo'lgan platformalar va texnologiyalar bilan ta'minlanadigan o'zaro aloqalar sifatida belgilanishi mumkin.Jismoniy dunyoni raqamli tarmoqlar bilan birlashtirishning datchiklar va boshqa ko'p sonli vositalari hayratlanarli sur'atlar bilan rivojlanmoqda.Hozirda dunyo bo'ylab tarmoq orqali Internetga ulangan milliardlab qurilmalar, jumladan, telefonlar, planshetlar va kompyuterlar mavjud. Ularning soni yaqin yillar ichida, ayrim

baholarga ko'ra – bir necha milliarddan trilliongacha jiddiy ravishda o'sadi, bu aktivlarni optimallashtirish va monitoring qilish imkoniyatini taqdim etib, ta'minot zanjirini boshqarish usulini, va shuningdek, korxona faoliyatini ham eng mukammal darajada tubdan o'zgartirib yuboradi. Ushbu jarayon doirasidabu ishlab chiqarish va infratuzilmadan tortib, sog'liqni saqlashgacha bo'lgan sanoatning barcha tarmoqlariga o'zgartiradigan ta'sir ko'rsata oladi.Raqamli inqilobalohida odamlar va muassasalar o'rtasida hamkorlik va o'zaro aloqa qilish usulini tubdan o'zgartiradigan tamomila yangi yondashuvlar yaratadi. Masalan, «taqsimlangan ma'lumotlar to'plami» deb ataladigan bloklar zanjiri uning doirasida kompyuterlar tarmog'i bitimni ro'yxatdan o'tkazish va tasdiqlashga qadar jamoaviy ravishda tasdiqlaydigan xavfsiz protokol hisoblanadi. Bloklar zanjiri va unga asoslangan texnologiya bir-biri bilan notanish bo'lgan (shu tariqa bir-biriga ishonish uchun asosga ega bo'lmagan) odamlarga o'zaro aloqa qilish imkoniyatini bergan holda, neytral markaziy organni, ya'ni, banklardan yoki markaziy registrdan aylanib o'tib, ishonch uchun asos beradi. Mohiyatan, bloklar zanjiridasturlashtirilgan, kriptografik himoya qilingan, demak, qandaydir bitta foydalanuvchi tomonidan nazorat qilinmaydigan ishonchli ma'lumotlar omborxonasini ifodalaydi.Raqamli iqtisodiyot natijasida mavjud siyosiy, iqtisodiy va ijtimoiy modellar sohasidagi rivojlanish mustaqil harakat qiladigan shaxslardan ularni o'zaro aloqa qilishning jamoaviy shakllarini nazarda tutadigan taqsimlangan hukumat tizimining bir qismi deb tan olishni talab qiladi.

Oxirgi yillarda kompaniyalar o'z ishlarni chet tashkilotlarga berish bo'yicha chora-tadbirlar doirasida ish o'rinlarini optimallashtirish va aniqroq belgilash, ularni mamlakat tashqarisiga chiqarish va masofadan turib ishlash yo'liga o'tkazish (masalan, Mechanical Turk yoki Mturk servisi, Amazon kompaniyasi orqali – internetda kraudsorsing jamoaviy bozori) uchun ko'p kuch va mablag' kiritganligi avtomatlashtirishni ta'minlaydigan juda muhim omil hisoblanadi. Ish joylarini bunday optimallashtirish odamlarni algoritmlar bilan almashtirish bo'yicha qo'shimcha imkoniyatlar taqdim etishini anglatadi, chunki diskret, aniq belgilangan topshiriqlar, topshiriq bilan bog'liq ma'lumotlar sifati yuqori bo'lishi va samarali monitoringga olib keladi, shu tariqa uning asosida ishlarni bajarish algoritmlarini ishlab chiqish mumkin bo'lgan qulay baza yaratadi.

Amalda aksariyat hollarda joriy o‘zgarishlarni ta’minlaydigan raqamli, jismoniy va biologik texnologiyalar birlashuvi kognitiv faoliyat deb ataladi va u inson mehnatini takomillashtirishga hizmat qiladi, ya’ni yetakchilar kadrlar resurslarini tayyorlashi, ish uchun ta’lim modellarini rivojlantirishi, shuningdek, doimiy kengayadigan imkoniyatlarga ega bo‘lgan o‘zaro bog‘liq va intellektual mashinalar yaratishiga to‘g‘ri keladi. XXI asrda, ya’ni raqamli davrda barcha tarmoqlar uchun to‘rt xil asosiy oqibatlar kelib chiqadi:

- iste’molchilar kutadigan natijalar o‘zgaradi;
- aktivlar unumdorligini oshiradigan ma’lumotlar hisobiga mahsulotlar sifati takomillashadi;
- yangi hamkorlik usullari kompaniyalarning yangicha sheriklik shakllarining muhimligini anglab etishi bilan shakllanadi;
- operatsion modellaryangi raqamli modellarga o‘zgaradi.

Jismoniy shaxslar (B2S) yoki korporatsiyalar (B2B) hisoblangan mijozlartobora ko‘proq raqamli iqtisodiyot markazida bo‘lib bormoqda, bu esa ularga hizmat ko‘rsatish shakllarini belgilab beradi.Mijozlar kutadigan natijalar tajriba orttirish sohasiga o‘tadi. Masalan, Apple kompaniyasiga nisbatan bu biz mahsulotdan qanday foydalanishimizga emas, balki shuningdek, uning o‘roviga, brendiga, xaridiga va mijozlarga hizmat ko‘rsatishga ham daxldor bo’ladi.Mahsulot va hizmatlarni ularning qiymatini oshiradigan raqamli takomillashtirish yordamida yaxshilash shunga olib keladiki, yangi texnologiyalar kompaniyalar tomonidan aktivlarni idrok qilish va boshqarish strategiyasini o‘zgartirib yuboradi. Masalan, Tesla kompaniyasi shuni namoyish etadiki, dasturiy ta’minot va ulanish imkoniyatlarini masofadan turib yangilash vaqt o’tishi bilan uning qadrsizlanishi o‘rniga mahsulot (avtomobil) qiymatini oshirish uchun foydalanilishi mumkin.Serg‘ayrat raqobatchilarqiymat yaratish zanjiri va an’anaviy ierarxik strukturalar vayron qilinishiga sababchi bo‘ladi, shuningdek, vositachilarni korxonalar va ularning mijozlari o‘rtasida mavjud munosabatlardan siqib chiqaradi. Yangi buzg‘unchilar bunga ular bilan raqobat qiluvchi an’anaviy firmalarga talab qilingandan ancha kamroq sarflab, o‘z faoliyatini tezda kengaytirishi mumkin. Bunda ushbu jarayon davomidatarmoq o‘zaro aloqalari samarasi hisobiga ta’minlanadigan tizumnning tez o‘sishi ro‘y beradi.Oddiy kitob do‘konidan yiliga 100 mlrd dollar daromad keltiradigan chakana

konglomeratga aylangan Amazon kompaniyasining evolyusiyasishuni ko‘rsatadiki, mijozlar sodiqligi, shuningdek,mijozlarning nimalarni afzal ko‘rishini tushunish va buyurtmalarni o‘z vaqtida bajarish kompaniyaga tovarlarni birdaniga bir nechta sektorda muvaffaqiyat bilan sotishga imkon berishi mumkin. Bu misol faoliyat ko‘lami afzalliklarini ham namoyish etadi.Moliya tarmog‘i ham xuddi shunday jiddiy o‘zgarishlar davrini boshidan kechirmoqda. Pirring platformalari (P2P) hozirgi paytdabozorga kirish to‘siqlarini olib tashlayapti va harajatlar pasayishini ta’minlamoqda. Raqamli asr davlat tuzilmalarini himoya qilish uchun foydalanib kelingan ko‘plab to‘siqlarni zaiflashtirdi, buning natijasidahukumatlar bugungi kundaancha samarasizroq faoliyat ko‘rsatishmoqda, chunki boshqariladigan sub’ekt, ya’ni aholiendilikda turli-tuman ma’lumotlardan yaxshiroq xabardor va o‘zining hukumatdan kutadigan natijalari borasida ancha talabchanroq bo‘lib qolgan. Kichkina bir nodavlat tashkiloti bolib turib, ulkan davlatga qarshi chiqqan WikiLeaks bilanbog‘liq mojarolari eski hukumat paradigmasining simmetrik emasligini va unga ko‘pincha hamrohlik qiladigan ishonchga putur yetkazilishini mumkinligini yaqqol namoyish etadi.Bugungi kunda, masalan, shimoliy amerikalik kompaniyalar avvalgidek, dunyoda deyarli istalgan nuqtai-nazardan eng innovatsion kompaniyalar bo‘lib qolavermoqda. Ular eng iqtidorli mutaxassislarni jalb qilmoqda, eng ko‘p sonli patentlar olmoqda, dunyodagi eng yirik miqdordagi venchurli kapitalni taqsimlashga rahbarlik qilmoqda, birjada kotirovka qilinadigan kompaniyalar esa eng yuqori kotirovkaga ega bo‘lmoqda. Shimoliy Amerika oxirgi paytda to‘rtta sinergetik texnologik inqilobga: texnologik yutuqlarga asoslangan energiya ishlab chiqarish sohasidagi innovatsiyalarga, ilg‘or va raqamli ishlab chiqarishga, hayot haqidagi fanlarga va axborot texnologiyalariga katta ahamiyat berib, turli sohasida oldingi o‘rinlarda borayotganini ko’rishimiz mumkin.Garchi bugungi kunda innovatsion iqtisodiyot eng yuqori darajada bo‘lgan ayrim mamlakatlar joylashgan Evropa Ittifoqi (EI) va Shimoliy Amerika dunyo miqyosidagi yetakchi davlatlar bo‘lsada, oxirgi paytlarda dunyoning boshqa mintaqalaridagi davlatlar ularni tezkorlik bilan quvib yetmoqda. Masalan, Xitoyning innovatsion faoliyatini baholash 2015 yil EI darajasining 49%igacha ko‘tarildi (2006 yilda bu ko‘rsatkich atigi 35%ni tashkil qilgan edi), chunki bu mamlakat

shiddat bilan innovatsiyalar va electron hizmatlarga yo‘naltirilgan iqtisodiy modelga o‘tmoqda. Xitoy, hattoki u erishgan taraqqiyotni hisobga olgan holda ham, doimiy ravishda dunyo ishlab chiqarishining qo‘shilgan qiymat yuqori bo‘lgan yangi segmentlariga kirib borayapti va butun dunyoda muvaffaqiyat bilan raqobat qilish uchun o‘zining jiddiy ko‘lamli tejamkorligini ishga solayapti.O‘ziga asosiy e’tibor qaratilgan, hamjamiyatlarning birgalikda bo‘lishi va aloqadorlikning yangi shakllarining paydo bo‘lishi va individuallashtirishga asoslangan jamiyat paydo bo‘lishi keng ijtimoiy nuqtai-nazardanraqamli texnologiyalarga o‘tishning eng muhim (va eng sezilarli) samaralaridan biriga aylandi. O‘tmishda bo‘lganidan farqli ravishda, jamiyatga mansublik haqida tasavvurlar bugungi kunda shaxsiy loyihalar va individual qadriyatlar bilan belgilanadi, makonga oid mulohazalar (ma’lum bir joydagi hamjamiyat) esa, ish va oilaviy munosabatlar bilan belgilanmayapti.Asosiy e’tibor o‘ziga qaratilgan jamiyat paydo bo‘lishjarayoni raqamli texnologiyalarga o‘tishning eng muhim (va eng sezilarli) samaralaridan biriga aylandi deyishimiz mumkin.Bunday murakkab masalalarni hal qilish ustida qalbimiz, ruhimiz va aqlimiz jamoaviy donoligini ishga solganimizdagina raqamli iqtisodiyot yo’nalishida ongli ravishda ishlashimiz mumkin bo‘ladi. Biz buni quyidagi to‘rtta asosiy intellekt turi qo‘llash va rivojlantirish yo‘li bilangina jamoa kuchlarni shakllantirgan, bo‘ysundirgan va tuzatishlar kiritgan holda amalga oshirishimiz mumkin bo‘ladi:

-kontekstual intellekt (aql) – biz bilimlarimizni tushunishimiz va ularni qanday qo’llashimiz mumkin;

-emotsional intellekt (qalb) – fikr va tuyg‘ularimizni qanday qayta ishlashimiz va integratsiyalashimiz,o‘zimizga va bir-birimizga qanday munosabatda bo‘lishimiz kerakligi;

-ruhlantiruvchi intellekt (ruh) – vaziyatni yaxshi tomonga o‘zgartirish va umumiy manfaatlarda harakat qilish uchun shaxsiy va umumiy maqsadni, ishonch va boshqa ne’matlarni qanday tushunishimiz lozimligi;

-jismoniy intellekt (tana) – shaxsiy o‘zgarish uchun ham, tizimlarni o‘zgartirish uchun ham zarur bo‘lgan energiyani safarbar qilish imkoniyatiga ega bo‘lish uchun shaxsiy sog‘liq va xotirjamlikni,

shuningdek, atrofdagilar sog‘lig‘i va xotirjamligini qanday qo‘llab-quvvatlashimiz va rivojlantirishimiz mumkinligi.

Yaxshi yetakchilar kontekstual intellekt vazifalarini juda yaxshi tushunadilar va o‘zlarida mos keluvchi ko‘nikmalarni rivojlantiradilar. Kontekstni his qilish qobiliyati yuzaga kelayotgan trendlarni oldindan ko‘ra bilish va «nuqtalarni birlashtirish»ga tayyorlik va bunga qodirlik sifatida tavsiflanadi. Bu xislatlar ko‘plab avlodlar mobaynidasamarali rahbarlik qilish tavsifnomasi bo‘lib hizmat qilib kelgan, raqamli inqilob davrida esa yangicha vaziyatga moslashish va o‘z mavjudligini davom ettirish imkonini beradigan majburiy shartga aylangan.Qaror qabul qiladigan shaxslarga kontekstual intellektni rivojlantirish uchun dastlab turli guruhlar qadriyatlarini tushunish zarur. Ular tarmoqqa ko‘proq ulangan va an’anaviy ravishda ularni chegaralar ajratib turgan shaxslar bilan birlashtiradigan aloqalarni yo‘lga qo‘ygan hollardagina kuch jihatidan ustunlik qiladilar va buzg‘unchi ta’sirlarga qarshilik ko‘rsatishlari mumkin. Qaror qabul qiladigan shaxslar ko‘rib chiqilayotgan masalada manfaatdor bo‘lgan barcha shaxslar bilan hamkorlik qilishga tayyor bo‘lishlari va hamkorlik qila olishlari lozim. Shunday qilib, biz ko‘proq inklyuzivlikka va ko‘proq muloqotga intilishimiz lozim bo‘ladi.

Faqat biznes yetakchilari, davlatlar, fuqarolik jamiyatlari, diniy tashkilotlar, fan va yosh avlod bilan birlashgan hamda ular nbilan birgalikda ishlagan holdagina ro‘y berayotgan voqea-hodisalar haqida to‘laqonli tasavvurga ega bo‘lish imkoni paydo bo‘ladi. Bundan tashqari, barqaror o‘zgarishlarga olib keladigan kompleks g‘oyalar va qarorlar ishlab chiqish va amalga oshirish o‘ta muhimdir.Bu manfaatdor tomonlar ko‘pligining asosida yotadigan tamoyildir. Sektorlar va kasblar o‘rtasidagi chegaralar sun’iy xarakterga ega bo‘lib, o‘zining qarshi samaradorligini namoyish etadi. Samarali hamkorlik munosabatlarini yo‘lga qo‘yish bo‘yicha tarmoqlar imkoniyatlarini ishga solgan holda, bu to‘siqlarni bartaraf qilish ilgari misli ko‘rilmagan darajada muhim ahamiyat kasb etgan. Bu ishni qilmaydigan kompaniyalar va tashkilotlarso‘zdan ishga o‘tmaydi, ya’ni diversifikatsiya qilinganjamoalar tashkil qilmaydi, raqamli asrning barqarorligi namoyon bo‘lishiga moslashish ancha qiyin bo‘ladi.

Biznes yetakchilari vasiyosatchilar uchun emotsional intellekt raqamli inqilob davrida muvaffaqiyatga erishish uchun hal qiluvchi rol

o‘ynaydigan ko‘nikmalar uchun, chunonchi, o‘zligini anglash, o‘zini nazorat qilish, motivatsiya, empatiya, ijtimoiy ko‘nikmalar uchun muhim tamal toshi bo‘lib hizmat qiladi. Emotsionalintellektni o‘rganishga ixtisoslashgan tadqiqotlar shuni ko‘rsatadiki, mashhur rahbarlaro‘rtacha darajadagi rahbarlardan emotsional intellekt bilan va bu sifatni uzluksiz rivojlantirish qobiliyati bilan farqlanadilar.Doimiy va jadal o‘zgarishlar unga xos jihat bo‘lgan dunyoda emotsional intellekti yuqori bo‘lgan yetakchilar soni ko‘p tashkilotlar nafaqat katta salohiyatga, balki ularga moslashuvchan va iztiroblardan keyin muvaffaqiyat bilan tiklanishga qodir vositalarga ega bo‘ladi, bu esa beqarorlashtiruvchi ta’sirni yengish qobiliyatining doimiy belgisi hisoblanadi. Raqamli kontekstga yo‘naltirilgan,funksionallararo hamkorlikni amalga oshirishga, ierarxiyani teng darajali munosabatlar tizimiga aylantirishga qodir bo‘lgan, shuningdek, yangi g‘oyalar ishlab chiqish rag‘batlantiriladigan fikrlash emotsional intellektga ko‘proq darajada bog‘liq bo‘ladi. Kontekstual va emotsional intellekt bilan bir qatorda raqamli inqilob sharoitlarida samarali yo‘l topishga imkon beradigan yana bitta, uchinchi muhim tarkibiy qism ham mavjud. Aynan u ruhlantiruvchi ong deb ataladi. Ruhlantiruvchi ong (inglizcha“inspire”, lotin tilidagi “spirare”, ya’ni ruhlantirish, ilhomlantirish so‘zidan) ma’no va bajarilishi lozim bo‘lgan vazifalarni uzluksiz izlashga yo‘naltiriladi. U insoniyatni taqdirni umumiy anglab yetishga asoslangan yangicha jamoaviy va axloqiy ongga impuls berishga qaratiladi.

Blokcheyn texnologiyasini amalga oshrishdagi asosiy g‘oya – «birgalikda» nimalardir, qilish, nimalarnidir bajarish demakdir. Agar blokcheyn texnologiya har bir kishi o‘ziga e’tibor qaratadigan jamiyat sari harakatlanadigan sabablardan biri deb hisoblanadigan bo‘lsa, rivojlanishni hayotning barcha jabhalarini qamrab oladigan umumiy maqsadni his qilish bilan o‘ziga e’tibor xos bo‘lgan ko‘proq muvozanatlanganlik tomon yo‘naltirish juda muhim bo’ladi. Bu vazifani biz barchamiz birgalikda hal qilishimiz lozim, chunki raqamli iqtisodiyot davrida yuzaga keladigan muammolarni yenga olmasligimiz yoki birgalikda umumiy maqsadga erishish tuyg‘usini ishlab chiqa olmasak, u bizga beradigan manfaatlardan foydalana olmasligimiz ham mumkin. Bitkoin blokcheyni bilan bog’liq ishlarni amalga oshirish uchun ishonchga ega bo‘lish juda muhim. Yuqori darajadagi ishonch jalb qilinganlik jamoaviy ishlashga hizmat qiladi.

Bularning barchasi hamkorlikda amalga oshiriladigan innovatsiyalar uning o‘zida yotadigan raqamli iqtisodiyot davrida yanada o‘tkirroq his qilinadi. Bu jarayonfaqat uni ishonch kuchaytirib turgan hollarda ro‘y berishi mumkin, chunki unga juda ko‘plab tarkibiy qismlar kiritilgan va xilma-xil muammolar o‘rin olgan. Oxir-oqibat, manfaatdor tomonlarning har biriga innovatsiyalarni umumiy manfaatlarga yo‘naltirish majburiyati yuklatiladi. Agar muhim manfaatdor tomonlarning istalgan biri bunday emasligini his qiladigan bo‘lsa, ishonchga putur etadi.

Ham kontekstual, ham emotsional, ham ruhlanitruvchi intellekt raqamli iqtisodiyot sharoitlarida faoliyat yuritishga va bundan o‘zi uchun foyda olishga imkon beradigan zarur vositalar hisoblanadi. Lekin shunga qaramay,ular uchun to‘rtinchi intellekt – inson salomatligi va farovonligi uchun asosiy va oziqlantiruvchi kuch bo‘lgan jismoniy intellekt ham muhim ahamiyat kasb etadi. Bu juda muhim, chunki o‘zgarishlar tobora tez ro‘y berayotgan sharoitlarda murakkablik o‘sib boradi, shuningdek, qaror qabul qilish jarayoniga jalb qilingan (faoliyati bizning faoliyat bilan bog‘liq bo‘lgan) tomonlar soni ortadi, keskin vaziyatlarda o‘zini yo‘qotmaslik va yaxshi holatda saqlash qobiliyati tobora muhim ahamiyat kasb etadi.Butun insoniyatga hizmat qiladigan kelajakni odamlarni jalb qilish, ularga huquq va vakolatlar berishdan boshlab, bu yangi texnologiyalarning barchasi eng avvalo, odamlar tomonidan odamlar uchun yaratilgan vositalar ekanligini o‘zimizga eslatib turgan holda boshlaymiz.Innovatsiyalar va texnologiyalar insoniyat ravnaqi uchun va jamiyat manfaatlariga hizmat qiladigan ehtiyojlarni ta’minlashga yo‘naltirilgan kelajak uchun jamoaviy javobgarlikni o‘z zimmamizga olamiz vaulardan barqaror rivojlanishga yo‘naltirilgan harakatlarimiz uchun datsuri-amal sifatida foydalanishni ta’minlaymiz.Biz bundan ham uzoq borishga harakat qilishimiz mumkin. Biz texnologiyalar asri (u samarali va mas’uliyatli tarzda shakllantirilishi shartida) bizga o‘zimizni haqiqatda global tamaddunning bir qismi deb his qilishga imkon beradigan yangi madaniy uyg‘onish katalizatori bo‘lib hizmat qilishi mumkin ekanligiga qat’iy ishonamiz. Raqamli iqtisodiyot insoniyatni robotlashtirish salohiyatiga ham ega bo‘lib, bu holat ish, jamiyat, oila va shaxsiyat kabi an’anaviy manbalarini havf-xatar ostiga qo‘yishi mumkin. Voqealar rivojlanishining bunday stsenariysiga yo‘l qo‘ymaslik va XXI asrda insoniyatning taqdir

haqida umumiy tasavvurga asoslangan yangi jamoaviy va axloqiy ong tomon yuksalishi uchun foydalanish bizning qo‘limizda. Biz hammamiz raqakirib kelishi iqtisodiyotning hayotimizga to’la-to’kiz aynan shunday – ijobiy ravishda ro‘y berishiga intilishimiz lozim.

1.3. Blokcheyn tizimlari va uning texnologik sxemasi

Blokcheyn (bloklar zanjiri) – taqsimlangan ma’lumotlar to‘plami bo‘lib, unda ma’lumotlar saqlash qurilmalari umumiy serverga ulanmagan bo‘ladi. Bu ma’lumotlar to‘plami bloklar deb ataladigan va tartibga solingan qaydlar doimiy o‘sib boradigan ro‘yxatda saqlanadi. Har bir blok vaqt belgisiga va bundan oldingi blokka havolaga ega bo‘ladi. Shifrlashni qo‘llash shuni kafolatlaydiki, foydalanuvchilarning ularsiz faylga yozuv kiritish imkoni bo‘lmydi, yopiq kalitlar mavjudligi esa bloklar zanjirlarining ma’lum bir qisminigina o‘zgartirishi mumkin. Bundan tashqari, shifrlash barcha foydalanuvchilarda bloklar taqsimlangan zanjirlari nusxalarini sinxronlashtirishni ta’minlaydi. Ba’zida blokcheyn texnologiyasi «qadriyatlar interneti» deb ataladi va biz buni yaxshi metafora deb hisoblaymiz. Har bir kishi internetda axborot joylashtirishi, so‘ngra boshqa odamlar unga dunyoning istalgan nuqtasidan turib ulanish imkoniga ega bo‘lishi mumkin. Bloklar zanjirlari blokcheyn fayli yoki qandaydir qadriyatlar ochiq bo‘ladigan dunyoning istalgan nuqtasiga ma’lumotlar jo‘natishga imkon beradi.

Biroq sizda faqat siz «egalik» qiladigan bloklarga kirish imkonini berish uchun kriptografik algoritm bo‘yicha yaratilgan yopiq kalit bo‘lishi lozim. Yopiq kalitni kimgadir berar ekansiz, mohiyatan bu shaxsga bloklar zanjirining mos keluvchi bo‘limida saqlanadigan pul mablag‘larini bergan bo‘lasiz.Bitkoinlar holatida, kalitlar to‘g‘ridan-to‘g‘ri moliyaviy qiymatni ifodalaydigan valyutadagi ayrim summalar saqlanadigan manzillarga ulanish uchun foydalaniladi. Xuddi shu bilan mablag‘larni o‘tkazishni qayd qilish funksiyasi amalga oshiriladi.Bundan tashqari, yana bir muhim funksiya – ishonchli munosabatlar o‘rnatish va shaxsning haqiqiyligini tasdiqlash amalga oshiriladi, chunki mos keluvich kalitlarsiz bloklar zanjirini hech kim o‘zgartira olmaydi. Tegishli kalitlar bilan tasdiqlanmagan o‘zgarishlar esa rad qilinadi. Albatta, kalitlar (jismoniy valyuta kabi) nazariy jihatdan o‘g‘irlanishi mumkin, lekin kompyuter kodining bir

nechta satrini himoya qilish odatda katta harajatlar talab qilmaydi (masalan, buni mash’ur Fort-Noksda oltin zaxirasini saqlash harajatlari bilan taqqoslang).

Bugungi kunda biz markazlashgan interaktiv internet platformasi orqali axborot almashinishga ko‘nikib qolganmiz. Biroq agar gap moddiy boyliklarni (pulni) o‘tkazish haqida borganda, biz odatda markazlashtirilgan moliyaviy muassasalar (banklar) hizmatlaridan foydalanishga murojaat qilamiz. Internet orqali to‘lovlar usullari amalda bu tarmoq dunyoga kelgan paytlarda paydo bo‘lgan (eng ko‘zga tashlanadigan misollardan biri — PayPal), biroq ular, qoidaga ko‘ra, bank hisobraqami yoki kredit kartasi bilan integratsiya qilishni talab qiladi.Blokcheyn texnologiyasi esa bular singari «ortiqcha bo‘g‘in»lardan xalos bo‘lishga imkoniyat yaratadi. U an’anaviy ravishda moliyaviy hizmatlar sektori bajaradigan uch muhim amalni o‘z zimmasiga olishi mumkin: bitimlarni ro‘yxatdan o‘tkazish, shaxs haqiqiyligini tasdiqlash va shartnomalar tuzish.Bu holat bank ishida ulkan ahamiyatga molik bo‘ladi, chunki butun dunyoda miqyosida moliyaviy hizmatlar bozori – bozor kapitallashuvi bo‘yicha eng katta bozordir. Bu tizimning hech bo‘lmasa bir qismini blokcheyn texnologiyasiga o‘tkazish moliyaviy hizmatlar sohasida ko‘p sonli uzilishlarga olib kelishi mumkin, lekin shu bilan bir paytda, bunday hizmatlar samaradorligini sezilarli oshirishga imkon beradi. Blokcheyn texnologiyalarining uchinchi ehtimoliy roli (shartnomalar tuzish) moliya sektoridan tashqarida ham juda foydali bo‘lib chiqishi mumkin. Yana bir valyutaning (bitkoin) muomalaga kiritilishi bilan, blokcheyn texnologiyasidan raqamli ma’lumotlarning har qanday turini, jumladan, kompyuter kodini saqlash uchun foydalanilishi mumkin.Ushbu kod fragmentini shunday dasturlash mumkinki, u ikkala kelishuvchi tomon o‘z kalitlarini kiritgan va shu tariqa shartnoma tuzishga rozilik bildirgan holda tegishli amal bajariladi. Xuddi shu kodtashqi ma’lumot oqimlaridan axborot olishi (aksiyalar narxi, meteorologiya ma’lumotlari, yangiliklar sarlavhalariva kompyuter tahlil qilishi mumkin bo‘lgan boshqa narsalar)vama’lum bir shartlar bajarilganda avtomatik ravishda ro‘yxatdan o‘tkaziladigan shartnomalar tuzishi mumkin.Ushbu mexanizm «aqlli shartnomalar» (smart-contract) deb ataladi va uni qo‘llash imkoniyatlari amalda cheklanmaydi.Masalan, termoregulyasiya intellektual tizimi energiya iste’moli haqidagi ma’lumotlarni intellektual elektr tarmog‘iga

uzatishi mumkin. Belgilangan miqdorda elektr energiyasi iste'mol qilinganda boshqa bloklar zanjiri avtomatik ravishda kerakli summani sizning hisobraqamingizdan energetika kompaniyasi hisobraqamiga o'tkazadi. Natijada hisoblagich ishi avtomatlashtiriladi.Mazkur yondashuv intellektual mulkdan foydalanishni nazorat qilish uchun ham to'g'ri keladi: u foydalanuvchiga necha marta axborotga ulanish, u bilan o'rtoqlashish yoki undan nusxa ko'chirishga ruxsat berilganini belgilashi mumkin. Undan yana qalbakilashtirishdan himoya qilingan ovoz berish tizimi yaratish, axborotni tsenzura cheklovisiz tarqatish va boshqa amallar uchun foydalanilishi mumkin.Yirik banklar va ayrim davlat strukturalari «blokcheyn»dan taqsimlangan registrlar sifatida ishlatishadi, oddiy «blokcheyn»dan esa axborot saqlash va tranzaksiyalar amalga oshirish usulini tubdan o'zgartirish uchun foydalanadilar. Ular maqtovga loyiq maqsadlarni ko'zlaydilar: tezlik va xavfsizlikni oshirish, qiymatni pasaytirish, xatolar sonini kamaytirish, ishdan chiqish va zaiflik markaziy nuqtalarini bartaraf qilish kabi ishlarni amalga oshirishni rejalashtiradilar. Bunday modellarto'lovlarni amalga oshirish uchun kriptovalyutalardan foydalanishi shart emas.Biroq eng muhim va istiqbolli blokcheynlar bitkoinning Satosi Nakomoto tomonidan ishlab chiqilgan blokcheyni va modeliga asoslanadi. Ular qanday ishlashini quyida ko'rib chiqamiz.

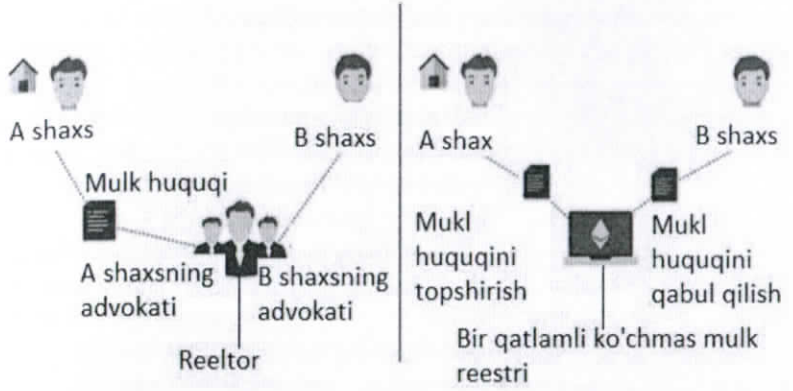
Bitkoyn, boshqa har qanday raqamli valyuta kabi, biron joyda faylda saqlanmaydi. U blokcheynda yozilgan tranzaksiyalar bilan ifodalanadi va bitkoin bir rangdagi katta tarmoq resurslari orqali bitkoindan foydalanilgan har bir tranzaksiyani tasdiqlash va uni ma'qullash uchun foydalaniladigan qandaydir butunjahon grossbux kitobi yoki katta jadval kabi boladi. Har qanday blokcheyn, bitkoyndan foydalanishi yoki foydalanmasligidan qat'i nazar, taqsimlangan hisoblanadi: u butun dunyo bo'ylab ushbu tizimga kirgan ko'ngillilar kompyuterlarida ishlaydi, shuning uchun ham, unda buzib kirish mumkin bo'lgan ma'lumotlar markaziy to'plami yo'q. Blokcheyn ommaviydir: uni istalgan kishi istalgan payt ko'rib chiqishi mumkin, chunki utranzatsiyalar auditi va hisobi bilan shug'ullanadigan bironta tashkilotga a'zo emas hamdataqsimlangan tarmoqda joylashgan. Blokcheyn shifrlangan: unda virtual xavfsizlikni ta'minlash uchun ommaviy va xususiy kalitlar (bank yacheykasi uchun foydalanoladigan ikkita kalit tizimi kabi) qo'llanadigan kuchli

shifrlash tizimidan foydalaniladi. Davlat muassasasi yoki moliyaviy korporatsiyaning vijdonsiz xodimi yoki supermarketlar ulkan tarmog'ining kuchsiz brandmauerlari haqida qayg'urishga esa hojat yo'q.

Iqtisodiy tranzaksiyalar yangi raqamli registrini insoniyat uchun muhim va qimmatli bo'lan istalgan axborotnisaqlash uchun ishlatish mumkin, shu jumladan, tug'ilganlik haqida, nikoh haqida va o'lim haqidagi guvohnomalar, oliy ma'lumot haqidagi diplomlar, moliyaviy hisobotlar, tibbiyot kartalari, sug'urta to'lovlari uchun murojaatlar, saylovlardagi ovozlar soni, mahsulotlarning kelib chiqishi – kod ko'rinishida taqdim etilishi mumkin bo'lgan istalgan ma'lumotni saqlashga dasturlab qo'yish mumkin. Yangi platforma dunyodagi hamma narsa haqida raqamli ma'lumotlarni onlayn rejimida birlashtirishga imkon beradi. Bundan tashqari, yaqin kelajakda moddiy dunyodagi milliardlab aqlli qurilmalar o'zgarishlar qabul qilishi va uzatishi, ularga javob qaytarishi, o'z ehtiyojlarini ta'minlash uchun elektrenergiyasi xarid qilishivamuhim axborotlarni tarqatishi, atrof-muhitni muhofaza qilishdan tortib, bizning sog'lig'imiz haqida qayg'urishgacha bo'lgan xilma-xil vazifalarni o'z zimmasiga olishi mumkin. Hulosa qilib aytganda, «Hamma narsa interneti»ga «hamma narsa registri» kerak boladi. Biznes, savdo va iqtisodiyotga ham raqamli hisoblashlar talab etiladi. Barchaga ma'lumki, tadbirkorlik iqtisodiyotning rivojlanishi va jamiyatning gullab-yashnashi uchun juda muhimdir.Internet tadbirkorlarga yirik kompaniyalarning meros bo'lib qolgan madaniyatini, rivojlanishdan to'xtagan ish jarayonlarini va o'tmishning og'ir ballasti kabi muammolarini emas, balki imkoniyatlar va vositalar taqdim etgan holda tadbirkorlikni tom ma'noda ozod qilishi lozim. Biroq o'z egalarini milliarderga aylantirgan dotkomlarning ovoza bo'lgan muvaffaqiyatlari yoqimsiz bir haqiqatni niqoblab turadi: ko'plab rivojlangan iqtisodiyotlardatadbirkorlik va yangi kompaniyalar paydo bo'lishi oxirgi o'ttiz yilda kuchli pasayishni his qilmoqda. Rivojlanayotgan mamlakatlarda Internet davlatning haloqatga eltadigan byurokratiyasiga qarshi kurashishga majbur bo'layotgan potensial tadbirkorlar uchun to'siqlarni deyarli pasaytirmadi. Internet milliardlab odamlarga o'z ishini boshlash uchun zarur bo'lgan moliyaviy vositalarga ulanish imkonini bermadi. Albatta, tadbirkor bo'lish hammaning ham taqdiriga bitilgan emas, lekin munosib pul

ishlab topishga harakat qilayotgan hatto o‘rtacha statistik insonga ham moliyaviy operatsiyalarn amalga oshirish imkoniyti yo‘qligi va davlat cheklovlarining kuchayib ketganligi ancha xalal beradi.Bu albatta, murakkab muammo, lekin blokcheyn ko‘p jihatdan tadbirkorlikka va mos ravishda, biznesni gullab-yashnashga kuch-quvvat baxsh etishga qodir. Endi, muhim ahamiyatga ega bo‘lish hamda o‘z jamiyatidan tashqarida ishbilarmonlik faoliyati yuritish imkoniyatiga ega bo‘lish uchun rivojlanayotgan mamlakatlardagi o‘rtacha statistik fuqaro internetga ulangan qurilmaga ham ega bo‘lishi zarur. Global iqtisodiyotga Internetga ulanishni kreditlash va moliyalashtirish manbalari, ta’minotchilar, hamkorlar va investitsiyalash uchun imkoniyatlarning keng miqyosdagi ochiqligini anglatadi. Har qanday iqtidor, har qanday resurs, hatto eng kichik bo‘lsada, blokcheynda monetizatsiya qilinishi mumkin. Yangi platforma biz nimani va qanday qilib onlayn amalga oshirishimiz mumkinligini, bunda kim ishtirok etishini, shu tariqa eng dolzarb ijtimoiy va iqtisodiy muammolarni hal qilish uchun texnologik sharoitlar yaratishga imkon beradi.Agar bu vazifani uddalashning imkoni bo‘lmasa, ko‘p narsa va’da qiladigan blokcheyn texnologiyasi cheklanadi yoki umuman yo‘q qilinadi. Bundan ham yomoni, u kuchli institutlar qo‘lidagi qurolga aylanishi mumkin bo‘lib, uning yordamida ular o‘z holatini saqlab qoladi, yoki, agar unga hukumat ulanish imkoniga ega bo‘lsa, blokcheyn yangi total kuzatuv jamiyati uchun bir vositaga aylanadi. Taqsimlangan dasturiy ta’minot, shifrlash, mustaqil agentlar va hatto sun’iy intellekt chambarchas bog‘langan texnologiyalarinazorat ostidan chiqishi va o‘z yaratuvchilariga qarshi ishlashi ham mumkin.

Endi mulkka egalik huquqini boshqarishda bir qatlamli tizimni ko‘rib chiqaylik. Bunday tizimda mulkka egalik huquqlari to‘g‘risidagi ma’lumotni ro‘yxatga oladigan reyestrlarga, biron bir markazlashtirilgan ma’lumotlar bazasi tomonidan emas, balki ushbu tarmoqqa ulangan alohida kompyuterlar tomonidan ma’lumot kiritiladi va tasdiqlanadi. Boshqacha aytganda, hamkor-ishtirokchilar o‘zlarining reyestr nusxalarini yuritadilar. Muayyan uyga egalik huquqi bir kishidan boshqasiga o‘tkazilgandan so‘ng, darhol reyestrning barcha nusxalari real hayotdagi so‘nggi o‘zgarishlarga mos kelishi uchun yangilanishi kerak (1.2- rasm).

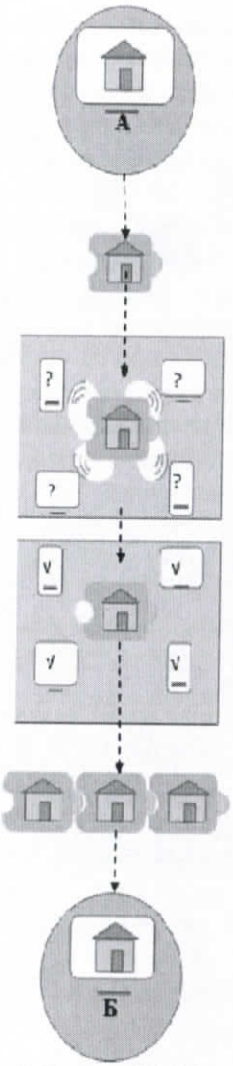


1.2-rasm. Oddiy bitimni, mulkka egalik huquqini boshqaradigan bir qatlamli tizim bilan solishtirish

Egalik huquqini *A* shaxsdan *B* shaxsga o‘tkazish Blokcheyn tizimida quyidagicha amalga oshiriladi. Avvalo, egalik huquqining *A* shaxsdan *B* shaxsga o‘tkazilishi bir qatlamli tizimdagi reyestrlarning birida hujjatlashtiriladi. Ushbu reyestr boshqa hamkorlarga egalik huquqining topshirilishi haqida xabar berishi kerak, hamkorlar, o‘z navbatida, ma’lumotni boshqa hamkorlarga uzatishi kerak - va hokazo, oxir-oqibat, tarmoqdagi barcha hamkorlar egalik huquqining *A* shaxsdan *B* shaxsga o‘tganligi to‘g‘risida xabardor bo‘lmaguncha bu jarayon davom etadi (1.3-rasm).

Bir qarashda, ko‘chmas mulkka egalik huquqini boshqarish bo‘yicha Blokcheyn tizimidan foydalanish texnologiyasi benuqson va ravonday ko‘rinadi.

Ammo hamkorlar o‘rtasida ma’lumot almashish va ayrim reyestrlarni yangilash tartibi muayyan vaqt talab etadi. Tizimning barcha ishtirokchilari yangi ma’lumotlarni olmaguncha va o‘zlarining reyestr nusxalarini yangilamaguncha, tizim kelishilgan hisoblanmaydi. Shunday payt bo‘ladiki, bunda hali ba’zi bir hamkorlar mulkka egalikning oxirgi o‘zgarishidan xabardor bo‘lishgan, ayrimlari esa bu ma’lumotni hali olishmagan bo‘ladi. Barcha reyestrlarning so‘nggi ma’lumotlarga ega emasligi, bunday ma’lumotlarga ega bo‘lgan shaxs tomonidan ushbu reyestrlardan o‘z manfaatlari yo‘lida noto‘g‘ri foydalanish imkoniyatini yaratadi.



A egalik huquqini **B**ga o‘tkazmoqchi

Tranzaksiyalar tarmoqqa uzatiladi va “blok”da yig‘iladi. Har bir “blok” oldingi “blok”ning tartib raqami va xeshiga ega

“Bloklar” tizimning barcha ishtirokchilariga tekshirish uchun yuboriladi

Agar biron bir xato aniqlanmasa, har bir ishtirokchi o‘zining ma’lumotlar bazasining nusxasiga yangi “blok”ni qayd etadi

“Blok” har bir oldingi tranzaksiyalar haqida ma’lumotlarga ega bo‘lgan “bloklar zanjiri”ga qo‘shiladi

Egalik huquqi **A**dan **B**ga o‘tkazildi

1.3-rasm. Ko‘chmas mulkka egalik huquqini boshqaradigan Blokcheyn tizimning ishlash sxemasi

Blokcheyn tizimlarida tranzaksiya, egalik huquqining boshqa shaxsga har qanday o‘tkazilishini tavsiflashning asosiy va yagona

usuli bo‘lib xizmat qiladi va tranzaksiyalarning to‘liq xronologiyasi mulkning hozirgi egalarini aniqlash uchun asosiy vositasi hisoblanadi.

Blokcheyn tizimlarida egalik huquqini olish-topshirish jarayoni ko‘p bosqichli amallar ketma-ketligi sifatida ko‘rib chiqilishi mumkin. Kengaytirilgan shaklda ularni yetti bosqichga bo‘lish mumkin:

- mulkka egalik huquqining tavsifi;
- mulkka egalik huquqining himoyasi;
- tranzaksiya ma’lumotlarini saqlash;
- reyestrlarni ishonchsiz muhitda tarqatish uchun tayyorlash;
- reyestrlarni tarqatish;
- yangi tranzaksiyalarni tekshirish va reyestrlarga kiritish;
- ishonchli ma’lumotlar qaysi reyestrlarga taqdim etilganligini aniqlash.

Blokcheyn tizimlarning har bir bosqichini amalga oshirish jarayonida yuqori hushyorlikni talab qiladigan ba’zi elementlar mavjud.

Xususan, *A* shaxs tizimning boshqa reyestriga kirishni tez qo‘lga kiritishga va o‘sha uyning egalik huquqini o‘tkazish uchun boshqa hujjatni: *A* shaxs tomonidan *V* shaxsiga sotish hujjatini rasmiylashtirishga harakat qiladi, deb faraz qilaylik. Agar ushbu hamkor egalik huquqini *A* dan *B* ga, hozirgina, o‘tkazilganligi haqidagi faktdan xabardor bo‘lmasa, u holda u o‘sha uyning egalik huquqining *A* dan *V* ga o‘tkazilishini qabul qiladi va hujjatlashtiradi. Shunday qilib, birinchi sotuv to‘g‘risida ma’lumot tarqatish uchun vaqt talab etilganligi faktidan foydalanilganligi sababli, *A shaxs o‘z uyini ikki marta sotadi*. Aslida esa, *B* va *V* shaxslar bir vaqtning o‘zida bitta uyga egalik qilishlari mumkin emas. Ulardan faqat bittasigina yangi qonuniy ega deb hisoblanishi mumkin. Bunday holat *ikki karra sotish (sarflash) muammosi* deb nomlanadi.

Bundan tashqari, Blokcheyn tizimi texnologiyasi tugunlarning, ya’ni tizim ishtirokchilarining o‘zaro ishonchiga asoslangan. Afsuski, bir qatlamli tarmoqda nafaqat «*ikki karra sotish (sarflash) muammosi*», balki ushbu tizim ishtirokchilari tomonidan avvalgi amallar natijalarini o‘z manfaatlari yo‘lida o‘zgartirishga urinishlar muammosi ham mavjud.

Buzg‘unchi-hamkorlar, ya’ni Blokcheyn tizimining nohalol ishtirokchilari bir qatlamli tizimlarda ishonchlilik uchun asosiy xavf manbalaridan biri hisoblanadi. *Bu texnik muammo emas, bu tizimni*

o'zlarining g'arazli maqsadlari uchun ishlatishga qaror qilgan ayrim nohalol shaxslarning niyatlari bilan paydo bo'ladigan muammo hisoblanadi.

Nopok va yovuz hamkorlar bir qatlamli tizimiga eng katta xavf tug'diradilar, chunki ular bir qatlamli tizimning fundamental asosiga: tizim ishtirokchilarining o'zaro ishonchiga tajovuz qiladilar. Foydalanuvchilar o'z hamkorlariga ishonmay qo'yganlaridan keyin, ular tizimni tark etadilar va hisoblash resurslaridan foydalanishga ruxsat berishni to'xtatadilar. Hamkorlar soni kamayadi va umuman tizim boshqa ishtirokchilar uchun o'z jozibadorligini yo'qotadi, bu esa o'z navbatida tizim imkoniyatlarining pasayishiga va oxir-oqibat uning yo'qolishiga olib keladi.

1- bob yuzasidan nazorat savollari

1. Taqsimlangan va markazlashtirilgan tarmoqlar arxitekturasi farqi nimada?
2. Taqsimlangan tarmoqlarning afzalliklari noqulayliklari nimalarda ko'rinadi?
3. Musiqa sanoatiga tatbiq etilgan birqatlamli taqsimlangan tarmoqning iqtisodiyotga keltirgan o'zgarishlari nimada?
4. Ko'chmas mulk savdosi algoritmi qanday?
5. Ko'chmas mulk savdosiga birqatlamli tarmoqni tatbiq etish qanday oqibatlarga olib keladi?
6. Ko'chmas mulkka egalik huquqini boshqaradigan Blokcheyn tizimning ishlash sxemasi qanday?
7. Blokcheyn tizimlarini ng tatbiqetishda yuqori hushyorlikni talab qiladigan qanday masalalar mavjud?

2-BOB.BLOKCHEYN TIZIMLARIDA TRANZAKSIYALARNING ISHONCHLILIGINI NAZORAT QILISH USULLARI

Blokcheyn tizimlarida ishonchlilikni nazorat qilish usullarini tushunish uchun, yuqorida ro'yxati keltirilgan, egalik huquqini o'tkazish jarayonining har bir bosqichini o'rganib chiqish lozim bo'ladi.

2.1. Blokcheyn tizimlarida mulkka egalik huquqi va blokcheyn shirkatlari

Bu bosqichining asosiy vazifasi – bu nafaqat qandaydir obyektning egasini e'lon qiladigan, balki egalik faktining qonuniy asosini ham taqdim etadigan, shuning uchun egalik huquqini tasdiqlaydigan hujjatni izlashdan iborat.

Egalik huquqini tavsiflashning ikki yo'li mavjud: inventarizatsiya qaydnomasi ma'lumotlari yordamida va tranzaksiyalar to'g'risidagi ma'lumotlar yordamida.

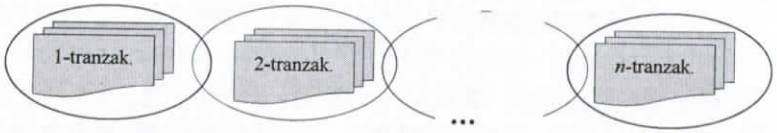
Inventarizatsiya qaydnomasi ma'lumotlari mulk obyektlarining hozirgi holatini tavsiflaydi. Agar bu ko'chmas mulkka egalik huquqi bo'lsa, unda kadastr hujjatini tekshirishga o'xshaydi.

Tranzaksiya ma'lumotlari esa mulkka egalik huquqini boshqa shaxsga o'tkazish faktini tavsiflaydi. Bu ko'chmas mulkni sotib olish va sotish bo'yicha barcha amallar ro'yxati keltirilgan kadastr hujjatini tekshirishga o'xshaydi. Tranzaksiya ma'lumotlarining to'liq ro'yxatidan foydalanib, inventarizatsiya ma'lumotlari qaydnomasini shakllantirish mumkin. Egalik huquqining har bir o'tkazilishi mazkur tranzaksiyalar ma'lumotlari bilan tavsiflanadi, unda kim egalik huquqini o'tkazyapti, o'tkazilayotgan obyekt, qachon va kimga o'tkazilganligi aniq ko'rsatiladi. Tranzaksiyalar to'g'risidagi ma'lumotlarning reyestrda saqlangan to'liq xronologik yozuvi, u yoki bu shaxsning mulk obyektini qanday olganligini ko'rsatadigan nazorat jurnali yozuviga aylanadi.

Blokcheyn tizimi tomonidan ishlatiladigan tranzaksiya quyidagi elementlarni o'z ichiga oladi.

- egalik huquqi boshqa shaxsga o'tkaziladigan hisob yozuvining identifikatori;

- egalikni o‘z zimmasiga oladigan shaxs hisob yozuvi identifikatori;
- egaligi topshiriladigan obyektlar (mahsulotlar) soni;
- ushbu tranzaksiyani bajarish vaqti;
- tranzaksiya uchun tizimga to‘lov;
- hisob yozuvi egasining mulk huquqini boshqaga o‘tkazish faktiga haqiqatdan ham rozi ekanligi to‘g‘risidagi tasdiq.



2.1-rasm. Ko‘chmas mulkka egalik huquqini tavsiflovchi Blokcheyn tizim tranzaksiyalarining blok zanjiri

Tranzaksiyaning bajarilishi – bu, ushbu tranzaksiya ma’lumotlariga to‘liq mos ravishda egalik huquqini topshirish jarayoni ijrosini anglatadi. Tranzaksiyani bajarish deganda reyestrga tranzaksiya ma’lumotlarini kiritish tushuniladi. Reyestrga tranzaksiya ma’lumotlarini kiritgandan so‘ng, ushbu tranzaksiya, egalik huquqini to‘g‘ri aniqlash uchun ishlatiladigan tranzaksiyalar xronologiyasining bir qismiga aylanadi. Shunday qilib, tranzaksiyalar bloklari zanjiri hosil bo‘ladi (2.1-rasm).

Ushbu tranzaksiyalar egalik huquqini o‘tkazuvchi shaxs hisob yozuvi to‘g‘risidagi, egalik huquqini qabul qiluvchi shaxs hisob yozuvi to‘g‘risidagi, o‘tkazilayotgan obyektlar yoki mulk miqdori to‘g‘risidagi barcha ma’lumotlarni o‘z ichiga olganligi sababli, har bir hisob yozuvi uchun egalik huquqining joriy holati to‘g‘risidagi ma’lumotlar, tranzaksiyalar xronologiyasi to‘liq mavjud bo‘lganda, istalgan vaqtda shakllantirilishi mumkin. Shunday qilib, ushbu tranzaksiyalar ma’lumotlarining to‘liq xronologiyasi egalik huquqi hujjatini rasmiylashtirish uchun yetarli bo‘ladi.

Shu bilan birga, tranzaksiya ma’lumotlarini birlashtirish bo‘yicha to‘g‘ri natijani olish uchun tranzaksiyani bajarish tartibiga rioya etish zarurligini tushunish muhim ahamiyatga ega. Ushbu tranzaksiyalarning tartibini o‘zgartirish ularni birlashtirish natijasini buzadi.

Masalan, Blokcheyn tizimning ishtirokchisi, agar u bunday xuquqga ega bo‘lmagan holda, ko‘chmas mulkka egalik huquqini o‘tkazish bo‘yicha tranzaksiyalarni qo‘shsa nima bo‘ladi? Bunday holda, mulkka egalik huquqini boshqa shaxsga o‘tkazish imkoniyati uning boshqa mulkdordan mulkka egalik qilish huquqini olgan-olmaganligiga bog‘liq. Aks holda, *kadastr xizmatlari mulk egalari reyestrida da’vogarning bunday huquqi yo‘qligi sababli mulk huquqi bo‘yicha har qanday amalni taqiqlaydi.* Shuning uchun tranzaksiyalarni bajarish tartibi Blokcheyn tizimida juda muhim rol o‘ynaydi. Bu jarayonda kadastr idoralari xizmatining muhimligini alohida ta’kidlash lozim bo‘ladi – bu xizmat vositachilik xizmatlaridan tubdan farq qiladi va ko‘chmas mulkni boshqarish jarayonida Blokcheyn tizimini qo‘llashda hal qiluvchi rol o‘ynaydi.

Bundan tashqari, Blokcheyn tizimi ma’lumotlari tarkibiga faqat ishonchli tranzaksiya ma’lumotlari qo‘shilishi uchun, kafolatli himoya vositalari bilan ham ta’minlanishlari kerak.Tranzaksiyalar ishonchliligini aniqlash uchun esa quyidagi nazorat turlari amalga oshiriladi:

- tranzaksiyalarning formatli nazorati;
- tranzaksiyalarning semantik (ma’no bo‘yicha) nazorati.

Formatli nazorat – bu tranzaksiya ma’lumotlari to‘g‘ri formatda taqdim etilgan bo‘lishi uchun barcha zarur ma’lumotlarni o‘z ichiga olgan bo‘lishini anglatadi.

Semantik (ma’no bo‘yicha) nazorat asosiy e’tiborni, tranzaksiya ma’lumotlarining ma’nosiga hamda ushbu ma’lumotlarning tranzaksiya natijaga nisbatan kutilayotgan ta’siriga qaratadi. Shunday qilib, semantik nazoratni amalga oshirishda amaliy soha, masalan, ko‘chmas mulkni boshqarish sohasidagi bilimlar talab qilinadi. Tranzaksiyalarning semantik to‘g‘riligini tadqiq qilish ko‘pincha quyidagi amallarni bajarish qoidalariga asoslanadi, masalan:

- tranzaksiyadagi hisob yozuvi (mulk egasi), o‘zining egaligida mavjud mulk obyektlari sonidan oshib ketadigan obyektlarni o‘tkazishga urinayotgani yo‘qmi?
- ikki karra sotish (sarflash) muammosini oldini olish;
- bitta tranzaksiya bo‘yicha berilayotgan obyektlar sonini cheklash;
- bitta foydalanuvchi uchun tranzaksiyalar sonini cheklash;

- muayyan vaqt oralig‘ida sarflangan (topshirilgan) obyektlarning umumiy sonini cheklash;

- ushbu obyektga egalik huquqini keyingi o‘tkazish imkoniyati paydo bo‘lgunga qadar obyekt mulk egasining hisob yozuvi tasarrufida qolishi kerak bo‘lgan minimal vaqt oralig‘ini belgilash.

Blokcheyn tizimlarida mulkka egalik huquqini himoyalash. Shunday qilib, biz Blokcheyn tizimning har bir blogi qanday qilib alohida-alohida paydo bo‘lishini aniqladik: bu ma’lum bir ma’lumotlar tuzilmasiga ega bo‘lgan va ma’lum tekshiruvdan o‘tadigan oddiy tranzaksiyalar ekan.

Endi biz *mulkka egalik huquqining himoyasi* qanday ta’minlanishini ko‘rib chiqamiz. Buning uchun Blokcheyn tizimining keyingi bloklari qanday tashkil etilishi, ular bir-biri bilan qanday aloqa qilishi va kutilmagan o‘zgarishlardan qanday himoyalanganligini o‘rganamiz. Bu esa Blokcheyn tizimida har bir tranzaksiyalar zanjirining butun hayot sikli davomida axborot ishonchliligini ta’minlash hisoblanadi.

Vaholanki, tranzaksiyalar semantik nazoratining yuqoridagi keltirilgan shartlari ularning butun hayot sikli davomida kafolatlangan ishonchliligini ta’minlay olishi gumon. Gap shundaki, agar avval boshdan ishonchli bo‘lmagan tranzaksiya tayyorlangan va bir qatlamli tarmoq ishtirokchilarining 50% dan ko‘prog‘i, ushbu tranzaksiya tafsilotlarining ishonchliligini tekshirish imkoniyatiga ega bo‘lmagan holda ma’qullab ovoz bergan bo‘lsa, u holda mazkur blok Blokcheyn tizimining ommaviy reyestriga bemalol qabul qilinishi mumkin. Shuning uchun semantik nazorat shartlarini shakllantirishda o‘tkaziladigan operatsiyaning amaliy sohasini bilish muhim rol o‘ynaydi.

Blokcheyn tizimining bloklar zanjirini shakllantirish jarayonini va ulardagi ma’lumotlarni himoya qilishni tushunish uchun, Blokcheyn tizimi mulkka egalik huquqini boshqarish uchun to‘liq taqsimlangan bir qatlamli tizim ekanligini esga olish zarur bo‘ladi. U tranzaksiyalar ma’lumotlarining to‘liq xronologiyasini saqlaydigan, umumiy o‘zgarmas reyestrning alohida xususiy versiyasini o‘zida saqlaydigan alohida kompyuterlardan iborat. Shunday qilib, alohida kompyuterlar, muayyan kompyuterning shaxsiy yozuvlariga muvofiq

qandaydir aniq bir tranzaksiya haqiqatan ham bajarilganligini tekshirishlari kerak.

Ammo dastlab alohida kompyuterlar o‘zlari a’zo bo‘lgan Blokcheyn tizimida ro‘y berayotgan tranzaksiyalar haqida qayerdan bilishadi degan savolga javob topishimiz zarur?

To‘liq taqsimlangan bir qatlamli tizimlarda markaziy kompyuter mavjud emas va shuning uchun tizimdagi barcha kompyuterlar bo‘yicha axborotlar markazlashmagan holda taqsimlanadi. Bunday sharoitda Blokcheyn tizimning asosiy vazifasi, tizimning barcha tugunlari – Blokcheyn tizimiga a’zo bo‘lgan kompyuterlar, alohida ajratilgan yoki markaziy kompyuterga murojaat qilmasdan, barcha operatsiyalar haqida to‘liq ma’lumot olishini ta’minlash hisoblanadi.

Taqsimlangan bir qatlamli tizimning tugunlari, ya’ni Blokcheyn tizimiga a’zo bo‘lgan kompyuterlar o‘rtasida axborot almashish tizimi uchta asosiy vazifani bajarishi kerak:

- mavjud ulanishlar uzilib qolmasdan, ularni ishchi holatda saqlash;
- yangi paydo bo‘lgan tugunlar bilan aloqalar o‘rnatish;
- yangi tranzaksiya ma’lumotlarini tarqatish.

Axborot almashuvining dastlabki ikki turi asosan teng hamkorlar tarmog‘ining umumiy ishchi holatini ta’minlashga qaratilgan.

Mavjud ulanishlarni tarmoqdagi har bir kompyuter uchun ish holatida saqlash, hamkorlarning o‘zlarining ro‘yxatlariga muvofiq *ping* shaklida qisqa xabar yuborish, *pong* shaklida javob kutish orqali amalga oshiriladi. Ushbu so‘rov xabarlariga uzoq muddat sukut saqlab, o‘rnatilgan vaqtlarda javob bermaydigan hamkorlar ro‘yxatdan o‘chiriladi.

Shu bilan birga, har bir kompyuter ushbu tizimga kirgan boshqa tugunga murojaat qilishi, ya’ni o‘z reyestriga qo‘shilish to‘g‘risida so‘rov yuborishi mumkin. So‘ralayotgan tugun murojaat qilayotgan tugunning manzilini o‘zining hamkorlari reyestriga qo‘shadi va so‘rovga tasdiq xabarini yuboradi. Javobni olgandan so‘ng, yangi tugun ham yuboruvchi manzilini o‘z hamkorlari reyestriga qo‘shadi. Natijada, yangi aloqa o‘rnatiladi va tizimga yangi tugun qo‘shildi.

Ammo bir qatlamli tizimning asosiy maqsadi mulkka egalik huquqini boshqarish ekanligini esdan chiqarmasligimiz lozim. Shuning uchun, axborot almashishning uchinchi turi blokcheyn ma’lumotlari tarkibiga yangi tranzaksiya bloklarini qo‘shishga

Raqamli texnologiyalar yordamida ular ko‘chmas mulk (kvartiralaradgi xonalar), yo’lovchilar tashish (taksi) va odamlar to’liq bo’lmagan shakldagi ishga joylasjtirish (pensionerlar va doimiy ishga ega bo‘lmagan, lekin ishga layoqatli kishilar) kabi vaqtinchalik foydalanilmayotgan resurslarga ulanadi. Ehtimol, blokcheyn texnologiyasibizni birgalikda iste’mol qilish iqtisodiyotidan bo‘sh turgan quvvatlarn ijaraga berish va ulardan foydalanishni o‘lchash mumkin bo‘lgan o‘lchash iqtisodiyotiga olib kelishi mumkin. Masalan, uy egalari elektr uskunalar, mayda qishloq xo‘jalik texnikasi, baliqchilik anjomlari, duragdorlik asboblari, garaj yoki avtomobillar qo‘yiladigan joyni umumiy foydalanishga rozilik bildiradigan birgalikda iste’mol qilish iqtisodiyotini amalga oshirish usuli yuzaga kelar. Ushbu sohalardagi muammolaridan biri, uzoq vaqt davomida shundan iborat ediki, bunday resurslar sohiblari jamoat uchun ko‘plab tashvishlar tug‘dirar edi. «AQSHda 80 million drel (parmalash uskunasi) bor va ularning har biridan shuncha vaqt ichida o‘rtacha 13 daqiqa foydalaniladi, –deb yozadi «NyuYork tayms» da Airbnb bosh direktori Brayan Cheski. –Shunday ekan, har bir kishi uyiga drel sotib olishi uchun ehtiyoj bormikan?»

Biroq blokcheyn texnologiyasi amalda nolga teng bo‘lgan harakatlar talab qiladigan ortiqcha resurslarni – simsiz ulanish nuqtalarini, kompyuterlarning hisoblash quvvatlarini yoki qattiq diskdagi bo‘sh joylarni, uyali aloqa telefoni orqali puli to‘lab qo‘yilgan ortiqcha daqiqalarni, hattoki o‘zining professional ko‘nikmalarini ijaraga berishga imkon yaratadi– yana shunisi ham borki, bularning barchasi uchun hattoki barmoqni qimirlashtish ham talab etilmaydi, qaergadir begona odamning oldiga borish va keyin qaytib kelish haqida esa gapirmasak ham bo‘ladi. Siz sayohat qilayotgan payt Wi-Finuqtasini ijaraga berib, undan foydalanilgan har bir soniya uchun arzimagan chaqa olishingiz mumkin. Bunda sizni faqat o’zinguzning tasavvuringiz (istiqbolda esa - qonunchilik ham) chegaralaydi, xolos. Sizning obunalaringiz, jismoniy makon, energiya manbalari qismlab boshqa tomonga berilgan va undan mikroto‘lovlar shaklida pul olgan holda daromad manbaiga aylanishi mumkin. Sizdan faqat tomonlar o‘zaro tranzaksiyalarni xavfsiz va ishonchli amalga oshiri uchun nomarkazlashgan uzatish protokoli talab qilinadi, xolos. Bu platformalar istalgan aktivlarga «litsenziyalash» huquqini beradi. Sizdan faqat boshqalarga ulanish va foydalanish huquqini

berish, qay darajada istaingizni hal qilish – hatto boshqalarga sizning aktivlaringizdan foydalanishga ruhsat bermalsik huquqi ham beriladi va buning uchun qandaydir narx belgilash so‘raladi, holos.

Korxonalar o‘z mahsulotlari va texnologik infratuzilmasini yangi biznes va qiymat yaratishda ishtirok etishi mumkin bo‘lgan jamiyatlar yoki tashqi foydalanuvchilarga ochib bergandagina qandaydir platformalar yaratadilar. Bunda mumkin bo’lgan variantlardan biri bu - ishlabchiqaruvchi iste’molchilardir. Mijozlar innovatsiyasi dinamik dunyosidaishlab chiqaruvchi-iste’molchilar yangi avlodi o‘zining «buzib kirish huquqi»ni bor narsa deb qabul qiladilar. Blokcheyn texnologiyasi «ishlab chiqarish-iste’molchi»ga imkon beradi. Nikekrossovkalari taqsimlangan registrda axborot hosil qilishi va saqlashi, o‘z navbatida, uni Nikeva oyoq kiyimini kiyib yurgan shaxs smart-shartnomaga muvofiq pulga aylantirishi mumkin. Agar foydalanuvchi krossovkadagi smart-tarkibiy qismlarni ishga tushirish yoki ularni puls o‘lchagich va qondagi glyukoza darajasini o‘lchash kalkulyatori yoki Nike uchun qimmatli bo‘lgan har qanday axborot to‘plash vositasi kabi boshqa qurilmalar bilan sinxronlashtirishga rozilik beradigan bo‘lsa, Nikeu sotadigan har bir juft oyoq kiyimidan aksiyalar juda kichik ulushini taklif qilishi mumkin.Ayrim platformalar kompaniya mijozlar bilan birgalikda mahsulotlar yaratishga qaror qiladigan iste’mol hamjamiyatlaridan farq qiladi. Ochiq platformalar kompaniyalarga yangi biznes yaratish yoki platformaga qiymat qo‘shish uchun kengroq imkoniyatlar taklif qilishga imkon beradi.Blokcheyn standart umumiy shartnomalar va standart umumiy ma’lumotlar to‘plami (ochiq interfeyslar) taqdim etishni eng yaxshi tarzda ta’minlaydi. Blokcheyn platformalar yaratishni soddalashtirishi va arzonlashtirishi mumkin. Bu hali jarayonning boshlanishi, holos. Eng yaxshisi, blokcheynning umumiy ma’lumotlar to‘plamiaxborot shaffofligi va mobilligini ta’minlash uchunhizmat qiladi, ya’ni, iste’molchilar va ta’minotchilar eng yaxshi shartlarni o’zlari tanlab olishlari mumkin. Shuningdek, elektron ijorat kompaniyalari an’anaviy kompaniyalarning resurslaridan foydalanish o‘rniga o‘z platformalarini yaratib, blokcheynda teng huquqlar bilan ishlashlari ham mumkin.Kelajak avtomobilini tasavvur qiling. U barcha axborotlar oqimlari bilan ishlay olishi, avtomobilning aqlli qismlari esa – tranzaksiyalarni amalga oshira olishi va bunda pul o‘tkazishi mumkin bo‘lgan blokcheyn asosida ishlashi kerak bo‘ladi.

Bunday ochiq platformada minglab dasturchilar va korxonalar sizning avtomobilingiz uchun shaxsiy ilova va dasturlar yaratadilar. Tez orada bunday platformalar butun boshli tarmoqlarni - masalan, moliyaviy hizmatlar sektorini - turli moliyaviy tranzaksiyalar va qiymatlar almashinishni blokcheyn yordamida tartibga solgan holda tubdan o'zgartirib yuborishi mumkin. Jahondagi eng yirik banklar va konsorsiumlar allaqachon bu g'oya ustida ishlashni boshlab yuborishgan. Obrazli qilib aytganda, electron platformalar – sizning omad kemalaringizni yuqoriga ko'taradigan havo oqimidir.

O'ziga xos va murakkab vazifalarni hal qilishga qodir bo'lgan malakali mutaxassislarni izlayotganlar ularni topish uchun o'zlarining talablari haqida registrga xabar berishlari mumkin. Endi InnoCentive o'rniga nafaqat foydalanuvchilarning mobil elektron shaxsni, balki potensial yo'llovchilar haqida ularga mos keladigan va to'ri bo'lgan qo'shimcha axborotlardan iborat bo'lgan mobil rezyumeni ham shakllantiradigan blokcheynnitasavvur qilib ko'ring. Hech kimga tegishli bo'lmagan va shu bilan bir paytda barchaniki sanalgan ko'nikmalar taqsimlangan ro'yxatini tasavvur qiling.Endilikda blokcheyn texnologiyasi va ochiq boshlang'ich kodlar kutubxonasi birgalikda har qanday kompaniya uchun yangi biznes qiymatlari yaratish, innovatsiyalar va bir qancha vazifalarni hal qilish uchun makon taqdim etishi mumkin.Blokcheyn va dasturiy ta'minot omborlari blokcheynlar asoida bunday faoliyatni oziqlantiradi. Kompaniyalar endi to'lov tizimlari ularga kiritilganblokcheyn Ethereum kabi yangi va kuchli dasturlash tillaridan foydalanishlari mumkin bo'ladi.

Turli tarmoqlar ishlab chiqarishga katta e'tibor qaratgan holda moddiy ob'ektlar tayyorlash, ularning loyihasini ishlab chiqish va moliyalashtirish uchun global ekotizimlarning rivojlanishini rag'batlantirishi va shu tariqa birgalikda bir rangdagi ishlab chiqarishning yangi bosqichini yaratish tashabbusi bilan chiqishi mumkin. Bu yerda asosiy masala va maqsad hamma ishni blokcheynda amalga oshirishdan iboratdir. Zamonaviy samolyotlar «saf bo'lib uchadigan mustaqil elementlar jamlanmasi» deb atalishi kabi, kompaniyalar ko'plab tarmoqlardaajralish va hamkorlar tarmog'iga birlashish tendensiyasini namoyish etadi. Individual buyurtmalar bo'yicha ommaviy ishlab chiqarishni yo'lga qo'yish maqsadidahuddi blokcheyn kabi, 3D-bosma texnologiyasi ham ishlab

chiqarishni foydalanuvchiga yaqinlashtirmoqda. Tez orada axborot egalari va huquq egalari inson hujayralaridan boshlab, alyuminiy kukunigacha bo'lgan har qanday narsa haqidagi metama'lumotlarni blokcheynda saqlashi mumkin bo'ladi va bu korporativ ishlab chiqarish chegaralarini misli ko'rilmagan darajada kengaytiradi.Bu texnologiyalar tovarlar bilan ta'minlanganlikni va ularning ta'minot tarmog'i bo'ylab harakatini kuzatish uchun ulkan imkoniyatlar beradi. Har bir kishining qalbiga (va boshqa tana a'zolariga) yaqin bo'lgan tarmoq – oziqovqat sanoatini tasavvur qilib ko'ramiz. Hozir supermarketda halol sharoitlarda va yaxshi boqilgan, dori-darmonlar berilmagan, ekologik tozaqoramol go'shti sotayotganini ta'kidlash va hatto bunga chin dildan ishonish ham mumkin. Lekin savdo tarmoqlari buni yuz foiz kafolatlay olmaydi. Hech kim har bir molning biografiyasini yozib o'tirmaydi,biz esa bu go'shtdan bifshteks pishiramiz, lekin uning «ishonchli» ekanligini tekshirish uchun esa vositalarga ega emasmiz. Odatda bunga ko'z yumish ham mumkin – axir butun dunyo bo'ylab milliardlab bifshtekslar sotiladi va sotilmoqda. Lekin ba'zida qoramol qutirish kasalligi epidemiyasi ham uchrab turadi, bu esa sog'lik uchun koni zarar.Oziq-ovqat sanoati blokcheynda nafaqat har bir buqaning raqamini, balki istiqbolda jonivorning DNKga bog'lab qo'yilgan har bir go'sht parchasi raqamini saqlashi mumkin. Uch o'lchamli qidirish imkoniyatlari foydalanuvchi jonivor tarixini va uning aynan o'xshashligini bog'lash uchun qoramol va parrandani to'liq miqyosda kuzatish imkonini beradi. Ma'lumotlar to'plamlarini intellektual boshqarish va ularni DNK asosida identifikatsiyalashga imkon beradigan murakkab (lekin qo'llash oson bo'lgan) texnologiyalar tufayli hatto eng yirik go'sht ishlab chiqaruvchilar hamhar bir bo'lak go'sht sifati va xavfsizligini kafolatlay oladilar. Tasavvur qiling, bu axborot laboratoriya tadqiqotlarini qanchalik soddalashtiradi va jiddiy vaziyatlarda sanitariya hizmatlariga javobgarliklarni tezlashtiradi.

Blokcheyn texnologiyasi firma ichida hamda firmalar va turli tashqi qatnashchilar o'rtasida ham teng huquqli qo'shma faoliyatni ta'minlashga qodir. Buxgalteriya hisobi uchun, istalgan muhitda raqamli resurslardan foydalanish va faoliyat yuritish uchun, bular valyutami, ijtimoiy munosabatlarmi yoki tashkilot bo'lishidan qat'i nazar, to'liq taqsimlangan mexanizmni ishlatishga imkon beradi.Bugungi kunda birgalikda ishlash uchun turli tijorat vositalari

asta-sekinlik bilan tashkilot ichida boshqaruv va axborot bilan ishlash mohiyatini ancha o‘zgartirib yuboradi. Jive, IBM Connections, Microsoft Yammer, Google Apps for Work va Facebook at Work kabi mahsulotlar innovatsiyalarni qo‘llabquvvatlash va unumdorlikni oshirish uchun qo‘llaniladi. Ijtimoiy dasturiy ta’minot tez orada mahsulot ishlab chiqishdan tortib, kadrlar siyosati, marketing, servis va sotuvgacha bo‘lgan biznes-operatsiyalarning har bir elementi uchun hayotiy muhhim vositaga –ma’lum ma’nodayigirma birinchi asr tashkiloti uchun yangi operatsion tizimga aylanadi. Biroq hozirdagi texnik va dasturiy vositalar to‘plami aniq cheklovlarga ega, blokcheyn esa bu texnologiyalarni yangi sifat darajasiga ko‘taradi. Blokcheynda korporativ ijtimoiy tarmoq qanday ko‘rinishga ega bo‘lishi mumkinligi masalasini ko’rib chiqamiz. Korporativ Facebookni (yoki boshqa istalgan ijtimoiy tarmoqni) tasavvur qiling. Har bir foydalanuvchi ko‘p fuknsionalli hamyonga, normarkazlashgan tizimga portal ko‘rinishida namoyon bo‘ladi. Aytish mumkinki, bu mobil profil – sizning hisob qaydingiz yoki ejektron shaxsdir. Facebook hisob qaydidan farqli ravishda, hamyon bir qator funksiyalarga ega bo‘lib, turli xildagi shaxsiy va professional axborotlarni, shuningdek, boyliklar, jumladan, pulni saqlaydi. Bundan tashqari, unga faqat siz ulanish imkoniga ega bo‘lasiz va o‘zingiz istagan axborotni ochib berishingiz mumkin bo‘ladi.Albatta, bu yerda reklama –uchinchi tomonlar yoki sizning HR-bo‘limining ijtimoiy paket tarkibidagi ochiq to‘plamyoki o‘zgartirilish haqida e’lonlar bo‘ladi, lekin siz ularni ko‘rib chiqqaningiz tufayli daromad yoki boshqa bir mukofot olasiz. Bu ko’pchilik tomonidan «e’tibor bozori» deb ataladi. Siz reklamani tomosha qilish yoki u bilan aloqa qilish uchun,yangi reklama kampaniyasida ishtirok etish uchun, robot emaslgingizni tasdiqlash yoki skaner qilingan hujjatlarni kiritish uchun mikrokompensatsiya olasiz. Yangiliklar oqimi, nashrlar tizimi vae’tiborbozori o‘xshashib ketadi, lekin ularda to‘lovlar turlicha usulda amalga oshiriladi.

Tajribaning ko‘rsatishicha, raqamli davrda g‘alaba oxir-oqibat qiymat (boylik) ortida qoladi. Taqsimlangan foydaning afzalliklari foydalanuvchilar va kompaniyalar uchun bir talay. Ijtimoiy media kompaniyalari resurslarning juda katta ekanligiga qaramay, ularda ochiq muhitda ishlab chiqish mumkin bo‘lgan funksionallik xilma-xilligining cheki yo‘q. Yopiq formatli operatsion tizimlar bilan Linux

muvaffaqiyatlari va kuchini taqqoslang. Blokcheyn texnologiyalari xavfsizlikni ham ta’minlaydi. Sizning hayotingiz siz istagan darajada maxfiy bo‘ladi. Hech qanday ijtimoiy tarmoqsizning axborotingizni sizning ruxsatingizsiz davlatga sota olmaydi yoki uning chiqib ketishiga yo‘l qo‘yishi mumkin emas. Agar siztotalitar davlatda dissident bo‘lsangiz, sizning tarmoqda yozayotgan yoki o‘qiyotgan narsalaringizni hech kim kuzata olmaydi. Siz o‘z axborotingizga ega ekanligingiz sababli, e’tiboring va harakatlaringiz bilan birga uni monetizatsiya qilishingiz ham mumkin. Kompaniyalar ham o‘z xodimlarinng bunday platformalardan biznes uchun foydalanishini rag‘batlantirishi lozim. Qimmatli kadrlarni jalb qilish uchun kompaniya xodimlarning shaxsiy ma’lumotlari va xavfsizlikka hurmatini va korporativ odob-axloqni namoyish etishi lozim. Yana ham muhimi, tarmoq tuzilmasiga ega bo‘lish va tashqaridan mutaxassislar jalb qilish bilan birga, har bir firma hamkorlar ularga ishonadigan bir nechta korxonalar birgalikda ishlashi uchun platformalar taklif qilishi ham mumkin. Bularni esa albatta barcha barsaga qodir bo’lgan vaqt ko‘rsatadi. Umuman, tarmoq tuzilmasiga ega bo‘lganochiq kompaniyalar innovatsiyalarni rag‘batlantirish hamda aksiyadorlar, mijozlar va butun jamiyat uchun sifatli boylik yaratish imkoniyatlaridan foydalanish uchun katta va radikal salohiyatga ega bo‘ladi. Texnologiya bozordagi harajatlarni pasaytirishda davom etadi, bas shunday ekan, korporatsiya doirasida kamida faqat dasturiy ta’minot va kapital qolishini tasavvur qilish mumkin.Birinchidan, «qidirish» harajatlari pasayishda davom etadi, yangi agentlarmavjud yoki qachonlardir mavjud bo‘lgan barcha tijorat axborotlarini Global Registr bo‘yicha uch o‘lchamli qidirishni amalga oshirishi mumkin. Shu sababli korporativ arxivlar, axborot bo‘yicha mutaxassislar, personal tanlash bo‘yicha mutaxassislar va biznes uchun zarur axborot xarid qilish bilan shug‘ullanadigan boshqa mutaxassislarga zarurat qolmaydi.Ikkinchidan, smartshartnomalarshartnoma tuzish harajatlarini, shartnomalar bajarilishi va to‘lovlar o‘tkazilishi ustidan nazoratni sezilarli darajada pasaytiradi. Qog‘oz shaklidagi hujjatlarga ehtiyoj sezmaydigan bu dasturlar shablonlar tizimi orqali shartlarni ifodalaydi, tashqi manbalardan to‘plangan keng axborotlar va qoidalar to‘plami asosida axborotni muhokama qiladi, qabul qiladi yoki inkor etadi, ish natijalarini bajarishga va tranzaksiyalar amalga oshirishga

talablarnibelgilaydi.Uchinchidan, tashkilot doirasidan tashqarida bu resurslarning barchasini muvofiqlashtirish harajatlari sof nominal bo‘ladi –korxona dasturiy ta’minoti bajariladigan serverlarda ishlashi uchun elektrenergiyasi uchun to‘lovlar kerak bo’ladi, xolos. Korxona yollagan odamlar, tashkilotlar va zavodlarni boshqarish uchun byurokratiya tizimi talab etilmaydi. Yangi platforma yordamida mijozlar uchun qiymat va mulkdorlar uchun boylik yaratish uchun an’anaviy menejment yoki ierarxiya umuman yoki deyarli talab qilinmaydigan yangi tashkilotlarni tasavvur qilish unchalik qiyin emas. Va nihoyat, ishonch asosidagi munosabatlar o‘rnatish harajatlarni nolga yaqinlashtiradi. Ishonch tashkilotga emas, blokcheyn ishini ta’minlaydigan ko‘plab odamlarning birgalikdagi ommaviy ishlariga, dasturiy kodni tekshirish va xavfsizlik hamda funksionallikka bog‘liq bo‘lib qoladi.

Taqsimlangan mustaqil korxonani qanday tashkil qilish mumkin? Bunday kompaniyakeng funksionalga–oldindan belgilangan reglament asosida ma’lum doiradagi vazifalarni yoki kengroq biznes-funksiyalarni bajaradigan agentlarga ega bo‘lishi lozim. Xususiy shaxslar, potensial aksiyadorlar yoki foydalanuvchilarning jamoalari yoki tashkilotlar quyidagi ko‘rsatkichlarni belgilagan holda bunday korxonalar ochishi mumkin.

1. Qiymatga yo‘naltiriganlik: dunyoni o’zgartirish va qiymat yaratish yoki uni o‘zgartirish uchun zarur bo‘lgan jarayonlarni tushunish.

2. Bajarishi lozim bo‘lgan vazifa: tashkilot mavjudligidan qanday ma’no kutiladi? Bu korxonani nima uchun tashkil qilyapmiz?

3. Konstitutsiya: tashkilotning umumiy maqsadlari va u qiymat yaratadigan qoidalarni tavsiflash lozim.

4. Ish usullari: masalan, tashkilot qiymat yaratishda o‘zini qanday tutishi, u qanday moliyalashtirilishi (kraudfanding orqali, ilk bosqichda an’anaviy investitsiyalar orqali, foyda hisobidan), resurslarni qanday xarid qilish zarur.

5. Mehnatning odamlar va mashinalar o‘rtasida taqsimlanishi: yaqin istiqbolga, aftidan, yaratilayotgan tizimda odamlar rahbarlik qilishi lozim.

6. Dastur funksiyalari: korxona tashqi shartlar o‘zgarishini qanday aniqlaydi va ularga qanday javob qaytaradi.

7. Odob-axloq kodeksi: bu yerda «yovuzlik qilma»Googletamoyili bilan cheklnaib bo‘lmaydi. Taqsimlangan mustaqil korxonaga maqbul keladigan xulqatvor aniq va ravshan ta’riflanishi kerak bo‘ladi.

Ehtimol, yaqin kelajakdataqsimlangan mustaqil korxonalar hali paydo bo‘lmaydi, lekin ular ortida turgan kontseptsiya biznes-strategiyaga ta’sir etishi mumkin. Global pirring platformalari rivojlanishi bilanshaxsni tasdiqlash, ishonch asosida munosabatlar o‘rnatish, nufuz shakllantirish va tranzaksiyalar o‘tkazish uchun biz nihoyat innovatsiyalarga hizmat qilish, birgalikda qiymat yaraitsh va ehtimol, kamchilikni boyitish emas, ko‘pchilikning muvaffaqiyatga erishishiga hizmat qilishi lozim bo‘lgan chuqur firma tuzilmalarini o‘zgartirish mumkin. Yuqoridagilarni diqqat bilan o’qib chiqqan bo’lsangiz, siz boylikni demokratik ruhda taqsimlashni ta’minlaydigan va tarmoqni muvozanatdan olib chiqishga yordam beradigan yangi biznes-modellar haqida ancha narsalarni bilib oldingiz.Umuman olganda, uzoqni ko‘zlab ish yuritadigan kompaniyalarblokcheyn iqtisodiyotida ishtirok etishga harakat qiladi. Rivojlanayotgan dunyoda qiymat yaratishni (tadbirkorlik tufayli) va qiymatda ishtirok etishni (kompaniyaga taqsimlangan mulkchilik orqali) taqsimlash mexanizmi muvaffaqiyatga erishish paradoksini hal qilishga qodir deb o’ylaymiz. Alohida shaxslar yoki markazlashtirilgan vositachi-ilovalar emas, piring tarmoqlari qatnashchilari tomonidan jarayonlarni modernizatsiya qilish va avtomatlashtirish yuqorida qayd qilingan qator ustunliklar keltirishga qodir, jumladan:

- tezlik (boshdan-oxir avtomatlashtirish);
- harajatlar pasayishi (amalda cheksiz ma’lumotlar hajmini ulkan qayta ishlash markazlariga yetkazish bilan bog‘liq; bunda qimmatga tushadigan vositachilarni istisno qilish);
- foyda, natijaviylik va yoki unumdorlikni oshirish (ortiqcha resurslarni ulardan takroriy foydalanish uchun bo‘shatish);
- samaradorlikni oshirish (kiritilgan nazorat reglamentlari va inson omilining ta’sirini pasaytiradigan boshqa protokollar);
- axloqiylik va xavfsizlikni oshirish (shaxsiy ishonch talab qilinmaydi, chunki ishon tarmoq arxitekturasiga kiritilgan bo‘ladi);
- tizimning ishdan chiqish ehtimoli pastroq (zaif jihatlarni bartaraf qilish, ishdan chiqishga chidamlilik);

-energiya iste'moli pastligi (energiya sarfi tarmoqning o'zi tomonidan yo'qotishlarni pasaytirish va samaradorlikni oshirish, dinamik narx shakllantirish va teskari aloqasirtmoqlari bilan o'rni qoplanadi);

-shaxsiy axborotlarning himoya qilinishini yaxshilash (vositachilar blokcheynda berilgan qoidalarni buzishi yoki pisand qilmasligi mumkin);

-«Cheksiz ma'lumotlar» to'plash va tahlil qilish tufayli ularni yaxshilash imkoniyatlari, jarayonlar va qonuniyatlarni yaxshiroq tushunish;

-turli xildagi ham salbiy (noqulay ob-havo, zilzila, sog'liq bilan bog'liq muammolar), ham ijobiy (qishloq xo'jalik ekinlari ekish uchun qulay vaqt, xarid shablonlari) hodisalarni bashorat qilish imkoniyatlarini yaxshilash.

Taqsimlangan ochiq model shuni anglatadiki, kompaniya bozorni tark etadigan yoki ishlab chiqaruvchi xonavayron bo'ladigan bo'lsa ham,buyumlar Interneti tarmoqlar io'zini-o'zi qo'llab-quvvatlashi mumkin. Tizimga kiritilgan birga bo'la olishlik buyumlar internetining turli tarmoqlarini birlashtirish va yanada kattaroq qiymatni amalga oshirishga imkon beradi.Bu afzalliklarning ko'pchiligi taqsimlangan yoki nomarkazlashgan tarmoqlar konsepsiyasiga hamda markaziy (ya'ni hukumat vertikali) va boshqa vositachilarni (masalan, kliring palatasi yoki boshqaruv dasturi) chiqarib tashlashga asoslanadi. Blokcheyn texnologiyasiistalgan shaxsga o'zining rivojlanish, gullab-yashnash yo'l xaritasini tuzishga imkon beradi. Raqamli iqtisodiyotda ishtirok etish uchun eng oddiy shartlar – uyali aloqa telefnoi va internetga ulanish imkoniyati yetarli boladi. Yuqorida ta'kidlaganimizdek, blokcheyn texnologiyasiilgari imkoni bo'lmagan, har bir kishiga iqtisodiy munosabatlar qatnashchisi bo'lish imkonini beradigan biznes-modellar yaratishga imkon beradi. Blokcheyn kompaniya yaratishning uchta tarkibiy qismi bor – uni tashkil qilish, moliyalashtirish va uni bozorda ilgari surishni atvomatlashtirish, soddalashtirish va sezilarli darajada takomillashtirish. Kelejakda bunday kompaniyani tashkil qilish qiymati sezilarli darajada pasayadi, chunki blokcheyn – korxonani ro'yxatdan o'tkazishning mashhur va ishonchli usuli hisoblanadi. Mulk hamma uchun ko'rinarli, qaydlar yuritish esa oson, bu ayniqsa,

qonunchilik bilan tartibga solish qiyin bo'lgan sohalarda foydali bo'ladi. Ishonchli va o'zgarmas rekgistrlar tufayli, tadbirkorlar o'z korxonalarini va korporativ aktivlarga egalik qilishni ro'yxatdan o'tkazishi, tovar zaxiralari va majburiyatlarini boshqarishi, shuningdek, uch karralik buxgalteriya hisobi yoki blokcheyndagi boshqa ilovalar uchun dasturiy ta'minot yordamida boshqa moliyaviy ko'rsatkichlardan foyda olishi mumkin, bu esa auditorlar, soliqqa tortish bo'yicha mutaxassislar va kichik korxonalarga boshqa hizmatlar ta'minotchilariga ehtiyojni pasaytiradi. Smart-shartnomalar tufaylitadbirkor kompaniya faoliyatining ko'plab jihatlarini avtomatlashtirishi mumkin, chunonchi: xaridlar, mehnatga haq to'lash, kredit bo'yicha foiz, real vaqt rejimida moliyaviy audit. Blokcheyn orqali yakka tartibdagi tadbirkorlikning ikkita yangi modeli yuzaga keladi:

-ortiqcha narsalarni dozalangan tarzda ijaraga olish va ijaraga berish. Blokcheyn xususiy shaxslarga noan'anaviy qiymat yaratish va daromad olishga imkon berad;

-ma'lumotlarni mikromonetalashtirish. Dekret ta'tilidagi ota-ona va kichkina bolalar yoki keksa ota-onaga qarash bilan band bo'lgan boshqa oila a'zolari nihoyat o'z uy mehnatini monetarizatsiyalashtirishi va ular har soat yaratadigan qiymat uchun e'tirofga ega bo'lishi mumkin;

- raqamli «aqliy hujum». Muammolar yoki ehtiyojlarni aniqlash maqsadida real vaqt rejimida davlat amaldorlari va oddiy fuqarolar moderatsiya qilinadigan onlayn-sessiyalar tashkil qilish. Bitimga jiddiy munozaralarga sababchi bo'ladigan va qoidabuzarlar, provokatorlar va zararkunandalar uchun butun jarayonga qandaydir ziyon etkazishni imkonsiz qilib qo'yadigan «bitta odam – bitta ovoz» onlayn ovoz berish tizimi orqali erishiladi;

-qasamyod qilgan onlayn hakamlar va oddiy fuqarolardan iborat bahsmunozaralar qatnashchilari. Fuqarolar turli mavzular bo'yicha masalalarni hal qilish uchun hakamlar va maslahatchilar sifatida ishlash uchun tasodifiy usul bilan tanlab olinadi. Hakamlar axborot bilan o'rtoqlashish, savollar berish, muammolarni muhokama qilish, dalil-isbotlarni bilib olish uchun Internetdan foydalanadilar. Blokcheyn nufuz tizimlari munozara qatnashchilari va hakamlar

nufuzi haqida ma'lumotlar va ularning tarjimai holini bilib olishga yordam beradi. Qarorlar va muhokamalar blokcheynda qayd qilinadi;

-deliberativ so'rovlar. Bu vositafuqarolargamuammolar haqida bilib olish va ular borasida o'z fikrini bildirishga imkon beradi. Bunday so'rovlar internetda tasodifiy tarzda tanlab olingan bir nechta olimlar bilan kichik guruhlarda muhokamalar tashkil qilishni ko'zda tutadi. Bularning barchasifuqarolarni siyosiy vazifalarni hal qilishga jalb qilish maqsadida amalga oshiriladi va bu yerda natija doimiy so'rovlar bilan taqqoslaganda samaraliroq bo'ladi;

-ssenariylarni modellashtirish. Iqtisodiyotning kelajakdagi ehtiyojlarini ifodalash va qarorlarning uzoq muddatli oqibatlarini tushunish uchun modellashtirish dasturiy vositalari yordamida ssenariylar tuziladi. Siyosatchilar, amaldorlar va fuqarolarsog'liqdan boshlab, atrof-muhit va iqtisodiyotgacha bo'lgan bir qator omillar potensial ta'sirini baholashi mumkin.

Blokcheyn texnologiy asi hukumat harajatlarini, shuningdek, uning hajmini qisqartirishi mumkin, lekin bizga baribir ko'plab sohalarda yangi qonunlar kerak. Mualliflik huquqlari va intellektual mulk muammolarini hal qilish uchun texnologik va biznes-modellar mavjud. Shu sababli, patentlarning ortiqcha himoya qilinishi tufayli innovatsiyalarni nobud qiladigan eski qonunlarni qayta yozish yoki ulardan umuman voz kechish zarur.

2.2. Tarmoqda blokcheyn va ishbilarmonlik axloqi

Ishonch – jarayonning tashqi emas, ichki elementi hisoblanadi. Blokcheynning asosi esa barcha qatnashuvchilar orasidag ishonchga asoslanga. Unda ma'lumotlar bir bosqichda kodlashtiriladi va bitta qatnashchi tomonidan nazorat qilinmasdan, balki nazorat barcha qatnashchilar o'rtasida taqsimlanadi. To'g'ridan-to'g'ri qadriyatlar almashinish ikkinchi tomon odob-axloq doirasida harakat qilishini kutgan holda amalga oshiriladi. Shunday qilib, ishbilarmonlik axloqi qadriyatlari – ishda va so'zda halollik, o'zgalarning manfaatlarini hisobga olish, o'z qarorlari va harakatlarining oqibatlari uchun javobgarlik, qaror qabul qilish va harakatlar shaffofligi – qaror qabul qilish huquqlari, rag'batlantirish tuzilmalari va operatsiyalarning o'zi ham kodlanadi, shunday ekan, blokcheynda jamoa odob-axloq me'yorlarini buzishning imkoni bo'lmaydi, yoki bu katta vaqt, pul,

kuch-quvvat va nufuz harajatlarini talab qiladi. Internetda bevosita biznes yuritish yoki tranzaksiya amalga oshirishshu paytgacha oddiy bir sababga ko'ra imkonsiz bo'lgan, chunki pul o'z tabiatiga ko'ra boshqa axborot tovarlari va intellektual mulkdan farq qiladi. Hamma do'stlarga bitta selfini yuborish mumkin, lekin kimgadir to'lab bo'lingan bir dollarni do'stingizga yubora olmaysiz. Pul sizning hisobraqamingizdan chiqarilishi va do'stingizning hisobraqamiga o'tkazilishi lozim. Pul bir vaqtning o'zida ikkita joyda bo'la olmaydi, katta miqdordagi pul haqida esa gapirmasak ham bo'ladi.

Turli joylarda raqamli valyuta birligini ikki marta sarflash riski bor – shunda ulardan biri to'lanmagan chek kabi to'lov uchun qabul qilinmaydi. Bu aktivni ikki marta sarflash muammosi deb ataladi.Bitkoynblokcheynida tarmoqdagi bitkoyin egasi muayyan bitkoyinni sarflagan birinchi tranzaksiyaga belgi qo'yadivabu bitkoyndan takroriy foydalanishga to'sqinlik qiladi, shu tariqa ikki marta sarflash imkoniyatini bartaraf qiladi. Tarmoq qatnashchilari, bitkoynto'liq funksional boshqaruvchilari, maynerlar, eng yangi tranzaksiyalar haqida ma'lumot to'playdi va ularni har o'n daqiqa ma'lumotlar bloki ko'rinishida saqlaydilar. Har bir blok faqat undan oldingi blok mavjudligidagina amalda bo'ladi. Bayonnomalarga shuningdek,har bir uzel blokcheynni to'laligicha saqlashi uchun disk makonini regeneratsiya qilish usuli kiritiladi. Nihoyat, blokcheyn ommaviydir, chunkiundagi tranzaksiyalar qanday o'tishi hammaga ko'rinib turadi. Shunday qilib, tranzaksiyaniyashirishning hech ham imkoni yo'q, bitkoynni kuzatish oddiy pulni kuzatishdan osonroqdir.Mayning jarayonlari – tranzaktsiyalar blokini yig'ish, resurslar sarflash, masalani hal qilish (boshqorimalar ketma-ketlikda bo'lganima'qul), murosa (consensus)ga erishish, tashqi registr nusxasini qo'llabquvvatlash shu qadar muhimki, ayrimlar bitkoyn blokcheynini huddi internet kabi foydali deb aytadi va uni ommaviy qo'llab-quvvatlashga chaqiradi. Endi esa bu holatlar blokcheynniiqtisodiyotda qo'llash masalasida nimalarni anglatadi, degan savolni ko'rib chiqamiz. Odamlar shaxsini tasdiqlash va ularning hozircha dog' tushmagan nomiga kafillik berishni yirik kompaniyalar va davlat muassasalariga ishonib topshirish o'rniga bu funksiyalarni tarmoqqa ishonamiz. Butun tarix davomida birinchi marta tranzatsiyalarga va ikkinchi tomon harakatlaridan qat'i nazar, yozilgan axborotlarning katta qismiga ishonchni ta'minlaydigan

blokcheyn ko'rinishidagi ochiq platforma paydo bo'ldi.Tizim ma'lumot saqlash va uni boshqarish jarayonini yagona nazorat markazi bo'lmagan bir rangdagi tarmoqda amalga oshiradi ma'lumotlarni tarmoq bo'yicha taqsimlaydi. Bironta tomon ham tizimni buzishga qodir emas. Agar bironta hukumat organibitta qatnashchi yoki qatnashchilar guruhini uzib qo'yish yoki alohida ajratishga erisha oladigan bo'lsa, tizim ishlashda davom etaveradi. Agar tarmoqning katta qismi uning ustidan nazoratni qo'lga kiritadigan bo'lsa, nima ro'y berayotganini hamma ko'rib turadi.Internet paydo bo'lgan paytda xodimlar, fuqarolar, mijozlar yoki boshqa tashkilotlardan iborat katta foydalanuvchilar bazasiga ega bo'lgan bironta yirik institut o'zining ijtimoiy majburiyatlari haqida o'ylamasdi. Markazlashgan hukumat organlari muntazam ravishda bu haqida xabardor qilmasdan foydalanuvchilar fikriga zid ravishda harakat qilish, ularning ma'lumotlarini to'plash va tahlil qilish, ularni davlat talabi bo'yicha taqdim etish, foydalanuvchilar roziligisiz keng ko'lamli o'zgarishlar joriy qilishga tayyorligi va qodirligini namoyish etib kelar edi.Bitkoyn blokcheynini nazorat qilishga urinish harajatlariolinishi mumkin bo'lgan moliyaviy foydadan ancha katta bo'lishi mumkin. Satosi Nakomoto foydalanuvchidan tarmoqni himoya qilish va yangi bitkoinlar ishlab chiqarish uchun katta hisoblash quvvatlari (demak, ko'p elektr energiyasi) sarflashni talab qiladigan ishni isbotlash usulini joriy qildi. Shu sababli, vositachilarga ehtiyoj yuzaga keladi. Blokcheyn faoliyatining eng yaxshi namoyon bo'lishga sabab ommaviy hamkorlikdir. Har bir kishi o'z axboroti, o'z mulki va o'zining ishtirok etish darajasi ustidan hukmronlik qiladi. Taqsimlangan hisoblash quvvatlari taqsimlangan jamoaviy hukumat tashkil qilishga imkon beradi.Ehtimol, bunday platforma ne'matlar yaratishning yangi taqsimlangan modellari sari yo'l ochib berar. Ehtimol, to'g'ridan-to'g'ri nomarkazlashgan hamkorlik yangi usullari jamiyatda yuzaga kelgan muammolarni hal qilishga imkon berar. Ehtimol, ishonchsizlik inqirozini va hatto hozirgi institutlarda noqonuniylikni bartaraf qilish, piar-qadamlar o'rniga so'zda emas, ishda muvaffaqiyatga erishish va jamiyat hayotida ishtirok etishga imkon beradigan aholi qo'liga real hokimlik qilishni topshirishga erishilishi mumkin. Blokcheyn tizimi barcha manfaatdor shaxslarning motivatsiyasini o'zaro muvozanatlashtiradi. Bitkoyn yoki qandydir qiymatni aks ettiradigan token – nufuz bilan bog'liq munosabatlarning

ajralmas qismdir. Satosi Nakomoto tizimda ishlaydiganlarni mukofotlashni dasturiy asoslab berdi va hamma uning saqlanishi haqida qayg'urishi uchun hokimlik qilishni tokendan foydalanuvchi barcha jamoaga topshirdi. Blokcheyn – moliyaviy ma'noda, global taqsimlangan savatlardagi tuxumlardir.

Internetning ilk avlodi davridahokimlik qilishnig korporatsiyalarda mujassam etilishi, ularning hajmi, murakkabligi va shaffofsizligiyangi imkoniyatlar taqdim etgan tarmoqlardan nomutanosib ravishda katta foyda olishga imkon berdi. Yirik banklaro'z faoliyati bilanmoliya tizimini shaffoflik chegarasiga yetkazdi, chunki bu banklarda ko'pchilik top-menejerlar va qator mutaxassislarni rag'batlantirish tizimi shunday ishlab chiqilgandiki, ular uzoqni ko'ra bilmaydigan va o'ta riskli xulq-atvorlilarga hizmat qilar edi.Jismoniy valyutalardan farqli ravishda, bitkoyn sakkizta o'nlik razryadgacha ulushga bo'linishi mumkin (ya'ni bitkoindagi summa verguldan keyin sakkizta belgigacha ega bo'lishi mumkin). Bu uzoq vaqt davomida bitta tranzaksiya doirasida summalarni birlashtirish va bo'lishga imkon beradi: summadan ma'lum miqdor olish va bu summadan moliyalashtiriladigan barcha chiquvchi to'lovlar yagona tranzatsiya sifatida ko'rib chiqilishi mumkin, bu esa tranzaksiyalar seriyasidan ancha qulaydir. Hizmatdan foydalanishni hisobga olish uchun smart-shartnoma tuzib, avtomatik raivshda uni muntazam vaqt oraliqlari orqali kichik ulushlar bilan to'lash mumkin.

Smart-shartnomalar. Moliya-kredit tizimidagi o'zgarishlar sur'ati smart-shartnomalar paydo bo'lishiga va uning tobora ko'proq ishlatilishiga hizmat qilmoqda. Hozir ko'pchilik kompyuter savodxonligiga ega bo'libgina qolmasdan, yangi texnologiyalarning nozik jihatlarini ham o'rganib olmoqda. Tranzaksiyalarni qayd qilishga keladigan bo'lsak, bu yangi raqamli vosita o'z xususiyatlari bo'yicha qog'oz shaklidagi o'tmishdoshlaridan jiddiy farq qiladi. Kriptograf Nik Sabo aytib o'tganidek, ular nafaqat kengroq doiradagi axborot (xususan, til bilan bog'liq bo'lmagan sensorik axborot) qayd etishga qodir, balki dinamik hususiyatlarga ega hisoblanadi ham. Ular axborot uzatishi va ayrim turdagi qarorlarlar avtomatik tarzda qabul qilishi mumkin. Sabo ta'rif berishicha, «raqamli intellektual media hisob-kitoblarni amalga oshirishi, bevosita mashinalarni boshqarishi va ayrim mulohazalarni odamlardan ham yaxshiroq bajarishi mumkin». Ushbu muhokamada biz smart-shartnoma deganda,

odamlar va tashkilotlar o‘rtasida qayd qilingan bitimlarni kafolatlaydigan, nimalarnindir bajarishga ruxsat etadigan va ularni ijro etadigan intellectual kompyuter dasturlarini tushunamiz. Shunday qilib, ular ushbu bitimlrani muhokama qilish va tavsiflashda ham ishtirok etadilar. Sabo ushbu atamani 1994 yil, birinchi web-brauzer, Netscape bozorga chiqqan vaqtda taklif etgan edi. Smart-shartnoma bu–shartnoma shartlarini ijroga keltiradigan kompyuterlashtirilgan aqlli tranzaksiya protokolidir. Smart-shartnomalar sxemasining asosiy maqsadlari–umumiy muayyan shartlarni qondirish (masalan, to‘lov shartlarini, garov huquqlarini, mahfiylikni, hatto sanksiyalar kabi shartlarni ham), ataylab qilingan va tasodifiy istisnolarni minimal holatga keltirish, ishonchli vositachilarga ehtiyojni pasaytirishdan iborat. Bunday kontraktlar bog‘langan iqtisodiy maqsadlarni amalga oshiradi, firibgarlik tufayli yo‘qotishlarni minimallashtiradi, arbitraj va majburiyatlarni majburiy ijro etish harajatlari va boshqa tranzaksiya harajatlarini pasaytirishni o‘z ichiga oladi. Smart-shartnoma g‘oyasi tajribaga asoslanmagan, sinalmagan bo‘lib ko‘ringan bir paytda hech qaysi mavjud texnologiyalar uni Sabo tavsiflaganidek amalga oshirishga imkon bermagan bo‘lardi. Strukturalangan axborotni sotuvchilar va xaridorlar kompyuterlari orasida uzatish uchun standartlarni ta’minlaydigan elektron ma’lumot almashinish (EDI) kabi kompyuter tizimlari bo‘lgan, lekin hech qanday raqamli texnologiya bungacha qadar real to‘lovlar bilan ishlash tashabbusi bilan chiqmagan va bevosita pul mablag’lari almashinishni amalga oshira olmagan.Bitkoyn va blokcheyn tizimi buni tubdan o’zgartirib yubordi. Endi tomonlar o’zaro bir tomonlama yoki ikki-uch tomonlama bitimlar tuzishi va bitim shartlari bajarilganda bitkoinlarni avtomatik ravishda sotishi mumkin. Oddiy misol: agar siz akangiz billan xokkey o‘yini natijasi borasida garov boylashgan bo‘lsangiz, u to‘lovdan qochib qola olmaydi. Murakkabroq misol: agar siz aksiyalar xarid qiladigan bo‘lsangiz, bitim darhol tartibga solinadi va aksiyalar shu ondayoq sizga o‘tkaziladi. Yanada murakkab bir misol: pudratchi tadbirkorga mos keladigan daturiy kod jo‘natishi bilan u avtomtik ravishda to‘lov oladi. Cheklangan smart-shartnomalarni amalga oshirishning texnologik vositalari hozirda mavjud va bir qancha platformalarda ishlab ham turibdi. Demak, bunday smart-shartnomalar –uni amalga oshirishning qonuniy yo‘li bilan avtomatik ravishda ta’minlanadigan, shartnoma

shartlarini intellectual ravishda avtomatik holda bajara oladigan, blokchyn tarmoqlarida mavjud bo’lgan hamda dastlabki muhokama va sinovdan o‘tgan virtual qiymatlar almashinishiningaqlli elektron texnologiyasidir.

2.3. Blokchyn tizimlarida tarmoq xavfsizligi va axborot himoyasining xesh-qiymatlar konsepsiyasi

Xavfsizlik tadbirlari tarmoqqa shunday joriy qilinganki, uning umumiy inkor etish nuqtasi bo‘lmaydi, nafaqat maxfiylik, balki har qanday harakat bekor qilinmasligi va autentifikatsiya ham ta’minlanadi. Tizimda ishtirok etishni istagan har bir shaxs shifrlashdan foydalanishi lozim – bu muhokama qilinmaydi va o‘ylamasdan qilingan harakatlar oqibatlarini faqat shu harakatlarni amalga oshirgan shaxsgina his qiladi.Xakerlik hujumlari, shaxsiy ma’lumotlarni o‘g‘irlash, firibgarlik, kiberqo‘rqitish, fishing, spam, ziyon keltiruvchi dasturlar, virustovlamachilar – bularning barchasi insonning jamiyatdagi xavfsizligiga tahdid soladi. Internetning ilk davri, ko‘plab jarayonlarni shaffof qilish va inson huquqlari buzilishini qiyinlashtirish o‘rniga, xusuiy shaxslar, institutlar va iqtisodiy faollik xavfsizligini oshirmas edi. O‘rtacha internetdan foydalanuvchi ko‘pincha elektron pochta va hisob qaydlarini oddiy parollar himoya qiladi deb umid qilardi, chunki provayderlar yoki ish beruvchilar ishonchliroq parollarni talab qilmasdi.

Shuni ham aytish kerakki, raqamli valyuta oddiy faylda saqlanmaydi. U kriptografik xeshbilan belgilangan tranzatsiyalarda aks ettiriladi.Foydalanuvchilar o‘z pullari uchun kriptokalitlarga ega bo‘ladi va tranzaksiyalarni to‘g‘ridan-to‘g‘ri bir-biri bilan birgalikda amalga oshiradi. Bunday xavfsizlik uchun ularning har biri mas’uliyatli bo‘lishi – shaxsiy kalitlarni ishonchli himoya qilishi zarurligidir.Bu yerda xavfsizlik standartlari muhim ahamiyatga ega bo’ladi. Bitkoyin blokcheyni AQSH Standartlar va texnologiyalar milliy instituti tomonidan chiqarilgan va axborotni qayta ishlash federal standarti sifatida qabul qilingan mashhur va puxta ishlab chiqilgan SHA-256 shifrlash standartida ishlaydi. Blok yechimini topish uchun zarur bo‘lgan ko‘p martalik matematik hisob-kitoblarni takrorlash murakkabligi hisoblash qurilmasidan masalani yechish va yangi bitkoinlar ishlab topish uchun ko‘p elektr energyasi sarflashni

talab qiladi. Ba'zi bir boshqa algoritmlar esa ancha kamroq energiya sarflaydi. Bizningcha, har qanday iqtisodiyot hamma uchun ishlaganda eng yaxshi tarzda ishlaydi. Bu unda ishtirok etish uchun to'siqlarni pasaytirish lozimligini anglatadi. Bu kapitalni qayta taqsimlash emas, balki qayta taqsimlangan kapitalizm uchun platforma yaratish kerakligini anglatadi.Ilk internet davri ko'plab odamlar uchun ko'plab mo''jizalar yaratdi. Biroq, yuqorida aytib o'tilganidek, dunyo aholisining katta qismi na texnologiyalarga, na moliya tizimiga va na iqtisodiy imkoniyatlarga ulanish imkoniga ega bo'lmagan holda, avvalgidek, tizimga ulanmasdan qolib ketmoqda. Boz ustiga, yangi kommunikatsiya vositasi hamma uchun farovonlik keltirishiga umid oqlanmadi. Ha, Internet rivojlangan mamlakatlardagi kompaniyalarga, rivojlanayotgan iqtisodiyotlarda, millionlab odamlarga ish taqdim etishga imkon berdi. U ko'plab tadbirkorlar uchun bozorga kirishga bo'lgan to'siqlarni pasaytirdi va aholining kam ta'minlangan qatlamlariga yangi imkoniyatlar va bazaviy axborotga ulanish imkoniyatlarini taqdim etdi.O'ylaymizki, blokcheyn texnologiyasihar har bir kishining huquqlari va insoniylikni saqlashva qodir bir texnologiyadir. Moliya hizmatlari butunjahon tarmog'i hozirgi kunda ko'plab muammolarga to'lib-toshib yotibdi. U ancha eskirib qolgan, chunki yuqori dinamikali raqamli dunyodan ortda qolib ketayotibdi va shu sababli ham sekin va ishonchsiz ishlaydigan, o'tgan asrdan qolgan texnologiyalarga asoslanadi. U monopol bo'lib, milliardlab odamlarga bazaviy moliyaviy vositalarga ulanish imkonini bermaydi. U markazlashtirilgan bo'lib, shu sababli axborotning sizib chiqishi va boshqa hujumlar hamda inkor qilishlarga uchraydi. U monopollashtirilgan bo'lib, shu sababli status-kvoni qo'llab-quvvatlashga intiladi vainnovatsiyalarga to'sqinlik qiladi. Blokcheyn novatorlar va tadbirkorlarga ushbu kuchli platformada qiymat yaratishning yangi usullarini topgan holda shu va boshqa ko'plab muammolarni hal qilishga imkon beradi.Jahon moliya mutaxassislari blokcheyn bilan bog'liq bo'lgan quydagi g'oyalar haqida puhta o'ylab ko'rishlari lozim:

Attestatsiya. Tarixda birinchi marta, turli sub'ektlar bir-birini bilmagan va bir-biriga ishonmagan holda bitim tuzishi va ishlarni yuritshi mumkin. Shaxsni tasdiqlash va ishonch o'rnatish moliyaviy vositachining huquqi va imtiyozi bo'lmay qo'ydi. Boz ustiga, moliyaviy hizmatlar nuqtai-nazaridan ishonch bayonnomasi yangi

ma'noga ega bo'ladi. Blokcheyn zarur bo'lgan paytda tranzaksiyalar tarixi (blokcheynda), nufuz qiymati (agregatsiyalangan fikrlar asosida) va boshqa umumiqtisodiy ko'rsatkichlar asosida har bir tomonning aynan o'xshashligi va to'lov layoqatini tasdiqlab, ishonchli munosabatlar o'rnatishi mumkin.

Qiymat. Blokcheynda tarmoqda qiymatni pirringli P2P uzatish kliringini amalga oshiradi va ularni tartibga soladi, buni doimiy bajaradi, shunday ekan, uning registri doimo dolzarb bo'ladi. Agar banklar o'zining biznes-modelini o'zgartirmagan holda bunday imkoniyatdan avvalboshdan foydalanganlarida edi, yiliga 20 mlrd dollar atrofida operatsion harajatlarni tejab qolgan bo'lar edilar – bu hisob-kitoblar Ispaniyaning Santander bankiga tegishli bo'lib, real raqamlar bundan ancha yuqori. Qiymatni keskin pasaytirish tufayli banklar bank hizmatlari ko'rsatish bilan yetarli darajada qamrab olinmagan jamiyatlarda xususiy va korporativ mijozlarga moliyaviy hizmatlar, bozorlar va kapitalga ulanish uchun kengroq imkoniyatlar taqdim eta olgan bo'lar edi. Bu nafaqat bozor yetakchilari uchun, balki butun dunyo bo'ylab endi ish boshlayotgan tadbirkorlar uchun ham foydali hisoblanar edi. Istalgan kishi istalgan joydan turib, faqat smartfonga va internetga ulanish imkoniga ega bo'lgan holdagina jahon moliyaviy oqimlariga qo'shilish imkoniga ega boladi.

Tezlik. Hozirgi paytda pul oqimini tartibga solish etti kun, birja bitimini tartibga solish – ikki-uch kun, bank ssudasi uchun esa naqd 23 kun talab qilinadi. SWIFT tarmog'i butun dunyo bo'ylab o'n minglab moliyaviy institutlar o'rtasida kuniga o'n besh million to'lovni o'tkazadi, lekin ularni tartibga solish va kliringga bir necha kun sarflaydi. Xuddi shu narsa AQSHda kuniga trillionlab dollarlik to'lovlar o'tkazadigan ACH (Automated Clearing House) tizimida ham ro'y beradi. Bitkoyn tarmog'idabu vaqtda amalga oshirilgan barcha tranzatsiyalarni tartibga solish va kliringga o'rtacha 10 daqiqa vaqt ketadi. Boshqa blokcheynlar yanada tezroq bo'lib, Bitcoin Lightning Network kabi zamonaviy novatorlik yechimlari tartibga solish va kliring vaqtini soniyaning ulushiga teng bo'lgan vaqtgacha qisqartirib, bitkoin blokcheyni hajmini oshirishga intiladi. «Pul jo'natuvchi bir tarmoqda, oluvchi esa boshqa tarmoqda bo'ladigan bank tizimida pul ko'plab registrlar, vositachilar, tranzit maydonlar orqali o'tib, tom ma'noda yo'lda yo'qolib qolishi mumkin. Aslida ham, qiymatni uzatishning bir onda ro'y beradigan va harajatlar bilan

bog‘liq bo‘lmagan turiga o‘tish uzoq vaqt davomida oraliq holatda turib qoladigan kapitalni ozod qiladi; Bu esa «yo‘ldagi» pul mablag‘laridan foyda oladigan vositachilarni xursand qilmaydi, albatta.

Risklarni boshqarish. Blokcheyn texnologiyasi bir necha xil moliyaviy risk turlarini bartaraf qilishga va’da beradi. Birinchidan, tartibga solish riski – to‘lovning bitimni tartibga solish jarayonida bironta xato natijasida o‘tmaslik riski. Ikkinchidan, kontragentlik riski– ikkinchi tomon bitimni tartibga solish ro‘y bermagunga qadar defolt e’lon qilish riski. Nihoyat, eng jiddiy tizimli risk, tizimdagi barcha yirik kontragentlik risklari yig‘indisi.

Qiymat innovatsiyasi. Bitkoyn blokcheynibitkoyinlar uzatish uchun yaratilgan, boshqa moliyaviy aktivlar bilan ishlash uchun emas. Biroq buochiq boshlang‘ich kodli, tajribalarni rag‘batlantiradigan texnologiyadir. Ayrim novatorlar bitkoyin to‘lovlari uchun emas, balki boshqa maqsadlar uchun mo‘ljallangan alohida blokcheynlar, ya’ni altkoynlar yaratadi. Saydcheynlar – imkoniyatlari va funksiyalari bo‘yicha bitkoyn blokcheynidan farq qiladigan, lekin uning xavfsizligini pasaytirmagan holda bitkoyn kompyuter infratuzilmasi va rivojlangan tarmog‘idan foydalanadigan blokcheynlardir. Saydcheynlar blokcheyn bilan ikki kanalli shtift – aktivlarni uchinchi tomon ishtirokisiz blokcheynga va blokcheyndan berish kriptografik vositasi yordamida aloqa qiladi. Xususiy blokcheynlarda savdo platformalari yaratib, umuman bitkoyin va boshqa tokenlardan foydalanishni istisno qilishga intiladigan novatorlar ham bor. Moliyaviy institutlaraktivlar va majburiyatlarni yozish, almashinish va sotish uchun blokcheyn texnologiyasidan foydalanmoqda, vaqt o‘tishi bilan esaan’anaviy birjalar va markazlashtirilgan bozorlarni u bilan almashtirishi mumkin, bu esa bizning qiymat haqidagi va u bilan savdo mexanizmlari haqidani tasavvurlarimizni o‘zgartirib yuborishi mumkin.

Ochiq boshlang‘ich kod. Moliyaviy hizmatlar tarmog‘ibu – eskirib qolgan tizimlar ulkan texnologikto‘plami bo‘lib, istalgan payt qulashi mumkin. Uni texnologik jihatdan takomillashtirish qiyin, chunki har bir innovatsiya uchun qaytuvchan bo‘la olishlik talab qilinadi. Blokcheyn esa, ochiq boshlang‘ich kodli tizim bo‘lgani holda, doimiy ravishda o‘zgarishi, rivojlanishi va tarmoq murosasi asosida takomillashishi mumkin.Bu afzalliklar – attestatsiya, ancha

past qiymat, bir lahzali tezlik, risklarning pasayishi, katta innovatsiya, moslashuv qobiliyati – istiqbolda nafaqat to‘lovlarni, balki qimmatli qog‘ozlar bilan operatsiyalarni, investitsion bank hizmatlari ko‘rsatishni, buxgalteriya hisobi va auditni, venchurli investitsiyalarni, sug‘urtalashni, tadbirkorlik risklarini boshqarishni, xususiy shaxslarga bank hizmatlari ko‘rsatish va tarmoqning boshqa asoslarini o‘zgartirishi mumkin.Odamlar o‘z ma’lumotlarini o’zlari nazorat qilishlari kerak. Har bir kishi o‘z shaxsiyati haqida nimani, qachon, qaerda va qanchalik batafsil gapirib berish haqida o‘zi qaror qabul qilishga haqlidir. Shaxsiy ma’lumotlarning dahlsizlik huquqini hurmat qilish va shaxsiy ma’lumotllarning xavfsizligini himoya qilish – ikkalasi bir xil narsa emas. Bizga unisi ham, bunisi ham kerak. Bir-biriga ishonish zaruratini bartaraf qilib, Satosi Nakomoto shu tariqa u bilano‘zaro aloqa qilish uchun ikkinchi tomon shaxsini yaxshi bilish zaruratini yo‘qqa chiqardi. Xususiy hayot daxlsizligi – insonning asosiy huquqi va erkin jamiyatning negizidir. Internet paydo bo‘lgandan keyingi oxirgi yigirma yil davomida davlat miqyosida ham, xususiy sektorda ham ma’lumotlar markaziy to‘plamlari xususiy shaxslar va tashkilotlar haqida, jumladan, ularga ma’lum qilmagan holda, xilma-xil maxfiy axborotlar to‘plagan. Hamma joyda odamlar korporatsiyalar axborot izlash asnosida butun raqamli dunyoni titib tashlagan holda qandaydir kiberklonlaryaratishidan havfsiraydi.Blokcheynda esa qatnashchilaristagan holda ma’lum darajagacha noma’lumlikni saqlashi mumkin – ular qandaydir qo‘shimcha ma’lumotlar xabar qilish yoki bu axborotlarni ma’lumotlar markaziy to‘plamida saqlashga majbur emas. Bu holatning muhimligiga noto‘g‘ri baho berib bo‘lmaydi. Blokcheynda shaxsiy ma’lumotlar ombori yo‘q. Blokcheyn protokollarihar bir muayyan tranzaksiya yoki vaziyat uchun kerakli bo’lgan noma’lumlik darajasini tanlashga imkon beradi. Shu tariqa biz o‘zimizning elektron nusxalarimizni va ularning dunyo bilan o‘zaro aloqalarini yaxshiroq boshqaramiz.

Blokcheynda huquqlarning saqlanishi Mulk huquqi shaffof hisoblanadi va huquqiy himoya bilan ta’minlanadi. Shaxsiy erkinliklar hamma tomonidan tan olinadi va hurmat qilinadi. Bu haqiqat biz uchun oshkora bo‘lib ko‘rinadi: har bir shaxs tug‘ilgan paytidan boshlab ulardan mahrum qilinishi mumkin bo‘lmagan, ularni himoya qilish mumkin va lozim bo‘lgan huquqlarga ega bo‘ladi.Raqamli

iqtisodiyotning birinchi davrida bu huquqlarni samaraliroq amalga oshirish usullariniizlab topishga harakat qilingan. Internet san'at, yangiliklar, ko'ngilocharliklar yangi shakllari uchun, she'r, qo'shiq, fotosurat, audio va videoyozuvlar uchun mualliflik huquqi o'rnatish vositasiga aylandi. Tarmoqda moddiy makondagi bilan bir xil narsalarga erishish uchun umumiy savdo kodini qo'llashga to'g'ri keladi: Moddiy substantsiyaning qiymati qanchalik past yoki baland bo'lishidan qat'i azar, har qanday predmetni sotib olish uchun shartnoma tuzish va uni muhokama qilish zaruratini bartaraf qilishga erishildi. Lekin bu holatda ham tranzaksiyalarni boshqarishda vositachilarga umid bog'lashimizga to'g'ri kelardi va vositachilarpulni o'z hisobraqamida ushlab turib (yo'ldagi pul mablag'lari) keyin o'tkazishi yoki uni o'tkazishi va so'ngra rad etishi mumkin bo'lgan holda tranzaksiyalarni rad qilish imkoniyatiga ega bo'ladi. Savdo bitimlari qatnashchilarning ma'lum bir qismi esa firibgarlik qilishi kutadi va har qanday bitimda ma'lum darajadagi firibgarlik muqarrar deb qabul qiladi.

Bizning fikrimizcha, raqamli iqtisodiyot usullarini qo'llash tufayli eng muhim o'zgarishlarga tayyor bo'lgan sakkizta asosiy funksiyani ko'rib chiqamiz.

Aynan shu bo'lishlik va qiymatni tasdiqlash. Hozirgi paytda bizishonch asosidagi munosabatlar o'rnatish va moliyaviy tranzaksiyada ikkinchi tomonning aynan shuligini tasdiqlashda yirik vositachilarga tayanamiz. Bu vositachilarbank hisobraqamlari va zayomlar kabi asosiy moliyaviy hizmatlarga ulanishda hakamlar rolini o'ynaydi. Blokcheyn ma'lum bir tranzaksiyalarga ishonch zaruratini pasaytiradi va bazida hatto olib tashlaydi ham. Bu texnologiya shuningdek, qatnashchilarga tasdiqlanadigan, to'liq funksionalliva kriptografikhimoya qilingan elektron profillardan foydalanish va zarur bo'lgan hollarda ishonch asosidagi munosabatlar o'rnatishga imkon beradi.

Qiymatlar ko'chishi. Moliya tizimi har kunipul mablag'larini butun dunyo bo'ylab ko'chiradi va hatto bir dollar ham ikki marta sarflanmasligini ta'minlaydi.iTunes da bitta qo'shiqni 99 sentga xarid qilishdan tortib, kompaniya ichida fondlarni berish, aktivlar sotib olish yoki kompaniyalar xarid qilishgacha bo'lgan milliardlab bitimlarnitekshirib turadi. Blokcheyn har qanday qiymatlar – valyuta, aktsiyalar, obligatsiyalar, huquqlarni – yirik va kichik miqdorda, uzoq

va yaqin masofaga, ma'lum va noma'lum tomonlarga ko'chirish uchun umumiy standart bo'lishga qodir. Shunday qilib, blokcheyn qiymatlarni ko'chirish uchun xuddi tovarlarni ko'chirish uchun kerak bo'lgan standart yuk konteyneri joriy qilish kabi ishlarni bajarishi mumkin. Bu esa bahoni sezilarni ravishda pasaytirishi, operatsion tezlikni oshirishi, iqtisodiy o'sish va farovonlikka hizmat qilishi mumkin.

Qiymatlarni saqlash. Moliyaviy institutlar xususiy shaxslar, tashkilotlar va davlatga tegishli bo'lgan qiymatlar saqlanadigan ombor vazifasini bajaradi. O'rtacha statistik fuqaro uchun bank ularni bank yacheykasi, jamg'arma yoki joriy hisobraqamida saqlaydi. Likvidlik zarur bo'lgan va naqd ekvivalentga kichik foiz talab qilinadigan yirik tashkilot uchun bu risksiz investitsiyalar, masalan, g'aznachilik obligatsiyalari yoki qisqa muddatli vositalar bozoriga investitsiyalar hisoblanadi. Blokcheyn bilan xususiy shaxslarqiymatlarni saqlash, jamg'arma yoki joriy hisobraqami hizmatlarini yagona taqdim etuvchilar sifatida banklarga tayanishga majbur bo'lmaydilar, tashkilotlarda esarisksiz moliyaviy aktivlar xarid qilish va ularga egalik qilishning samraaliroq mexanizmlari paydo bo'ladi.

Kreditlash. Moliyaviy institutlar ipotekadan tortib, qisqa muddatli veksellargacha kreditlar berishni: kredit kartalari, ipoteka kreditlari, korporativ, munitsipal vadavlat obligatsiyalari, aktivlar bilan ta'minlangan qimmatli qog'ozlarni bilan ishlash jarayonini ancha soddalashtiradi. Kreditlash mexanizmi kredit layoqatini tekshirish, kredit tarixi yuritish, kredit reytinglari tayinlash uchun bir qator qo'shimcha tarmoqlar yuzaga keltirdi. Xususiy shaxslar uchun kredit tarixi muhim, tashkilotlar uchun esa –«investitsion sinf»dan to «axlat»gacha bo'lgan kredit reytinglari mavjud. Blokcheynda istalgan shaxs an'anaviy qarz majburiyatlarini to'g'ridan-to'g'ri chiqarishi, ayirboshlashi va tartibga solishi, shu tariqa, risk va harajatlarni pasaytirishi hamda tezlik va shaffoflikni oshirishi mumkin. Iste'molchilar bevosita boshqa iste'molchilardan qarz olishi mumkin bo'ladi. Bu ayniqsa, bank hizmatlari bilan qamrab olinmaganlar va butun dunyo bo'ylab tadbirkorlar uchun juda muhim amaldir.

Qiymatlar almashinish. Har kuni bozorlar butun dunyo bo'ylab umumiy qiymati trillionlab dollarni tashkil qiladigan moddiy aktivlarni ayirboshlashga imkon beradi. Savdo bu – investitsiyalash, birjada o'ynash, xedjirlash va arbitraj, jumladan, bitimdan keyingi

kliring tsikli, tartibga solish va saqlash maqsadida aktivlar va moliyaviy vositalar sotish va sotib olishdir. Blokcheyn har qanday tranzaksiyalarni tartibga solish vaqtini hafta va kunlardan daqiqa va soniyalargacha qisqartiradi.

Homiylik va investitsiyalar. Aktiv, kompaniyayoki yangi korxonaga investitsiya kiritish kapital qiymatining ortishi, dividendlar, foizlar, renta va ularning xilma-xil kombinatsiyalari ko‘rinishida daromad olish imkonini beradi. Tarmoq investorlarni tadbirkorlar va kompaniyalar egalari bilan rivojlanishning «farishta»dan tortib, IPOgacha va boshqa turli bosqichlarida uchrashtirgan holda bozorlar vujudga keltiradi. Mablag‘lar jalb qilish odatda vositachilarni, masalan, investitsion banklar, venchurli investorlar, huquqshunoslarni talab qiladi. Blokcheyn ularning ko‘plab funksiyalarini avtomatlashtiradi, to‘g‘ridan-to‘g‘ri pirringli moliyalashtirish uchun yangi modellardan foydalanishga imkon beradi, shuningdek,dividendlar yozish va kupon to‘lovlarini yanada samarali, ularni shaffof va ishonchli qiladi.

Qiymatni sug‘urta qilish va risklarni boshqarish. Risklarni boshqarish va uning xususiy holati bo‘lgan sug‘urtalash xususiy shaxslar va kompaniyalarni ko‘zda tutilmagan yo‘qotishlar va haloqatlardan himoya qilish uchun mo‘ljallangan. Kengroq ma’noda moliya bozorlarida risklarni boshqarish oldindan aytish yoki nazorat qilish qiyin bo‘lgan hodisalarni xedjirlash uchun bir talay hosila, murakkab strukturalangan moliyaviy mahsulotlar va boshqa moliyaviy vositalar yuzaga keltirgan. So‘nggi hisob-kitoblarga ko‘ra, barcha ommaviy ochiq bo‘lgan hosila qimmatli qog‘ozlarning nominal qiymati 600 trln dollarni tashkil qiladi. Blokcheyn sug‘urta qilish nomarkazlashgan modellarini qo‘llabquvvatlaydi, burisklarni boshqarish uchun hosila qimmatli qog‘ozlardan foydalanishni yanada shaffof qiladi. Insonning ijtimoiy va iqtisodiy kapitaliga, uning harakatlari va boshqa nufuzga oid ko‘rsatkichlarga asoslangan nufuz tizimining o‘zi sug‘urta qiluvchilarga aktuar riskni yaxshiroq tushunish va qarorlardan xabardor bo‘lgan holda qabul qilishga imkon yaratadi.

Qiymatlar buxgalteriya hisobi. Buxgalteriya hisobi – iqtisodiy jarayonlar qatnashchilari haqidagi moliyaviy axborotni o‘lchash, qayta ishlash va uzatishdir. Ko‘p milliardli ushbu tarmoqni to‘rtta audit giganti: Deloitte Touche Tohmatsu, Pricewaterhouse Coopers, Ernst

& Young va KPMG nazorat qiladi. An’anaviy buxgalteriya hisobi amaliyotchilarizamonaviy moliyani tezligi va murakkabligi tufayli unchalik yaxshi boshqara olmayapti. Blokcheyn taqsimlangan registrini qo‘llaydigan yangi usullar audit va moliyaviy hisobotlarni shaffof qiladi va ularni real vaqt rejimida faol borishga imkon beradi. Shuningdek, utartibga soluvchi organlar va boshqa manfaatdor shaxslarning korporatsiya ichidagi moliyaviy faollikni kuzatib borish imkoniyatlarini sezilarli darajada kengaytiradi.Blokcheyn shuningdek, davlatning moliya hizmatlari sohasini nazorat qilishdagi roli haqida munozaralarni ancha jonlantirib yubordi. Agar ularni so‘zning keng ma’nosida kommunal hizmatlar sifatida qabul qiladigan bo‘lsak, odatda davlat tomonidan qattiq tartibga solinadigan xomashyo monopoliyalarga o‘xshatish yuzaga keladi. Biroq, blokcheyn texnologiyasi risklarni pasaytirish hamda shaffoflik va tezkorlikni oshirishni va’da qilishi sababli texnologiyaning o‘zi tartibga solish funksiyalarini bajaradi 15 . Biroq, agar tartibga soluvchi organlar banklar va bozorlarda ichki jarayonlarga yo‘l topish imkoniga ega bo‘lsa, unda ayrim qonunlarni soddalashtirish, boshqalarini esa umuman bekor qilish mumkindir? Bu savolga javob berish ancha qiyin masala. Bir tomondan, tartibga soluvchi organlar innovatsiyalar ulkan tezligini hisobga olgan holda o‘zining nazorat funksiyasini qayta ko‘rib chiqishiga to‘g‘ri keladi. Boshqa tomondan, banklar davlat nazoratidan chetda qolib ketgan holda bir necha marta halollikni esidan ham chiqarib qo‘ygan.Tadbirkorlar uchun investorlar izlab topish – jiddiy o‘zgarishlar kutib turganmoliya hizmatlari industriyaining sakkizta funksiyasidan biridir. Qimmatli qog‘ozlarni qisman joylashtirish, aksiyalar va xususiy investitsiyalarni tijorat kapitaliga birlamchi va ikkilamchi joylashtirish (PIPE) orqali aksiyadorlik kapitali to‘plash jarayoni 1930-yillardan buyon jiddiy o‘zgarishlarga uchramadi. Barchamizga ma’lum va mashhur bo’lgan kraudfandingplatformalari tufayli kichik biznes internet orqali kapitalga yo‘l topdi. Horijiy mamlakatlarda qo’llaniladigan Oculus Rift va Pebble Watch platformalari – ushbu modelning birinchi qadamlari desak ham bo’ladi. Lekin avvlagidek, qatnashchilar kapitalni to‘g‘ridan-to‘g‘ri xarid qila omlaydilar. AQSHda startaplarga ko‘maklashish haqida yangi qonun maydainvestorlargabevosita kraudfanding kampaniyalari orqali mablag‘ kiritishga imkon beradi, lekin investorlar va tadbirkorlarga

buning uchun avvalgidek Kickstarter yoki Indiegogo kabi vositachilar hamdaan'anaviy to'lov usuli, odatda bank kartalari PayPal zarur. Vositachi bu ishlarning hakami hisoblanadi, jumladan, kimga nima tegishli ekanligini u hal qiladi.Blokcheynda aksiyadorlashtirish (bu bir variant) ushbu konsepsiyani yanada rivojlantiradi. Endi kompaniyalar«blokcheynda» moliyalashtirish to'plashi, kompaniyaning moddiy qiymatlariga mos keladigan tokenlar yoki virtual qimmatli qog'ozlar chiqarishi mumkin. Ular aksiyalar, obligatsiyalar yoki boshqalar bilan bog'liq holatda bo'lgani kabi, ularning egalariga kompaniya qaysi bashorat bozorlarini ochishini hal qilish huquqini bergan holda platformada kotirovka qiladigan bozor qatnashchilari pozitsiyalarini aks ettirishi mumkin. Ethereum oldindan berilgan buyurtmalar bo'yicha o'z tokeni, ether sotish uchun tamomila yangi blokcheyn rivojlantirishni moliyalashtirib, yanada katta muvaffaqiyatga erishdi. Hozirda Ethereum –uzunligi bo'yicha ikkinchi va rivojlanish sur'ati bo'yicha birinchi o'rinda turadigan ommaviy blokcheyn hisoblanadi. Augur kraudfandingida investitsiyalar o'rtacha summasi 750 dollarni tashkil qildi, lekin 1 dollar yoki hatto 10 sentlik minimal obunalarni tasavvur qilish qiyin emas. Dunyoda istalgan kishi – hatto aholining eng qashshoq qatlamlari va eng uzoq mintaqalar aholisi ham – fond bozorinig investoriga aylanishi mumkin.Augurrahbarlar jamoasining hisoblashicha, bashorat bozorlarining yagona amaliy chegarasi - tasavvurdir. Augurga istalgan shaxs yakuniy sanasi aniq bo'lgan ma'lum bir bashorat e'lon qilishi mumkin.Augur kelajakdagi hodisalar – sport musobaqalari, saylovlar, yangi mahsulotlar ishlab chiqarish, mashhur kishilarning farzandlari kelajagini aniq bashorat qilish uchun foydalanuvchilarni mukofotlaydigan bozorlarni bashorat qilish uchun nomarkazlashgan platforma yaratadi. U qanday faoliyat ko'rsatadi? Augur foydalanuvchilari ularning qiymati u yoki bu natija ehtimoli bilan belgilanadigan bo'lg'usi hodisa natijasi aksiyalarini sotishi yoki sotib olishi mumkin. Agar ehtimol 50 ga 50 ni tashkil qiladigan bo'lsa, aksiyalar xarid qiymati 50 sentni tashkil qiladi. Augur «omma donishmandligi»ga – hodisaning natijasini ko'p sonli odamlar guruhi bitta yoki bir nechta ekspertdan ko'ra aniqroq aytib berishi mumkin deb hisoblaydigan ilmiy tamoyilga tayanadi. Boshqacha qilib aytganda, Augur bashoratlar aniqligini oshirish uchun bozor mexanizmidan foydalanadi. Avvalroq Hollywood Stock Exchange,

Intrade va HedgeStreet (endi Nadex) kabi markazlashtirilgan bashorat bozorlari harakatlari bo'lgan, lekin ularning katta qismi yopilib ketgan yoki yuridik va tartibga solish bilan bog'liq muammolar tufayli umuman ishga tushirilmagan.Blokcheyn texnologiyasidan foydalanish tizimni ishlab chiqishga nisbatan chidamli, aniqroq, xatlar, majburlashlar va likvidlik muammosiga nisbatan barqaror va Augur jamoasi «eskirgan yurisdiksiyalar tomonidan tartibga solish» deb ataydigan holatga olib keladi. Augur platformasida hakamlar «referi» deb ataladi, ularning qonuniyligi esa ularning nufuzi bilan belgilanadi. «To'g'ri xulq-atvor uchun» - ya'ni ro'y bergan voqea, saylov yoki o'yin natijasi uchun – ko'proq nufuz ochkosi yoziladi. Tizimda axloqiy me'yorlarga rioya qilish boshqa moddiy foydaga ham olib keladi: foydalanuvchida qanchalik ko'p nufuz ochkosi bo'lsa, u shunchalik ko'p bozorlar tashkil qilishi va ko'proq pul ishlab topishi mumkin. Augur ta'kidlashicha, «bizning bashorat bozorlarimiz boshqa tomon bilan, markazlashtirilgan serverlar bilan bog'liq risklarni bartaraf qiladi hamda kriptovalyutalar, jumladan, blokcheyn, ether va barqaror kriptovalyutalarni qo'llagan holda global bozorni shakllantiradi. Barcha mablag'lar smart-shartnomalarda saqlanadi, pullarni o'g'irlab bo'lmaydi». Augur huquqbuzarliklarga nisbatan nolga teng bo'lgan sabr-toqatni joriy qilib, noaxloqiy shartnomalar muammosini ham hal qiladi.Bashorat bozorlari yakuniy hodisalarga stavkalardan manfaatdor bo'lgan investorlar uchun foydali, masalan: «IBM daromadi bu chorak hech bo'lmasa 10 sentga o'sadimi?» Hozir korporativ foydaning dastlabki bahosi – bir nechta ekspert tahlilchilar bashoratlarining o'rtacha yoki mediana qiymati, xolos. «Omma donishmandligi»dan foydalanib, biz kelajak uchun realistik bashorat qilamiz, bu esa bozorlarni yanada samarali qiladi. Bashorat bozorlarianomal hodisalar va global noaniqlikka qarshi xedjirlash uchun hizmat qilishi ham mumkin. Bashorat bozorlari butun dunyo bo'ylab investorlarni ertaroq xabardor qilish tizimi sifatida xolisona ishlashi mumkin.Bashorat qilish bozorlari moliya tizimining ko'plab jihatlarini to'ldirishi va oxir-oqibat o'zgartirishi mumkin. Xaridlar, rahbariyatning almushinuvi haqida hisobotlar bo'yicha bashorat bozorlarini tasavvur qilib ko'ring. Bashorat bozorlari axborotlari asosida bozorni xedjirlash va qadriyatlarni sug'urtalash amalga oshirilishi mumkin va istiqbolda ular hatto optsionlar, foiz stavkasi svoplari va kredit defolti svoplari kabi mistik moliyaviy vositalarni

siqib chiqaradi. Albatta, bashorat bozori hamma joyda ham kerak emas, albatta. U yetarli miqdorda odamlar qiziqib qolmagunga qadar e'tiborni jalb qilish qilish uchun kerakli darajada likvidli bo'lmaydi. Lekin baribir uning salohiyati ulkan va hamma uchun ochiq hisoblanadi. Blokcheyn texnologiyalarimoliya hizmatlari bozorining chakana banking va kapital bozoridan tortib buxgalteriya hisobi va tartibga solishgacha bo'lgan barcha turlari va funksiyalariga ta'sir etadi. Shuningdek, ular banklar va moliyaviy institutlarning jamiyatdagi rolini qayta ko'rib chiqishga majbur qiladi. Agar eski dunyo qattiq ierarxiyaga ega, sust, yopiq va shaffof emas bo'lsa, o'zgarishlarga qarshilik ko'rsatsa va kuchli vositachilar tomonidan nazorat qilinsa, yangi dunyo tekisroq, piring qarorlari taklif qiladigan, tez-tez ro'y beradigan va ishonchli, shaffof, birbiriga kiritilgan va innovatsion bo'ladi. Albatta, o'zgarishlarnormal faoliyat ko'ratishning buzilishi va beqarorlikka olib keladi, lekin tarmoq yetakchilari bugunning o'zidayoq bu borada qandaydir choralar ko'rish imkoniyatiga ega bo'ladilar. Moliyaviy hizmatlar sohasini yaqin yillarda qisqarish ham, o'sish ham kutib turibdi: kamroq sonli vositachilar ancha kichik harajatlar bilan ko'p sonli kishilarga ko'proq mahsulot va hizmatlar taklif qilishlari mumkin. Bu juda yaxshi deb hisoblaymiz. Nomarkazlashgan dunyoda ochiq va yopiq blokcheynlar o'ziga joy topa oladimi, yo'qmi – bu tortishuvli masala. O'ylaymizki, blokcheyn texnologiyasining bartaraf qilib bo'lmaydigan kuchi hozirgi kunda zamonaviy moliyaning mustahkam o'rnashib olgan, tartibga solib tashlangan va rivojlanishdan to'xtagan infratuzilmasiga hujum qilmoqda. Ularning to'qnashuvi moliya tizimi landshaftini o'n yilliklarga o'zgartirib yuboradi.Umid qilamizki, u nihoyat industrial davrning pul mashinasidan platformasiga aylanadi.Potensial foyda olish taklifi bilan jalb qilinganbir nechta kompaniya blokcheynlar uchun qidiruv dasturlari ustida ishlamoqda. Google dunyodagi barcha axborotlarni yig'ish va tashkil qilish missiyasini o'z zimmasiga olgan va bu masalani tadqiq etishga kompaniya juda ko'p mablag' inson resurslari sarflashiga ajablanmasa ham bo'ladi. Internetda qidirish va blokcheynda qidirish o'rtasida uchta asosiy farq bor. Birinchidan, bu foydalanuvchining shaxsiy ma'lumotlari daxlsizligi. Shu bilan bir vaqtda tranzaksiyalar shaffof, har biri o'zining shaxsiy ma'lumotlari egasi bo'lib, ular bilan qanday muomala qilishni o'zlari hal qiladilar. Jarayonda nomini ma'lum qilmagan holda yoki taxallus ostida (o'ylab

topilgan nom ostida - anonim) yoki soxta-anonim (qisman anonim) ravishda ishtirok etishi mumkin. Ko'plab kompaniyalar personal yollash jarayonini qayta ko'rib chiqishi va qayta tashkil qilishiga to'g'ri keladi. Masalan, kadrlar bo'yicha mutaxassis blokcheynga yopiq savollar (ha/yo'q) berishni o'rganishi lozim: «Siz odammisiz?», «Amalyi matematika sohasida oliy ma'lumotingiz bormi?», «Scrypt, Python, Java, C++ dasturlarida dasturlashtirishni bilasizmi?»

Firmalarda paydo bo'ladigan mojarolarga yana bir sabab, shartnoma harajatlari, narx muhokamasi, tovar yoki hizmatlar taqdim etish shartlarini tavsiflash va hajmini aniqlash, bu bitimlarning bajarilishini ta'minlash va tartibga solish hamda ularning ijro etilmagani uchun choralar ko'rish hisoblanadi. Shartnoma va bitimlar – nisbatan yangi hodisa bo'lib, biz mulkni emas, majburiyatlarni almashina boshlaganda paydo bo'lgan. Og'zaki bitimlar ishonchsiz bo'lib chiqdi: ularni buzib ko'rsatish, noto'g'ri eslab qolish oson bo'lgan, guvohlarga esa doim ham umid qilib bo'lmagan. Shubha va ishonmaslik yangi odamlar bilan birgalikda ishlashga to'sqinlik qiladi. Shartnomalarni zudlik bilan ijro etish lozim, shartlarning bajarilishini ta'minlashga esa faqat kuch bilan tahdid solish hisobiga erishilgan – buning rasmiy mexanizmlari mavjud bo'lmagan. Yozma shakldagi shartnoma majburiyatlarni qayd qilish, ishonch asosida munosabatlar o'rnatish va bir-biridan kutadigan natijalarni tavsiflash usuliga aylangan. Yozma shartnomalar tomonlardan biri o'z majburiyatlarini bajarmagan yoki kutilmagan voqea yuz bergan hollarda nima qilish kerakligini ko'rsatar edi. Lekin ular bo'shliqda mavjud bo'la olmasdi– shartnomalarni tan oladigan va tomonlardan har birining huquqlariga rioya qilinishini ta'minlaydigan qonunchilik tuzilmasi talab qilinar edi.Blokcheyn, shartnoma harajatlarini pasaytirib, firmalarga ochilish va o'z sarhadidan tashqarida yangi munosabatlarni rivojlantirishga imkon beradi. Consensys (kelishuv), masalan, uning hududida ham, hududidan tashqarida ham turli qatnashchilar guruhi bilan o'zaro munosabatlarni yuzaga keltirishi mumkin, chunki bu munosabatlari an'anaviy menejerlar emas, smart-shartnomalar boshqaradi. Qatnashchilarning o'zlari hammani qoniqtiradigan maqsadlarni belgilaydi va ularga erishganlik uchun mukofot oladi – bularning hammasi blokcheynda bajariladi.

Blokcheyn tizimlarda yuqoridagi uchta element *xesh-qiymatlar konsepsiyasi* bilan bog'liq.

Ma'lumotlarni saqlash uchun o'zgartirilmasligi zarur bo'lgan xesh-qiymatlaridan foydalanishning ikkita keng tarqalgan taniqli shablonlari mavjud:

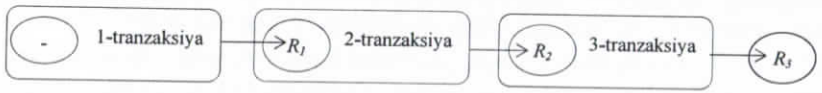
- zanjir ko'rinishdagi shablon;
- daraxt ko'rinishidagi shablon.

Agar har bir axborot fragmentida (yoki tranzaksiyada) boshqa axborot fragmenti (yoki tranzaksiya) xesh-qiymatiga (xesh-havola) ega bo'lsa, bunda bog'langan axborotning *zanjiri* hosil bo'ladi. Axborotlarning bunday bog'lanishi, agar axborot fragmentlari (yoki tranzaksiyalar) bir-biriga ketma-ket o'tish orqali amalga oshirilsa, u holda zanjir usuli ma'lumotlarni saqlash va birlashtirish uchun qulay hisoblanadi.

Zanjir shabloni yondashuvining sxemasi shartli ramziy belgilardan foydalangan holda 2.2-rasmda ko'rsatilgan. Bunda zanjirdagi axborot uchun «n-tranzaksiya» va ularning xesh-qiymatlari uchun «R_n» belgilashidan foydalanilgan. Zanjirni yaratish "1-tranzaksiya" nomli ma'lumotlar fragmenti va R_1 xesh-havolasi bilan boshlanadi. Dastlabki fragment sifatida, "1-tranzaksiya" hech qanday xesh-havolani o'z ichiga olmaydi, chunki ushbu tranzaksiyadan avvalgi axborot mavjud emas. Yangi ma'lumotlar esa, "1-tranzaksiya"ning R_1 xesh-havolasi bilan birga yaratiladi. R_2 xesh-havolasi esa hozirgina olingan "2-tranzaksiya" ma'lumotlari va R_1 xesh-havolasi asosida yaratiladi. R_3 xesh-havola "3-tranzaksiya" va R_2 xesh-havolasiga asoslangan tarzda xuddi avvalgi qadamdagiday yaratiladi.

R_3 xesh-havolasi zanjirdagi barcha ma'lumotlarga, ularning qabul qilingan vaqtiga teskari tartibda kirish uchun zarur bo'lgan barcha ma'lumotlarni o'zida mujassam etadi.

R_3 xesh-havolasi zanjirning *boshi* deb ham ataladi, chunki u eng so'nggi qo'shilgan ma'lumot fragmentiga ishora qiladi.



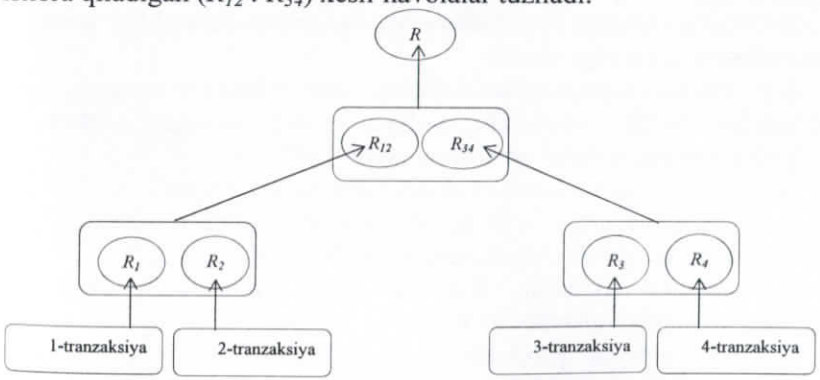
2.2-rasm. Zanjirga birlashtirilgan tranzaksiyalar

Odatda, Blokcheyn tizimlarini tavsiflashga bag'ishlangan asarlarda tranzaksiyalar va ularning xesh-havolalari, xesh-havoladan

tranzaksiya ma'lumotlariga yo'naltirilgan strelka bilan birlashtirilib, bu xesh-havola tranzaksiya ma'lumotlari bilan bog'liqligini ifodalaydi. Biz bu yerda, strelkani xatolikka yo'l qo'yib emas, balki ongli ravishda tranzaksiya ma'lumotlaridan uning xesh-havolasiga yo'naltirdik, chunki har qanday xesh-havola tranzaksiyaning aniq ma'lumotlariga muayyan ishlov berish natijasida kelib chiqadi, ya'ni umuman olganda xesh-havola, ma'lumotlarning hosilasi hisoblanadi, aksi emas.

Ma'lumotlarni o'zgartirilmay saqlanishi uchun zarur bo'lgan xesh-qiymatlaridan foydalanishning ikkita keng tarqalgan shablonlaridan yana biri – bog'langan ma'lumotlar *daraxti* 2.7-rasmda ko'rsatilganidek shakllantiriladi. Unda tranzaksiya ma'lumotlari xesh-havolalar yordamida daraxt shaklidagi tuzilishga birlashtirilishi mumkin. Ushbu struktura, shuningdek, uni ishlatishni birinchi bo'lib taklif qilgan kompyuter kriptografiyasi bo'yicha mutaxassis Merkle sharafiga, Merkle daraxti deb nomlanadi.

Ushbu shablon bir vaqtning o'zida bitta xesh-havola orqali kirish mumkin bo'lgan ko'plab har xil ma'lumotlar fragmentlarini yig'ish uchun qulay hisoblanadi. 2.3-rasmda ko'rsatilgan daraxtni hosil qilish uchun, birinchi navbatda, sxemaning pastki qismida to'rtburchaklar shaklida ko'rsatilgan tranzaksiya ma'lumotlarining to'rtta fragmenti tuziladi. Shundan so'ng xesh-havolalar tranzaksiya ma'lumotlarining alohida fragmentlarida (R_1-R_4) tuziladi va bu havolalar juft-juft bo'lib birlashtiriladi. Keyingi qadamda esa, birinchi xesh-havolalar juftlariga ishora qiladigan (R_{12} *i* R_{34}) xesh-havolalar tuziladi.



2.3-rasm. Daraxtsimon shablonda birlashtirilgan ma'lumotlar

Protsedura yagona xesh-havola yaratilgunga qadar takrorlanadi va hosil bo‘lgan xesh-havola Merkle daraxtining *ildizi* deb ham atalib, u sxemada *R* sifatida ko‘rsatilgan.

Daraxt tuzilishi bir vaqtning o‘zida bitta xesh-havola orqali kirish mumkin bo‘lgan ma’lumotlarning turli xil fragmentlarini yig‘ish uchun qulay bo‘lishiga qaramay, amalda ko‘pincha zanjir shablonidan foydalaniladi, chunki Blokcheyn tizimi bloklari ketma-ket tashkil qilinadi. Amalda, bir vaqtning o‘zida tan olingan ikkita tranzaksiya, masalan, 2.3-rasmda ko‘rsatilganiga o‘xshash 3 va 4-tranzaksiyalar kam uchraydi. Agar uchrasalar, ular vaqtincha mavjud bo‘ladilar, chunki kelajakda ulardan faqat bittasi tasdiqlanadi.

Yuqorida tavsiflangan sxemalar ma’lumotlarda saqlash va ularda ro‘y bergan o‘zgarishlarni aniqlash imkoniyati beradi, chunki ularda ma’lumotlar xesh-havolalar yordamida birlashtiriladi va bog‘lanadi.

Xesh-havolalar tuzilganidan so‘ng, tegishli ma’lumotlardagi har qanday o‘zgarish, xesh-havolalarning shikastlanishiga (buzilishiga) olib keladi. Shunday qilib, xesh-havolalar shikastlanganligining aniqlanishi, ma’lumotlar tarkibi shakllantirilganidan keyin o‘zgartirilganlik faktini isbotlaydi. Agar barcha xesh-havolalar buzilmagan bo‘lsa, ma’lumotlarning umumiy tarkibi u shakllanganidan beri o‘zgarmagan degan xulosaga kelishga asos bo‘ladi.

2- bob yuzasidan nazorat savollari

1. Ko‘chmas mulkka egalik huquqini tavsiflovchi Blokcheyn tizim tranzaksiyalarining blok zanjiri qanday?
2. Blokcheyn tizimi tomonidan ishlatiladigan tranzaksiyalar qanday elementlarni o‘z ichiga oladi?
3. Blokcheyn tizimning ishtirokchisi, agar u bunday xuquqga ega bo‘lmagan holda, ko‘chmas mulkka egalik huquqini o‘tkazish bo‘yicha tranzaksiyalarni qo‘shsa nima bo‘ladi?
4. Tranzaksiyalarni formatli va semantik nazorati nima?
5. Blokcheyn tizimiga a’zo bo‘lgan kompyuterlar o‘rtasida axborot almashish tizimi qanday vazifalarni bajarishi kerak?
6. Blokcheyn tizimida mulkka egalik huquqining himoya mexanizmi qanday qismlardan iborat?
7. Identifikatsiya, autentifikatsiya va avtorizatsiya jarayonlari qanday masalalarni o‘z ichiga oladi?

8. Blokcheyn tizimlarining axborot himoyasida xesh-qiymatlar o‘rni qanday?
9. Blokcheyn tizimlarida zanjir boshi qanday axborotning xesh qiymatini ifodalaydi?
10. Merkle daraxti nima?

3-BOB. AXBOROTNI XESHLASH USULLARI, ALGORITMLARI VA BARQARORLIGI

Yuqoridagi dalillar shuni ko‘rsatadiki, Blokcheyn tizimlarda ma’lumotlarning ishonchliligini ta’minlash asosan axborotni xeshlash usullari yordamida amalga oshiriladi

Axborotni xeshlash (*inglizcha hashing*) deganda ixtiyoriy uzunlikdagi ma’lumotlar kirish massivini, olingan belgilangan uzunlikdagi chiqish qatoriga o‘tkazish operatsiyasi tushuniladi. Bunday o‘zgartirishlar, shuningdek, *xesh-funksiyalari* yoki *o‘ram funksiyalari*, ya’ni kirish massivining prototipi va o‘zgartirish natijalari esa *xesh, xesh-kod, xesh obraz, axborotning raqamli izi* kabi nomlar bilan nomlanadi.

“Xeshlash” mexanizmi ilgaridan ma’lum bo‘lsa ham, dasturlash asarlarida bu atama paydo bo‘lganiga ko‘p bo‘lgani yo‘q. Ba’zi tadqiqotlarda, jumladan [18] da ta’kidlanganidek, xeshlash g‘oyasi birinchi marta 1953-yil yanvar oyida IBMning ichki memorandumini yaratishda G.P.Lan tomonidan bildirilgan deb ta’kidlanadi.

O‘z maqsadiga ko‘ra, xeshlash oxir-oqibat axborot ishonchliligini ta’minlashga xizmat qilishi lozim. Axborotni xeshlash masalasiga ko‘plab tadqiqotlar bag‘ishlangan va u bugungi kunda ham gurkirab rivojlanmoqda [11, 17, 18]. Ko‘pgina tadqiqotchilar «Xesh jadvallari axborotlashtirishning eng katta ixtirolaridan biridir. Massivlar va ro‘yxatlar birikmasiga bir oz qo‘shilgan matematika dinamik ma’lumotlar olish va saqlash uchun samarali mexanizm yaratishga imkon berdi»,- deb hisoblashadi [17].

Axborotni xeshlash jarayonida xesh-funksiyasi asosiy rol o‘ynaydi.

3.1. Xesh-funksiyaning asosiy tushunchalari va blokcheyn tizimlarida axborotni xeshlash usullari

Xesh-funksiyasi - bu ixtiyoriy uzunlikdagi kirish xabarini, belgilangan uzunlikdagi xabarga o‘zgartiradigan, oson hisoblanadigan qandaydir *h(x)* funksiya deb ta’riflanadi [11].

Umumiy holda, xesh-funksiyalar qiymatlari soni har doim *x* argumentning variantlaridan kam bo‘lganligi sababli, *x* argumenti va xesh-funksiyasining qiymati o‘rtasida bir qiymatli moslik mavjud emas. Shuning uchun, xesh-funksiyalarning bir qiymatiga mos

ko‘plab kirish xabarlari mavjud bo‘lganda, ular *kolliziyalar* deb nomlanadi.

h funksiyasi uchun *kolliziya* – bu *shunday* $x \neq y$ bo‘lgan *x va y* qiymatlar juftligiki, unda $h(x) = h(y)$ bo‘ladi.

Shunday qilib, xesh-funksiyalarga qo‘yiladigan asosiy talablarni quyidagicha ifodalash mumkin:

- xesh-funksiyasi har qanday uzunlikdagi axborotga qo‘llash mumkin bo‘lishi kerak;
- funksiya qiymatini hisoblash yetarlicha tez bajarilishi kerak;
- xesh-funksiyasining ma’lum qiymatida, unga muvofiq keladigan axborotni topish qiyin bo‘lishi kerak;
- biror *x* axborotdagi kabi xesh-funksiya qiymatiga ega bo‘lgan boshqa bir *u* axborotni topish qiyin bo‘lishi kerak;
- xesh-funksiya qiymati bir xil bo‘lgan har qanday tasodifiy turli xil axborot juftligini topish qiyin bo‘lishi kerak.

Eng oddiy xesh-funksiyani «*2 moduli bo‘yicha summa*» amalidan foydalanib quyidagicha tuzish mumkin: kirish satri olinadi, 2 moduli bo‘yicha barcha baytlar qo‘shiladi va bayt - natija xesh-funksiyaning qiymati sifatida qabul qilinadi. Xesh-funksiyasi qiymatining uzunligi, kirish xabarining hajmidan qat’iy nazar, 8 bitni tashkil etsin deb oldindan shart qo‘yiladi.

Masalan, o‘n oltilik formatga o‘girgandan keyin raqamli shakldagi axborot quyidagicha bo‘lsin:

43 E5 4A 01 FB

Har bir belgini chap tomondan 8 bitgacha nollar bilan to‘ldirib, uni ikkilik sanoq tizimi formatiga o‘giramiz, baytlarni bir-birining ostiga yozamiz va ustunlar bo‘yicha xar bir bitlarni 2 moduli bo‘yicha qo‘shamiz (3.1-jadval).

3.1-jadval

43	0	1	0	0	0	0	1	1
E5	1	1	1	0	0	1	0	1
4A	0	1	0	0	1	0	1	0
01	0	0	0	0	0	0	0	1
FB	1	1	1	1	1	0	1	1
Natija								
	0	0	0	1	0	1	1	0

Ma'lumki, 2 moduli bo'yicha qo'shish funksiyasi quyidagicha aniqlanadi: 2 ta o'zgaruvchi bo'lgan holatda, agar faqat va faqat argumentlardan biri 1 bo'lsa amalning bajarish natijasi 1 bo'ladi. Uch yoki undan ortiq o'zgaruvchilar funksiyasi uchun, faqatgina qiymati 1 ga teng bo'lgan argumentlar soni toq bo'lgandagina amalni bajarish natijasi 1 bo'ladi:

(0001 $0110_{(2)}$yoki $16_{(16)}$) natija xesh-funksiyasining qiymati bo'ladi. 3.1-jadvaldagi ostiga chizilgan nollar axborotdagi har bir belgini 8 bitgacha to'ldirish uchun qo'shilganligini bildiradi.

Eslatib o'tish lozimki, xesh-funksiyalar quyidagi maqsadlar uchun foydalaniladi:

- ma'lumotlarni qidirishni tezlashtirish;
- xabarlarning yaxlitligi va rostligini tekshirish;
- elektron-raqamli imzodan foydalanilishda axborotning siqilgan obrazini yaratish;
- autentifikatsiya jarayonida parolni himoya qilish.

Kolliziyasi mavjud bo'lmagan xesh-funksiyani aniqlash nazariy jihatdan yechimi yo'q hisoblanadi. Biroq, amalda oddiy arifmetik amallar yordamida juda yaxshi natijalar beruvchi xesh-funksiyalarni yaratish mumkin. Bundan tashqari, ko'pincha, minimal kolliziyalarga ega bo'lgan xesh-funksiyalarni yaratish uchun axborot xususiyatlaridan ham foydalanish mumkin.

O'tkazilgan ko'p sonli tajribalar ikkita asosiy xeshlash turlarining yaxshi natijalar berishini ko'rsatdi, ulardan biri *bo'lishga* va ikkinchisi *ko'paytirishga* asoslangan. Biroq, bu mavjud bo'lgan yagona usullar emas, bundan tashqari ular har doim ham yagona optimal yechim bo'lavermasligi kuzatilgan.

Bo'lish usuli juda sodda - axborot kodi ifodalangan sonni M butun soniga bo'lishdan qolgan qoldiqdan foydalaniladi:

$$h(x) = x \bmod M \qquad (3.1)$$

Bunday holda, o'zgarmas son M - konstantani tanlashga alohida e'tibor berish talab etiladi. Masalan, agar uni 100 ga teng deb olsak va kalit sifatida tug'ilgan yil olinsa, unda taqsimot bir qator masalalar uchun juda notekis bo'ladi. Bundan tashqari, juft konstantada

funksiyaning qiymati juft va konstanta toq bo'lganda esa - toq bo'ladi, bu esa maqsadga muvofiq bo'lmagan natijalarga olib kelishi mumkin.

Agar M - bu sanoq tizimining darajasi bo'lsa, masalan ikkilik sanoq tizimida 2 bo'lsa, ahvol bundan ham battarroq bo'ladi, chunki bunda natija faqatgina o'ngdagi kalitning bir necha raqamlariga bog'liq bo'lib qoladi. Xuddi shu tarzda, M ning 3 ga karrali bo'lmasligi kerakligini ko'rsatish mumkin, chunki harfli kalitlarda ularning ikkitasini o'rnini almashtirish natijasida farqi uchga karrali bo'lgan qiymatlar bo'lishi mumkin.

Yuqorida keltirilgan mulohazalar tub sondan foydalanish yaxshiroq degan fikrga olib keladi. Aksariyat hollarda bunday yechim juda qoniqarli natijalar beradi. Amalda, bo'lish usuli axborotni xeshlashning eng keng tarqalgan usullaridan biri hisoblanadi.

Ko'paytirish usuli. Ko'paytirish usuli yordamida axborotni xeshlash uchun quyidagi formuladan foydalaniladi:

$$h(K) = [M * ((C * K) \bmod 1)] \qquad (3.2)$$

Bu yerda [ ] bu argumentning butun qismi.

Ko'paytirish usulida axborotni xeshlash uchun kalitni [0,1] oraliqda joylashgan ma'lum bir doimiy S songa ko'paytiriladi. Shundan so'ng, ushbu ifodaning kasr qismi olinadi va natija M modul chegaralaridan chiqib ketmaydigan qilib tanlangan ma'lum bir doimiy M soniga ko'paytiriladi.

Agar C konstanta to'g'ri tanlangan bo'lsa, unda juda yaxshi natijalarga erishish mumkin, ammo bunday tanlovni amalga oshirish qiyin. Olib borilgan tajribalar shuni ko'rsatadiki, ko'paytirish usuli ba'zan bo'lish usuliga qaraganda tezroq bajarilishi mumkin [18].

Dinamik xeshlash ma'lumotlar bazasining hajmi tez-tez va sezilarli darajada o'zgarib turadigan hollarda ma'lumotlarni qidirishni tezlashtirish yechish uchun qo'llaniladi.

Ma'lumki, ma'lumotlar bazasi o'sib borishi bilan:

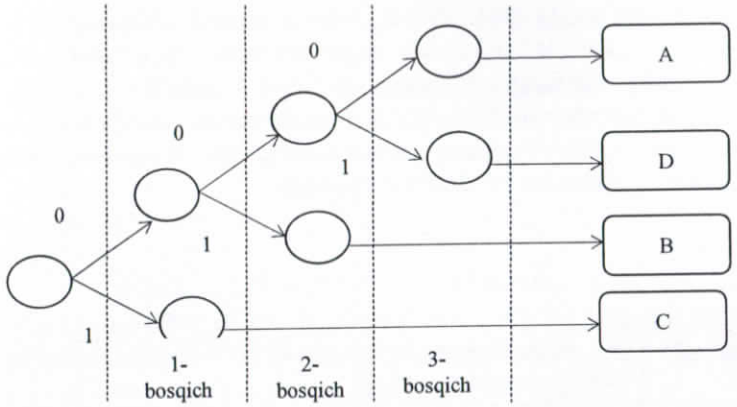
- dastlabki xesh-funksiyadan, kolliziyalarning kuchayishi natijasida qadamba-qadam tezlikni yo'qotgan holda, foydalanish;
- disk xotirasidagi joylarni asossiz band qilishga olib keladigan "zaxirali" xesh-funksiyani tanlash;

- xesh-funksiyalarning barcha qiymatlarini qayta hisoblab, funksiyani doimiy o‘zgartirib borish talab etiladi. Bu esa katta texnik resurslarni band qiladi.

Dinamik xeshlashda, xesh-funksiya elementiga kirish uchun faqat qisman foydalaniladigan vaqtinchalik kalitni hosil qilish zarur bo‘ladi. Boshqacha qilib aytganda, bo‘lishi mumkin bo‘lgan barcha xesh-funksiya elementlari uchun disk xotirasida adreslar ajratishga yetarli bo‘lishi uchun, yetarlicha uzun axborot uzunligi (bit) ketma-ketligi hosil qilinadi. Bu yerda band qilingan xotiraning hajmi ma’lumotlar bazasidagi elementlar soniga to‘g‘ri proporsional bo‘ladi. Jadvaldagi har bir yozuv alohida-alohida emas, balki ma’lumotlarni saqlash qurilmasidagi, masalan xotira diskidagi jismoniy bloklarga mos keladigan alohida bloklarda saqlanadi. Agar yozuvni joylashtirish uchun blokda boshqa bo‘sh joy bo‘lmasa, u holda blok ikkiga bo‘linadi va uning o‘rniga ikkita yangi blok ajratilib, uning adres ko‘rsatgichlari qo‘yiladi.

Masala, bloklarga havola qiladigan shoxlarga ega binar daraxtini hosil qilish bo‘lib, vaqtinchalik kalitga asoslangan holda yo‘naltirishni amalga oshirilishi ko‘zda tutiladi. Bunda daraxt tugunlari ikki xil - boshqa tugunlarni ko‘rsatadigan tugunlar yoki bloklarni ko‘rsatadigan tugunlar bo‘lishi mumkin.

Dinamik xeshlashning dastlabki qadamida faqat dinamik ravishda ajratilgan bo‘sh blok uchun ko‘rsatgich mavjud bo‘ladi. Yangi element qo‘shilganda, vaqtinchalik kalit hisoblab chiqiladi va uning bitlari blokning joylashgan o‘rnini aniqlash uchun navbatma-navbat ishlatiladi. Masalan, 00 ... vaqtinchalik kalitlari bo‘lgan elementlar A blokka va 01 ... esa B blokka joylashtiriladi. A to‘lgandan keyin, u shunday bo‘linadiki, bunda 000 ... va 001 ... elementlar turli bloklarga joylashtiriladi va hokazo (3.1-rasm).



3.1-rasm. Dinamik xeshlash bloklari

Yuqoridagilarga qo‘shimcha ravishda, ko‘plab xeshlash usullari mavjudligi, masalan, kengaytiriladigan xeshlash usuli, ketma-ketlikni saqlash usuli, minimal ideal xeshlash usuli, mukammal xeshlash usuli, universal xeshlash usuli va boshqalar mavjudligi aytib o‘tish joiz. Ularning har biri axborotni xeshlash uchun ishlatilishi mumkin. Albatta, xeshlash usulini tanlash ko‘p jihatdan har bir masalaning aniq qo‘yilishiga bog‘liq bo‘ladi.

Shuni ta’kidlash kerakki, axborotni xeshlash masalasi mavjud usullar bilan cheklanmaydigan masalalar sirasiga kiradi. Ko‘plab matematiklar xeshlash usullari hamda masala yechimini to‘liq qamrab oluvchi algoritmlar yaratish ustida katta kuch va salohiyatlarini sarflagan bo‘lishlariga qaramay, bugungi kunda ushbu mavzuda o‘ylab ko‘rishga arzigudek muammolar mavjud.

3.2. Blokcheyn tizimlarida mavjud axborotni xeshlash algoritmlari tahlili va axborotni xeshlashning MD5 algoritmi

Bugungi kunga kelib, axborotni xeshlash uchun Message Digest (*ML4, MD5*), Secure Hashing Algorithm (*SHA1, SHA2, SHA3, SHA256*) kabi ko‘plab algoritmlar qo‘llaniladi.Ularning barchasi o‘ziga yuklangan vazifalarni, o‘z afzalliklari va muayyan kamchiliklari bilan muvaffaqiyatli uddalab kelmoqda desak xato bo‘lmaydi. Tabiiyki, ularning har birini bir xil matnni xeshlashda

ishlatish natijasida turli xil qiymatlar olinadi. Masalan, "Salom, Toshkent!" matnini turli xil algoritmlardan foydalanib xeshlash natijasida biz quyidagi natijalarni olamiz (3.2-jadval):

Turli xil algoritmlar qo'llab, biror matnning xeshlash natijalarini taqqoslash uchun : http://www.blockchain-basics.com. elektron manzilidagi tizimdan foydalanish mumkin

3.2-jadval

MD5:	9F8FAB46A797B1C00A3C66723528DF2B
SHA1:	BEB372A61A9068F6F5B3C3957D339D756F15E7F1
SHA256:	2F5A666C516C01212431F19513C57BC56B73A0E885EF1C7E5E087178BE197FE0
SHA512:	A4DD9D7765EB8A5819E6C789F4347BEC72AB33BE27DDFF165C4335D4A89941465913318020FD301D7000B434F64CC62984670CF10ED10F863403E330D4CD6B48

Ko'rinib turibdiki, jadvalda ko'rsatilgan xesh-qiymatlar, ushbu qiymatlarni hosil qiladigan xesh-funksiyalarni amalga oshirish algoritmlaridagi farqlar tufayli bir xil emas.

Aniq misol sifatida MD5 algoritmni ko'rib chiqaylik. MD5 - bu 128-bitli xeshlash algoritmi bo'lib, u 1991-yilda Massachusets texnologiya instituti professori Ronald L.Rivest tomonidan ishlab chiqilgan. Xesh-funksiyani MD5 hisoblash algoritmini umumlashgan shaklda quyidagicha ifodalash mumkin.

Birinchi qadam: oqimni tekislash. L uzunlikdagi dastlabki axborotning oxiriga yakka bit qo'shiladi, so'ngra yangi hosil bo'lgan L' ning o'lchami 512 (L' mod 512 = 448) moduli bo'yicha 448 bilan taqqoslanish imkoni bo'lishi uchun zarur bo'lgan bitlarga nol soni qo'shib chiqiladi. Nol sonli bitlarni qo'shish, hatto yakka bit qo'shilgandan keyin yangi hosil bo'lgan L' uzunligi 448 bilan taqqoslanadigan bo'lsa ham amalga oshiriladi.

Ikkinchi qadam: axborotga unga karrali ravishda o'z uzunligini qo'shish. Modifikatsiyalangan axborotga uzunligi 64-bit bo'lgan tasvir (axborotdagi bitlar soni) qo'shib yoziladi. Ya'ni T axborot uzunligi 512 (T mod 512 = 0) ga karrali holga keladi. Agar dastlabki axborotning uzunligi 264 - 1 dan oshsa, unda 64 bitdan kichiklari qo'shib yoziladi. Bundan tashqari, taqdim etilgan 64 bitli

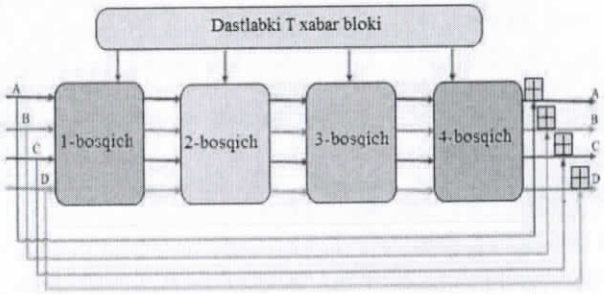
uzunlikni ko'rsatish uchun avval kichik 32 bit, keyin katta 32 bit yoziladi.

Uchinchi qadam: buferni belgilash. Hisoblashlar uchun 32 bit o'lchamdagi 4 ta o'zgaruvchilar kiritiladi va ularga o'n oltilik sanoq tizimidagi quyidagi boshlang'ich qiymatlar beriladi:

A = 67 45 23 01;
B = EF CD AB 89;
C = 98 BA DC FE;
D = 10 32 54 76.

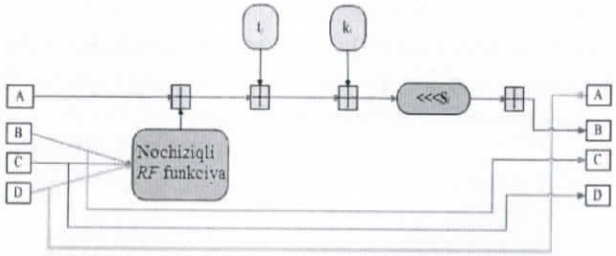
Ushbu o'zgaruvchilarda algoritmning har bir qadamidagi oraliq hisob-kitoblar natijalari saqlanadi. ABCDning boshlang'ich holatini *initsializatsiyalovchi vektor* deb ataladi.

To'rtinchi qadam: xeshni hisoblash. Dastlabki axborot uzunligi 512 bit bo'lgan T bloklarga bo'linadi. Sikldagi har bir blok uchun 3.2-rasmda ko'rsatilgan operatsiyalar bajariladi. Ya'ni, ABCD o'zgaruvchilari 32 bitli qiymatlarining birlashmasi shaklidagi dastlabki axborot barcha bloklarga ishlov berish natijasi, xesh-funksiyalarining qiymati bo'lib hisoblanadi [10].



3.2-rasm. Xeshni hisoblash asosiy siklining bir qadami

Algoritm jami 16 ta iteratsiyani ko'zda tutib, *i*- siklning har bir bosqichda ABCD o'zgaruvchilari va dastlabki T matn bloki ustida quyidagi sxema bo'yicha bir xil turdagi o'zgarishlar amalga oshiriladi (3.3-rasm).



3.3-rasm. Raund siklining bitta iteratsiyasi

3.2- va 3.3-rasmlarda quyidagi shartli belgilar qo‘llanilgan:

- umumlashtirilgan *RF* funksiya nomi ostida, quyidagicha aniqlanuvchi 4 ta *F, G, H* va *I* yordamchi nochiziqli funksiyalar:

$$\left.\begin{aligned} F(B,C,D) &= (B \wedge C) \vee (\neg B \wedge D) \\ G(B,C,D) &= (B \wedge D) \vee (\neg D \wedge C) \\ H(B,C,D) &= B \oplus C \oplus D \\ I(B,C,D) &= C \oplus (\neg D \vee B) \end{aligned}\right\} \quad (3.3)$$

Mazkur funksiya va argumentlari qiymati 32 bitli so‘zdan iborat.

- t_j - dastlabki T axborotning baytlari teskari tartibda keladigan 32-bitli bloki j-inchi qismi; - k_i–quyidagi formula bilan aniqlanadigan konstantaning butun qismi

$$k_i = 2^{32} \times |\sin(i + 16 \times (r - 1))| \quad (3.4)$$

bu yerda:i-siklning iteratsiya raqami ($i = 1..16$);
r-hisoblash bosqichi raqami ($r = 1..4$);
x- sin(x) funksiyasining argumenti, radianlarda o‘lchanadi.

$\boxplus$ - 2^{32} modul bo‘yicha qo‘shish.

$<<<s_i$– chap tomonga s_i razryad siklik siljish.

Dastlabki T axborot blokining t_j foydalaniladigan 32-bitli bloki j-inchi qismi va s_i- chap tomonga siklik siljish qiymati iteratsiya raqamiga bog‘liq bo‘lib, u 3.3-jadvalda keltirilgan.

3.3-jadval. Sikl bosqichida ishlatiladigan kattaliklar

Iteratsiyalar raqami		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
1-bosqich	t_j	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9	t_{10}	t_{11}	t_{12}	t_{13}	t_{14}	t_{15}	t_{16}	
	s_i	7	12	17	22	7	12	17	22	7	12	17	22	7	12	17	22	
2-bosqich	t_j	t_2	t_7	t_{12}	t_1	t_6	t_{11}	t_{16}	t_5	t_{10}	t_{15}	t_4	t_9	t_{14}	t_3	t_8	t_{13}	
	s_i	5	9	14	20	5	9	14	20	5	9	14	20	5	9	14	20	
3-bosqich	t_j	t_6	t_9	t_{12}	t_{15}	t_2	t_5	t_8	t_{11}	t_{14}	t_1	t_4	t_7	t_{10}	t_{13}	t_{16}	t_3	
	s_i	4	11	16	23	4	11	16	23	4	11	16	23	4	11	16	23	
4-bosqich	t_j	t_1	t_8	t_{15}	t_6	t_{13}	t_4	t_{11}	t_2	t_9	t_{16}	t_7	t_{14}	t_5	t_{12}	t_3	t_{10}	
	s_i	6	10	15	21	6	10	15	21	6	10	15	21	6	10	15	21	

Har 4 ta bosqichdan keyin har bir *ABCD* o‘zgaruvchining yangi (modifikatsiyalangan) qiymati o‘zgaruvchining dastlabki qiymati (o‘zgaruvchining 1-bosqichgacha qiymati) bilan 2^{32} moduli bo‘yicha ($\boxplus$)qo‘shiladi.

Beshinchi qadam: hisob-kitoblar natijasi. Hisob-kitoblarning natijasi *ABCD* buferida joylashgan bo‘lib, u xesh-funksiyasining yakuniy qiymati hisoblanadi. Agar hisob-kitoblar natijasi baytlar shaklida chiqarilib, kichik *A* baytdan boshlanib, katta *D* bayt bilan yakunlangan bo‘lsa, unda biz ushbu 1, 0, 15, 34, 17, 18… MD5-xeshni olamiz.

MD5 algoritmini tahlil qilayotganda, beixtiyor ushbu algoritm mualliflari xesh-funksiya kolliziyasining oldini olish uchun qanday chuqur tafakkur va zarur choralar qo‘llaganligiga guvoh bo‘lamiz. Shunga qaramay, tadqiqotlar hali ham davom etmoqda va xesh-qiymatlarning kolliziyasiz hisoblash algoritmini yaratish maqsadiga hali to‘liq erishilgan deb ayta olmaymiz.

MD5 algoritmini umumlashtirib, xesh-funksiyasini hisoblash jarayonini 3.4-rasmdagi kabi blok-sxemada tasvirlash mumkin.

Ushbu blok-sxemaning tavsifi quyidagicha:

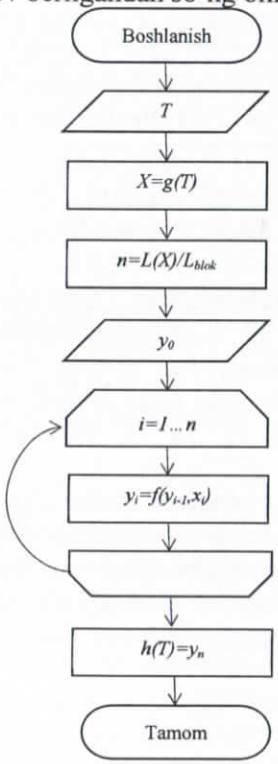
a) T dastlabki axborotga yordamchi axborotlar, masalan, axborotning tasvir (obraz) uzunligi, yordamchi belgilar va boshqalar shunday qo‘shiladiki, yangi hosil bo‘lgan X axborot uzunligi xesh-

funksiyaning muayyan spetsifikatsiyasi bilan aniqlangan L_{blok} kattalikka karrali bo'lsin.

b) Xeshlash jarayonini belgilash uchun dastlabki y_0 qiymat-sinxron jo'natmasidan foydalaniladi.

v) X axborot obrazi x_i shaklidagi shunday o'zgarmas uzunlikka ega L_{bl} n bloklarga bo'linadiki, uning ustida oldingi blokning y_{i-1}. xeshlash natijasiga bog'liq bo'lgan bir hil turdagi $f(y_{i-1}, x_i)$ xeshlash operatsiyasi bajariladi.Bu yerda $i = 1,2,...,n$,

g) dastlabki X axborotning $h(X)$ xesh-obrazi oxirgi x_n blokka ishlov berilgandan so'ng olingan y_n xeshlash natijasi bo'ladi.



3.4-rasm. Xesh-funksiya qiymatini hisoblash algoritmining blok-sxemasi

3.3. Blokcheyn tizimlarida xeshlash algoritmlari kolliziyalarini aniqlash usullari

Avval aytib o'tganimizdek, xesh-funksiyasining kolliziyasi - turli xil axborotlar uchun funksiyaning bir xil qiymat qabul qilishi hisoblanadi.

Bunday holatni MD5 algoritmi misolida ko'rib chiqaylik.

2004-yilda Vang Syaoyun boshchiligidagi xitoylik tadqiqotchilar MD5 algoritmi kolliziyalarini qisqa - 1 soat vaqt ichida IBM p690 klasterida ham topishga imkon beradigan zaiflikni kashf etganliklarini e'lon qilishdi. Shuningdek ular 2005-yilda bir xil MD5 xeshini beradigan 128 baytdan iborat turli xil ketma-ketlikni topadigan algoritmni nashr etishdi. Ushbu juftliklardan biri 3.4-jadvalda keltirilgan (farqli razryadlar ajratib ko'rsatilgan va tagiga chizilgan):

Ushbu bloklarning har biri 79054025255fb1a26e4bc422aef54eb4 ga teng bo'lgan MD5 xesh beradi.

Vang Syaoyun va Yuy Xunbo usuli MD5 algoritmi Merkl-Damgardning iteratsiya usuli asosida yaratilganligi faktidan foydalanadi. MD5 algoritmi kirishiga berilgan T fayli avval uning uzunligi 64 baytga karrali bo'lishi uchun to'ldiriladi, so'ngra har biri 64 bayt uzunlikka ega bo'lgan n ta $M_0, M_1, ..., M_{n-1}$. bloklarga bo'linadi. Shundan so'ng, 16 baytlik holatlar s_0, s_1, ..., s_n ketma-ketligi $s_{i+1}=f(s_i, M_i)$ formuladan foydalanib hisoblanadi, bu yerda f ma'lum bir fiksirlangan funksiya. Boshlang'ich s_0 holati initsializatsiyalovchi vektor olinadi.

3.4-jadval. Bir xil MD5 xesh beradigan turli ketma-ketliklar misoli

d131dd02c5e6eec4693d9a0698aff95c	2fcab58712467eab4004583eb8fb7f89
55ad340609f4b30283e48883257 1415a	085125e8f7cdc99fd91dbdf28037 3c5b
d8823e3156348f5bae6dacd436c9 19c6	dd53e2b487da03fd02396306d24 8cda0
e99f33420f577ee8ce54b67080a8 0d1e	c69821bcb6a8839396f9652b6ff7 2a70

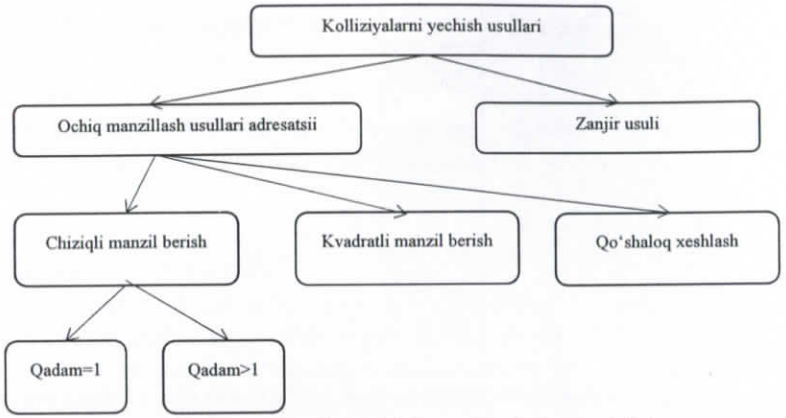
d131dd02c5e6eec4693d9a0698aff95c	2fcab50712467eab4004583eb8fb7f89
55ad340609f4b30283e4888325f1415a	085125e8f7cdc99fd91dbd7280373c5b
d8823e3156348f5bae6dacd436c919c6	dd53e23487da03fd02396306d248cda0
e99f33420f577ee8ce54b67080280d1e	c69821bcb6a8839396f965ab6ff72a70

Yuqorida aytib o‘tganimizdek, kolliziyalar xesh-funksiyalarining eng zaif nuqtasi hisoblanadi. Gap shundaki, axborotlarning xeshlanishi turli xil muammolarni yechishda, jumladan foydalanuvchini autentifikatsiya qilishdagi parolni himoyalash uchun ham ishlatiladi. Bunday holda, xesh-funksiyaning kolliziyasi maxfiy axborotlarning xavfsizligiga tahdid soladi, chunki foydalanuvchi autentifikatsiya qilinayotganda u tomonidan kiritilgan parol har safar bitta xesh-funksiya qo‘llanib xeshlanadi va natijasi ma’lumotlar bazasida qayd etilgan parol xeshi bilan solishtiriladi.

Bunday yondashuv bilan, buzg‘unchi fikrli odam ma’lumotlar bazasiga kirish imkoniyatini qo‘lga kiritish uchun foydalanuvchining dastlabki parollarini tiklay olmaydi, lekin agar xesh-funksiyasining kolliziyalarni qanday topishni bilsa, unga soxta parolni topish qiyin bo‘lmaydi.

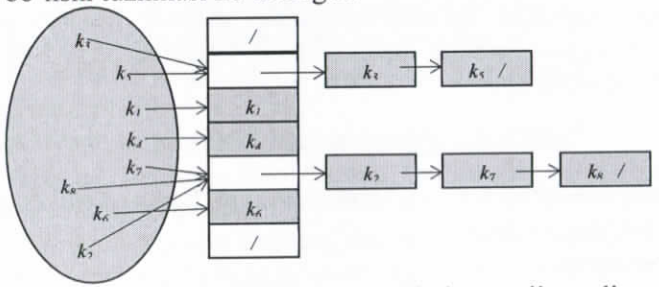
Ushbu muammoni yechishning, ya’ni xesh-funksiyasi kolliziyalari muammosini yechishning o‘z afzalliklari va kamchiliklariga ega bo‘lgan bir nechta yechimlari mavjud (3.5-rasm).

Zanjir usuli eng keng tarqalgan usul bo‘lib hisoblanadi. Uning texnologiyasi shundan iboratki, bir xesh-qiymatiga mos keladigan to‘plam elementlari bitta zanjir- ro‘yxatga bog‘lanadi. *i* raqamli pozitsiyada, kalitning xesh-qiymati *i* ga teng bo‘lgan elementlar ro‘yxati boshiga havola qiladigan ko‘rsatgich saqlanadi. Agar to‘plamda bunday elementlar bo‘lmasa, *j* pozitsiyada NULL yoziladi.



3.5-rasm. Kolliziyalarni yechish usullarining tarkibi

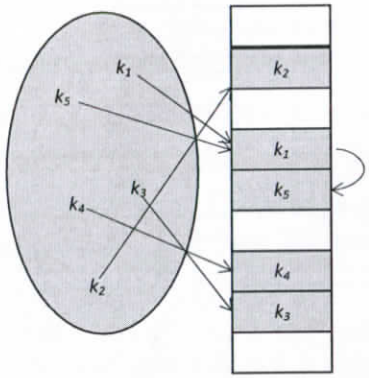
Natijada, agar xesh-funksiyasining bir xil qiymati kalitning bir nechta turli xil qiymatlari uchun qaytarilsa, unda ushbu manzilda barcha qiymatlarni o‘z ichiga olgan ro‘yxatga ko‘rsatgich joylashadi. 3.6-rasmda kolliziyalar sodir bo‘lganda xesh-jadval va zanjirlarning hosil bo‘lishi tuzilmasi ko‘rsatilgan.



3.6-rasm. Kolliziyalarni yechishning zanjir usuli sxemasi

Kolliziya muammolarini yechishning yana bir usuli *ochiq manzillash* deb nomlanadi.

Zanjirli xeshlashdan farqli o‘laroq, ochiq manzillashda hech qanday ro‘yxatlar yo‘q va barcha yozuvlar xesh-jadvalning o‘zida saqlanadi. Jadvalning har bir katakchasi yoki dinamik to‘plam elementini yoki *NULL*ni o‘z ichiga oladi.



3.7-rasm. Kolliziyalarni ochiq manzillash usuli orqali yechish

Ochiq manzillash usuli g'oyasi shundan iboratki, ilgari band qilinmagan katakni topmaguncha, ularni *h(k)*dan boshlab ma'lum tartibda ko'rib chiqiladi. Katakni qidirishda, ular element topilmaguncha yoki element yo'qligini ko'rsatadigan bo'sh katak topilmaguncha davom etadi (3.7-rasm).

Buning uchun biz xesh-funksiyani ikkinchi argument - urinish raqami degan argument qo'shib modifikatsiyalanadi. *K* kaliti uchun ko'rib chiqiladigan kataklar ketma-ketligi (sinovlar ketma-ketligi) quyidagicha shaklga ega:

$$H(k,0),\ H(k,1),\ H(k,2),\ \ldots,\ H(k,\ m\text{-}1).$$

Funksiya shunday bo'lishi kerakki, *0 ... m-1*ketma-ketlikdagi har bir raqam bir marta uchrasin.

Chiziqli manzil berish

Chiziqli manzil berish deb nomlanadigan ochiq manzillashning eng oddiy sxemasi tekshiruvlarning quyidagi siklik ketma-ketligidan foydalanadi:

$$h(K),\ h\ (K-1),\ \ldots,\ 0,\ M-1,\ M-2,\ \ldots,\ h(K)+1$$

va *M* elementlar jadvalidagi *K* kaliti qidiriladi. Agar jadval to'liq bo'lmasa va kalit mavjud bo'lmasa, u qo'shiladi.

Tajribalar shuni ko'rsatadiki, jadvalning boshini to'ldirishda algoritm yaxshi ishlaydi, ammo u to'lib borgan sayin jarayon

sekinlashadi va sinovlarning uzun seriyalari borgan sayin tez-tez uchraydi.

Kvadrat manzil berish

Chiziqli manzil berish usulida, doimiy ravishda bir qadamga o'zgarish o'rniga, quyidagi formuladan foydalanish ham mumkin:

$$h = h + a^2,$$

bu yerda *a* - urinish soni.

Manzillashning ushbu turi yetarlicha tez ishlaydi va har doim 1, 4, 9, 16, 25, 36 siljishlar bo'ylab doimo yakka-yu yagona yo'lni bosib o'tadi. Jadvalda kolliziyalar qancha ko'p bo'lsa, bu yo'l shuncha uzun bo'ladi. Bir tomondan, bu usul jadval bo'yicha yaxshi taqsimlanishni ta'minlaydi, boshqa tomondan qayta hisoblashlar uchun ko'proq vaqt talab etadi.

Xesh-funksiyalar va ularning kolliziyalarini qidirish va yechish usullari masalaning qo'yilishi va xeshlanadigan ma'lumotlar miqdoriga qarab tanlanadi. Ularning har biri o'zining afzalliklari va kamchiliklariga egaligini yodda saqlash lozim.

3- bob yuzasidan nazorat savollari

1. Xesh-funksiyasi deganda nimani tushunasiz?
2. Xesh-funksiya qanday maqsadlarda foydalaniladi?
3. Kolliziya nima?
4. Axborot xeshini aniqlashning qanday usllari bor?
5. Axborot xeshini aniqlashning bo'lishga va ko'paytirishga asoslangan usullari qanday?
6. Axborotni dinamik xeshlash deganda nimani tushunasiz?
7. Axborotni xeshlashning qanday algoritmlari mavjud?
8. Axborotni xeshlashning MD5 algoritmi kim tomonidan va qachon yaratilgan?
9. MD5 algoritmida xesh qiymatni hisoblash siklining bir qadami nechta bosqichdan iborat?
10. 2^{32} modul bo'yicha qo'shish deganda nimani tushunasiz?
11. Blokcheyn tizimlarida xeshlash algoritmlari kolliziyalarini aniqlashning qanday usullari mavjud?
12. Blokcheyn tizimlarida xeshlash algoritmlari kolliziyalarini aniqlashning zanjir usuli qanday bosqichlardan iborat?

4-BOB. BLOKCHEYN TIZIMLARIDA AXBOROTNI SHIFRLASH VA TRANZAKSIYALAR KETMA-KETLIGINI NAZORAT QILISH USULLARI

Blokcheyn tizimlarida tranzaksiya ma'lumotlarini himoyasi uchun xesh-funksiyalariga qo'shimcha ravishda, yana bir muhim texnologiya - asimmetrik kriptografiyadan faol foydalaniladi. Bu foydalanuvchilarni aniqlash va tranzaksiyalar ma'lumotlarining ishonchliligini himoya qilish uchun asos, poydevor bo'lib xizmat qiladi.

Ushbu texnologiyaning asosiy g'oyasi biz ko'rib chiqqan, ma'lumotlarni xeshlashga o'xshash turli usullar yordamida tranzaksiya ma'lumotlarini *shifrlash hisoblanadi*. Ma'lumotlarni shifrlashning ko'plab usullari mavjud bo'lib, ularning kelib chiqishi qadimgi davrlarga borib taqaladi va ular, aslida, ma'lumotlarni xeshlash usullaridan tubdan farq qiladi.

4.1. Blokcheyn tizimlarida axborotni shifrlashning simmetrik va assimetrik usullari hamda elektron raqamli imzodan foydalanish modeli

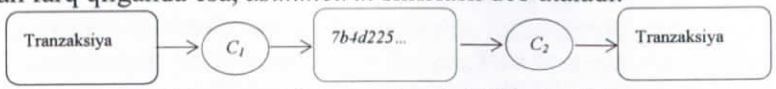
Shifrlangan matn, uni ochishni bilmaydiganlar uchun, harflar va belgilarning ma'nosiz ketma-ketligiga o'xshaydi. Shifrlangan matndan faqat shifrni ochish kalitiga ega bo'lgan kishigina foydalanishi mumkin. Shifri ochilgan matn, shifrlanishdan avvalgi, dastlabki axborot bilan bir xil bo'lishi lozim. Ushbu jarayonda shifrlash kaliti tushunchasi muhim rol o'ynaydi.

Axborotni shifrlash usullarini qo'llashning to'liq siklini quyidagicha ta'riflash mumkin:

- kriptografik kalit yordamida shifrlash amallaridan foydalanib, dastlabki axborotning shifrlangan matni hosil qilinadi;
- shifrlangan axborot biron bir joyda saqlanadi yoki kimgadir uzatiladi;
- dastlabki axborot kriptografik kalit yordamida shifrlarni yechish amali orqali qayta tiklanadi.

Axborotni shifrlash jarayonining to'liq sikli sxemasi 4.1-rasmda keltirilgan bo'lib, unda shifrlash kalitlarni C_1 va C_2 deb belgilangan. Ular bir xil bo'lishi ham, yoki bir-biridan farq qilishi ham mumkin. Birinchi holda, ya'ni shifrlash va shifrni yechish kalitlari bitta

bo'lganda, jarayon *simmetrik* shifrlash deb ataladi va kalitlar bir-biridan farq qilganda esa, *asimmetrik* shifrlash deb ataladi.



4.1-rasm. Ma'lumotlarni shifrlash sikli

Axborotni shifrlash jarayoni bilan amaliyotda yaqindan tanishish uchun http://crypt-online.ru/crypts/rsa/ manzilda joylashgan ochiq saytdan foydalanish mumkin: Bu ish axborotni shifrlash sikliga oid tasavvurlarni sinab ko'rish va mustahkamlashga imkon beradi.

Buning uchun ushbu saytda quyidagi parametrlarni tanlash lozim.:

- « Преобразования
- Без ключа
- Симметричные
- Асимметричные
- PCA
- Математические
- Утилиты
- Размер ключей: 256».

Yuqorida keltirilgan ochiq saytning o'zbekcha varianti yo'q bo'lganligi tufayli, uning parametrlari rus tilida keltirildi.

Unda agar"Generirovat" tugmachasini bossak, tizim quyidagi ochiq va yopiq kalitlarni tayyorlab beradi:

C_1=b7f7939051292c05ebbf4ef987cb5e246f4aee50944d84d9fdd8500013a62179 - ochiq kalit;

C_2=82c9801f19942bb809e1f8436e4726a5885bbf85e595258e0f5d83285f03181 - yopiq kalit.

Shundan so'ng, masalan, matnni shifrlash uchun, "Tranzaksiya" so'zini olib, "Kodirovat" tugmachasi bosilsa, natijada C_1 shifrlash kalitiga muvofiq ravishda quyidagi shifrlash natijasini olish mumkin:

"7b4d225a44dbd55c6b7ab7f6822041bf0f16fe90aa82c93c77ce50d63362bf2a".

"Dekodirovat" tugmachasini bosish orqali esa shifrlash natijasini tekshirib ko'rishimiz mumkin. Bu holda C_2 shifrni ochish kalitiga muvofiq ravishda quyidagi matnni olamiz:

"Tranzaksiya"

Albatta, keltirilgan misoldan kelib chiqib, quyidagi ikkita eslatmani aytib o'tish kerak:

- http://crypt-online.ru/crypts/rsa/ sayti hamma uchun ochiq foydalanishdagi sayt bo'lgani uchun, "Generirovat" tugmachasini har bosganda C_1 va C_2 shifrlash kalitlarining har xil qiymatlarni beradi va bu tushunarli: kalitlar takrorlanmas bo'lishi kerak. Shuning uchun yuqoridagi kalit sifatida keltirilgan C_1 va C_2 kalitlar boshqa foydalanuvchilar uchun boshqa qiymatlarga ega bo'ladi. Demak, shifrlash natijasi ham boshqacha bo'ladi. Lekin shifrni ochish natijasi bir xil bo'lib qoladi.

- foydalanuvchi shifrlash - shifrni ochish jarayonida kalitlarni shakllantirish uchun tizimning qanchalik to'g'ri (yoki ishonchli) ishlashini tekshira olmaydi, chunki dastlabki matnni shifrlash - shifrni ochish jarayonida algoritmlarning ishlashi ko'rinmaydi. Ammo, shu bilan birga, http://crypt-online.ru/crypts/rsa/ sayt faqat bugun ishlayotgani yo'q, u yetarli darajada mashhur sayt va shuning uchun uning ishlashi natijalariga ishonmaslik uchun hech qanday asos yo'q. Aks holda, mutaxassislar va ayniqsa kriptografiya sohasidagi matematiklar ushbu mavzu bo'yicha sayt egalariga o'z tanqidiy mulohazalarini bildirgan bo'lar edilar.

Blokcheyn tizimlarida elektron raqamli imzodan foydalanish modeli. Blokcheyn tizimlarida tizimi ishtirokchisining avtorizatsiyasi va axborot saqlanishi nazorati uchun assimetrik kriptografiya qo'llaniladi. Bunday holda, kalitlardan biri *ochiq kalit*, ikkinchisi esa *yopiq kalit* hisoblanadi.

Asimmetrik kriptografiyada kalitlar o'z-o'zidan ochiq va yopiq bo'lib hisoblanmaydi, chunki ma'lumotlarni har qanday kalit bilan shifrlash mumkin, lekin shifrni unga juft bo'lgan kalit yordamidagina ochish mumkin. Foydalanuvchining o'zi qaysi kalit ochiq, yoki qaysi kalit yopiq bo'lishini tayinlaydi. Ochiq kalit, ularga ishonish darajasidan qat'iy nazar, barcha xohlovchilarga tarqatiladi. Blokcheyn tizimining deyarli barcha ishtirokchilari ochiq kalit nusxasiga ega bo'lishi mumkin. Ammo yopiq kalit xavfsiz va begonalardan himoyalangan joyda saqlanishi shart.

Asimmetrik kriptografiyadan foydalanganda quyidagi amallarni bajarish kerak:

- kriptografik dasturlardan foydalanib bir-birini to'ldiruvchi kalitlar juftini hosil qilish;

- bitta kalitni ochiq kalit sifatida belgilash;
- ikkinchi kalitni yopiq yoki maxfiy kalit sifatida belgilash;
- yopiq kalitni xavfsiz joyda saqlash;
- ochiq kalitni hamma xohlovchilarga tarqatish.

Ochiq kalitlar, odatda, egalik huquqi berilishi mumkin bo'lgan foydalanuvchilarni identifikatsiyalash uchun ishlatiladi, muayyan bir foydalanuvchining axborotiga esa faqat tegishli yopiq kalitlar egalarigina kirish huquqiga ega bo'ladi. Ushbu kalit juftligi foydalanuvchilarni identifikatsiyalashga imkon beradi va ularga o'z axboroti tarkibini nazorat qilish imkoniyatini beradi, ularga foydalanuvchining elektron-raqamli imzosi (ERI) sifatida qaraladi.

Yuqorida aytilganlar tushunarli bo'lishi uchun, Blokcheyn tizimlarida ochiq-yopiq kalitlar juftidan foydalanish jarayonini ko'rib chiqaylik. Blokcheyn tizimlarida, birinchi tranzaksiyani hosil qilish uchun, mulkka egalik huquqini beruvchi foydalanuvchi quyidagi harakatlarni bajarishi lozim:

1-qadam. foydalanuvchining ixtiyorida bo'lgan barcha zarur axborotlardan foydalangan holda, masalan, tranzaksiyada qatnashgan barcha hisob yozuvlarning raqamlari, o'tkazib beriladigan mulk obyektlarining soni va boshqalar yordamida tranzaksiyani tavsiflash.

2-qadam. Tranzaksiyaning kriptografik xesh-qiymatini hosil qilish;

3-qadam. Egalik huquqini beradigan yopiq kalitdan foydalanib tranzaksiyaning xesh-qiymatini shifrlash.

4-qadam. 3-qadamda hosil qilingan shifrlangan matnni elektron raqamli imzo bilan imzolagan holda tranzaksiya sifatida qo'shish (4.2-rasm).

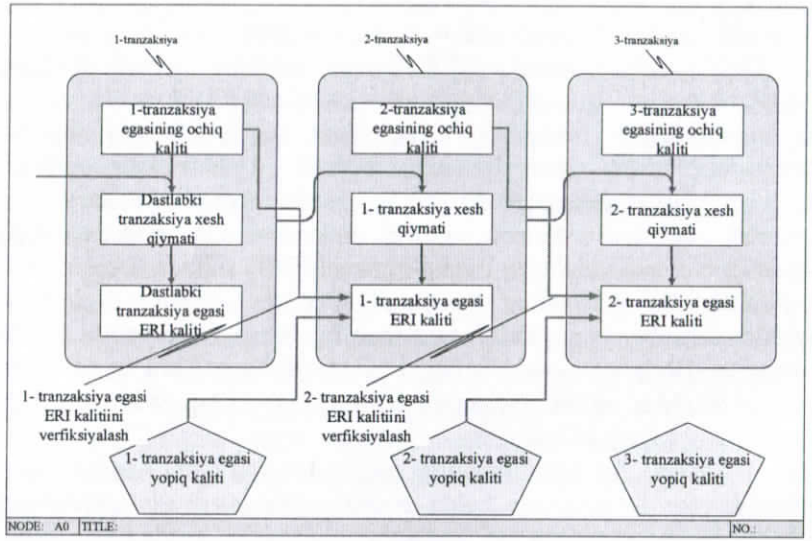
Tranzaksiyani tekshirish uchun Blokcheyn tizimlarining boshqa ishtirokchilari quyidagi amallarni bajarishlari zarur bo'ladi:

1-qadam. Elektron raqamli imzoning o'zini hisobga olmasdan, tekshirilishi kerak bo'lgan tranzaksiya ma'lumotlarining xesh-qiymatini hosil qilish.

2-qadam. Egalik huquqini beradigan ochiq kalitdan foydalanib, ko'rib chiqilayotgan tranzaksiyaning raqamli imzosi shifrini yechish.

3-qadam. 1-qadamda hisoblangan xesh-qiymatni 2-qadamda olingan xesh-qiymat bilan taqqoslash. Agar qiymatlar teng bo'lsa, tranzaksiya sanksiyalangan va egalik huquqini beradigan yopiq kalit

egasi tomonidan tasdiqlangan hisoblanadi. Agar xesh-qiymatlari teng bo‘lmasa, tranzaksiya noqonuniy hisoblanadi.



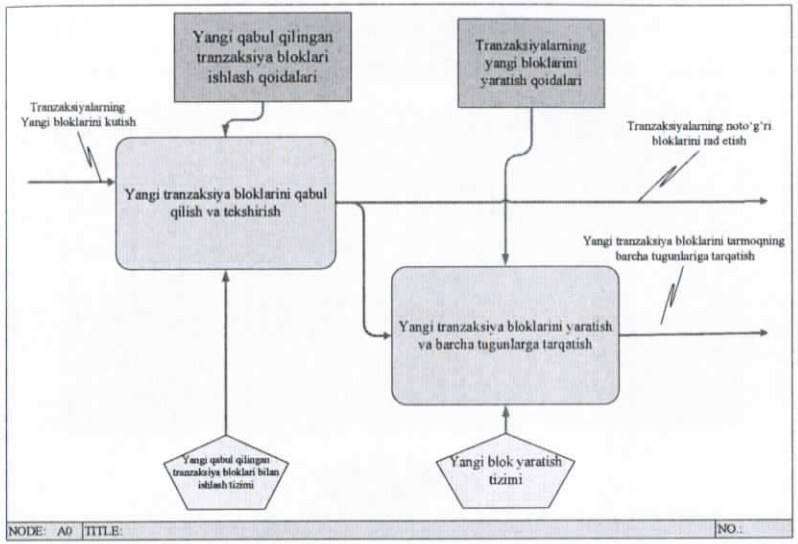
4.2-rasm. Blokcheyn tizimda ERIdan foydalanish sxemasi

4.2. Blokcheyn tizimlarida tranzaksiya bloklarini qabul qilish modeli va tahlil qilish algoritmi

Blokcheyn tizimlari texnologiyasini tushunish uchun boshlagan tadqiqotimizning *reyestrlarni ishonchsiz muhitda tarqatish uchun tayyorlash* bosqichiga o‘tamiz.

Xesh-qiymatlar va shifrlashdan foydalangan holda yangi tranzaksion bloklarni hosil qilish, tekshirish, tasdiqlash va tarqatish jarayonini ko‘rib chiqaylik.

Bir qatlamli tarmoq tugunlari, tranzaksiyaning yangi ma’lumotlarini va o‘z hamkorlaridan olingan bloklarga ishlov berishni boshqaruvchi jarayon ikki qismdan iborat (4.3-rasm):

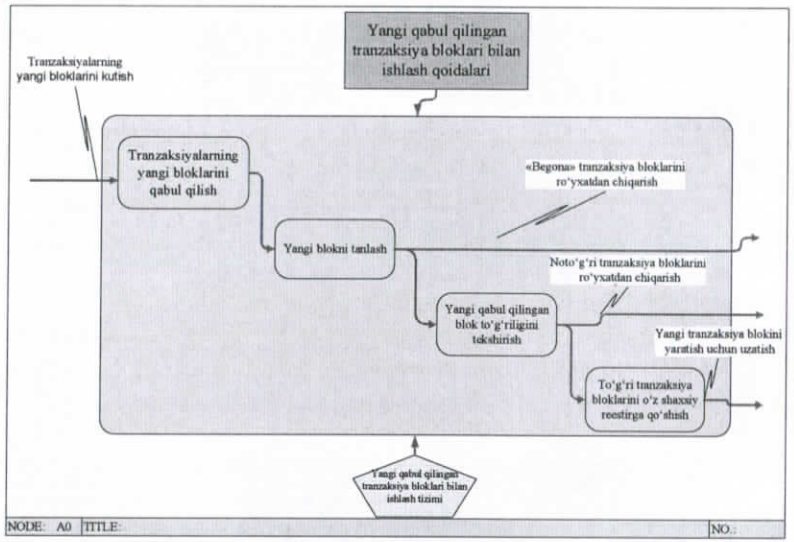


4.3-rasm. Bir qatlamli himoyalanmagan tarmoqda Blokcheyn tizimlar bloklariga ishlov berish modeli

I. Tranzaksiya bloklarini qabul qilish va ishlov berish;

II. Yangi blokni hosil qilish va boshqa tugunlarga tarqatish.

Bu yerda shuni inobatga olish lozimki, Blokcheyn tizimining har bir ishtirokchisi ham faqat doimo tranzaksiya bloklarini qabul qilish uchun kutish bilan band bo‘ladi deb bo‘lmaydi. Gap shundaki, Blokcheyn tizimining ayrim ishtirokchisi yangi tranzaksiya bloklarini hosil qilishning initsiatori bo‘lishi ham mumkin. Bunday holatda u tranzaksiya bloklarini qabul qilish uchun kutmasdan, tranzaksiyaning yangi blokini shakllantiradi va boshqa ishtirokchilarga tarqatadi. Ya’ni bunday holatda Blokcheyn tizimining mazkur ishtirokchisi tranzaksiya bloklariga ishlov berish jarayonining birinchi qismini tashlab, to‘g‘ridan-to‘g‘ri ikki qismidan ish boshlaydi.



4.5-rasm. Blokcheyn tizimlarning yangi qabul qilingan tranzaksiya bloklarini qabul qilish va ishlov berish jarayonining modeli

Yangi qabul qilingan tranzaksiya bloklarini qabul qilish va ishlov berish quyidagi qadamlardan iborat (4.4-rasm):

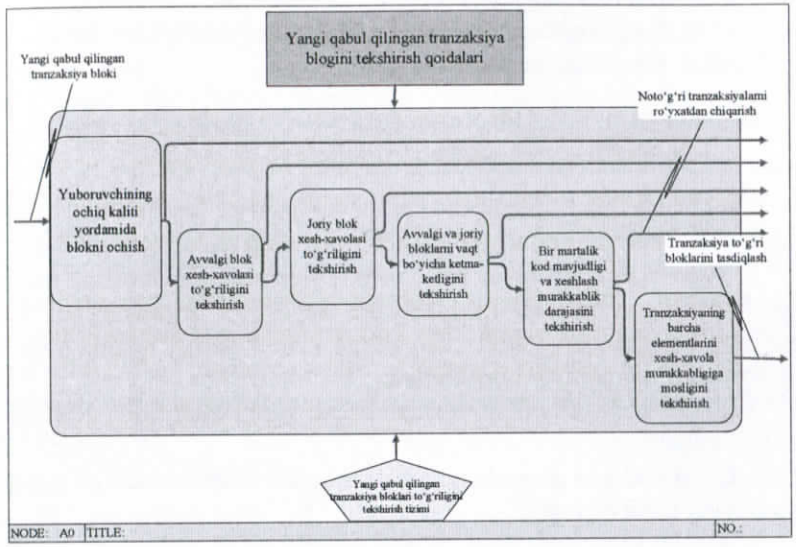
1. Yangi tranzaksiya bloklari Blokcheyn tizimlarining barcha tugunlariga (ya'ni Blokcheyn tizim a'zolari kompyuterlariga) kelib tushadi;

2. Har bir tugun yangi tranzaksiya ma'lumotlarini qabul qiladi va ular ichidan ular bilan ishlash zarur bo'lgan ma'lumotlarni tanlaydi.

3. Tegishli xesh-jumboqning yechimini tekshirib, shuningdek blokdagi barcha tranzaksiya ma'lumotlar formatlari va semantik to'g'riligi hamda avtorizatsiyasini tekshirib bo'yicha yangi bloklarga ishlov beriladi;

4. To'g'ri deb topilgan bloklar blokcheyn ma'lumotlari tarkibining (umumiy reyestrning) o'z nusxasiga qo'shiladi;

5. Agar yaqinda olingan blok noto'g'ri deb topilsa, u holda u rad qilinadi va tugunlar boshqa tranzaksiya ma'lumotlariga ishlov berishni davom ettiradi.



4.6-rasm. Blokcheyn tizimlarining yangi qabul qilingan tranzaksiyalar blokining to'g'riligini tekshirish jarayoni modeli

Shuni payqash qiyin emaski, "Yangi qabul qilingan tranzaksiya bloklarini qabul qilish va ishlov berish" bosqichida yangi qabul qilingan tranzaksiya bloklarining to'g'riligini tekshirish asosiy hal qiluvchi element hisoblanadi. Chunki yangi qabul qilingan tranzaksiya bloklari to'g'riligini tekshirish salbiy natija bilan yakunlangan taqdirda tranzaksiyaning keyingi bloklarini yaratish jarayoniga o'tilmaydi va jarayonda uzilish hosil bo'ladi.

Yangi qabul qilingan tranzaksiya bloklarining to'g'riligini tekshirish qoidalari quyidagicha (4.6-rasm):

1. Tranzaksiyada albatta o'zidan oldingi blokning to'g'ri xesh-havolasi mavjud bo'lishi shart;

2. Ko'rilayotgan tranzaksiya ma'lumotlarini ham o'z ichiga olgan to'g'ri xesh-havola albatta mavjud bo'lishi shart;

3. Murakkablik darajasi albatta to'g'ri bo'lishi shart;

4. Tranzaksiyadagi vaqt belgisi o'zidan avvalgi blok sarlavhasidagi vaqt belgisidan kechroq bo'lishi shart.

5. Bir martalik tasodifiy kod albatta mavjud bo'lishi shart;

6. Yuqorida keltirilgan beshta ma'lumotlar elementlarining barchasi xesh-qiymati birgalikda olinganda, oldindan berilgan murakkablik darajasiga mos kelishi shart.

4.3. Blokcheyn tizimlarida yangi tranzaksiya bloklarini yaratish modeli va xesh-jumboqni aniqlash algoritmi

Yangi blok hosil qilish va boshqa tugunlarga (ya'ni Blokcheyn tizim a'zolari kompyuterlariga) yuborish quyidagi qadamlardan iborat:

1. Agar qabul qilingan blok to'g'ri deb topilgan bo'lsa, unda faqat tekshirilgan to'g'ri tranzaksiyalar reyestrga birlashtiriladi va unga mos bo'lgan yangi tranzaksiyalarga ishlov berish hamda yangi blokni hosil qilish jarayoni boshlanadi.

2. Tegishli xesh-jumboqni yechish orqali yangi blok hosil qilinadi. Bunday holda:

2.1. Qo'shiladigan tranzaksiyaning ma'lumotlarini o'z ichiga olgan xesh-havola hosil qilinadi;

2.2. Yangi blok sarlavhasi uchun oldingi blok sarlavhasi xesh-havolasi hosil qilinadi;

2.3. Kerakli murakkablik darajasi o'rnatiladi;

2.4. Joriy vaqt belgilandi;

2.5. 2.1-2.4-bandlarda sanab o'tilgan ma'lumotlarni o'z ichiga olgan blok sarlavhasi hosil qilinadi;

2.6. Blok sarlavhasi uchun murakkablik darajasi yetarli bo'lgan xesh-jumboq yechiladi;

2.7. tayyorlangan sarlavha uchun xesh-jumboqni yechadigan bir martalik tasodifiy kodni qo'shiladi va yangi blokni hosil qilish yakunlanadi;

2.8. 2.7-bandda hosil qilingan blokni shaxsiy yopiq kalit yordamida shifrlanadi.

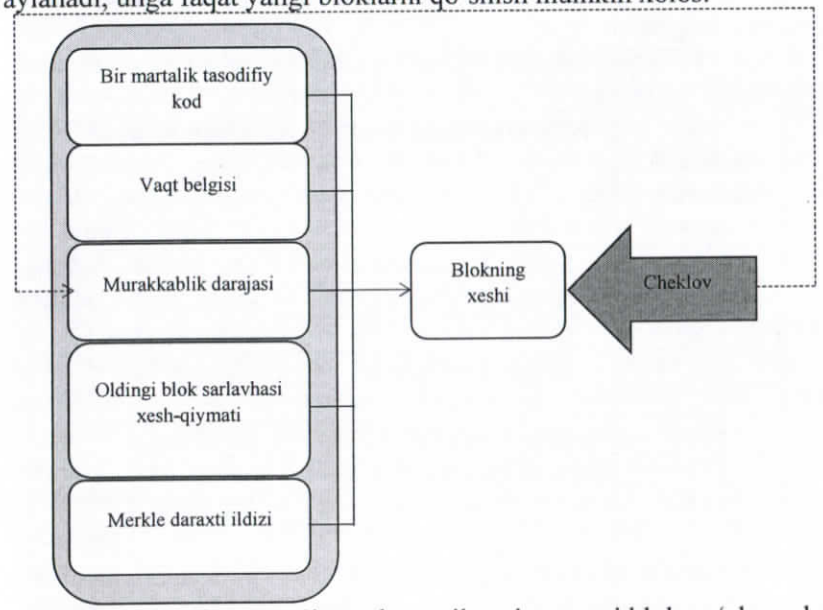
3. Xesh-jumboqni yechish tugaganidan so'ng, yangi hosil qilingan blok boshqa barcha tugunlarga yuboriladi.

"Yangi blokni hosil qilish va barcha boshqa tugunlarga tarqatish" jarayonida blokning sarlavhasi uchun xesh-jumboqni yechish eng muhim elementligini sezish qiyin emas.

Oldin ko'rib chiqqanimizdek, Blokcheyn tizimi ma'lumotlari tarkibi xesh-havolalarining yuqori sezuvchanlik xususiyati tufayli axborotning har qanday o'zgarishlarini darhol aniqlashga imkon

berishi zarur. Kimdir biror o'zgarishni amalga oshirmoqchi bo'lsa, u holda bundan ta'sirlanadigan barcha bloklarni qaytadan yozishni talab qilinishi kerak.

Agar Blokcheyn tizimidagi ishtirokchilardan biri avvalgi bloklarga o'zgartirishlar kiritishga qaror qilsa, unda o'zgarishlar kiritilishi oqibatida qayta yozishni talab qiladigan har bir blok uchun xesh-jumboqni hisoblab chiqish jarayoni katta texnik resurslar va xarajatlarini talab qiladi. Bir dona tranzaksiyaga kiritiladigan yagona o'zgarish blokcheyn ma'lumotlarining butun tarkibini qayta yozishga ketadigan vaqt hamda uning umumiy xarajati albatta: "tranzaksiyalar xronologiyasini o'zgartirishga bo'lgan har qanday urinish maqsadga muvofiqmi?" - degan savolni o'ylashga majbur qiladi. Natijada, blokcheyn ma'lumotlarning tarkibi o'zgarmas ma'lumotlar omboriga aylanadi, unga faqat yangi bloklarni qo'shish mumkin xolos.



4.7-rasm. Blokcheyn ma'lumotlar tuzilmasiga yangi blok qo'shganda yechish kerak bo'lgan xesh-jumboqni hisoblash jarayoni sxemasi

Blokcheyn ma'lumotlar tuzilmasiga yangi blok qo'shish paytida yechilishi kerak bo'lgan xesh-jumboqni hisoblash jarayonining sxemasi 4.7-rasmda ko'rsatilgan. Bu yerda, xesh-qiymatga qo'yilgan

cheklov yoki murakkablik darajasiga mos kelishi kerak bo‘lgan blok sarlavhasi ma’lumotlari ko‘rsatilgan. E’tibor berishimiz kerakki, murakkablik darajasi blok sarlavhasining bir qismi bo‘lib hisoblanadi va shuning uchun ushbu blok xesh-qiymatining ham bir qismi hisoblanadi. Bu esa, hech kim, xesh-jumboqni yechishda texnik resurslar uchun ortiqcha xarajatlarsiz, murakkablik darajasini ixtiyoriy ravishda pasaytirishga erisholmasligiga umid bag‘ishlaydi.

Xesh-jumboqlarining ishlashini yaxshiroq tushunish uchun aniq bir misol ko‘raylik. Avvalroq biz, “Salom Toshkent!” jumlasi uchun xesh-qiymatni hisoblash natijalarini ko‘rib chiqqan edik. Endi savolni boshqacha qo‘yamiz: “Salom Toshkent!” jumlasi bilan birlashganda uchta noldan boshlanadigan xesh-qiymatini hosil qiladigan bir martalik tasodifiy kod - *S* sonini topish talab etilsin. Bu yerda “uchta noldan boshlanadigan xesh-qiymat” sharti jumboqning murakkablik darajasini belgilaydi.

4.1-jadval.Xesh-jumboqni yechish uchun bir martalik tasodifiy kod qiymatini aniqlash

Bir martalik tasodifiy kod	**Xeshlanadigan matn**	**Xeshlash natijasi**
0	Salom Toshkent! 0	B91D099F
1	Salom Toshkent! 1	BC1C7069
2	Salom Toshkent! 2	B3EA9E3D
3	Salom Toshkent! 3	33161228
	…	
1728	Salom Toshkent! 1728	8BD9865D
1729	**Salom Toshkent! 1729**	**000AC65C**
1730	Salom Toshkent! 1730	64653CDD

Bir martalik tasodifiy kod qiymatlari bilan birlashgan matnning qisqartirilgan yakuniy xesh-qiymatni hisoblash natijalari 4.1-jadvalda berilgan. Jadvaldan 1729 raqamli bir martalik tasodifiy kod qo‘yilgan shartlar ostidagi xesh-jumboqni berishini ko‘rish mumkin. Yechimni topish uchun 0 qiymatdan 1 qadam bilan boshlab bir martalik tasodifiy kodning qiymatini asta-sekin oshirib borib, talab etilgan xesh-qiymatni olish uchun 1729 qadam tashlash talab etiladi.

4.4. Blokcheyn tizimlarida tranzaksiya xronologiyasini yaratish va tekshirish algoritmi

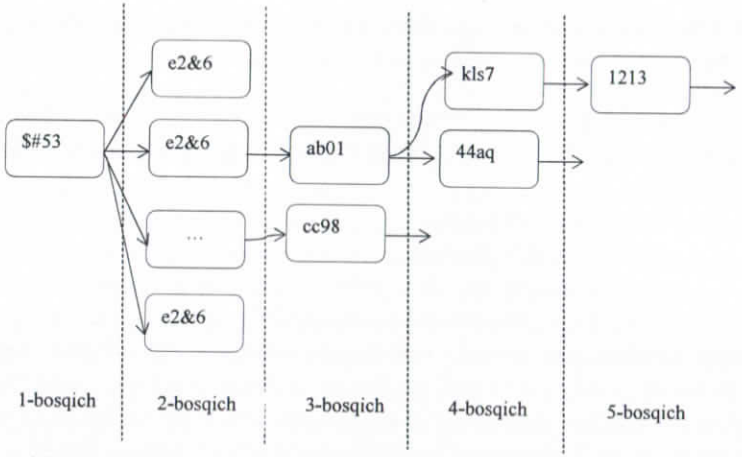
Tranzaksiyalar xronologiyasi hosil qilish uchun hisoblash xarajatlari miqdori bo‘yicha tanlash g‘oyasi quyidagi ikkita mezonga olib keladi:

- eng uzun zanjir mezoni;
- eng qimmat zanjir mezoni.

Eng uzun zanjir mezoni, bloklarning eng ko‘p sonidan iborat bo‘lgan blokcheyn ma’lumotlarining tarkibi, alal-oqibat hisob-kitob xarajatlarining maksimal miqdoriga olib keladi degan farazga asoslanadi. Ushbu mezonni yaxshiroq tushunish uchun, taqsimlangan tizimning barcha tugunlari blokcheyn ma’lumotlari tarkibining bir xil versiyasini qo‘llab-quvvatlaydigan va tasdiqlaydigan boshlang‘ich vaziyatni ko‘rib chiqaylik (4.8-rasm).

Har bir to‘rtburchak qisqartirilgan xesh-qiymati bo‘yicha aniqlanadigan bitta blokni anglatadi. Bir to‘rtburchakdan ikkinchisiga yo‘naltirilgan strelka blok sarlavhasini oldingi sarlavha bilan bog‘laydigan xesh-havolani anglatadi. 2-bosqich, ya’ni«ye2&6» blokga tayanadigan vaziyatda barcha tugunlar tranzaksiyalar ma’lumotlarining yagona xronologiyasiga rozi va mavjud zanjirga keyingi blokni qo‘shishi, ya’ni Blokcheyn tizimni bir blokka kattalashtirish uchun harakat qiladi deb qabul qilinadi.

Yangi blokni hosil qilish - bu barcha tugunlar o‘rtasidagi musobaqa kabi vaziyatni keltirib chiqaradi. Chunki bu jarayon «ye2&6» blok uchun maxsus xesh-jumboqni yechishni talab qiladi. Aytaylik, qandaydir vaqtdan keyin bir tugun yangi blokning xesh-jumbog‘ini yechib, uni barcha hamkorlarga yuboradi va navbatdagi blokcheyn bloki ma’lumotlari tarkibini taqdim etadi. Natijada, ushbu blokcheyn bloki ma’lumotlar tarkibini qo‘llab-quvvatlaydigan tugunlar uni “ab01” blokka tayanadigan yangi blok yordamida kengaytirishga harakat qiladi.



4.8-rasm. Maksimal uzunlikdagi yagona zanjirga ega bo‘lgan Blokcheyn tizimi tarkibi sxemasi

Ammo tarmoq orqali yangi blokni barcha tugunlarga yetkazish muayyan vaqt talab etadi va barcha turdagi raqobatchilar bundan muammoga duch kelishadi. Xabarlarni yuborish kechikishi sababli, ba’zi tugunlar (ular ozchilik), “ab01” blokini hali olmagan bo‘ladi. Shuning uchun ular 2-bosqichdagi zanjirni jadallashtirishga urinishni davom ettiradilar. Oxir-oqibat, ushbu tugunlardan yana biri yangi blok uchun xesh-jumboqni muvaffaqiyatli hal qiladi, “cc98” xesh-qiymatini oladi va uni hamkorlarga uzatadi.

Shunday qilib, blokcheyn tugunlari ham «ab01»blokni, ham “cc98” bloklarni oladilar. Natijada, tugunlarning aksariyati, umumiy blokning tepasida ikkita shoxchasi bo‘lgan blokcheyn ma’lumotlari tarkibini qo‘llab-quvvatlaydi. Bunday vaziyatda eng uzun zanjir mezoni yagona natijaga erishishga imkon bermaydi, chunki ikkita zanjir: «$#53 →e2&6 →ab01» va «$#53 →e2&6 → cc98» bir xil uzunlikka ega.

Bunday vaziyatda tugunlarga zanjir o‘sadigan shoxchani tanlash erkinligi beriladi.

Ba’zi tugunlar, o‘zidan oldingi blok sifatida «ab01» blokka tayanadigan yangi blokni qidirishda davom etishlari mumkin, shu vaqtning o‘zida boshqa tugunlar esa oldingi blok sifatida “cc98” blokka tayanadigan yangi blokni qidirishlari mumkin. Alal-oqibat

shunday bo‘ladiki, jarayon davomida ko‘pchilik bloklar ikkita yangi blokni oladi, “kls7” va “44ad”, va ikkala blok ham oldingi blok sifatida «ab01» ga tayanadi. Bunday vaziyat ikkita tugun o‘z bloklari uchun bajarilgan ishlarni deyarli bir vaqtda tasdiqlaganligi sababli sodir bo‘lishi mumkin. Ushbu ikkita yangi blokni blokcheyn ma’lumotlari tarkibiga kiritish 4-qadamda ko‘rsatilganidek, strukturada uchta zanjir (zanjir shoxlari) mavjudligiga olib keladi. Bitta zanjir uchta blokdan iborat, ikkinchisi to‘rttadan iborat. Eng uzun zanjir mezoni bo‘yicha eng qisqa zanjir,ya’ni «$#53 →ye2&6 →cc98» shubhasiz reyestrdan o‘chiriladi,.

Ammo bu holat ham yakuniy natijani bermaydi, chunki bir xil uzunlikdagi ikkita zanjir hali ham mavjudligicha qolmoqda.

Bunda ayrim tugunlar“44ad” blokka tayangan yangi blokni qidirishga harakat qilib turgan bir paytda, boshqa tugunlarning “kls7” blokka tayangan yangi blok qidirishga harakat qilishi davom etadi.

Shubhasiz, muayyan vaqtdan so‘ng, “kls7” blokka tayanadigan yangi blok paydo bo‘ladi va ma’lumotlar tuzilishi 5-bosqichda namoyish etilgani kabi ko‘rinish oladi.

Blokcheyn ma’lumotlari tarkibi tranzaksiyalar xronologiyasi bir nechta nizoli versiyalarini o‘z ichiga olsa-da, ammo eng uzun zanjirning mezoni yagona aniq natijani, ya’ni aynan «$#53 →e2&6 →ab01→ kls7→1213» bloklardan iborat zanjirni olish imkonini beradi. Ko‘pgina tugunlar va oxir-oqibat tizimning barcha tugunlari aynan ushbu shoxchani kengaytirishga harakat qiladilar va “1213” blokka tayanadigan yangi blokni qidira boshlaydilar.

v) Blokcheyn tizimlarini o‘rganishda ko‘rishimiz lozim bo‘lgan so‘ngi mavzu – bu uning ishiga begonalar tomonidan aralashuv, ya’ni begonalar manipulyatsiyasiga qarshi barqarorligini ta’minlash masalasi qoldi.

Yuqorida ko‘rdikki, daraxt shaklidagi blokcheyn ma’lumotlari tarkibiga kirishning yagona yo‘li - bu hisob-kitob va texnik resurslarning katta xarajatlari evaziga paydo bo‘lgan tranzaksiya xronologiyasining tasdiqlangan to‘g‘ri versiyasi bilan ishlash xolos. Butun Blokcheyn tizimi hisoblash quvvatining asosiy boshqarish obyekti - to‘g‘ri yo‘lni belgilash va uni saqlab turish hisoblanadi. Blokcheyn ma’lumotlari tarkibining biror ichki blokidan boshlanuvchi yangi yo‘lni belgilash esa ushbu yo‘lning ko‘pchilik tugunlar

tomonidan qo‘llab-quvvatlanishi va nazorat qilinishini talab qiladi. Bu fakt Blokcheyn tizimining barqarorligi va ishonchliligining asosini tashkil etadi.

Blokcheyn tizimining halol tugunlari tomonidan butun tizim hisoblash manbalarining ko‘piga egalik qilib turar ekan, ular qo‘llab-quvvatlaydigan yo‘l maksimal tezlikda o‘sib boradi va barcha raqobatdosh yo‘llarni quvib o‘tadi. Biror ichki blokni boshqarish, ya’ni manipulyatsiya qilish imkoniyatini olish uchun, tajovuzkor albatta ushbu blokni reyestrga qo‘shilishi uchun avval amalga oshirilgan barcha amallarni takroran amalga oshirishi va keyingi barcha bloklar uchun xesh-jumboqlarni ketma-ket yechishi, so‘ngra halol tugunlar tomonidan qo‘llab-quvvatlanayotgan yo‘lni tutib olishi va ular ustidan nazorat o‘rnatishi kerak bo‘ladi.

Ko‘pchilik halol tugunlar qo‘llab-quvvatlaydigan yo‘l firibgarlik tranzaksiyalarini o‘z ichiga olgan yangi “rasmiy” yo‘lni o‘rnatishga bo‘lgan har qanday urinishdan ilgarilab ketadi va uni istisno qiladi. Shuning uchun tizim tomonidan xizmat ko‘rsatiladigan tranzaksiyalar xronologiyasi begona tomonning manipulyatsiyasiga qarshi barqaror hisoblanadi.

4- bob yuzasidan nazorat savollari

1. Blokcheyn tizimlarida axborotni shifrlashning maqsadi va vazifalari nimadan iborat?
2. Axborotni shifrlashning to‘liq sikli qanday bosqichlardan iborat?
3. Simmetrik va asimmetrik shifrlash deganda nimani tushunasiz?
4. Ochiq va yopiq kalitlarning vazifalari qanday?
5. Elektron raqamli imzo nima va u Blokcheyn tizimlarida qanday rol o‘ynaydi?
6. Asimmetrik kriptografiyadan foydalanish ketma-ketligi qanday?
7. Blokcheyn tizimlarida birinchi tranzaksiyani hosil qilish uchun harakatlar ketma-ketligi qanday?
8. Tranzaksiyani tekshirish uchun Blokcheyn tizimi ishtirokchilari qanday amallarni bajarishlari zarur?
9. Blokcheyn tizimlarida Elektron raqamli imzodan karrali foydalanish nimani anglatadi?

10. Blokcheyn tizimlarning yangi qabul qilingan tranzaksiya bloklarini qabul qilish va ishlov berish jarayoni necha bosqichdan iborat?
11. Blokcheyn tizimlarida yangi tranzaksiya bloklarini yaratish qanday bosqichlardan iborat?
12. Xesh-jumboq nima va uning aniqlash algoritmi qanday?
13. Blokcheyn tizimlarida tranzaksiya xronologiyasining o‘rni qanday?
14. Tranzaksiya xronologiyasini tekshirish algoritmi qanday?

5-BOB. BLOKCHEYN TEXNOLOGIYASI ELEMENTLARINI AMALIYOTGA JORIY ETISH (BOJXONA VA SOLIQ IDORALARI MISOLIDA)

5.1. Bojxona idoralari axborot tizimlari va ularda Blokcheyn tizimlaridan foydalanishning huquqiy asoslari

O‘zbekiston Respublikasi Prezidenti Sh. Mirziyoyev 2019-yil yakunlari va kelgusi taraqqiyot strategiyasi to‘g‘risida Oliy majlisga murojaatida “Taraqqiyotga erishish uchun raqamli bilimlar va zamonaviy axborot texnologiyalarini egallashimiz zarur va shart. Bu bizga yuksalishning eng qisqa yo‘lidan borish imkoniyatini beradi”,- deb ko‘rsatib o‘tdi [1].

Mazur murojaatda belgilab berilgan vazifalar ijrosini ta’minlash maqsadida 2020-yil 5-oktyabr kuni tasdiqlangan “Raqamli O‘zbekiston — 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi PF-6079-son Prezident Farmoni bilan Respublikada raqamli industriyani jadal rivojlantirish, milliy iqtisodiyot tarmoqlarining raqobatbardoshligini oshirish maqsadida “Raqamli O‘zbekiston - 2030” strategiyasi tasdiqlandi [2].

Strategiyaning “2.4. Raqamli texnologiyalar milliy bozorini rivojlantirishning ustuvor yo‘nalishlari” bobida “*IT-park asosida ilg‘or texnologiyalardan (Big Data, IoT, AI blokcheyn va boshqalar) foydalangan holda ustuvor tarmoqlar uchun “aqlli yechimlar” ni ishlab chiqishni rag‘batlantirish*” vazifasi belgilab berildi.

Shuningdek, mazkur farmon bilan tasdiqlangan “Yo‘l xaritasida” bojxona idoralari faoliyatini raqamlashtirish va bir qator axborot tizimlarini amaliyotga joriy etish vazifalari qo‘yildi.

Bundan tashqari, O‘zbekiston Respublikasi Prezidentining “Bojxona ma’muriyatchiligini isloh etish va O‘zbekiston Respublikasi davlat bojxona xizmati organlari faoliyatini takomillashtirish to‘g‘risida” 2020-yil 5-iyundagi 6005-son farmoni e’lon qilindi. Mazkur farmon bilan bojxona ma’muriyatchiligini isloh etish, bojxona organlari faoliyatini yana-da takomillashtirish hamda samaradorligini oshirish, “qog‘ozsiz va elektron bojxona”ning mantiqiy davomi va rivojlanishi bo‘lgan “raqamli bojxona”ni shakllantirish asosiy vazifa etib belgilab berildi [3].

Prezident farmonining birinchi ilovasi bilan tasdiqlangan 2020 - 2023-yillarda bojxona ma’muriyatchiligini isloh qilish va O‘zbekiston Respublikasi davlat bojxona xizmati organlari faoliyati samaradorligini oshirish Konsepsiyasida bojxona organlari faoliyatini rivojlantirishning ustuvor yo‘nalishlaridan biri sifatida “Raqamli iqtisodiyot doirasida zamonaviy va ilg‘or axborot-kommunikatsiya texnologiyalarini bojxona sohasiga joriy etish orqali bojxona organlari faoliyati shaffofligi hamda samaradorligini ta’minlash” belgilangan.

Bunda tadbirkorlik subyektlariga qulayliklar yaratish maqsadida quyidagi funksiyalarni o‘zida mujassam etgan avtomatlashtirilgan bojxona axborot tizimlarini amaliyotga joriy etish lozim bo‘ladi:

- tashqi iqtisodiy faoliyat ishtirokchisi olib kirilayotgan tovarlar bo‘yicha moliyaviy kafolatni ta’minlanishi;
- tovarlarni olib chiqishning asosiy sharti bo‘lib, tashqi iqtisodiy faoliyat ishtirokchisini tovarlarni buxgalterlik hisobiga qo‘yishi, bojxona to‘lovlarini to‘g‘ri hisoblanganligi hamda to‘langanligi tasdiqlash majburiyati;
- mazkur tizimni soliq organlari tizimlari bilan integratsiyalanganligi.

Yuqorida keltirib o‘tilgan normativ hujjatlar bojxona idoralari axborot tizimlari va ularda Blokcheyn tizimlaridan foydalanishning huquqiy asoslarini belgilab beradi.

Bojxona organlariga axborot-kommunikatsiya texnologiyalarini joriy etish mamlakatimiz miqyosida qabul qilinayotgan qonun va normativ-huquqiy hujjatlar talablariga mos bo‘lish bilan bir qatorda, u barcha xalqaro me’yorlarni ham saqlashga va ijrosini ta’minlashga qaratilgan.

Xususan, 2006-yildan boshlab Butunjahon bojxona tashkiloti (BBT) tomonidan “KOLUMB” dasturini tatbiq etish bo‘yicha ishlar olib borilmoqda. Ushbu dasturning mohiyati BBT a’zosi bo‘lgan davlatlar bojxona xizmatiga yordam berish, “Jahonda savdoni yengillashtirish va xavfsizlik standartlari” (Frameworks of standarts to secure and facilitate global trade yoki “Xavfsizlik standartlari”) hujjatining talablarini tatbiq etishdan iborat [6]. «Xavfsizlik standartlari” XXI asr boshida Rossiya Federatsiyasi, AQSH, Saudiya Arabistoni, Turkiya va boshqa davlatlarda sodir bo‘lgan terroristik harakatlarga javob tariqasida ishlab chiqilgan bo‘lib, 2005-yil 23-iyun kuni Bryussel shahrida bo‘lib o‘tgan BBT ning navbatdagi sessiyasida

166 ta davlat bojxona xizmatlari rahbarlari tomonidan imzo chekilib, qabul qilingan edi.

Hujjat xalqaro jinoiy uyushmalarning tajovuzlari va boshqa tahdidlar oldida yaxshi himoyalanmagan xalqaro savdo–sotiqning xavfsizligini ta'minlash, uni yangi bosqichga ko'tarishga qaratilgan. Hujjatning 1.1 - bandida bojxona xizmatlarining terrorizmga qarshi kurashdagi roli quyidagicha belgilab berilgan:

"Xalqaro savdo iqtisodiy farovonlikning muhim, harakatga keltiruvchi kuchi hisoblanadi. Jahon savdo tizimi butun dunyo iqtisodiyotiga jiddiy zarar yetkazishi mumkin bo'lgan terror tajovuzlari oldida haligacha zaif va ojiz ahvolda qolmoqda. Bojxona ma'muriyatlari xalqaro yuklar oqimini nazorat qiluvchi va boshqaruvchi, yuk va tovarlarni tashish dunyo tizilmasi xavfsizligini ta'minlash hamda daromadlar yig'imi va savdoni yengillashtirish vositasida ijtimoiy - iqtisodiy taraqqiyotga ko'maklashish imkoniyatiga ega bo'lgan yagona davlat tashkilotidir".

Xavfsizlikni ta'minlash va xalqaro savdo–sotiqqa ko'maklashish – faqatgina BBT uchun emas, balki tashqi iqtisodiy faoliyatning barcha qatnashchilari uchun nihoyatda muhim bo'lgan mavzu hisoblanadi. Bunga erishish uchun turli davlatlar bojxona xizmatlarining o'zaro hamkorligi, boshqa davlat va huquqni muhofaza qiluvchi organlar hamda biznes uyushmalar bilan birdamlikda harakat qilish zarur bo'lmoqda. Shunday paytda turli davlatlar bojxona xizmatlarining bir–biri bilan, boshqa davlat va huquqni muhofaza qilish organlari hamda biznes uyushmalar bilan o'zaro hamkorlik qilishning asosiy vositasi sifatida axborot texnologiyalari o'rtaga chiqadi.

Jumladan, BBT «Xavfsizlik standartlari" hujjati 1.3–bandida uning to'rt asosiy elementlari quyidagicha belgilab berilgan:

"BBT Standartlari to'rt asosiy elementdan iborat.

Birinchidan, hududga kirayotgan, undan chiqayotgan va tranzit tarzda o'tayotgan yuk–tovarlar haqida oldindan elektron pochta orqali xabar berishga oid talablarni uyg'unlashtirishni nazarda tutadi.

Ikkinchidan, Asosiy Standartlarga qo'shilgan barcha mamlakatlar, xavfsizlik masalalarini hal qilish maqsadida, xavf–xatarlarni boshqarish majburiyatini o'z zimmalariga oladilar.

Uchinchidan, Asosiy Standartlar qabul qiluvchi tarafning, xavf-xatarlarni kuzatishning qiyosiy metodikasiga asoslangan so'roviga

muvofiq, jo'natuvchi mamlakat bojxona idorasidan yuqori xavf–xatarga ega bo'lgan konteyner va yuklarni eksport qilish chog'ida yirik formatdagi rentgen apparatlari va radiatsiya detektorlaridan foydalangan holda tekshirib chiqishlarini talab qiladi.

To'rtinchidan, Asosiy Standartlarda, bojxona xizmatlari yuk–tovarlar tashish xalqaro tuzilmasida xavfsizlikning minimal (eng kam) standartlariga rioya qilayotgan va ishda samarali uslublardan foydalanayotgan kompaniyalarga beradigan imtiyozlar aniqlab beriladi".

Ko'rinib turibdiki, «Xavfsizlik standartlari" ning to'rttadan uchta asosiy elementi bojxonada axborot–kommunikatsion texnologiyalarni qo'llash bilan bevosita bog'liqdir. Ya'ni:

- yuk qabul qiluvchi mamlakat bojxona xizmatiga import, eksport va tranzit yo'nalishidagi yuklar to'g'risida oldindan elektron axborot taqdim etish;
- xavfsizlikni ta'minlash maqsadida yuklarning xavf-xatarlarini boshqarish;
- katta formatli rentgen apparatlar va radiatsiya detektorlari kabi intruziv bo'lmagan apparatura yordamida konteyner va yuklarni tekshiruvdan o'tkazish.

"Xavfsizlik standartlari" me'yorlarining yuqoridagi qisqacha ko'chirmasi tahlili O'zbekiston Respublikasi bojxona xizmatida ham olib borilayotgan ishlar shu talablar doirasida, ular ijrosini ta'minlashga yo'naltirilganligini ko'rsatadi.

Shu munosabat bilan, raqamli iqtisodiyot, jumladan, bojxona organlariga tatbiq etilgan axborot-kommunikatsiya texnologiyalari asoslarini o'rganish va uni o'rganishga imkon beradigan o'quv qo'llanmalar yaratish bugungi kunda dolzarb masala bo'lib qolmoqda.

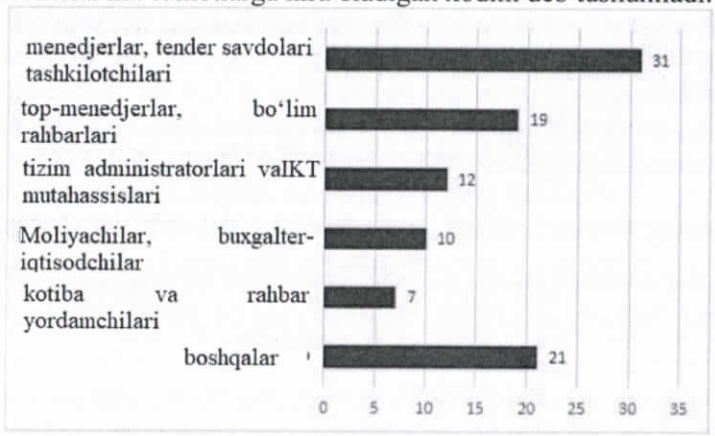
5.2. Bojxona idoralari axborot tizimlaridan foydalanuvchilar o'rtasida axborot almashish, elektron raqamli imzoni ikki karra qo'llash algoritmi

Bojxona organlari axborot tizimlaridan foydalanishga ruxsat berilgan "mijoz"lar haqida gap ketganda, ular umumiy holdagi, ya'ni nafaqat davlat organlari axborot tizimlari, balki barcha turdagi axborot tizimlaridan foydalanuvchilarning xususiy holi deb qaraladi.

Shu bilan birgalikda, bunday "mijoz"lar bilan ishlaganda axborot xavfsizligini ta'minlash masalasi xos jihatlariga ega hisoblanadi. Masalan, xususiy kompaniyalar axborot tizimlaridan foydalanuvchilarning axborot xavfsizligi talablariga rioya etmasliklari ushbu kompaniya biznes – rejalarining barbod bo'lishi yoki kompaniyaning bankrotlikka uchrashiga olib kelsa, davlat organlari axborot tizimlaridan foydalanishga ruxsat berilgan "mijoz"larning bunday xatti – harakatlari qonunchilikning qo'pol ravishda buzilishi, fuqarolar xavfsizligi va manfaatlari, davlat iqtisodiy xavfsizligi masalalariga zarar yetkazilishiga olib kelishi mumkin [19].

Axborot xavfsizligini ta'minlash talablariga rioya etmaydigan axborot tizimlaridan foydalanuvchilar faoliyatini o'rganish yuzasidan keng ko'lamli tadqiqotlar olib borilgan bo'lib, ilmiy adabiyotda ular "insayderlar" deb nomlanadi [12,15,19].

"Insayder" tushunchasi inglizcha termin bo'lib, turli manbalarda turli xil talqinlarga ega va u umumiy holda "keng jamoatchilik uchun yopiq bo'lgan axborotlarga ruxsati bo'lgan odamlarning biror guruhi a'zosi" degan ma'noni anglatadi [19]. Axborot xavfsizligi nuqtayi nazaridan esa "insayder" – biror korxonaning axborot tarmog'iga kirish uchun ruxsati bo'lgan hamda konfidensial ma'lumotlarga kira oladigan xodim deb tushuniladi.



5.1- rasm. Axborot xavfsizligiga tahdid soluvchi foydalanuvchilar ulushlari

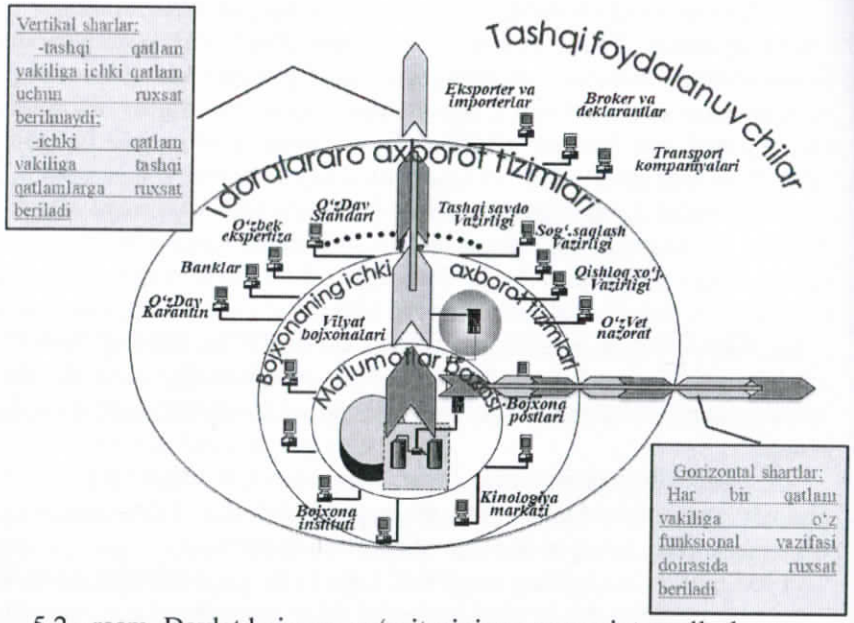
Insayderlar odatda 4 guruhga bo'linadi: "Itoatkor xodimlar", "Buzg'unchilar", "Jinoyatchilar", "Krot-sotqinlar" [15]. Rossiyaning SearchInform kompaniyasi o'tkazgan tadqiqotlarga qaraganda eng ko'p axborot o'g'rilari top – menendjerlar va o'rta bo'g'in rahbarlar ekanligi ma'lum bo'lgan (31%). Undan keyin esa yuqori bo'g'in rahbarlari turar ekan - 19% (5.1. – rasm) [12].

Axborot xavfsizligini ta'minlash talablariga rioya etmaydigan axborot tizimlaridan foydalanuvchilari - "insayderlar" qaysi guruhga kirishlaridan qat'iy nazar, ularni ajratib olish uchun zarur choralar ko'rilishi va ro'y berishi mumkin bo'lgan xavf oldi olingan bo'lishi lozim. Shu bilan birga bunday choralar axborot tizimlarining "halol" foydalanuvchilari uchun qiyinchiliklar paydo qilmasligi va oqibatda bunday tizimlarning samaradorligiga jiddiy putur yetkazilmasligi talab etiladi.

Ushbu holatni inobatga olgan holda axborot tizimlarini ishlab chiqish va joriy etishda axborotlar xavfsizligini ta'minlashning quyidagi ustivor jihatlari hisobga olinishi zarur bo'ladi:

- axborot tizimi foydalanuvchilari uchun real vaqt rejimida kerakli axborotlarni to'liq va qiyinchiliklarsiz olish imkoniyatining mavjud bo'lishi;
- axborotlarning yaxlitligi, ishonchliligi, aktualligi, tashqi ta'sirlardan himoyalanganligi va noqonuniy yo'l bilan kirib, o'zgartirib qo'yishdan himoyalanganligi [20];
- axborotlarning noqonuniy yo'l bilan kirib, ko'chirib oluvchilar ta'siridan himoyalanganligi.

Garchi axborot tizimlari foydalanuvchilari uchun ular tomonidan axborot xavfsizligi buzilishini oldini olishga imkon beruvchi kafolatli texnik yechimlar mavjud bo'lmasa ham, ma'lumotlar bazasini g'arazli maqsadda o'zgartirish yoki axborot o'g'irlanishining oldini olishga qaratilgan bir qator shartlarni o'rnatish mumkin.



5.2 - rasm. Davlat bojxona qo'mitasining yagona integrallashgan ma'lumotlar bazasi foydalanuvchilari uchun gorizontal va vertikal talablar

Davlat bojxona qo'mitasi yagona ma'lumotlar bazasi foydalanuvchilari barcha hududiy bojxona boshqarmalari va bojxona postlari xodimlari, shuningdek, boshqa vazirlik va idoralar vakillari, deklarantlar, tashqi savdo yuklarini tashuvchilar bo'lishi mumkin (5.2-rasm). Bunda ular "Tashqi foydalanuvchilar", "Idoralararo axborot tizimlari foydalanuvchilari", "Bojxona ichki axborot tizimlari foydalanuvchilari" hamda "Ma'lumotlar bazasi administratorlari" kabi huquq va imkoniyatlari turlicha bo'lgan foydalanuvchilar guruhlariga bo'linadi.

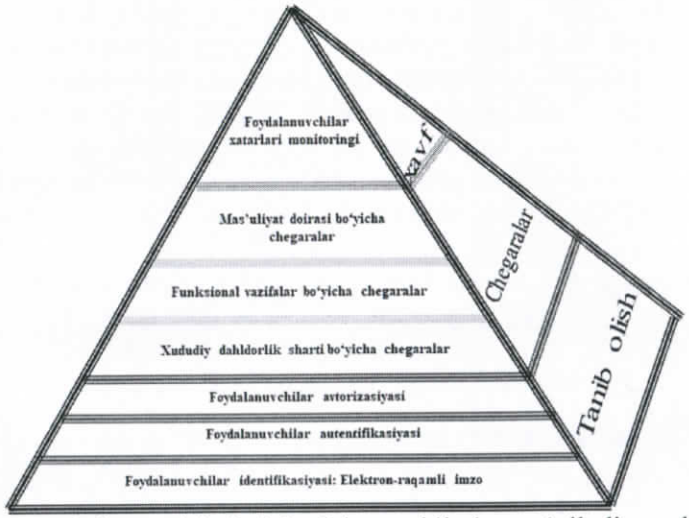
Bularning asosiylariga quyidagilar kiradi:

- foydalanuvchilar identifikatsiyasi: elektron-raqamli imzo;
- foydalanuvchilar autentifikatsiyasi;
- foydalanuvchilar avtorizatsiyasi;
- hududiy daxldorlik sharti bo'yicha chegaralash;
- funksional vazifalar bo'yicha chegaralash;
- mas'uliyat doirasi bo'yicha chegaralash;

- log jurnallar yuritish, foydalanuvchilar tomonidan ro'y bergan xatarlar monitoringi [7,14,16].

Mazkur shartlar o'z navbatida axborot tizimlari foydalanuvchilariga qo'yiladigan shartlar piramidasini tashkil etadi (5.3. – rasm). O'tkazilgan tadqiqotlar shuni ko'rsatadiki, axborot tizimlaridan foydalanuvchilar axborot xavfsizligini ta'minlashning eng bo'sh nuqtasi hisoblanib, ular uchun kafolatli natija beradigan texnik yechim mavjud emas.

Shu sababli, bu masalada asosan huquqiy-me'yoriy usullar qo'llaniladi. Xususan, O'zbekiston Respublikasining 2007-yil 25-dekabrdagi O'RQ-137 – son qonuniga muvofiq Jinoyat kodeksiga alohida "XX-1 bob. Axborot texnologiyalari sohasidagi jinoyatlar" kiritilgan bo'lib, unda axborot xavfsizligini buzish uchun ham tegishli moddalar ko'zda tutilgan [5].



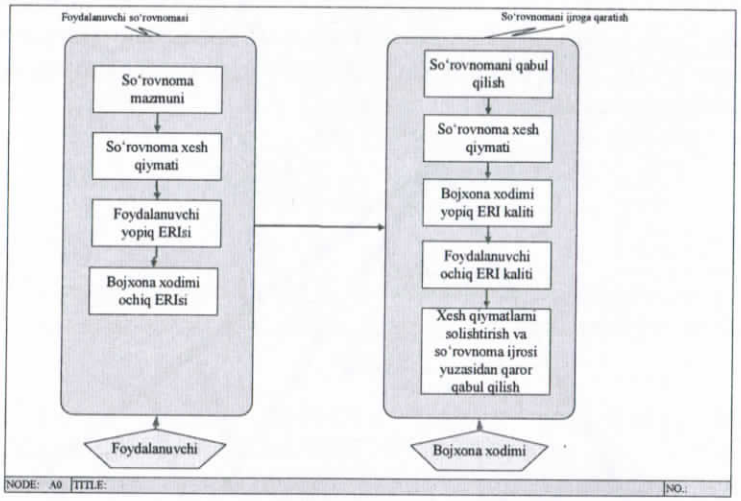
5.3 - rasm. Axborot tizimlari foydalanuvchilariga qo'yiladigan shartlar piramidasi

Axborot tizimlari foydalanuvchilariga qo'yiladigan shartlar piramidasi 7 qatlamdan iborat shartlarni o'z ichiga olib, bu shartlar quyidagi 3 guruhga bo'linadi:

- foydalanuvchi tanib olish va uning huquqlarini aniqlash;
- foydalanuvchiga qo'yilgan chegaralar ijrosini nazorat qilish;

- xavf guruhiga kiruvchi foydalanuvchilar uchun choralar.

Mazkur shartlar ichida 1-guruhga kiruvchi shartlar ijrosini mukammal ta'minlash uchun blokcheyn texnologiyasida qo'llaniladigan ERIni ikki karrali qo'llash algoritmini tatbiq etish kutilgan natijalar beradi. Bu algoritm ikki bloklan iborat bo'lib, birinchi blokda foydalanuvchi tomonidan axborot tizimiga yuboriladigan so'rovnomani shakllantirish amallari, ikkinchi blokda esa foydalanuvchi so'rovnomasini "tanib olish" va ijroga uchun qabul qilish amallari aks etgan (5.4.-rasm).



5.4.-rasm. ERIni ikki karrali qo'llash algoritmi

O'tkazilgan tajriba – sinovlari yuqorida bayon etilgan algoritm axborot tizimi foydalanuvchilari uchun qo'yiladigan cheklovlar samarali natijalar berishini ko'rsatmoqda. Jumladan, bu usulning Davlat bojxona qo'mitasi axborot tizimlarida qo'llanishi natijasida foydalanuvchining o'ziga tegishli bo'lmagan axborotlarni olishga urinishlari bartaraf etilib, boshqa xodimning ye-imzosidan foydalanish holatlarini aniqlash imkoniyatlaridan foydalanib kelinmoqda.

5.3. Bojxona va soliq idoralari o'rtasida axborot almashish, axborot ishonchliligini ta'minlashning ikki karra nazorati algoritmi

Davlat siyosati darajasida olib borilayotgan keng ko'lamli ishlar tufayli, bugungi kunda mamlakatimiz raqamli iqtisodiyot va axborotlashgan jamiyatga o'tish yo'nalishida ishonch bilan odimlamoqda, yaxshi rivojlangan infratuzilma va kadrlar salohiyatiga ega. Bugungi kunda vazirlik yoki idoralar darajasida axborotlashtirish emas, balki idoralararo axborot tizimlari va kommunikatsiyalarini yaratish hamda ularni xalqaro integratsiyalash vazifasi dolzarb masalaga aylandi.

Bunga misol sifatida 2018-yil 3-avgustda qabul qilingan O'zbekiston Respublikasi Vazirlar Mahkamasining "Berilgan bojxona imtiyozlaridan maqsadli foydalanilishini kameral nazorat qilish bo'yicha O'zbekiston Respublikasi Davlat soliq qo'mitasi va Davlat bojxona qo'mitasining o'zaro hamkorligi mexanizmi to'g'risidagi nizomni tasdiqlash haqida "gi 617-sonli qarorini [4]keltirish mumkin.

Mazkur Qaror bilan O'zbekiston Respublikasi Davlat soliq qo'mitasi va Davlat bojxona qo'mitasining o'zaro hamkorligi mexanizmi to'g'risidagi Nizom tasdiqlangan bo'lib, unda keltirilgan talablar barcha shunga o'xshash axborot tizimlari uchun deyarli bir xil hisoblanadi.

Jumladan, ushbu Nizomning 2-bobi: Davlat bojxona qo'mitasi tomonidan bojxona imtiyozlari berilgan soliq to'lovchilar to'g'risidagi ma'lumotlarni Davlat soliq qo'mitasiga taqdim qilish uchun quyidagi tartibni belgilaydi:

«6. Davlat bojxona qo'mitasi tomonidan bojxona imtiyozlari berilgan soliq to'lovchilar to'g'risidagi ma'lumotlar ushbu Nizomga 2-ilovaga muvofiq shakl bo'yicha Davlat soliq qo'mitasiga onlayn rejimda taqdim qiladi.

7. Bojxona imtiyozlari berilgan soliq to'lovchilar to'g'risida olingan ma'lumotlar ushbu ma'lumotlardan kameral nazorat qilish jarayonida foydalanish uchun Davlat soliq qo'mitasining yagona ma'lumotlar bazasiga avtomatik tarzda kiritiladi.».

Bundan ko'rinadiki, idoralararo ma'lumotlar almashinuvi, birinchi navbatda, real vaqt rejimida amalga oshirilishi kerak,

ikkinchidan, ma'lumotlar almashinuvi avtomatik tarzda yagona ma'lumotlar bazasiga kiritilishi kerak.

Ko'rib chiqilayotgan muammoning uch jihati bor:

- idoralararo axborot almashinuv tizimida elektron axborot almashinuvi real vaqt rejimida amalga oshirilishi kerak;
- uzatilgan ma'lumot ishonchli bo'lishi kerak, ya'ni obyektlar, hodisalar yoki jarayonlar ularning haqiqiy holatiga mos kelishi, ma'lumotlar amalda sodir bo'lganidan farq qilmasligi kerak;
- ma'lumot to'liq bo'lishi kerak, ya'ni, tavsiflanayotgan obyektning barcha parametrlarini o'z ichiga olgan bo'lishi kerak;
- qabul qilingan ma'lumotlar axborot almashinuvi ishtirokchilarining yagona ma'lumotlar bazasiga avtomatik ravishda, insonga bog'liq bo'lmagan holda, quyilishi lozim.

Belgilangan vazifalar ijrosini ta'minlovchi idoralararo axborot almashuvni ta'minlashning ikki karrali nazorat algoritmi quyidagidan iborat.

Ikkita subyekt: **A** va **B** subyektlarning axborot almashuv tizimini ko'rib chiqaylik. **A** subyektining ma'lumotlar bazasi on-layn tartibda shakllanib boradi deb shart qo'yiladi va axborot almashuv natijalariga asosan, **B** subyektining ma'lumotlar bazasida **A** subyektdan kelgan ma'lumotlar OLAP-kub shaklida yig'ilib boradi. (OLAP - On-Line Analytical Processing).

Elektron ma'lumotlar ishonchliligi va to'liqligini nazorat qilinishining maqsadi ushbu hujjatlardagi ma'lumotlar normativ-huquqiy hujjatlarda belgilangan talablarga, shuningdek hujjatlarni to'ldirish tartibi va ulardagi shakllardagi talablarga javob berishini ta'minlashdan iborat.

Elektron ma'lumotlar bir necha bosqichda nazorat qilinadi:

- tarkibiy nazorat;
- format nazorati;
- mantiqiy nazorat.

Tarkibiy nazorat bosqichida ma'lum elektron hujjatning sintaktik tarkibini belgilovchi *XSD-sxemalari* reglamentiga muvofiqligini tekshiriladi *(XSD - XML schema definition - XML hujjatning tarkibini tasvirlash uchun foydalaniladigan maxsus til)* [21]. Dastlab xabarning umumiy tarkibi, so'ngra uning sarlavha qismi tarkibi tekshiriladi. Shundan keyin hujjatga ichki joylashgan elektron hujjatlar tarkibi texnik topshiriq bilan belgilangan talablarga muvofiqligi tekshiriladi.

Format nazorati bosqichida O'zbekiston Respublikasining me'yoriy-huquqiy hujjatlari orqali belgilangan tartibda ma'lumotlar maydonlari to'ldirishning to'g'riligi tekshiriladi.

Mantiqiy nazorat bosqichida ma'lumotlar mavjud tasniflagichlar va ma'lumotnomalarga mosligi, shuningdek elektron ma'lumotlar maydonlarining o'zaro mosligi va muvofiqligi tekshiriladi.

Amalga oshirilgan nazorat-tekshiruvlar natijalariga ko'ra, agar xatoliklar mavjud bo'lsa, aniqlangan xatoliklar har biri o'z kodi, manbasi va ta'rifi ko'rsatilgan holda elektron xabarnoma shakllantiriladi. Shakllantirilgan xabarnoma dastlabki xabarni yuborgan axborot tizimiga yo'naltiriladi.

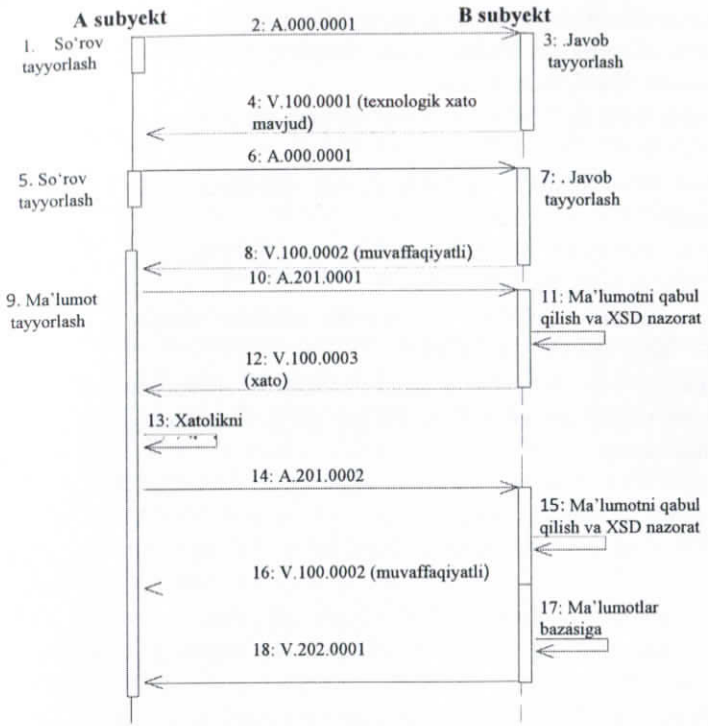
Idoralararo axborot almashuv tizimida har bir tranzaksiya tashabbuskori axborot uzatuvchi tomon hisoblanadi. Subyektlar o'rtasida axborot almashuv jarayoni quyidagi tartibda amalga oshiriladi (5.5.-rasm):

1. **A** subyekti tomonidan **B** subyekt tizimiga uning ishchi =olatini tekshirish uchun A000.0001 kodli elektron xabarni yuboradi.
2. Tizimning uning ishchi holatini tekshirish to'g'risidagi xabarni olgandan so'ng, **B** subyekt axborotni qabul qilishga tayyorligi (B.100.0002) yoki tizimning texnologik xatosi (B.100.0001) mavjudligi to'g'risida mos ravishda **A** subyektga javob xabari yuboradi.
3. Agar **B** subyekt ma'lumotlarni qabul qilishga tayyor bo'lsa, **A** subyekt o'z ma'lumotlar bazasida yangi hosil bo'lgan A.201.0001 kodli elektron xabarni **B** subyektga yuboradi. Agar tizimning texnologik xatosi mavjud bo'lsa, **A** subyekt ushbu operatsiyani 1-qadamdan boshlab takrorlaydi.
4. **A** subyektning ma'lumotlar bazasida yangi paydo bo'lgan ma'lumotlar haqida elektron xabarni olganidan so'ng, **B** subyekt ushbu A201.0001 kodli elektron xabarni qabul qiladi va XSD nazoratdan o'tkazadi. Har bir idoralararo axborot almashish tizimi uchun umumiy *XSD-sxemalari* reglamenti hamda almashinuvchi ma'lumotlar bazasi xususiyatlaridan kelib chiqib, alohida talablar texnik topshiriqda batafsil bayon etilgan bo'lishi lozim.
5. Agar tekshiruv natijasida A201.0001kodli elektron xabar xatosiz deb topilsa, u holda **B** subyekt ma'lumotlarni muvaffaqiyatli qabul qilinganligi to'g'risida **A** subyektga xabar yuboradi.

Bunday holda, **B** subyekt A201.0001kodli elektron xabar elementlarini o‘z ma’lumotlar bazasiga mos ravishda qabul qiladi va o‘z ma’lumotlar bazasida yangi paydo bo‘lgan ma’lumotlarning identifikatsiya raqami to‘g‘risida B.202.0001 raqamli elektron xabarni **A** subyektga yuboradi.

6. Tekshiruv natijalari to‘g‘risidagi axborot noto‘g‘ri deb topilgan hollarda, **B** subyekt xabarning tizimli va mantiqiy nazoratiga oid xatoliklarni o‘z ichiga olgan B.100.0003 kodli xabarni **A** subyektga yuboradi.

7. Agar B.100.0003 kodli elektron xabar kelib tushsa, u holda A201.0001 kodli elektron xabar **B** subyektga yuborilmagan hisoblanadi. Bunday holda **A** subyekt B.100.0003 kodli elektron xabar elementlari qiymatlariga mos keladigan xatoliklarni bartaraf etishi va algoritm operatsilarini 3-banddan boshlab takrorlashi lozim bo‘ladi.



5.5.-rasm. Idoralararo axborot almashuv tizimlarida axborotning kafolatlangan ishonchliligini ta’minlash ikki karrali nazorat algoritmi diagrammasi

Xulosa sifatida ta’kidlash joizki, idoralararo axborot almashish tizimlarida axborot ishonchliligini kafolatli ta’minlash uchun yuqorida keltirilgan algoritm ma’lumotlarni ikki karrali nazorat qilish imkonini beradi. Ushbu algoritm ma’lumotlarning nafaqat muvaffaqiyatli qabul qilinishini ta’minlaydi, balki olingan ma’lumotlar kafolatlanganligini tasdiqlash imkonini beradi, ya’ni ma’lumotlar bazasining har bir qabul qilingan yangi elementi uchun reyestrdagi identifikatsiya raqami bilan kafolatlaydi.

Ushbu algoritm Davlat bojxona qo‘mitasi hamda Davlat soliq qo‘mitalari o‘rtasida axborot almashuvini tashkil qilishda qo‘llanilgan bo‘lib, o‘z ijobiy natijalarini berib kelmoqda.

5 - bob yuzasidan nazorat savollari

1. Bojxona idoralarida blokcheyn - tizimlaridan foydalanishning huquqiy asoslari nimalardan iborat?
2. "Insayder"larning axborot xavfsizligini ta'minlashga tahdidi qanday?
3. Axborot xavfsizligini ta'minlashning gorizontal va vertikal talablari qanday?
4. Axborot tizimlari foydalanuvchilariga qo'yiladigan shartlar piramidasi qanday qatlamlardan iborat?
5. Bojxona idoralari axborot tizimlarida elektron raqamli imzoni ikki karra qo'llash algoritmi qanday?
6. Bojxona va soliq idoralari o'rtasida axborot almashish, axborot ishonchliligini ta'minlashning ikki karrali nazorat algoritmi qanday bosqichlardan iborat?

Blokcheyn tizim usullaridan amaliyotda foydalanish haqida xulosalar

Bu yerda so'zni, shubhasiz, so'ngi yillarda erishilgan eng yaxshi yutuqlardan biri bu Blokcheyn tizimlari texnologiyasi ekanligini ta'kidlashdan boshlash lozim. Hech ajablanarli joyi yo'qki, ba'zi uning muxlislari blokcheynni Internet paydo bo'lganidan buyon paydo bo'lgan eng katta ixtiro deb e'lon qilishmoqda.

Ayniqsa, Internet butun axborot makonini butunlay qamrab olgandan so'ng, uning foydalanuvchilarida axborot ishonchliligini ta'minlash masalasiga keskin zarurat tug'ilmoqda. So'nggi paytlarda Internet nafaqat foydalanuvchilar darajasida, balki ba'zi davlat va hattoki xalqaro miqyosda ham eng "nafis, ilmiy asoslangan" va isbotlab bo'lmaydigan firibgarlik sxemalarini amalga oshirish vositasiga aylanib qolmoqda. Bugun haqiqiy dalillarga "o'ralgan" yolg'on axborotni taqdim etish usuli jadal qo'llanilmoqda. Internetdan olingan axborot ishonchliligini aniqlash uchun juda katta kuch va mablag'lar sarflanmoqda.

Bundan tashqari, Internet va boshqa yondosh texnologiyalar barcha rivojlangan mamlakatlarning maxsus xizmatlari uchun asosiy ma'lumot manbaiga aylandi. Natijada, Internet xizmatlari, ijtimoiy tarmoqlar va boshqa yondosh texnologiyalar bo'yicha, shu jumladan rivojlangan mamlakatlarning maxsus xizmatlariga ajratilgan moliyaviy manbalar hisobidan xizmat ko'rsatadigan odamlar dunyodagi eng boy odamlar bo'lib qolmoqdalar. Bugun hech kimga sir emaski, Internet texnologiyalaridan foydalanish foydalanuvchilar shaxsiy ma'lumotlarining ishonchliligi yoki maxfiyligini kafolatlay olmaydi.

Ushbu sharoitda Blokcheyn tizimlari texnologiyasi nafaqat bugungi kunda, balki yaqin kelajakda ham eng istiqbolli texnologiyalardan biri bo'lib qolaverish ehtimoli katta.

Tabiiyki, biz yuqorida bergan bunday qisqa sharh bilan Blokcheyn tizimlari texnologiyasining imkoniyatlarini har tomonlama namoyish etish va ochib berish mumkin emas. Shunga qaramay, ushbu texnologiyaning afzalliklari bilan bir qatorda, ayrim bu sohani rivojlantirish zarurligini ko'rsatuvchi fikrlarni ham ta'kidlash mumkin.

1. Birinchidan, bu sohadagi deyarli barcha tadqiqotlarning mualliflari Blokcheyn tizimlari axborot ishonchliligini to‘liq kafolatlaydigan texnologiya emasligini bir ovozdan takrorlaydilar. Gap shundaki, agar avval boshdan ishonchli bo‘lmagan tranzaksiya tuzilgan bo‘lsa va bir qatlamli tarmoq ishtirokchilarining 50% dan ko‘prog‘i unga ixtiyoriy yoki beixtiyor ravishda ovoz bergan bo‘lsa, demak, ushbu blok Blokcheyn tizimining ommaviy reyestriga qabul qilinishi mumkin. Ushbu muammoni ba’zan “51% hujumlar” deb nomlashadi. Boshqacha qilib aytganda, agar bir guruh tarmoq ishtirokchilari hisoblash quvvatining 51 foizini o‘z qo‘llariga jamlasa, faqat o‘zi uchun foydali bo‘lgan operatsiyalarni tasdiqlab, o‘z manfaati uchun harakat qila olishlari mumkin.

2. Bundan tashqari, ular blokcheyn texnologiyasining afzalliklari haqida gapirganda ta’kidlaydilarki, mulkka egalik huquqini o‘tkazishda vositachilarsiz to‘g‘ridan-to‘g‘ri beruvchi va oluvchi o‘rtasida amalga oshirish blokcheyn texnologiyasining asosiy afzalliklaridan biri. Bunday holda, kadastr xizmatlari, banklar va boshqa vakolatli vakilliklarni esa ishlab chiqaruvchilar va iste’molchilar o‘rtasida oddiy vositachi deb baholaydilar.

Ammo, masalan, Blokcheyn tizimining ishtirokchisi, agar u bunday xuquqga ega bo‘lmay turib, ko‘chmas mulkka egalik huquqini boshqaga o‘tkazish bo‘yicha tranzaksiyalarni reyestrga qo‘shsa nima bo‘ladi? Bunday holda, mulkka egalik huquqini boshqa shaxsga o‘tkazish imkoniyati uning boshqa mulkdordan mulkka egalik qilish huquqini olganiga bog‘liq. Aks holda, kadastr xizmatlari ushbu obyekt egalari reyestrida bunday huquq yo‘qligi sababli bunday operatsiyani taqiqlaydi.

Ko‘rib chiqilayotgan vaziyatning muhim xususiyati shundan iboratki, Blokcheyn tizimining ishtirokchilari tomonidan muomalaga kiritiladigan mulk huquqini boshqa shaxslarga o‘tkazish bo‘yicha yangi tranzaksiyalarni yaratishda tranzaksiyalarning ishonchliligini ta’minlash uchun axborotni kafolatli ishonchliligini tasdiqlovchi muayyan instansiya talab qilinadi.

3. Ehtiyotkorlik bilan yondashuvni talab qiladigan Blokcheyn tizimlari texnologiyasining navbatdagi elementi tranzaksiyalarni ro‘yxatdan o‘tkazishda foydalanuvchilarni aniqlashdir. Foydalanuvchilarning bir qiymatli identifikatsiyasi, odatda, parol, kalit, ERI yoki foydalanuvchilarning boshqa identifikatsiyalash

vositalari xesh-qiymatiga asoslanadi. Lekin biz yuqorida aytib o‘tganimizdek, nazariy jihatdan, xesh-qiymat kolliziyasi muammosi hali to‘liq hal qilinmagan.

4. Blokcheyn tizimlari texnologiyasining yana bir muhim kamchiliklaridan biri bu “ishlov berishning muayyan bosqichlaridan o‘tgan tranzaksiyalarga o‘zgartirish kiritish imkoniyatining yo‘qligi” deb nomlanadi. Ya’ni, agar o‘tgan tranzaksiyalarda keyinchalik xato topilsa, bu yuridik ahamiyatga ega barcha harakatlar ketma-ketligini bekor qilishga olib keladi. Muammoni barcha tomonlarning oldindan roziligi bilan va yangi tranzaksiyani kiritish va ehtimol eski tranzaksiyani bekor qilish orqali yechish mumkin bo‘ladi xolos. Bu, o‘z navbatida, Blokcheyn tizimlari texnologiyasining muhim afzalliklaridan biri - mulkiy huquqlarni topshirish amallari vaqtini sezilarli darajada qisqartirishni ta’minlaydi degan afzallikka soya soladi.

5. Blokcheyn tizimlari texnologiyasini takomillashtirishni talab qiladigan ba’zi texnik jihatlar mavjud. Masalan, bugungi kunda u har bir tranzaksiyaga ishlov berish paytida juda katta texnik yuklama paydo bo‘lishi tufayli, tizim qisqa vaqt ichida juda ko‘p miqdordagi tranzaksiyalarni taqdim eta olmaydi. Bundan tashqari, tarmoq kompyuterlarida saqlanadigan tranzaksiyalar ma’lumotlar bazasi har kuni ortib boradi. Doimiy yuklama bilan ishlaydigan tarmoqlar haqida gap ketganda, elektr tarmog‘idagi yuklama haqida ham unutmaslik kerak. Ushbu murakkab hisob-kitoblar kompyuterlarni juda ko‘p energiya sarflashga majbur qiladi.

Blokcheyn tizimlari bobidagi fikrlarimizni yakunlashdan avval, ilmiy tadqiqotlarni sharhlovchilar odatda doimo takrorlaydigan bir fikrni takrorlashni xohlaymiz: yuqorida keltirilgan ayrim muammolar va kamchiliklar Blokcheyn tizimlari texnologiyasining ahamiyatini hech qanday tarzda kamaytirmaydi. U butun global axborot makonini egallashga kun sayin, soat sayin o‘z qamrovini oshirib, o‘ziga yo‘l ochib bormoqda. Yuqorida keltirilgan muammolarni bartaraf etish uchun esa ming-minglab mutaxassislar tinimsiz va ijodiy ishlamoqdalar.

MUSTAQIL ISHLASH UCHUN MAVZULAR

Blokcheyn texnologiyasi asosida ishlovchi "Electrum hamyon" tizimi bilan ishlash

Blokcheyn texnologiyalari to'g'risidagi adabiyotlar, ayniqsa Internet materiallari ichida asosiy o'rinni "Kriptovalyuta", "Bitkoin", "Mayning" tushunchalari egallab olgan. Yuqorida, Blokcheyn texnologiyalari asoslarini o'rganish jarayonida ko'rdikki, bu fikr judayam to'g'ri emas ekan. Ya'ni, Blokcheyn texnologiyalari birqatlamli tarmoqlarda ishonchli axborot almashishning noyob usuli bo'lib, mulkni xavfsiz boshqarish jumladan, valyuta operatsiyalari, turli xildagi to'lovlarni amalga oshirishda ham foydalanish mumkin.

Shu sababli, kriptovalyuta operatsiyalari bilan ishlovchi Blokcheyn texnologiyasining yorqin misoli sifatida "Electrum hamyon" tizimini o'rganish muayyan malakalarni hosil qilishga yordam beradi.

Quyida "Electrum hamyon" tizimini o'rganish jarayonida bir qator savollarga javob topamiz. Jumladan:

1. Kriptovalyuta hamyoni nima?
1.1. Sovuq hamyonlar
1.2. Issiq hamyonlar
2. "Electrum hamyon" nima?
3. "Electrum hamyon" qanchalik yaxshi?
3.1. "Electrum hamyon"ning afzalliklari va kamchiliklari
3.2. "Electrum hamyon"ning Xavfsizligi haqida umumiy ma'lumot
4. "Electrum hamyon" ni qanday o'rnatish kerak
5. "Electrum hamyon" dan qanday foydalanish kerak
5.1. "Bitkoin" olish
5.2. "Bitkoin" yuborish
6. Xulosa

1. Kriptovalyuta hamyon

"Electrum hamyon" tizimiga o'tishdan oldin, umuman kriptovalyuta hamyonlari haqida qisqacha ma'lumot berib o'tish maqsadga muvofiq hisoblanadi.

Kriptovalyuta hamyoni - bu tasodifiy juft kriptografik kalitlarni yaratadigan dastur. Ushbu kalitlar "Bitkoin"ni (va boshqa har qanday

kriptovalyutani) bir kishidan boshqasiga yuborish yoki qabul qilish uchun ishlatiladi. Albatta, "hamyon" so'zi odamni chalg'itishi mumkin. Bu yonimizda yuradigan hamyondan farqli o'laroq, kriptovalyuta hamyoni hech qanday kriptovalyutani o'z ichida saqlamaydi. U shunchaki o'zi uchun yaratilgan ma'lum bir kriptovalyutaning blokcheyni bilan aloqa qilish uchun xizmat qiladi.

Bugungi kunda amaliyotda bir nechta kriptovalyuta hamyonlari mavjud. Ba'zilarida faqat bitta turdagi kriptovalyuta mavjud, boshqalari esa bir necha turdagi kriptovalyutani qo'llab-quvvatlashi mumkin. Ularning ayrimlari yaxshi xavfsizlik tizimiga ega, boshqalari esa unchalik ishonchli emas.

"Electrum hamyon" tizimini o'rganishdan oldin, bu to'g'rida to'liqroq ma'lumotga ega bo'lish uchun har xil turdagi hamyonlarni ko'rib chiqaylik.

1.1. Sovuq kriptohamyonlar

Kriptovalyutani saqlash uchun eng xavfsiz variant deb "sovuq hamyonlar" deb tan olinadi. Ular kriptovalyutani uzoq muddatli saqlash uchun qulay va juda yaxshi. Bu hamyonlarning ikki turi mavjud: *qog'oz hamyonlar va apparat hamyonlari*.

Qog'oz hamyonlar. Qog'oz hamyonlar, ularni yaratish jarayoni to'g'ri ijro etilgan taqdirda, eng yuqori himoya darajasini ta'minlaydi.Biroq, bu jarayon unchalik oddiy emas va biroz e'tibor va sa'y-harakatlar talab qiladi. Bunday hamyonlar tekin, ammo sozlash va ulardan foydalanishning murakkabligi sababli, ular kriptovalyuta dunyosida yangi bo'lganlar uchun tavsiya etilmaydi.

Ma'lumki, barcha qog'oz hamyonlar kriptografik kalitlarni chop etish va ularni oflayn rejimda saqlashga imkon beradi. Bunda foydalanuvchi o'sha qog'ozning o'zini xavfsizligi to'g'risida g'amxo'rlik qilishi zarur xolos. Agar kimdir qog'ozdagi kalitlarni ko'rib qolsa, u hamyonga muammosiz kira oladi.

Apparat hamyonlari. Apparat hamyonlari - bu kriptovalyutani uzoq muddatli saqlash uchun xavfsiz hamyon va qog'oz hamyondan ancha qulay. Bunday hamyonlarga misol qilib Ledger Nano S va Trezor moslamalarini keltirish mumkin.

Ular xavfsizlik va qulaylik o'rtasidagi yechimni taqdim etadi. Ammo ular tekin emas va nisbatan ancha qimmat. Shu sababli,

foydalanuvchi o‘zida mavjud bo‘lgan kriptovalyuta miqdori apparat hamyonini sotib olishga arziydimi yoki yo‘qligini o‘ylab ko‘rishi kerak bo‘ladi.

1.2. Issiq hamyonlar

Odatda “issiq hamyon”lar “sovuq hamyon”lardan ko‘ra xavfsizligi pastroq deb hisoblanadi. Biroq, ular ham ancha mashhur. Issiq hamyon kriptovalyutadan kundalik foydalanish uchun ideal vosita hisoblanadi.

Tushunish soddaroq bo‘lishi uchun “issiq hamyon”ni kundalik hamyon sifatida tasavvur etish kifoya. Chunki kishining barcha valyuta qimmatliklari solingan hamyonni shahar bo‘ylab ko‘tarib yurishi judayam aqlli qaror hisoblanmaydi. Balki, faqat zarur bo‘lgan miqdordagi mablag‘largina olib yuriladi.

Shu ma’noda qaraganda, “issiq hamyon”lar judayam xavfsiz emas. Ammo shunga qaramay, o‘zingizga biror narsa sotib olish uchun qo‘lingizda ozgina pul bo‘lishi maqsadga muvofiq bo‘ladi. Buning uchun “issiq kriptovalyuta hamyonlari” juda zarur.

“Issiq hamyon”larning ikkita asosiy turi mavjud: *onlayn hamyonlar va dasturiy ta’minot hamyonlari.*

Onlayn hamyonlar. Onlayn hamyonlar kriptovalyuta saqlash uchun har doim ham qulay bo‘lavermaydi. Biroq, ularning ham o‘ziga munosib tatbig‘i mavjud. Ular ko‘pincha birjalarda yoki kriptovalyutadan foydalanadigan boshqa onlayn xizmatlarda qo‘llaniladi. Bunda har qanday xizmat uchun to‘lovni amalga oshirish yoki ushbu hamyonga osongina pul o‘tkazish mumkin.

Biroq, kriptovalyutalarni uzoq vaqt davomida bunday hamyonlarda saqlash tavsiya etilmaydi. Chunki bu hamyonlar deyarli har doim xizmat ko‘rsatuvchi provayder nazorati ostida bo‘ladi. Shuni unutmaslik kerakki, agar kimdir sizning shaxsiy kalitlaringizga kirish huquqiga ega bo‘lsa, demak u sizning kriptovalyutangizga ham kirish huquqiga ega. Masalan, agar sizning kriptovalyutangiz Bittrex birjasida saqlangan bo‘lsa va u bir muncha vaqt o‘z faoliyatini to‘xtatsa, siz kriptovalyutangizdan foydalana olasizmi? Menimcha – yo‘q.

Dasturiy hamyonlar. Va nihoyat biz asosiy maqsadimiz bo‘lgan dasturiy hamyonlarni o‘rganishga yetib keldik. “Electrum hamyon” - bu dasturiy hamyon hisoblanadi.

Ma’lumki har qanday hamyonda xavfsizlik va qulaylik ma’lum ma’noda qarama-qarshi qiymatlarga ega. Ya’ni agar hamyon o‘ta qulay bo‘lsa, uning xavfsizlik darajasi yetarli bo‘lmaydi. Va aksincha, hamyonning xavfsizligi yetarli darajada bo‘lsa, u foydalanish uchun ancha noqulay bo‘ladi.

Dasturiy hamyonlar ham Apparat hamyonlar kabi xavfsizlik va qulaylik o‘rtasidagi muqobil yechimni ta’minlaydi. Dasturiy hamyonlar Apparat hamyonlar kabi xavfsiz bo‘lmasa ham, ular qulayroq va tekin. Apparat hamyonlar esa, yuqorida ko‘rib o‘tdikki, ancha qimmat turadi. Ushbu xususiyat Dasturiy hamyonlarni kriptovalyutadan kundalik foydalanish uchun ajoyib imkoniyatga aylantiradi, ammo bunday hamyonlarda uzoq vaqt davomida katta miqdordagi pulni saqlash uchun to‘g‘ri emas.

Dasturiy hamyonlar oddiy kompyuter yoki mobil qurilmada ishlashi mumkin. Ular hech qanday muammosiz kriptovalyutani o‘tkazish yoki qabul qilish imkoniyatini beradi. Biroq, Dasturiy hamyonlar o‘rnatilgan qurilmaning o‘zi viruslar yoki shu kabi xavflar oldida zaif bo‘lganligi uchun, ular ham himoyasi kuchsiz hisoblanadi.

2. Electrum hamyon

“Electrum hamyon”i 2011-yil noyabr oyida ishlab chiqilgan bo‘lib, u faqat “Bitkoin” kriptovalyutasi bilan ishlash uchun mo‘ljallangan. Bu uni dunyodagi dastlabki “Bitkoin” hamyonlaridan biri ekanligini ko‘rsatadi. Shu bilan birga, ekspertlar fikriga ko‘ra, u eng yaxshi “Bitkoin” hamyonlaridan biri hisoblanadi.

“Electrum hamyon”i faqat “Bitkoin” kriptovalyutasini saqlashi mumkin. U boshqa kriptovalyutalarni, hatto “Bitkoin” kriptovalyutasining hosilasi bo‘lgan Bitcoin Cashni ham tanimaydi. Biroq, hozirda Bitcoin Cashga o‘xshash “Bitkoin” kriptovalyutasining hosilasini taniydigan, “Electrum hamyon”i kodiga asoslangan norasmiy hamyonlar mavjud.

Bunga misol sifatida “Electron Cash” elektron hamyonini ko‘rish mumkin. Ushbu hamyon “Electrum hamyon”i bilan hech qanday bog‘liqligi yo‘q, lekin deyarli bir xil koddan foydalanadi. Shu

bilan birga u "Bitkoin" kriptovalyutasining hosilasi bo'lgan Bitcoin Cash bilan ishlay oladi.

"Electrum hamyon"i haqida gapirganda, alohida ahamiyat berish kerakki, uning foydalanuvchilari to'g'risida aniq ma'lumotlar mavjud emas. Shunga qaramay, ba'zi manbalar 2018-yilda bu "Bitkoin" operatsiyalarining 10% dan ortig'ini "Electrum hamyon"i orqali amalga oshirilgan deb da'vo qilmoqdalar.

3. Electrum hamyoning yaxshiligi

Yuqorida aytib o'tganimizdek, "Electrum hamyon"i dasturiy hamyon hisoblanadi. Bu shuni anglatadiki, u onlayn hamyonga qaraganda xavfsizroq muhitni taqdim etadi, ammo apparat hamyoniga qaraganda xavfsiz emas. Garchi eng xavfsiz variant bo'lmasa-da, ekspertlar "Bitkoin" operatsiyalarini amalga oshirishda juda qulayligi haqida ko'p ta'kidlashadi. Ya'ni, agar siz sotib olish uchun "Bitkoin" kriptovalyutasidan foydalanmoqchi bo'lsangiz, u holda "Electrum hamyon"i eng yaxshi variant hisoblanadi.

3.1. "Electrum hamyon"ning afzalliklari va kamchiliklari

Quyida ekspertlar tomonidan doimo ta'kidlanadigan "Electrum hamyon"ning afzalliklari va kamchiliklari keltirilgan.

"Electrum hamyon"ning afzalliklari

- "Bitkoin" kriptovalyutasi bo'yicha doimiy to'lovlarni amalga oshirishda foydalanuvchilar uchun ideal tizim hisoblanadi.
- Parol bilan himoyalanganlik xakerlarning hamyonga kirishini ancha qiyinlashtiradi.
- Foydalanuvchilar blokcheyn tizimini o'z qurilmalariga to'liq yuklab olishiga hojati yo'q. "Electrum hamyon"i serverdan ma'lumotlarni olishda mustaqil ishlaydi. Bu esa olingan ma'lumotlarda hech qanday kechikish yo'qligi va ma'lumotlar aktualligini anglatadi.
- Shaxsiy kalitlar hech qachon foydalanuvchi qurilmasidan boshqa yoqqa chiqmaydi. Demak, tashqi serverlarga ishonish va doimo hadiksirab yurish shart emas!
- Foydalanuvchi to'g'risidagi ma'lumotlar serverda saqlanmaydi. Shuning uchun, foydalanuvchilar o'zlarining shaxsiy kalitlari va kriptovalyutasini nazorat qilish imkoniyatiga ega.

- "Electrum hamyon" dasturi kodining ochiqligi. Har kim qurilma kodini tizimdagi baglar, xatolar va zaifliklar bo'yicha tekshirishi mumkin.
- "Electrum hamyon" dasturini yuklab olishning to'liq tekinligi.
- "Electrum hamyon" dasturini tranzaksiya komissiyasi to'lovlarini avtomatik ravishda hisoblab chiqish imkoniyati. Bu foydalanuvchiga uning tranzaktsiyasi zarurligiga qarab, uni tezlashtirish yoki shoshilmasdan amalga oshirish bo'yicha tanlashga imkon beradigan foydali slayderga ega. Foydalanuvchining tanloviga qarab, operatsiya tez bajarilishi va shunga mos ravishda, tranzaksiya uchun komissiya ham o'zgaradi.
- "Electrum hamyon" ko'p imzoli (multi ERI) hamyon sifatida ishlatilishi mumkin. Bu esa hamyonning xavfsizlik darajasini sezilarli darajada oshiradi.
- Foydalanuvchilar ikki faktorli autentifikatsiyadan foydalanishlari mumkin. Bu ham hamyonning xavfsizlik darajasini oshiradi.

"Electrum hamyon"ning kamchiliklari

-Bir qator qo'shimcha xavfsizlik funksiyalariga ega bo'lishiga qaramasdan, "Electrum hamyon"i bari bir Internetga ulangan holda ishlaydi. Bu degani, barcha issiq hamyonlarga tegishli bo'lgan muammolar unga ham tegishli bo'lib qolaveradi. Ya'ni "Electrum hamyon"i o'rnatilgan qurilma Internet bilan bog'liq bo'lgan xavfsizlik xatarlariga nisbatan zaif bo'lganligi tufayli, xakerlar tomonidan foydalanuvchining "Bitkoin"iga nisbatan ham xavf saqlanib qolaveradi.

- "Electrum hamyon"ining kamchiliklaridan yana biri, u faqat "Bitkoin" kriptovalyutasi bilan ishlay oladi. Agar foydalanuvchi faqat "Bitkoin" kriptovalyutasidan foydalansa, bu unchalik katta kamchilik emas. Lekin "Bitkoin" kriptovalyutasining biror hosilasi paydo bo'lishi bilan "Electrum hamyon"ni almashtirshga to'g'ri keladi.
- "Electrum hamyon"ining kamchiliklaridan yana biri - yaqinda, 2017-yilda xavfsizlik bilan bog'liq yangi muammolar yuzaga keldi. "Electrum hamyon" jamoasi ularni bartaraf etish uchun anchagina vaqt sarflashdi. Buni e'tiborga olish kerak.

"Electrum hamyon"ining xavfsizlik tizimi haqida umumiy ma'lumot

"Electrum hamyon"ining "Bitkoin" kriptovalyutasini himoya qilishga yordam beradigan bir nechta qo'shimcha funksiyalari mavjud. Mazkur funksiyalar uning sohadagi eng xavfsiz hamyonlardan biri bo'lishiga asosiy sabab hisoblanadi. Biroq, u doimiy Internetga ulanmay ishlaydigan hamyonlarga nisbatan, masalan sovuq hamyonlar kabi xavfsiz emas.

"Electrum hamyon"ining xavfsizlik tizimining o'ziga xos xususiyatlari:

- foydalanuvchining yopiq kalitlari saqlanadigan shifrlangan hamyon fayli parol bilan himoyalangan.
- "Electrum hamyon"i tiklash usuli sifatida "SEED" iborasini ishlatadi. Bu foydalanuvchining yopiq kalitlar yoki dastur o'rnatilgan qurilmani yo'qotish xavfidan himoya qiladi. "SEED" iborasi – bu "Electrum hamyon"i yopiq kalitlarini yaratish uchun foydalaniladigan so'zlar ketma-ketligi.
- "Electrum hamyon"i hech qanday skriptlarni Internetdan yuklab olmaydi. Bu shuni anglatadiki, agar server buzilgan bo'lsa ham, foydalanuvchining "Bitkoin" kriptovalyutasi yo'qolmay qolaveradi.
- "Electrum hamyon"i server kodi ochiq bo'lganligi sababli istalgan kishi yangi serverni ishga tushirishi mumkin. Bunday markazlashmagan model dastur uzilishlarini oldini oladi.
- "Electrum hamyon"i Python dasturlash tilida yozilgan. Bu ancha taniqli til bo'lganligi tufayli "Electrum hamyon"i kodi muntazam ravishda jamoa a'zolari tomonidan tekshirib turiladi.

"Electrum hamyon"i yuqorida keltirilgan ko'plab xavfsizlik choralariga ega bo'lishiga qaramay, ushbu masalada ba'zi muammolar mavjudligi ko'rinmoqda. Masalan, yuqorida aytganimizdek, 2017-yil noyabr oyida "Electrum hamyon"i jamoasi bunday muammolardan birini bartaraf etish uchun ancha-muncha ter to'kishdi.

Agar London universiteti kolleji aspiranti Mustafo Al-Bassam tomonidan chop etilgan maqolaga ishonadigan bo'lsak, muammo 2016-yil fevral oyidan beri kuzatilmoqda edi(2.6 versiya). Maqolada dasturdagi xato foydalanuvchilar xavfsizligiga qanday tahdid solishi tushuntirib berilgan:

"Dasturdagi mavjud kamchilik (bag) har qanday zararli saytga sizning hamyoningizni boshqarish, masalan "Bitkoin"ni uzatish huquqini beradi, shu jumladan hamyon parol bilan shifrlanmagan

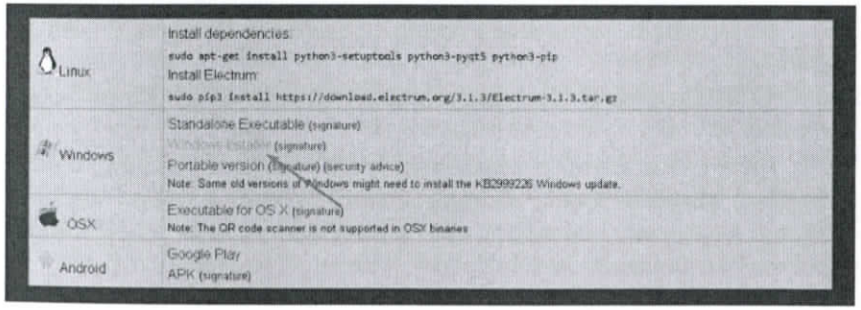
bo'lsa. Biroq, parol mavjud bo'lsa ham, foydalanuvchi hamyonidagi "Bitkoin"ni xakerning manziliga qayta yo'naltirish mumkin"-deb yozadi u.

"Electrum hamyon"i jamoasi mazkur zaiflikni faqat 2018-yilning yanvar oyi boshlarida tuzatishga muvaffaq bo'ldi. Ular muammoning bunday jiddiyligidan xabardor emasliklarini da'vo qilishib, o'zlarini oqlashga urinishgan. Ammo bu muammoni yengillashtirmaydi. Kamchilmik bartaraf etildi, ammo ushbu muammo tufayli qancha foydalanuvchi (agar mavjud bo'lsa) o'z "Bitkoin"larini yo'qotganligi ma'lum emas.

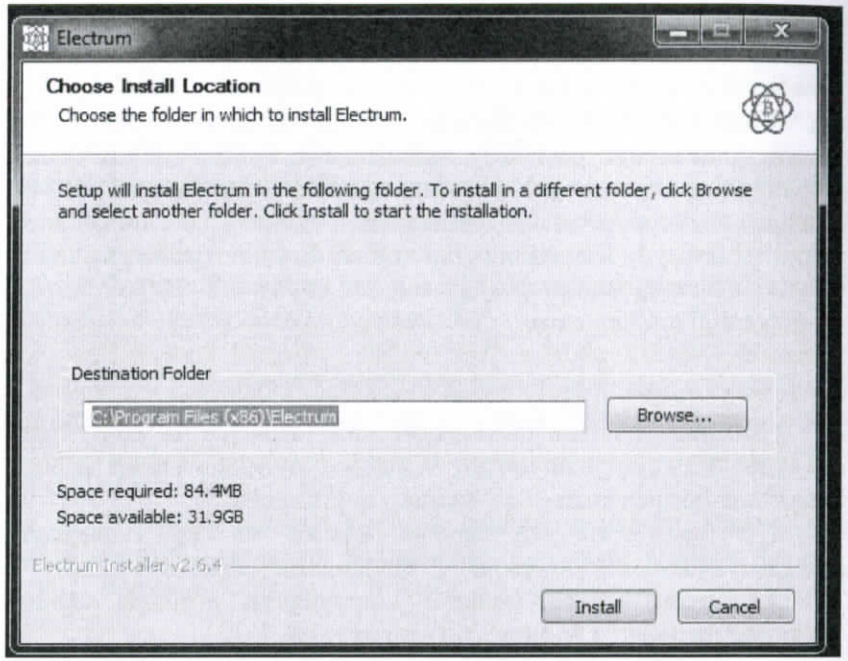
3.2.Electrum hamyonini sozlash

"Electrum hamyon"ini sozlash juda oson va u ko'p vaqt olmaydi. "Electrum hamyon"ini Windows foydalanuvchilari uchun bosqichma-bosqich sozlash qo'llanmasi quyidagicha:

1. www.electrum.org caytiga kiriladi va va yuqoridagi navigatsiya panelida "Download" ("Yuklab olish") tugmasi bosiladi.
2. Keyin, kerakli fayllarni kompyuterga o'rnatish uchun "Windows Installer" (Windows o'rnatuvchi) bosiladi.



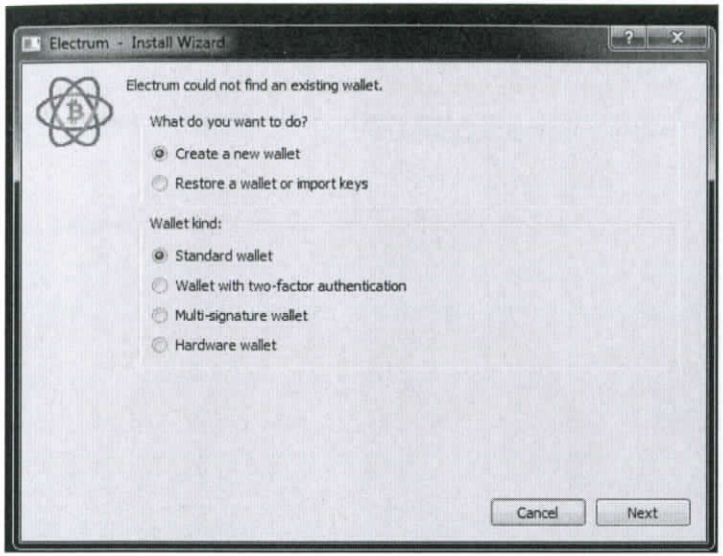
3. Yuklab olingan fayllar ochiladi va o'rnatish jarayonida o'rnatuvchi dasturning ko'rsatmalariga amal qilib boriladi.



4. O‘rnatish tugagandan so‘ng, “Electrum hamyon”i ishga tushiriladi.

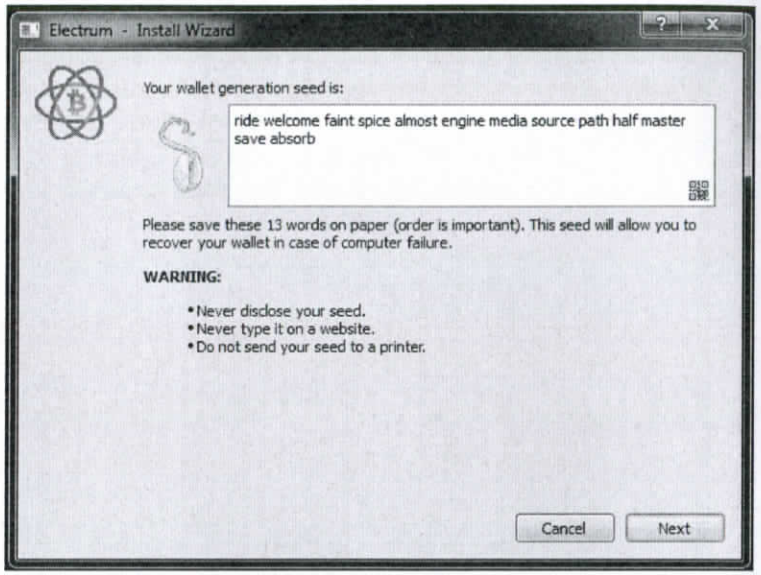
5. So‘ngra yangi hamyon yaratish yoki mavjudini tiklash talab qilinadi.

Agar avval hamyon yaratilmagan bo‘lsa, ya’ni bizning holda yangisini yaratish lozim. Buning uchun “Create a New Wallet” (“Yangi hamyon yaratish”) va “Standard Wallet” (“Standart hamyon”)lar tanlanadi hamda “Next” (“keyingi”) tugmasi bosiladi.



6. Shundan so‘ng biz uchun “SEED” iborasi yaratiladi. Ushbu iborani yozib olish va xavfsiz joyda saqlash juda muhimdir. Chunki u agar hamyonni qayta tiklash ehtiyoji paydo bo‘lsa, bizga juda kerak bo‘ladi.

“Electrum hamyon”ining ko‘pgina ekspertlari ushbu ma’lumotlarning yo‘qolishi sababli paydo bo‘ladigan muammolar haqida xabar berishgan. Bu holda kompyuterda matnli fayl yaratish va unda “SEED” iborasini saqlash tavsiya etilmaydi. Yaxshisi uni qog‘ozga yozib, hujjatlar yoki boshqa muhim narsalar bilan birga saqlash maqsadga muvofiq hisoblanadi.



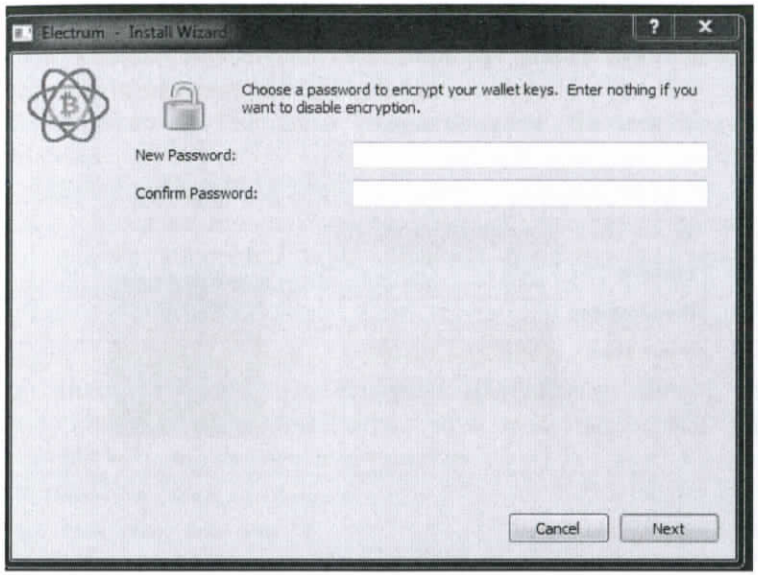
7. Keyingi bosqichda "SEED" iborasi kiritish zarur bo'ladi. Bu yozib olingan "SEED" iborasining to'g'ri ekanligiga ishonch hosil qilish uchun qilingan.

Aslida, bu juda muhim bosqich - xavfsizlik bo'yicha tavsiyalarni e'tiborsiz qoldirmaslik lozim.

8. Keyingi qadamda parol o'ylab topish zarur. Bunda iloji boricha ishonchlilikka e'tibor qaratish zarur. Bu xavfsizlik tizimining yana bir muhim qismi hisoblanadi.

Oddiy, eslab qolish oson bo'lgan parollarga ishonmagan ma'qul, chunki - agar eslash oson bo'lsa, uni sindirish ham oson bo'ladi

Parol yaratish jarayoni yakunlangandan so'ng, uni qayta kiritib, "Next" ("keyingi") tugmasi bosiladi.



9. Bu bizning birinchi hamyonimiz bo'lganligi tufayli, endi ulanish uchun server tanlashimiz kerak bo'ladi. Buning uchun dastlab"Auto Connect" ("Avtomatik ulanish") variantini tanlash tavsiya etiladi

10. Shundan so'ng "Next" ("Keyingi"!) tugmasi bosiladi.

Shu bilan "Electrum hamyon"i foydalanishga tayyor bo'ldi.

3.3.Electrum hamyondan foydalanish

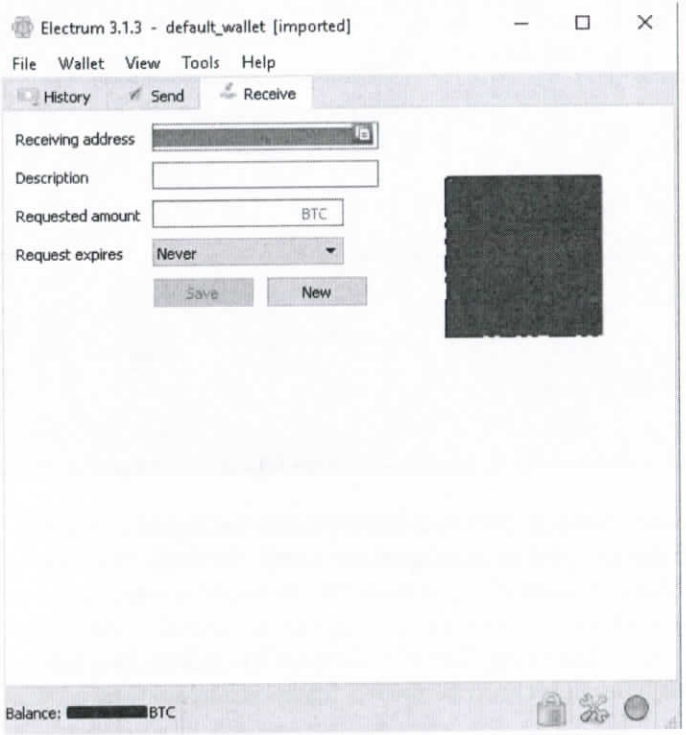
Endi "Electrum hamyon" yordamida tranzaksiyalarni qanday yuborish va qabul qilishni bilib olaylik. Bu, ayniqsa, kriptovalyuta dunyosiga yangi kelganlar uchun foydali bo'ladi.

"Bitkoin" olish

Birinchi qadamda o'rganishimiz zarur bo'lgan narsa - bu hamyonimizga qanday qilib "Bitkoin" olish bo'ladi. Chunki hozircha hamyonimiz butunlay bo'sh.

"Electrum hamyon" yordamida"Bitkoin" olish juda oson. Bu quyida keltirilgan asosiy qadamlardan iborat:

1. “Electrum hamyon” dasturining asosiy oynasida “Receive” (“Qabul qilish”) varag‘iga o‘tiladi.



2. Bunda “Receiving Address” (“qabul qilish manzili”) yonida turli belgilarga ega qatorni ko‘ramiz (u yuqoridagi rasmda qizil to‘rtburchakda ko‘rsatilgan). Ko‘k fondagi ikkita varaqning belgisi bo‘lgan nusxa olish tugmachasi bosiladi. Bu bizning (ya’ni, qabul qiluvchining) ommaviy manzilimizni buferga ko‘chiradi.

3. Bitkoinlarni o‘tkazayotgan joyga ochiq kalit (manzil) joylashtiriladi. Bunda agar ularni valyuta almashtiruvchidan yoki birjadan yuborayotgan bo‘lsak, u holda kriptovalyutani olish maydoniga ochiq kalit kiritiladi. Tranzaksiya tasdiqlagandan so‘ng, mablag‘larimiz “Electrum hamyon”ga etib borishi uchun biroz vaqt ketishi mumkin.

4. Agar “Bitkoin” mobil qurilmadan yuborilayotgan bo‘lsa, u holda QR kodidan foydalanish ham mumkin. Yuqoridagi rasmda u binafsha rangdagi kvadrat bilan belgilangan.

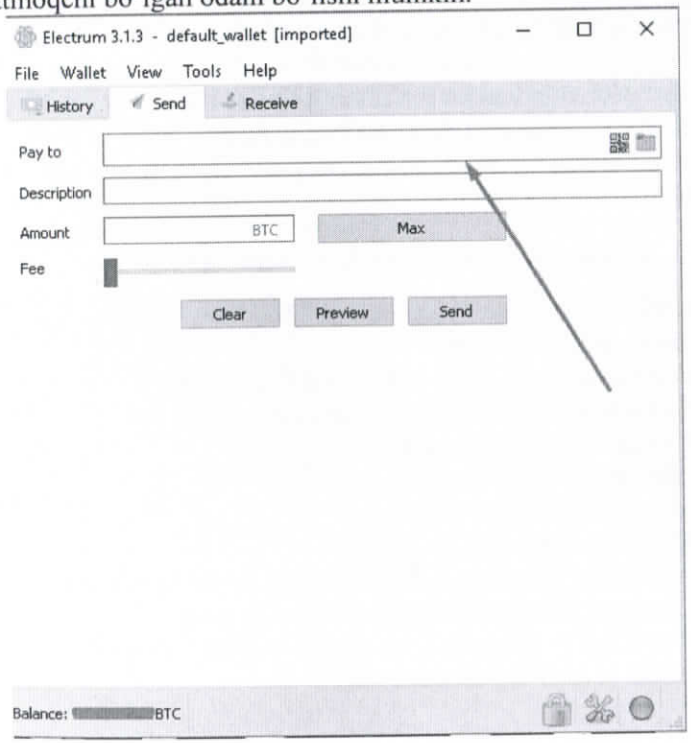
Shundan so‘ng “Electrum hamyon”imizda “Bitkoin” paydo bo‘lishi kerak.

“Bitkoin” yuborish

Endi “Electrum hamyon”imizda “Bitkoin” mavjudligi sababli, biz uni qanday yuborishni bilib olishimiz mumkin. Bu jarayon quyidagi qalamlardan iborat bo‘ladi:

1. “Electrum hamyon”imizning yuqori menyusidagi “Send” (“Yuborish”) varag‘iga o‘tiladi.

2. “Bitkoin” yubormoqchi bo‘lgan manzil nusxasi olinadi. Bu onlayn-do‘kon, valyuta almashtirish joyi yoki shunchaki pul jo‘natmoqchi bo‘lgan odam bo‘lishi mumkin.



3. Nusxasi olingan manzilni “Pay To” (“...ga to‘lansin”) yozuvi yonidagi maydonga joylashtiriladi. Bunda har doim manzilni ikki marta tekshirib ko‘rish kerak, chunki hatto nusxalashda ham ba’zan xatoliklar bo‘lishi mumkin. Buni birinchi va oxirgi uchta belgini tekshirish orqali amalga oshirish mumkin.

4. “Amount” (Summa) maydonining yoniga biz yubormoqchi bo‘lgan “Bitkoin” miqdori kiritiladi.

5. Slayder yordamida amalga oshirilayotgan tranzaksiya uchun komissiya summasi (xizmat haqi) belgilanadi. Shuni unutmaslik lozimki, komissiya qancha kam bo‘lsa, tranzaksiyaning amalga oshirish vaqti ham shuncha uzoq davom etadi.

Agar iloji boricha “Bitkoin” yuborish operatsiyasini tezroq amalga oshirish zarur bo‘lsa,u holda slayderni chiziqning o‘ng tomoniga yaqinroq o‘rnatish tavsiya etiladi. Bunda komissiya qimmatroq bo‘ladi, ammo tranzaksiya tezligi ham sezilarli darajada oshadi.

6. Bu qadamda barcha ma’lumotlar yana bir bor qayta tekshirib chiqiladi. Agar hammasi to‘g‘ri bo‘lsa, u holda “Send” (“yuborish”) tugmachasi bosiladi. Tranzaksiya deyarli yakunlandi, faqat uni tugashini kutish kerak xolos.

Mustaqil ish yuzasidan nazorat savollari

Ushbu “Electrum hamyon”i sharhini o‘qib bo‘lgach, quyidagilarni bilishimiz lozim:

- Hamyonlarning har xil turlari orasidagi farqlar.
-Ularning har birining afzalliklari va kamchiliklari.
-“Electrum hamyon”i nima?
-Ushbu hamyon nima uchun foydali?
-Uning kamchiliklari nimada?
-“Electrum hamyon”i xavfsizmi?
-2017-yilda “Electrum hamyon”ida paydo bo‘lgan zaiflik nima?
-“Electrum hamyon”ini qanday o‘rnatish kerak.
- “Bitkoin” yuborish va qabul qilish uchun “Electrum hamyon”idan qanday foydalanish zarur?

Adabiyotar ro`yxati

1. Могайар У. Блокчейн для бизнеса. – М: Издательство «Эксмо», 2018. – 224 с.
2. Дрешер Д. Основы блокчейна: вводный курс для начинающих в 25 небольших главах // М.: «ДМК Пресс». - 2018. - 196 с.
3. Прасти Н., Блокчейн. Разработка приложений. Разработка децентрализованных приложений в реальном времени на платформе Ethereum. СПб.: «БХВПетербург», 2018.
4. Даннен Крис. Введение в Ethereum и Solidity//Самара, Самиздат, 2018. — 90 с.
5. Свэн М. Блокчейн. Схема новой экономики; перевод, оформление, издание – М,: Издательство «Олимп – Бизнес», 2017. – 240 с
6. Анисимов В.В., Ешенко Р.А. Криптографические методы защиты информации // Хабаровск: Изд-во ДВГУПС. - 2017. URL:<https://www.sites.google.com/site/anisimovkhv/learning/kripto/lecture>
7. Акбаров Д. Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши // Тошкент. «Ўзбекистон маркаси». - 2009. - 432 б.
8. S.S. Gulyamov, R.H. Ayupov, O.M. Abdullaev, G.R. Baltabaeva. Raqamli iqtisodiyotda blokcheyn texnologiyalar. T.: TMI, “Iqtisod-Moliya” nashriyoti, 2019, 404 bet.
9. https://www.bigcommerce.com
10. https://ru.wix.com
11. https://squarespace.sjv.io
12. http://www.jdoqocy.com
13. http://ziyonet.uz

UO‘K 35.074, 519. 253
A.A. Saidov, J.Usmonov
Elektron hukumat tizimlarida blokcheyn texnologiyalarini qo‘llash asoslari // O‘quv qo‘llanma, Toshkent. 2021. -142 b.

O‘quv qo‘llanma

«Mahalla va oila nashriyoti»
Toshkent – 2021

Nashr uchun mas’ul: B. Mavlonov

Muharrir: U. Yunusov

Badiiy muharrir: F. Sobirov

Dizayner-sahifalovchi: L. Abdullayev

Nashriyot ro‘yxat raqami № 1043191. 24.09.2021-y.
Bichimi 60x84 1/16 Offset qog’ozi.
Times New Roman garniturasi.
Shartli bosma tabog’i 8,75. Nashr hisob tabog’i 6,5.
Adadi 100 nusxada. Buyurtma № 10-12.

1940

100000, Toshkent shahri, Mirzo Ulug‘bek tumani,
M.Ismoiliy ko‘chasi 1-G uy.

«ZUXRA BARAKA BIZNES» MChJ bosmaxonasida chop etildi.
Toshkent shahri Bunyodkor shoh ko‘chasi 27 A–uy.