BLOKCHEYN TEXNOLOGIYASIGA ASOSLANGAN MARKAZLASHTIRILMAGAN DNS-SERVERNI ISHLAB CHIQISH

Xabibullayev Jahongirbek Doniyorbek o‘g‘li
Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti,
Chunayev Norquvvat Eshquvat o‘g‘li
Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti

Annotatsiya. *Ushbu maqolada klassik DNS-serverlardan foydalanish ssenariylari ko‘rib chiqilgan va ular bilan bog‘liq mavjud kamchiliklar yoritilgan. Muqobil yechim sifatida blokcheyn texnologiyasiga asoslangan taqsimlangan (markazlashmagan) DNS-server tahlil qilingan, u klassik DNS-serverlar bilan axborot xavfsizligi nuqtai nazaridan solishtirilgan, uning afzalliklari va kamchiliklari ajratib ko‘rsatilgan. Shuningdek, taqsimlangan DNS-serverni ishlab chiqish bilan bog‘liq muammolar yoritilgan va ularni hal qilish bo‘yicha takliflar berilgan.*

Kalit so‘zlar: axborot xavfsizligi, DNS, taqsimlangan reyestr, blokcheyn, Ethereum

Kirish

Ko‘plab holatlarda o‘z DNS-serveriga egalik qilish zarurati yuzaga keladi. Masalan, bu korporativ tarmoq va uning intraneti, tashkilotda qayta ishlanayotgan DNS nomlarini cheklash masalalari yoki shunchaki mustaqil, o‘ziga tegishli DNS-serverga ega bo‘lish istagi bo‘lishi mumkin. Biroq, o‘z DNS-serverini yaratishda bir qator muammolar paydo bo‘ladi:

DNS-serverning uzluksiz ishlashini ta’minlash (barqarorlik masalasi). Agar yagona DNS-serverga xizmatdan voz kechish (DoS – Denial of Service) turidagi hujum amalga oshirilsa, ushbu serverga bog‘langan butun infratuzilma faoliyatini davom ettira olmaydi — ayniqsa, agar tizim ishlashi server tomonidan qayta ishlanadigan domen nomlariga bog‘liq bo‘lsa.

Rekursiv DNS-serverlarning ildiz (root) DNS-serverlariga bog‘liqligi. Agar DNS-server ildiz server bo‘lmasa, unda mavjud bo‘lmagan yozuvlar uchun u yuqori darajadagi DNS-serverga murojaat qiladi. Shu sababli, agar ildiz DNS-serverlar to‘plami ishlamay qolsa, ma’lum vaqt o‘tgach (kesh eskirganidan so‘ng), unga bog‘liq pastki darajadagi DNS-serverlar ham ishlamay qoladi. Amaldagi ildiz DNS-serverlari haqidagi ma’lumotni https://root-servers.org saytidan topish mumkin. Aytib o‘tish lozimki, Rossiya Federatsiyasi hududida bu bog‘liqlik yanada dolzarb bo‘lishi mumkin.

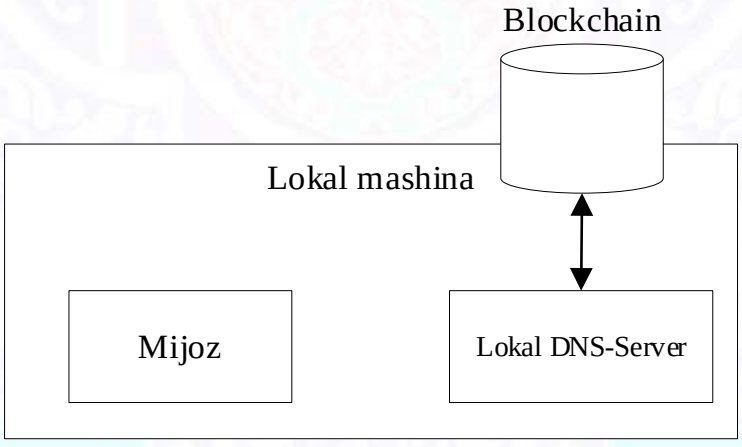
DNS-serverlarning tashqi regulyatorga bog‘liqligi. Hozirda ko‘plab kompaniyalar VPN xizmatlarini taklif qilayotganda o‘z DNS-serverlarini ham foydalanishni tavsiya qiladilar. Ular buni foydalanuvchi qiziqish doirasi haqida ma’lumot olish maqsadida DNS-so‘rovlarni tahlil qilish imkoniyati bilan asoslaydilar. Bu haqiqatga yaqin, biroq tashqi regulyator yoki boshqaruvchi tashkilot bosimi ostida DNS-server nafaqat tahlil qilishi, balki ba’zi so‘rovlarni soxtalashtirishi yoki umuman ko‘rib chiqmasligi ham mumkin. Soxtalashtirishdan sertifikatlar yordamida himoyalanish mumkin bo‘lsa-da, domen nomini qayta ishlashdan bosh tortish holatida biz muayyan ma’lumotlarga kirish imkoniyatini yo‘qotishimiz mumkin.

sDNS-serverlarga qarshi mumkin bo‘lgan hujumlar. DNS keshini zaharlash (cache poisoning) turidagi hujumlar ma’lum bo‘lib, bu holatda yuqori darajadagi DNS-serverdan rasmiy javob kelguniga qadar serverga ataylab noto‘g‘ri javob yuboriladi. Bunday hujumlar nafaqat mahalliy yoki ofis DNS-serverlariga, balki ildiz bo‘lmagan yuqori darajadagi serverlarga ham nisbatan amalga oshirilishi mumkin. Shuningdek, yuqori darajadagi DNS-serverlardan birining buzilishi ehtimolini ham inkor etib bo‘lmaydi.

Usullar va materiallar

Oldingi bo‘limlarda keltirilgan barcha muammolarni blokcheyn texnologiyasiga asoslangan taqsimlangan (markazlashmagan) DNS-server orqali hal qilish taklif etiladi.

1. Quyidagi arxitektura taklif qilinmoqda (1-rasm).



1-rasm. Taqdim etilayotgan taqsimlangan DNS-server arxitekturasi

DNS-server (Name-server, nameserver, NS) — bu foydalanuvchilar ishlatadigan domen nomlarini kompyuterlar uchun tushunarli bo‘lgan IP-manzillarga yoki aksincha, IP-manzillarni domen nomlariga aylantiruvchi serverdir. Odatda NS va DNS-server atamalari orasida farq qilinmaydi.

Taklif etilayotgan sxemada mijoz (klient) tashqi DNS-server bilan emas, balki ma’lumotlarni to‘g‘ridan-to‘g‘ri taqsimlangan tarmoqdan so‘raydigan mahalliy (lokal) DNS-server bilan o‘zaro aloqada bo‘ladi.

Yuqorida ta’riflangan muammolar quyidagi tarzda hal etiladi:

DNS-serverning uzluksiz ishlashini ta’minlash (barqarorlik). Taqsimlangan tarmoqlar alohida ishlovchi serverlarga nisbatan ancha barqarorroq. Yagona serverni ishdan chiqarish oson, biroq bir nechta tugun (node) ishlaydigan taqsimlangan tarmoqni ishdan chiqarish juda mushkul.

Rekursiv DNS-serverlarning ildiz serverlariga bog‘liqligi. Bu yerda mahalliy DNS-server uchun manba sifatida taqsimlangan tarmoq xizmat qiladi. Bu tarmoq hech qachon yakka tartibda qandaydir mijoz uchun kirishni cheklash qarorini qabul qila olmaydi.

DNS-serverlarning tashqi regulyatorga bog‘liqligi. Masalan, Ethereum kabi markazlashtirilmagan taqsimlangan tarmoqda yagona regulyator yo‘q, bu esa tegishli xavf-xatarlardan xoli bo‘lish imkonini beradi.

DNS-serverlarga qarshi hujumlar. Mahalliy server dasturi mijoz bilan bir xil qurilmada joylashganligi sababli, unga qarshi ko‘plab hujumlar amalda imkonsiz bo‘ladi yoki bunday hujumlar mijoz qurilmasining o‘zini buzishni talab qiladi. So‘nggi holatda esa DNS-serverni himoya qilish mantiqsiz, chunki yomon niyatli shaxs butun tizim ustidan nazoratga ega bo‘ladi.

Blokcheyn texnologiyasi (Inglizcha *Blockchain*, bevosita tarjimada — *bloklar zanjiri*) — bu vaqt tamg‘alari bilan bog‘langan, o‘zgartirib bo‘lmaydigan yozuvlar (bloklar) ketma-ketligini yaratib beruvchi taqsimlangan reyestr texnologiyasidir. Bu texnologiya ma’lumotlar bazasi administratorini yoki markaziy saqlash joyini talab qilmaydi, va yangi yozuvlarni qo‘shish faqat tugunlar o‘rtasidagi konsensusga erishilgandagina amalga oshadi.

Shunday qilib, blokcheyn texnologiyasi markazlashtirilmagan DNS-server yaratish vazifasiga mos keladi va DNS yozuvlarini saqlovchi reyestrning uzluksizligi hamda yaxlitligini ta’minlaydi. Shu bilan birga, tashqi yoki ichki regulyatorlar bilan bog‘liq xavflarni yo‘q qiladi.

Biroq, blokcheyn texnologiyasi quyidagi xususiyatlarga ega bo‘lib, ularni DNS-serverni yaratishda e’tiborga olish lozim:

a) *Transaksiyalarni qayta ishlashda kechikishlar mavjud.* i-blok reyestrga qo‘shilgach, nafaqat ko‘pchilik tugunlar konsensusga kelishi kerak, balki i-blokdan keyin yana bir nechta (i+n) bloklar qabul qilinishi lozim. Bu jarayon tarmoq tomonidan 30 daqiqagacha vaqt olishi mumkin.

b) *Reyestrdan o‘qishdagi tarmoq javobi ham darhol bo‘lmaydi,* bu holat DNS-server ishlash tezligiga salbiy ta’sir ko‘rsatishi mumkin.

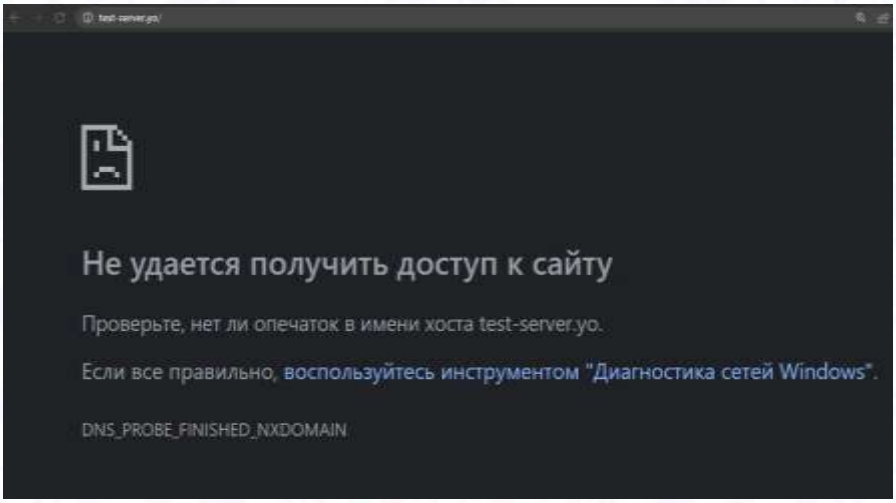
Natijalar

Ushbu ish natijasida avval tavsiflangan arxitekturaga muvofiq DNS-server ishlab chiqildi.

DNS-server ishini tekshirish uchun **test-server.yo** domeni tanlandi. Oldindan bu nom uchun **A-zapisi** qo‘shilgan bo‘lib, u **127.0.0.1** (localhost) manzilga yo‘naltirilgan edi. Hozirda ushbu manzilda, ya’ni **80-portda**, mahalliy server ishga tushirilgan va DNS-server ishlashi natijasida biz quyidagi natijani ko‘ramiz (2-rasm).

2-rasm. 127.0.0.1 manzilida 80-portda ishlayotgan server javobi

Hozirgi bosqichda tizim bu DNS-nomga IP-manzilni moslashtira olmayapti (3-rasm).



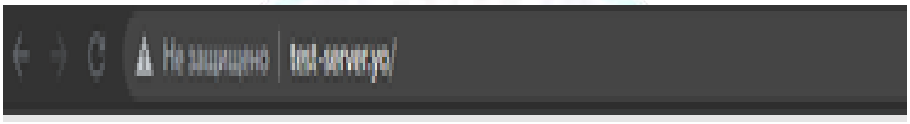
3-rasm. DNS-server o‘chirilgan, test-server.yo nomi aniqlanmagan

Endi biz DNS-serverni ishga tushiramiz, sahifani yangilaymiz va natijani ko‘ramiz (4-rasm).

4-rasm. DNS-server konsolida taqsimlangan tarmoqqa murojaat qilinganligi aks ettirilgan

DNS-server taqsimlangan tarmoqqa murojaat qilib, ilgari biz tomonidan kiritilgan **127.0.0.1** qiymatini o‘qidi, bu esa **localhost** yoki **mahalliy kompyuter** manziliga to‘g‘ri keladi.

Endi tekshirib ko‘ramiz: server ishga tushirilgandan so‘ng **test-server.yo** DNS-nomiga IP manzilni moslashtira oladimi (5-rasm).



5-rasm. DNS-server muvaffaqiyatli ishladi

Eksperimental tadqiqot doirasida taklif qilingan yondashuvni mavjud echimlar bilan solishtiruvchi tahlilda quyidagi xulosalarga keldik: taqsimlangan DNS-server ba’zi parametrlar bo‘yicha oddiy DNS-serverlardan ortda qoladi:

Yozuvlarni qo‘shish tezligi. Har bir tranzaksiya tarmoqda bir nechta bloklar tomonidan tasdiqlanishi va qat’iylanishi lozim. Yangi yozuvni blokcheynga kiritish vaqti 30 daqiqagacha cho‘zilishi mumkin.

Javob berish tezligi. Taqsimlangan tarmoqdan kelayotgan javoblar qanchalik tez bo‘lmasin, DNS-serverning to‘g‘ri ishlashi uchun yetarli darajada tez emas. Birinchi so‘rovda ham javob kelishini kutmasdan ishlashga majbur bo‘lish, holbuki tarmoqdan yana javob kelgach, DNS nomini qayta aniqlash zarurati tug‘iladi.

Yukni boshqarish masalasi. Ehtimol, serverni ishga tushirishda barcha ro‘yxatdan o‘tgan zonalarni so‘rab olish mumkin, ammo real tarmoq operatsiyalari pullik bo‘lgani uchun bu samarali bo‘ladimi-yo‘qligi noma’lum.

Birinchi darajali domenlarni cheklash zarurati. Resurslar chegaralanganligi sababli, taqsimlangan tarmoqqa barcha mavjud domenlar bo‘yicha so‘rov yuborish tarmoqni ortiqcha yuklaydi. Shu bois masalan, faqat “.yo” domenlarini qabul qilish tavsiya etiladi.

Xulosa

Ushbu ish doirasida quyidagi natijalarga erishildi:

- markazlashtirilmagan DNS-server konsepsiyasining afzalliklari va kamchiliklari baholandi.
- Ethereum blokcheyn platformasida taqsimlangan DNS-serverning muvaffaqiyatli prototipi yaratilib, uning ishlash imkoniyati namoyish etildi.
- yuqorida sanab o‘tilgan kamchiliklarga qaramay, ishlab chiqilgan server axborot xavfsizligini ta’minlash uchun zarur bo‘lgan yaxlitlik va mavjudlik xususiyatlariga ega.

Server quyidagi xususiyatlarni ta’minlaydi:

– taqsimlangan tarmoqlar alohida serverlarga nisbatan ancha bardoshli, birgina tugunni inaktiv qilish oddiy, tarmoqning ko‘p tugunini esa buzish deyarli imkonsiz.

– root DNS-serverlarga bog‘liqlikning yo‘qligi (mavjudlik). Mahalliy DNS-server manbai sifatida taqsimlangan tarmoq xizmat qiladi, u esa hech kim uchun yakka tartibda kirishni cheklay olmaydi. Shuning uchun har bir lokal DNS-server o‘rnatilgan qurilma uchun ildiz server vazifasini bajaradi.

– tashqi regulyatordan mustaqillik (yaxlitlik va mavjudlik). Ethereum platformasi yagona boshqaruvchi organni nazarda tutmaydi, bu esa tegishli xavflarni yo‘qqa chiqaradi.

– DNS hujumlariga chidamlilik (yaxlitlik). Mahalliy server dasturi mijoz kompyuterida ishlagani uchun aksar hujumlar imkonsiz yoki butun mijoz tizimini buzishni talab qiladi. Bunday holda DNS-serverni himoya qilmoqchining iloji qolmaydi, chunki hujumchi allaqachon mijoz tizimi ustidan to‘liq nazoratga ega bo‘ladi.

Umuman olganda, blokcheyn asosidagi taqsimlangan DNS-server gibrid yondashuv sifatida yuqori darajadagi xavfsizlik va mavjudlikni ta’minlaydi, ammo kechikish va yuk masalalarini hal etish uchun qo‘shimcha optimizatsiyalar talab etiladi.

Foydalanilgan adabiyotlar

1. Xabibullayev J.D., DDoS-hujumlarning oldini olishda blockchain texnologiyasining imkoniyatlarini tahlili // Лучшие интеллектуальные исследования, 2025-yil 26-fevral. Vol. 39, №-3. –b 121-131.
2. Chunayev N.E., Xabibullayev J.D., Application of blockchain technology to ensuring reliability and data security in the internet of things, “Moliya-kredit tizimini strategik rivojlantirishning muammolari va ustuvor yo‘nalishlari” mavzusida xalqaro ilmiy-amaliy konferensiya 2024-yil 25-aprel. –b. 27-29.
3. Natalia M., Alexander T., Vladimir B., Maniklal D., Blockchain Application for Cybersecurity Management - 2019. - 141-168 c. – Режим до- ступа: https://www.researchgate.net/publication/339720704.