Raqamli Infratuzilma uchun Cross-Chain Xavfsizlik Arxitekturasi: Relayer Validator Nazorati va Anomaliya Monitoringi

Xaitbayev Azizbek Pirnazarovich
UrDU “Axborot xavfsizligi” kafedrasi o’qituvchisi
Rustamova Dilshoda Islomxo‘ja qizi
UrDU “Axborot xavfsizligi” talabasi

Annotatsiya. Cross-chain bridge’lar (qulflash va yaratish, yo`q qilish va chiqarish) turli blokcheynlar o‘rtasida aktiv almashinuvini ta’minlaydi, ammo relayer/validator va trust assumptions sababli qo‘shimcha xavflarni keltirib chiqaradi. Ushbu tezisda bridge uchun tahdid modeli qisqacha yoritilib, anomaliya aniqlash orqali shubhali tranzaksiyalarni erta aniqlash va xavfni kamaytirish choralarini (nazorat, cheklovlar, verifikatsiya) qo‘llash yondashuvi bayon etiladi.

Kalit so‘zlar: cross-chain bridge, qulflash va yaratish, yo`q qilish va chiqarish, trust assumptions, tahdid modeli, relayer/validator, anomaliya aniqlash, xatarni kamaytirish, raqamli infratuzilma

Ko‘p zanjirli raqamli infratuzilma tez rivojlanayotgan sharoitda cross-chain bridge’lar aktivlar va xabarlarni turli blokcheynlar o‘rtasida uzatishning tayanch mexanizmlaridan biri bo‘lib qoldi. Biroq bridge’lar yuqori qiymat jamlanadigan (TVL) “kritik tugun” sifatida ko‘pincha eng yirik hujumlar va ekspluatatsiyalar markazida turadi. Ushbu tezis qulflash va yaratish, yo`q qilish va chiqarish arxitekturasining amaliy dizaynini, unga bog‘liq trust assumptions (yakuniylik, validatorlar halolligi, kalitlar xavfsizligi, yangilanish boshqaruvi)ni va keng tarqalgan xatoliklarni tahdid modeli asosida tahlil qiladi. Natijada kriptografik tekshirish, formal tekshiruvlar va AI-asosli anomaliya aniqlashga tayangan xavflarni kamaytirish yo‘li taklif etiladi.

Bridge arxitekturasida xavfning asosiy manbalari uch yo‘nalishda jamlanadi: (i) xabar/tasdiqlash tekshiruvining noto‘g‘ri qurilishi (qayta uzatish hujumi, soxtalashtirish,blok sarlavhasi va tizim holatini tekshiruvining to‘liq bajarilmasligi), (ii) ishonch qatlamining markazlashuvi (relayer/validatorlarning yashirin hamkorligi orqali tizim xavfsizligiga tahdid, multisig chegarasining zaifligi), (iii) operatsion

boshqaruv va boshqaruv(admin huquqlari, yangilanish orqali yashirin kirish yo‘li, kalitlar kompрometatsiyasi). Bundan tashqari, manba zanjir yakuniylik talablari aniq belgilanmagan bo‘lsa, qayta tashkil qilish holatlari noto‘g‘ri “tasdiqlangan” o`tkazishlarga olib kelishi mumkin. Bridge’lar raqamli transformatsiya infratuzilmasiga bevosita ta’sir qilgani uchun ular bo‘yicha xavflarni tizimli boshqarish milliy raqamli rivojlanish strategiyalari bilan hamohang vazifadir.

Taklif etilayotgan yondashuv bridge dizaynini “arxitektura + tahdid modeli + nazoratlar” zanjiri sifatida quradi:

Trust assumptions’ni aniq yozish: yakuniylik mezoni, validator relayer modeli, kalitlarni saqlash (MPC/HSM), administrator va yangilashni boshqarish mexanizmlari (vaqt qulfi, audit izlari), xabar yaxlitligi (bir martalik raqam, domenni ajratish).

Xavflarni kamaytirish nazoratlari:

- Tizimni ishlashi uchun kamroq ishonch talab qiladigan xavfsiz tekshiruv:imkon qadar mijoz/ma’lumotni ko‘rsatmasdan uning haqiqiyligini tekshirish yoki kuchli tekshiruvga yaqinlashish; markazlashuv xavfini kamaytirish.
- **Formal tekshiruv va qat’iy validatsiya:** bridge xatti-harakatini formal model asosida tekshirish, “fail-safe” tamoyilini isbotlash.
- **AI-asosli monitoring (anomaliya aniqlash):** zanjirli izlar (hodisalar, tranzaksiya graflari, relayer signallari) bo‘yicha hujum xulqini aniqlash, xavfni baholash va avtomatik cheklovlar (kunlik chegara, avtomatik o'chirish, qo‘shimcha tasdiq).
- **Operatsion mustahkamlash:** ko‘p relayerli arxitektura, narx chegarasi, hodisaga javob berish bo'yicha qo'llanma, doimiy audit +xatolarni topib mukofot olish dasturi.

1-jadval

“Tahdid → Nazorat” moslashtirish jadvali

Tahdid ssenariysi	Eng muhim nazoratlar	Kuzatuv signallari
Soxta xabar	Tekshiruvchi qat’iyligi, ma’lumotni oshkor qilmasdan tekshiradigan yengil mijoz yoki chegara, domenni ajratish	Noodatiy xabar manbasi, imzolovchi kombinatsiyasi, tasdiqlash formatidagi xatolik

Javob	Bir martalik raqamlar ketma-ketligini saqlash,bir necha marta bajarilsa ham natija o‘zgarmaslik xossasi	Bir xil bir martalik raqam bilan takror urinishlar
Kirishni boshqarish	RBAC,vaqt qulfi, ko‘p tomonlama hisoblash, o‘zgarmas asos	Admin chaqiruvlar soni, noodatiy yangilash takliflari
Ta’minotning siljishi	O‘zgarmas shartni tekshirish, moslashtirish vazifasi, xavfsizlik to‘xtatuvi	Saqlash balanslari va umumiy ta'minot tafovuti
Qayta kirish/mantiqiy xato	qayta kirishni oldini oluvchi himoya, tekshiruv/xatolarni qidirish, tashqi chaqiriqlarni kamaytirish	Bir tranzaksiya ichida ko‘p chaqiruv, **kutilmagan yoki murakkab chaqiruv grafigi**.
xizmat ko‘rsatishni rad etish(DoS)/faollik	bir nechta vositachilar,uzilish, so‘rovlar tezligini cheklash	relayer kechikishi keskin oshishi, navbatdagi ishlarning ortiqcha yig‘ilishi

Cross-chain bridge’lar raqamli infratuzilmaning strategik qismi bo‘lib, ularning xavfsizligi faqat smart-kontrakt darajasidagi tekshiruv bilan cheklanmaydi: taxminlarga ishonishni formal ifodalash, isbotni tekshirishni kuchaytirish, boshqaruv va kalit boshqaruvini qat’iylashtirish hamda AI-asosli real-vaqt monitoringni joriy etish birgalikda qo‘llanganda xavflar sezilarli kamayadi. Kelgusida ushbu yondashuv raqamli infratuzilmani kengaytirishda (ko‘p zanjirli servislar, raqamli aktivlar, davlat va xususiy sektordagi integratsiyalar) xavfsizlikni proaktiv boshqarish uchun amaliy metodik asos bo‘lib xizmat qiladi.

Foydalanilgan adabiyotlar ro‘yxati

1. O‘zbekiston Respublikasining Qonuni “Axborotlashtirish to‘g‘risida” (11.12.2003).
2. O‘zbekiston Respublikasining Qonuni “Elektron hukumat to‘g‘risida” (2015).

3. O‘zbekiston Respublikasining Qonuni “Shaxsga doir ma’lumotlar to‘g‘risida” (02.07.2019, O‘RQ-547).
4. O‘zbekiston Respublikasi Prezidentining Farmoni “Raqamli O‘zbekiston — 2030” strategiyasini tasdiqlash… (05.10.2020, PF-6079).
5. Xolov A. “Raqamli O‘zbekiston – 2030” strategiyasi va uni amalga oshirish… (2024).
6. ACM: “A Security Analysis of Web3.0 Cross-Chain Bridges” (2025).
7. Marić F. va boshq. “Formal Verification of a Fail-Safe Cross-Chain Bridge” (FMBC 2025).
8. Lin D. va boshq. “BridgeShield: Enhancing Security for Cross-chain Bridge…” (arXiv, 2025).