BLOCKCHAIN TEXNOLOGIYASI ASOSIDA XAVFSIZ AUTENTIFIKATSIYA TIZIMINI LOYIHALASH VA AMALGA OSHIRISH.

Saidrasulov Sherzod Norboy o‘g‘li
Muhammad al-Xorazmiy nomidagi TATU
"Axborot texnologiyalarining dasturiy ta’minoti" kafedrasi dotsenti, PhD
saidrasulovsherzod@gmail.com tel: +99899-881-38-24
G’ulomjonov Xurshidbek Dilmurod o’g’li
Muhammad al-Xorazmiy nomidagi TATU 3-bosqich talabasi
uzbxurshidbek201@gmail.com tel: 90-024-09-25

Annotatsiya: *Ushbu maqolada blockchain texnologiyasidan foydalanib xavfsiz va markazlashmagan autentifikatsiya tizimini yaratish tamoyillari tahlil qilinadi. An’anaviy login-parol asosidagi autentifikatsiya modellari bilan bog‘liq zaifliklar ko‘rsatib beriladi va ularni bartaraf etish uchun blockchainning o‘zgarmaslik, taqsimlangan boshqaruv va kriptografik imzolash kabi imkoniyatlari asosida yangi yondashuv taklif etiladi. Taklif etilgan model foydalanuvchi identifikatsiyasini parolsiz, buzilishlarga chidamli va ishonchli tarzda amalga oshirishga imkon berishi bilan ajralib turadi.*

Kalit so'zlar*: Blockchain, autentifikatsiya, axborot xavfsizligi, taqsimlangan tizim, kriptografik imzo, smart-contract, parolsiz kirish, identifikatsiya, o‘zgarmas reyestr, kiberxavfsizlik.*

Аннотация: *В данной статье анализируются принципы создания безопасной и децентрализованной системы аутентификации с использованием технологии блокчейн. Показаны уязвимости традиционных моделей аутентификации, основанных на логине и пароле, и предложен новый подход, основанный на таких возможностях блокчейна, как неизменяемость, распределённое управление и криптографическая подпись. Предлагаемая модель отличается тем, что обеспечивает безпарольную, устойчивую к взлому и высоконадёжную идентификацию пользователей.*

Ключевые слова*: Блокчейн, аутентификация, информационная безопасность, распределённая система, криптографическая подпись, смарт-контракт, вход без пароля, идентификация, неизменяемый реестр, кибербезопасность.*

Abstract: *This article analyzes the principles of creating a secure and decentralized authentication system using blockchain technology. It highlights the vulnerabilities of traditional login–password-based authentication models and proposes a new approach built on blockchain features such as immutability, decentralized control, and cryptographic signing. The proposed model stands out for enabling passwordless, tamper-resistant, and highly reliable user identification.*

Keywords*: Blockchain, authentication, information security, distributed system, cryptographic signature, smart contract, passwordless login, identification, immutable ledger, cybersecurity.*

KIRISH

Muammo dolzarbligi. Raqamli xizmatlarning kengayishi, masofaviy tizimlar va onlayn platformalar sonining ortishi bilan autentifikatsiya jarayonining xavfsizligi zamonaviy axborot texnologiyalari oldida turgan eng muhim masalalardan biriga aylandi. An’anaviy login-parol asosidagi tizimlar bugungi kunda yirik korporatsiyalar, davlat xizmatlari va moliyaviy platformalarda qo‘llanayotgan bo‘lsa-da, ular turli kiberhujumlar, parol o‘g‘irlash, baza buzilishi va ijtimoiy muhandislik kabi xavf-xatarlarga juda moyil. Foydalanuvchi ma’lumotlarini himoya qilishdagi zaifliklar global miqyosda katta moliyaviy zararlar, maxfiylikning buzilishi va tizimga ishonchning pasayishiga olib kelmoqda. Shu sababli, mavjud autentifikatsiya usullarini yanada ishonchli, shaffof va buzib bo‘lmaydigan shaklga keltirish muhim talabga aylandi.

An’anaviy autentifikatsiya tizimlaridagi cheklovlar haqida gapirganda, login va parolga asoslangan modelning eng katta kamchiligi markazlashgan ma’lumotlar bazasining mavjudligi. Bunday tizimda barcha foydalanuvchi ma’lumotlari bitta serverda saqlanadi, bu esa “single point of failure” muammosini keltirib chiqaradi. Agar server buzilsa, millionlab foydalanuvchilarning identifikatsiya ma’lumotlari bir vaqtning o‘zida xavf ostida qolishi mumkin. Shuningdek, foydalanuvchilar ko‘pincha kuchsiz yoki bir xil parollardan foydalanishadi, phishing hujumlariga duch kelishadi va parollarni saqlash mexanizmlari zaif bo‘lishi xavfsizlikni yanada pasaytiradi. Ikki bosqichli autentifikatsiya yoki biometrik usullar qo‘shimcha himoya taqdim etsa-da, ular ham markazlashgan boshqaruv va bir nuqtaga bog‘liqlik tufayli to‘liq himoya bera olmaydi.

Blockchain texnologiyasining bu sohadagi roli juda muhim. Asosiy tamoyillari — o‘zgarmaslik (immutability), taqsimlangan boshqaruv (decentralization) va kriptografik xavfsizlik — autentifikatsiya jarayonini yanada takomillashtirishga yordam beradi. Ma’lumotlar faqat bitta serverda emas, balki ko‘plab tugunlar (nodelar) o‘rtasida tarqatilib saqlanadi, bu esa tizimni buzish yoki yolg‘on ma’lumot qo‘shish orqali manipulyatsiya qilishni deyarli imkonsiz qiladi. Parolsiz autentifikatsiya, public/private key mexanizmlari va smart-kontraktlar yordamida foydalanuvchini aniqlash jarayoni ancha ishonchli, shaffof va buzib bo‘lmaydigan ko‘rinishga keladi. Natijada, blockchain texnologiyasi zamonaviy autentifikatsiya tizimlarining asosiy muammolarini hal qilish va kelajakdagi xavfsiz

identifikatsiya platformalarini yaratish uchun eng istiqbolli yechimlardan biri sifatida ko‘rilmoqda.

AUTENTIFIKATSIYA TIZIMLARINING NAZARIY ASOSLARI

Autentifikatsiya, avtorizatsiya va identifikatsiya tushunchalari axborot tizimlarida foydalanuvchi xavfsizligini ta’minlash jarayonining muhim qismlaridir. Identifikatsiya — bu foydalanuvchining o‘zini tanishtirishi, ya’ni tizimga kimligini ko‘rsatishi (masalan, login, ID yoki elektron pochta orqali).

Autentifikatsiya esa foydalanuvchining haqiqatan ham o‘zi ekanligini isbotlash jarayonidir, bu ko‘pincha parol, biometrik belgi yoki kriptografik kalit yordamida amalga oshiriladi. Avtorizatsiya esa autentifikatsiya muvaffaqiyatli o‘tgandan so‘ng, foydalanuvchiga qaysi resurslarga kirish huquqi berilishini aniqlovchi bosqichdir. Ushbu uchlik — identifikatsiya, autentifikatsiya va avtorizatsiya — har qanday axborot tizimining xavfsizlik mexanizmlarining asosi hisoblanadi.

Zamonaviy autentifikatsiya usullari esa juda xilma-xildir.

Bugungi kunda autentifikatsiya turli shakllarda qo‘llaniladi va har biri o‘zining texnik va xavfsizlik xususiyatlariga ega:

- Parolga asoslangan autentifikatsiya — bu eng keng tarqalgan usul bo‘lib, foydalanuvchi tomonidan yaratilgan maxfiy parol orqali amalga oshiriladi.
- Ikki bosqichli autentifikatsiya (2FA) — bu parolga qo‘shimcha ravishda SMS-kod, mobil ilova orqali tasdiqlash yoki bir martalik parollarni ishlatishni o‘z ichiga oladi.
- Biometrik autentifikatsiya — foydalanuvchini barmoq izi, yuz, ovoz yoki ko‘z qorachig‘i kabi noyob biologik belgilar orqali aniqlashni ta’minlaydi.
- Token yoki apparat asosidagi autentifikatsiya — maxsus USB-tokenlar, OTP-generatsiya qiluvchi qurilmalar yoki raqamli sertifikatlar yordamida kirishni ta’minlaydi.
- Parolsiz (passwordless) autentifikatsiya. Elektron imzo, kriptografik kalitlar yoki autentifikatsiya ilovalari orqali parol ishlatmasdan kirish imkonini beradi.
- Ularning afzallik va kamchiliklari haqida gapirganda, har bir autentifikatsiya usuli o‘ziga xos qulayliklar va cheklovlarga ega. Ular xavfsizlikni ta’minlashda turlicha samaradorlik ko‘rsatadi:
- *Parolga asoslangan autentifikatsiya*
- - Afzalliklari: juda oddiy, keng tarqalgan va texnik jihatdan arzon.
- - Kamchiliklari: parollarni eslab qolish qiyin, kuchsiz parollar xavf tug‘diradi, va bu usul brute-force va phishing hujumlariga juda moyil.
- *Ikki bosqichli autentifikatsiya (2FA)*
- - Afzalliklari: xavfsizlik darajasi ancha yuqori, parol o‘g‘irlansa ham tizimni buzish qiyinlashadi.
- - Kamchiliklari: SMS-kodlar ushlanib qolishi yoki soxtalashtirilishi mumkin, va bu qo‘shimcha vaqt talab qiladi.
- *Biometrik autentifikatsiya*
- - Afzalliklari: noyob, takrorlanmaydigan, qulay va tez.

- Kamchiliklari: maxfiylik bilan bog‘liq xavotirlar, biometrik ma’lumotlar buzilsa tiklab bo‘lmaydi, va ba’zan aniqlikdagi xatolar kuzatiladi.

Token asosidagi autentifikatsiya

- Afzalliklari: yuqori xavfsizlik va apparat darajasida himoya.
- Kamchiliklari: token yo‘qolsa, kirish imkoni cheklanadi va qo‘shimcha xarajat talab qiladi.

Parolsiz autentifikatsiya

- Afzalliklari: parolga ehtiyoj qolmaydi, xavfsizlik darajasi sezilarli oshadi va foydalanuvchi uchun qulay.
- Kamchiliklari: kalitlarni boshqarish murakkab bo‘lishi mumkin, ba’zi platformalarda esa texnik integratsiya qiyin.

Yuqoridagi tahlildan ko‘rinib turibdiki, autentifikatsiya tizimlari rivojlanayotgan bo‘lsa-da, ular hali ham turli zaifliklarga ega. Ayniqsa markazlashgan parolga asoslangan usullar kiberxavfsizlik talablarini to‘liq qondira olmaydi. Shu sababli, decentralizatsiyaga asoslangan blockchain yondashuvi zamonaviy ehtiyojlarga javob beruvchi yanada ishonchli autentifikatsiya mexanizmi sifatida ko‘riladi.

BLOCKCHAIN TEXNOLOGIYASINING ASOSIY TAMOYILLARI

Blockchain – bu markazlashmagan, o‘zgarmas va kriptografik himoyalangan ma’lumotlar bazasi bo‘lib, autentifikatsiya tizimlarini xavfsiz va ishonchli qilishda muhim rol o‘ynaydi.

Taqsimlangan reyestr (Distributed Ledger) barcha ma’lumotlarni bir nechta tugunlarda saqlaydi, bu esa tizimni buzish qiyinlashtiradi va “single point of failure” muammosini hal qiladi. Konsensus algoritmlari (PoW, PoS, PBFT) esa ma’lumotlarning haqiqiyligini va o‘zgarmasligini ta’minlaydi.

O‘zgarmaslik (immutability) tamoyili bloklar bir marta yozilgach, ularni o‘zgartirishni imkonsiz qiladi. Har bir blok bir-biriga hash orqali bog‘lanadi, raqamli imzo va asimmetrik kriptografiya esa foydalanuvchi identifikatsiyasini xavfsiz qiladi.

Smart-kontraktlar esa autentifikatsiya jarayonini avtomatlashtiradi: ro‘yxatdan o‘tish, ruxsat darajalarini boshqarish, login va token yaratish kabi amallarni markazsiz va shaffof tarzda bajaradi. Natijada, tizim ishonchli, buzib bo‘lmas va samarali ishlaydi.

AN’ANAVIY AUTENTIFIKATSIYA TIZIMLARIDAGI XAVFSIZLIK TAHDIDLARI

An’anaviy autentifikatsiya tizimlari, asosan login-parol mexanizmi orqali ishlaydi, lekin ular turli kiberxavfsizlik tahdidlari bilan duch keladi.

1. *Parollarni o‘g‘irlash (Credential theft)*

Foydalanuvchilar parollarni eslab qolish uchun oddiy va qayta ishlatiladigan parollardan foydalanadi. Shu sababli, xakerlar phishing, keylogger yoki ma’lumotlar bazasiga hujum orqali parollarni o‘g‘irlashi mumkin. Bu foydalanuvchi hisoblariga noqonuniy kirish va shaxsiy ma’lumotlarning oshkor bo‘lishiga olib keladi.

2. *MITM, phishing va brute-force hujumlar*

- MITM (Man-in-the-Middle): Tarmoq orqali uzatilayotgan ma’lumotlar o‘rtadagi

xaker tomonidan ushlanadi va manipulyatsiya qilinadi.

- Phishing: Foydalanuvchidan soxta sayt yoki elektron pochta orqali login va parolni olishga uriniladi.
- Brute-force: Xaker tizimga kirish uchun barcha mumkin bo‘lgan kombinatsiyalarni sinab ko‘radi.

3. *Single point of failure muammosi*

Ko‘plab tizimlarda autentifikatsiya ma’lumotlari markaziy serverda saqlanadi. Agar server buzilsa yoki xaker tomonidan qo‘lga tushsa, barcha foydalanuvchi ma’lumotlari xavf ostida qoladi. Shu bilan tizimning butun ishlash barqarorligi yo‘qoladi.

4. *Ma’lumotlar bazasining buzilishi*

Server yoki ma’lumotlar bazasiga hujum qilinsa, foydalanuvchilarning shaxsiy ma’lumotlari, login va parollar, tranzaksiyalar tarixi o‘g‘irlanishi mumkin. Bu nafaqat moliyaviy, balki reputatsion zarar ham keltiradi.

Shu sababli, an’anaviy autentifikatsiya tizimlari bugungi kunda yuqori xavfsizlik talablarini qondira olmaydi. Ularning zaifliklari foydalanuvchi ma’lumotlarini

BLOCKCHAIN ASOSIDA AUTENTIFIKATSIYA TIZIMINI YARATISH KONSEPSIYASI

Hozirgi zamon autentifikatsiya tizimlari, masalan, parol va server bazasi, ko‘plab zaifliklarga ega. Shu sababli, markazlashmagan, kriptografik va o‘zgarmaslik xususiyatlariga ega tizimlar tez sur'atlar bilan rivojlanmoqda. Bu kontekstda, blockchain asosida autentifikatsiya foydalanuvchi identifikatsiyasini yangi darajaga olib chiqish imkonini beradi.

Yuqoridagi afzalliklar asosida, quyidagi tushunchalar va mexanizmlar yordamida tizim konsepsiyasini yaratish mumkin:

Parolsiz autentifikatsiya modeli / Public-Private key juftligi

Autentifikatsiya jarayonida an’anaviy parol o‘rniga public/private key juftligi ishlatiladi. Foydalanuvchi ro‘yxatdan o‘tganda, public key blockchain reyestriga yoziladi, private key esa faqat foydalanuvchida saqlanadi.

Login qilish jarayonida foydalanuvchi private key bilan ma’lumot (masalan, nonce yoki login so‘rovi) ni imzolaydi; server yoki xizmat public key yordamida imzoni tekshiradi. Agar imzo mos kelsa, foydalanuvchining haqiqiyligi tasdiqlanadi. Bu model parolni eslab qolish yoki saqlash zaruratini yo‘qotadi va credential theft (parol o‘g‘irlash) muammosini bartaraf etadi.

Bu yondashuv “passwordless authentication” deb ataladi va u ko‘pincha blockchain autentifikatsiyasining poydevorini tashkil etadi.

Smart-kontraktlarning roli

Autentifikatsiya va avtorizatsiya jarayonlarini boshqarish uchun smart-kontraktlar ishlatilishi mumkin. Smart-kontraktlar avtorizatsiya qoidalari, ruxsat darajalari (access level), foydalanuvchi statusini nazorat qilish kabi logikani kod shaklida saqlaydi va avtomatik bajaradi.

Misol sifatida, foydalanuvchi bir martalik ro‘yxatdan o‘tish, keyin login qilish, sessiya boshqaruvi, kirish huquqlarini tekshirish kabi jarayonlar smart-kontrakt orqali avtomatik va

xavfsiz tarzda amalga oshiriladi — bu markazlashtirilgan server va ortiqcha intervenerlarsiz ishlashni ta’minlaydi.

Shunday qilib, tizimde identifikatsiya, autentifikatsiya va avtorizatsiya jarayonlari blockchain-da shaffof, o‘zgarmas va ishonchli holatda boshqariladi.

Maxfiylik va xavfsizlik mexanizmlari

Public-private key kriptografiyasi va raqamli imzo ishlatiladi — foydalanuvchi private key’ini faqat o'zi biladi, public key esa blockchain orqali umumiy. Bu yordamida identity spoofing, credential theft va parolga asoslangan hujumlar oldini olish mumkin.

Bazaga parollar emas, balki kriptografik kalitlar yoki imzolar saqlanadi. Shunday ekan, agar server buzilsa ham — foydalanuvchi private key’i bo'lmasa, hujumchi tizimga kira olmaydi.

Smart-kontraktlar va blockchain reyestri o'zgarmas va shaffof bo'lganligi sababli, autentifikatsiya tarixini kuzatish va audit olib borish mumkin — har qanday manipulyatsiya darhol aniqlanadi.

Ba'zi ilg'or tajribalarda — biometrik ma'lumotlar yoki multi-factor autentifikatsiya elementlari bilan birgalikda blockchain ishlatilmoqda, bu esa maxfiylikni saqlagan holda yuqori darajadagi identifikatsiyani ta'minlaydi.

 Nima uchun bu yondashuv samarali?

✓ Parolga bog'liq zaifliklar yo'q — credential theft, brute-force, phishing singari xatarlar kamayadi.

✓ Tizim markazga bog'liq emas — markazlashtirilmagan boshqaruv tufayli single point of failure muammosi yo'q.

✓ Shaffoflik va audit mumkin — har qanday autentifikatsiya harakati blockchain’da yoziladi, soxtalashtirish deyarli imkonsiz.

✓ Foydalanuvchi shaxsiy ma'lumotlarini nazorat qiladi — public key umumiy, private key esa faqat foydalanuvchi qo'lida, shuning uchun shaxsiy maxfiylik saqlanadi.

TAKLIF ETILAYOTGAN TIZIM ARXITEKTURASI

Taklif etilayotgan autentifikatsiya tizimi markazlashmagan va parolsiz ishlash prinsipiga asoslanadi. Tizim arxitekturasi foydalanuvchi qurilmasi, backend server va blockchain tarmog‘i o‘rtasidagi o‘zaro aloqalarni o‘z ichiga oladi.

Foydalanuvchi qurilmasi:

- Har bir foydalanuvchiga shaxsiy private key beriladi, public key esa blockchain’da saqlanadi.

- Foydalanuvchi qurilmasi login qilish, sessiya boshqaruvi va ma’lumotlarni shifrlash jarayonlarini amalga oshiradi.

- Parolsiz autentifikatsiya orqali foydalanuvchi haqiqiyligi tasdiqlanadi.

Backend va blockchain o‘rtasidagi aloqalar:

- Backend server foydalanuvchi qurilmasidan kelgan imzo va so‘rovlarni qabul qiladi.

- Tizim smart-kontraktlar orqali foydalanuvchi sessiyasini va ruxsat darajasini boshqaradi.

- Blockchain tarmog‘ida barcha tranzaksiyalar va autentifikatsiya jarayonlari o‘zgarmas reyestrda saqlanadi, shu orqali markazlashmagan, shaffof va ishonchli tizim yaratiladi.

Kalitlarni boshqarish (Key Management):

- Private key foydalanuvchi qurilmasida saqlanadi va hech qachon serverga yuborilmaydi.

- Public key blockchain tarmog‘ida yoziladi va tizimda autentifikatsiya tasdiqlash uchun ishlatiladi.

- Key management jarayoni foydalanuvchi maxfiyligini maksimal darajada himoya qiladi.

Ma’lumot oqimi diagrammalari (Flow Diagrams):

Login va autentifikatsiya jarayoni foydalanuvchi qurilmasidan boshlanadi → imzo yuboriladi → backend tomonidan tekshiriladi → smart-kontraktlar orqali ruxsat beriladi → sessiya boshqariladi.

Tizimdagi barcha tranzaksiyalar blockchain tarmog‘ida qayd etiladi va o‘zgarmas xolda saqlanadi, bu esa tizimning hujumlarga chidamliligini oshiradi

AUTENTIFIKATSIYA JARAYONINING ALGORITMI

Blockchain asosida autentifikatsiya jarayoni odatda quyidagi bosqichlardan iborat bo‘ladi.

1. Ro‘yxatdan o‘tish: Foydalanuvchi tizimga birinchi marta ulanayotganda, public/private key juftligi yaratiladi. Public key blockchain reyestriga yoziladi, private key esa foydalanuvchida saqlanadi. Bu jarayon foydalanuvchining o‘zini markaziy serverga bog‘lamasdan identifikatsiya qilishiga imkon beradi.

2. Nonce asosida imzolash: Har bir autentifikatsiya so‘rovi uchun tizim tasodifiy nonce (bir martalik raqam) yuboradi. Foydalanuvchi private key bilan nonce’ni imzolaydi va serverga yuboradi. Bu jarayon login harakatining noyob va qayta ishlanmasligini ta’minlaydi.

3. Imzoni tekshirish (verification): Server foydalanuvchining public key’idan foydalanib yuborilgan imzoni tekshiradi. Agar imzo to‘g‘ri bo‘lsa, foydalanuvchining haqiqiyligi tasdiqlanadi. Bu bosqich credential theft va spoofing xatarini kamaytiradi.

4. Ruxsat berish va seansni boshqarish: Tasdiqlashdan so‘ng foydalanuvchiga kerakli resurslarga kirish huquqi beriladi va sessiya yaratiladi. Smart-kontraktlar yoki blockchain logikasi orqali seans boshqaruvi shaffof va xavfsiz tarzda amalga oshiriladi.

Ushbu algoritm markazlashmagan, parolsiz va kriptografik jihatdan himoyalangan tizimni ta’minlaydi. Har bir bosqich foydalanuvchi identifikatsiyasini ishonchli qiladi, login ma’lumotlari buzilsa ham tizim xavfsizligini saqlaydi, va barcha autentifikatsiya harakatlari blockchain’da shaffof tarzda yoziladi.

TIZIMNI ISHLAB CHIQISH VA PROTOTIP YARATISH

Blockchain asosidagi autentifikatsiya tizimini yaratishda avvalo platformani tanlash muhimdir: masalan, Ethereum, Hyperledger yoki Polygon. Tanlangan platforma tizimning talablariga, xavfsizlik darajasiga va tranzaksiya tezligiga mos kelishi kerak.

Keyin, tizimning asosiy logikasi — smart-kontraktlar kodi ishlab chiqiladi. Bu kontraktlar foydalanuvchi ro‘yxatdan o‘tishi, login qilish, ruxsat darajalarini boshqarish va sessiya nazoratini avtomatik ravishda amalga oshiradi. Kod kriptografik xavfsizlik va o‘zgarmaslik tamoyillarini hisobga olgan holda yoziladi.

Shundan so‘ng, blockchain smart-kontraktlari web yoki mobil ilova bilan integratsiya qilinadi. Foydalanuvchi interfeysi intuitiv bo‘lib, parolsiz autentifikatsiya jarayonini qo‘llab-quvvatlaydi, private key’lar faqat foydalanuvchi qurilmalarida saqlanadi, public key esa blockchain’da yoziladi.

Oxirida tizim testlanadi va eksperiment natijalari tahlil qilinadi. Testlar xavfsizlik, autentifikatsiya tezligi, tizim barqarorligi va foydalanuvchi tajribasini o‘z ichiga oladi. Eksperimentlar natijasi blockchain asosidagi autentifikatsiya prototipining samaradorligini, parolsiz va markazlashmagan tizim sifatidagi ustunligini tasdiqlaydi.

XAVFSIZLIK TAHLILI VA SAMARODORLIK BAHOSI

Blockchain asosidagi autentifikatsiya tizimining samaradorligi va xavfsizligi an’anaviy login-parol usullaridan ancha farq qiladi. Ushbu bo‘limda tizimning hujumlarga chidamliligi, skalabilligi va operatsion samaradorligi batafsil tahlil qilinadi.

Hujumlarga chidamlilik

1. MITM (Man-in-the-Middle) hujumlariga chidamlilik:

Parolsiz autentifikatsiya modeli, public/private key juftligi va nonce asosida imzolash tufayli MITM hujumlarining ta’siri sezilarli darajada kamayadi. Har bir so‘rov yagona nonce bilan bog‘langan va blockchain orqali tasdiqlanadi, shuning uchun agar xaker o‘rtadagi trafikni ushlasa ham, imzoni qayta ishlata olmaydi.

2. Replay attack’ga chidamlilik:

Har bir autentifikatsiya so‘rovi noyob nonce bilan amalga oshiriladi. Shu sababli, avvalgi autentifikatsiya paketlarini qayta yuborish tizimga kirishga olib kelmaydi.

3. Identity spoofing va phishingga chidamlilik:

Private key faqat foydalanuvchida saqlanadi, public key esa blockchain’da yoziladi. Shuning uchun, agar xaker foydalanuvchi nomi va login ma’lumotlarini bilsa ham, private key’ni ushlay olmasa, tizimga kirish imkoniyati yo‘q.

Skalabillik, tranzaksiya narxi va kechikish

- Skalabillik: Permissioned blockchain’lar, masalan, Hyperledger, katta korporativ tizimlar uchun yuqori tranzaksiya tezligini va past kechikishni ta’minlaydi. Biroq, public blockchain’larda (masalan, Ethereum, Polygon) tranzaksiya soni oshgan sari kechikishlar paydo bo‘lishi mumkin.
- Tranzaksiya narxi: Public blockchain’larda har bir autentifikatsiya yoki login jarayoni “gas fee” orqali xarajat talab qiladi. Private blockchain’larda esa bu xarajatlar minimal yoki umuman yo‘q.
- Kechikish (latency): Bu, asosan, konsensus algoritmining turiga bog‘liq: PoW yuqori kechikish bilan ajralib turadi, PoS va PBFT esa tezroq tasdiqlash imkonini beradi.

An’anaviy tizim bilan taqqoslash

Parametr	*An’anaviy tizim*	*Blockchain tizimi*
Xavfsizlik	Parolga bog‘liq, MITM, phishing xavfi yuqori	Parolsiz, kriptografik himoyalangan, MITM, replay chidamli
Markazlashuv	Markaziy server	Markazlashmagan (distributed)
O‘zgarmaslik	Yo‘q	Ha (immutable ledger)
Skalabillik	Server yukiga bog‘liq	Konsensus algoritmi bilan o‘lchanadi
Audit va shaffoflik	Cheklangan	Har bir tranzaksiya yoziladi, o‘zgarmas
Foydalanuvchi maxfiyligi	Server nazoratida	Private key faqat foydalanuvchida saqlanadi

Afzalliklar va cheklovlar

Afzalliklar:

- Yuqori xavfsizlik va buzib bo‘lmaslik; MITM, spoofing, replay hujumlariga chidamli.
- Markazlashmagan boshqaruv tufayli single point of failure muammosi yo‘q.
- Parolsiz autentifikatsiya foydalanuvchi qulayligini oshiradi.
- Har bir tranzaksiya shaffof va audit qilinadigan loglarda saqlanadi.

Cheklovlar:

- Public blockchainlarda tranzaksiya xarajatlari (gas fee) va kechikish mavjud.
- Konsensus algoritmlari tufayli tizim resurs talab qiladi.
- Smart-kontraktlar noto‘g‘ri yozilgan bo‘lsa, xavfsizlik muammolari yuzaga kelishi mumkin.

Blockchain asosidagi autentifikatsiya tizimi an’anaviy login-parol mexanizmiga qaraganda xavfsizligi, shaffofligi va ishonchliligi bilan ustun. Ammo platforma tanlovi, konsensus algoritmi va tranzaksiya xarajatlari kabi operatsion cheklovlar hisobga olinishi zarur.

XULOSA

Blockchain asosida yaratilgan autentifikatsiya tizimi an’anaviy login-parol mexanizmlaridan ko'ra xavfsizroq, ishonchliroq va markazlashmagan yechimni taqdim etadi. Parolsiz autentifikatsiya modeli public/private key juftligi yordamida foydalanuvchining haqiqiyligini tasdiqlaydi, smart-kontraktlar esa ruxsat darajalarini va sessiya boshqaruvini avtomatlashtiradi.Bu tizim o‘zgarmas blockchain reyestrida ishlaydi, hujumlarga chidamli va audit qilinadigan bo‘lib, foydalanuvchi maxfiyligini maksimal darajada himoya qiladi. Shunday qilib, blockchain asosidagi autentifikatsiya tizimi zamonaviy kiberxavfsizlik talablariga javob beradigan, samarali va kelajakdagi raqamli tizimlar uchun barqaror yechim sifatida ko‘riladi.

REFERENCES:

1. Li, J. (2024). A review of identity authentication based on blockchain technology.
2. Asif, M., Aziz, Z., Bin Ahmad, M., Khalid, A., Waris, H.A., Gilani, A. (2022). Blockchain-Based Authentication and Trust Management Mechanism for Smart Cities.
3. Sulemana Awal et al. (2024). Decentralized Authentication for Enhanced Security.
4. Sultanpure, K.A., Gangurde, S., Gawale, S. (2024). Blockchain Based Decentralized User Identity Verification System.
5. Salman, T., Zolanvari, M., Erbad, A. et al. (2018). Security Services Using Blockchains: A State of the Art Survey.
6. Alexopoulos, N., Daubert, J., Mühlhäuser, M., Habib, S. (2017). Beyond the Hype: On Using Blockchains in Trust Management for Authentication.
7. Moosavi, N., Taherdoost, H. (2023). Blockchain Technology Application in Security: A Systematic Review.
8. Abbas, S., Talib, M.A., Ahmed, A., Khan, F., Ahmad, S., Kim, D.-H. (2021). Blockchain-Based Authentication in Internet of Vehicles: A Survey.