BANKLAR O'RTASIDA KYC MA'LUMOTLARINI XAVFSIZ ALMASHISH UCHUN BLOKCHEYN ASOSIDAGI KRIPTOGRAFIK RUXSATLARNI BOSHQARISH MODELI

Janxojaev Asqar Ayxoja uli
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, stajyor-o'qituvchi.
Email: askarjankhojaev02@gmail.com

Aralbaev Islam Abatbay ulı
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, magistratura talabasi.
Email: islamaralbaev9@gmail.com
DOI:https://doi.org/10.5281/zenodo.23251958

Annotatsiya. Maqolada tijorat banklarida "Mijozingni bil" (KYC) tartib-taomillarini bajarishda bir mijoz hujjatlarining har bir bankda qayta yig'ilishi va tekshirilishi natijasida yuzaga keladigan ortiqcha xarajatlar hamda shaxsga doir ma'lumotlarni banklararo uzatishdagi xavfsizlik muammolari tahlil qilingan. Muammoni hal etish uchun xususiy ruxsat etilgan (permissioned) blokcheyn, aqlli shartnoma, salted xeshlash, psevdonim identifikatorlar va ochiq kalitli shifrlashga asoslangan ma'lumot almashish modeli taklif etilgan. Modelda hujjatlar blokcheynda saqlanmaydi, zanjirda faqat mijoz bergan ruxsatlar va hujjatlarning salted xeshlari qayd etiladi. Adabiyotlarda keltirilgan eksperimental natijalar asosida modelning unumdorligi va iqtisodiy samaradorligi baholangan.

Kalit so'zlar: blokcheyn, KYC, aqlli shartnoma, salted xesh, psevdonimlashtirish, kirishni boshqarish, Proof of Authority, shaxsga doir ma'lumotlar, bank xavfsizligi.

Аннотация. В статье анализируются избыточные затраты банков на выполнение процедур «Знай своего клиента» (KYC), вызванные повторным сбором и проверкой одних и тех же документов клиента в каждом банке, а также проблемы безопасности при межбанковской передаче персональных данных. Предложена модель обмена данными на основе частного разрешённого блокчейна, смарт-контракта, хеширования с солью, псевдонимных идентификаторов и шифрования с открытым ключом. Документы не хранятся в блокчейне: в цепочке фиксируются только разрешения клиента и солёные хеши документов. На основе экспериментальных данных из литературы оценены производительность и экономическая эффективность модели.

Ключевые слова: блокчейн, KYC, смарт-контракт, хеш с солью, псевдонимизация, управление доступом, Proof of Authority, персональные данные, банковская безопасность.

Kirish

Moliyaviy tizimda jinoiy daromadlarni legallashtirish va terrorizmni moliyalashtirishga qarshi kurashish (AML/CFT) talablari banklardan har bir yangi mijozni identifikatsiya qilish, uning hujjatlarini yig'ish, tekshirish va doimiy yangilab borishni talab qiladi. Bu jarayon "Mijozingni bil" (Know Your Customer, KYC) deb ataladi. Shu bilan birga, shaxsga doir ma'lumotlarni himoya qilish qonunchiligi

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

(O'zbekistonda – "Shaxsga doir ma'lumotlar to'g'risida"gi Qonun, Yevropa Ittifoqida – GDPR) ma'lumotlar egasining roziligisiz ularni uchinchi shaxslarga berishni cheklaydi va ma'lumotlarni o'chirishni talab qilish huquqini kafolatlaydi.

Amaliyotda bir mijoz bir nechta bankka xizmat ko'rsatish uchun murojaat qilganda, har bir bank aynan bir xil hujjatlarni (pasport, manzil tasdig'i, yuridik shaxs hujjatlari va h.k.) qaytadan yig'adi va tekshiradi. Banklar bozorda raqobatchi bo'lgani va o'zi saqlayotgan ma'lumot uchun yuridik javobgar bo'lgani sababli ular o'rtasida ishonch yetishmaydi, markazlashgan uchinchi tomon KYC xizmatlari esa bankni bitta provayderga haddan tashqari qaram qilib qo'yadi. R. Norvill tadqiqotida (Lyuksemburg universiteti, 2020) Lyuksemburg banklar assotsiatsiyasi (ABBL) bilan hamkorlikda ushbu muammoni hal etuvchi blokcheyn asosidagi tizim ishlab chiqilgan [1]. Mazkur maqolada ushbu yondashuvning kiberxavfsizlik va kriptografik jihatlari tahlil qilinib, uni milliy bank tizimiga moslashtirish imkoniyatlari ko'rib chiqiladi.

Muammoning qo'yilishi va xavfsizlik talablari

Banklararo KYC ma'lumotlarini almashish tizimi quyidagi talablarga javob berishi kerak:

– **ishonch** – banklar bir-biriga to'liq ishonmasa ham, ruxsatlar va almashuvlar yozuvi o'zgartirib bo'lmaydigan va barcha ishtirokchilar tomonidan tasdiqlangan bo'lishi;

– **mijoz nazorati** – ma'lumot faqat mijozning aniq ruxsati bilan uzatilishi;

– **maxfiylik** – taqsimlangan reyestrda shaxsga doir ma'lumotlar ochiq holda saqlanmasligi va o'chirish huquqi ta'minlanishi;

– **yaxlitlik** – qabul qilingan hujjat asl nusxaga mosligini kriptografik tekshirish imkoniyati;

– **mustaqillik** – ma'lumotlar har bir bankning o'z ichki himoyalangan omborida qolishi va markaziy uchinchi tomonga bog'liqlik bo'lmasligi.

Ochiq blokcheynlarda barcha tranzaksiyalar hamma uchun ko'rinadi, zanjirdagi yozuvni o'chirib bo'lmaydi. Bu esa o'chirish huquqi bilan to'g'ridan-to'g'ri ziddiyatga kiradi. Shuning uchun asosiy ilmiy vazifa – blokcheynning o'zgarmaslik xususiyatidan foydalangan holda shaxsga doir ma'lumotlarni zanjirdan tashqarida saqlash va ular bilan zanjirdagi yozuv o'rtasidagi bog'liqlikni kerak bo'lganda uzish mexanizmini yaratishdir.

Taklif etilayotgan model arxitekturasi

Model faqat banklar ishtirok etadigan xususiy, ruxsat etilgan Ethereum tarmog'iga asoslanadi. Konsensus sifatida Proof of Authority (Clique) algoritmi qo'llaniladi: har bir bank bitta validator manziliga ega bo'lib, "bir bank – bir ovoz" tamoyili amal qiladi, bloklar faqat tranzaksiya kelganda hosil qilinadi. Har bir bankda tizim uchta izolyatsiyalangan Docker konteyneridan iborat bo'ladi (1-jadval).

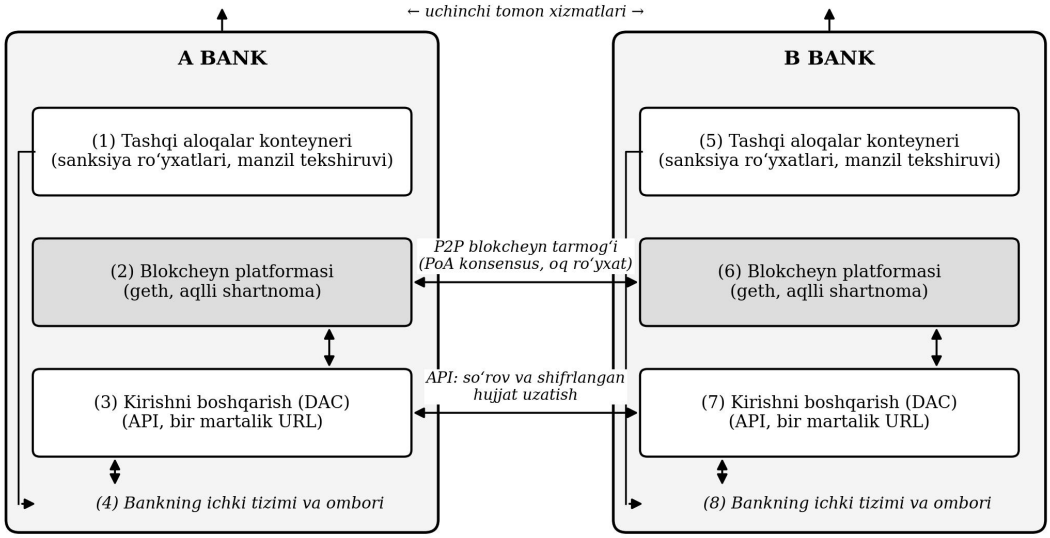
1-jadval

Tizimning har bir bankdagi tarkibiy qismlari

Konteyner	Vazifasi	Xavfsizlik funksiyasi
Tashqi aloqalar	Sanksiya ro'yxatlari, manzil tekshiruvi kabi uchinchi tomon xizmatlariga murojaat	Tashqi tarmoq bilan yagona aloqa nuqtasi
Blokcheyn platformasi (geth)	Aqlli shartnoma orqali ruxsatlarni qayd etish va tekshirish	Oq ro'yxatdagi tugunlar bilangina aloqa; hujjatlarga kirish yo'q
Ma'lumotlarga kirishni boshqarish	Ruxsat tasdiqlangach, hujjatni bank ichki tizimidan API orqali	"Pull" modeli: bank har bir so'rovni rad etishi mumkin

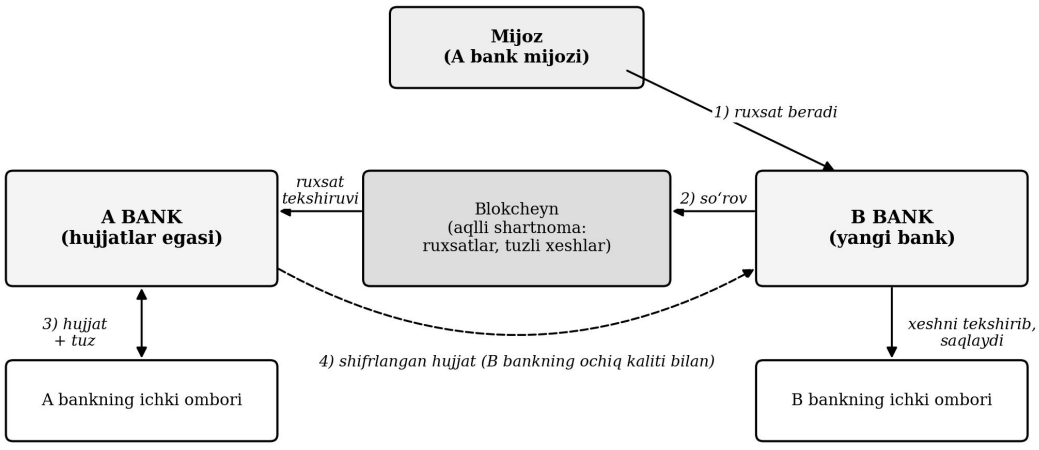
© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

(DAC)	so‘rash va uzatish	



1-rasm. Ikki bank misolida tizim arxitekturasi ([1] asosida tuzilgan)

Ma’lumot oqimi “pull” (so‘rov asosida) tamoyiliga qurilgan: ruxsatning mavjudligi hujjatning avtomatik yuborilishini anglatmaydi. Masalan, A bankning mijozi B bankka o‘tmoqchi bo‘lsa: (1) mijoz B bankka o‘z hujjatlariga kirish ruxsatini beradi va bu ruxsat aqlli shartnomada qayd etiladi; (2) B bank so‘rov yuboradi; (3) A bankning DAC konteyneri blokcheyndan ruxsatni tekshiradi va hujjatni bankning ichki omboridan API orqali oladi; (4) hujjat shifrlangan holda B bankka uzatiladi va u o‘z omborida saqlaydi. Blokcheyn kim, qachon va qaysi ma’lumotni berganligi haqida o‘zgarmas audit izini hosil qiladi.



2-rasm. Mijoz yangi bankka o‘tganda hujjatlarni olish jarayoni ([1] asosida tuzilgan)

Kriptografik himoya mexanizmlari

Psevdonim identifikatorlar. Zanjirda mijoz tasodifiy generatsiya qilingan ID bilan ifodalanadi. ID va mijoz o‘rtasidagi moslik faqat mijoz bilan ishlaydigan bankning ichki bazasida saqlanadi. Mijoz bank

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

bilan munosabatni to‘xtatib, o‘chirishni talab qilsa, moslik o‘chiriladi va zanjirdagi ID shu bank uchun anonim bo‘lib qoladi.

Salted xeshlash. Har bir hujjat d uchun yagona tasodifiy tuz s generatsiya qilinadi va zanjirga h = SHA3(d ‖ s) qiymati yoziladi. Tuz bankning ichki omborida saqlanadi. Tuzsiz xeshdan hujjatni tiklash yoki lug‘at hujumi orqali uni aniqlash amalda mumkin emas. O‘chirish so‘rovida bank hujjat bilan birga tuzni ham o‘chiradi – zanjirdagi h qiymati saqlanib qolsa-da, uni hech kim shaxsga bog‘lay olmaydi. Shu tariqa blokcheynning o‘zgarmasligi va “unutilish huquqi” o‘rtasidagi ziddiyat kriptografik usulda hal qilinadi.

Uzatishda shifrlash va yaxlitlik nazorati. Hujjat va uning tuzi so‘rovchi bankning ochiq kaliti bilan shifrlanadi (ushbu kalit bankning zanjirdagi identifikatori ham hisoblanadi). Shifrlangan fayl faqat operativ xotirada saqlanadi va bir martalik URL orqali beriladi; URL ham qabul qiluvchining ochiq kaliti bilan shifrlanadi. Qabul qilgan bank shifrni ochib, h′ = SHA3(d ‖ s) ni qayta hisoblaydi va zanjirdagi h bilan solishtiradi. Mos kelmasa, blokcheynga nizo tranzaksiyasi yoziladi.

Bir martalik onboarding kodi. Mijozning joriy banki bir martalik kod k yaratadi va aqlli shartnomaga faqat H(k) hamda mijoz ID sini yuboradi. Mijoz k ni yangi bankka taqdim etadi, shartnoma H(k) ni tekshirib, ID ni qaytaradi. Tashqi kuzatuvchi faqat xesh va psevdonim ID ni ko‘radi, kodni qayta ishlatib bo‘lmaydi, u oshkor bo‘lsa bekor qilinadi.

Eksperimental natijalar va samaradorlik

[1] ishda tizim Kaliforniya, Parij va Tokioda joylashgan uchta AWS serverida (2 vCPU, 4 GiB RAM) PoA validatorlari sifatida sinovdan o‘tkazilgan. Har 2 soniyada 10 tadan parallel so‘rov yuborilgan holda 100 soniyalik yuklama testlari natijalari 2-jadvalda keltirilgan.

2-jadval

Yuklama testlari natijalari

Operatsiya	Tranzaksiyalar soni	O‘tkazuvchanlik, iter./s	O‘rtacha kechikish, s
Hujjat qo‘shish	2	1,52	6,38
Hujjatga ruxsat berish	3	1,00	9,18
Toifaga ruxsat berish	3	0,81	11,09
Toifa ruxsatini o‘zgartirish	4	0,69	13,01
Ruxsatni bekor qilish	5	0,32	22,50

Natijalar tizim yuqori yuklamada ham 100 soniyada taxminan 150 ta yangi mijozni ro‘yxatga olishga qodirligini ko‘rsatadi. Holatni o‘zgartirmaydigan ruxsat tekshiruvi mahalliy zanjir nusxasidan o‘qilgani sababli o‘rtacha 39 ms da bajariladi, to‘liq tranzaksiya esa taqsimlangan konsensus tufayli taxminan 3,7 s talab etadi. Bu bank amaliyoti uchun maqbul ko‘rsatkichdir.

Iqtisodiy jihatdan, hujjatni birinchi yig‘ib tekshirgan bank uni tizim ichida boshqa banklarga tannarxiga yaqin narxda taqdim etganda, sotib oluvchi banklar qo‘lda yig‘ish va tekshirishga nisbatan kamida 45 % tejaydi, hujjatni yig‘gan bank esa qo‘shimcha daromad oladi [1]. Ma’lumotlar har bir bankda saqlangani va bir nechta bank tomonidan taqdim etilishi mumkinligi sababli yagona provayderga qaramlik yo‘qoladi.

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

Xulosa

Tahlil shuni ko‘rsatadiki, xususiy ruxsat etilgan blokcheyn banklararo KYC ma’lumotlari almashinuvida ishonchli vositachi o‘rnini bosuvchi, o‘zgartirib bo‘lmaydigan ruxsatlar va audit reyestri vazifasini bajara oladi. Taklif etilgan modelning asosiy afzalliklari: hujjatlarning zanjirdan tashqarida, bankning o‘z omborida saqlanishi; salted xeshlash va psevdonim ID lar orqali o‘chirish huquqining kriptografik ta’minlanishi; so‘rovchi bankning ochiq kaliti bilan shifrlash va xesh orqali yaxlitlik nazorati; konteynerlash yordamida ma’lumotlarni qayta ishlash, saqlash va uzatishni bir-biridan ajratish.

Modelni O‘zbekiston bank tizimiga joriy etishda validator tugunlarini tijorat banklari va tartibga soluvchi organ o‘rtasida taqsimlash, xeshlash va shifrlash uchun milliy kriptografik standartlarni qo‘llash hamda “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun talablariga moslashtirish istiqbolli ilmiy yo‘nalish hisoblanadi. Keyingi tadqiqotlar HTTPS va boshqa barcha himoya mexanizmlari yoqilgan holda unumdorlikni baholash va hujjatlarni uzatish tezligini o‘lchashga qaratiladi.

Foydalanilgan adabiyotlar

1. Norvill R. E. Blockchain Technology for Data Sharing in the Banking Sector: PhD dissertation. – University of Luxembourg, 2020.
2. Norvill R. et al. Blockchain for the Simplification and Automation of KYC Result Sharing // IEEE International Conference on Blockchain and Cryptocurrency (ICBC). – 2019. – P. 9–10.
3. Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Yellow Paper. – 2014.
4. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). – 2016.
5. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni. – 02.07.2019, O‘RQ-547-son.

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.