IQRO JURNALI , IQRO JOURNAL, ИКРО ЖУРНАЛИ
ISSN:2181-4341| wordlyknowledge.uz/index.php/iqro
Volume 24. Issue 01. Oktabr, 2026

BIOMETRIK KALIT ORQALI BLOKCHEYN TRANZAKSIYASINI IMZOLASH

Abdupattayev Xondamirjon Elyorjon o‘g‘li
Vatan Universiteti 2-kurs magistranti
https://doi.org/10.5281/zenodo.23276111

Annotatsiya. Mazkur maqolada biometrik autentifikatsiya vositalari yordamida blokcheyn tranzaksiyalarini kriptografik imzolash mexanizmlari, ularning ishlash tamoyillari va axborot xavfsizligini ta’minlashdagi ahamiyati tahlil qilinadi. Biometrik ma’lumotlar asosida foydalanuvchini aniqlash, kriptografik kalitlardan foydalanish, tranzaksiyalar yaxlitligini ta’minlash hamda raqamli aktivlar bilan bog‘liq operatsiyalarda ruxsatsiz harakatlarning oldini olish masalalariga alohida e’tibor qaratiladi. Shuningdek, biometrik ma’lumotlarni himoyalash, kalitlarni xavfsiz saqlash va mazkur texnologiyani amaliy tizimlarga joriy etish istiqbollari yoritiladi.

Kalit so‘zlar: biometrika, blokcheyn, kriptografiya, tranzaksiya, autentifikatsiya, imzo, xavfsizlik, identifikatsiya.

KIRISH

Raqamli iqtisodiyotning rivojlanishi moliyaviy operatsiyalar, elektron xizmatlar va raqamli aktivlarni boshqarishda ishonchli identifikatsiya hamda xavfsiz tasdiqlash mexanizmlariga bo‘lgan ehtiyojni oshirmoqda. Blokcheyn texnologiyasi ma’lumotlarni taqsimlangan reyestrda saqlash, tranzaksiyalar tarixini tekshirish va amalga oshirilgan operatsiyalarning yaxlitligini ta’minlash imkonini beradi. Biroq blokcheyn tizimlarida tranzaksiyani yuborish uchun ishlatiladigan kriptografik kalitning xavfsizligi foydalanuvchi aktivlari va huquqlarini himoyalashda muhim o‘rin tutadi.

An’anaviy kalitlarni boshqarish usullarida maxfiy kalitni yo‘qotish, uning begona shaxslar qo‘liga tushishi yoki tiklash ma’lumotlarining oshkor bo‘lishi jiddiy xavflarni keltirib chiqarishi mumkin. Bunday muammolarni kamaytirish yo‘llaridan biri biometrik autentifikatsiyani kriptografik kalitlardan foydalanish jarayoni bilan birlashtirishdir. Bunda barmoq izi, yuz tasviri yoki boshqa biometrik belgi foydalanuvchini tekshirish va kalitdan foydalanishga ruxsat berish uchun xizmat qiladi. Mazkur yondashuv qulaylikni oshirish bilan birga, xavfsizlik talablariga mos ravishda loyihalashtirilgan taqdirda blokcheyn tranzaksiyalarini himoyalash imkoniyatlarini kengaytiradi.

ASOSIY QISM

Blokcheyn — tranzaksiyalar yoki boshqa raqamli yozuvlar ketma-ket bloklarda qayd etiladigan, bloklar o‘zaro kriptografik bog‘lanadigan va ma’lumotlar bir nechta tugunlar o‘rtasida taqsimlangan holda saqlanishi mumkin bo‘lgan texnologiyadir. Uning muhim xususiyatlaridan biri tranzaksiyalarni tekshirishda kriptografik vositalardan foydalanilishidir. Ko‘plab blokcheyn tizimlarida foydalanuvchi o‘z aktivlarini boshqarish yoki muayyan operatsiyani amalga oshirish uchun tranzaksiyani maxfiy kriptografik kalit yordamida imzolaydi.

Tarmoq ishtirokchilari esa tegishli ochiq kalit yoki undan hosil qilingan manzilga bog‘liq ma’lumotlar orqali imzoning haqiqiyligini tekshiradi.

Kriptografik imzo tranzaksiyaning muhim tarkibiy qismlaridan biri bo‘lib, u operatsiya ma’lumotlari imzolashdan keyin o‘zgartirilmaganini aniqlash va imzolash uchun ishlatilgan kalit bilan bog‘liq nazoratni amalga oshirish imkonini beradi. Masalan, foydalanuvchi raqamli aktivni boshqa manzilga yuborishni rejalashtirganda tranzaksiyada qabul qiluvchi manzil, aktiv miqdori, tegishli tarmoq parametrlari va boshqa zarur maydonlar belgilanadi. Ushbu ma’lumotlarning belgilangan qismi kriptografik imzo hosil qilish jarayonida ishlatiladi. Agar imzolangandan keyin imzo bilan bog‘langan ma’lumotlar o‘zgartirilsa, tekshiruv muvaffaqiyatsiz yakunlanishi kerak. Bunda kriptografik imzo foydalanuvchining biologik xususiyatlarini bevosita ifodalamaydi. U matematik usullar asosida maxfiy kalit bilan yaratiladi. Biometrik autentifikatsiya esa ushbu kalitdan foydalanishga, kimga va qanday sharoitda ruxsat berilishini belgilashga yordam beradi. Shu sababli biometrik vosita va kriptografik imzo bir-birini to‘ldiruvchi, ammo vazifalari turlicha bo‘lgan xavfsizlik mexanizmlari hisoblanadi.

Blokcheyn tranzaksiyasini biometrik vosita yordamida tasdiqlashda uchta asosiy vazifani farqlash lozim: foydalanuvchini biometrik tekshirish, kriptografik kalitdan foydalanishga ruxsat berish va tranzaksiyani raqamli imzo bilan tasdiqlash. Birinchi vazifa shaxsning qurilmada ro‘yxatga olingan biometrik belgiga mosligini baholaydi. Ikkinchi vazifa kalitga kirishni boshqaradi. Uchinchi vazifa esa blokcheyn protokoli talablariga mos kriptografik imzoni hosil qiladi. Ushbu bosqichlarning to‘g‘ri tashkil etilishi foydalanuvchi uchun qulaylik yaratish bilan birga, kalitni oddiy dasturiy muhitda ochiq holda saqlash zaruratini kamaytiradi.

Biometrik autentifikatsiya va uning asosiy turlari. Biometrik autentifikatsiya — insonning o‘ziga xos anatomik yoki xulq-atvor belgilarini tahlil qilish orqali uning avval ro‘yxatga olingan foydalanuvchiga mosligini tekshirish jarayonidir. Biometrik texnologiyalar amaliyotda barmoq izi, yuz geometriyasi, ko‘zning ayrim xususiyatlari, ovoz va boshqa belgilar asosida ishlashi mumkin. Ularning har biri ma’lumotni yig‘ish usuli, aniqlik darajasi, tashqi sharoitlarga sezgirligi va soxtalashtirishga qarshi imkoniyatlari bilan farqlanadi.

Barmoq izi orqali autentifikatsiya mobil qurilmalar va maxsus sensorlarda keng tarqalgan. Uning asosiy afzalligi — tezkorligi va foydalanuvchidan murakkab parolni muntazam kiritishni talab qilmasligidir. Biroq sensor yuzasining ifloslanishi, barmoqning nam yoki shikastlangan bo‘lishi, shuningdek, soxta barmoq izidan foydalanishga urinish tekshiruv natijasiga ta’sir ko‘rsatishi mumkin. Shu sababli biometrik tekshiruvning sifati sensorning o‘ziga, dasturiy algoritmlarga va soxtalashtirishga qarshi qo‘llaniladigan himoya vositalariga bog‘liq.

Yuz orqali autentifikatsiya foydalanuvchining yuz tasviridan olingan xususiyatlarni tahlil qilishga asoslanadi. Mazkur usul qo‘llarni sensor yuzasiga tekkizishni talab qilmasligi va ayrim qurilmalarda tezkor ishlashi bilan ajralib turadi. Shu bilan birga, yorug‘lik, kamera sifati, yuzning burilishi, tashqi ko‘rinishdagi o‘zgarishlar va tasvirni soxtalashtirishga qaratilgan hujumlar uning ishonchliligiga ta’sir qilishi mumkin. Zamonaviy tizimlarda tiriklikni tekshirish yoki taqdim etilgan biometrik namunani haqiqiy insondan olinganini aniqlashga qaratilgan qo‘shimcha mexanizmlar qo‘llanishi mumkin.

Ovoz orqali autentifikatsiya nutq xususiyatlari asosida amalga oshiriladi. Bunda ovoz tembri, talaffuz va boshqa akustik ko‘rsatkichlar tahlil qilinadi. Biroq shovqinli muhit, kasallik,

charchoq, ovozning tabiiy o‘zgarishi yoki sun’iy yaratilgan ovozdan foydalanish ehtimoli hisobga olinishi lozim. Shu sababli katta moliyaviy qiymatga ega blokcheyn tranzaksiyalarida faqat bitta biometrik belgiga tayanish har doim ham yetarli xavfsizlikni ta’minlamaydi.



1-rasm. Biometrik autentifikatsiya va blokcheyn tranzaksiyasini imzolashning umumiy ko‘rinishi

Biometrik tizimlarning samaradorligi odatda noto‘g‘ri qabul qilish va noto‘g‘ri rad etish ko‘rsatkichlari orqali baholanadi. Noto‘g‘ri qabul qilish begona shaxsning tizim tomonidan qonuniy foydalanuvchi sifatida tan olinishini, noto‘g‘ri rad etish esa haqiqiy foydalanuvchining tekshiruvdan o‘ta olmasligini anglatadi. Ushbu ko‘rsatkichlar o‘rtasida amaliy muvozanat mavjud bo‘lib, xavfsizlik talablarini oshirish ayrim sharoitlarda foydalanuvchi uchun qo‘shimcha noqulaylik tug‘dirishi mumkin. Shuning uchun biometrik autentifikatsiya algoritmini tanlashda faqat tezlik yoki qulaylik emas, balki hujumlarga chidamlilik, qurilma imkoniyatlari va foydalanish muhiti ham baholanishi zarur.

Biometrik kalit va kriptografik kalit o‘rtasidagi farq. Mavzuni to‘g‘ri tushunish uchun biometrik ma’lumot, biometrik shablon va kriptografik kalit tushunchalarini farqlash muhim. Biometrik ma’lumot — insonning barmoq izi yoki yuz tasviri kabi o‘ziga xos belgisini aks ettiruvchi ma’lumotdir. Biometrik shablon esa ushbu ma’lumotdan algoritm yordamida ajratib olingan va solishtirish uchun ishlatiladigan xususiyatlar to‘plamidir. Kriptografik kalit esa raqamli imzo yaratish yoki tekshirish kabi matematik amallarni bajarishda qo‘llanadigan maxsus qiymatdir.

Amaliy tizimlarda “biometrik kalit” atamasi ba’zan biometrik tekshiruv bilan faollashtiriladigan kriptografik kalitni anglatadi. Biroq barmoq izini bevosita maxfiy kriptografik kalit sifatida ishlatish xavfsiz yechim hisoblanmaydi. Biometrik belgilar parol singari istalgan vaqtda yangidan tanlanmaydi: agar biometrik ma’lumot oshkor bo‘lsa, uni almashtirish imkoniyati cheklangan. Bundan tashqari, biometrik namunalar har safar bir xil raqamli natijani bermasligi mumkin, chunki sensor va tasvirga olish sharoitlari o‘zgaradi. Kriptografik kalit esa aniq matematik talablarga javob berishi va belgilangan algoritm doirasida to‘g‘ri ishlashi kerak. Shu sababli xavfsiz arxitekturada biometrik ma’lumot maxfiy kalitning o‘zi sifatida emas, balki undan foydalanishni faollashtiruvchi autentifikatsiya omili sifatida qo‘llanadi. Masalan,

qurilmada maxfiy kalit himoyalangan apparat muhitida saqlanadi va oddiy dasturlar tomonidan bevosita o‘qib olinmaydi. Foydalanuvchi biometrik tekshiruvdan muvaffaqiyatli o‘tgach, apparat moduli yoki operatsion tizimning himoyalangan komponenti kalitdan imzolash maqsadida foydalanishga ruxsat beradi. Bunda kalit qurilmadan tashqariga chiqarilmasdan tranzaksiya imzolanishi mumkin. Mazkur yondashuv foydalanuvchining biometrik belgisi bilan tranzaksiyaning kriptografik imzosi o‘rtasida aniq chegarani saqlaydi. Biometrik tekshiruv shaxsning qurilmaga kirishini tasdiqlashga xizmat qiladi, kriptografik imzo esa tranzaksiya ma’lumotlarining haqiqiyligini tekshirish imkonini beradi. Ushbu farqni e’tiborsiz qoldirish tizimning xavfsizlik modelini noto‘g‘ri shakllantirishga olib kelishi mumkin.

Biometrik autentifikatsiya orqali tranzaksiyani imzolash mexanizmi. Biometrik autentifikatsiyaga asoslangan blokcheyn tranzaksiyasini imzolash tizimi bir necha o‘zaro bog‘liq bosqichdan tashkil topadi. Birinchi bosqichda foydalanuvchi tizimda ro‘yxatdan o‘tadi va uning hisobiga tegishli kriptografik kalitlar juftligi yaratiladi. Ochiq kalit tegishli blokcheyn manzili yoki identifikatsiya mexanizmi bilan bog‘lanishi mumkin, maxfiy kalit esa himoyalangan qurilma yoki apparat modulida saqlanadi. Biometrik ma’lumotni ro‘yxatga olish va undan foydalanish uchun qonuniy asos, foydalanuvchining roziligi hamda ma’lumotlarni himoyalash tartibi belgilanishi lozim. Ikkinchi bosqichda foydalanuvchi blokcheynda bajariladigan operatsiyani shakllantiradi. Tizim qabul qiluvchi manzil, yuboriladigan aktiv miqdori, tarmoq komissiyasi va zarur texnik parametrlarni ko‘rsatadi. Foydalanuvchi ushbu ma’lumotlarni tekshirishi uchun interfeys ularni tushunarli shaklda namoyish etishi kerak. Ayniqsa, manzilning o‘zgarishi, miqdorning noto‘g‘ri kiritilishi yoki zararli dastur tomonidan tranzaksiya parametrlarining almashtirilishi kabi xavflarni kamaytirish muhimdir. Uchinchi bosqichda tizim foydalanuvchidan biometrik tekshiruvdan o‘tishni talab qiladi. Sensor orqali olingan yangi namuna qurilmada saqlangan biometrik shablon bilan solishtiriladi. Moslik belgilangan mezonlarga javob bergan taqdirda, tizim kalitdan foydalanishga ruxsat beradi. Agar biometrik tekshiruv muvaffaqiyatsiz bo‘lsa, maxfiy kalitdan foydalanish to‘xtatiladi yoki qo‘shimcha autentifikatsiya talab qilinadi. Bunda ketma-ket muvaffaqiyatsiz urinishlar sonini cheklash, urinishlar orasidagi vaqtni boshqarish va shubhali faoliyatni qayd etish kabi choralar qo‘llanishi mumkin. To‘rtinchi bosqichda tranzaksiyaning blokcheyn protokoli belgilagan qismi kriptografik imzo uchun tayyorlanadi. Tizim tegishli ma’lumotlardan xesh qiymat hosil qiladi yoki protokol talab qilgan imzolash formatini shakllantiradi. Shundan so‘ng himoyalangan modul maxfiy kalitdan foydalanib raqamli imzoni yaratadi. Imzo tranzaksiya ma’lumotlariga biriktirilib, tarmoqqa yuborishga tayyorlanadi. Bu jarayonda maxfiy kalit foydalanuvchi interfeysi, tashqi server yoki blokcheyn tuguniga ochiq shaklda uzatilmasligi lozim. Beshinchi bosqichda imzolangan tranzaksiya blokcheyn tarmog‘iga yuboriladi. Tarmoq tugunlari tranzaksiyaning protokolga muvofiqligini, raqamli imzoning haqiqiyligini va boshqa tegishli shartlarni tekshiradi. Tranzaksiya qabul qilinganidan keyin u tarmoqning kelishuv mexanizmi asosida blokka kiritilishi mumkin. Shuni ta’kidlash kerakki, biometrik tekshiruvning muvaffaqiyatli o‘tishi tranzaksiyaning avtomatik ravishda tasdiqlanishini anglatmaydi: operatsiya blokcheynning texnik qoidalari va konsensus talablariga ham javob berishi kerak. Mazkur mexanizmning muhim afzalligi shundaki, foydalanuvchi murakkab maxfiy kalitni har bir operatsiyada qo‘lda kiritmaydi. Biroq biometrik tasdiqlashning o‘zi tranzaksiya mazmunini

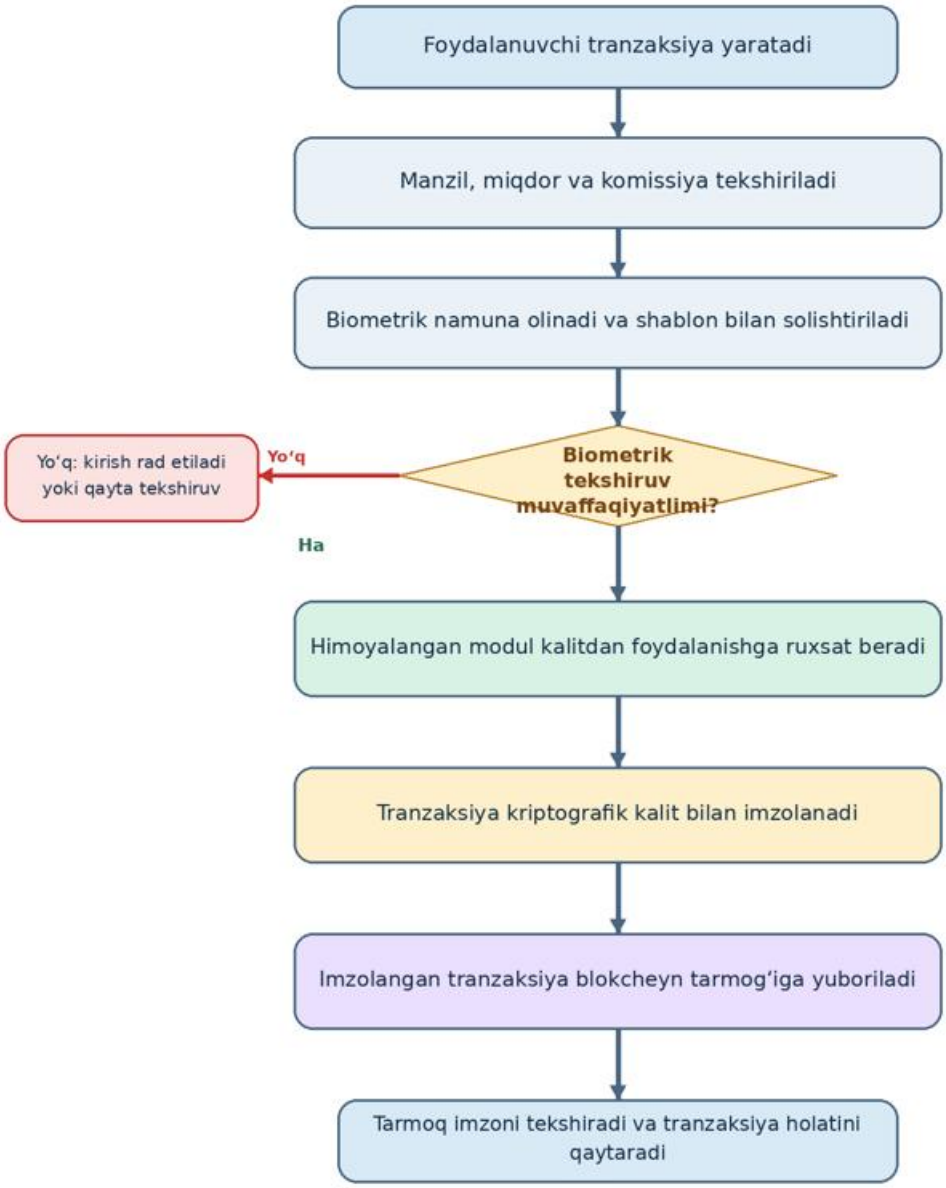
tushunish yoki uning iqtisodiy oqibatlarini anglashni kafolatlamaydi. Shu sababli yuqori qiymatli operatsiyalar uchun tranzaksiya tafsilotlarini qayta tasdiqlash, qo‘shimcha PIN-kod yoki xavfsiz qurilma orqali tasdiqlash kabi ko‘p bosqichli choralar nazarda tutilishi mumkin.

Tizimning umumiy arxitekturasi va asosiy komponentlari. Biometrik kalit orqali blokcheyn tranzaksiyasini imzolash tizimini ishlab chiqishda bir nechta texnik komponentning o‘zaro uyg‘unligi talab etiladi. Birinchi komponent foydalanuvchi interfeysi bo‘lib, u tranzaksiyani shakllantirish, operatsiya tafsilotlarini ko‘rsatish va biometrik tekshiruvni boshlash vazifalarini bajaradi. Interfeysda foydalanuvchi imzolayotgan ma’lumotlar aniq aks ettirilishi, muhim parametrlarni yashirish yoki chalg‘ituvchi tarzda taqdim etishga yo‘l qo‘yilmasligi zarur. Ikkinchi komponent biometrik autentifikatsiya moduli hisoblanadi. U sensor ma’lumotlarini qabul qilish, biometrik shablon bilan solishtirish, tekshiruv natijasini baholash va ruxsat berish jarayonini boshqaradi. Xavfsizlik nuqtayi nazaridan biometrik namunalarni markaziy serverga yuborishdan ko‘ra, ularni foydalanuvchi qurilmasining himoyalangan muhitida qayta ishlash afzal bo‘lishi mumkin. Bu yondashuv markazlashgan biometrik ma’lumotlar bazasiga bo‘lgan ehtiyojni kamaytiradi, lekin qurilma xavfsizligi, dasturiy ta’minot ishonchliligi va zaxira tiklash jarayonlarini to‘g‘ri tashkil etish talabini bekor qilmaydi. Uchinchi komponent kalitlarni boshqarish modulidir. U kriptografik kalitlarni yaratish, himoyalangan holda saqlash, ulardan foydalanishga ruxsat berish, zarur bo‘lganda kalitlarni almashtirish va eski kalitlarni bekor qilish jarayonlarini nazorat qiladi. Maxfiy kalitni oddiy matn ko‘rinishida dasturiy kodga yozish, ochiq konfiguratsiya fayllarida saqlash yoki server jurnallariga chiqarish xavfli hisoblanadi. Kalitni apparat darajasida himoyalash, foydalanish huquqlarini cheklash va muhim operatsiyalarni audit qilish tizim xavfsizligini oshiradi. To‘rtinchi komponent tranzaksiyani shakllantirish va imzolash modulidir. U blokcheyn protokoli talablariga muvofiq tranzaksiya maydonlarini tayyorlaydi, kerakli kriptografik algoritmni chaqiradi va hosil bo‘lgan imzoni tranzaksiyaga biriktiradi. Bu modulda imzolanadigan ma’lumotlarning to‘liq va to‘g‘ri shakllantirilishi alohida ahamiyatga ega. Turli blokcheynlar turlicha imzolash formatlari, xesh funksiyalari va kalit turlaridan foydalanishi mumkinligi sababli, bitta universal mexanizmni barcha tarmoqlarga o‘zgartirishsiz tatbiq etish mumkin emas. Beshinchi komponent blokcheyn bilan aloqa modulidir. U tayyor tranzaksiyani tegishli tugun yoki xizmat orqali tarmoqqa yuboradi, tranzaksiya identifikatorini oladi va uning holatini kuzatadi. Ushbu komponentning vazifasi foydalanuvchiga tranzaksiya yuborilganmi, tarmoq tomonidan qabul qilinganmi yoki blokka kiritilganmi, degan savollarga asoslangan javob berishdan iborat. Bunda tranzaksiyaning yuborilganligi uning yakuniy tasdiqlanganini anglatmasligi interfeysda aniq ko‘rsatilishi lozim.

Tizim arxitekturasida audit va xavfsizlik monitoringi ham muhim ahamiyatga ega. Bunda biometrik tasvirning o‘zi yoki maxfiy kalit yozuvlarini saqlash o‘rniga, autentifikatsiya urinishlari, ruxsat berish natijalari, operatsiya vaqti, xatolik turi va tranzaksiya identifikatori kabi zarur texnik ma’lumotlar qayd etilishi mumkin. Jurnallar foydalanuvchining shaxsiy hayotiga ortiqcha aralashmasligi, ulardan foydalanish huquqi cheklanishi va saqlash muddati belgilanishi kerak.

Biometrik imzolashning afzalliklari va amaliy qo‘llanilishi. Biometrik autentifikatsiyani blokcheyn tranzaksiyalariga bog‘lashning asosiy afzalligi foydalanuvchi tajribasini soddalashtirish va kriptografik kalitdan ruxsatsiz foydalanish xavfini kamaytirish imkoniyatidir.

Ko‘plab foydalanuvchilar maxfiy kalit yoki tiklash iboralarini xavfsiz saqlash, ularni begonalarga bermaslik va kerakli vaqtda to‘g‘ri qo‘llashda qiyinchilikka duch kelishi mumkin. Biometrik tekshiruv bilan himoyalangan kalitlar foydalanuvchiga operatsiyani nisbatan sodda usulda tasdiqlash imkonini beradi. Bunda kalitning o‘zi biometrik ma’lumotdan hosil qilinishi shart emas, aksincha, qurilmada xavfsiz saqlanib, biometrik tekshiruvdan so‘ng ishlatiladi. Bunday yechim raqamli aktivlar hamyonlarida, markazlashmagan moliyaviy xizmatlarda, raqamli identifikatsiya tizimlarida va ayrim elektron boshqaruv xizmatlarida qo‘llanishi mumkin. Masalan, raqamli aktivlar hamyonida foydalanuvchi pul o‘tkazmasini tasdiqlash uchun barmoq izidan foydalanadi, qurilma esa tegishli maxfiy kalit bilan tranzaksiyani imzolaydi. Markazlashmagan ilovalarda biometrik autentifikatsiya foydalanuvchi hisobiga kirish yoki muhim harakatni tasdiqlash jarayonini qulaylashtirishi mumkin. Korporativ tizimlarda esa xodimning biometrik tekshiruvdan o‘tishi uning muayyan raqamli operatsiyani bajarish vakolatini tekshiruvchi boshqa mexanizmlar bilan birlashtirilishi mumkin.



1-chizma. Biometrik tasdiq orqali tranzaksiyani imzolash algoritmi

Blokcheyn asosidagi raqamli hujjat aylanishi tizimlarida ham biometrik tekshiruv bilan himoyalangan kriptografik kalitlardan foydalanish imkoniyati mavjud. Masalan, hujjatni tasdiqlash, ma’lumotlar almashinuvini qayd etish yoki ruxsat berilgan operatsiyani imzolashda kalitdan foydalanish jarayonini foydalanuvchining biometrik tasdig‘iga bog‘lash mumkin. Biroq bunday texnik imzo har qanday holatda ham qonuniy ma’nodagi elektron raqamli imzo talablarini avtomatik ravishda bajarmaydi. Huquqiy kuch tegishli yurisdiksiya, qo‘llaniladigan vosita va qonunchilik talablariga muvofiqlik bilan belgilanadi. Biometrik kalitlardan foydalanish, shuningdek, ko‘p foydalanuvchili boshqaruv tizimlarida muhim bo‘lishi mumkin. Masalan, tashkilotdagi muhim tranzaksiya bir nechta vakolatli shaxs tomonidan alohida tasdiqlanishi talab etilsa, har bir foydalanuvchining kriptografik kaliti o‘ziga tegishli qurilmada saqlanishi mumkin. Bunday holatda biometrik tekshiruv har bir kalitdan foydalanishga ruxsat beruvchi omil sifatida ishlaydi. Ko‘p imzoli mexanizm bilan birgalikda qo‘llanganda, bu yondashuv bitta xodimning hisobiga noqonuniy kirish orqali muhim operatsiyani yakka tartibda amalga oshirish xavfini kamaytirishga yordam beradi. Shu bilan birga, biometrik autentifikatsiya tizimning barcha xavflarini bartaraf etmaydi. Qurilma o‘g‘irlanishi, zararli dasturlar, foydalanuvchini aldash, operatsiya parametrlarining o‘zgartirilishi, tiklash jarayonidagi zaifliklar yoki server hisob ma’lumotlarining buzilishi kabi muammolar saqlanib qolishi mumkin. Shuning uchun biometrik tekshiruv blokcheyn protokolining xavfsizlik mexanizmlari, kalitlarni himoyalash, foydalanuvchi huquqlarini boshqarish va operatsiyalarni kuzatish vositalari bilan birgalikda joriy etilishi lozim.

Axborot xavfsizligi, zaifliklar va ularni kamaytirish choralari. Biometrik ma’lumotlar bilan ishlashdagi asosiy xavflardan biri ularning o‘g‘irlanishi yoki ruxsatsiz qayta ishlatilishidir. Oddiy parol buzilganida uni almashtirish mumkin, biroq barmoq izi yoki yuz kabi biologik belgini to‘liq yangilash deyarli imkonsiz. Shu sababli biometrik ma’lumotlar bazasini markazlashgan tarzda yaratish va uni himoyasiz saqlash jiddiy xavf tug‘diradi. Imkon qadar biometrik tekshiruvni foydalanuvchi qurilmasida bajarish, shablonlarni himoyalangan muhitda saqlash, uzatilishi zarur bo‘lgan ma’lumotlarni shifrlash va ularga kirishni qat’iy cheklash maqsadga muvofiqdir.

Ikkinchi xavf — biometrik tekshiruvni aldashga urinishlar. Hujumchi fotosurat, video, soxta barmoq izi yoki sun’iy yaratilgan ovoz yordamida tizimni chalg‘itishga harakat qilishi mumkin. Bunday tahdidlarni kamaytirish uchun tiriklikni aniqlash, sensorning ishonchliligini tekshirish, takroriy urinishlarni cheklash va qurilmaning apparat himoyasidan foydalanish mumkin. Biroq hech bir biometrik algoritm barcha hujumlarga qarshi mutlaq kafolat bermaydi. Shu sababli xavfsizlik sinovlari real foydalanish sharoitlarini, turli foydalanuvchilar guruhlarini va ehtimoliy hujum ssenariylarini qamrab olishi kerak.

Uchinchi xavf kriptografik kalitning o‘g‘irlanishi yoki undan ruxsatsiz foydalanilishidir. Agar maxfiy kalit oddiy fayl sifatida saqlansa, zararli dastur yoki qurilmaga kirish imkoniga ega hujumchi uni nusxalab olishi mumkin. Kalitni himoyalangan apparat modulida saqlash, undan faqat imzolash operatsiyasi doirasida foydalanishga ruxsat berish va imkon qadar kalitni tashqariga eksport qilishni taqiqlash ushbu xavfni kamaytiradi. Shuningdek, kalitning hayotiy

sikli — yaratish, ishlatish, zaxira nusxalarini boshqarish, bekor qilish va almashtirish — oldindan belgilangan siyosat asosida yuritilishi lozim.

To‘rtinchi xavf tranzaksiya mazmunining foydalanuvchi roziligisiz o‘zgartirilishidir. Foydalanuvchi ekranda bir manzilni ko‘rib, qurilma yoki zararli dastur ta’sirida boshqa manzilga yuboriladigan tranzaksiyani imzolab qo‘yishi mumkin. Bunday holatning oldini olish uchun imzolashdan oldin qabul qiluvchi manzil, miqdor, komissiya va tarmoq nomini aniq ko‘rsatish, imkon qadar tranzaksiya tafsilotlarini mustaqil ishonchli qurilmada tekshirish va yuqori qiymatli operatsiyalar uchun qo‘shimcha tasdiqlash talab qilish mumkin. Imzo kriptografik jihatdan haqiqiy bo‘lishi tranzaksiya foydalanuvchi ko‘zlagan maqsadga muvofiq ekanini o‘z-o‘zidan isbotlamaydi.

Beshinchi xavf tiklash va favqulodda holatlarga taalluqlidir. Foydalanuvchi barmog‘ini jarohatlashi, yuzni aniqlash tizimidan foydalana olmasligi yoki qurilmasini yo‘qotishi mumkin. Agar biometrik autentifikatsiya yagona kirish usuli sifatida joriy etilsa va xavfsiz tiklash mexanizmi bo‘lmasa, foydalanuvchi o‘z aktivlariga yoki hisobiga kirish imkoniyatini yo‘qotishi ehtimoli mavjud. Shu sababli oldindan belgilangan zaxira autentifikatsiya usuli, tiklash kalitlari yoki ko‘p tomonlama tiklash mexanizmi ishlab chiqilishi kerak. Biroq tiklash jarayoni asosiy himoyani chetlab o‘tishning oson yo‘liga aylanmasligi lozim.

Oltinchi masala maxfiylik va huquqiy muvofiqlikdir. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni biometrik ma’lumotlarni shaxsga doir ma’lumotlar doirasida ko‘rib chiqadi va ularga ishlov berish uchun qonuniy asoslarni talab qiladi. Shuning uchun biometrik ma’lumotlarni yig‘ishdan oldin qayta ishlash maqsadi, saqlash muddati, ma’lumotlarga kimlar kirishi va foydalanuvchining huquqlari aniqlashtirilishi zarur. Shuningdek, biometrik ma’lumotlarni himoyalash bo‘yicha tegishli normativ-huquqiy talablar, jumladan, ma’lumotlarni saqlash va ulardan foydalanish shartlari amaldagi qonunchilik asosida tekshirilishi lozim.

XULOSA

Biometrik autentifikatsiyani blokcheyn tranzaksiyalarini kriptografik imzolash jarayoni bilan birlashtirish raqamli aktivlar va elektron operatsiyalar xavfsizligini oshirishning istiqbolli yo‘nalishlaridan biridir. Mazkur yondashuv foydalanuvchining biometrik belgisi orqali kriptografik kalitdan foydalanishga ruxsat berish, tranzaksiyalarni qulay tasdiqlash va maxfiy kalitni himoyalangan muhitda saqlash imkonini beradi. Biroq biometrik ma’lumotni bevosita kriptografik kalit sifatida ishlatish o‘rniga, undan autentifikatsiya omili sifatida foydalanish maqsadga muvofiqdir. Tizim samaradorligi biometrik tekshiruv, kalitlarni boshqarish, tranzaksiya ma’lumotlarini nazorat qilish va blokcheyn protokoli talablarining uyg‘unligiga bog‘liq. Kelgusida ushbu texnologiyani amaliyotga tatbiq etishda biometrik ma’lumotlarning maxfiyligi, xavfsiz tiklash mexanizmlari, standartlarga muvofiqlik va qonunchilik talablariga rioya etish asosiy ustuvor yo‘nalishlar bo‘lishi kerak.

FOYDALANILGAN ADABIYOTLAR

1. O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-son “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni. https://lex.uz/docs/-4396419
2. O‘zbekiston Respublikasi Vazirlar Mahkamasining 2022-yil 5-oktabrdagi 570-son qarori. Shaxsga doir ma’lumotlarga ishlov berish sohasidagi ayrim normativ-huquqiy hujjatlarni tasdiqlash to‘g‘risida. https://lex.uz/acts/-6225462
3. O‘zbekiston Respublikasi. “Elektron raqamli imzo to‘g‘risida”gi Qonun. O‘zbekiston Respublikasi Qonunchilik ma’lumotlari milliy bazasi. https://lex.uz/
4. O‘zbekiston Respublikasi Adliya vazirligi. Shaxsga doir ma’lumotlar va ularni himoya qilish. Huquqiy axborot portali. https://advice.adliya.uz/oz/document/2116
5. FIDO Alliance. FIDO User Authentication Specifications. Rasmiy texnik standartlar va tavsiflar. https://fidoalliance.org/specifications/
6. National Institute of Standards and Technology. Digital Identity Guidelines: Authentication and Authenticator Management. NIST Special Publication 800-63B. https://pages.nist.gov/800-63-4/sp800-63b/authenticators/