VILNIAUS UNIVERSITETO
KAUNO FAKULTETAS

SOCIALINIŲ MOKSLŲ IR TAIKOMOSIOS INFORMATIKOS INSTITUTAS

Finansų technologijų studijų programa
Kodas 6211BX022

DOMANTAS GUDONIS

MAGISTRO BAIGIAMASIS DARBAS

TARPUSAVIO SKOLINIMOSI PLATFORMŲ FINANSINĖS VEIKLOS AUDITO BLOKŲ GRANDINĖS INTEGRAVIMO MODELIS

Kaunas 2025

VILNIAUS UNIVERSITETO
KAUNO FAKULTETAS

SOCIALINIŲ MOKSLŲ IR TAIKOMOSIOS INFORMATIKOS INSTITUTAS

DOMANTAS GUDONIS

MAGISTRO BAIGIAMASIS DARBAS

TARPUSAVIO SKOLINIMOSI PLATFORMŲ FINANSINĖS VEIKLOS AUDITO BLOKŲ GRANDINĖS INTEGRAVIMO MODELIS

Leidžiama ginti

Magistrantas_____
(parašas)

Darbo vadovas_____
(parašas)

_____
(darbo vadovo mokslo laipsnis, mokslo pedagoginis vardas, vardas ir pavardė)

Darbo įteikimo data

Registracijos Nr.

Kaunas 2025

Turinys

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

SANTRUMPŲ IR TERMINŲ SĄRAŠAS

BDAR (Bendrasis duomenų apsaugos reglamentas) – Europos Sąjungos teisės aktas (angl. GDPR), nustatantis asmens duomenų tvarkymo ir apsaugos reikalavimus. Darbo kontekste BDAR aktualus dėl blokų grandinės nekintamumo savybės, kuri gali prieštarauti duomenų subjektų teisei „būti pamirštam“, todėl integruojant blokų grandinę į audito procesus būtina užtikrinti atitiktį šiam reglamentui.

LB (Lietuvos bankas) – Lietuvos centrinis bankas, atliekantis ir finansų rinkos priežiūros funkciją. Darbe LB minimas kaip tarpusavio skolinimo platformų veiklos reguliatorius ir prižiūrėtojas: jis nustato ataskaitų teikimo reikalavimus, tikrina platformų veiklą bei užtikrina, kad P2P operatoriai laikytųsi teisės aktų.

P2P (peer-to-peer) – tiesioginio ryšio tarp dalyvių modelis, kai paslaugos teikiamos be tradicinių tarpininkų. Tarpusavio skolinimas yra šio modelio pritaikymas finansuose – platforma suveda skolintojus ir skolininkus tiesiogiai. Darbo kontekste P2P skolinimo platformos veikia tokiais pagrindais, suteikdamos galimybę fiziniams asmenims tarpusavyje skolinti ir skolintis, o blokų grandinės integracija skirta realiu laiku fiksuoti šias operacijas ir palengvinti jų auditą bei ataskaitų rengimą.

Blokų grandinė – paskirstytas duomenų registras (angl. blockchain), kuriame informacija saugoma chronologiškai susietų blokų grandinėje, užtikrinant duomenų nekintamumą ir patikimumą kriptografijos metodais. Ši technologija darbo kontekste naudojama siekiant padidinti P2P platformų finansinių operacijų skaidrumą, atsekamumą ir duomenų vientisumą audito procesuose.

Išmanioji sutartis – programinis kodas blokų grandinėje, automatiškai vykdantis sutarties sąlygas, kai įvykdomos iš anksto nustatytos sąlygos (angl. smart contract). Darbo kontekste išmaniosios sutartys naudojamos automatizuoti finansinių ataskaitų sudarymą ir verslo taisyklių užtikrinimą P2P skolinimo platformoje – jos realiu laiku tikrina bei fiksuoja duomenis, svarbius auditui.

Konsensuso mechanizmas – blokų grandinės tinklo algoritmas, užtikrinantis, kad visi mazgai (tinklo dalyviai) sutaria dėl vieningos transakcijų sekos ir duomenų būsenos. Nuo pasirinkto konsensuso metodo (pvz., darbo įrodymo algoritmas (PoW) ar Bizantijos gedimams atsparus algoritmas (BFT)) priklauso sistemos greitis, saugumas ir patikimumas – todėl darbe analizuojami keli mechanizmai siekiant parinkti audito poreikius tenkinantį sprendimą P2P platformai.

Finansinis auditas – įmonės finansinių operacijų ir ataskaitų tikrinimo procesas, kuriuo siekiama įvertinti jų teisingumą ir atitikimą nustatytiems apskaitos standartams bei teisės aktams. Darbo kontekste auditas P2P skolinimo platformose yra esminis užtikrinant skaidrumą ir pasitikėjimą tarp dalyvių, o blokų grandinės integravimas padeda automatizuotai ir nekintamai fiksuoti audituojamus duomenis realiu laiku.

Gudonis, Domantas (2025). *Blockchain integration model for auditing financial activities of peer-to-peer lending platforms.* MBA Graduation Paper. Kaunas: Vilnius University, Kaunas Faculty, Institute of Social Sciences and Applied Informatics. 67 p.

SUMMARY

This paper examines the application of blockchain technology in the financial auditing processes of peer-to-peer lending platforms with the aim of increasing data transparency and reliability and reducing the risk of manual work and human error. The rapid growth of the P2P lending market increases the requirements for the integrity and traceability of financial data, but traditional reporting processes often rely on manual data processing, making them inefficient and vulnerable.

The aim of this work is to investigate the applicability of permissioned blockchain technology in the audit processes of peer-to-peer lending platforms and to create a solution model that allows the automation of financial report generation. To achieve this objective, the following tasks were set: to review the principles of blockchain technology and its application possibilities in financial reporting, to assess the advantages of its integration for the transparency and reliability of P2P platforms, to analyze the challenges and limitations of implementation, to create and implement a prototype, and to evaluate its performance under realistic load conditions.

Both qualitative and quantitative methods were used in the study. An analysis and synthesis of scientific literature was performed, a decision architecture was modeled, and a prototype of a permissioned blockchain based on Hyperledger Fabric technology was designed and implemented. In the practical part, experimental measurements were performed to evaluate the system's performance, latency, resource usage, and financial report generation time by changing network configurations and data volumes.

The results of the work showed that a permissioned blockchain can be effectively applied to the automated generation of financial reports on peer-to-peer lending platforms. In the developed prototype, all financial events (loan issuance and repayment) are recorded immutably and in real time, and smart contracts automatically generate report data without additional human intervention. Experiments have shown that when processing up to 10,000 loans, a financial report is generated in approximately 5 seconds, and the system's resource requirements remain low. The maximum throughput achieved significantly exceeds the actual transaction flows of P2P platforms and can therefore be considered a technical reserve.

This leads to the conclusion that blockchain technology increases the traceability of financial data, ensures its integrity, and improves the transparency of the audit process. However, the practical application of such a solution requires updates with the existing legal and regulatory environment, particularly regarding data protection (GDPR) and reporting forms. A properly selected blockchain configuration allows the solution to be adapted to the real operating conditions of peer-to-peer lending platforms.

This paper consists of 67 pages, with 4 tables, 30 figures, and 2 appendices.

ĮVADAS

Temos aktualumas

Šiuolaikinėje finansinių technologijų aplinkoje P2P (tarpusavio) skolinimosi rinka sparčiai plečiasi: 2025 m. jos vertė siekia 7,29 mlrd. USD (Fortune Business Insights, 2025), o iki 2034 m. prognozuojama išaugsianti iki 33,81 mlrd. USD. Toks augimas atspindi didėjantį alternatyvių finansavimo šaltinių poreikį ir kelia naujus iššūkius duomenų skaidrumui bei pasitikėjimui tarp platformos naudotojų, investuotojų ir reguliuotojų. Tradiciniuose P2P portaluose finansinės veiklos duomenys dažnai tvarkomi rankiniu būdu arba mišriai: darbuotojai suderina duomenis iš skirtingų sistemų, atlieka skaičiavimus ir rengia ataskaitas. Toks procesas yra lėtas, linkęs į duomenų neatitikimus ir didesnę sukčiavimo riziką.

Siekiant spręsti šiuos trūkumus, vis aktualesni tampa technologiniai sprendimai, leidžiantys automatizuoti duomenų apdorojimą ir pagerinti finansinių ataskaitų patikimumą. Vienas tokių sprendimų – blokų grandinė. Įrašius duomenis jų keisti neįmanoma, todėl ženkliai sustiprėja operacijų vientisumas ir patikimumas. Taip pat išmaniųjų sutarčių mechanizmai leidžia automatizuoti finansinių ataskaitų generavimą ir patikrinimą realiu laiku, mažinant rankinio darbo ir su juo susijusių klaidų skaičių. Dėl šių savybių blokų grandinė plačiai vertinama kaip priemonė didinti finansinių duomenų skaidrumą ir pasitikėjimą P2P platformose.

Problemos ištyrimo lygis

Blokų grandinės taikymas finansinių procesų automatizavimui sulaukė vis didesnio dėmesio tiek mokslinėje literatūroje, tiek praktikoje. Autoriai kaip Sarker (Sarker, 2025) pabrėžia, kad ši technologija gali užtikrinti realaus laiko įrašus, stiprinti duomenų vientisumą ir mažinti klaidų bei sukčiavimo riziką. Victory ir Yazid analizuoja P2P skolinimo aplinką ir teigia, kad blokų grandinė padeda didinti skaidrumą bei pasitikėjimą finansinėmis operacijomis. Tačiau nepaisant teorinių įžvalgų, išlieka trūkumas taikomuosiuose tyrimuose, kurie parodytų, kaip tokie sprendimai veikia konkrečiose situacijose – pavyzdžiui, automatizuojant ataskaitų sudarymą tarpusavio skolinimo platformose. Todėl kyla pagrindinis klausimas: kaip blokų grandinė, gali būti pritaikyta automatizuoti finansinių veiklos ataskaitų generavimą tarpusavio skolinimo platformoje?

Darbo problema – Kaip blokų grandinės technologija gali išspręsti duomenų vientisumo ir pasitikėjimo problemas tarpusavio skolinimo platformų finansinės veiklos audito procese?

Darbo objektas – blokų grandinės technologijos taikymas tarpusavio skolinimo platformų audito procesuose, siekiant padidinti pasitikėjimą ir skaidrumą.

Darbo tikslas – Išnagrinėti blokų grandinės technologijos taikymą tarpusavio skolinimo platformų audito procesuose, siekiant padidinti pasitikėjimą ir skaidrumą ir sukurti atitinkamą modelį

Darbo uždaviniai:

1. Apžvelgti blokų grandinės technologiją bei jos panaudojimo galimybes finansinės ataskaitos automatizavime.

2. Nustatyti blokų grandinės integravimo privalumus, kurie galėtų pagerinti tarpusavio skolinimosi platformų finansinės atskaitomybės skaidrumą ir patikimumą.

3. Išanalizuoti pagrindinius iššūkius ir apribojimus diegiant automatizuotą finansinių ataskaitų rengimo sistemą blokų grandinės pagrindu.

4. Sukurti ir įgyvendinti blokų grandinės prototipą, demonstruojantį leidimų reikalaujančios grandinės galimybes automatizuoti finansinių veiklos ataskaitų generavimą tarpusavio skolinimo platformoje.

5. Įvertinti sukurtos sistemos veikimą: jos našumą, duomenų vientisumo užtikrinimą bei tinkamumą tarpusavio skolinimo platformų veiklos sąlygoms.

Darbe naudoti literatūros šaltiniai

Naudoti įvairūs šaltiniai: nuo naujausių mokslinių publikacijų iki pramonės ataskaitų ir techninės dokumentacijos. Literatūroje dominavo 2020–2025 m. tyrimai, tarp jų – akademiniai straipsniai (Sarker, Victory, Wüst & Gervais ir kt.). Taip pat remtasi ir technine dokumentacija („Hyperledger Fabric“ bei kitos analizuos blokų grandinės).

Darbo struktūra ir apimtis

Pirmame skyriuje analizuojami blokų grandinės technologijos principai ir tarpusavio skolinimosi platformų veiklos ypatumai. Antrajame skyriuje pristatoma tyrimo metodologija bei suprojektuoto sprendimo (prototipo) architektūra. Trečiame skyriuje pateikiami eksperimento rezultatai ir vertinamas sistemos našumas bei veikimas. Galiausiai pabaigoje apibendrinami pagrindiniai tyrimo rezultatai ir pateikiamos išvados bei rekomendacijos. Bendra apimtis – 67 puslapiai, pateiktos 4 lentelės, 30 paveikslėlių bei 2 priedai.

Darbo ir tyrimo metodai

Taikyti kokybiniai ir kiekybiniai tyrimo metodai: mokslinės literatūros analizė ir sintezė, sprendimo modeliavimas ir projektavimas, prototipo kūrimas, eksperimentiniai matavimai bei rezultatų analizė. Literatūros analizė naudota nagrinėjant blokų grandinės technologijos principus, audito metodikas ir tarpusavio skolinimo verslo modelį. Praktinėje dalyje taikytas empirinio modeliavimo metodas – sukurtas ir suprojektuotas sprendimo prototipas naudojant „Hyperledger Fabric“ blokų grandinę. Eksperimentų metu atlikti našumo matavimai, keičiant tinklo konfigūracijas ir transakcijų apkrovas, o gauti rezultatai analizuoti siekiant įvertinti sprendimo efektyvumą.

Darbo rezultatų teorinė ir praktinė reikšmė.

Leidimų reikalaujanti blokų grandinė su išmaniosiomis sutartimis gali būti efektyviai taikoma finansinių ataskaitų automatizavimui. Sukurtas prototipas parodė, jog kiekvienas finansinis įvykis (paskolos išdavimas, įmoka) registruojamas nekintamai ir realiu laiku, o ataskaitos sugeneruojamos automatiškai, be papildomo žmogaus įsikišimo. Tai užtikrina didesnį duomenų tikslumą, sumažina klaidų ir manipuliavimo riziką bei padidina audito proceso skaidrumą. Sistemos testai patvirtino, kad net esant padidintam transakcijų srautui, ji išlaiko reikalingą našumą.

Darbo sunkumai, taikymo apribojimai.

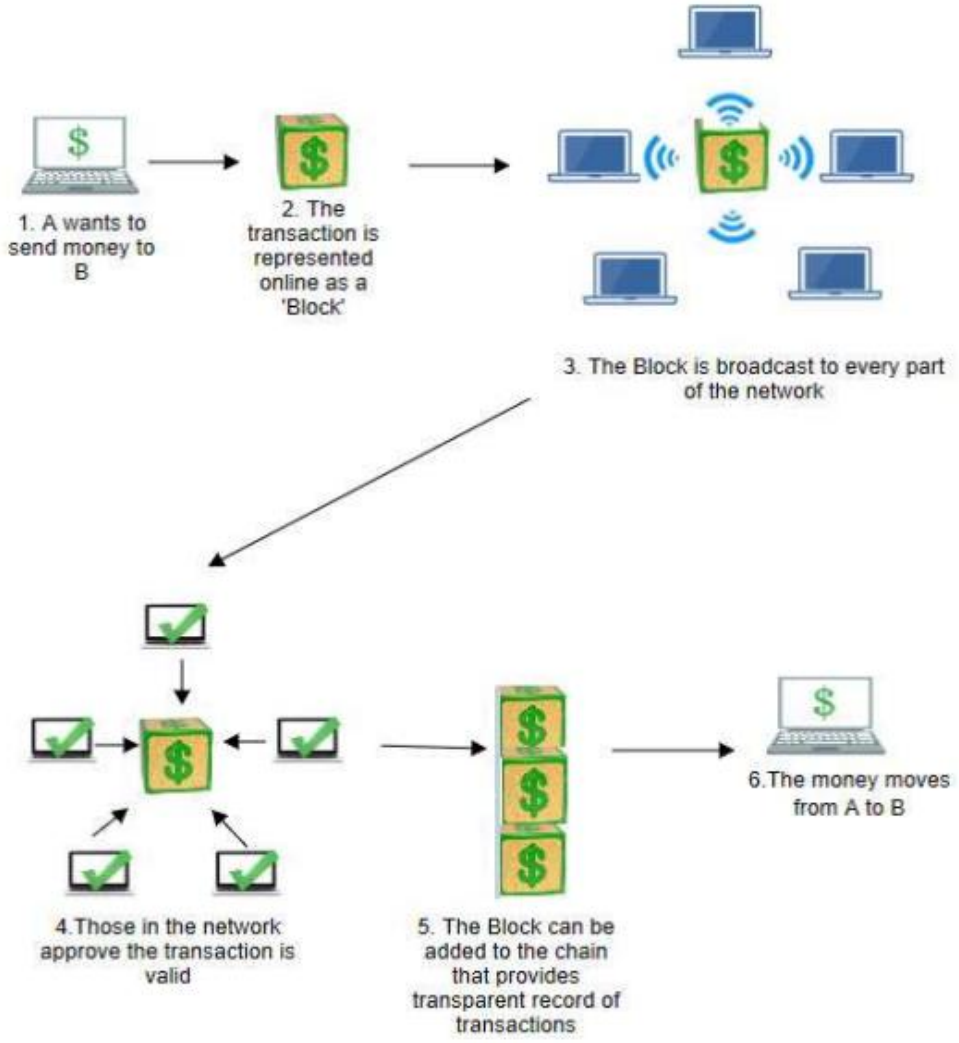
Vykdant tyrimą paaiškėjo, kad pagrindiniai iššūkiai susiję ne su technine sistema, bet su jos integracija į esamą ataskaitų teikimo praktiką. Šiuo metu platformos teikia ataskaitas periodiškai, dažniausiai Excel formatu, tuo tarpu siūlomas modelis generuoja duomenis realiu laiku JSON struktūroje. Norint šį sprendimą taikyti praktikoje, reikėtų atitinkamų teisinių pakeitimų, reglamentuojančių duomenų teikimo formą ir dažnumą. Taip pat būtina įvertinti duomenų apsaugos ir privatumo reikalavimus, ypač kalbant apie dalijimąsi informacija per blokų grandinės tinklą – tai reikalauja specifinių sprendimų, atitinkančių BDAR ir kitas reguliavimo nuostatas.

1. BLOKŲ GRANDINĖS TECHNOLOGIJOS TAIKYMO AUDITO PROCESUOSE TEORINIAI ASPEKTAI

1.1. Blokų grandinės technologijos apžvalga

Blokų grandinės siūlo unikalią galimybę užtikrinti duomenų saugumą ir skaidrumą. Šiame skyriuje aptarsiu pagrindinius blokų grandinės veikimo principus, remdamiesi įvairių autorių darbais ir įžvalgomis.

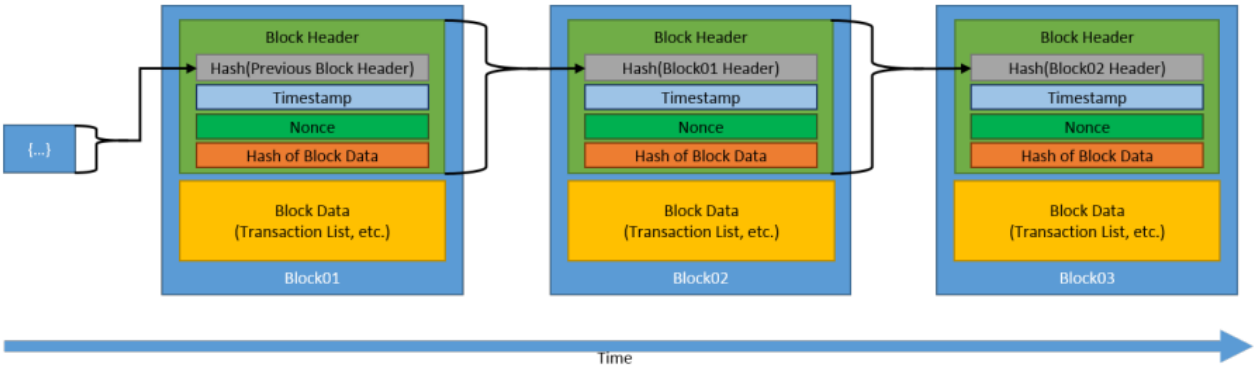
Pagal Sarmah (Sarmah, 2018) blokų grandinė veikia kaip decentralizuota duomenų bazė, kurios įrašai yra paskirstyti tarp daugybės tinklo dalyvių. Vietoj centrinės valdžios, sandoriai yra patvirtinami tinklo mazgų, kurie naudojasi kriptografiniais algoritmais, užtikrinančiais sandorių vientisumą. Kai vartotojas atlieka sandorį, jis siunčiamas visiems tinklo mazgams. Šie mazgai patikrina sandorio galiojimą ir užtikrina, kad siuntėjo lėšos yra galiojančios ir nepanaudotos anksčiau. Sandoris tada grupuojamas su kitais sandoriais ir sudaromas blokas, kuris turi būti patvirtintas naudojant tam tikrą konsensuso mechanizmą (žr. 1 pav.)



1 pav. Blokų grandinės veikimo principas (Sarmah, 2018)

Kiekvienas naujai sukurtas blokas yra sujungtas su ankstesniu bloku (Yaga, Mell, Roby, & Scarfone, 2019), naudojant maišos (angl. hash) funkcijas. Maiša yra unikali, sukurta pagal bloko

turinį. Jei informacija būtų pakeista, jo maiša taip pat pasikeistų, ir tai būtų akivaizdu visiems tinklo dalyviams. Dėl šios priežasties, bet koks bandymas keisti informaciją būtų pastebėtas ir atmestas tinklo dalyvių. (žr. 2 pav.)



2 pav. Blokų grandinės blokų jungimas (Yaga, Mell, Roby, & Scarfone, 2019)

Blokų grandinės technologija buvo suskirstyta į tris pagrindinius etapus pagal Swan (Swan, 2015) remiantis taikymo sritimis kiekvienoje kategorijoje:

1. „Blockchain 1.0“ yra pirmoji karta, kuri daugiausia skirta kriptovaliutoms. Ši technologija buvo įvesta kartu su Bitcoin atsiradimu. Į šią kategoriją patenka ne tik Bitcoin, bet ir kitos valiutos. Bitcoin buvo pirmasis realus šios technologijos pavyzdys, sukurtas siekiant užtikrinti skaitmeninių mokėjimų saugumą ir decentralizaciją
2. „Blockchain 2.0“ yra antroji karta, naudojama finansinėse paslaugose ir pramonės šakose. Ši karta apima ir kitokius finansinius įrankius (akcijos, obligacijos ir t.t.). „Blockchain 2.0“ taip pat pirmą kartą pristatė išmaniuosius kontraktus, kurie yra naudojami sandorių metu tikrinant, ar produktai ir paslaugos buvo pristatyti tiekėjo. Tai leidžia automatizuoti ir užtikrinti sandorius tarp šalių, sumažinant tarpininkų poreikį ir didinant procesų efektyvumą
3. „Blockchain 3.0“ yra trečioji karta, kuri siūlo didesnį saugumą, mastelio keitimą (angl. scalability) ir pritaikomumą, lyginant su ankstesnėmis kartomis. Ši technologija naudojama įvairiose pramonės šakose. „Blockchain 3.0“ suteikia galimybę užtikrinti duomenų vientisumą ir skaidrumą įvairiose srityse

Taip pat, autorė išskiria skirtingus blokų grandinės tipus:

- Viešosios blokų grandinės (angl. Public Blockchains): Atviros visiems, kuriose kiekvienas gali dalyvauti sprendimų priėmime.
- Privačios blokų grandinės (angl. Private Blockchains): Prieinami tik tam tikrai žmonių ar organizacijų grupei.
- Pusiau privačios blokų grandinės (angl. Semi-private Blockchains): Dalinai vieši, dalinai privatūs, priklausomai nuo naudojimo sąlygų.
- Šoninės grandinės (angl. Sidechains): Leidžia perkelti monetas iš vienos blokų grandinės į kitą.
- Leidimų reikalaujančios knygos (angl. Permissioned Ledgers): Dalyviai yra žinomi ir patikimi, naudoja sutarimo protokolą.
- Paskirstytosios knygos (angl. Distributed Ledgers): Duomenų bazės, kurios yra paskirstytos tarp dalyvių.
- Dalijamos knygos (angl. Shared Ledgers): Taikomosios programos ar duomenų bazės, kurios yra dalijamos viešai ar organizacijos viduje.

Visi šie tipai turi savo privalumus ir trūkumus, šio darbo kontekste toliau bus nagrinėjamos knygos (angl. ledgers) kaip paskirstytosios knygos bei privačios blokų grandinės – žinoma, viešosios blokų grandinės suteiktų daugiau skaidrumo, tačiau kai kurie įrašai gali būti jautrūs ir neskelbiami viešai, t.y. prieinami tik auditoriams. Blokų grandinės technologija užtikrina saugumą, skaidrumą ir decentralizaciją, leidžiant patikimai vykdyti skaitmeninius sandorius be tarpininkų poreikio. Tai suteikia plačias galimybes įvairiose srityse, ypatingai finansų srityje. Dėl decentralizuoto pobūdžio ir duomenų vientisumo užtikrinimo blokų grandinės ypatingai tinka audito procesams, kadangi tikrinti duomenis, kai jie negali būti pakeisti išorinių veiksnių yra paprasčiau.

1.2. Blokų grandinės integravimas į audito procesus

Norint aptarti blokų grandinės integravimą į finansinius ir tarpusavio skolinimo procesus svarbu aptarti ir du pagrindinius jų tipus: be leidimo t.y. viešos (angl. permissionless) viešosios ir su leidimu t.y. privačios (angl. permissioned) blokų grandinės. Kiekvienas tipas turi savo privalumus ir trūkumus, dėl kurių tinka skirtingiems panaudojimo atvejams. Leidimų neturinčios blokų grandinės, žinomos dėl savo atvirumo ir decentralizacijos, leidžia bet kam dalyvauti tinkle. Kita vertus, blokų grandinės su leidimais skirtos kontroliuojamai aplinkai, kurioje privatumas ir prieigos kontrolė yra svarbiausi dalykai. Šiose blokų grandinėse gali dalyvauti tik iš anksto nustatyti dalyviai, todėl jos idealiai tinka įmonių taikomosioms programoms, kuriose labai svarbus duomenų konfidencialumas ir sandorių efektyvumas. Norint pasirinkti konkrečius poreikius atitinkančią technologiją, labai svarbu suprasti šių dviejų tipų blokų grandinių skirtumus.

Apie šiuos skirtumus kalba ir Gamage su kolegomis (Gamage, Weerasinghe, & Dias, 2020) Blokų grandinėms be leidimų, būdingas atvirumas ir decentralizacija. Šios blokų grandinės netaiko jokių apribojimų dalyviams, todėl kiekvienas gali prisijungti prie tinklo, skaityti ir rašyti duomenis bei dalyvauti konsensuso procese. Toks aukštas decentralizacijos lygis užtikrina, kad nė vienas dalyvis nekontroliuotų tinklo, atsakomybė yra paskirstoma visiems dalyviams. Skaidrumas yra esminė blokų grandinių be leidimų savybė; visi sandoriai yra matomi visiems tinklo. Kitas svarbus aspektas – nekeičiamumas, užtikrinantis, kad kartą patvirtinus sandorius jų negalima pakeisti, todėl jie yra saugūs nuo klastojimo. Nepaisant šių privalumų, leidimo neturinčios blokų grandinės dažnai susiduria su iššūkiais, susijusiais su mastelio keitimu ir pralaidumu (angl. throughput) – sandoriai apdorojami lėčiau negu centralizuotoje sistemoje.

Leidimus turinčios blokų grandinės suteikia prieigą tik atrinktai dalyvių grupei, kuri yra iš anksto patvirtinta. Šios blokų grandinės paprastai naudojamos įmonių aplinkoje, kur privatumas ir kontrolė yra svarbiausi dalykai. Dalyvavimas ribojamas, o kontroliuojama prieiga užtikrina, kad duomenis skaityti ir rašyti gali iš anksto nustatyti dalyviai. Leidimus turinčiose blokų grandinėse dažnai naudojami konsensuso mechanizmai, kurie yra efektyvesni aplinkoje, kurioje yra patikimų dalyvių. Tai leidžia greičiau apdoroti sandorius ir užtikrinti didesnį pralaidumą, palyginti su leidimo neturinčiomis blokų grandinėmis. Svarbūs privalumai yra privatumas ir konfidencialumas, nes duomenys gali būti prieinami tik įgaliotiems dalyviams, todėl šios blokų grandinės tinka tvarkyti slaptą informaciją tokiuose sektoriuose kaip finansai. Nors leidimų turinčios blokų grandinės užtikrina tam tikrą decentralizacijos lygį, jos yra labiau centralizuotos, palyginti su leidimų neturinčiomis blokų grandinėmis.

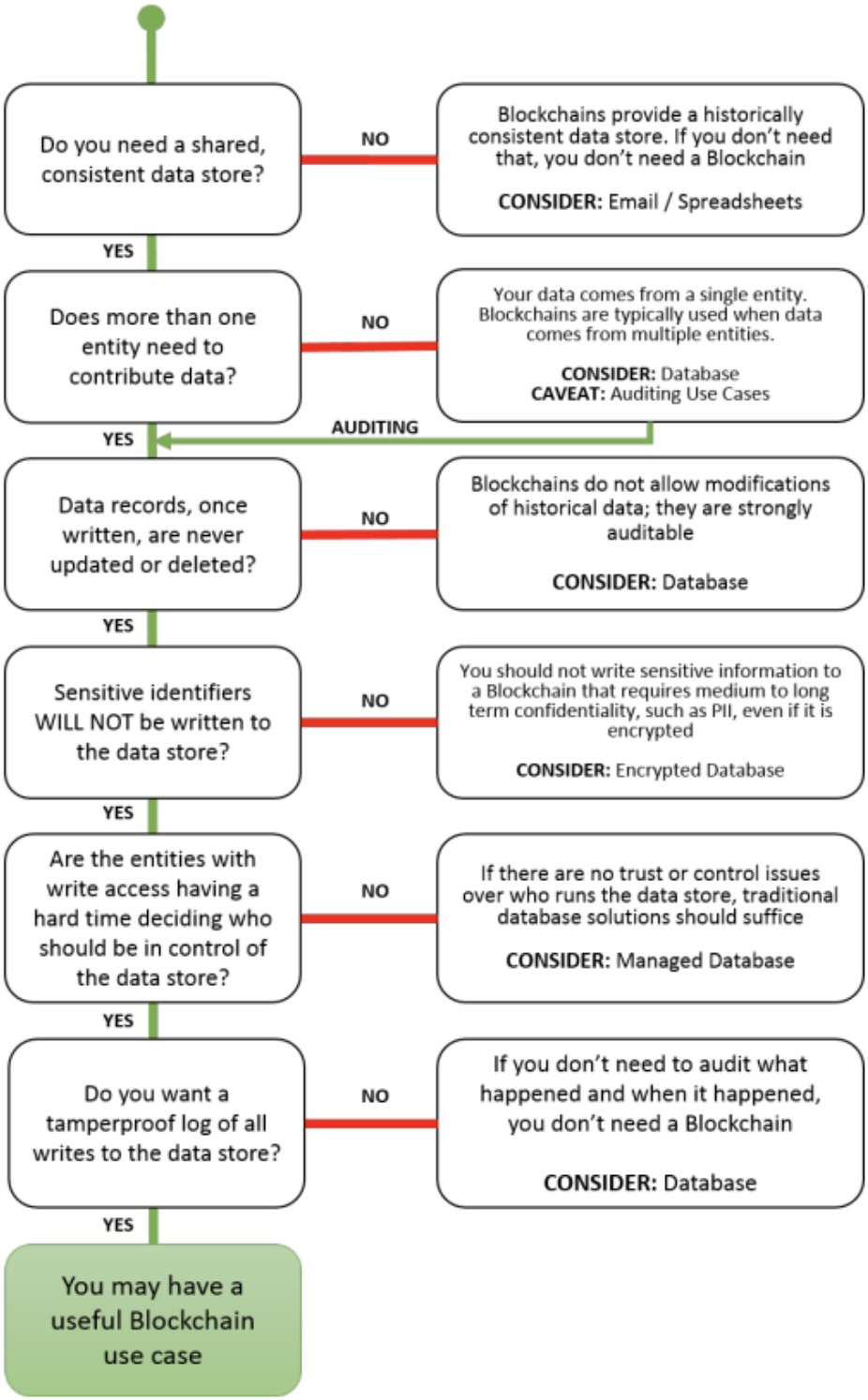
Daugiau informacijos apie bloko grandinių skirtumus pateikiama lentelėje (lentelė 1)

1 lentelė Bloko grandinių tipų palyginimas (Gamage, Weerasinghe, & Dias, 2020)

Savybė	Be Leidimų Blokų Grandinė	Atvira Leidimus Turinti Blokų Grandinė	Uždara Leidimus Turinti Blokų Grandinė	Ribota Paskirstyta Duomenų Baze
Vieša Skaitymo Prieiga	Yra	Yra	Nėra	Nėra
Vieša Rašymo Prieiga	Yra	Nėra	Nėra	Nėra
Nekintamumas	Aukštas	Vidutinis	Žemas	Žemas
Pralaidumas	Žemas	Vidutinis	Aukštas	Aukštas
Mastelio keitimas	Žemas	Vidutinis	Aukštas	Aukštas
Decentralizacija	Aukšta	Vidutinė	Žema	Žema

Šioje lentelėje pabrėžiami kompromisai tarp skirtingų tipų blokų grandinių ir ribotų paskirstytų duomenų bazių. Leidimų neturinčios blokų grandinės išsiskiria decentralizavimu, skaidrumu ir nekeičiamumu, tačiau susiduria su pralaidumo ir mastelio iššūkiais. Atviros blokų grandinės su leidimais užtikrina pusiausvyrą tarp skaidrumo ir kontrolės, todėl jos tinka toms taikomosioms programoms, kuriose tam tikro lygio vieša prieiga yra naudinga, tačiau būtina duomenų įrašymo kontrolė. Kita vertus, uždaros leidimais grindžiamos blokų grandinės ir riboto naudojimo paskirstytosios duomenų bazės teikia pirmenybę kontrolei ir efektyvumui, todėl idealiai tinka aplinkoms, kuriose labai svarbu privatumas ir didelis pralaidumas, tačiau jose aukojami visiškos decentralizacijos ir skaidrumo privalumai.

Daugiau apie blokų grandinės taikymą ir panaudojimo atvejus kaip auditą kalba Yaga su kolegomis (Yaga, Mell, Roby, & Scarfone, 2019) (žr. 3 pav.)



3 pav. JAV VSD Mokslo ir technologijų direktorato blokų grandinės panaudojimo atvejų schema (Yaga, Mell, Roby, & Scarfone, 2019)

Vertinant blokų grandinės tinkamumą, reikia atsižvelgti į keletą pagrindinių aspektų, kuriais vadovaujamasi pagal nurodytą sprendimų metų. Pirma, blokų grandinės gebėjimas išlaikyti nuoseklų istorinį duomenų įrašą yra labai svarbus, kai daugeliui suinteresuotųjų šalių, pavyzdžiui, reguliavimo institucijoms reikia bendros prieigos. Blokų grandinė idealiai tinka aplinkoje, kurioje duomenis teikia keli subjektai, užtikrinant, kad visi dalyviai galėtų naudotis ta pačia informacija. Duomenų įrašų nekintamumas yra dar vienas svarbus veiksnys. Blokų grandinė užtikrina, kad kartą įrašyti duomenys

negali būti pakeisti ar ištrinti, todėl ji tinka istorinių įrašų vientisumui išlaikyti. Ir atvirkščiai, jei įrašus reikia dažnai atnaujinti ar ištrinti, tradicinė duomenų bazė suteikia daugiau lankstumo. Kitas aspektas – jautrių duomenų tvarkymas. Blokų grandinės nerekomenduojama naudoti neskelbtinai informacijai, reikalaujančiai ilgalaikio konfidencialumo, pavyzdžiui, asmenį identifikuojančiai informacijai, saugoti. Blokų grandinė puikiai tinka aplinkoje, kurioje kyla pasitikėjimo ar kontrolės problemų tarp subjektų, turinčių prieigą prie duomenų, nes tai neutralus, nuo klastojimo apsaugotas sprendimas.

Apibendrinant galima teigti, kad blokų grandinė yra labai veiksminga atliekant finansų įstaigų auditą, jei duomenis teikia keli subjektai, įrašai turi išlikti nekeičiami, nesaugomi jautrūs identifikatoriai, kyla pasitikėjimo problemų ir reikalingas neklastojamas žurnalas. Esant tokioms sąlygoms, blokų grandinė užtikrina neprilygstamą saugumą, skaidrumą ir patikimumą, užtikrina duomenų vientisumą, didina suinteresuotųjų šalių pasitikėjimą ir atitinka reguliavimo reikalavimus.

1.3. P2P skolinimo ir sutelktinio finansavimo ekosistema

Sutelktinis finansavimas leidžia investuotojams jungtis ir bendrai finansuoti verslus, projektus ar individualius paskolos gavėjus. Finansavimas neapsiriboja bankais ar kitais instituciniais paskolų tiekėjais, bet tampa atviras. Sutelktinis finansavimas paprastai skirstomas į kelis modelius – finansavimą paramos ar atlygio pagrindu ir paskolomis grindžiamą modelį. Pastarasis variantas dar vadinamas tarpusavio skolinimu (angl. peer-to-peer lending, P2P), kuriame per tam skirtas interneto platformas investuotojai tiesiogiai skolina lėšas kitiems asmenims ar įmonėms, o pati platforma veikia tik kaip tarpininkė. Taip technologinės decentralizacijos principas derinamas su tradicine kredito logika – paskolos suteikimo procesas išlieka reglamentuotas, tačiau tampa labiau atviras, lankstus ir prieinamas.

Europos Sąjungoje 2020 m. priimtas Reglamentas (ES) 2020/1503 (Reglamentas (ES) 2020/1503 dėl Europos sutelktinio finansavimo paslaugų verslui teikėjų, 2020), nustato reikalavimus sutelktinio finansavimo paslaugų teikėjams, apimantį tiek investicinį, tiek skolinimo modelį. Nuo jo įsigaliojimo tarpusavio skolinimo platformos įtrauktos į reguliuojamą sutelktinio finansavimo paslaugų sektorių. Lietuvoje šių platformų veiklą prižiūri Lietuvos bankas (LB) – platformos operatorius gali verstis tarpusavio skolinimo veikla tik įsirašęs į viešąjį tarpusavio skolinimo platformų operatorių sąrašą, (Lietuvos Bankas, 2024) kurį tvarko LB. Tam operatorius turi atitikti vartojimo kredito įstatymo ir LB nustatytus reikalavimus.

Tarpusavio skolinimo platformos generuoja didelius duomenų srautus, tačiau šie duomenys dažnai lieka uždaryti platformų vidinėse sistemose. Nors operatoriai teikia reguliarias ataskaitas priežiūros institucijoms (pvz., LB) ir perduoda informaciją į bendras registrų sistemas (pvz., Paskolų rizikos duomenų bazę), praktikoje priežiūra remiasi periodiniu, o ne nuolatiniu tikrinimu. Duomenų atnaujinimai priklauso nuo pačių platformų ir kartais pateikiami vėluojant, todėl priežiūros institucijos neturi galimybės realiuoju laiku stebėti įsipareigojimų vykdymo ar operacijų kokybės ir laiku aptikti galimų pažeidimų. Be to, audito įrodymai dažnai būna centralizuoti – juos kaupia pati platforma, todėl kyla klausimas, kiek galima pasitikėti pačia platforma kaip vieninteliu duomenų šaltiniu.

Šioje situacijoje blokų grandinės gali būti sprendimas, galintis sukurti nekintamą ir atsekamą duomenų infrastruktūrą. Kiekviename paskolos gyvavimo ciklo etape – nuo paraiškos pateikimo, kreditingumo vertinimo, sutarties sudarymo iki galutinio grąžinimo –galima išsaugoti transakcijas, kurios taptų automatiniais audito įrodymais. Taip būtų iš esmės pakeista duomenų kontrolė:

informacija nebepriklausytų vien tik platformos operatoriui, o reguliatoriai galėtų tikrinti sandorius realiu laiku.

Tarpusavio skolinimo ekosistema dėl savo pobūdžio itin tinkama tokio tipo technologinėms inovacijoms, nes joje susikerta trys kertiniai blokų grandinės taikymo elementai – pasitikėjimas, skaidrumas ir duomenų nekintamumas. Šioje srityje veikia daug nepriklausomų dalyvių (paskolos gavėjai, investuotojai, platformų operatoriai, auditoriai, reguliuotojai), todėl nėra vieno dominuojančio dalyvio, kuriuo visos šalys galėtų besąlygiškai pasitikėti – tai sukuria terpę decentralizuotų sprendimų naudai. Be to, tarpusavio skolinimo platformos privalo derinti duomenų viešumą su konfidencialumu: investuotojams turi būti užtikrinamas reikiamas skaidrumas (pvz., informacija apie paskolų portfelio būklę), tačiau kartu saugoma jautri asmeninė ir finansinė informacija. Toks balanso poreikis atitinka blokų grandinės principus, kai duomenų nekintamumas ir patikimumas gali būti garantuojamas be visiško jų atskleidimo viešai.

Dėl šių priežasčių šiame darbe nagrinėjamas būtent paskolomis pagrįstas sutelktinio finansavimo modelis. Tarpusavio skolinimo veikla, turinti aiškiai apibrėžtą teisinę struktūrą ir realius audito iššūkius, leidžia praktiškai įvertinti, kaip blokų grandinės technologija gali pagerinti duomenų valdymo, atsekamumo ir audito procesus finansų rinkoje. P2P sektorius tampa ne tik eksperimentine, bet ir reprezentacine sritimi, atspindinčia platesnį finansinių technologijų transformacijos poveikį: nuo centralizuoto pasitikėjimo modelio – prie skaidrios, automatizuotos ir technologiškai patikimos finansinės atskaitomybės aplinkos. Sekančiame skyriuje plačiau aptariamas reguliavimas Lietuvoje ir susiję Europos Sąjungos įstatymai.

1.4. Tarpusavio skolinimo reguliavimas Lietuvoje ir Europos Sąjungoje

Tarpusavio skolinimo platformų veikla Lietuvoje reglamentuojama daugiausiai nacionalinio vartojimo kredito teisės normomis. Lietuvos Respublikos Vartojimo kredito įstatyme numatyta, kad tarpusavio skolinimo platformos operatorius yra juridinis asmuo (ne pelno nesiekiantis juridinis asmuo negali būti operatoriumi), administruojantis informacinę sistemą – tarpusavio skolinimo platformą – per kurią sudaromi vartojimo kredito sandoriai tarp fizinių asmenų (paskolos davėjų ir gavėjų). Norint teisėtai vykdyti tarpusavio skolinimo platformos operatoriaus veiklą, būtina įsirašyti į „Viešąjį tarpusavio skolinimo platformos operatorių sąrašą“, kurį prižiūri Lietuvos bankas. LB, kaip priežiūros institucija, įtraukia įmonę į šį sąrašą tik įsitikinęs, kad ji atitinka įstatymo ir priežiūros reikalavimus (pateikti visi reikalingi dokumentai, vidaus taisyklės, procedūros ir kt.). Pagrindiniai reikalavimai operatoriui apima minimalaus kapitalo ir veiklos tęstinumo užtikrinimą: įstatinis kapitalas turi būti ne mažesnis nei 40000 eurų (Lietuvos Respublikos vartojimo kredito įstatymas, 2018), privaloma turėti parengtą bei patvirtintą veiklos planą, numatantį priemones nepertraukiamai veiklai užtikrinti net ir nenumatytomis aplinkybėmis.

Tarpusavio skolinimo platformų operatoriams taip pat taikomi visi bendrieji atsakingojo skolinimo reikalavimai, kurie galioja vartojimo kredito davėjams (išskyrus kredito įstaigas). Operatorius privalo įvertinti kiekvieno vartojimo kredito gavėjo mokumą prieš sudarant sutartį, naudodamas pakankamą informaciją apie kliento finansinę padėtį iš vidinių ir išorinių šaltinių. Praktikoje tai reiškia, kad tarpusavio skolinimo platforma, gavusi paskolos paraišką, turi patikrinti kliento finansinius įsipareigojimus bei kredito istoriją tokiose sistemose kaip Paskolų rizikos duomenų bazė (PRDB).

Tarpusavio skolinimo platformų operatoriai privalo reguliariai teikti ataskaitas Lietuvos bankui, kad šis galėtų vykdyti priežiūrą. LB valdybos nutarimu (Nr. 03-248) patvirtintos Vartojimo kredito davėjų ir tarpusavio skolinimo platformos operatorių privalomos informacijos teikimo taisyklės nustato, kokią informaciją, kokiu formatu ir periodiškumu tarpusavio skolinimo operatoriai turi pateikti. Paprastai reikalaujama kas ketvirtį pateikti finansinės veiklos ataskaitą, kurioje nurodoma: per ketvirtį naujai sudarytų vartojimo kredito sutarčių skaičius ir bendra suma, vidutinės palūkanų normos, portfelio kokybės rodikliai, per tą laikotarpį nurašytos ar išieškotos sumos ir kt. Detalus ataskaitos pavyzdys pateikiamas 1 priede. Pagal galiojančias taisykles ketvirtinė ataskaita turi būti pateikta pasibaigus ketvirčiui iki kito ketvirčio antro mėnesio 1 dienos (pvz., I ketv. ataskaita – iki gegužės 2 d., II ketv. – iki rugpjūčio 1 d., III ketv. – iki lapkričio 2 d., IV ketv. (metinė) – iki vasario 1 d.) (Lietuvos Bankas, 2018) . Ataskaitos LB pateikiamos elektroniniu būdu, naudojantis specialia Lietuvos Banko sistema.

Atitinkamai, tarpusavio skolinimo operatoriai privalo teikti duomenis ir į Paskolų rizikos duomenų bazę (PRDB) – centralizuotą kredito rizikos duomenų sistemą, kurią administruoja Lietuvos bankas. PRDB kaupiami duomenys apie kiekvieną paskolos gavėją ir jo turimus finansinius įsipareigojimus, taip pat kredito sutarčių vykdymo istorija. Visi vartojimo kredito rinkos dalyviai (bankai, kredito unijos, vartojimo kredito davėjai ir tarpusavio skolinimo operatoriai) privalo periodiškai teikti detalias ataskaitas LB apie naujas paskolas ir atnaujinti esamų sutarčių duomenis nustatytais terminais. PRDB Lietuvoje veikia pagal Europos Centrinio Banko inicijuotą „AnaCredit“ standartą, todėl duomenys teikiami apie kiekvieną paskolą. LB yra paskelbęs techninius dokumentus, duomenų teikimo schemas ir tikrinimo taisykles, kad visi rinkos dalyviai teiktų informaciją vienodu standartu. Šios informacijos pagrindu LB gali gauti bendrą vaizdą apie kiekvieno paskolos gavėjo skolos naštą visoje rinkoje, o kredito davėjai (įskaitant tarpusavio skolinimo platformas) – patikrinti klientų įsipareigojimus prieš suteikdami naują paskolą.

Kuriant blokų grandinės sprendimus finansų srityje, būtina atsižvelgti į Europos Bendrojo duomenų apsaugos reglamento (BDAR, angl. GDPR) reikalavimus, ypač į duomenų subjektų teisę būti pamirštam. Blokų grandinės technologijos nekintamumo principas – kartą įrašyti duomenys yra nepakeičiami ir neištrinami – iš pirmo žvilgsnio prieštarauja BDAR nuostatai, leidžiančiai reikalauti ištrinti asmens duomenis. Todėl diegiant P2P skolinimo sprendimus būtina vengti tiesioginio jautrių asmens duomenų saugojimo viešoje nekintamoje grandinėje.

Apibendrinant, diegiant blokų grandinės pagrindu veikiančią duomenų audito sistemą tarpusavio skolinimo platformoje, būtina kruopščiai suplanuoti duomenų struktūrą taip, kad į nekintamą grandinę nepatektų tiesiogiai identifikuojami klientų duomenys. Gali būti taikomas duomenų maišos įrašymas vietoje originalių įrašų, šifravimas su galimybe selektyviai sunaikinti raktus, ar net specialiai pritaikytos redaguojamos blokų grandinės platformos. Tai užtikrintų, kad inovatyvus sprendimas atitiktų ne tik finansų reguliavimą, bet ir privatumo apsaugos teisės aktus. Aptarus teisinius reikalavimus, toliau galima aptarti ir Lietuvoje įvykusius panašius pažeidimus

1.5. Finansinių ataskaitų teikimo problemos ir pažeidimai Lietuvoje

Nepaisant aiškiai apibrėžtų reikalavimų, praktikoje kai kurie finansų rinkos dalyviai vis tiek susiduria su pažeidimais – vėluoja teikti finansines ataskaitas arba pateikia nevisiškai patikimus duomenis. Žemiau aptariami keli pastarųjų metų Lietuvos atvejai, atskleidžiantys tokios problemos mastą ir pasekmes.

„Paysera LT“ – 2025 m. Lietuvos bankas skyrė bendrovei 20 tūkst. eurų baudą už tai, kad ši septynis mėnesius nepateikė privalomų finansinių ataskaitų laiku. Be vienkartinės baudos, LB nustatė ir baudą po 1 tūkst. eurų už kiekvieną uždelstą dieną, kuri dar galėjo būti didinama iki 2 tūkst. ar 3 tūkst. eurų per dieną, jei bendrovė ir toliau neįvykdytų pareigos. „Payseros“ vadovybė aiškino, kad vėlavimą lėmė techniniai iššūkiai – užsitęsęs apskaitos sistemos pertvarkymas, dėl kurio duomenų migracija užtruko ilgiau nei planuota. Vis dėlto LB sprendimu bendrovė buvo įpareigota nedelsiant pateikti trūkstamas ataskaitas ir parengti priemonių planą, kaip ateityje išvengti tokio pažeidimo. Šis atvejis parodė, kad net rinkos lyderiai privalo laikytis nustatytų terminų, o techniniai nesklandumai nelaikomi pateisinančia priežastimi nesilaikyti priežiūros reikalavimų. (Klimaševska, 2025)

„Curve Europe“ – 2025 m. LB analogiškai bendrovę „Curve Europe“ 22,5 tūkst. eurų bauda, kai ši laiku nepateikė metinių finansinių ataskaitų. Pasibaigus finansiniams metams bendrovė nepateikė finansinės ataskaitos, dėl to pažeidė prievolę pateikti ataskaitas laiku. „Curve Europe“ pripažino padariusi pažeidimą ir kreipėsi į LB – bendrovė sutiko su nustatytais trūkumais ir ėmėsi priemonių jiems pašalinti. Įvertinęs šias aplinkybes, LB sudarė susitarimą, tačiau vis tiek skyrė baudą, atsižvelgdamas į tai, kad ataskaitos buvo pateiktos gerokai pavėluotai. Šis pavyzdys parodo, kad priežiūros institucija net ir bendradarbiaujant įmonei vis tiek taiko nuobaudas, proporcingas pažeidimo mastui, siekdama užtikrinti drausmę rinkoje.

„Foxpay“ – 2024 m. Lietuvos bankas, atlikęs patikrinimą, nustatė šiurkščių ir sistemingų teisės aktų pažeidimų visose tikrintose srityse (pinigų plovimo prevencijos, klientų lėšų apsaugos, informacijos saugumo ir kt.). Tarp pažeidimų paminėtas ir netinkamas priežiūrai teikiamos informacijos užtikrinimas – įmonė neužtikrino tikslių duomenų teikimo Lietuvos bankui apie visas klientų lėšų saugojimo sąskaitas. Dėl šių nusižengimų LB iš pradžių apribojo „Foxpay“ veiklą: 2024 m. liepą paskirtas laikinasis atstovas, per kurį turėjo būti prižiūrima įmonės veikla ir kontroliuojamas informacijos teikimas LB. Vėliau, lapkritį, centrinis bankas priėmė sprendimą panaikinti „Foxpay“ licenciją, faktiškai uždarydamas įmonės veiklą. Tai kraštutinis atvejis, kai už sistemingus atitikties pažeidimus (įskaitant atskaitomybės nevykdymą) įstaiga praranda savo licenciją. Šis pavyzdys pabrėžia, kokia svarbi yra patikima ir savalaikė informacijos teikimo priežiūrai pareiga – jos nevykdymas kelia grėsmę ne tik vartotojų interesams, bet ir pačios įmonės išlikimui. (ELTA, 2024)

Aukščiau apžvelgti atvejai išryškina tradicinės atskaitomybės sistemos trūkumus – finansinių ataskaitų teikimas po fakto (pasibaigus ataskaitiniam laikotarpiui) ir pasikliaujant vien vidinėmis įmonių procedūromis gali lemti reikšmingus vėlavimus ar duomenų neatitikimus. Žmogiškosios klaidos, techniniai trikdžiai ar net sąmoningas vilkinimas gali sutrikdyti informacijos srautą priežiūrai, o tai kelia rizikų tiek investuotojams, tiek visos rinkos stabilumui. Tai, kad per pastaruosius kelerius metus LB turėjo skirti baudas ar net imtis kraštutinių priemonių keliems žinomiems rinkos dalyviams, rodo, jog esama ataskaitų teikimo praktika nėra iki galo patikima ir efektyvi. Ši problematika suteikia pagrindą ieškoti naujų sprendimų. Būtent šiame kontekste nagrinėjama blokų grandinės technologija gali pasiūlyti išeitį – sukurti realiu laiku veikiančią, automatiškai audituojamą atskaitomybės sistemą, kurioje duomenų nekintamumas ir skaidrumas ženkliai sumažintų vėlavimo bei informacijos iškraipymo galimybes. Tolimesniuose skyriuose bus analizuojama, kaip šis sprendimas galėtų būti pritaikytas P2P skolinimo platformos duomenų audito poreikiams ir kokią vertę jis sukurtų sprendžiant aptartas atitikties problemas. Toliau aptariami blokų grandinės privalumai ir trūkumai audito procesuose.

1.6. Blokų grandinės privalumai audito procesuose

Didesnis skaidrumas ir pasitikėjimas

Bonyuet (Bonyuet, 2020) įžvalgiai aptaria blockchain būdingas savybes, tokias kaip nekeičiamumas ir decentralizacija, teigdamas, kad „blokų grandinės teikiamas skaidrumas atsiranda dėl jos gebėjimo pateikti nepažeidžiamą ir atvirai patikrinamą sandorių knygą, kuri yra prieinama visoms suinteresuotosioms šalims.“. Ši savybė yra ypač svarbi, nes ji ne tik užtikrina, kad blokų grandinėje esantys duomenys būtų matomi, bet ir patikimai patikrinami bet kurio asmens, taip pat skatina ir skaidrumą. Toliau plečiant šį pagrindą, Schmitz, ir Leoni (Schmitz & Leoni, 2019) pabrėžia blokų grandinėje saugomų duomenų nuoseklumą ir patikimumą. Jos aiškina, kad blokų grandinės didina dalyvių pasitikėjimą, nes užtikrina, kad kiekvienas į apskaitos knygą įrašytas sandoris yra nepakeičiamas, taip gaunama ir nekintama istorija. Šis dėmesys patikimumui yra labai svarbus – svarbu ne tik tai, kad duomenys būtų skaidrūs, bet ir tai, kad jie būtų nuolat patikimi, taip laikui bėgant stiprinant suinteresuotųjų šalių pasitikėjimą. Appelbaum ir Nehmer (Appelbaum & Nehmer, 2017) aptaria decentralizacijos vaidmenį didinant pasitikėjimą. Jie teigia: „Decentralizuotas blokų grandinės pobūdis gerokai sumažina riziką, susijusią su manipuliavimu duomenimis ir sukčiavimu, taip padidindamas visos finansinės atskaitomybės ekosistemos patikimumą.“ Panaikindama centralizuotus kontrolės taškus, blokų grandinė ne tik sumažina riziką, bet ir išsklaido galią, o tai savaime sumažina duomenų klastojimo ir sukčiavimo galimybes. Ši decentralizacija yra esminė pasitikėjimo finansų sistemomis architektūros raida, leidžianti manyti, kad bus pereita prie demokratiškesnės ir saugesnės finansinės atskaitomybės sistemos.

Apibendrinant galima teigti, kad nuo tiesioginės prieigos ir tikrumo iki sandorių įrašų patikimumo ir decentralizuotos architektūros – sukuria įtikinamą pagrindą teigti, kad blokų grandinė yra ne tik technologinis patobulinimas, bet ir nauja galimybė finansiniam skaidrumui. Kiekvienas šių mokslininkų iškeltas elementas išryškina skirtingą aspektą, kaip blokų grandinė gali iš esmės pakeisti audito praktiką ir sukurti patikimesnę sistemą.

Pasinaudojant blokų grandinės galimybėmis, audito srityje gali įvykti pokytis link sistemos, kurioje skaidrumas ir pasitikėjimas ne tik padidėtų, bet ir įsitvirtintų.

Išlaidų mažinimas

Ši technologija leidžia sukurti skaidrias ir nekintamas operacijų įrašų sistemas, užtikrinančias duomenų saugumą ir vientisumą. Automatizuoti procesai mažina rankinio darbo poreikį ir žmogiškųjų klaidų riziką, didina tikslumą ir leidžia auditoriams greičiau bei lengviau patikrinti sandorius realiuoju laiku.

Appelbaum ir Nehmer (Appelbaum & Nehmer, 2017) aptaria, kaip blokų grandinė gali iš esmės pakeisti tradicines apskaitos sistemas. Jie teigia, kad blokų grandinės technologija įveda našumą apskaitos sistemose, nes automatizuoja daugelį procesų, kurie tradiciškai reikalaudavo daug darbo ir laiko, todėl sumažėja bendros audito sąnaudos. Tai ne tik didina audito praktikos finansinį efektyvumą, bet ir glaudžiai siejasi su platesnėmis finansinių operacijų technologinės pažangos tendencijomis.

Tam pritaria ir Jiang (Jiang, 2018) pabrėždamas automatizavimo vaidmenį mažinant auditorių darbo krūvį. Anot jo, blokų grandinės gebėjimas tikrinti sandorius realiuoju laiku gali „sumažinti auditui atlikti reikalingą darbo jėgą ir taip gerokai sumažinti išlaidas“. Toks veiklos efektyvumas supaprastina audito procesus, gerokai sutrumpindamas audito laiką ir darbo sąnaudas, o tai tiesiogiai prisideda prie bendrų išlaidų taupymo.

Be to, Schmitz ir Leoni (Schmitz & Leoni, 2019) pabrėžia nuolatinio audito potencialą. Jos teigia, kad blokų grandinės technologija gali padaryti periodinį auditą beveik nebereikalingą, nes galima sukurti realiuoju laiku vykstančius nuolatinio audito procesus. Anot Schmitz, ir Leoni (Schmitz & Leoni, 2019): „Perėjimas prie nuolatinio audito naudojant blokų grandinę galėtų gerokai

sumažinti tradicinių auditų dažnumą ir darbo sąnaudas, o tai lemtų mažesnes sąnaudas.“. Šis požiūris patvirtina teiginį apie našumą ir leidžia manyti, kad ateityje gali iš esmės pasikeisti audito atlikimo būdai, pabrėžiant dar didesnio sąnaudų mažinimo potencialą, nes mažėja dažnų tradicinių auditų poreikis.

Šios įžvalgos kartu rodo, kad sutariama dėl blokų grandinės taupymo galimybių audito srityje. Sumažinus rankinio darbo sąnaudas ir suteikus galimybę vykdyti operacijas realiuoju laiku ir sumažinus auditų dažnumą, blokų grandinė gali pasiūlyti skaidresnį, veiksmingesnį ir pigesnį audito procesą.

Patobulintas saugumas

Dėl blokų grandinės sumažėja sukčiavimo rizika, nes visi duomenys yra viešai patikrinami ir negali būti pakeisti nepalikus aiškaus pėdsako.

Francati et al. (Francati, et al., 2021) gilinasi į tai, kaip blokų grandinė apsaugo už grandinės ribų esančius duomenis. Jie pažymi, kad sistema naudoja blokų grandinės technologiją, kad apsaugotų už grandinės ribų esančius duomenis kriptografiniais įrodymais, užtikrindama duomenų vientisumą ir sumažindama klastojimo riziką.

Remdamasis šiuo saugumo pagrindu, Bonyuet (Bonyuet, 2020) daug dėmesio skiria decentralizacijai. Jis aiškina, jog decentralizuota blokų grandinės architektūra gerokai sumažina riziką, susijusią su manipuliavimu duomenimis, nes keičiant blokų grandinės duomenis reikia kelių mazgų sutarimo. Ši decentralizacija yra esminis blokų grandinės saugumo komponentas, nes ji išsklaido duomenis daugybėje mazgų, todėl nesankcionuotus pakeitimus nepastebėjus itin sunku atlikti.

Be to, Appelbaum ir Nehmer (Appelbaum & Nehmer, 2017) aptaria, kaip blokų grandinės atsekamumas ir nekintamumas dar labiau sumažina sukčiavimo riziką. Jie teigia, jog blokų grandinės technologija pagerina sandorių atsekamumą ir padaro sandorių atšaukimą neįmanomą be tinklo sutarimo (konsensuso). Tai užtikrina, kad kiekvienas sandoris būtų skaidrus ir atsekamas, o tai užkerta kelią sukčiavimui, nes bet koks bandymas pakeisti užregistruotus sandorius tampa lengvai aptinkamas.

Šiam požiūriui pritaria ir Supriadi, Hendra ir Miya (Supriadi, Hendra, & Miya, 2020), anot jų, blokų grandinė yra inovatyvi apskaitos technologija, kuri ne tik automatizuoja tradicinius procesus, bet ir didina sandorių patikimumą ir greitį.

Abi autorių grupės sutinka, kad blokų grandinė įveda didelį efektyvumą, tačiau Appelbaum, ir Nehmer (2017) daugiausia dėmesio skiria sisteminiams pokyčiams, o Supriadi et al. (2020) pabrėžia tiesioginį poveikį kasdienei apskaitos praktikai ir galimą tradicinių vaidmenų sumažėjimą dėl automatizavimo.

Šie požiūriai kartu pabrėžia blokų grandinės technologijos saugumo savybes audito srityje. Apsaugant už grandinės ribų esančius duomenis, panaudojant decentralizuotas architektūras ir didinant sandorių atsekamumą bei nekeičiamumą, blokų grandinė yra patikima sukčiavimo prevencijos ir duomenų vientisumo užtikrinimo sistema.

1.7. Blokų grandinės pritaikymo audito procesuose iššūkiai ir apribojimai

Techniniai ir infrastruktūros iššūkiai

Blokų grandinės integravimas į esamas audito ir apskaitos sistemas kelia daug sudėtingų iššūkių. Ši technologija reikalauja ne tik naujų IT sprendimų, bet ir esamų sistemų atnaujinimo bei pritaikymo. Organizacijos turi užtikrinti, kad jų infrastruktūra galėtų palaikyti blokų grandinės veikimą ir būtų suderinama su kitomis naudojamomis technologijomis. Be to, reikia spręsti duomenų

saugumo, privatumo ir reguliavimo klausimus, kurie yra itin svarbūs siekiant išlaikyti operacijų vientisumą ir atitikimą teisės aktams. Šie iššūkiai reikalauja tiek techninių žinių, tiek strateginio planavimo, kad blokų grandinės technologija galėtų būti sėkmingai integruota į audito ir apskaitos procesus.

Francati et al. (Francati, et al., 2021) pateikia iššūkius, susijusius su duomenų integracija už grandinės ribų. Jie pabrėžia, kad norint integruoti blokų grandinę su tradicinėmis sistemomis, reikalingi naujoviški kriptografiniai metodai ir infrastruktūros koregavimai, kad būtų išlaikytas duomenų vientisumas ir saugumas.

Appelbaum ir Nehmer (Appelbaum & Nehmer, 2017) toliau plėtoja integracijos iššūkių temą ir gilinasi į plačius techninius iššūkius, susijusius su esamų apskaitos sistemų konfigūracija, kad jos būtų pritaikytos blokų grandinėms. Anot jų, pritaikant blokų grandinės technologiją dažnai reikia iš esmės keisti esamą apskaitos programinę įrangą ir infrastruktūrą, todėl kyla didelių techninių iššūkių. Tai rodo, kad integracija dažnai susijusi su esminiais senųjų sistemų pertvarkymais, o ne su paprastais pritaikymais.

Be to, Bonyuet (Bonyuet, 2020) aptaria suderinamumo problemas, kylančias integruojant blokų grandinę su esamomis finansų sistemomis. Jis teigia, kad integruojant blokų grandinę į nusistovėjusias finansines sistemas kyla didelių suderinamumo iššūkių, nes esamos sistemos dažnai nepalaiko decentralizuotų architektūrų. Tai dar vieną sudėtingumo sluoksnį, pabrėždama būtinybę suderinti blokų grandinės funkcijas su dabartiniais audito standartais ir praktika.

Francati ir kt. (2021), Appelbaum ir Nehmer (2017) bei Bonyuet (2020) įžvalgos kartu išryškina techninių ir infrastruktūros iššūkių, su kuriais susiduriama integruojant blokų grandinę į esamas sistemas įvairovę. Šie iššūkiai apima naujų kriptografinių sprendimų kūrimą, visišką sistemos pertvarkymą ir suderinamumo su senosiomis sistemomis problemų sprendimą. Tokios integracijos pastangos nėra lengvai išsprendžiamos ir susijusios su giliais struktūriniais esamų sistemų pakeitimais, kurie gali būti ir brangūs, ir reikalaujantys daug laiko.

Profesinių įgūdžių trūkumas

Liu, Wu, ir Xu (2019) teigimu, blokų grandinės technologijos integracija į audito ir apskaitos sektorius reikalauja reikšmingų profesinio mokymo ir įgūdžių ugdymo pokyčių. Savo tyrime (Liu, Kean, & Xu, 2019) pabrėžia, kad auditoriai turi gerai suprasti blokų grandinės technologinius pagrindus, kad galėtų efektyviai panaudoti jos galimybes.

Schmitz ir Leoni (Schmitz & Leoni, 2019) pabrėžia nuolatinio švietimo svarbą, kad būtų galima neatsilikti nuo technologinės pažangos, ypač blokų grandinės. Anot autorių, nuolatinis profesinis mokymas blokų grandinės technologijų srityje yra būtinas auditoriams, kad jie neatsiliktų nuo pažangos ir išlaikytų savo profesinę kompetenciją. Tai sustiprina nuolatinio mokymosi sąvoką ir pabrėžia būtinybę dabartiniams specialistams reguliariai atnaujinti savo įgūdžius, kad galėtų veiksmingai valdyti ir audituoti blokų grandinės sistemas.

Šios Liu, Wu, ir Xu (2019), Schmitz, ir Leoni (2019) diskusijos kartu pabrėžia reikšmingą auditorių profesinio tobulėjimo pokytį. Autoriai atkreipia dėmesį į tai, kad auditoriams būtina nedelsiant prisitaikyti prie naujų technologijų ir kad švietimo sistemos turi atitinkamai vystytis platesniu mastu. Šis scenarijus kelia dvigubą iššūkį: užtikrinti, kad dabartiniai specialistai būtų pasirengę dirbti su naujomis technologijomis ir kad būsimieji auditoriai nuo pat pradžių būtų mokomi šių kompetencijų.

2. BLOKŲ GRANDINĖS TECHNOLOGIJOS TAIKYMO AUDITO PROCESUOSE METODOLOGIJA

2.1. Tyrimo dizainas ir metodologinis požiūris

Šio skyriaus tikslas – apibrėžti tyrimo metodologiją, kuria remiantis kuriamas prototipas, įvertinami architektūriniai variantai bei atliktas eksperimentinis našumo tyrimas. Šiame darbe taikomas empirinio modeliavimo metodas. Tai reiškia, kad tyrimo idėja grindžiama idėjos realizavimu prototipo forma ir jo patikrinimu. Tyrimo tikslas – išnagrinėti blokų grandinės technologijos taikymą tarpusavio skolinimo platformų finansinės veiklos auditų procesuose ir sukurti atitinkamą modelį. Prototipas suteikia galimybę šiuos aspektus išmatuoti ir palyginti, kadangi jame realizuotas funkcinis sprendimas tiesiogiai demonstruoja, kokią naudą duomenų atsekamumui, skaidrumui ir audito galimybei suteikia blokų grandinės taikymas. Tyrimo metu bus suformuoti keli skirtingi tinklo architektūros scenarijai, kuriuose organizacijų sąveika su reguliatoriumi (Lietuvos banku) įgyvendinama skirtingais būdais. Šie scenarijai leis įvertinti, kaip techniniai sprendimai – kanalų struktūra, tapatybės valdymas, duomenų paskirstymas – veikia audito galimybes, našumą ir atitiktį BDAR reikalavimams. Prototipas bus naudojamas ne kaip galutinis produktas, bet kaip eksperimentas idėjoms patikrinti. Kuriant prototipą galime identifikuoti sistemos veikimo ribas, bei modeliuoti grandinės suteikiamas vertę. Kaip pažymi Victory ir Yazid) (Victory & Yazid, 2023), prototipo kūrimas padeda įvertinti, kaip pasiūlytos blokų grandinės technologijos sprendimai pagerina skaidrumą, saugumą ir efektyvumą skolinimo sandoriuose bei ataskaitų generavime. Tokiu būdu prototipas tampa šio tyrimo priemone: jo pagalba tikrinama hipotezė ir renkama informacija apie sistemos savybes.

Tyrimo hipotezė remiasi mintimi, jog leidimų reikalaujanti blokų grandinė suteikia audito pranašumus, kurių negali garantuoti tradicinės duomenų bazės. Leidimų blokų pasižymi savybėmis, kurios iš esmės keičia duomenų valdymą: nekintamumas (angl. immutability), veiksmų atsekamumas (angl. traceability), skaitmeninis pasirašymas ir laiko žymos. Wüst ir Gervais (Wüst & Gervais, 2018) siūlo struktūrizuotą metodą, padedantį identifikuoti, kada blokų grandinės technologija pagrįsta: ji tinka tada, kai sistemoje veikia kelios tarpusavyje nepasitikinčios šalys, o duomenų vientisumas ir skaidrumas yra kritiniai. Jų analizėje nurodoma, kad tokios platformos kaip „Hyperledger Fabric“ ar „Corda“ yra tinkamiausios įmonės (angl. enterprise) lygio sprendimams.

Audito požiūriu, blokų grandinės technologija užtikrina aukštesnį duomenų vientisumo ir nekintamumo lygį. Kiekviena transakcija blokų grandinėje yra kriptografiškai susiejama su ankstesne, o blokai formuoja nuoseklią grandinę, kurios turinio neįmanoma pakeisti be visų sekančių blokų perrašymo – tai technologiškai ir ekonomiškai neefektyvu. Leidimų reikalaujančios platformos, tokios kaip „Hyperledger Fabric“ ar „Corda“, įrašo transakcijas su laiko žymomis ir skaitmeniniais parašais, todėl kiekvieno veiksmo kilmė yra atsekama ir patvirtinama konsensuso būdu. Taip pat, šios platformos turi savo atitikmenis išmaniesiems kontraktams, kurie gali būti pritaikyti audito/stebėjimo tikslams kaip finansinių ataskaitų kūrimas.

Tyrimai parodė, kad blokų grandinės sistemose duomenys iš karto tampa atsparūs manipuliacijai – jų kopijos paskirstomos tinklo dalyviams, o kiekvienas bandymas pakeisti istorinius duomenis būtų akivaizdžiai pastebimas. Priešingai, tradicinėse sistemose net ir žurnalų apsaugai

dažnai reikia papildomų sprendimų. Dėl šių savybių, blokų grandinės audito pėdsakas laikomas labiau patikimu, ypač aplinkoje, kur egzistuoja vidinių grėsmių rizika ar būtina garantuoti skaidrumą tarp nesusijusių šalių. (Khazaei & Arabsorkhi, 2024)

Apibendrinant galima teigti, kad pasirinktas metodologinis požiūris – empirinio modeliavimo pagrindu sukurtas prototipas – leidžia praktiškai įvertinti leidimų reikalaujančios blokų grandinės potencialą sprendžiant realias skaidrumo, ir audito problemas tarpusavio skolinimo platformose. Norint detaliau kalbėti apie prototipus, svarbu aptarti ir palyginti įvairias galimas technologijas, tai yra aprašoma sekančiame skyriuje.

2.2. Bloko grandinės technologijų palyginimas

Šiame skyriuje lyginamos pagrindinės leidimų reikalaujančios (privačios) blokų grandinės platformos – „Hyperledger Fabric“ (Hyperledger Fabric, 2025), „R3 Corda“ (R3, 2025), „Quorum“ (ConsenSys, 2024). Palyginimas atliekamas pagal esminius aspektus: konsensuso mechanizmus, našumą (pralaidumą, vėlavimą, mastelio keitimą (angl. scalability), privatumo ir prieigos kontrolės galimybes, audituojamumą ir skaidrumą. Toks įvertinimas leidžia nustatyti, kuri platforma geriausiai tenkina tiriamo atvejo poreikius. Ankstesni tyrimai rodo, kad nors „Hyperledger Fabric“ išsiskiria daug žadančiomis savybėmis, galutinis pasirinkimas visuomet yra kompromisas tarp skirtingų platformų savybių. (Bakos & Halaburda, 2021).Toliau detaliai aptariami kiekvienas palyginimo aspektas.

2.2.1. Konsensuso mechanizmas

Konsensuso algoritmas užtikrina, kad paskirstytoje sistemoje visi mazgai (angl. node) sutartų dėl vieningos operacijų sekos ir blokų grandinės būsenos. Leidimų reikalaujančiose platformose konsensusas paprastai pasiekiamas greitesniais, mažiau resursų reikalaujančiais metodais nei viešose blokų grandinėse, kadangi dalyviai yra žinomi ir patikimi. Konsensuso mechanizmus aptarė ir Polge su kolegomis (lentelė 2)

2 lentelė. Bloko grandinės technologijų konsensų palyginimas (Polge, Robert, & Le Traon, 2021)

	Konsensusas
Hyperledger Fabric	Balsavimu grįstas arba pasirenkamas (Raft, Kafka ir kt.)
Qourum	POA, RAFT,
MultiChain	Round robin validation
R3 Corda	Balsavimu grįstas/ RAFT

„Hyperledger Fabric“ Fabric naudoja CFT konsensusą – pagal numatytuosius nustatymus siūlomi „Raft“ protokolas. Tinklo architektūroje konsensuso funkcija atskirta – specialūs mazgai (angl. „Ordering Service Nodes“, arba užsakymo mazgai) surenka transakcijas į blokus ir užtikrina jų užsakymą, o kiti mazgai (angl. peers) vykdo transakcijas ir tikrina jų galiojimą pagal iš anksto nustatytą politiką. Dėl tokio požiūrio (transakcijų vykdymo, užsakymo ir patvirtinimo atskyrimo) Fabric galima lanksčiai keisti konsensuso komponentą nepriklausomai nuo išmaniųjų sutarčių logikos.

„R3 Corda“. „R3 Corda“ neturi bendros blokų grandinės – transakcijos dalijamos tik tarp susijusių šalių. Galiojimą tikrina patys dalyviai, o dvigubas išlaidas užkerta Notaro mazgas. Konsensusas pasiekiamas sandorio lygmeniu, suteikiant didesnį privatumą.

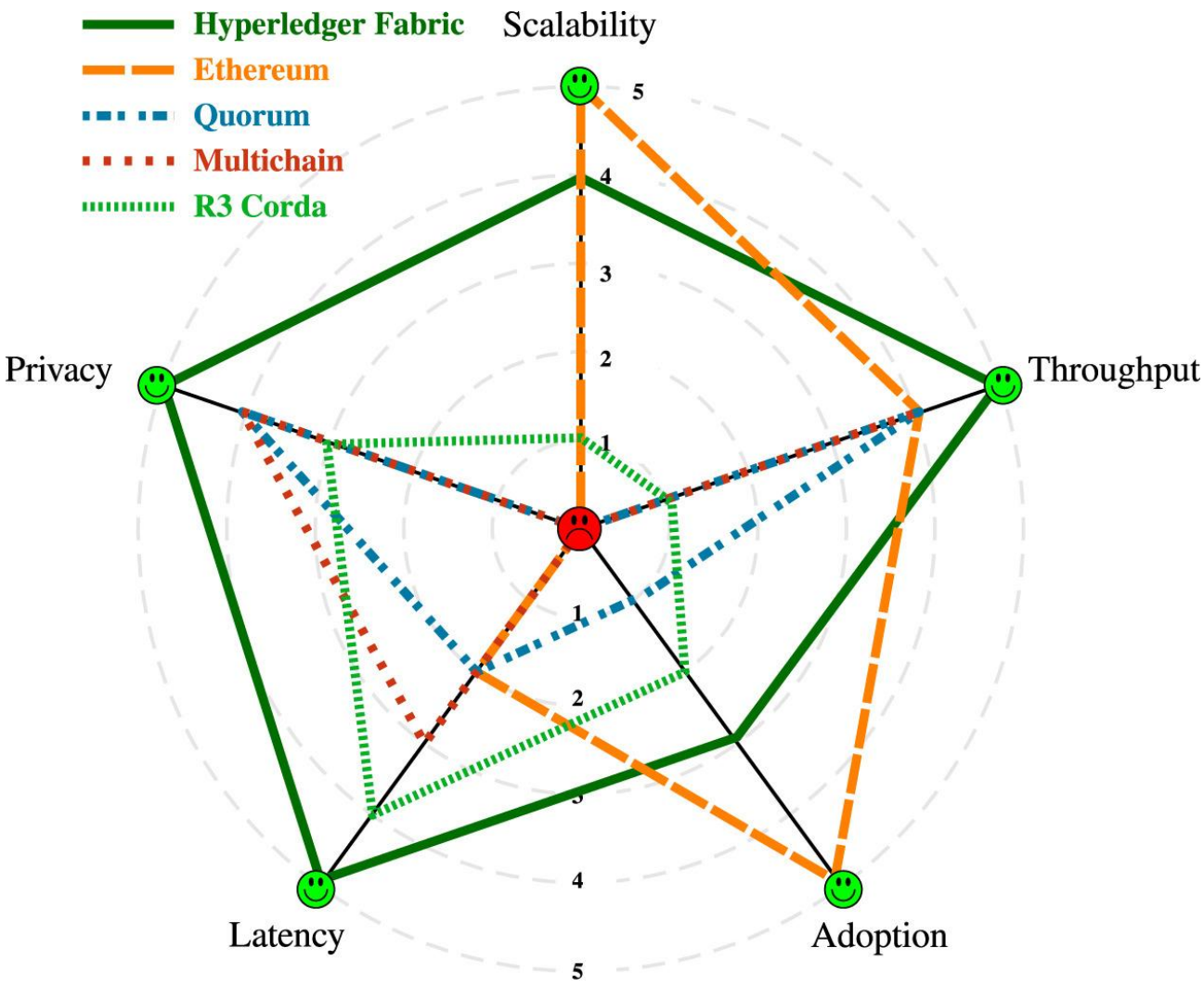
„Quorum“. „Quorum“ yra privatūs Ethereum tinklai, palaikantys EVM išmaniąsias sutartis. Vietoje kasimo naudojami RAFT (CFT) arba IBFT (BFT) konsensuso algoritmai tarp leidžiamų mazgų.

„MultiChain“. MultiChain leidžia tik autorizuotiems mazgams kurti blokus, kurie tai daro paeiliui. Nėra „Proof of Work“ – konsensusas grindžiamas pasitikėjimu dalyviais ir CFT modeliu. Sprendimas paprastas ir greitas, bet neatsparus piktavališkiems mazgams.

2.2.2. Našumas: pralaidumas, vėlavimas, mastelio keitimas

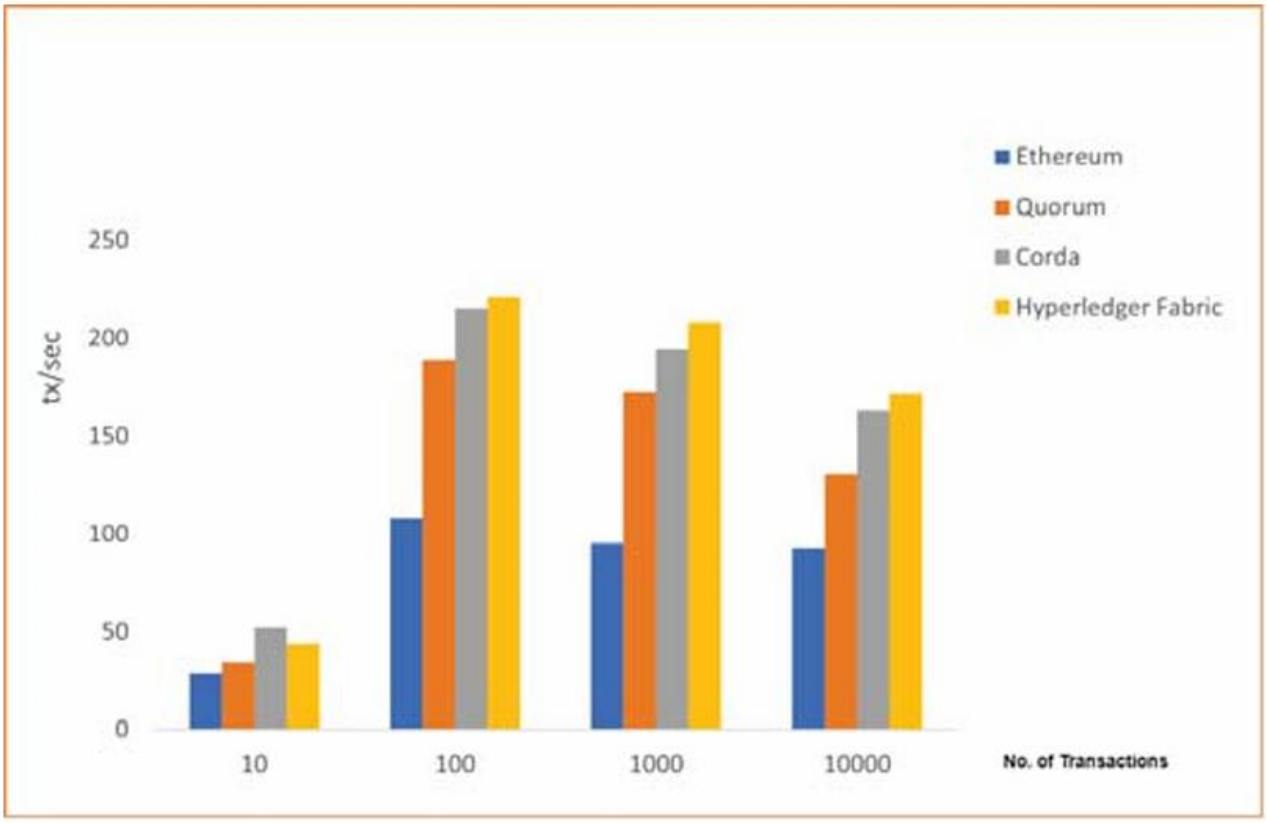
Našumas apima, kiek transakcijų per sekundę platforma pajėgi patvirtinti (pralaidumas, TPS angl. trasactions per second), kiek laiko užtrunka transakcijos patvirtinimas (vėlavimas, angl. latency) ir kaip šie rodikliai kinta didėjant masteliui (angl. scalability). Viešos blokų grandinės sunkiai pasiekia didelį našumą dėl lėto konsensuso mechanizmo ir didelio dalyvių skaičiaus. Privačiose platformose, kontroliuojant dalyvių skaičių ir naudojant efektyvesnį konsensusą, pasiekiamas žymiai didesnis pralaidumas ir mažesnis vėlavimas. Visos lyginamos platformos deklaruoja aukštesnį našumą nei viešos grandinės, tačiau jų realus palyginimas sudėtingas, nes atlikti tyrimai naudoja skirtingas versijas, konfigūracijas ir testavimo sąlygas. Nepaisant to, literatūros apžvalga leidžia išskirti tam tikras tendencijas.

Pagal Polge su kolegomis apibendrintą keliolikos tyrimų analizę (Polge, Robert, & Le Traon, 2021), „Hyperledger Fabric“ demonstravo aukščiausius našumo rodiklius tarp visų platformų (žr. 4 pav.)



4 pav. Bendras bloko grandinių technologijų palyginimas (Polge, Robert, & Le Traon, 2021)

Audito kriterijais suteikus geriausiai platformai įvertinimą 5, „Fabric“ gavo 4.2,“ Ethereum“ (privatus) – 3.3, o „Quorum“,“ Corda“ ir „MultiChain“ – apie 2.0–2.2 balo. Tai reiškia, kad „Fabric“ aplenkė kitas platformas pagal derinį pralaidumo, vėlavimo ir mastelio keitimo metrikų. Monrat ir kt. (Monrat, Schelén, & Andersson, 2020) eksperimentiškai patvirtino šią išvadą: „Hyperledger Fabric“ jų bandymuose aplenkė „Ethereum“ (PoA režimu) ir „Quorum“ didele persvara, o taip pat buvo šiek tiek pranašesnė už „Corda“ našumo atžvilgiu (žr. 5 pav.)



5 pav. Ethereum, Qourum, Corda ir Hyperledger Fabric pralaidumo palyginimas (Monrat, Schelén, & Andersson, 2020)

„Fabric“ pasižymėjo trumpiausiu transakcijos patvirtinimo laiku tarp visų tirtų platformų. Toks efektyvumas siejamas su „Fabric“ moduliniu konsensuso mechanizmu ir lygiagrečiu transakcijų apdorojimu (lygiagrečiai vykdomi sandoriai skirtingose grandinės kanalų aplinkose). „Quorum“ platformos našumas eksperimentuose buvo prastesnis – didėjant mazgų skaičiui, sandorių vėlavimas augo beveik tiesiškai, o maksimalus pralaidumas siekė tik kelis šimtus TPS. „Corda“ atvirojo kodo versija („Corda OSS“) paprastai apsiriboja keliomis dešimtimis TPS dėl to, kad kiekviena transakcija reikalauja unikalaus notaro patvirtinimo; vis dėlto naujesnės „Corda Enterprise“ versijos ženkliai pagerino našumą (pvz., „Corda Enterprise“ 4.4–4.5 pasiekė >2x didesnį TPS palyginti su 4.3 versija, optimizavus lygiagretų srautų vykdymą). „MultiChain“ literatūroje vertintas rečiau – Polge pažymi (Polge, Robert, & Le Traon, 2021) , kad nėra daug eksperimentinių duomenų apie „MultiChain“ pralaidumą didesnėse konfigūracijose. „MultiChain“ 1.0 versija neturėjo pažangių optimizacijų, tačiau dėl supaprastinto konsensuso mažoje privačių mazgų grupėje gali pasiekti šimtų TPS eilės pralaidumą (blokų generavimo intervalą galima konfigūruoti. Apibendrinant, „Hyperledger Fabric“ vertinama kaip labiausiai pritaikyta dideliam transakcijų kiekiui apdoroti, nors ir ji susiduria su mastelio keitimo iššūkiais (pvz., tinklui viršijant kelias dešimtis mazgų, pralaidumas mažėja). Tuo tarpu „Corda“ ir „Quorum“ gali geriau tikti mažesnėms, specializuotoms grupėms, kur itin didelio TPS nereikia, o „MultiChain“ tinkama nedidelėms privačioms diegimo aplinkoms su ribotu dalyvių skaičiumi.

2.2.3. Audituojamumas ir skaidrumas

Audituojamumas ir skaidrumas – tai gebėjimas atsekti sistemos operacijas, patikrinti jų teisingumą ir užtikrinti, kad duomenys nebuvo klastojami. Blokų grandinės technologija savo

prigimtimi suteikia tam tikrą skaidrumo ir audito garantiją: kiekvienas tinklo dalyvis turi prieigą prie savo registro kopijos, o visi blokų istorijos pakeitimai išsaugomi nekeičiant ankstesnių duomenų. Dėl grandinės nekintamumo galima patikrinti, kokia buvo sistemos būsena praeityje, ir įsitikinti, kad nė viena transakcija nebuvo neteisėtai pakeista ar ištrinta. Vis dėlto audito požiūriu svarbios detalės: ar visi audituotini duomenys prieinami vienoje vietoje, ar jie paskirstyti, ar galima nustatyti, kas atliko konkrečią operaciją.

„Hyperledger Fabric“ aplinkoje audituoti paprasčiausia tuos duomenis, kurie yra bendrame kanale. Kiekvienas Fabric mazgas saugo pilną atitinkamo kanalo blokų grandinę, todėl reguliuotojas ar auditorius, turintis prieigą prie kanalo, gali gauti pilną transakcijų žurnalą. Kadangi visi dalyviai identifikuoti (pagal sertifikatus), kiekvieną transakciją galima priskirti konkrečiai organizacijai ar net naudotojui, pasirašiusiam ją skaitmeniniu parašu. Tai palengvina finansinių srautų sekimą ir atsakomybės priskyrimą – audito metu galima parodyti ne tik “kas ir kada” įvyko, bet ir “kas patvirtino”, nes „Fabric“ transakcijos reikalauja patvirtinimo (angl. endorsement) – kelių narių pritarimo pagal nustatytą politiką. P2P skolinimo atveju tai reiškia, kad, pvz., paskolos sutarties sudarymą gali patvirtinti abi pusės ir tai bus užfiksuota; vėliau galima patikrinti, jog sutartį iš tiesų patvirtino tam įgalioti subjektai, o duomenys nepakito. Skaidrumo lygį „Fabric“ galima reguliuoti: visi kanalo nariai mato viską tame kanale, bet jei duomenys labai jautrūs, jie gali būti atskirti į privatų rinkinį – tuomet audituoti galės tik tie, kam suteikta prieiga (pvz., priežiūros institucija). Tai lankstu, bet reikalauja teisingai nustatyti, kad auditoriai būtų įtraukti ten, kur reikia.

„Corda“ aplinkoje nėra bendros blokų grandinės – kiekvienas mazgas mato tik savo transakcijas. Dėl to auditas yra sudėtingesnis: auditorius turi gauti duomenis iš visų dalyvių arba būti įtrauktas kaip „stebėtojas“ į transakcijas. Praktikoje dažnai naudojamas specialus audito ar reguliatoriaus mazgas. Tai užtikrina privatumą, bet reikalauja papildomų sprendimų audito duomenims surinkti.

„Quorum“ tinkle viešos transakcijos matomos visiems dalyviams, todėl jas lengva audituoti. Privačias transakcijas mato tik jų gavėjai, tad auditorius turi būti įtrauktas tarp jų arba gauti duomenis iš dalyvių. Dažnai reguliatorius iš anksto pridedamas kaip privačių transakcijų gavėjas. Taip suderinamas privatumas su audito reikalavimais.

„MultiChain“ tinkle visi autorizuoti dalyviai turi pilną blokų grandinės kopiją. Todėl auditas yra paprastas – bet kuris narys gali matyti visą istoriją. Transakcijos siejamos su adresais, kurie konsorciume priskiriami konkrečioms organizacijoms. Tai suteikia didelį skaidrumą, bet mažiau privatumo.

2.2.4. Bloko grandinės technologijų pasirinkimas

Atsižvelgiant į atliktą analizę, šiame darbe eksperimentinei daliai pasirinkta „Hyperledger Fabric“ platforma dėl keleto įtikinamų priežasčių. Pirma, „Fabric“ išsiskiria savo moduline architektūra ir lankstumu, leidžiančiu pritaikyti sistemą pagal P2P skolinimo platformos poreikius. P2P skolinimo atveju turime kelias dalyvių grupes – skolintojus, skolininkus, tarpininką (platformos operatorių) ir priežiūros institucijas. „Fabric“ kanalo mechanizmas užtikrina duomenų konfidencialumą (detalės matomos tik dalyvaujančioms šalims) ir. Nors analogišką privatumą galėtų pasiūlyti ir „Corda“ (su point-to-point sandoriais) ar „Quorum“ (su privačiomis transakcijomis), „Fabric“ privalumas – patogi prieigos valdymo infrastruktūra.

Antra, „Hyperledger Fabric“ demonstruoja aukštą našumą ir tinklo efektyvumą, lyginant su kitomis aptartomis platformomis. P2P skolinimo scenarijuje tai svarbu, nes platformoje gali vykti daug smulkių transakcijų (pvz., paskolų pasiūlymų teikimas, sutarčių sudarymas, įmokų registravimas). Remiantis literatūra, „Fabric“ gali apdoroti kelis šimtus transakcijų per sekundę net be specialių optimizacijų, o pritaikius tinkamus nustatymus – ir daugiau. Tai suteikia pasitikėjimo, kad prototipo masto sistema veiks sklandžiai ir nebus veiklos trukdžių. Mažas „Fabric“ sandorių vėlavimas reiškia, jog vartotojai (skolininkai ir skolintojai) galės beveik realiu laiku gauti patvirtinimus dėl savo veiksmų, kas gerina naudotojo patirtį ir atitinka šiuolaikinių finansinių platformų standartus.

Trečia, audituojamumo ir skaidrumo požiūriu „Fabric“ taip pat yra itin tinkamas pasirinkimas. Siekiama pasiekti audito procesų stiprinimą, o „Fabric“ pasižymi nekintančiu įrašų žurnalu, kurį galima tiesiogiai suteikti auditoriams. Pavyzdžiui, platformoje galima įsteigti atskirą auditoriaus mazgą, priklausantį, tarkime, priežiūros institucijai (pvz., Lietuvos bankui ar kitai finansų priežiūros įmonei). Tas mazgas gali būti prijungtas prie visų kanalų kaip stebėtojas, suteikiant jam prieigą prie visų P2P paskolų sutarčių duomenų realiu laiku. „Fabric“ kanalų politika leidžia tai padaryti gana nesunkiai – auditoriaus organizacijai suteikiamos skaitymo teisės visuose kanaluose, ir jos mazgas gaus visus blokų duomenis. Taip auditorius galės savarankiškai ir tiesiogiai tikrinti grandinėje fiksuotus duomenis, negendant jų patikimumu. Kadangi visi „Fabric“ transakcijų veiksmai yra pasirašyti identifikuotų šalių raktų, auditas galės atsekti “ką, kas ir kada” atliko. Tai milžiniškas pranašumas prieš tradicinį auditą, kur tenka kliautis centralizuotų duomenų bazių įrašais ir imti daugumos paaiškinimus – čia patikimumą garantuoja pati technologija.

Ketvirta, „Hyperledger Fabric“ plačiai palaikomas ir dokumentuotas, kas labai svarbu akademiniam eksperimentui. Yra gausybė pavyzdžių, atvirojo kodo įrankių (pvz., „Hyperledger Caliper“ našumo matavimams, „Explorer“ duomenų peržiūrai) ir aktyvi bendruomenė, galinti pagelbėti sprendžiant iškilusias problemas. Renkantis platformą darbui, kur laikas ir ištekliai riboti, tai ženkliai sumažina riziką nepasiekti rezultato dėl techninių kliūčių.

Apibendrinant, „Hyperledger Fabric“ geriausiai atitinka P2P skolinimo platformos poreikių ir reguliacinių reikalavimų sankirtą: ji garantuoja dalyvių identifikavimą ir prieigos kontrolę, suteikia lanksčias privatumo priemones jautriai informacijai apsaugoti, užtikrina aukštą sandorių apdorojimo spartą, ir tuo pačiu sukuria skaidrią, audituojamą aplinką, kurioje visi veiksmai fiksuojami nekintamai. Toks pasitikėjimo ir efektyvumo derinys yra būtent tai, ko siekiama diegiant blokų grandinės technologiją audito procesuose. Dėl šių argumentų tolimesniame darbe prototipo realizacijai pasirinkta „Hyperledger Fabric“ platforma, tikintis, kad ji leis praktiškai pademonstruoti blokų grandinės privalumus audituojant tarpusavio skolinimo transakcijas ir padės pagrįsti šios technologijos naudą tarpusavio skolinimo platformos finansinės veiklos ataskaitų ir audito procesuose.

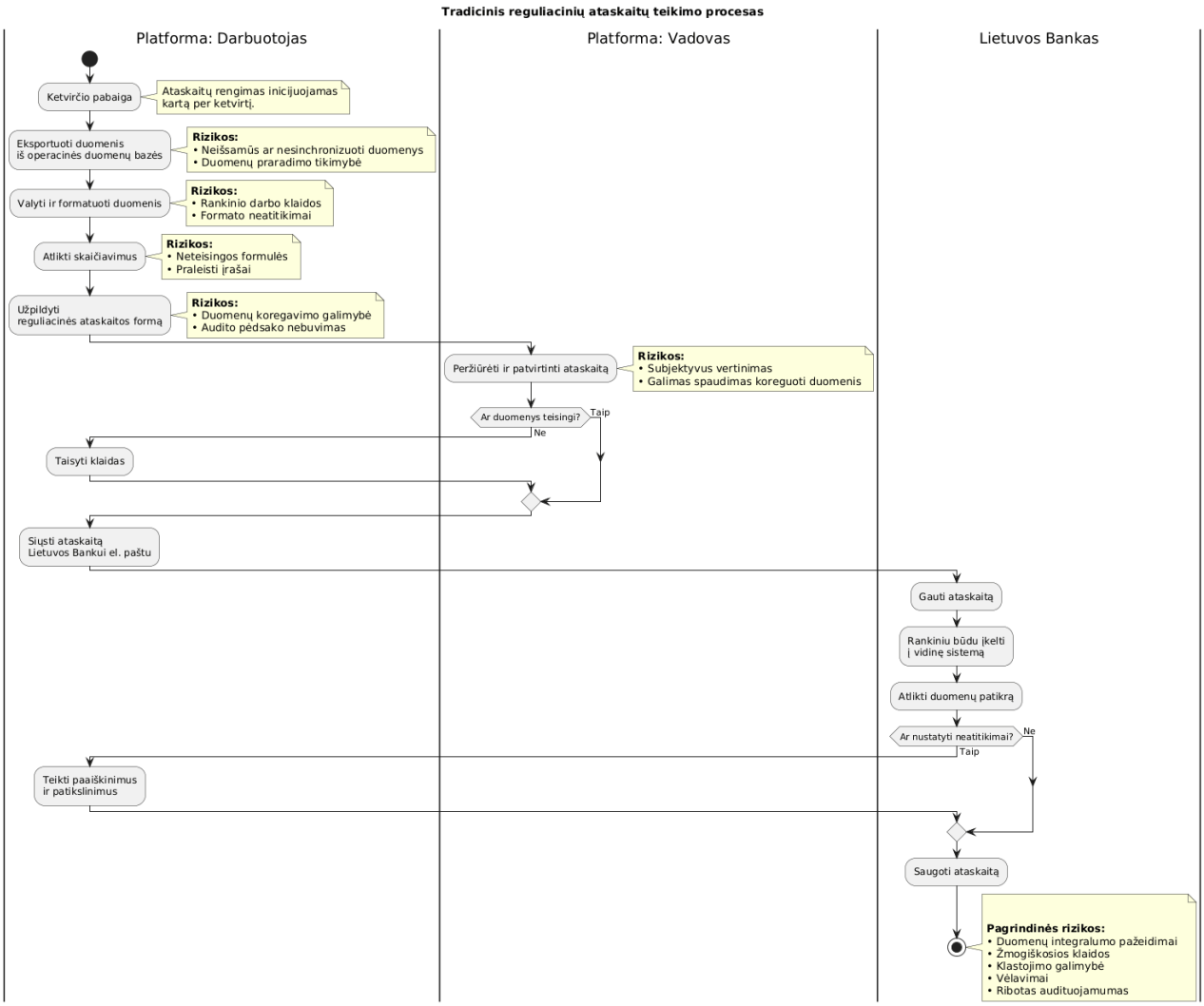
2.3. Blokų grandinės integravimo į finansinės veiklos ataskaitą modelis

Reguliacinis ataskaitų teikimas P2P skolinimo sektoriuje yra itin svarbus siekiant užtikrinti veiklos skaidrumą ir atitiktį finansų priežiūros reikalavimams. P2P platformos, veikdamos kaip tarpininkai tarp skolintojų ir skolininkų, privalo reguliariai teikti detalias ataskaitas priežiūros institucijai – Lietuvos bankui (LB) (Lietuvos Bankas, 2018). Tradiciškai šie procesai vykdomi pusiau

rankiniu būdu, pasitelkiant vidines ataskaitų ruošimo sistemas ar skaičiuokles, o tai sukuria nemažai iššūkių.

Tradiciniuose P2P ataskaitų teikimo procesuose išryškėja kelios pagrindinės problemos (remiantis 1.5 poskyryje aptartomis išvadomis). Pirma, duomenys kaupiami skirtingose sistemose ir nėra centralizuotai prieinami priežiūros institucijai realiu laiku, todėl trūksta skaidrumo. Antra, didelė dalis veiksmų atliekama žmogaus – duomenų surinkimas, formatavimas, tikrinimas – todėl išauga klaidos rizika. Trečia, ataskaitos rengiamos periodiškai (kas ketvirtį), todėl priežiūros institucija negali vykdyti nuolatinės stebėsenos – informacija atkeliauja pavėluotai. Galiausiai, pats rankinis ataskaitų rengimas reikalauja laiko ir išteklių. Apibendrinant, tradicinis metodas dažnai yra lėtas, neefektyvus lyginant su galimu automatizuotu būdu.

Automatizavus reguliacinį ataskaitų teikimą, galima sumažinti ne tik klaidų kiekį, bet ir padidinti bendrą skaidrumą. Šiame poskyryje apžvelgiama automatizuoto reguliacinio ataskaitų teikimo procesas tarpusavio skolinimo platformoje – nuo tradicinio ir blokų grandine pagrįsto modelio palyginimo iki automatinės ataskaitų generavimo eigos paaiškinimo. (žr. 6 pav.)



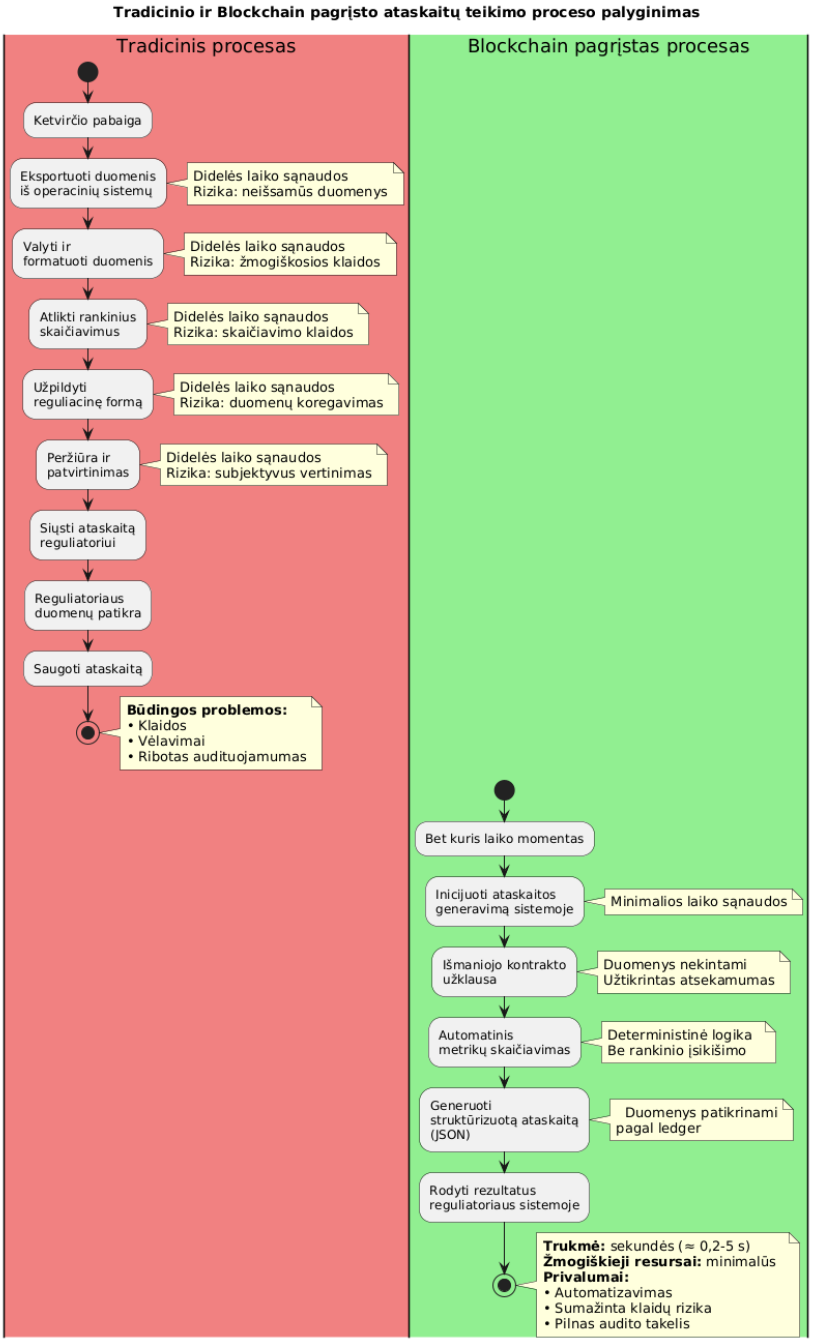
6 pav. Tradicinis finansinės veiklos ataskaitų teikimo procesas

Tradicinis reguliacinių ataskaitų ruošimo kelias P2P platformose susideda iš kelių etapų:

1. Platformos darbuotojai arba IT sistema iš vidinių duomenų bazių surenka visus priežiūrai reikalingus duomenis (pvz., naujų suteiktų paskolų sumas, grąžinimo grafikus, vėluojančias įmokas, investuotojų skaičių ir pan.).
2. Surinkti duomenys eksportuojami į nustatytą formatą (Excel formatą). Šiame žingsnyje gali prireikti duomenis transformuoti, apjungti iš skirtingų sistemų, pritaikyti prie nustatytų ataskaitos šablonų.
3. Parengtos ataskaitos duomenys tikrinami atsakingų darbuotojų, lyginami su pirminiais šaltiniais siekiant išvengti klaidų. Neretai aptikus neatitikimų, duomenis tenka taisyti ir vėl kartoti tikrinimo procesą.
4. Galutinė ataskaita pateikiama Lietuvos bankui per tam skirtą informacinę sistemą. LB gavęs duomenis gali juos papildomai analizuoti, lyginti su ankstesnėmis ataskaitomis, o nustačius netikslumus – paprašyti patikslinimų.

Akivaizdu, kad tradiciniame procese kiekviename žingsnyje dalyvauja žmogus, todėl visas kelias yra lėtas ir linkęs į klaidas. Tarpiniuose etapuose perduodant duomenis gali atsirasti neatitikimų Toks ataskaitų rengimo įgyvendinimas yra būna sudėtingas, brangus ir užima daug laiko; rankinis duomenų derinimas bei formų pildymas lemia, jog galutinis rezultatas ne visuomet tenkina priežiūros institucijos lūkesčius

Naudojant blokų grandinės technologija grindžiamą sprendimą, siūlomas visiškai kitoks kelias (žr. 7 pav.)



7 pav. Tradicinio ir blokų grandine pagrįsto ataskaitų teikimo proceso palyginimas

Schematiškai lyginami tradicinis ir blokų grandine pagrįstas ataskaitų teikimo procesai. Kairėje pusėje pavaizduotas tradicinis modelis su daugybe etapų ir žmogiškų įsikišimų, o dešinėje – supaprastintas blokų grandinės sprendimo modelis.

Blokų grandinės technologijos taikymas leidžia užtikrinti, kad visi reikšmingi tarpusavio skolinimo platformų veiklos įvykiai būtų registruojami realiu laiku. Kiekvienas naujos paskolos suteikimas ar kitas reguliavimui svarbus veiksmas sistemoje fiksuojamas kaip atskira transakciją, į kurią įtraukiami visi būtini duomenys, tokie kaip paskolos suma, valiuta, palūkanų norma, terminas, sutarties sudarymo data bei sandorio šalys. Tokiu būdu duomenys įrašomi į blokų grandinę iš karto. Jei atsiranda poreikis patikslinti ar papildyti informaciją, tai daroma ne keičiant esamą įrašą, bet

registruojant naują transakciją, kuri logiškai susiejama su ankstesne. Šis principas užtikrina duomenų nekintamumą ir leidžia aiškiai atsekti visą informacijos pokyčių istoriją.

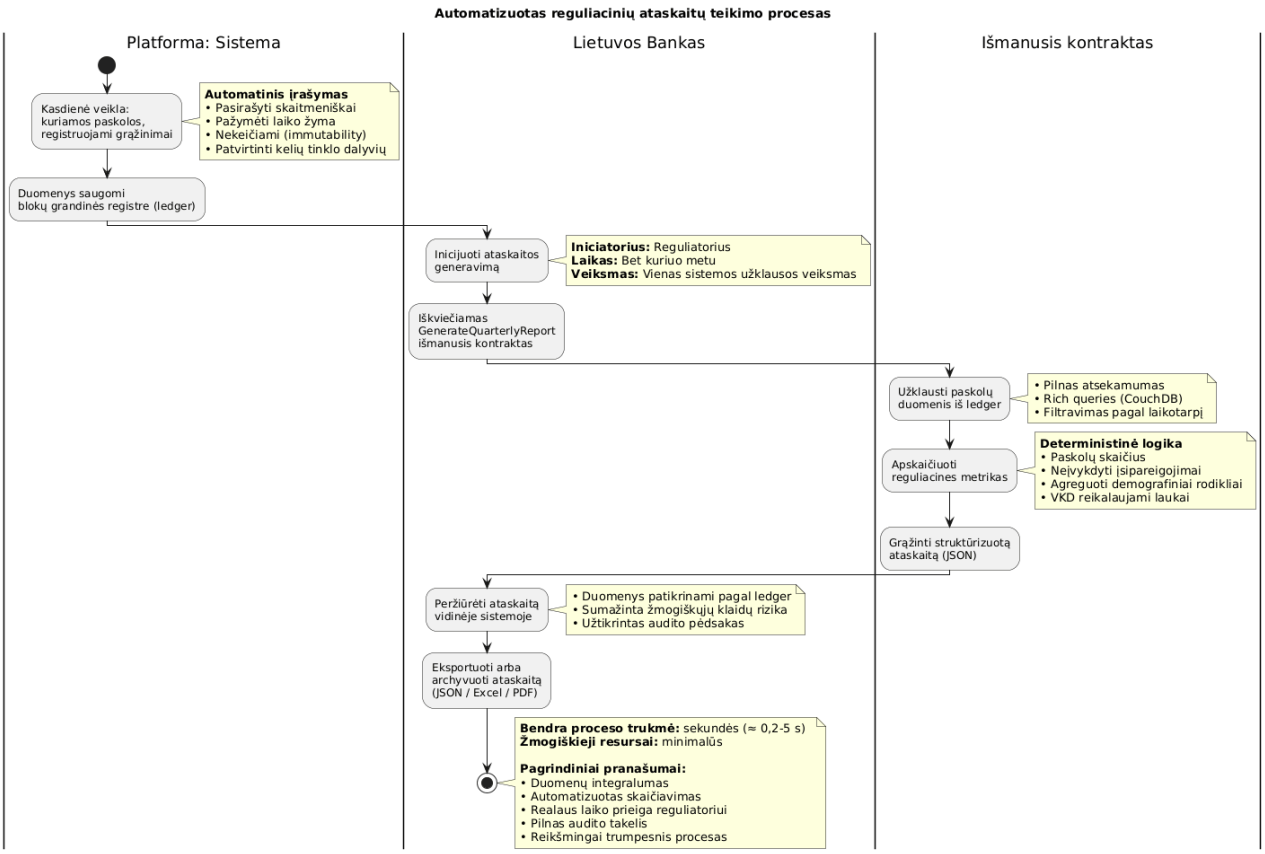
Kadangi blokų grandinė veikia kaip bendra, visiems dalyviams prieinama duomenų infrastruktūra, visi tinklo mazgai nuolat palaiko vienodą registro kopiją. Tai reiškia, kad tarpusavio skolinimo platformos, investuotojai ir priežiūros institucija remiasi tais pačiais duomenimis. Tokia architektūra pašalina tradiciniuose modeliuose dažnai pasitaikančius duomenų neatitikimus tarp skirtingų sistemų ir sumažina poreikį papildomam duomenų tikrinimui tarp šalių.

Svarbų vaidmenį šiame procese atlieka išmaniosios sutartys (angl. smart contracts), kurios leidžia reguliacinius ir verslo reikalavimus perkelti tiesiogiai į programinį kodą. Jose gali būti apibrėžtos taisyklės, pagal kurias automatiškai tikrinama, ar į blokų grandinę įrašomi duomenys atitinka nustatytus kriterijus, pavyzdžiui, ar kiekvienai paskolai priskirtas unikalus identifikatorius, ar neviršijamos reglamentuotos sumos. Duomenys, neatitinkantys šių reikalavimų, negali būti patvirtinti arba yra iš karto pažymimi papildomai peržiūrai. Tokiu būdu duomenų kokybės kontrolė vykdoma iš anksto, o ne po fakto, todėl sumažėja rankinio taisymo ir aiškinimosi poreikis.

Kadangi visi reguliavimui reikalingi duomenys jau saugomi blokų grandinėje, priežiūros institucija turi galimybę bet kuriuo metu pasiekti naujausią informaciją. Praktiškai tai gali būti įgyvendinama suteikiant priežiūros institucijai atskirą tinklo mazgą, per kurį ji realiu laiku stebi naujus sandorius ir duomenų atnaujinimus. Toks sprendimas leidžia pereiti nuo periodinio ataskaitų teikimo prie nuolatinės, realiu laiku vykdomos rinkos stebėsenos.

Galiausiai, oficialių ataskaitų rengimo procesas taip pat gali būti integruotas į šią infrastruktūrą. Kai ateina laikas teikti reguliacines ataskaitas, jos gali būti sugeneruojamos automatiškai, tiesiogiai iš blokų grandinėje sukauptų duomenų. Tai reiškia, kad nebereikia atskiro duomenų rinkimo, agregavimo ar papildomo tikrinimo ciklo – pakanka pradėti ataskaitos formavimo procesą, o išmanieji kontraktai tai atlieka automatiškai.

Apibendrinant, blokų grandine pagrįstas modelis iš esmės sujungia duomenų generavimą ir ataskaitų paruošimą į vieningą, automatinį procesą (žr. 8 pav.). Skirtingai nei tradiciniame metode, čia nėra atskirų duomenų ištraukimo, tikrinimo ir persiuntimo etapų – informacija į ataskaitai skirtą registrą patenka realiu laiku dar vykstant verslo operacijoms. Tai sumažina veiklos sąnaudas ir klaidų tikimybę, be to, užtikrina, jog priežiūros institucija turėtų prieigą prie tikslių duomenų beveik realiuoju laiku.

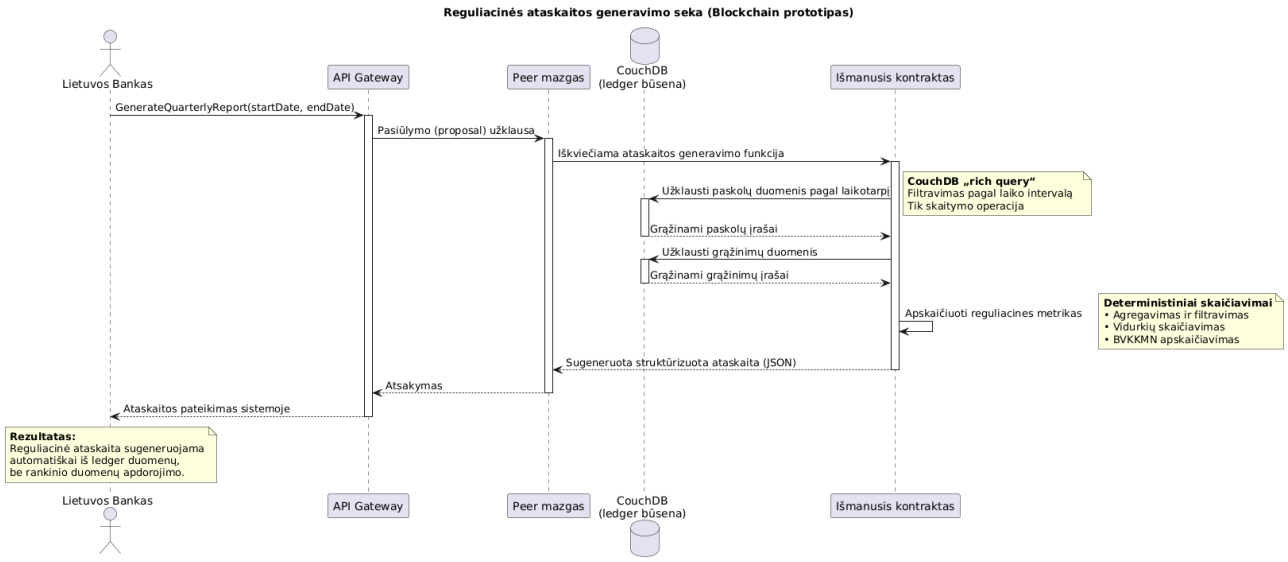


8 pav. Automatizuotas blokų grandine grįstas finansinės veiklos ataskaitų teikimo procesas

Žemiau pateikiamas reguliacinės ataskaitos duomenų modelis, naudojamas prototipe. Visi rodikliai agreguojami iš blokų grandinėje saugomų nekintamų įrašų, o pati struktūra atitinka Lietuvos banko reikalavimus ketvirtinėms P2P skolinimo platformų ataskaitoms. Toliau pateikiama siūloma ataskaitos generavimo sekos diagrama (žr. 9 pav.). Visas programinis kodas prieinamas 2 priede.

```
type RegulatoryReport struct {
    ReportPeriod  string `json:"reportPeriod"`
    StartDate     string `json:"startDate"`
    EndDate       string `json:"endDate"`
    GeneratedDate string `json:"generatedDate"`
    GeneratedBy   string `json:"generatedBy"`

    Snapshot  SnapshotMetrics  `json:"snapshot"`
    Period    PeriodMetrics    `json:"period"`
    Analytics AnalyticsMetrics `json:"analytics"`
}

type SnapshotMetrics struct {
    TotalLoansIssued   int `json:"totalLoansIssued"`
    RemainingAmount    int `json:"remainingAmount"`
    AmountExtended     int `json:"amountExtended"`
    TotalBorrowers     int `json:"totalBorrowers"`
    BorrowersUnder25   int `json:"borrowersUnder25"`
    TotalLenders       int `json:"totalLenders"`

    LoansDelayed       int `json:"loansDelayed"`
    LoansDelayed30to60 int `json:"loansDelayed30to60"`
    LoansDelayed60to90 int `json:"loansDelayed60to90"`
```

```
    LoansDelayed90Plus int `json:"loansDelayed90Plus"`

    DebtDelayed       int `json:"debtDelayed"`
    DebtDelayed30to60  int `json:"debtDelayed30to60"`
    DebtDelayed60to90  int `json:"debtDelayed60to90"`
    DebtDelayed90Plus  int `json:"debtDelayed90Plus"`
}

type PeriodMetrics struct {
    LoansIssued     int     `json:"loansIssued"`
    AmountIssued    int     `json:"amountIssued"`
    AvgBVKK         float64 `json:"avgBVKK"`
    AvgInterestRate float64 `json:"avgInterestRate"`
    TotalCostPaid   int     `json:"totalCostPaid"`
    AvgTermMonths   float64 `json:"avgTermMonths"`
    LoansDefaulted  int     `json:"loansDefaulted"`
    LoansCompleted  int     `json:"loansCompleted"`
    AmountRepaid    int     `json:"amountRepaid"`
    NewBorrowers    int     `json:"newBorrowers"`
    NewLenders      int     `json:"newLenders"`
}

type AnalyticsMetrics struct {
    LoansByStatus     map[string]int `json:"loansByStatus"`
    TotalInterestRate float64        `json:"totalInterestRate"`
    TotalDefaultRate  float64        `json:"totalDefaultRate"`
}
```



9 pav. Finansinės veiklos ataskaitos generavimo sekos diagrama

Čia aprašomas automatinio ataskaitų generavimo procesas, nurodoma kaip priežiūros institucijos informacinė sistema, P2P platformos serveris ir blokų grandinės infrastruktūra sąveikauja ataskaitos formavimo metu. Procesas pradedamas tada, kai priežiūros institucijos sistema per saugią programinę sąsają pateikia užklausą gauti tam tikro laikotarpio ar tipo ataskaitą, kuri perduodama blokų grandinės sprendimui. Gavusi šią užklausą, platformos sistema automatiškai atrenka reikalingus duomenis iš blokų grandinės registro, išfiltruodama atitinkamus sandorius ir atlikdama būtinus apibendrinimus bei skaičiavimus pagal iš anksto apibrėžtas taisykles. Apdoroti duomenys

suformuojami į nustatytą ataskaitos struktūrą, atitinkančią priežiūros institucijos keliamus reikalavimus, todėl sugeneruota ataskaita jau pateikimo momentu yra parengta tiesioginiam naudojimui ir nereikalauja papildomo rankinio tikrinimo ar koregavimo. Parengta ataskaita perduodama priežiūros institucijai tuo pačiu saugiu ryšio kanalu, per kurį buvo inicijuota užklausa, o P2P platforma tuo pačiu metu užfiksuoja ataskaitos pateikimo faktą, sudarydama audito pėdsaką, diagramos pateikta seka parodo, kad ataskaitų teikimas tokioje architektūroje tampa integruota sistemos funkcija, o ne atskiru rankiniu procesu, leidžiančiu užtikrinti greitą informacijos pateikimą ir sumažinti klaidos tikimybes.

Apžvelgus tradicinį ir blokų grandine pagrįstą reguliacinio ataskaitų teikimo modelį P2P skolinimo sektoriuje, matyti esminiai skirtumai tiek procesų struktūroje, tiek jų efektyvume. Tradicinis ataskaitų rengimo būdas pasižymi fragmentuotais duomenų srautais, žmogiškųjų klaidų tikimybe ir periodiniu informacijos pateikimu, dėl ko išauga klaidų rizika, didėja administracinės sąnaudos ir ribojamos priežiūros institucijos galimybės vykdyti nuolatinę rinkos stebėseną. Tuo tarpu blokų grandinės technologija grindžiamas sprendimas leidžia sujungti duomenų generavimą, tikrinimą ir ataskaitų formavimą į vieningą, automatinį procesą, kuriame reguliavimui reikalinga informacija registruojama realiu laiku ir tampa iš karto prieinama visiems įgaliotiems dalyviams. Išmaniosios sutartys užtikrina duomenų kokybės kontrolę dar įrašymo momentu, o automatinis ataskaitų generavimas eliminuoja rankinio duomenų apdorojimo poreikį. Tokia architektūra sudaro prielaidas ne tik efektyvesniam reguliaciniam ataskaitų teikimui, bet ir didesniam skaidrumui, patikimumui bei operatyvesnei priežiūros institucijos reakcijai sparčiai besikeičiančioje P2P skolinimo rinkoje. Tolimesniuose skyriuose kalbama apie specifines prototipo architektūras

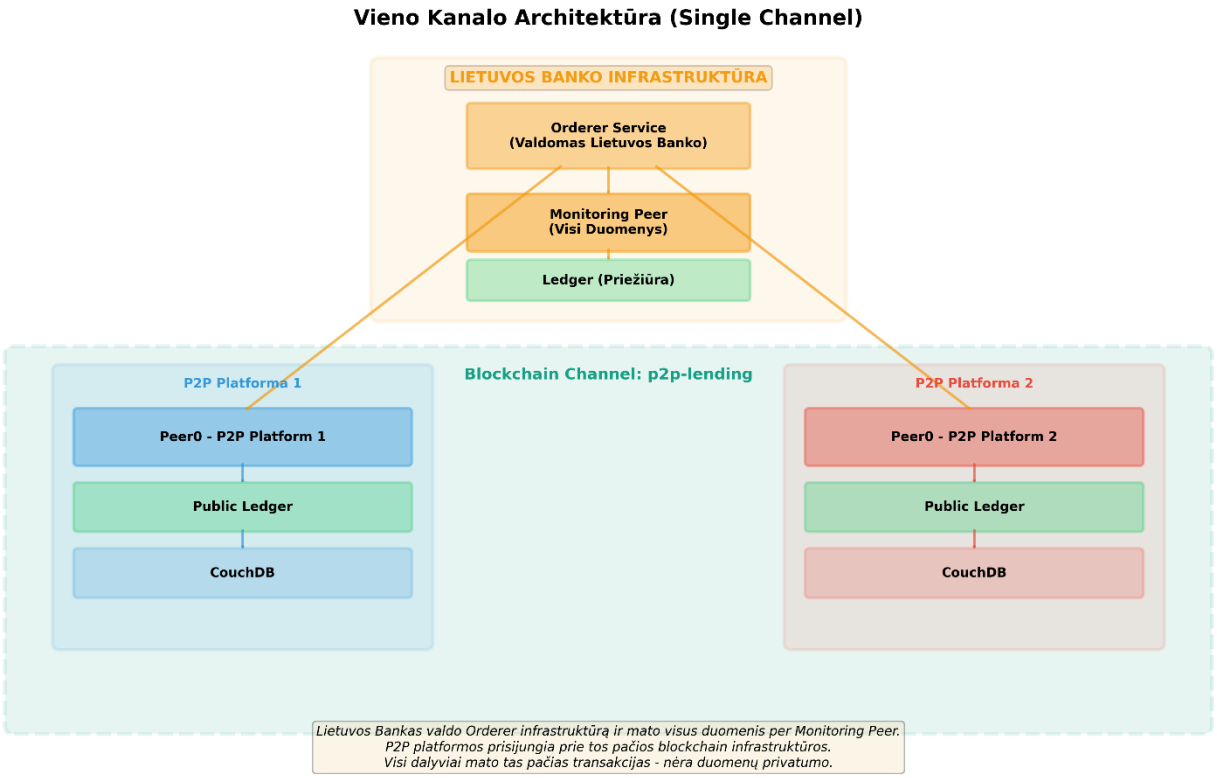
2.4. Prototipo architektūra

Metodika orientuota į kelių skirtingų architektūrinių scenarijų išskyrimą, jų palyginimą. Toks struktūruotas eksperimentinis požiūris grindžiamas ankstesnių tyrėjų darbais: Baliga su kolegomis (Baliga, et al., 2018) sistemingai analizavo „Hyperledger Fabric“ našumą, o Nguyen (Nguyen, Loghin, & Dinh, 2021) nagrinėjo „Fabric“ mastelio problematiką. Atsižvelgiant į šių autorių įžvalgas, šiame darbe planuojamas tyrimas siekia įvertinti skirtingų architektūrų privalumus ir trūkumus audito sistemos kontekste. Išrinkus tinkamiausią architektūrą, bus vykdomi našumo testai remiantis autorių jau naudotais testavimo moduliais. Architektūros pateikiama žemiau (lentelė 3), svarbu prieš kalbant apie architektūrą paminėti PDC (angl. Private Data Collections, privačios duomenų kolekcijos). Tai yra viena iš „Fabric“ funkcijų kurios leidžia jautrius duomenis laikyti privačiose kolekcijose, kurios nėra tiesiogiai prieinamos visiems kanalo nariams.

3 lentelė Architektūrų palyginimas

Architektūra	Kanalų struktūra	Privatumo lygis	Išmaniųjų kontraktų vykdymas	Lietuvos banko vaidmuo	BDAR atitikimas
Bendras kanalas (be PDC)	1 kanalas (visi bankai + LB vienoje grandinėje)	Žemas – visi mato viską	1 visiems nariams (vykdomas kiekvieno peer)	Pilnateisis kanalo narys (gauna ir mato visus duomenis; gali	Neužtikrinamas (duomenys atskleidžiami per plačiai)

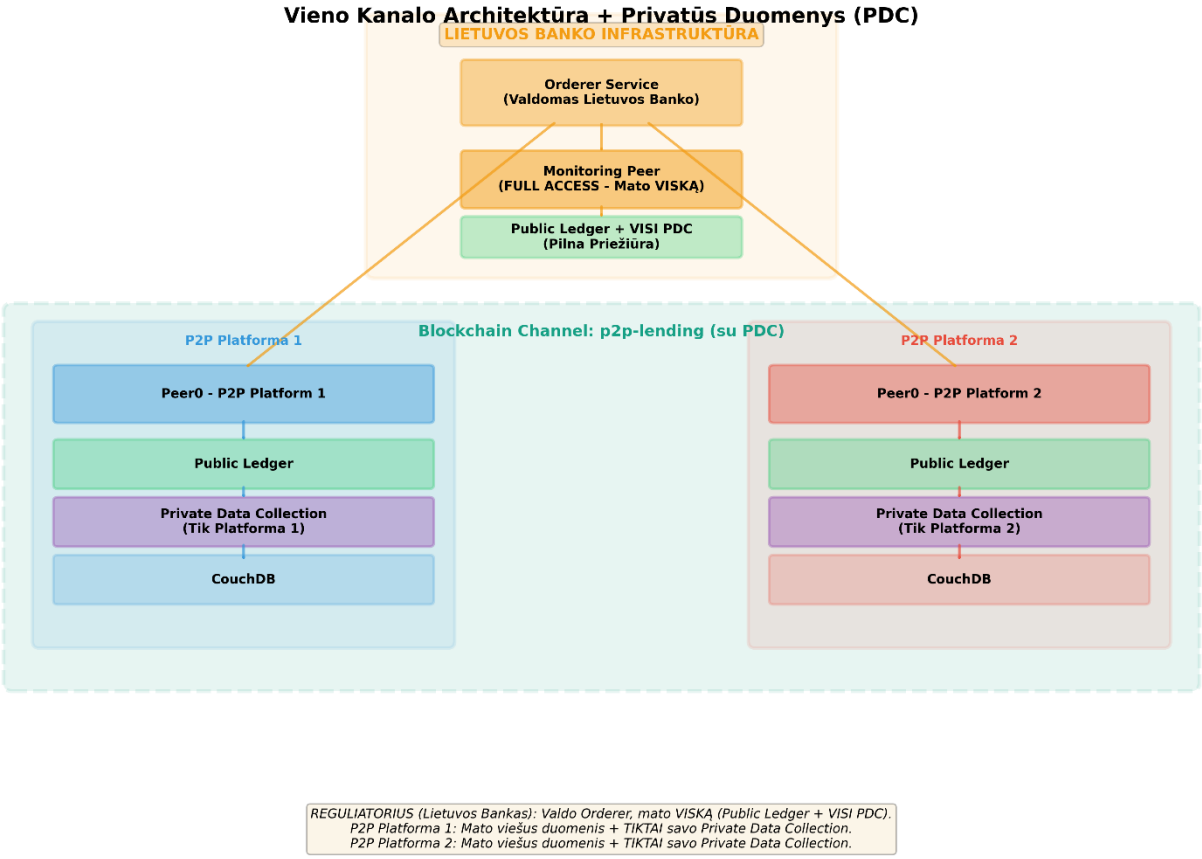
				tvirtinti sandorius)	
Bendras kanalas su PDC	1 kanalas (visi kartu) + privatus duomenų atskyrimas	Vidutinis – jautrūs duomenys slepiami kolekcijose	1 visiems (su PDC logika; duomenys skaidomi į viešus/privačius)	Kanalo narys, įtrauktas į atitinkamas kolekcijas (mato reikalingus privačius duomenis)	Užtikrinamas (nes neturintis teisės dalyviai mato tik maišą; ribojamas platinimas)
Atskirų kanalų	N atskirų kanalų (kiekvienam bankui atskiras su LB)	Aukštas – duomenys izoliuoti kanaluose	N atskirų (po 1 kiekviename kanale)	Dalyvauja visuose kanaluose (agreguoja duomenis; gali būti transakcijų tvirtintojas arba tik stebėtojas)	Užtikrinamas (kiekvienas kanalas privatus)



10 pav. Vieno kanalo architektūra

Vieno kanalo architektūra (žr. 10 pav.) visi dalyviai (Lietuvos bankas ir visos organizacijos) veikia viename bendrame kanale. Šiame variante visa informacija bendrai matoma visiems kanalo

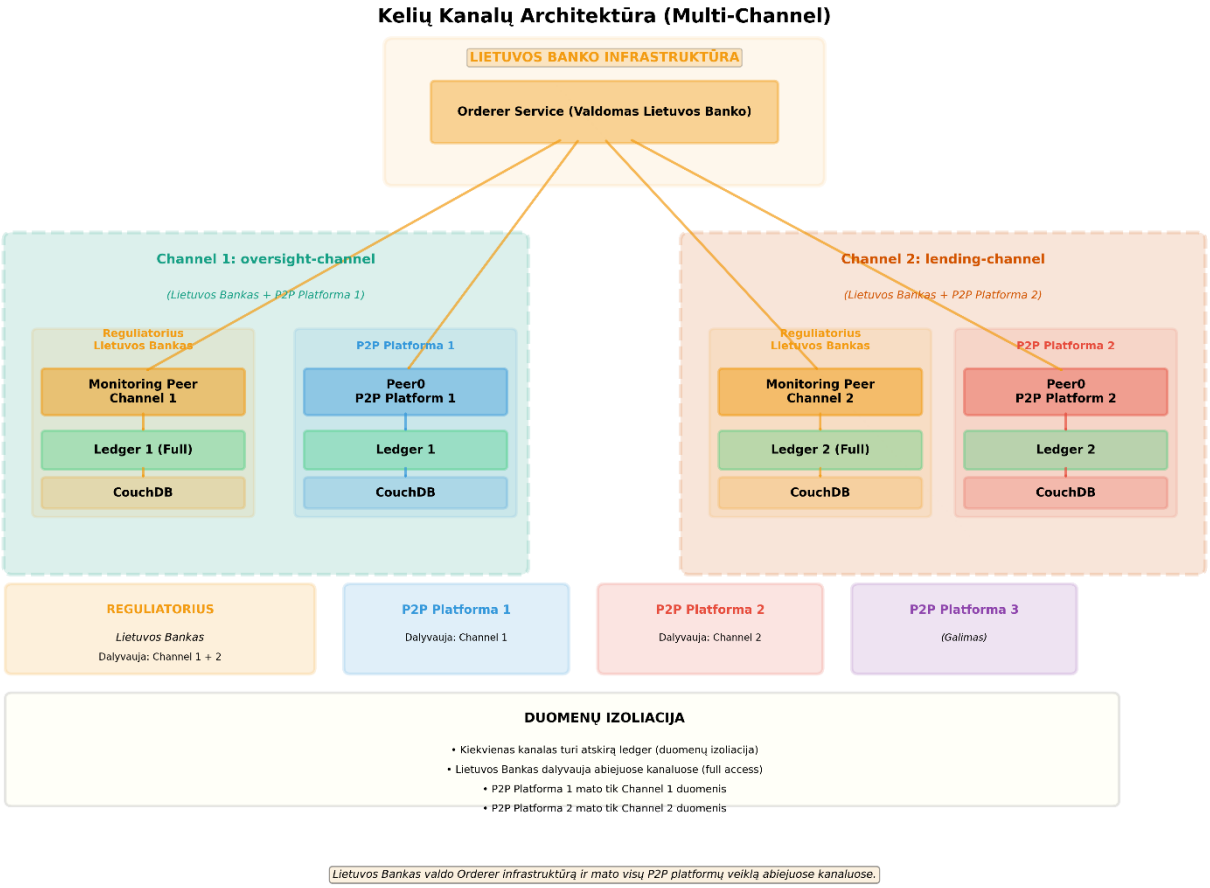
nariams – kiekviena transakcija įrašoma į bendrą knygą, prieinamą visoms organizacijoms. Toks sprendimas paprasčiausias valdyti (vienas kanalas, vientisa grandinė), tačiau privatumo lygis yra žemas, nes ir konfidencialūs duomenys būtų prieinami nereikalingiems subjektams (pvz., organizacijos matytų vieni kitų duomenis). BDAR atitiktis tokiu atveju nėra užtikrinama – asmens duomenys platinami platesniam ratui, nei būtina. Grandininis kodas (angl. chaincode – taip Hyperledger ekosistemoje vadinami išmanieji kontraktai) vykdomas visų kanalo narių mazguose (kiekviena organizacija turi įdiegtą grandininį kodą). Lietuvos bankas šiame scenarijuje yra pilnateisis kanalo narys, gaunantis visus duomenis; jis gali veikti pasyviai (tik gauti blokų duomenis) arba aktyviai (taip pat dalyvauti transakcijų tvirtinime). Kadangi infrastruktūra centralizuota viename kanale, tikėtinas efektyvumas yra didžiausias – nereikia derinti kelių kanalų, naudojama mažiau išteklių.



11 pav. Vieno kanalo architektūra su PDC (privačių duomenų kolekcijomis)

Bendro kanalo architektūra su privačių duomenų kolekcijomis (žr. 11 pav.) šis scenarijus – tai pirmojo scenarijaus variantas, pritaikytas didinti privatumą naudojant „Hyperledger Fabric“ privačių duomenų kolekcijų mechanizmą. Visi dalyviai lieka viename bendrame kanale, tačiau jautrūs duomenys nėra tiesiogiai įrašomi į visų bendrą knygą – vietoje to grandininis kodas juos saugo atskirose privačiose kolekcijose, prieinamose tik nustatytoms organizacijoms. Pavyzdžiui, konfidenciali transakcijos dalis bus matoma tik Lietuvos bankui ir atitinkamai organizacijai, o kiti kanalo nariai tą įrašą matys tik kaip neaiškinamą maišos reikšmę. Taip užtikrinamas vidutinis privatumo lygis: viešojoje kanalo knygoje lieka tik bendro pobūdžio informacija, o detalūs asmens

duomenys dalinami tik su tais dalyviams, kuriems reikia žinoti (pagal iš anksto apibrėžtą kolekcijos politiką). Šis sprendimas tiesiogiai orientuotas į BDAR suderinamumą – naudojant PDC, galima apriboti duomenų plitimą (kiekviena organizacija gauna tik būtinus duomenis) ir nustatyti duomenų gyvavimo trukmę. Kanalų struktūra išlieka paprasta (vis dar vienas kanalas), o išmaniųjų kontraktų vykdymas technologiškai nesiskiria nuo įprasto – tas pats grandininis kodas apdoroja tiek bendrus, tiek privačius duomenis (reikalingas papildomas kodas kolekcijų įrašams formuoti). Lietuvos banko vaidmuo analogiškas kaip ir pirmame scenarijuje – jis yra bendro kanalo narys, be to, įtraukiamas į visas privačių duomenų kolekcijas, kad galėtų matyti pilnus duomenis audito tikslais.



12 pav. Atskirų kanalų architektūra

Atskirų kanalų architektūra (žr. 12 pav.) – šiame scenarijuje kiekviena organizacija turi atskirą dedikuotą kanalą su Lietuvos banku. Tai reiškia, kad suformuojamas N kanalų (jei yra N audituojamų organizacija), ir kiekviename iš jų dalyvauja tik dvi šalys – konkreti organizacija ir Lietuvos bankas (galimi ir kiti variantai, kai kelios organizacijos grupuojami į kanalą, tačiau čia nagrinėjamas kraštutinis atvejis „po kanalą kiekvienam“ maksimaliam privatumui). Toks daugiakanalis modelis užtikrina aukščiausią privatumo lygį – duomenys izoliuoti: jokio kanalo turinys nėra prieinamas kitai organizacijai, kiekvienos organizacijos transakcijas mato tik ji pati ir centrinė institucija. BDAR atitiktis tokiu būdu pasiekiama natūraliai, nes asmens duomenys nėra bendrinami su trečiosiomis šalimis – kiekviename kanale jie lieka vietiniai to kanalo dalyviams. Išmaniųjų kontraktų vykdymas šiame scenarijuje vyksta lokaliai kiekviename kanale – reikia įdiegti

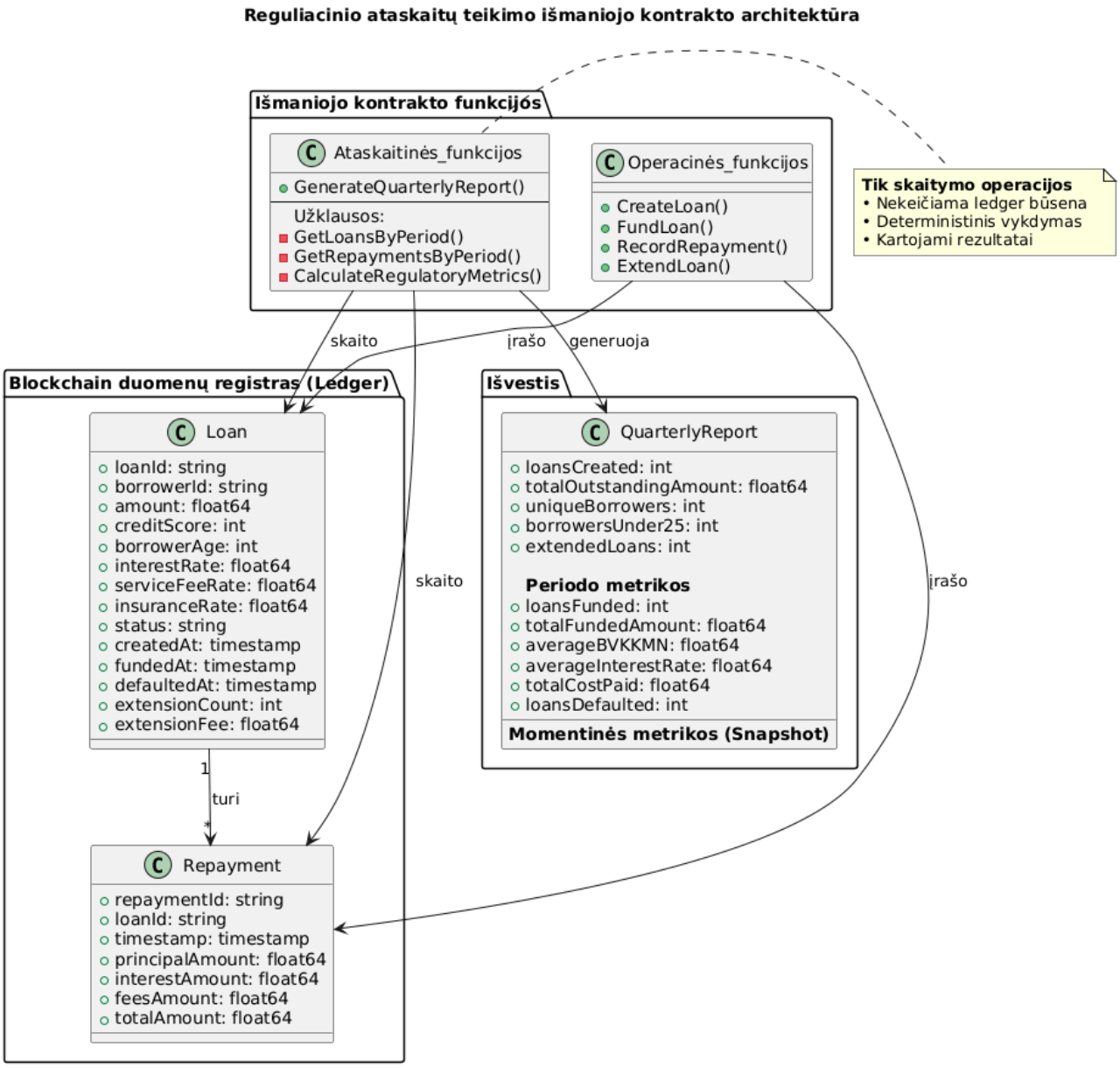
atskirą grandininio kodo instanciją kiekviename organizacijos - LB kanale. Transakcijos generuojamos ir vykdomos kiekviename kanale nepriklausomai; Lietuvos banko mazgai dalyvauja visuose kanaluose (gauna visų kanalų blokus), tokiu būdu Lietuvos bankas agreguoja visą audito informaciją iš atskirų srautų. Jo vaidmuo – būti jungiančiąja grandimi: LB yra bendras tinklo narys, turintis prieigą prie visų kanalų; jis gali pasirinkti dalyvauti kiekvieno kanalo transakcijų tvirtinime arba tik stebėti ir vėliau tikrinti duomenis. Pastaroji konfigūracija būtų efektyvesnė, nes tuomet kiekvieno sandorio tvirtinime nedalyvautų papildomas mazgas. Tikėtinas efektyvumas šioje architektūroje – mažesnis nei bendro kanalo variantuose. Taip yra dėl padidėjusios koordinavimo naštos: daugelio kanalų priežiūra reikalauja daugiau resursų, dubliuojamas grandininis kodas, o jei norima apdoroti tą pačią transakcijų apkrovą, ji pasiskirsto per kelis kanalus (didesnė apkrova bendram užsakymo servisui). Literatūroje pažymima, kad didėjant kanalų skaičiui, platformos pralaidumas pastebimai krenta – pavyzdžiui, Baliga (Baliga, et al., 2018) eksperimente padidinus kanalų skaičių iki 320, maksimalus pralaidumas sumažėjo ~52% lyginant su vieno kanalo atveju. Nors realioje audito sistemoje kanalų būtų tiek, kiek yra organizacijų (kur kas mažiau nei minėtas ekstremalus atvejis), ši tendencija rodo galimą horizontalų mastelio ribotumą: plečiant tinklą naujais kanalais, vieno kanalo pajėgumai negali būti pilnai išnaudojami problemų su bendrų resursų pasidalinimu.

Aprašyta eksperimentinė metodika leidžia kryptingai įvertinti skirtingų architektūrų tinkamumą audito sistemos poreikiams. Įvertinus skirtingas architektūras toliau nuspręsta tirti kelių kanalų architektūrą. Nors ir tikėtina, kad ji yra mažiau naši už vieną kanalą dėl komunikacijos ir lygiagretumo iššūkių ir reikalauja daugiau konfigūracijos – ji turi vieną didelį pliusą, natūralus BDAR pritaikymas ir paskirstymas – t.y. kanalų duomenys yra atskirti ir skirtingos P2P operatorių platformos net ir klaidos atveju nematytų kitos platformos privačių duomenų.

2.5. Duomenų šaltiniai ir įrankiai

Viena pagrindinių tyrime naudotų informacijos bazių yra Lietuvos banko reguliariai renkama vartojimo kredito davėjo veiklos ataskaita (Lietuvos bankas, 2012). Šią ataskaitą privalo teikti tiek vartojimo kreditų bendrovės, tiek tarpusavio skolinimo platformų operatoriai, siekdami užtikrinti finansinės veiklos skaidrumą ir priežiūrą. Ataskaitoje apibrėžti iš viso 66 rodikliai, apimantys pagrindinius vartojimo kreditų portfelio ir veiklos aspektus. Dėl ataskaitos struktūros dalis rodiklių yra dubliuojami: pusė jų skirta įprastiems vartojimo kreditams, o likusi pusė – mažiesiems vartojimo kreditams. Vadinasi, unikaliai ataskaita apima apie 33 skirtingus veiklos rodiklius (kiekvienas rodiklis turi atitikmenį mažųjų kreditų sekcijoje).

Šiame darbe analizuojami būtent įprastų vartojimo kreditų rodikliai, išvengiant dubliavimo su mažųjų kreditų duomenimis. 1 priede pateikiamas vartojimo kredito davėjo veiklos ataskaitos rodiklių sąrašas – tai pilnas minėtų 33 rodiklių sąrašas su pavadinimais ir aprašymais (šiame priede rodikliai pateikti taip, kaip jie apibrėžti oficialioje ataskaitos formoje). Kaip matyti 1 priede, ataskaita suskirstyta į dvi dalis: (A) rodiklius ataskaitinio laikotarpio pabaigai (pvz., išmokėtų kreditų skaičius, portfelio sumos, pradelsti mokėjimai ir kt.) ir (B) rodiklius ataskaitinio laikotarpio metu (pvz., per ataskaitinį laikotarpį suteiktų kreditų skaičius ir suma, vidutinės normos, skundų skaičius ir pan.). Tokiu būdu surinkti duomenys vėliau naudojami kuriant išmaniojo kontrakto modelį ir atliekant tyrimo eksperimentinę dalį. Žemiau pateikiama nurodytų duomenų schema ir jų sąveika su išmaniaisiais kontraktais (žr. 13 pav.)



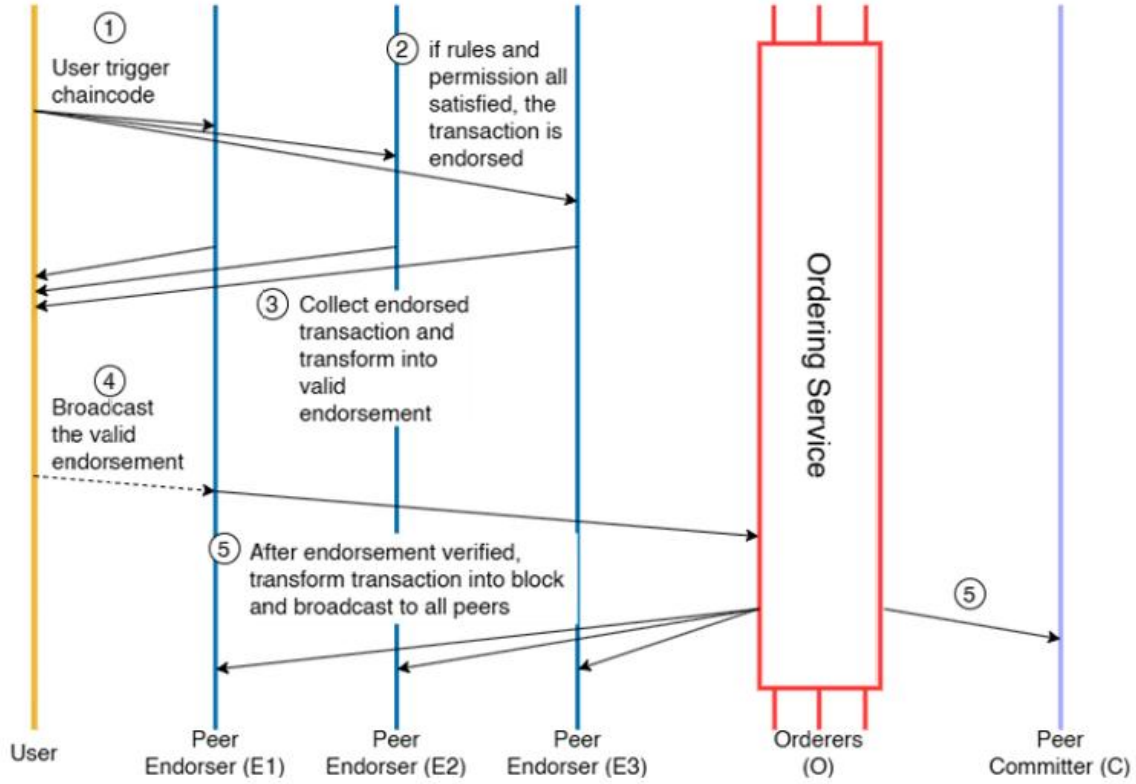
13 pav. Finansinės veiklos ataskaitų teikimo išmaniojo kontrakto architektūra

Žemiau pateikiama ir ataskaitos generavimo išmaniojo kontrakto kodo dalis (visas kodas prieinamas 2 priede)

```
func (s *SmartContract) GenerateQuarterlyReport(
    ctx contractapi.TransactionContextInterface,
    startDate string, endDate string, reportPeriod string,
) (*RegulatoryReport, error) {

    callerMSPID, err := ctx.GetClientIdentity().GetMSPID()
    if err != nil {
        return nil, fmt.Errorf("failed to get caller MSP ID: %v", err)
    }
    startTime, err := time.Parse(time.RFC3339, startDate)
    if err != nil {
        return nil, fmt.Errorf("invalid start date format: %v", err)
    }
    endTime, err := time.Parse(time.RFC3339, endDate)
```

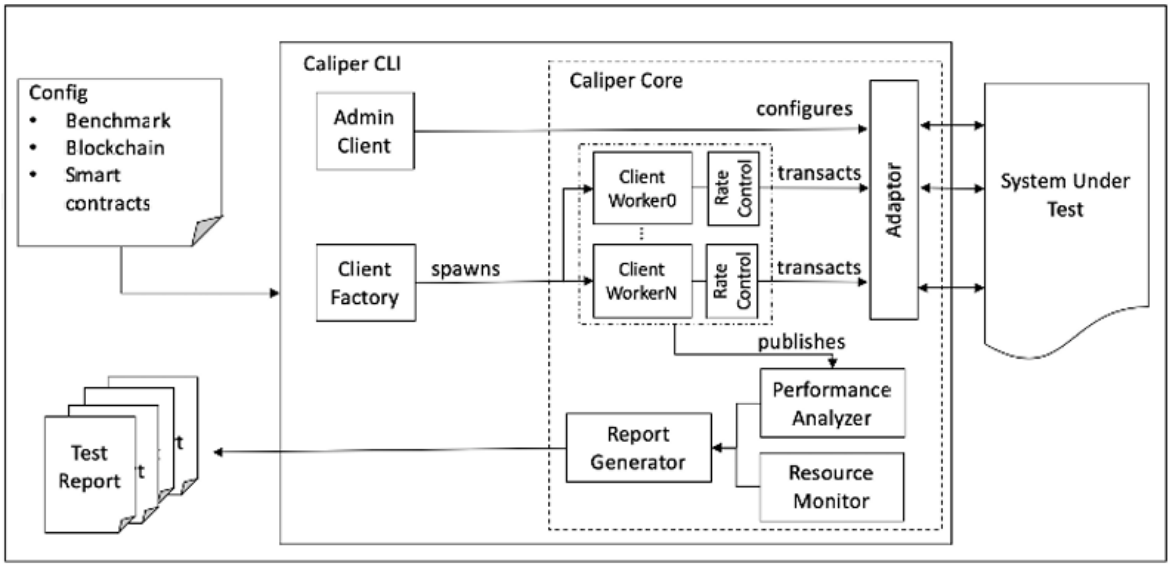
```
    if err != nil {
        return nil, fmt.Errorf("invalid end date format: %v", err)
    }

    report := &RegulatoryReport{
        ReportPeriod:  reportPeriod,
        StartDate:     startDate,
        EndDate:       endDate,
        GeneratedDate: time.Now().UTC().Format(time.RFC3339),
        GeneratedBy:   callerMSPID,
        Analytics: AnalyticsMetrics{
            LoansByStatus: make(map[string]int),
        },
    }

    _ = startTime
    _ = endTime
    return report, nil
}
```

Prototipo našumui testuoti naudojamas „Hyperledger Caliper“ – atvirojo kodo blokų grandinės našumo vertinimo įrankis. Pasak kūrėjų, „Hyperledger Caliper“ leidžia vartotojams testuoti įvairias blokų grandinės platformas pagal iš anksto nustatytus scenarijus ir gauti išsamų veikimo rodiklių rinkinį. Žemiau pateikiama transakcijų vykdymo architektūra, kurios dėka įrankis pateikia tokius našumo rodiklius kaip sandorių sėkmės lygis, pralaidumas (TPS, t. y. sandorių per sekundę skaičius), sandorių vėlinimas (minimali, maksimali, vidutinė trukmė) bei sistemos išteklių sunaudojimas (procesoriaus apkrova, atminties naudojimas, tinklo I/O). „Hyperledger Caliper“ plačiai naudojamas moksliniuose tyrimuose „Hyperledger Fabric“ tinklų veikimui vertinti. Žemiau pateikiama įrankio architektūra (žr. 14 pav.)



14 pav. Laiko diagrama, rodanti grandinės kodo patvirtinimo ir blokų paskirstymo srautą skirtingų tipų mazguose Hyperledger Fabric sistemoje. (Zulkarnain, Ramli, & Nordin, 2025)

Šiame darbe naudojama „Hyperledger Caliper“ 0.7.0 versiją, sukonfigūruota testuoti „Hyperledger Fabric“ tinklą pagal kelis tarpusavio skolinimo (P2P) scenarijus. Testų scenarijai imituos tipines P2P operacijas: pavyzdžiui, naujos paskolos išdavimą, periodinių įmokų mokėjimą ar užklausą paskyros likučiui patikrinti. Tokie scenarijai padės įvertinti prototipo veikimą esant realistiškam krūviui, atspindinčiam tikrovišką P2P skolinimo platformos naudojimą. Bandymams atlikti bus naudojama lokali „Hyperledger Fabric“ 2.5 tinklo aplinka, sudiegta „Docker“ konteineriuose („Docker Compose“). Tinkle veiks keli lygiaverčiai mazgai (angl. peer nodes) ir sandorių užsakymo paslauga (angl. ordering service), taip sukuriant nedidelio masto blokų grandinės tinklą. „Caliper“ siunčia į šį tinklą nustatytą srautą transakcijų kiekvienam scenarijui ir fiksuoja minėtus našumo rodiklius (TPS, sandorių patvirtinimo vėlinimą, klaidų dažnį ir kt.). Žemiau pateikiama įrankio architektūra (žr. 15 pav.)



15 pav. Hyperledger Caliper ir testuojamos sistemos architektūra (Zulkarnain, Ramli, & Nordin, 2025)

Vienas „Caliper“ privalumų yra integruota stebėjimo funkcija – įrankis bandymų metu registruoja procesoriaus apkrovą, atminties (RAM) sąnaudas, tinklo I/O ir kitus resursų naudojimo parametrus kartu su transakcijų statistika.

Duomenų šaltiniai

Tyrime naudojami viešai prieinamus tarpusavio skolinimo (P2P) rinkos duomenis. Šie duomenys apima agreguotą informaciją apie sudarytas paskolas. Lietuvos bankas viešina tarpusavio skolinimo platformų veiklos statistiką: ataskaitose pateikiamas sudarytų paskolų skaičius ir apimtys, palūkanų normų vidurkiai, pavėluotų įmokų dalis ir kiti rodikliai. Taip pat P2P skolinimo platformos skelbia viešas ataskaitas, kuriose atsispindi tokie rodikliai kaip tipinė paskolos suma, vidutinė grąžos norma investuotojams, vėlavimo ar nevykdo procentai ir panašiai. Šie vieši duomenys užtikrina, kad eksperimentui pasirinkti parametrai būtų paremti realios rinkos situacija.

Remdamiesi surinkta statistika, generuosime duomenų kiekį, kad apkrova blokų grandinės tinklui kuo labiau imituotų realias P2P operacijas. Kitaip tariant, blokų grandinės prototipas bus apkraunamas transakcijomis, kurių dažnumas, dydis ir pasiskirstymas laike atitinka realiai stebimus rinkos scenarijus. Pavyzdžiui, pagal rinkos duomenis nustatysime vidutinę paskolos sumą ir tipinį sandorių dažnį – tai užtikrins, kad testų metu siunčiamų paskolų srautas atspindėtų realų aktyvumą (pvz., staigesnį paskolų išdavimo suaktyvėjimą tam tikru laikotarpiu ar periodinių įmokų mokėjimų bangas). Tai sukuria bandymų sąlygas, artimas tikrovei, ir leidžia stebėti, kaip blokų grandinės sistema susidoroja su P2P veiklos apkrova realistiškomis sąlygomis.

Be to, planuojama išbandyti skirtingus transakcijų apkrovos lygius – nuo įprasto vidutinio krūvio iki padidinto srauto – siekiant įvertinti sistemos atsparumą ir mastelio keitimą. Atskiri testai vykdomi palaipsniui didinant sandorių intensyvumą (pavyzdžiui, imituojant staigų operacijų suaktyvėjimą piko metu) ir stebint, kaip kinta pralaidumas bei sandorių patvirtinimo vėlinimas didėjant apkrovai. Tokie streso testai padės nustatyti prototipo pajėgumų ribas, t. y. maksimalų tinklo pralaidumą, kurį sistema dar gali patikimai aptarnauti, ir ar jis atitinka realių P2P platformų poreikius.

Galiausiai gauti rezultatai bus lyginami su tradicinių sistemų rodikliais, kad būtų galima geriau interpretuoti blokų grandinės prototipo efektyvumą. Pavyzdžiui, jeigu įprasta centralizuota P2P platforma per tam tikrą laiko tarpą apdoroja X paskolų operacijų, šis dydis pasitarnaus kaip atskaitos taškas vertinant, ar siūlomas blokų grandinės sprendimas pajėgus pasiekti panašų pralaidumą. Toks viešų duomenų ir testavimo priemonių derinimas užtikrina, kad eksperimento sąlygos yra maksimaliai realistiškos, o gauti rezultatai – praktiškai reikšmingi. Skaidrus naudojamų duomenų šaltinių ir priemonių aprašymas atitinka šiuolaikinius metodinius reikalavimus – tai didina tyrimo patikimumą ir palengvina rezultatų atkuriamumą. Toliau, aptariama našumo vertinimas detaliau.

2.6. Vertinimo metrikos ir kriterijai

Šiame skyriuje aprašomi bloko grandinės prototipo našumo vertinimo kriterijai, skirti audito skaidrumui ir pasitikėjimui stiprinti. Parinktos ir išmatuotos metrikos leidžia įvertinti, ar sukurta „Hyperledger Fabric“ pagrįsta sistema atitinka keliamus reikalavimus. Literatūroje pabrėžiama, kad efektyvumas (našumas) dažnai lemia, kokiose srityse blokų grandinės technologija gali būti pritaikyta. Kitaip tariant, jei sistema nepajėgi apdoroti reikiamo transakcijų srauto ar užtikrinti priimtino operacijų vėlavimo, jos nauda bus ribota. Capocasale ir kt. (Capocasale, Gotta, & Perboli, 2023) atkreipia dėmesį, jog efektyvumas yra pagrindinis veiksnys, kuris žymiai riboja, kokios programos gali naudoti blokų grandinės technologiją. Todėl procedūra, leidžianti teisingai įvertinti įvairių blokų grandinės sprendimų veikimą, yra labai svarbi. Todėl šiame skyriuje apibrėžiamos pagrindinės našumo metrikos ir paaiškinama jų svarba audito kontekste.

Atsižvelgiant į Capocasale (Capocasale, Gotta, & Perboli, 2023) siūlomą metodiką leidimų reikalaujančių blokų grandinių testavimui, vertinant sistemą fokusuojamasi į kelis esminius aspektus. Visų pirma, tai operacijų spartą ir vėlavimą, kurie apibrėžia transakcijų apdorojimo greitį. Taip pat matuojamas sistemos išteklių naudojimas (procesoriaus apkrova, atminties sąnaudos ir pan.), įvertinant technologijos efektyvumą. Šių metrikų visuma leidžia įvertinti, ar blokų grandinės sprendimas užtikrina reikiamą našumą ir patikimumą. Toliau detalizuojamos šios metrikos, pagrindžiant jų pasirinkimą teorinėje literatūroje ir atsižvelgiant į praktinį P2P platformų duomenų dinamikos kontekstą Lietuvoje.

Našumo metrikos: TPS, vėlavimas

Transakcijų per sekundę (TPS) – rodo, kiek transakcijų blokų grandinė gali apdoroti per vieną laiko vienetą (dažniausiai per sekundę). TPS dažnai laikomas pagrindiniu pralaidumo rodikliu. „Hyperledger Caliper“ našumo testavimo įrankis būtent skiria didelį dėmesį TPS rodikliui, nes jis apibrėžia sistemų gebėjimą susidoroti su tam tikru operacijų srautu realiu laiku. Jeigu audito metu generuojama daug operacijų (pvz., finansinių transakcijų), blokų grandinė turi turėti pakankamą pralaidumą, kad nė viena transakcija neliktų neįtraukta ar pavėluotai įtraukta į grandinę. Didelis TPS rodiklis reiškia, kad sistema gali apdoroti daug įrašų per trumpą laiką, tokiu būdu užtikrindama skaidrumą realiuoju laiku – visi įvykiai greitai atsispindi bendrame registre.

Transakcijų vėlavimas (angl. latency) – tai laiko tarpas nuo transakcijos pateikimo iki jos patvirtinimo blokų grandinėje. Ši metrika parodo, kiek užtrunka, kol operacija tampa nekeičiama grandinės dalimi. Kuo greičiau transakcija patvirtinama, tuo greičiau auditoriai ar kiti suinteresuoti asmenys gali ja pasikliauti. Pavyzdžiui, jei finansinės operacijos auditas vykdomas beveik realiu laiku, svarbu, kad tarp įvykio ir jo atsiradimo nekintamame registre praeitų minimalus laikas. Didelis

vėlavimas gali kenkti skaidrumui, nes informacija apie įvykusius veiksmus vėluoja, o tai gali sumažinti pasitikėjimą sistema. Todėl vėlavimo matavimas eksperimento metu leidžia įvertinti, ar „Hyperledger Fabric“ prototipas tinkamas naudoti aplinkoje, kur reikia operatyviai sekti ir tikrinti įvykius.

Pažymėtina, kad TPS ir vėlavimas tarpusavyje susiję – siekiant aukšto pralaidumo, dažnai nukenčia vėlavimas (ir atvirkščiai). Testuojant sistemą, bus stebimos šių rodiklių tarpusavio priklausomybės: pvz., didelio apkrovimo sąlygomis (kai inicijuojama daug transakcijų per sekundę) matuosime, kaip kinta vidutinis patvirtinimo laikas. Šie du rodikliai kartu suteikia išsamų vaizdą apie našumo ribas: TPS parodo kiek galime padaryti, o vėlavimas – kaip greitai tai padaroma.

Išteklių naudojimas: CPU, RAM

Kitas svarbus vertinimo aspektas – skaičiavimo išteklių naudojimas. „Hyperledger Caliper“ generuojamose ataskaitose paprastai pateikiami procesoriaus (CPU) apkrovos ir operatyviosios atminties (RAM) sąnaudų rodikliai testavimo metu. Išteklių naudojimo metrikos leidžia įvertinti sistemos efektyvumą bei mastelio keitimą. Jei mazgai, apdorodami tam tikrą transakcijų srautą, naudoja per daug CPU laiko ar atminties, tai gali rodyti apie našumo trūkumus arba ribotą tinkamumą didesnio masto diegimui. Ypač reguliuojamose srityse (pvz., finansuose) infrastruktūros efektyvumas svarbus dėl kaštų ir patikimumo – perteklinis resursų naudojimas gali reikšti didesnes išlaidas bei didesnę gedimų tikimybę.

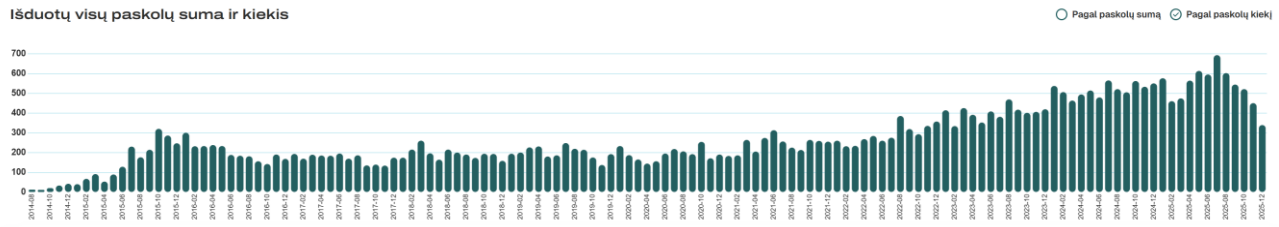
Eksperimento metu stebėsime, kokia vidutinė ir maksimali CPU apkrova tenka „Hyperledger Fabric“ mazgams, vykdant tipinį audito transakcijų krūvį. Taip pat fiksuosime naudojamos atminties dydį. Šie duomenys padės atsakyti, ar prototipas gali veikti nenutrūkstamai ir efektyviai su realistišku apkrovimu. Pavyzdžiui, jei pastebėsime, kad esant ~1 TPS apkrovai procesoriaus apkrova išlieka žema (pvz., <20%), tai rodys, jog sistema turi pakankamą našumo rezervą. Tačiau jei net ir nedidelis transakcijų srautas sąlygotų artimą 100% CPU apkrovą ar didelį atminties naudojimą, tai keltų abejonių dėl sprendimo tinkamumo praktikoje (galimai reikėtų optimizacijų arba galingesnės aparatinės įrangos).

Be to, išteklių naudojimo stabilumas taip pat svarbus. Audito blokų grandinė turėtų veikti numatomoje, stabilioje būsenoje, nepatirdama didelių apkrovos šuolių. Todėl metrikų rinkinyje atsižvelgsime ir į ilgesnio testavimo periodo duomenis – ar nėra tendencijų, jog resursų poreikis nuolat auga. Apibendriant, CPU ir RAM stebėsena padeda įvertinti blokų grandinės sprendimo efektyvumą ir praktinį pritaikomumą: mažesni resursų poreikiai reiškia lengvesnę integraciją į esamas sistemas bei didesnį pasitikėjimą, kad sprendimas veiks sklandžiai.

Kontekstinė analizė: P2P platformų transakcijų apimtys Lietuvoje

Norint empiriškai pagrįsti testavimo scenarijų, svarbu atsižvelgti į realius duomenų srautų dydžius srityje, kurioje siūlomas sprendimas bus taikomas. Mūsų nagrinėjamu atveju – tai Lietuvos tarpusavio skolinimo (P2P) platformų opreacijos. Remiantis Lietuvos banko 2020 m. atlikta P2P platformų veiklos apžvalga (Lietuvos Bankas, 2020). Šioje apžvalgoje pateikiami duomenys apie per platformas suteikiamas paskolas ir jų pokyčius. Svarbu pažymėti, kad P2P platformose transakcija galime laikyti tiek naujos paskolos sutarties sudarymą, tiek investavimo į paskolą veiksmą. Paprastumo dėlei, orientuosimės į naujų paskolų sudarymo skaičių, kadangi kiekviena paskola atitinka vieną pilną finansinę transakciją tarp šalių.

Lietuvos banko duomenimis, 2020-aisiais per tarpusavio skolinimo platformas vidutiniškai sudaroma keliolika ar kelios dešimtys naujų sandorių per dieną. Tai taip pat pastebima ir viename iš tarpusavio skolinimo platformų „Savy“ viešai pateiktų ataskaitų (žr. 16 pav.)



16 pav. Tarpusavio skolinimo platformos „Savy“ išduotų paskolų kiekis

Pavyzdžiui, COVID-19 pandemijos metu 2020 m. balandį P2P platformose suteikta „tik 1,99 mln. Eur naujų vartojimo kreditų“ – tai buvo ~34% mažiau nei sausio mėnesį. Įvertinus, kad vidutinė vieno kredito suma tuo laikotarpiu siekė apie „šiek tiek daugiau kaip 3 tūkst. Eur“, balandžio mėnesį per platformas sudaryta vos ~600–700 naujų paskolų (tai atitinka ~20–23 paskolas per dieną). Net ir aktyvesniais laikotarpiais (pvz., 2020 m. pradžioje, prieš pandemiją) mėnesinė suteikiamų kreditų suma (~3 mln. Eur sausį) reiškė maždaug 1000 naujų paskolų per mėnesį, t. y. apie 30–40 transakcijų per dieną. Šie skaičiai rodo, kad realus P2P platformų transakcijų srautas yra labai nedidelis – <1 transakcija per sekundę (tiksliau, apie 0,0003–0,005 TPS diapazone). Kitaip tariant, dabartinės tarpusavio skolinimo ekosistemos poreikiai blokų grandinės sprendimui nesiekia net 1 TPS.

Šią našumo ribą svarbu turėti omenyje interpretuojant „Hyperledger Fabric“ testavimo rezultatus. Jeigu prototipas sugeba be vargo apdoroti, tarkime, 1 TPS srautą (arba 86 400 transakcijų per parą), vadinasi, jis technologiškai pajėgus patenkinti dabartinius P2P platformų poreikius su didele atsarga. Testavimo metu vis dėlto sieksime išbandyti sistemą ir didesniais krūviais – tai leis nustatyti maksimalias prototipo galimybes ir įvertinti jo perspektyvą, jei ateityje P2P platformų aktyvumas augtų (pvz., transakcijų skaičius padidėtų dešimteriopai). Taip pat atsižvelgsime į tai, kad vienos paskolos finansavimas platformoje gali apimti daug smulkių investuotojų įnašų (t. y. viena paskola gali generuoti kelias dešimtis mažesnių transakcijų). Todėl modeliuojant eksperimentą galima prilyginti 100–300 transakcijų per dieną scenarijų (atitinkantį kelias dešimtis naujų paskolų su keliais investuotojais) realistiškam audituojamos P2P sistemos apkrovimui.

Apibendrintai, Lietuvos banko apžvalgos duomenys suteikia praktinį etaloną: blokų grandinės sprendimo sėkmė nemaža dalimi priklausys nuo to, ar jis bent jau nenusileis tradiciniams sprendimams efektyvumu tokiame nedideliame sraute. Audito skaidrumui užtikrinti nebūtina itin didelė transakcijų apdorojimo sparta, tačiau būtina, jog esamas srautas būtų apdorojamas be trikdžių, stabiliai ir laiku.

3. BLOKŲ GRANDINĖS TECHNOLOGIJOS TAIKYMO AUDITO PROCESUOSE EKSPERIMENTAS

3.1. Eksperimentinė aplinka ir infrastruktūra

Testavimas vykdomas lokalioje aplinkoje. Testai atliekami naudojant „Docker“ konteinerius.

3.1.1. Techninė ir operacinė įranga

CPU:

- Apple M4 Pro
- 10 branduolių CPU:6 našumo (angl. Performance) branduoliai, 4 efektyvumo (angl. Efficiency) branduoliai
- Architektūra: ARM64 (Apple Silicon)
- CPU, GPU naudoja bendrą atmintį
- Atminties pralaidumas: 273 GB/s

Operatyvinė atmintis:

- 32 GB vieningos atminties
- Tipas: LPDDR5X

SSD (saugykla):

- Talpa: 512 GB NVMe SSD
- Sąsaja: PCIe 4.0 x4 (Apple custom controller)
- Atminties tipas: TLC NAND
- Skaitymas: ~ 5 000 – 5 900 MB/s
- Rašymas: ~ 4 200 – 5 200 MB/s
- Dydis: 512 GB

Operacinė sistema:

- macOs Tahoe 26.1

Docker aplinka

- CPU: 2 branduoliai
- RAM: 8 GB

HyperLedger Fabric:

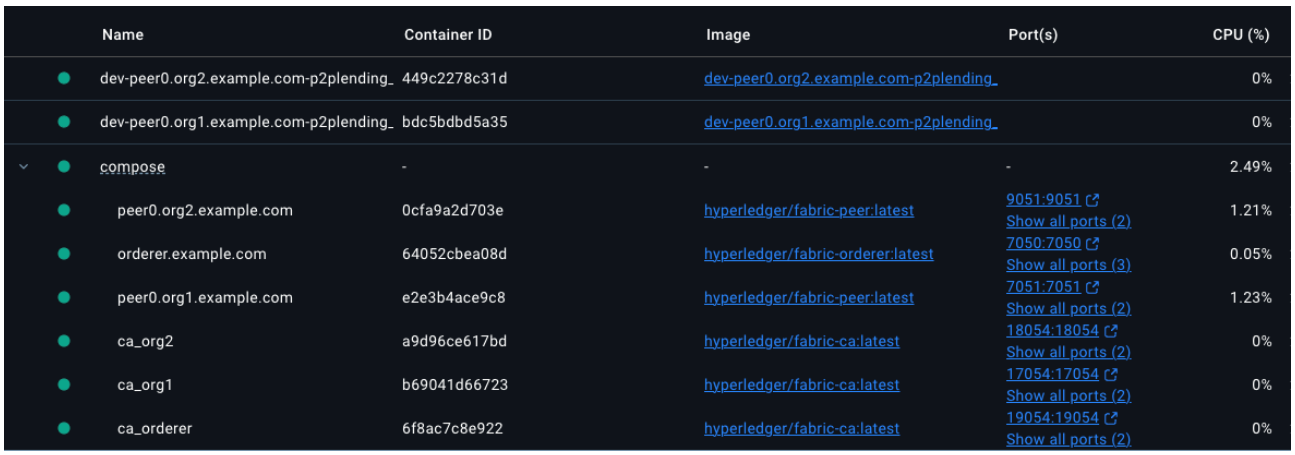
- Versija: 2.5.12
- Chaincode: Docker konteineriai
- Peer duomenų bazė: CouchDb

Hyperledger Caliper:

- Versija: 0.7.0

3.1.2. Tinklo architektūra

Žemiau pateikiamia Docker tinklo architektūra (žr. 17 pav.)



	Name	Container ID	Image	Port(s)	CPU (%)
	dev-peer0.org2.example.com-p2plending_	449c2278c31d	dev-peer0.org2.example.com-p2plending_		0%
	dev-peer0.org1.example.com-p2plending_	bdc5bdbd5a35	dev-peer0.org1.example.com-p2plending_		0%
	compose	-	-	-	2.49%
	peer0.org2.example.com	0cfa9a2d703e	hyperledger/fabric-peer:latest	9051:9051 Show all ports (2)	1.21%
	orderer.example.com	64052cbea08d	hyperledger/fabric-orderer:latest	7050:7050 Show all ports (3)	0.05%
	peer0.org1.example.com	e2e3b4ace9c8	hyperledger/fabric-peer:latest	7051:7051 Show all ports (2)	1.23%
	ca_org2	a9d96ce617bd	hyperledger/fabric-ca:latest	18054:18054 Show all ports (2)	0%
	ca_org1	b69041d66723	hyperledger/fabric-ca:latest	17054:17054 Show all ports (2)	0%
	ca_orderer	6f8ac7c8e922	hyperledger/fabric-ca:latest	19054:19054 Show all ports (2)	0%

17 pav. Docker aplinka

Org1:

- Peer: peer0.org1.example.com (7051)
- Išmanieji kontraktai: Go
- Rolė: P2P platforma

Org2:

- Peer: peer0.org2.example.com (9051)
- Rolė: Reguliatorius (pvz LB)

Orderer (Reguliatorius, pvz LB):

Raft node (7050)

3.1.3. Bloko konfiguracijos parametrai

Eksperimente keičiamas *MaxMessageCount*, kuris nurodo maksimalų transakcijų skaičių bloke.

Fiksuoti parametrai:

- *BatchTimeout*: 2 s
- *PreferredMaxBytes*: 50 MB
- *AbsoluteMaxBytes*: 200 MB

Kintami parametrai (lentelė 4)

4 lentelė Testų konfiguracijos

Konfiguracija	***MaxMessageCount***
B1	10
B2	25
B3	50
B4	100

3.1.4. Testavimo parametrai

Apkrovos konfigūracija:

- Transakcijų dažnis: 1000 TPS
- Transakcijų skaičius: 10000

Resursų stebėjimas:

- CPU
- RAM
- Tinklo I/O
- Disko I/O

Našumo metrikos:

- Pralaidumas (TPS)
- Vėlavimas (vid., max, min)

Eksperimento kontrolė:

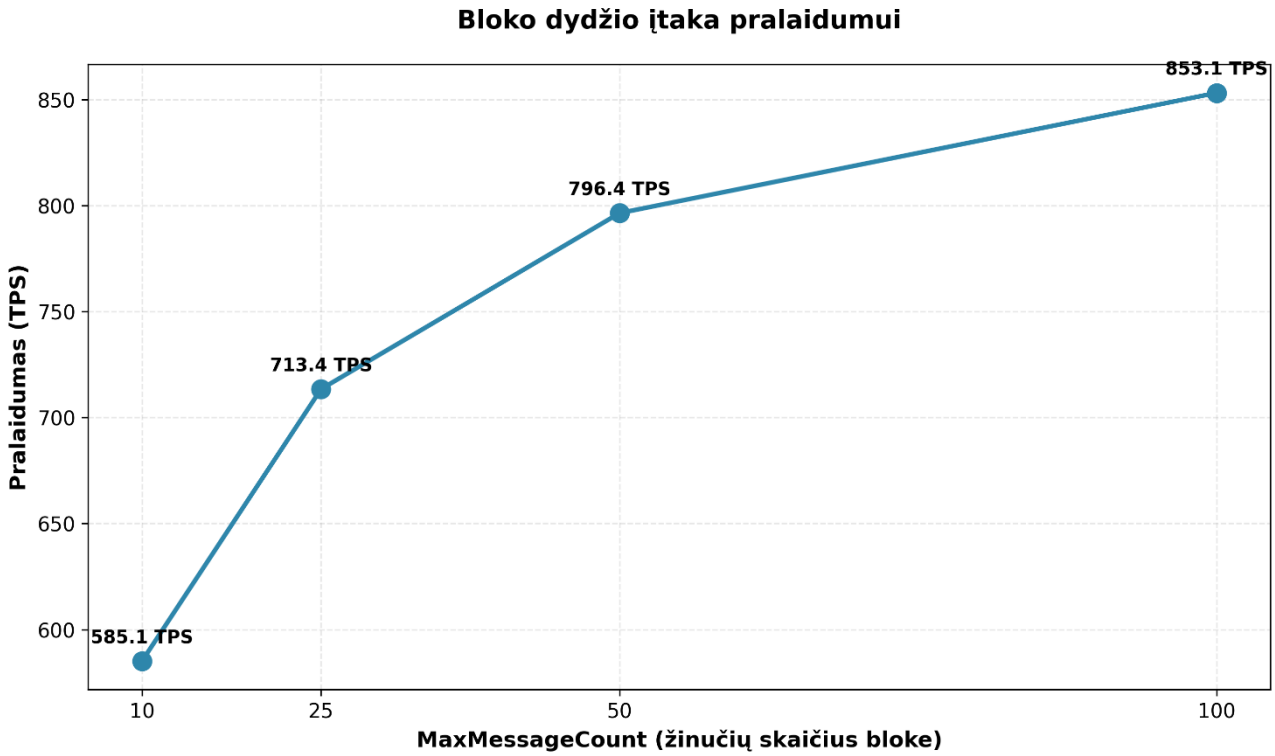
- Po kiekvieno testo tinklas sukuriamas iš naujo
- Išmanieji kontraktai įdiegtas iš naujo
- Testai vykdomi tvarka B1 → B2 → B3 → B4
- Tarp testų – 2 min. pertrauka

3.1.5. Eksperimento apribojimai

- Naudojama vieno mazgo Raft
- macOs + Docker desktop (ne Linux aplinka). Susidurta su problemomis matuojant resursų išteklių naudojimą, „Caliper“ turi problemų matuojant išteklius, todėl reikia papildomo kodo keitimo
- Limituota transakcijų apimtis

3.2. Eksperimentiniai rezultatai

Šiame skyriuje pateikti tyrimo rezultatai pagal turimas konfigūracijas. Pirmasis tyrimo rezultatas – bloko dydžio įtaka sistemos pralaidumui. Rezultatai pateikti paveikslėlyje (žr. 18 pav.)



18 pav. Bloko dydžio įtakos pralaidumui grafikas

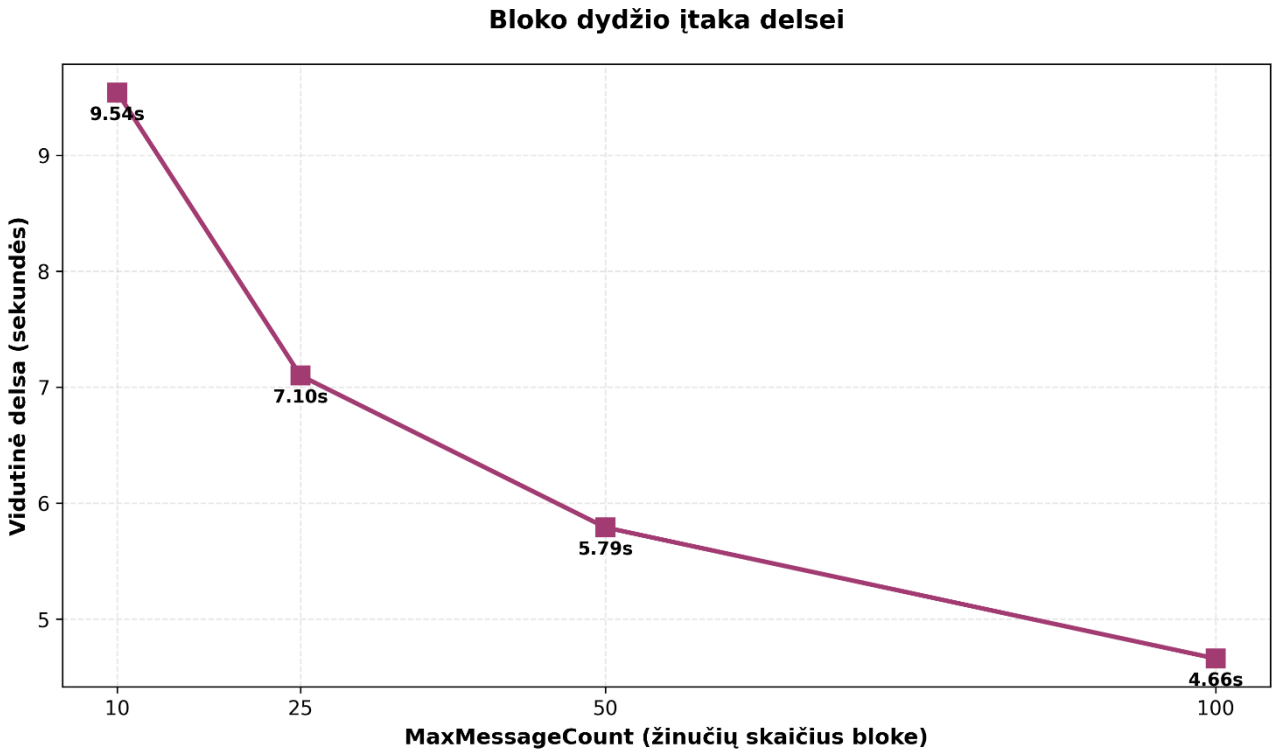
Atliekant eksperimentą buvo matoma aiški tendencija – didėjant *MaxMessageCount* parametrui nuo 10 iki 100 transakcijų, pralaidumas nuosekliai kyla nuo 585,1 TPS iki 853,1 TPS, t. y. maždaug 45,8 %. Grafike atsiskleidžianti beveik tiesinė augimo dinamika rodo, kad didesni blokai leidžia efektyviau panaudoti sistemos resursus ir sumažina vieno bloko apdorojimo sąnaudas.

Analizuojant gautus rezultatus galima pastebėti, kad mažiausias, 10 transakcijų dydžio, blokas veikia kaip pradinė konfigūracija – ji pasiekia 585,1 TPS, tačiau dėl labai dažno konsensuso ciklų kartojimo šioje konfigūracijoje juntamas ryški apkrova (angl. overhead). Padidinus bloką iki 25 transakcijų pralaidumas išauga beveik penktadaliu – apie 21,9 %. Tai rodo, kad sistemoje iš karto sumažėja fiksuotų veiksmų, susijusių su kanalo narių pritarimu ir transakcijų tvirtinimo proceso organizavimu.

Dar labiau padidinus bloką iki 50 transakcijų, pralaidumas pasiekia 796,4 TPS, t. y. apie 36 % daugiau nei pradinėje konfigūracijoje. Nors augimo tempas šiek tiek lėtėja, jis išlieka aiškiai matomas. Galiausiai, pasirinkus didžiausią tyrime naudotą 100 transakcijų bloką, pasiekiamas aukščiausias pralaidumas – 853,1 TPS. Tai jau beveik pusės našumo padidėjimas, palyginti su mažiausiu bloko dydžiu.

Bendras rezultatas yra pakankamai aiškus: didesni blokai leidžia geriau paskirstyti fiksuotą kiekvienam blokui tenkančią apkrovą, susijusį su transakcijų tvirtinimo etapais. Kitaip tariant, 100 transakcijų turintis blokas yra kur kas efektyvesnis nei dešimt mažų blokų po 10 transakcijų. Tokia

dinamika patvirtina, kad „Hyperledger Fabric“, kaip ir daugelyje kitų blokų grandinių su leidimais, našumas tiesiogiai priklauso nuo to, kiek operacijų galima sutalpinti į vieną konsensuso ciklą. Toliau galima stebėti delsą (žr. 19 pav.)



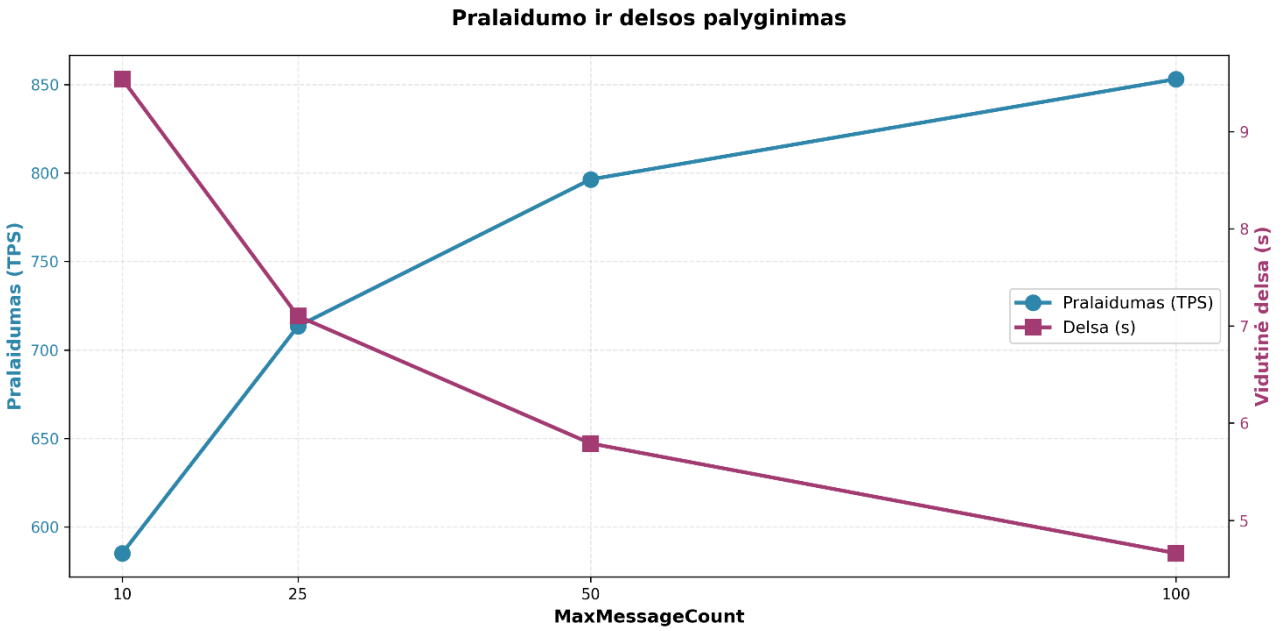
19 pav. Bloko dydžio įtakos delsai (angl. latency) grafikas

Įdomu tai, kad analizuojant bloko dydžio poveikį vėlavimui paaiškėjo netikėtas, tačiau labai palankus rezultatas – didesni blokai ne tik didina pralaidumą, bet ir mažina transakcijų vėlavimą. Tradiciškai blokų grandinėse tikimasi priešingo efekto: kuo didesnis blokas, tuo ilgiau transakcija turi laukti, kol blokas bus užpildytas, todėl bendras vėlavimas turėtų didėti. Tačiau ši prielaida labiau galioja žemų apkrovų scenarijuose, kur blokai pildosi lėtai. Mūsų eksperimente, kuriame sistema buvo testuojama esant 1000 TPS apkrovai, blokai nepaisant dydžio užsipildė itin sparčiai, todėl klasikinis kompromisas čia nepasitvirtino.

Faktiniai rezultatai rodo priešingą tendenciją: didžiausio, 100 transakcijų, bloko konfigūracija pasižymėjo net 51,2 % mažesniu vėlavimu nei mažiausias 10 transakcijų blokas. Tai leidžia manyti, kad realų vėlavimą lemia ne laukimo trukmė iki bloko užpildymo, o bendras sistemos vykdomų konsensuso ciklų kiekis.

Norint tai aiškiai iliustruoti, verta įvertinti paprastą matematinį scenarijų. Apdorojant 10000 transakcijų su 10 transakcijų blokais, susidaro apie 1000 blokų. Jei vienam konsensuso ciklui vidutiniškai reikia apie 2 sekundes, bendras šių ciklų apimtis sudaro maždaug 2000 sekundžių, o vienai transakcijai tenkantis papildomas vėlavimas siekia apie 0,2 s. Tuo tarpu naudojant 100 transakcijų blokus, tų pačių 10000 operacijų apdorojimui pakanka vos 100 blokų. Sistemai reikia atlikti tik apie 200 sekundžių konsensusų ciklo darbo, todėl vienai transakcijai tenkanti apkrova sumažėja iki maždaug 0,02 s.

Ši analizė leidžia daryti aiškią išvadą: didesni blokai gali ženkliai sumažinti delsą didelės apkrovos scenarijuose, nes sumažina bendrą konsensuso ciklų skaičių ir taip optimizuoja sistemos resursų panaudojimą. Tai reiškia, kad tam tikrose realiose P2P skolinimo platformų darbo situacijose, kur vyksta intensyvus transakcijų srautas, didesnių blokų konfigūracija gali būti ne tik našesnė, bet ir greitesnė vartotojo požiūriu. Siekiant pilnai suprasti kaip pralaidumas ir delsa įtakoja vienas kitą, galima juos pateikti viename grafike (žr. 20 pav.)



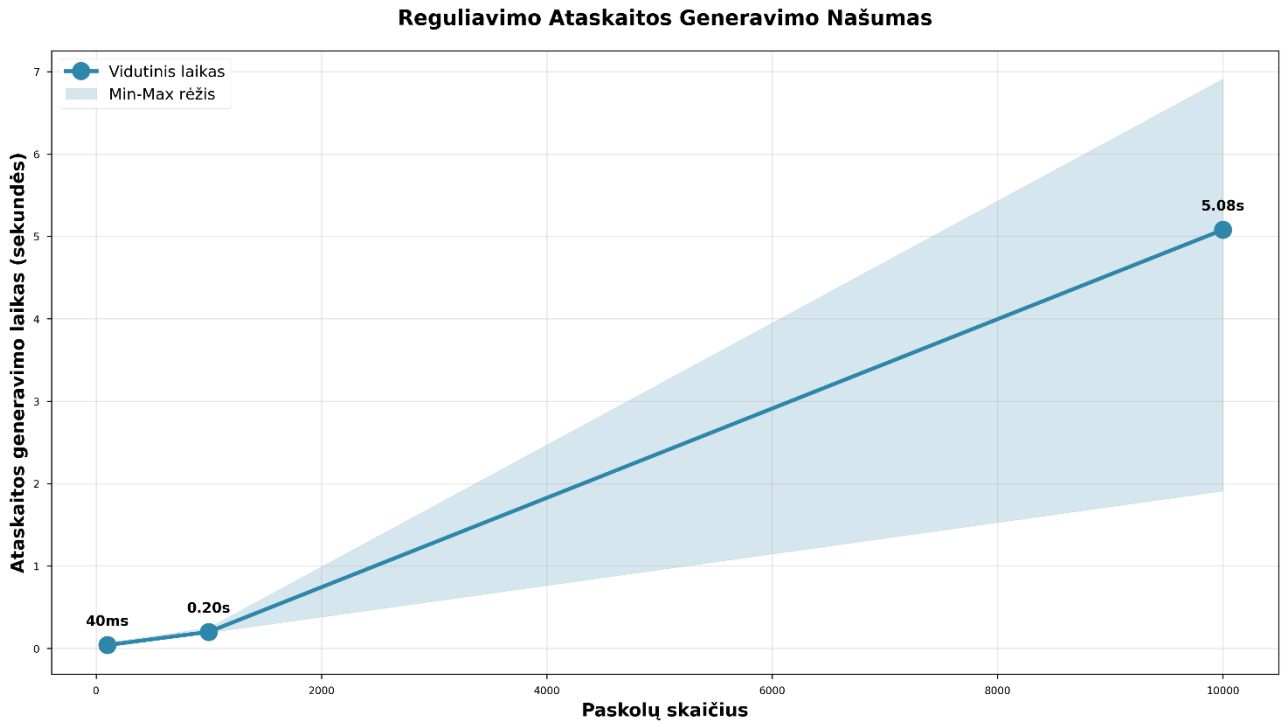
20 pav. Pralaidumo ir delsos grafikas

Dviejų ašių grafikas aiškiai atskleidžia bendrą tendenciją, kuri yra ypač svarbi vertinant bloko dydžio įtaką sistemos veikimui: abi pagrindinės našumo metrikos – pralaidumas ir vėlavimas – gerėja vienu metu. Mėlyna linija, atvaizduojanti pralaidumo (TPS) pokytį kairiojoje ašyje, nuosekliai kyla didėjant bloko dydžiui. Tuo pat metu rožinė linija, rodanti transakcijų vėlavimą dešiniojoje ašyje, juda priešinga kryptimi ir reikšmingai mažėja. Toks paralelus metrikų pokytis yra netipiškas klasikinėms blokų grandinių architektūroms, kuriose dažnai egzistuoja kompromisas tarp greičio ir pralaidumo.

Šiame eksperimente matomas rezultatas reiškia, kad didesni blokai sistemos veikimą optimizuoja dvejopai – jie ne tik leidžia apdoroti daugiau transakcijų per laiko vienetą, bet tuo pačiu sumažina kiekvienos transakcijos keliamą vėlavimą. Tai dar kartą patvirtina, kad „Hyperledger Fabric“ architektūroje konsensuso ciklų skaičius yra kritinis veiksnys – kuo jų mažiau, tuo efektyviau sistema funkcionuoja visais aspektais.

Eksperimento metu buvo išmatuoti keli pagrindiniai sistemos veikimo rodikliai: ataskaitos generavimo laikas, našumo mastelio keitimas didėjant duomenų kiekiui, sprendimo palyginimas ir veikimo rezultatų pastovumas. Toliau pateikiami šiuos aspektus iliustruojantys grafikai bei jų analizė.

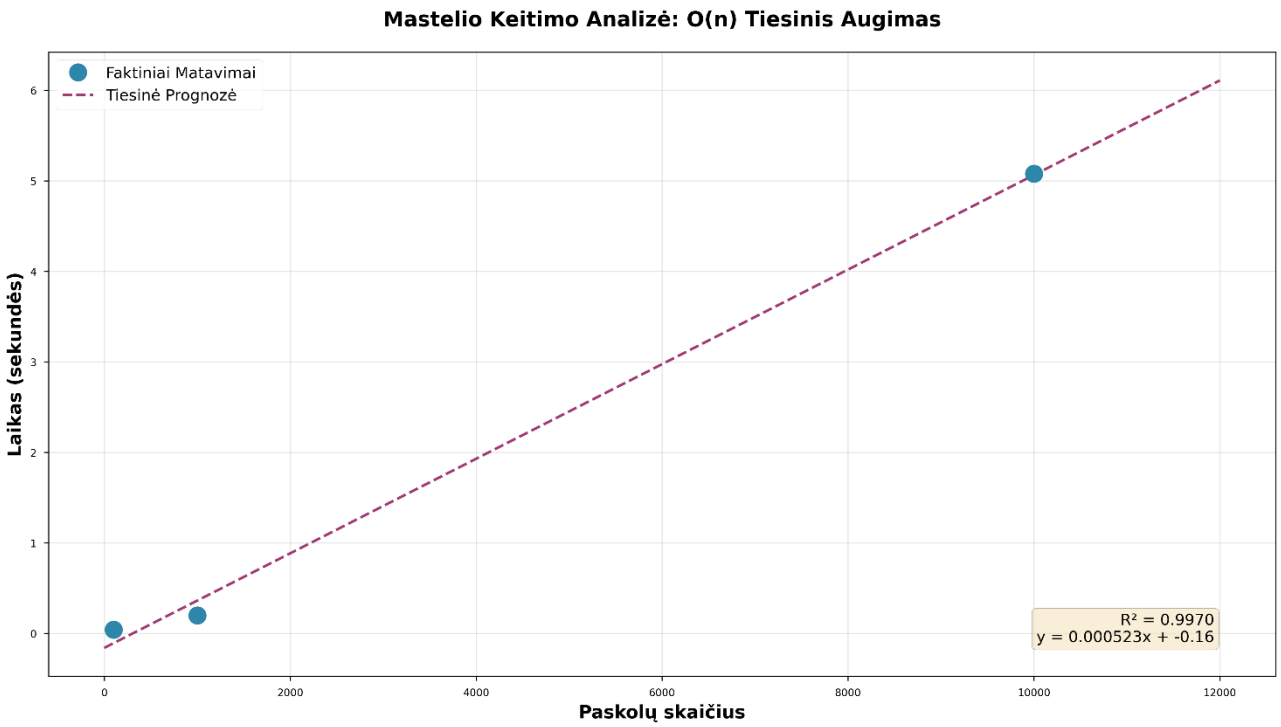
Reguliavimo ataskaitos generavimo laikas priklauso nuo paskolų skaičiaus (žr. 21 pav.)



21 pav. Reguliavimo ataskaitos generavimo laikas priklausomai nuo paskolų skaičiaus

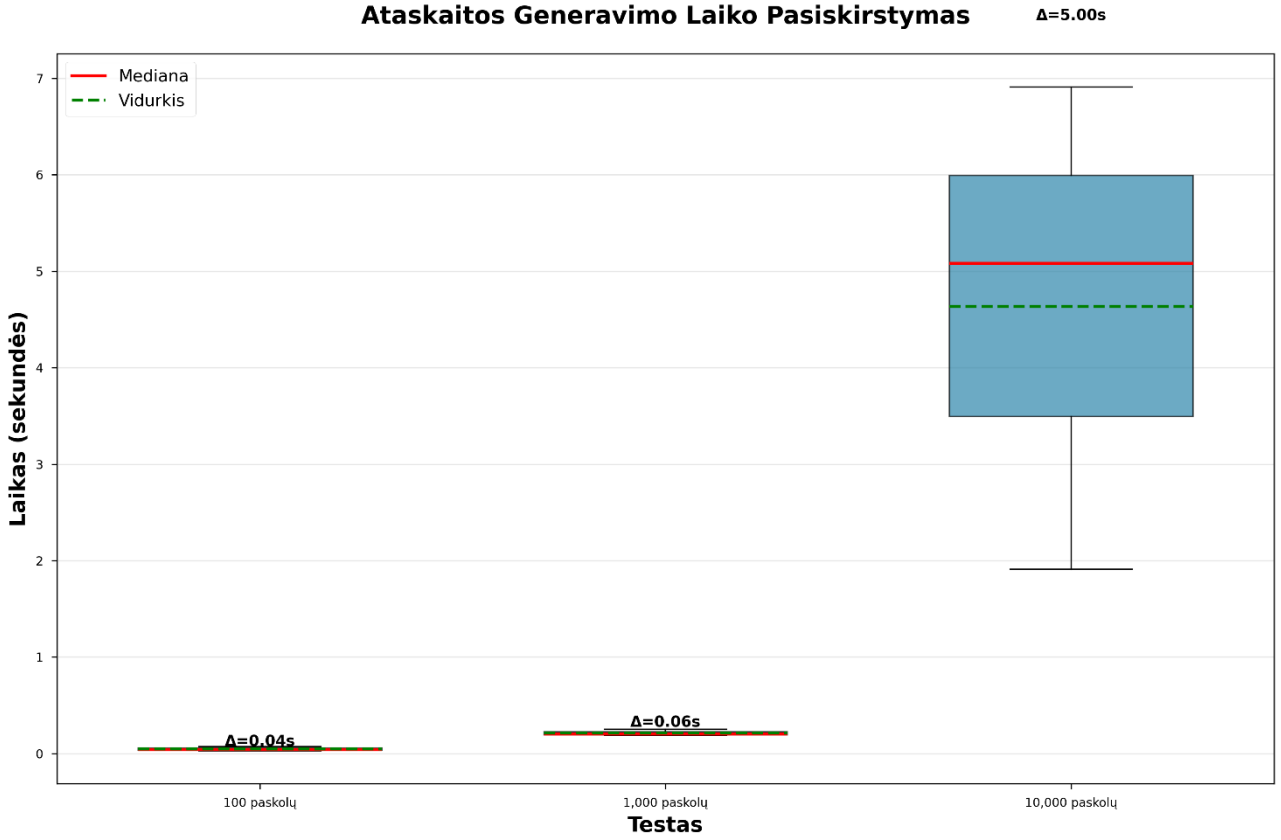
Šis grafikas parodo, kiek laiko vidutiniškai trunka sugeneruoti ataskaitą, esant skirtingam paskolų kiekiui duomenų bazėje (mėlyna linija žymi vidurkį, o mėlyna šešėliuota sritis – minimalias ir maksimalias reikšmes 10 bandymų metu). Matyti, kad esant 100 paskolų duomenų apimčiai ataskaita sugeneruojama maždaug per 0,04 s, padidinus apimtį iki 1000 paskolų – apie 0,20 s, o didžiausiu bandytu mastu (10000 paskolų) – maždaug per 5,08 s. Tai rodo, jog ataskaitų rengimas išlieka labai spartus net ir žymiai padidėjus duomenų apimčiai. Palyginimui, tradicinis rankinis tokios apimties ataskaitos parengimas paprastai trunka kelias dienas, todėl net 5 sekundžių trukmė yra milžiniškas efektyvumo šuolis. Taip pat pastebėtina, kad rezultatų sklaida labai maža (vidutinės trukmės beveik sutampa su minimaliomis ir maksimaliomis), vadinasi, sistema veikia stabiliai ir be didelių našumo šuolių.

Toliau atliekama mastelio keitimo analizė (žr. 22 pav.) Mėlynais taškais pavaizduotos faktinis vėlavimas (generavimo laiko) reikšmės esant 100, 1000 ir 10000 paskolų, o violetinė punktyrinė linija – statistiškai gauta tiesinė regresija. $R^2 =$ 0,997 įrodo, kad ataskaitos generavimo laiko augimas tiesiškai priklauso nuo duomenų kiekio. Regresinės tiesės nuolydis (~0,0005 sekundės vienai paskolai) reiškia, jog kiekviena papildoma paskola prideda tik ~0,5 milisekundės prie bendros ataskaitos sudarymo trukmės. Toks O(n) tiesinis mastelio keitimas leidžia patikimai prognozuoti sistemos veikimą didesniais mastais. Pavyzdžiui, stebint linijinę priklausomybę, galima numatyti, kad net 50000 paskolų ataskaita truktų tik apie ~25 s, o tai vis tiek yra itin trumpas laikas palyginus su tradiciniais metodais.



22 pav. Ataskaitos generavimo našumo mastelio analizė

Galiausiai galime atkreipti dėmesį ir į ataskaitos generavimo laiko pasiskirstymą (žr. 23 pav.)

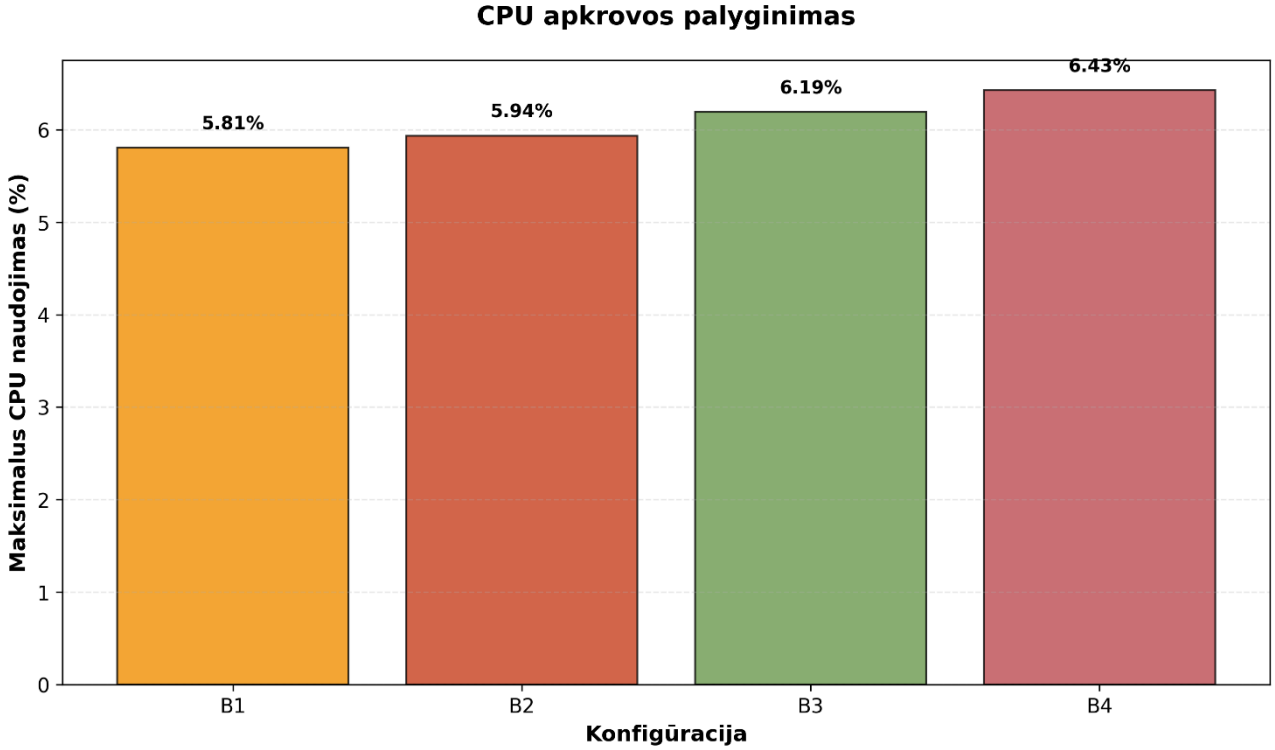


23 pav. Ataskaitos generavimo laiko pasiskirstymas skirtingo masto testuose

Grafike pateiktos diagramos, vaizduojančios ataskaitos sudarymo trukmes esant 100, 1000 ir 10000 paskolų. Medianos (raudona linija) ir vidurkio (žalia punktyrinė linija) reikšmių artumas rodo, kad duomenys pasiskirstę apytiksliai simetriškai be ryškių atsitiktinių šuolių. Esant nedideliam duomenų kiekiui (100 paskolų), trukmės variacija yra labai maža (nuo ~0,03 s iki 0,07 s, skirtumas = 0,04 s), todėl nors santykinis variacijos koeficientas didokas (~50%), praktiškai visi bandymai įvyksta per kelias dešimtis milisekundžių. 1000 paskolų atveju rezultatai itin pastovūs – trukmė kinta vos per 0.03s (skirtumas apie 0,06 s). Prie didžiausio duomenų kiekio (10000 paskolų) matyti platesnė sklaida – trukmė svyravo apytiksliai nuo 1,9 s iki 6,9 s (skirtumas apie 5,0 s). Visgi, net lėčiausias užfiksuotas laikas (~6–7 s) yra vis tiek žymiai greitesnis nei tradicinis metodas, todėl tokia sklaida yra visiškai priimtina. Rezultatai leidžia daryti išvadą, kad sistema demonstruoja pakankamai stabilų ir patikimą veikimą, o didesni vėlavimų svyravimai pasireiškia tik esant itin dideliam apkrovimui (10 ataskaitų vykdoma vienu metu), kuris realybėje pasitaikytų retai.

3.3. Resursų naudojimo analizė

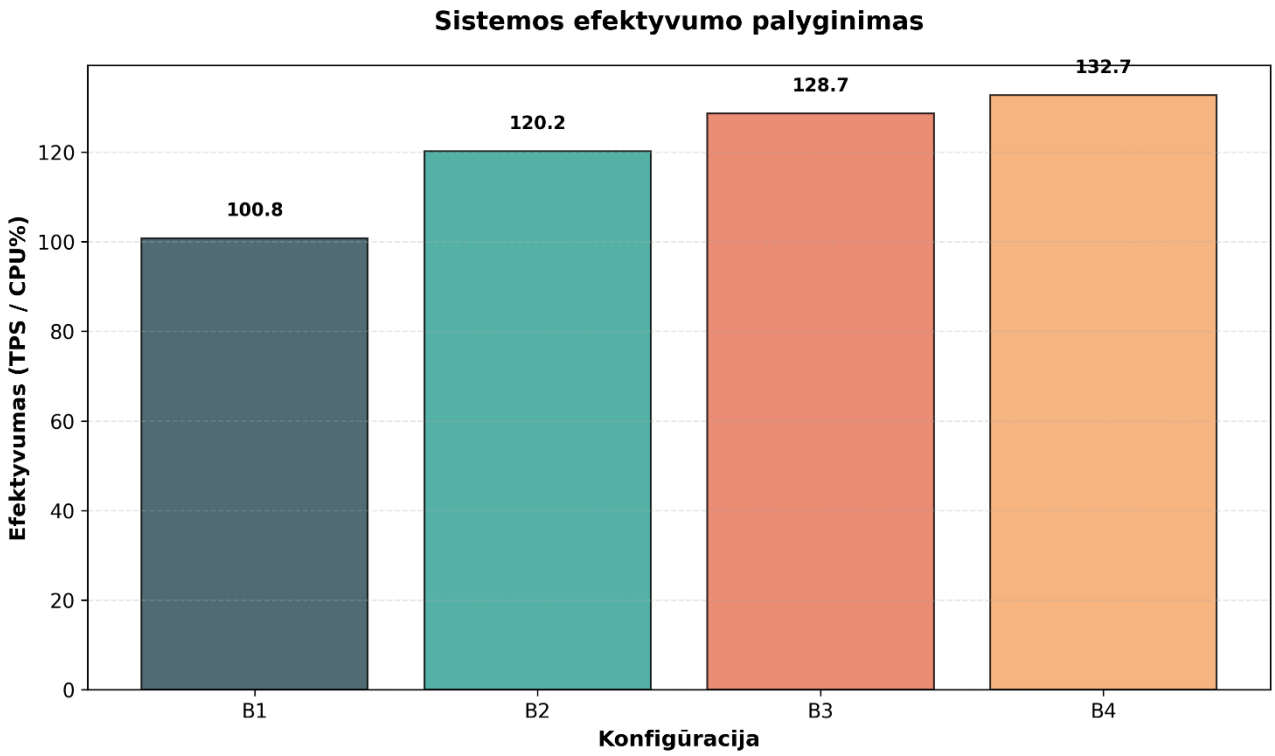
Svarbu įvertinti ar pralaidumas gerėja su CPU ir kitų išteklių naudojimu (žr. 24 pav.)



24 pav. CPU apkrovos diagrama

CPU naudojimo palyginimas parodo, kad didesni blokai leidžia gerokai pagerinti sistemos efektyvumą beveik nedidinant skaičiavimo išteklių poreikio. Analizuojant mazgo elgseną matyti, kad maksimalus procesoriaus apkrovimas didėja tik labai nežymiai – nuo 5,81 % iki 6,43 %. Tai yra labai žemas resursų naudojimas, tačiau to poveikis sistemos našumui yra didelis: pralaidumas, palyginti su mažiausiu bloko dydžiu, išauga 45,8 %.

Dar aiškiau šį efektą atskleidžia TPS/CPU santykis(žr. 25 pav.), kuris rodo kaip efektyviai sistema išnaudoja skaičiavimo galią.

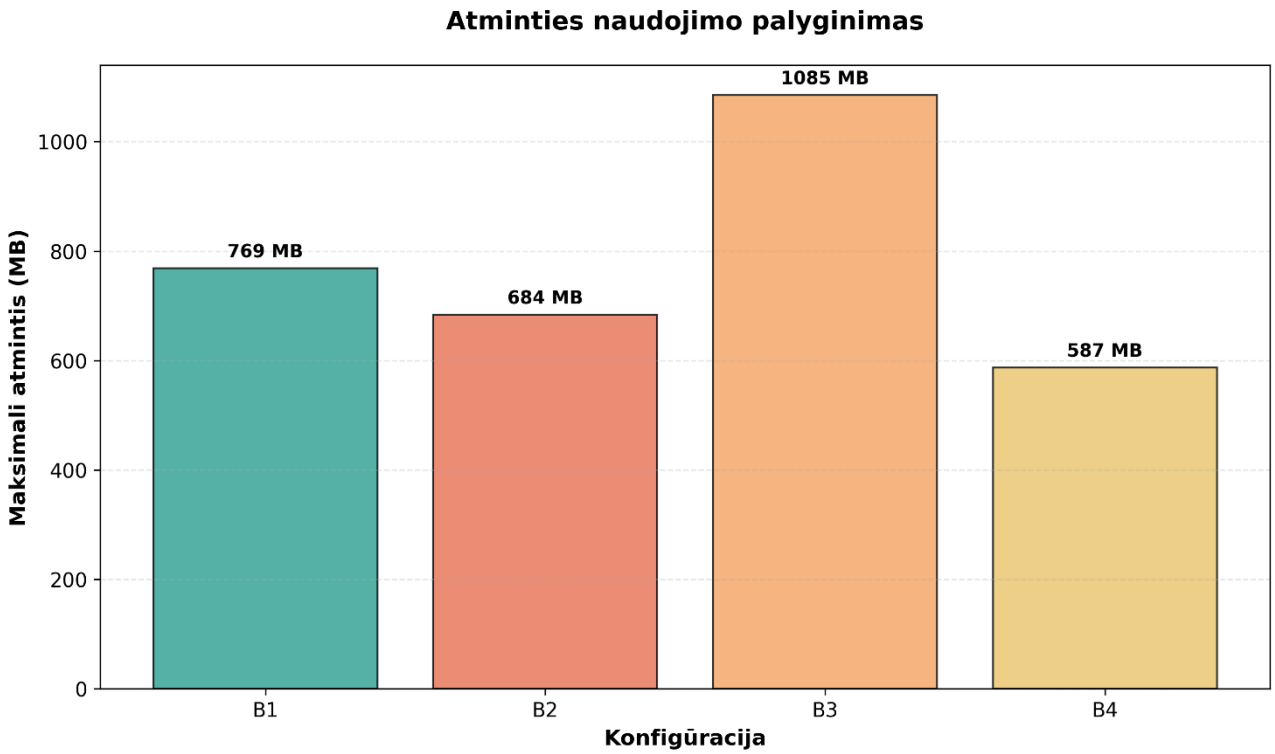


25 pav. Sistemos efektyvumo palyginimas

Pradinėje B1 konfigūracijoje vienam CPU procentui tenka apie 178,4 TPS, o B4 konfigūracijoje tas pats CPU kiekis jau leidžia apdoroti 316 TPS. Tai reiškia, kad naudojant didžiausią bloką, sistemos efektyvumas išauga net 77,2 %, o tai reiškia, kad sistema apdoroja beveik dvigubai daugiau transakcijų neprašydama daugiau skaičiavimo resursų.

Didžioji dalis konsensuso mechanizmo darbo – yra fiksuota kiekvienam blokui, nepriklausomai nuo to, kiek transakcijų jame yra. Didesni blokai leidžia „amortizuoti“ šią fiksuotą apkrovą, paskirstant jį didesniam transakcijų skaičiui. Todėl sistema atlieka daugiau naudingos veiklos už tą patį CPU laiką, o tai tiesiogiai atsispindi našumą ir efektyvumą.

Kalbant apie resursus, svarbu aptarti ir atminties naudojimą (žr. 26 pav.)



26 pav. Atminties naudojimo diagrama

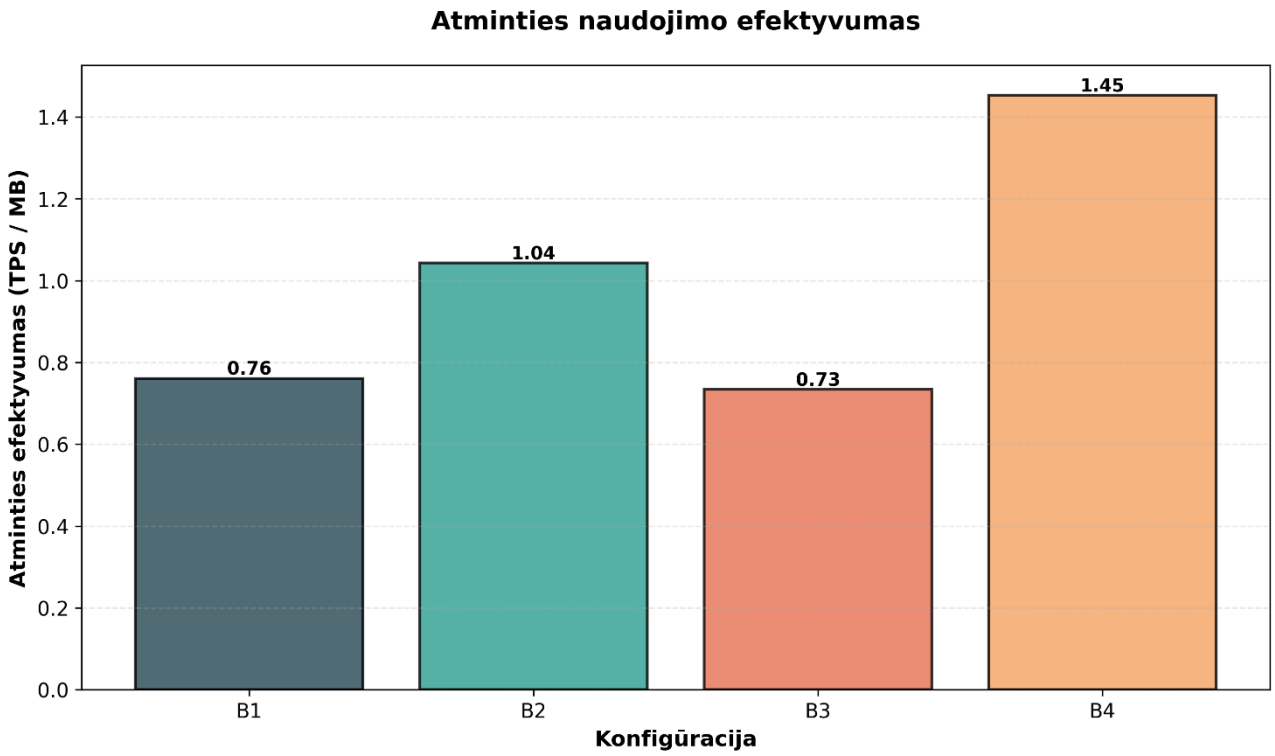
Diagrama atskleidžia netikėtą, tačiau įdomią tendenciją – atminties naudojimas nėra tiesiogiai proporcingas bloko dydžiui. Iš pirmo žvilgsnio būtų galima tikėtis, kad didesni blokai pareikalaus daugiau RAM, tačiau gauti rezultatai rodo priešingą situaciją: didžiausias atminties naudojimas pasiekiamas ne su didžiausiu, o su vidutinio dydžio, B3 konfigūracija (50 transakcijų blokas), kuri sunaudoja net 1085 MB. Tuo tarpu didžiausias 100 transakcijų blokas (B4) yra pats efektyviausias ir apsiriboja tik 587 MB. Tai leidžia identifikuoti aiškią anomaliją, reikalaujančią detalesnės analizės.

Vertinant B3 konfigūraciją, galima teigti, kad ji patenka į tarpinę zoną. Blokas yra per didelis, kad užsipildytų taip greitai, kaip mažesni B1 ir B2 blokai, tačiau ir per mažas, kad pilnai išnaudotų B4 konfigūracijos privalumus. Kitaip tariant, ši konfigūracija nepatenka nei į greitai pildomą, nei į efektyviai amortizuojančią apkrovą kategoriją. Dėl to sistemoje susidaro daugiau laukiamųjų transakcijų, kurios kurį laiką laikomos atmintyje, kol susiformuoja pilnas 50 transakcijų blokas.

Nors B3 blokas užsipildo per maždaug 0,05 sekundės, transakcijos patvirtinimo laikas užtrunka ilgiau, todėl tuo metu sistemoje jau ima kauptis naujas transakcijų rinkinys. Dėl to atmintis nuolat pilnėja ir tarp apdorojimo ciklų susidaro papildomos vėluojančios transakcijos, kurie talpinami RAM. Šis reiškinys paaiškina, kodėl būtent B3 konfigūracija pasižymi didžiausiu atminties piku.

Visai kitaip elgiasi B4 konfigūracija. 100 transakcijų blokas užsipildo šiek tiek lėčiau (apie 0,1 sekundės), tačiau jo dydis leidžia vieno ciklo metu apdoroti dvigubai daugiau operacijų. Tai sumažina transakcijų kaupimąsi tarp blokų formavimo intervalų ir leidžia atmintį naudoti labiau apkrovai proporcingu būdu. Dėl to B4 konfigūracija tampa ne tik našiausia, bet ir efektyviausiai naudojančia RAM resursus.

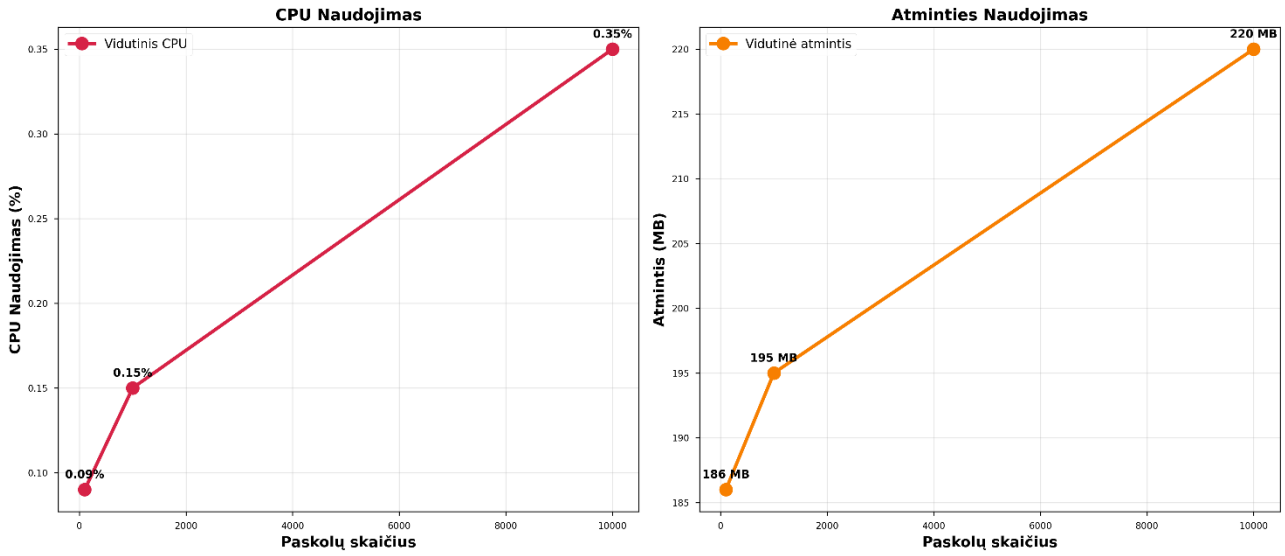
Norint kiekybiškai įvertinti šį efektyvumą, apskaičiuotas TPS/MB (žr. 27 pav.)



27 pav. Atminties naudojimo efektyvumo palyginimas

Šis rodiklis leidžia palyginti, kiek transakcijų per sekundę sistema sugeba apdoroti vienam megabaitui naudojamos atminties. Rezultatai išryškina itin aiškią tendenciją: B4 konfigūracija pasiekia geriausią rezultatą – 1,45 TPS vienam MB, o tai yra beveik dvigubai geriau nei B3 konfigūracijos 0,73 TPS/MB. Tai dar kartą patvirtina, kad didesni blokai ne tik gerina pralaidumą ir mažina vėlavimą, bet ir leidžia sistemai naudoti resursus taupiau bei subalansuotai.

Galiausiai, svarbu paminėti ir resursų naudojimą generuojant reguliacines ataskaitas (žr. 28 pav.)



28 pav. CPU ir atminties naudojimas generuojant ataskaitą skirtingo dydžio duomenų bazėje

Kairėje pateikiamas CPU apkrovos procentas, dešinėje – sunaudotos RAM atminties kiekis (MB). Matyti, kad resursų poreikiai auga labai nežymiai: esant 100 paskolų, vidutinė CPU apkrova siekė vos ~0,09%, prie 1000 paskolų – ~0,15%, o esant 10000 paskolų pakilo iki ~0,35%. Atminties sąnaudos didėjo nuo ~186 MB (100 pask.) iki ~195 MB (1000 pask.) ir ~220 MB (10000 pask.). Šie dydžiai rodo, kad net maksimalios apkrovos metu sistema sunaudoja mažiau nei ketvirtadalį vieno gigabaito RAM ir mažiau nei pusę procento procesoriaus laiko. Praktiškai tai reiškia labai nedidelę infrastruktūrinę naštą – tokiai apkrovai nebūtina galinga techninė įranga. Toliau aptariami ir apibendrinami visi rezultatai.

3.4. Rezultatų apibendrinimas

Eksperimento metu gauti rezultatai leidžia aiškiai suprasti, kaip bloko dydžio parametras *MaxMessageCount* veikia „Hyperledger Fabric“ tinklo našumą, vėlavimą ir resursų naudojimą. Pirmiausia pastebima, kad didesni blokai turi tiesioginį ir labai ryškų teigiamą poveikį pralaidumui. Padidinus bloką nuo 10 iki 100 transakcijų, TPS išauga net 45,8 %, o augimas išlieka beveik tiesinis visame intervale – 10, 25, 50 ir 100 transakcijų blokai atitinkamai pasiekia 585, 713, 796 ir 853 TPS. Tai leidžia daryti išvadą, jog didesni blokai reikšmingai padidina sistemos pralaidumą .Ne ką mažiau įdomus rezultatas susijęs su vėlavimu. Tradiciškai būtų tikimasi kompromiso tarp didesnių blokų ir delsos, tačiau šiame eksperimente tokio kompromiso nepastebėta. Priešingai – 100 transakcijų blokai sumažino vidutinį vėlavimą daugiau nei perpus, nuo 9,54 iki 4,66 sekundės. Tai reiškia, kad esant dideliam transakcijų srautui, dideli blokai ne tik nedidina laukimo, bet netgi pagerina reagavimo laiką, nes sumažėja bendras konsensuso ciklų skaičius. CPU naudojimo analizė pateikia dar vieną svarbų aspektą. Nors pralaidumas auga beveik 46 %, CPU naudojimas kyla tik apie 10 %. Tai rodo žymų efektyvumo šuolį: TPS/CPU santykis pagerėja net 77,2 %, nuo 178,4 iki 316 TPS už kiekvieną procesoriaus procentą. Kitaip tariant, didesni blokai leidžia sistemai atlikti žymiai daugiau darbo faktiškai nepakeičiant skaičiavimo apkrovos.

Atsižvelgiant į gautus rezultatus, galima pateikti aiškias ir praktiškai taikomas rekomendacijas, kurios padėtų pasirinkti tinkamiausius bloko parametrus skirtingoms darbo apkrovoms. Didelio transakcijų srauto scenarijuose (1000 TPS ir daugiau) optimaliausiu pasirinkimu išlieka *MaxMessageCount* = 100 ir *BatchTimeout* = 2 s. Ši konfigūracija užtikrina didžiausią pralaidumą, mažiausią vėlavimą ir geriausią procesoriaus bei atminties naudojimo efektyvumą. Ji ypač tinka gamybinėms sistemoms, intensyviausioms veiklos valandoms ir masiniam duomenų apdorojimui. Mažos apkrovos scenarijuose, kai transakcijos nepasiekia *MaxMessageCount* ribos, svarbesniu parametru tampa *BatchTimeout*. Todėl rekomenduojama išlaikyti 100 transakcijų bloką, tačiau sumažinti *BatchTimeout* iki 0,5–1 sekundės, kad sistemos atsakas nevėluotų. Tai ypač aktualu testavimo aplinkoms, mažo srauto laikotarpiams ar vystymo tinklams.

Apibendrinant ataskaitų generavimo rezultatus, galima išskirti vieną pagrindinių pranašumų – itin greitas ataskaitų generavimas: tipinės ketvirčio ataskaitos (apie 1000 paskolų) parengiamos per ~0,2 s, o net 10 kartų didesnio duomenų kiekio ataskaita – greičiau nei per 10 s. Tokie rezultatai turi reikšmingų praktinių implikacijų. Lietuvos bankas, kaip reguliatorius, galėtų pasinaudoti realaus laiko ataskaitų gavimo galimybėmis – tai leistų dažniau ir operatyviau stebėti finansų rinkos dalyvių būklę, greičiau identifikuoti rizikas ir užtikrinti atitiktį teisės aktams. Tarpusavio skolinimo platformų operatoriams šis sprendimas suteikia galimybę automatizuoti ataskaitų rengimą, taip smarkiai sumažinant žmogiškųjų išteklių poreikį ir pašalinant žmogiškųjų klaidų riziką. Vietoje ilgo duomenų

ruošimo ir derinimo proceso, platformos galėtų vos per kelias sekundes pateikti finansines ataskaitas. Be to, dėl mažų resursų sąnaudų, toks sprendimas būtų ekonomiškas – potencialiai sumažėtų IT infrastruktūros ir ataskaitų rengimo sąnaudos.

Remiantis atlikto eksperimentavimo rezultatais, siūloma sukurti blokų grandinės pagrindu veikiančią ataskaitų sistemą, kurią administruotų Lietuvos bankas. Siūloma architektūra grįsta „Hyperledger Fabric“ tinklu su išmaniaisiais kontraktais, kurio dalyviai – P2P skolinimo platformos ir Lietuvos bankas – būtų atskiri tinklo nariai (organizacijos). Kiekviena platforma ir Lietuvos bankas būtų sujungti per atskirą kanalą, užtikrinant privatumą ir tiesioginį duomenų srautą tarp platformos ir reguliatoriaus. Lietuvos banko mazgas veiktų kaip stebėtojas visų kanalų atžvilgiu, gaudamas transakcijų duomenis realiu laiku. Toks sprendimas leistų reguliatoriui iškart stebėti platformų veiklą ir fiksuoti reikšmingus įvykius be papildomo tarpinių ataskaitų apdorojimo.

Svarbu paminėti, pagal anksčiau pateiktus duomenis, per dieną yra pateikiama iki keliasdešimt paskolų, sukurtas prototipas įrodo, kad net ir nenaudojant didelių išteklių galima išgauti kelis šimtus transakcijų per sekundę. „Hyperledger Fabric“ architektūra leidžia reguliatoriui gauti duomenis beveik be vėlavimo, nes blokų kūrimo periodiškumas ir dideli blokų dydžiai užtikrina aukštą našumą. Tokiu būdu Lietuvos bankas galėtų bet kada išsitraukti reikiamus duomenis ar parengti ataskaitas per kelias sekundes, kaip rodo atlikto eksperimento ataskaitų generavimo greitis. Dėl to realiose sąlygose reguliatorius galėtų dažniau stebėti rinką, greičiau identifikuoti rizikas ir operatyviau užtikrinti atitiktį teisės aktams. Pavyzdžiui, net ir dirbant labai intensyviai, ataskaitos, kurios dabar ruošiasi valandomis, būtų gaunamos tinkle vos per kelias sekundes, sudarant galimybę reaguoti beveik realiu laiku. Tokie rezultatai patvirtina, kad rinkos dalyvių P2P paskolinimas nepatirtų apribojimų diegiant šį sprendimą – atvirkščiai, jis gerokai pagerintų duomenų prieinamumą ir apskaitą operatyvumo požiūriu.

Šiuo metu P2P paskolų platformos ataskaitas Lietuvos bankui teikia kas ketvirtį, jas pateikdamos informacinėje sistemoje Excel formatu, tačiau siūlomas pokytis – sudaryti galimybę naudoti blokų grandinę, kurioje duomenys būtų kaupiami struktūrizuotai (pvz., JSON formatu) ir būtų prieinami reguliatoriui realiu laiku, taip leidžiant Lietuvos bankui tiesiogiai generuoti reikiamas ataskaitas iš pačių duomenų ir, jei reikia, jas eksportuoti į Excel, pereinant nuo rankinio ir periodinio ataskaitų teikimo prie automatizuoto ir nuolatinio duomenų gavimo; tam reikėtų teisės aktų pakeitimų, aiškiai įtvirtinant, kad duomenų gavimas per siūlomą blokų grandinės modelį yra oficialus ataskaitų teikimo būdas ir kad tokie duomenys teisiškai prilygsta tradicinėms ataskaitoms, užtikrinant konfidencialumą.

IŠVADOS

1. Leidimų reikalaujanti blokų grandinė sudaro prielaidas efektyviam finansinių ataskaitų automatizavimui, nes užtikrina visų finansinių operacijų nekintamą įrašymą ir griežtą prieigos kontrolę. Tai leidžia išsaugoti duomenų vientisumą ir konfidencialumą. Išmaniųjų sutarčių mechanizmas suteikia galimybę apskaitos taisykles įgyvendinti tiesiogiai blokų grandinėje, todėl finansiniai įrašai formuojami automatiškai pagal iš anksto apibrėžtas sąlygas, o finansinės ataskaitos gali būti generuojamos realiu laiku, sumažinant rankinio darbo apimtį ir žmogiškų klaidų riziką.
2. Blokų grandinės integravimo analizė parodė, kad ši technologija gali pagerinti tarpusavio skolinimosi platformų finansinės atskaitomybės skaidrumą ir patikimumą. Visi finansiniai įvykiai registruojami vieningoje, nekintamoje duomenų grandinėje, todėl sudaromos sąlygos duomenų atsekamumui. Tai ypač aktualu auditui ir reguliacinei priežiūrai, nes ataskaitų duomenys formuojami tiesiogiai iš pirminių, nekintamų įrašų.
3. Diegiant automatizuotą finansinių ataskaitų sistemą blokų grandinės pagrindu, nustatyti keli esminiai iššūkiai. Pirmiausia, blokų grandinės nekintamumo principas kelia suderinamumo su asmens duomenų apsaugos reikalavimais (pvz., BDAR teisė būti pamirštam) klausimų, todėl būtina taikyti papildomas duomenų valdymo ir privatumo priemones. Taip pat nustatyta, kad sistemos našumas ir delsimas priklauso nuo pasirinktų blokų formavimo parametrų, todėl jų parinkimas turi būti pritaikytas konkrečiam P2P platformos transakcijų srautui ir veikimo scenarijui.
4. Sukurtas blokų grandinės prototipas, paremtas „Hyperledger Fabric“ leidimų reikalaujančia architektūra, pademonstravo praktinę automatizuoto finansinių ataskaitų generavimo galimybę. Prototipe kiekvienas paskolos suteikimo ar grąžinimo įvykis buvo nedelsiant įrašomas į blokų grandinę, o išmaniosios sutartys automatiškai vykdė ataskaitų formavimo logiką. Eksperimentų metu nustatyta, kad finansinės ataskaitos generavimo trukmė siekė apie 0,20 s, kai duomenų apimtis buvo iki 1000 paskolų, ir apie 5,08 s, kai apdorota 10000 paskolų, kas patvirtina sprendimo tinkamumą praktiniam taikymui.
5. Sistemos veikimo vertinimas parodė, kad „Hyperledger Fabric“ pagrindu sukurta sistema yra tinkama tarpusavio skolinimo platformų veiklos sąlygoms. Atsižvelgiant į tai, kad realus P2P platformų transakcijų srautas yra labai nedidelis ir neviršija maždaug 1 transakcijos per sekundę, testavimo metu pasiektas maksimalus 853,1 TPS pralaidumas laikytinas technine atsarga, o ne praktiniu poreikiu. Vertinant realius veikimo scenarijus, kuriems būdingas retesnis ir netolygus transakcijų srautas, tinkamesnėmis laikytinos mažesnio bloko dydžio konfigūracijos, užtikrinančios stabilesnį transakcijų apdorojimą ir mažesnį delsą esant žemai apkrovai. Ataskaitų generavimo testai parodė, kad net apdorojant 10000 paskolų duomenų rinkinį ataskaita sugeneruojama per ~5,08 s, o sistemos išteklių poreikis išlieka nedidelis (~0,35 % CPU ir ~220 MB RAM). Tai patvirtina, kad leidimų reikalaujanti blokų grandinė su tinkamai parinkta konfigūracija gali būti efektyviai taikoma automatizuotai P2P platformų finansinei apskaitai.

LITERATŪROS SĄRAŠAS

1. Al-Abdullah, M., Izzad, A., Ruwaida, A., & Farkas, B. (2020). Designing privacy-friendly data repositories: a framework for a blockchain that follows the GDPR. *{Digital Policy, Regulation and Governance*, 389-411.
2. Appelbaum, D., & Nehmer, R. (2017). Designing and auditing accounting systems based on blockchain and distributed ledger principles. *Feliciano School of Business, 1*, 1-19.
3. Bakos, Y., & Halaburda, H. (2021). Permissioned vs permissionless blockchain platforms: tradeoffs in trust and performance. *NYU Stern School of Business working paper*.
4. Baliga, A., Solanki, N., Verekar, S., Pednekar, A., Kamat, P., & Chatterjee, S. (2018). Performance Characterization of Hyperledger Fabric. *arXiv preprint arXiv:1809.03421*.
5. Bonyuet, D. (2020). Overview and Impact of Blockchain on Auditing. *The International Journal of Digital Accounting Research, 20*, 31-43.
6. Capocasale, V., Gotta, D., & Perboli, G. (2023). Comparative analysis of permissioned blockchain frameworks for industrial applications. *Blockchain: Research and Applications, 4*(1), 100-113.
7. ConsenSys. (2024). *ConsenSys GoQuorum*. Nuskaityta iš https://docs.goquorum.consensys.io/
8. ELTA. (2024 m. 11 01 d.). LB sustabdžius Foxpay licenciją, Migracijos departamentas nepatogumų nepatyrė. *LRT*.
9. Fortune Business Insights. (2025 m. 12 01 d.). *Peer-to-Peer Leding Market Size, Share & Industry Analysis.* Nuskaityta iš https://www.fortunebusinessinsights.com/peer-to-peer-lending-market-114634
10. Francati, D., Ateniese, G., Faye, A., Milazzo, A. M., Perillo, A. M., Schiatti, L., & Giordano, G. (2021). Audita: A Blockchain-based Auditing Framework for Off-chain. *Proceedings of the Ninth International Workshop on Security in Blockchain and Cloud Computing*, (p. 5-10).
11. Gamage, H. T., Weerasinghe, H. D., & Dias, N. G. (2020). A survey on blockchain technology concepts, applications, and issues. *SN Computer Science, 1*, 1-15.
12. Hyperledger Fabric. (2025). *A Blockchain Platform for the Enterprise*¶.
13. Jiang, X. (2018). The application of blockchain in auditing. *2018 2nd International Conference on Education Science and Economic Management (ICESEM 2018)* (p. 1018-1023). Atlantis Press.
14. Kalajdjieski, J., Raikwar, M., Arsov, N., Velinov, G., & D., G. (2023). Databases fit for blockchain technology: A complete overview. *Blockchain: Research and Applications., 4*, 100-116.
15. Khazaei, E., & Arabsorkhi, A. (2024). Comparative Studies: Blockchain Technology Applications in GDPR-Representing an Applicability Model. *2024 10th International Conference on Web Research (ICWR)*, (p. 187-194).
16. Klimaševska, Ū. (2025 m. 11 06 d.). LB: finansines ataskaitas vėluojančiai pateikti Payserai – 20 tūkst. eurų bauda. *LRT*.
17. Lietuvos bankas. (2012 m. 12 06 d.). *Dėl Vartojimo kredito davėjų ir tarpusavio skolinimo platformos operatorių privalomos informacijos teikimo Lietuvos bankui taisyklių patvirtinimo.* Nuskaityta iš https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.439434/asr

18. Lietuvos Bankas. (2018 m. 12 20 d.). *Ataskaitų teikimo kalendorius.* Nuskaityta iš https://www.lb.lt/lt/ataskaitu-teikimo-kalendorius
19. Lietuvos Bankas. (2020). *Tarpusavio skolinimo platformos operatorių veiklos apžvalga.*
20. Lietuvos Bankas. (2024 m. 07 30 d.). *Tarpusavio skolinimo platformos operatoriai*. Nuskaityta iš https://www.lb.lt/lt/tarpusavio-skolinimo-platformos-operatoriai
21. (2018). *Lietuvos Respublikos vartojimo kredito įstatymas.*
22. Liu, M., Kean, W., & Xu, J. J. (2019). How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain. *Current Issues in auditing, 13*, A19-A29.
23. Milne, A., & Parboteeah, P. (2016). *The Business Models and Economics of Peer-to-Peer lending. ECRI Research Report No 17, May 2016.*
24. Monrat, A. A., Schelén, O., & Andersson, K. (2020). Performance evaluation of permissioned blockchain platforms. *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, (p. 1-8).
25. Nguyen, M., Loghin, D., & Dinh, T. (2021). Understanding the scalability of Hyperledger Fabric. *arXiv preprint arXiv:2107.09886*.
26. Ofir, M., & Tzang, I. (2022). An Empirical View of Peer-to-Peer (P2P) Lending Platforms. *Berkeley Bus. LJ, 19*, 175.
27. Polge, J., Robert, J., & Le Traon, Y. (2021). Permissioned blockchain frameworks in the industry: A comparison. *Ict Express, 7*(2), 229-233.
28. R3. (2025). *R3 Technical Documentation*. Nuskaityta iš https://docs.r3.com/
29. (2020). *Reglamentas (ES) 2020/1503 dėl Europos sutelktinio finansavimo paslaugų verslui teikėjų.* Nuskaityta iš https://eur-lex.europa.eu/legal-content/lt/ALL/?uri=CELEX:32020R1503
30. Sarker, J. (2025). Blockchain Technology in Accounting and Auditing: Benefits, Challenges, and Emerging Practices. *South Asian Res J Bus Manag, 7*(6), 517-526.
31. Sarmah, S. S. (2018). Understanding blockchain technology. *Computer Science and Engineering, 8*, 23-29.
32. Schmitz, J., & Leoni, G. (2019). Accounting and Auditing at the Time of Blockchain Technology: A Research Agenda. *Australian Accounting Review, 29*, 331-342.
33. Supriadi, M., Hendra, P. D., & Miya, D. (2020). The effect of applying blockchain to the accounting and auditing. *Ilomata International Journal of Tax and Accounting, 1*, 161-169.
34. Swan, M. (2015). *Blockchain: Blueprint for a new economy.* O'Reilly Media, Inc.
35. Victory, T., & Yazid, S. (2023). Review of Peer-to-Peer (P2P) Lending Based on Blockchain. *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika (JITEKI), 9*(4), 1154-1167.
36. Wüst, K., & Gervais, A. (2018). Do you need a blockchain?, (p. 45-54).
37. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.
38. Zulkarnain, M. M., Ramli, N., & Nordin, A. N. (2025). Performance benchmarking of hyperledger fabric on heterogeneous hardware for iot applications. *IIUM Engineering Journal, 26*(3), 156-170.

PRIEDAI

VARTOJIMO KREDITO DAVĖJO VEIKLOS ATASKAITA

		Iš viso	Pagal vartojimo kredito sutarties rūšis		
			Sąskaitos kreditavimo sutartys	Susietojo vartojimo kredito sutartys	Kitos vartojimo kredito sutartys
		1	2	3	4
1	**A. Informacija apie vykdytą vartojimo kreditų teikimo arba tarpusavio skolinimo platformos operatoriaus veiklą ataskaitinio laikotarpio pabaigoje**				
2	Išmokėtų vartojimo kreditų skaičius, vnt.	13760			13760
3	Likusi grąžinti išmokėtų vartojimo kreditų suma, Eur	42366535,52			42366535,52
4	Iš jų, Eur. Likusi grąžinti išmokėtų vartojimo kreditų suma, kai vartojimo kredito grąžinimo terminas buvo praėstas, vartojimo kredito gavėjui sumokėjus praėsimo mokestį	0			
5	Vartojimo kredito gavėjų skaičius, vnt.	10400			10400
6	Iš jų, vnt. Vartojimo kredito gavėjų, jaunesnių nei dvidešimt penkerių metų, skaičius	1658			1658
7	Paskolos davėjų skaičius, vnt.	15372			15372
8	Išmokėtų vartojimo kreditų, kurių grąžinimui užtikrinti pritaikytos prievolės įvykdymo užtikrinimo priemonės, skaičius, vnt.	0	0	0	0
9	Iš jų, vnt. Garantijos ir laidavimai	0			0
10	Iš jų, vnt. Draudimas (įskaitant, kai vartojimo kredito gavėjas draudžia gyvybę vartojimo kredito davėjo, tarpusavio skolinimo platformos operatoriaus arba paskolos davėjo naudai)	0			0
11	Iš jų, vnt. Turto įkeitimas	0			0
12	Iš jų, vnt. Vekseliai	0			0
13	Vartojimo kreditų, kai mokėjimas buvo pradelstas, skaičius, vnt.	3153	0	0	3153
14	Iš jų, vnt. Vartojimo kreditų, kai mokėjimas buvo pradelstas daugiau kaip 30 dienų, bet ne daugiau kaip 60 dienų iš eilės, skaičius	330			330
15	Iš jų, vnt. Vartojimo kreditų, kai mokėjimas buvo pradelstas daugiau kaip 60 dienų, bet ne daugiau kaip 90 dienų iš eilės, skaičius	206			206
16	Iš jų, vnt. Vartojimo kreditų, kai mokėjimas buvo pradelstas daugiau kaip 90 dienų iš eilės, skaičius	2617			2617
17	Vartojimo kredito gavėjų įsiskolinimų, kai mokėjimas buvo pradelstas, suma, Eur	12739091,9	0	0	12739091,9
18	Iš jų, Eur. Vartojimo kredito gavėjų įsiskolinimų, kai mokėjimas buvo pradelstas daugiau kaip 30 dienų, bet ne daugiau kaip 60 dienų iš eilės, suma	1659512,02			1659512,02
19	Iš jų, Eur. Vartojimo kredito gavėjų įsiskolinimų, kai mokėjimas buvo pradelstas daugiau kaip 60 dienų, bet ne daugiau kaip 90 dienų iš eilės, suma	942154,23			942154,23
20	Iš jų, Eur. Vartojimo kredito gavėjų įsiskolinimų, kai mokėjimas buvo pradelstas daugiau kaip 90 dienų iš eilės, suma	10137425,65			10137425,65
21	Vartojimo kredito sutarčių, pagal kurias skola buvo perduota išieškoti tretiesiems asmenims, skaičius, vnt.	2817	0	0	2817
22	Iš jų, vnt. Vartojimo kredito sutarčių, pagal kurias skola buvo perduota išieškoti teismo būdu, skaičius, vnt.	2277			2277
23	Iš jų, vnt. Vartojimo kredito sutarčių, pagal kurias skola buvo perduota išieškoti ikiteisminiu būdu, skaičius, vnt.	540			540
24	**B. Informacija apie vykdytą vartojimo kreditų teikimo arba tarpusavio skolinimo platformos operatoriaus veiklą per ataskaitinį laikotarpį**				
25	Išmokėtų vartojimo kreditų skaičius, vnt.	2076			2076
26	Išmokėtų vartojimo kreditų suma, Eur	7718577,49			7718577,49
27	Vidutinė bendros vartojimo kredito kainos metinė norma, proc.	20,62			20,6
28	Vidutinė vartojimo kredito palūkanų norma, proc.	12,16			12,14
29	Per ataskaitinį laikotarpį vartojimo kredito gavėjų sumokėta bendra vartojimo kredito kaina, Eur	1794312,7			1794312,7
30	Vidutinė per atskaitinį laikotarpį suteikto vartojimo kredito trukmė, mėnesiais	47			46
31	Nutrauktų vartojimo kredito sutarčių, kai vartojimo kredito gavėjas nevykdė savo įsipareigojimų, skaičius, vnt.	174			174
32	Gautų vartojimo kredito gavėjų skundų skaičius, vnt.	0			0
33	Gautų iš trečiųjų asmenų skundų skaičius, vnt.	0			0

29 pav. Vartojimo kredito davėjo veiklos ataskaitos pavyzdys (1)

34	**C. Informacija apie vykdytą mažųjų vartojimo kreditų teikimo arba tarpusavio skolinimo platformos operatoriaus veiklą ataskaitinio laikotarpio pabaigoje**	
35	Išmokėtų mažųjų vartojimo kreditų skaičius, vnt.	56
36	Likusi grąžinti išmokėtų mažųjų vartojimo kreditų suma, Eur	6808,05
37	Iš jų, Eur. Likusi grąžinti išmokėtų mažųjų vartojimo kreditų suma, kai vartojimo kredito grąžinimo terminas buvo pratęstas, vartojimo kredito gavėjui sumokėjus pratęsimo mokestį	
38	Mažojo vartojimo kredito gavėjų skaičius, vnt.	56
39	Iš jų, vnt. Mažojo vartojimo kredito gavėjų, jaunesnių nei dvidešimt penkerių metų, skaičius	13

40	Išmokėtų mažųjų vartojimo kreditų, kurių grąžinimui užtikrinti buvo pritaikytos prievolės įvykdymo užtikrinimo priemonės, skaičius, vnt.	0
41	Iš jų, vnt. Garantijos ir laidavimai	
42	Iš jų, vnt. Draudimas (įskaitant, kai vartojimo kredito gavėjas draudžia gyvybę vartojimo kredito davėjo, tarpusavio skolinimo platformos operatoriaus arba paskolos davėjo naudai)	
43	Iš jų, vnt. Turto įkeitimas	
44	Iš jų, vnt. Vekseliai	
45	Mažųjų vartojimo kreditų, kai mokėjimas buvo pradelstas, skaičius, vnt.	6
46	Iš jų, vnt. Mažųjų vartojimo kreditų, kai mokėjimas buvo pradelstas daugiau kaip 30 dienų, bet ne daugiau kaip 60 dienų iš eilės, skaičius	3
47	Iš jų, vnt. Mažųjų vartojimo kreditų, kai mokėjimas buvo pradelstas daugiau kaip 60 dienų, bet ne daugiau kaip 90 dienų iš eilės, skaičius	0
48	Iš jų, vnt. Mažųjų vartojimo kreditų, kai mokėjimas buvo pradelstas daugiau kaip 90 dienų iš eilės, skaičius	3
49	Mažojo vartojimo kredito gavėjų įsiskolinimų, kai mokėjimas buvo pradelstas, suma (įskaitant netesybas ir palūkanas), Eur	832,75
50	Iš jų, Eur. Mažojo vartojimo kredito gavėjų įsiskolinimų, kai mokėjimas buvo pradelstas daugiau kaip 30 dienų, bet ne daugiau kaip 60 dienų iš eilės, suma	75,42
51	Iš jų, Eur. Mažojo vartojimo kredito gavėjų įsiskolinimų, kai mokėjimas buvo pradelstas daugiau kaip 60 dienų, bet ne daugiau kaip 90 dienų iš eilės, suma	75,37
52	Iš jų, Eur. Mažojo vartojimo kredito gavėjų įsiskolinimų, kai mokėjimas buvo pradelstas daugiau kaip 90 dienų iš eilės, suma	681,96
53	Mažojo vartojimo kredito sutarčių, pagal kurias skola buvo perduota išieškoti tretiesiems asmenims, skaičius, vnt.	0
54	Iš jų, vnt. Vartojimo kredito sutarčių, pagal kurias skola buvo perduota išieškoti teismo būdu, skaičius, vnt.	
55	Iš jų, vnt. Vartojimo kredito sutarčių, pagal kurias skola buvo perduota išieškoti ikiteisminiu būdu, skaičius, vnt.	
56	**D. Informacija apie vykdytą mažųjų vartojimo kreditų teikimo arba tarpusavio skolinimo platformos operatoriaus veiklą per ataskaitinį laikotarpį**	
57	Išmokėtų mažųjų vartojimo kreditų skaičius, vnt.	75
58	Išmokėtų mažųjų vartojimo kreditų suma, Eur	11550
59	Iš jų, Eur. Ryšio priemonėmis (telefonu, internetu) suteiktų mažųjų vartojimo kreditų suma	
60	Vidutinė bendros mažųjų vartojimo kreditų kainos metinė norma, proc.	54,62
61	Vidutinė mažųjų vartojimo kreditų palūkanų norma, proc.	23,72
62	Vidutinė per ataskaitinį laikotarpį suteikto mažojo vartojimo kredito trukmė, mėnesiais	2
63	Grąžintų mažųjų vartojimo kreditų suma, Eur	10301,8
64	Iš jų, Eur. Grąžintų mažųjų vartojimo kreditų suma, kai mažasis vartojimo kreditas ar jo dalis buvo grąžinti pritaikius prievolės įvykdymo užtikrinimo priemones	
65	Per ataskaitinį laikotarpį mažojo vartojimo kredito gavėjų sumokėta bendra vartojimo kredito kaina, Eur	546,76
66	Nutrauktų vartojimo kredito sutarčių, pagal kurias buvo išmokėti mažieji vartojimo kreditai, kai vartojimo kredito gavėjas nevykdė savo įsipareigojimų, skaičius, vnt.	0
67	Gautų mažojo vartojimo kredito gavėjų skundų skaičius, vnt.	

30 pav. Vartojimo kredito davėjo veiklos ataskaitos pavyzdys (2)

2 PRIEDAS

Visas išeities kodas pateikiamas GitHub saugykloje. Nuoroda: https://github.com/domgud/p2p-lending-magistras-new