

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
INFORMACIJOS IR INFORMACINIŲ TECHNOLOGIJŲ SAUGA (6211BX008)

SIMAS KRUŠNIAUSKAS

ELEKTRONINĖ BALSAVIMO SISTEMA, PAGRĮSTA BLOKŲ GRANDINIŲ TECHNOLOGIJA

Baigiamasis projektas

Vadovas
Prof. dr. A. Venčkauskas

(parašas) (data)

Recenzentas
Doc. dr. Gedeiminas Činčikas

(parašas) (data)

Studentas
S. Krušniauskas

(parašas) (data)

Kaunas, 2023



Kauno technologijos universitetas

Informatikos fakultetas

Simas Krušniauskas

Elektroninė balsavimo sistema, pagrįsta blokų grandinių technologija

Akademinių sąžiningumo deklaracija

Patvirtinu, kad:

1. baigiamąjį projektą parengiau savarankiškai ir sąžiningai, nepažeisdama(s) kitų asmenų autoriaus ar kitų teisių, laikydamasi(s) Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo nuostatų, Kauno technologijos universiteto (toliau – Universitetas) intelektinės nuosavybės valdymo ir perdavimo nuostatų bei Universiteto akademinės etikos kodekse nustatytų etikos reikalavimų;
2. baigiamajame projekte visi pateikti duomenys ir tyrimų rezultatai yra teisingi ir gauti teisėtai, nei viena šio projekto dalis nėra plagijuota nuo jokių spausdintinių ar elektroninių šaltinių, visos baigiamojo projekto tekste pateiktos citatos ir nuorodos yra nurodytos literatūros sąrašė;
3. įstatymų nenumatytų piniginių sumų už baigiamąjį projektą ar jo dalis niekam nesu mokėjęs (-usi);
4. suprantu, kad išaiškėjus nesąžiningumo ar kitų asmenų teisių pažeidimo faktui, man bus taikomos akademinės nuobaudos pagal Universitete galiojančią tvarką ir būsiu pašalinta(s) iš Universiteto, o baigiamasis projektas gali būti pateiktas Akademinės etikos ir procedūrų kontrolieriaus tarnybai nagrinėjant galimą akademinės etikos pažeidimą.

Simas Krušniauskas

Patvirtinta elektroniniu būdu

Krušniauskas, Simas. „Elektroninė balsavimo sistema, pagrįsta blokų grandinių technologija“. Magistro baigiamasis projektas / vadovas prof. dr. Algimantas Venčkauskas; Kauno technologijos universitetas, Informatikos fakultetas.

Studijų kryptis ir sritis (studijų krypčių grupė): Informatikos inžinerija, informacijos ir informacinių technologijų sauga.

Reikšminiai žodžiai: elektroninis balsavimas, blokų grandinė, internetinis balsavimas.

Kaunas, 2023. 84 p.

Santrauka

Demokratija visuomet susiduria su įvairiais iššūkiais ir bandymais šią valdymo formą pažeisti ar net visai sužlugdyti. Dėl šios priežasties yra labai svarbu visais įmanomais būdais užtikrinti saugius ir nepažeidžiamus prezidento, seimo ar savivaldos rinkimus. Tobulėjant technologijoms ir siekiant rinkėjams sumažinti nepatogumus atiduoti balsui keliaujant į numatytas rinkimines vietas, siekiama pereiti prie elektroninių sistemų, kuriomis būtų galima išreikšti savo valią renkant kandidatus į atitinkamas valdymo pozicijas. Kadangi rinkimai yra labai jautri tema, elektroninės balsavimo sistemos turi užtikrinti teisę į slaptą balsavimą bei atitikti tradiciniam balsavimui keliamus reikalavimus ir principus, t. y. turi užtikrinti visuotinę rinkimų teisę, lygią rinkimų teisę, tiesioginius ir laisvus rinkimus, slaptą balsavimą bei skaidrų rinkimų mechanizmą. Siekiant ne tik užtikrinti standartinius reikalavimus, bet ir užtikrinti rinkėjų anonimiškumą, skaidrumą ir balsų vientisumą, siūloma kurti elektroninę balsavimo sistemą, pagrįstą blokų grandinių technologija. Siūlomas sprendimas nenaudoja jokių jau egzistuojančių karkasų, taip pat nenaudoja visiems gerai žinomos standartinės blokų grandinės struktūros (kai viename bloke yra saugoma n transakcijų). Priešingai, sprendime siūloma tokia blokų grandinės struktūra, kai kiekvienas rinkėjo balsas būtų saugomas atskirame bloke, kuriame būtų perskaičiuojami ir kartu įrašomi rinkimų rezultatai einamuoju momentu. Kuriamo sprendimo blokų grandinės tinklas būtų paskirstytas, privatus tinklas. Rinkėjo atiduoto balso bloke nėra tiesioginių duomenų apie rinkėją, saugoma tik iš rinkėjo duomenų apskaičiuota maišos reikšmė, taip užtikrinant galimybę rinkėjui pareiškus norą, atvaizduoti, kaip ir kur buvo įrašytas jo balsas, ar balsas buvo išsaugotas teisingai ir nepakeistas.

Siekiant įvertinti, ar sprendimas užtikrina pagrindinius reikalavimus buvo aprašyta siūlomo sprendimo vizija ir architektūra, papildomai aprašyta idėja, kaip būtų galima rinkėjus registruoti sistemoje, įsitikinant, kad tai yra tikrai tas asmuo, kuriuo jis teigia esąs. Sukurtas sistemos prototipas, atlikti kiekybinis ir kokybinis tyrimai, taip įvertinant siūlomo sprendimo saugumą, efektyvumą ir atitikimą iškeltiems reikalavimams.

Krušniauskas, Simas. Electronic Voting System Based on Blockchain Technology. Master's Final Degree Project / supervisor prof. dr. Algimantas Venčkauskas; The Faculty of Informatics, Kaunas University of Technology.

Study field and area (study field group): Informatics Engineering, Information and Information Technology Security.

Keywords: electronic voting, blockchain, online voting.

Kaunas, 2023. 84 p.

Summary

Democracy faces various challenges and attempts to disrupt or destroy this form of governance. Because of that, it is very important to ensure safe and inviolable elections of the President or other government. With the development of technology and with intention to reduce the inconvenience of traveling to the intended polling places to cast the vote, the aim is to move to electronic voting systems, which could be used to express one's will in electing candidates for the relevant management positions. Since elections are very delicate topic, electronic voting systems must ensure the right to secret voting and meet the requirements and principles of traditional voting. I. e. must ensure universal suffrage, equal suffrage, direct and free elections, secret ballot and transparent election mechanism. In order not only to ensure the standard requirements, but also to ensure the anonymity of voters, transparency and integrity of votes, it is proposed to create an electronic voting system based on blockchain technology. The proposed solution does not use any existing frameworks, nor does it use well-known standard blockchain structure (where n transactions are stored in one block). On the contrary, the solution proposes a blockchain structure where each voter's vote would be stored in a separate block, where the election results would be recalculated and simultaneously recorded at the current moment. A blockchain network would be a distributed, private network. The voter's cast block does not contain direct data about the voter. In the block, only the hash value calculated from the voter's personal data is stored, thus ensuring the possibility, if the voter wishes, to display how and where his vote was recorded, whether the vote was saved correctly and unaltered.

In order to assess whether the solution meets the basic requirements, the vision and architecture of the proposed solution were described. Additionally the idea of how voters could be registered in the system, making sure that they are really the person they claim to be, was described. A prototype of the system was created, quantitative and qualitative studies were carried out in order to evaluate the safety, efficiency and compliance of the proposed solution with the requirements.

Turinys

Paveikslų sąrašas	7
Įvadas.....	9
1. Analitinė dalis	10
1.1.Lietuvos Respublikos Seimo rinkimų procesas	10
1.1.1. Rinkimų organizavimo tvarka	10
1.1.2. Rinkėjų sąrašai	10
1.1.3. Kandidatų kėlimas.....	10
1.1.4. Parengtinė rinkimų organizavimo veikla	11
1.1.5. Balsavimas.....	11
1.1.6. Balsų skaičiavimas ir rinkimų rezultatų nustatymas.....	12
1.2.Balsavimo internetu rinkimuose ir referendumuose koncepcijos apžvalga	13
1.3.Popierinio balsavimo proceso schema	14
1.4.Elektroninio balsavimo proceso schema	15
1.5.Tradicinio balsavimo trūkumai ir blokų grandinių pritaikymo galimybės.....	16
1.6.Elektroninių balsavimo sistemų ir jų saugos analizė	17
1.6.1. Išskirtų kortelių balsavimo sistemos.....	17
1.6.2. Optinio skenavimo balsavimo sistemos	18
1.6.3. Tiesioginio įrašymo elektroninės sistemos.....	19
1.6.4. Internetinis balsavimas	20
1.7.Elektroninių balsavimo sistemų saugos problemos, apsaugų prieš jas galimybės	21
1.7.1. Sudėtingų sistemų problemos	21
1.7.2. Kriterijai nustatantys e. balsavimo sistemų patikimumą.....	22
1.7.3. Apsisaugojimo nuo pasitaikančių grėsmių pasiūlymai	24
1.7.4. Blokų grandinių naudojimas e. balsavimo sistemose	24
1.8.Blokų grandinių technologijų, metodų ir karkasų analizė	25
1.8.1. Blokų grandinių technologijos.....	25
1.8.2. Blokų grandinių privalumai	26
1.8.3. Blokų grandinių sunkumai	26
1.8.4. Blokų grandinių karkasai	26
1.9.Blokų grandinių technologijų naudojimo elektroninėse balsavimo sistemose analizė	27
1.9.1. Projektai naudojantys blokų grandinių technologiją balsavimo sistemoms.....	28
1.10. Estų balsavimo sistemos pavyzdys	29
1.10.1. Estų nacionalinės asmens tapatybės kortelės.....	29
1.10.2. Internetinio balsavimo sistema.....	30
1.11. Analizės dalies išvados	31
2. Elektroninės balsavimo sistemos pagrįstos blokų grandinių technologija architektūra	32
2.1.Vizija.....	32
2.2.Elektroninės balsavimo sistemos, pagrįstos blokų grandinių technologija tinklo architektūra.....	34
2.3.Elektroninės balsavimo sistemos, pagrįstos blokų grandinių technologijomis blokų grandinių ir blokų schemas	34
2.4.Elektroninės balsavimo sistemos, pagrįstos blokų grandinių technologijomis veiklos diagramos	37
2.4.1. Rinkėjo registracija elektroninėje balsavimo sistemoje	37

2.4.2.	Rinkėjo prisijungimas prie elektroninės balsavimo sistemos.....	38
2.4.3.	Balsavimas elektroninėje balsavimo sistemoje	40
2.4.4.	Rinkėjų bloko grandinės bloko kūrimas elektroninėje balsavimo sistemoje.....	40
2.4.5.	Balsų bloko grandinės pirmojo bloko kūrimas.....	41
2.4.6.	Balsų bloko grandinės bloko kūrimas elektroninėje balsavimo sistemoje	42
2.5.	Elektroninės balsavimo sistemos pagrįstos blokų grandinių technologijomis diegimo diagrama.....	43
2.6.	Projektavimo dalies išvados.....	45
3.	Elektroninės balsavimo sistemos, pagrįstos blokų grandinių technologijomis prototipo realizacija	46
3.1.	Realizacijai naudotos priemonės.....	46
3.2.	Balsuotojų blokų grandinės architektūra ir komponentai	47
3.2.1.	Balsuotojų blokų grandinės valdymo programa	48
3.2.2.	Balsuotojų blokų grandinės elgsenos modeliai	50
3.3.	Rinkimų balsų blokų grandinės architektūra ir komponentai	54
3.3.1.	Balsų blokų grandinės valdymo programa	57
3.3.2.	Balsų blokų grandinės elgsenos modeliai	58
3.4.	Testavimo ir demonstracijos naudotojo sąsaja.....	60
3.5.	Prototipo realizacijos dalies išvados	67
4.	El. balsavimo sistemos, pagrįstos blokų grandinių technologija tyrimas.....	68
4.1.	Kokybinis tyrimas	68
4.2.	Kiekybinis tyrimas.....	70
4.3.	Prototipo blokų grandinės struktūros palyginimas su įprasta blokų grandinės struktūra	79
4.4.	Tyrimo dalies išvados	81
	Išvados	82
	Literatūros sąrašas	83

Paveikslų sąrašas

1 pav. Popierinio balsavimo schema.....	15
2 pav. Elektroninio balsavimo schema.....	16
3 pav. Elektroninės balsavimo sistemos pagrįstos blokų grandinių technologija vizija	33
4 pav. Centralizacija, decentralizacija ir paskirstyti duomenys (angl. Centralized, Decentralized, and Distributed Ledger) [27].....	34
5 pav. Elektroninės balsavimo sistemos registruotų naudotojų blokų grandinės schema.....	35
6 pav. Elektroninės balsavimo sistemos registruotų naudotojų blokų grandinės bloko schema	35
7 pav. Elektroninės balsavimo sistemos balsų blokų grandinės schema	36
8 pav. Elektroninės balsavimo sistemos balsų blokų grandinės bloko schema	37
9 pav. Rinkėjo registravimosi elektroninėje balsavimo sistemoje veiklos diagrama.....	38
10 pav. Rinkėjo prisijungimo prie elektroninės balsavimo sistemos veiklos diagrama	39
11 pav. Balsavimo elektroninėje balsavimo sistemoje veiklos diagrama	40
12 pav. Rinkėjų blokų grandinės bloko kūrimo elektroninėje balsavimo sistemoje veiklos diagrama	41
13 pav. Pirmojo balsų bloko grandinės bloko kūrimo elektroninėje balsavimo sistemoje veiklos diagrama	42
14 pav. Bloko kūrimo elektroninėje balsavimo sistemoje veiklos diagrama.....	43
15 pav. Elektroninės balsavimo sistemos, pagrįstos blokų grandinių technologijomis diegimo diagrama	44
16 pav. Blokų grandinės mazgo paleidimo elgsenos modelis	51
17 pav. Registracijos termino nustatymo elgsenos modelis	52
18 pav. Bloko kūrimo balsuotojų blokų grandinėje elgsenos modelis.....	53
19 pav. Registracijos draudimo (užbaigimo) elgsenos modelis.....	54
20 pav. Bloko kūrimo balsų blokų grandinėje elgsenos modelis.....	59
21 pav. Naudotojo sąsaja - Prisijungimas	60
22 pav. Naudotojo sąsaja – Registracija	60
23 pav. Naudotojo sąsaja – Administratoriaus panelė (1)	61
24 pav. Naudotojo sąsaja – Administratoriaus panelė (2)	61
25 pav. Naudotojo sąsaja – Administratoriaus panelė (3)	62
26 pav. Naudotojo sąsaja – Administratoriaus panelė (4)	62
27 pav. Naudotojo sąsaja – Administratoriaus panelė (5)	63
28 pav. Naudotojo sąsaja – Administratoriaus panelė (6)	63
29 pav. Naudotojo sąsaja – Administratoriaus panelė (7)	64
30 pav. Naudotojo sąsaja – Administratoriaus panelė (8)	64
31 pav. Naudotojo sąsaja – Rinkėjo panelė (1).....	65
32 pav. Naudotojo sąsaja – Rinkėjo panelė (2).....	65
33 pav. Naudotojo sąsaja – Rinkėjo panelė (3).....	66
34 pav. Rinkėjo duomenų nuasmeninimas (1).....	68
35 pav. Rinkėjo nuasmeninimas (2).....	68
36 pav. Rinkėjo balso atvaizdavimas	69
37 pav. Mazgo blokų grandinės sukompromitavimas.....	69
38 pav. Resursų sąnaudos	71
39 pav. Balso išrinkimas pagal indeksą, tikrinant blokų grandinės integralumą.....	72
40 pav. Balso išrinkimas pagal indeksą, netikrinant blokų grandinės integralumo	73

41 pav. Bloko išrinkimas pagal rinkėją, tikrinant blokų grandinės integralumą	74
42 pav. Bloko išrinkimas pagal rinkėją, netikrinant blokų grandinės integralumo	75
43 pav. Balsų perskaičiavimas, tikrinant blokų grandinės integralumą.....	76
44 pav. Balsų perskaičiavimas, netikrinant blokų grandinės integralumo.....	77
45 pav. Veiksmai MySQL duomenų bazėje	78
46 pav. Standartinė blokų grandinės struktūra.....	79
47 pav. Siūlomo sprendimo balsų blokų grandinės struktūra	79

Ivadas

Demokratija – pastaruoju metu viena bene plačiausiai minimų ir diskutuojamų temų. Šiai valdymo sistemai įgavus pripažinimą ir tapus pagrindine valdymo forma daugelyje valstybių, piliečiai gali laisva valia rinktis savo atstovus valdžioje, balsuodami valdžios atstovų, Lietuvoje LR Seimo, LR prezidento ar savivaldos, rinkimuose. Todėl, tam, kad rinkimai būtų sąžiningi ir skaidrūs, o rinkimų rezultatai atspindėtų realius piliečių pasirinkimus, demokratijoje yra labai svarbu sauga balsavimo metu, tai galima prilyginti nacionaliniam saugumui. Bėgant dešimtmečiams į saugumo užtikrinimą balsavimo metu atkreipiama vis daugiau dėmesio. Siekiama išvengti rinkiminio papirkinėjimo, rezultatų klastojimo, todėl stengiamasi ne tik padidinti rinkimų saugumą, tačiau šį procesą padaryti kuo efektyvesnį bei reikalaujantį mažiau kaštų. Metai iš metų yra tobulinamas kompiuterinių sistemų saugumas, todėl pradėta diskutuoti ir apie rinkimų proceso perkėlimą į elektroninę erdvę.

Pirmąsias elektronines balsavimo sistemas galima laikyti gana sėkmingomis, kadangi tai padėjo paspartinti rinkimų procesą, tačiau buvo susidurta su labai rimtomis saugumą kompromituojančiomis pasekmėmis. Atsiradus blokų grandinių technologijai, ji per labai trumpą laiką tapo labai populiari. Šią technologiją stengiamasi panaudoti kuo įvairesnėse srityse ir kurti ne tik efektyvias, bet ir labai saugias sistemas. Žinoma, elektroninės balsavimo sistemos taip pat neapsiėjo be blokų grandinių technologijos įtraukimo. Tačiau didžioji dalis e. balsavimo sistemų, pagrįstų blokų grandinių technologijomis, yra gana naujos, neišsprendžiančios visų saugos problemų, nėra patogios naudoti arba turi kitokių trūkumų. Būtent todėl šią sritį vis dar reikia tobulinti ir ieškoti sprendimų, kurie padėtų vykdyti saugesnius balsavimus rinkimų metu, o iš skubančios šių dienų visuomenės reikalautų kuo mažiau pastangų.

Darbo tikslas – sukurti e. balsavimo sistemos, pagrįstos blokų grandinių technologija, prototipą. Tikslą pasiekti padės šie uždaviniai:

1. išanalizuoti balsavimo sistemų saugos problemas, e. balsavimo saugą;
2. išanalizuoti e. balsavimo saugos problemas, apsaugų prieš jas galimybes;
3. atlikti blokų grandinių technologijos analizę, jų karkasų analizę;
4. išanalizuoti blokų grandinių naudojimą elektroninėse balsavimo sistemose;
5. pasiūlyti e. balsavimo sistemos pagrįstos blokų grandinių technologija, sprendimo būdą;
6. praktiškai realizuoti e. balsavimo sistemos prototipą, atlikti analizę, pagrindžiančią minėtų problemų sprendimą.

1. Analitinė dalis

1.1. Lietuvos Respublikos Seimo rinkimų procesas

Pagal Lietuvos Respublikos (toliau – LR) įstatymus, LR seimo deputatai renkami ketveriems metams vienmandatėse ir daugiamandatėse rinkimų apygardose. Rinkimai remiasi visuotine ir lygia rinkimų teise, slaptu balsavimu tiesioginiuose mišrios sistemos rinkimuose. Rinkimų teisę turi visi LR piliečiai, ne jaunesni (rinkimų dieną) nei aštuoniolika metų. Deputatu gali būti renkamas LR pilietis, ne jaunesnis nei dvidešimt vienerių metų (rinkimų dieną) ir paskutinius trejus metus nuolatos gyvenęs Lietuvoje. [1]

Kiekvienas LR pilietis, kuris turi teisę rinkti, rinkimuose gauna po vieną balsą tiek vienmandatėje, tiek daugiamandatėje apygardoje. Visų rinkėjų balsai yra lygiaverčiai. Verta paminėti, kad Seimo deputatai rinkėjų yra renkami be tarpininkų (tiesioginiai rinkimai). Visi rinkėjai balsuoja asmeniškai ir slapta, o rinkėjų valios kontroliavimas yra draudžiamas. [1]

1.1.1. Rinkimų organizavimo tvarka

Pagal įstatymus rinkimus į LR Seimą organizuoja ir vykdo vyriausioji rinkimų komisija, apygardų rinkimų komisija ir apylinkių rinkimų komisija. [1]

1.1.2. Rinkėjų sąrašai

Norint vykdyti rinkimus, turi būti sudaromi kiekvienos apylinkės rinkėjų sąrašai. Į šiuos sąrašus įrašomi LR piliečiai turintys teisę rinkti. Rinkėjas yra priskiriamas tos apylinkės rinkimų sąrašui, kurioje apylinkėje sąrašo sudarymo metu jis nuolat gyvena. Užsienyje gyvenantys piliečiai neįrašyti į sąrašus bendraja tvarka, pagal jų pasirinkimą gali būti įrašyti į tos rinkimų apygardos sąrašą, kurios teritorijoje jie nuolatos gyveno iki išvykimo. Asmenys, kurie atlieka tikrąją karinę tarnybą arba alternatyvią tarnybą yra įrašomi į tos apylinkės rinkėjų sąrašą, kurioje gyveno iki tarnybos pradžios. Labai svarbu atsiminti, kad kiekvienas rinkėjas gali būti įrašytas tik į vieną rinkėjų sąrašą, o tai užtikrina Vyriausioji rinkimų komisija. Sudaryti rinkėjų sąrašai yra paskelbiami likus ne mažiau kaip dvidešimt dienų iki rinkimų. Rinkėjams yra sudaroma galimybė susipažinti su šiais sąrašais, nustatant laiką ir vietą. [1]

1.1.3. Kandidatų kėlimas

Tiek vienmandatėse, tiek daugiamandatėse rinkimų apygardose kandidatus į deputatus turi teisę kelti politinės partijos, kurios įregistruotos rinkimams pagal politinių partijų įstatymą ne vėliau, kaip prieš trisdešimt penkias dienas iki rinkimų pradžios. Taip pat tokią teisę turi ir politiniai judėjimai. Jų įstatai su nuoroda į politinį organizacijos pobūdį ir jų pakeitimai turi būti įregistruoti LR Teisingumo ministerijoje ne vėliau kaip prieš du mėnesius iki rinkimų pradžios. Taip pat turi būti surinkta ne mažiau kaip vienas tūkstantis rinkėjų parašų, remiančių judėjimo dalyvavimą rinkimuose. Reiktų nepamiršti, kad ir pavieniai asmenys gali iškelti save į kandidatus vienmandatėse rinkimų apygardose, tačiau jų kandidatūrą turi raštu remti ne mažiau kaip vienas tūkstantis tos apygardos rinkėjų. Daugiamandatėje rinkimų apygardoje visuomeniniai politiniai judėjimai ir politinės partijos pateikia kandidatų sąrašą (sąrašė negali būti mažiau nei 20 kandidatų), taip pateikdami savo kandidatus. Keliant kandidatus turi būti pateikiami visi pareiškiniai dokumentai, nurodyti LR Seimo rinkimų įstatymo 31 straipsnyje (31 straipsnis. Kandidatų iškėlimo pareiškiniai dokumentai). [1]

Svarbu paminėti, kad kiekvienas kandidatas gali būti įrašytas tik į vienos politinės partijos ar visuomeninio politinio judėjimo iškeltų kandidatų sąrašą daugiamandatėje rinkimų apygardoje. Taip pat šis asmuo (įrašytas į prieš tai minėtą sąrašą) tuo pat metu turi teisę būti iškeltas kandidatu ir dar vienoje vienmandatėje rinkimų apygardoje. Kelios politinės partijos ar visuomeniniai politiniai judėjimai turi galimybę sujungti savo iškeltų kandidatų sąrašus, jeigu iki rinkimų dienos liko ne mažiau kaip trisdešimt penkios dienos. Pasibaigus terminui teikti kandidatų sąrašus, LR Teisingumo ministerija per vieną dieną Vyriausiosios rinkimų komisijos reikalavimu oficialiai patvirtina įregistruotas politines partijas ir visuomeninius politinius judėjimus. Eilės numerių suteikimas pagal burtus atskirais sąrašais yra organizuojamas Vyriausiosios rinkimų komisijos, dalyvaujant politinėms partijoms, visuomeniniams politiniams judėjimams ir jų koalicijoms. Rinkėjų sąrašai skelbiami Vyriausiosios rinkimų komisijos, likus ne mažiau kaip trisdešimt dienų iki rinkimų pradžios. Nuo šio momento prasideda rinkimų kampanija. [1]

1.1.4. Parengtinė rinkimų organizavimo veikla

Vyriausioji rinkimų komisija nustato balsavimo pažymėjimų, balsavimo biuletenių, vidinių ir išorinių vokų balsavimui paštu, kitų rinkimuose naudojamų oficialių vokų, paketų, dokumentų ir antspaudų pavyzdžius. Rinkimų į Seimą metu rinkėjui pateikiami du rinkimų biuleteniai, vienas balsavimui konkrečioje vienmandatėje rinkimų apygardoje, antrasis dėl politinės partijos ar visuomeninio politinio judėjimo kandidatų sąrašų daugiamandatėje apygardoje. [1]

Pirmajame rinkėjui pateiktame dokumente įrašyti kandidatai pagal abėcėlę, nurodyti kiekvieno kandidato į deputatus pavardė, vardas ir jį iškėlusios politinės organizacijos pavadinimas. [1]

Daugiamandatės rinkimų apygardos biuletenyje pateikiamas kandidatų sąrašas (politinių organizacijų) pavadinimai pagal joms suteiktus eilės numerius didėjančia tvarka. [1]

Kalbant apie rinkimų biuletenių pristatymą, reikia paminėti, kad jie pristatomi kartu su vokais rinkimų apylinkėms ir pašto skyriams (likus ne mažiau kaip septynioms dienoms iki rinkimų).

Numeruoti balsavimo pažymėjimai yra išduodami apylinkių rinkimų komisijai. Šiuose pažymėjimuose nurodomas rinkėjo vardas ir pavardė, gimimo data, adresas, apygarda (kurioje rinkėjas balsuoja), apylinkės, į kurios rinkėjų sąrašus įtrauktas rinkėjas, adresas. Šie pažymėjimai rinkėjams įteikiami likus ne mažiau, kaip dešimt dienų iki rinkimų dienos. [1]

1.1.5. Balsavimas

Balsavimas vyksta nustatytą dieną nustatytoje vietoje (nuo 7 iki 22 valandos). Balsavimo patalpoje, balsavimo kabinos yra įrengiamos taip, kad niekas negalėtų matyti balsuojančio asmens. Tuo metu vykstančių rinkimų kandidatų sąrašai yra iškabinami balsavimo patalpoje. Balsavimo patalpos rinkimų dieną nėra atidaromos iki tol, kol joje nėra susirinkusių bent dviejų trečiųjų apylinkės komisijos narių. Susirinkus komisijos nariams yra patikrinama balsadėžė, ar ji yra tuščia ir ji užantspauduojama. Patikrinamos visos patalpos, ar jos atitinka visus rinkimų procesui šalyje keliamus reikalavimus. Rinkimų komisijos pirmininkas išdalina rinkimų biuletenius ir rinkėjų sąrašus komisijoms nariams ir atidaro balsavimo patalpą. Apylinkės balsų skaičiavimo protokole yra įrašomas išdalintų rinkimų biuletenių skaičius. Rinkėjai atvykę balsuoti turi pateikti savo balsavimo pažymėjimą ir tapatybę patvirtinantį dokumentą, tai atlikę, pasirašo rinkėjų sąrašė. Pasirašius, rinkėjui yra pateikiamas rinkimų biuletenis, taip pat, vertėtų paminėti, kad rinkėjui balsavimo

pažymėjimas nėra gražinamas. Jeigu šio pažymėjimas rinkėjas nėra gavęs, jį gali gauti rinkimų vietoje, pateikęs tapatybės dokumentą. [1]

Rinkėjas, turintis balsavimo biuletenį, jį užpildo įrengtoje balsavimo kabinoje. Užpildytas biuletenis, kiekvieno rinkėjo asmeniškai, yra įmetamas į balsadėžę. Sugadintus rinkėjų biuletenius, reikalaujant rinkėjui, yra galimybė pakeisti naujais. Sugadintas biuletenis yra laikomas atskirai, išdavus naują biuletenį, rinkimų komisijos narys jį perbraukia ir ant jo pasirašo. Jeigu rinkėjas dėl tam tikrų fizinių trūkumų negali pats atlikti balsavimo proceso, už jį tai gali padaryti kitas jo nurodytas asmuo (išskyrus rinkimų komisijos pirmininką ar narį). [1]

Yra sudaroma galimybė balsuoti paštu. Balsavimas pradedamas likus septynioms dienoms iki rinkimų dienos ir baigiamas likus vienai dienai iki rinkimų pradžios. Už šio tipo balsavimo organizavimą atsako pašto skyriaus viršininkas. Pašto skyriaus viršininkas yra atsakingas už balsavimo vokų išdavimą ir priėmimą bei rinkėjų biuletenių išdavimą. Rinkimų biuletenių ir vokų išdavimui ir surinkimui, kai vyksta balsavimas paštu, yra skiriamas atsakingas pareigūnas. Šio balsavimo laikotarpiu, pašto skyriuose turi būti įrengta patalpa, kurioje rinkėjas gali užpildyti rinkimų biuletenį ir jį įdėti į balsavimo voką. Balsavimo voką rinkėjas užklijuoja ir kartu su savo balsavimo pažymėjimu įdeda į išorinį voką, kurį taip pat užklijuoja. Šis, išorinis, vokas yra antspauduojamas ryšių skyriaus antspaudu. Šie vokai yra adresuojami į atitinkamas apylinkes, pagal tai, kurioje apylinkėje rinkėjas yra įtrauktas į rinkėjų sąrašą. Dalis LR piliečių turi teisę balsuoti namuose (rinkėjai sulaukę 70 metų amžiaus, neįgalūs rinkėjai, juos slaugantys / prižiūrintys, laikiną nedarbingumą turintys piliečiai), tokiu atveju balsavimas taip pat vyksta paštu, išorinį voką, balsavimo voką ir rinkimų biuletenį, to prašant rinkėjui ir nurodant savo balsavimo pažymėjimo numerį, paštininkas gali atnešti į namus. Rinkėjas gavęs ir tvarkingai sutvarkęs (užpildęs biuletenius, užklijavęs vidinį voką, patalpinęs balsavimo pažymėjimą ir užklijavęs išorinį voką) vokus, juos gali įteikti pašto skyriuje, įteikti paštininkui (atnešusiam jam rinkimų dokumentus rinkėjo pageidavimu) arba įmesti jį į pašto dėžutę. [1]

Taip pat yra sudaromos galimybės balsuoti diplomatinėje atstovybėje, laive, kariniuose daliniuose, baumės atlikimo vietose. Plačiau apie šių balsavimų tvarką galima pasiskaityti Lietuvos Respublikos Seimo rinkimų įstatyme. [1]

1.1.6. Balsų skaičiavimas ir rinkimų rezultatų nustatymas

Pašto skyriuose nepanaudoti vokai ir rinkimų biuleteniai pašto viršininko yra gražinami apygardos rinkimų komisijai. Balsavimo vokų ir biuletenių apskaita yra tvarkoma pašto skyriaus viršininko tam specialiai skirtame žurnale. [1]

Rinkimų dieną, rinkimų apylinkėse, kai uždaroma balsavimo patalpa, iš kiekvieno apylinkės rinkimų komisijos nario komisijos pirmininkas surenka nepanaudotus rinkimų biuletenius, juos suskaičiuoja ir patikrina ar nėra neteisėtai išduotų biuletenių. Visi nepanaudoti ir sugadinti rinkimų biuleteniai suskaičiuojami ir sudedami į specialius vokus bei užantspauduojami. [1]

Rinkimų apylinkėje, pagal rinkėjų sąrašą yra nustatomas apylinkės rinkėjų ir balsavusių rinkėjų skaičius. Balsadėžė apžiūrima rinkimų komisijos, taip įsitikinant, kad ji visų rinkimų metu nebuvo atidaryta ar kitaip pažeista, siekiant pakeisti, išimti ar įdėti netikrus balsus. Jeigu balsadėžė yra pažeista – surašomas aktas ir balsai nėra skaičiuojami. Jeigu balsadėžė nepažeista – ji atidaroma ir

balsai pradedami skaičiuoti. Balsai turi būti skaičiuojami taip, kad šį procesą galėtų stebėti visi balsų skaičiavimo metu dalyvaujantys asmenys. [1]

Visose rinkimų apylinkėse surašomi po du balsų skaičiavimo protokolai, kuriuose įrašomi šie duomenys: rinkėjų skaičius rinkimų apylinkėje, balsavusių rinkėjų skaičius, komisijos nariams išduotų rinkimų biuletenių skaičius, nepanaudotų biuletenių skaičius, sugadintų biuletenių skaičius, negaliojančių biuletenių skaičius, galiojančių biuletenių skaičius. Abu protokolai pasirašomi rinkimų komisijos pirmininko. [1]

Svarbu paminėti, kad negaliojančiais laikomi biuleteniai – nenustatyto pavyzdžio rinkimų biuleteniai, užantspauduoti ne tos rinkimų apylinkės antspaudu, ne tos rinkimų apygardos rinkimų biuleteniai, tie, kuriuose pažymėtas daugiau kaip vienas kandidatas ar politinės partijos pavadinimas. Sprendimas dėl biuletenio negaliojimo priimamas rinkimų komisijos. [1]

Visi rinkimų biuleteniai iš rinkimų apylinkės, kartu su visais kitais dokumentais yra užantspauduojami ir perduodami apygardos rinkimų komisijai. Apygardos rinkimų komisija balsus pradeda skaičiuoti, kai gauna visus balsų skaičiavimo dokumentus iš visų rinkimų apylinkių. [1]

Platesnė informacija apie paštu gautų balsų skaičiavimą bei kitus dokumentus pateikiama Lietuvos Respublikos Seimo rinkimų įstatyme. [1]

1.2. Balsavimo internetu rinkimuose ir referendumuose koncepcijos apžvalga

2006 metais, Vyriausiosios rinkimų komisijos posėdyje buvo patvirtinta balsavimo internetu rinkimuose ir referendumuose koncepcija. Šioje koncepcijoje yra septyni pagrindiniai skyriai. [2]

Koncepcijoje nutarta, kad balsuojant internetu privalo būti laikomasi Konstitucijoje nustatytų rinkimų principų, t. y.: visuotinė, lygi tiesioginė rinkėjų teisė ir slaptas balsavimas. Buvo nustatyta, kad internetinis balsavimas turi atitikti visus tradiciniam balsavimui keliamus reikalavimus ir principus. Šio tipo balsavimas savo saugumu neturi nusileisti tradiciniam balsavimui. Koncepcijoje minima, kad internetinis balsavimas turi užtikrinti 5 pagrindinius reikalavimus [2]:

1. visuotinė rinkimų teisė – balsavimo sistema turi būti prieinama visiems, suprantama ir lengvai naudojama; [2]
2. lygi rinkimų teisė – laisvas balsavimo būdo pasirinkimas. Nepriklausomai nuo balsavimo būdo, įskaitomas tik vienas rinkėjo balsas, taip pat balsas yra lygiavertis kitam bet kuriam, bet kurio rinkėjo balsui; [2]
3. tiesioginiai rinkimai ir laisvi rinkimai – rinkėjai balsuoja be jokių tarpininkų. El. balsavimo sistemos turi garantuoti laisvą rinkėjo balso pasirinkimą, turi būti užtikrinta galimybė pakeisti balsą iki balso įregistravimo balsadėžėje. Jeigu balsuotojui leidžiama internetu balsuoti pakartotinai, yra įskaitomas tik vėliausias rinkėjo balsas. Taip pat internetinė balsavimo sistema turi aiškiai rinkėjui nurodyti, kad jo balsas buvo sėkmingai įskaitytas ir šio balso neįmanoma pakeisti; [2]
4. slaptas balsavimas – internetinis balsavimas organizuojamas taip, kad balso konfidencialumas išlaikomas bet kurioje balsavimo stadijoje. Taip pat tokios balsavimo sistemos turi užtikrinti, kad balsadėžėje esantys balsai išliktų anoniminiai, turi būti neįmanoma nustatyti ryšio tarp balso ir jį atidavusio asmens. Balsavimo sistema turi užtikrinti, kad balsų skaičius elektroninėje balsadėžėje

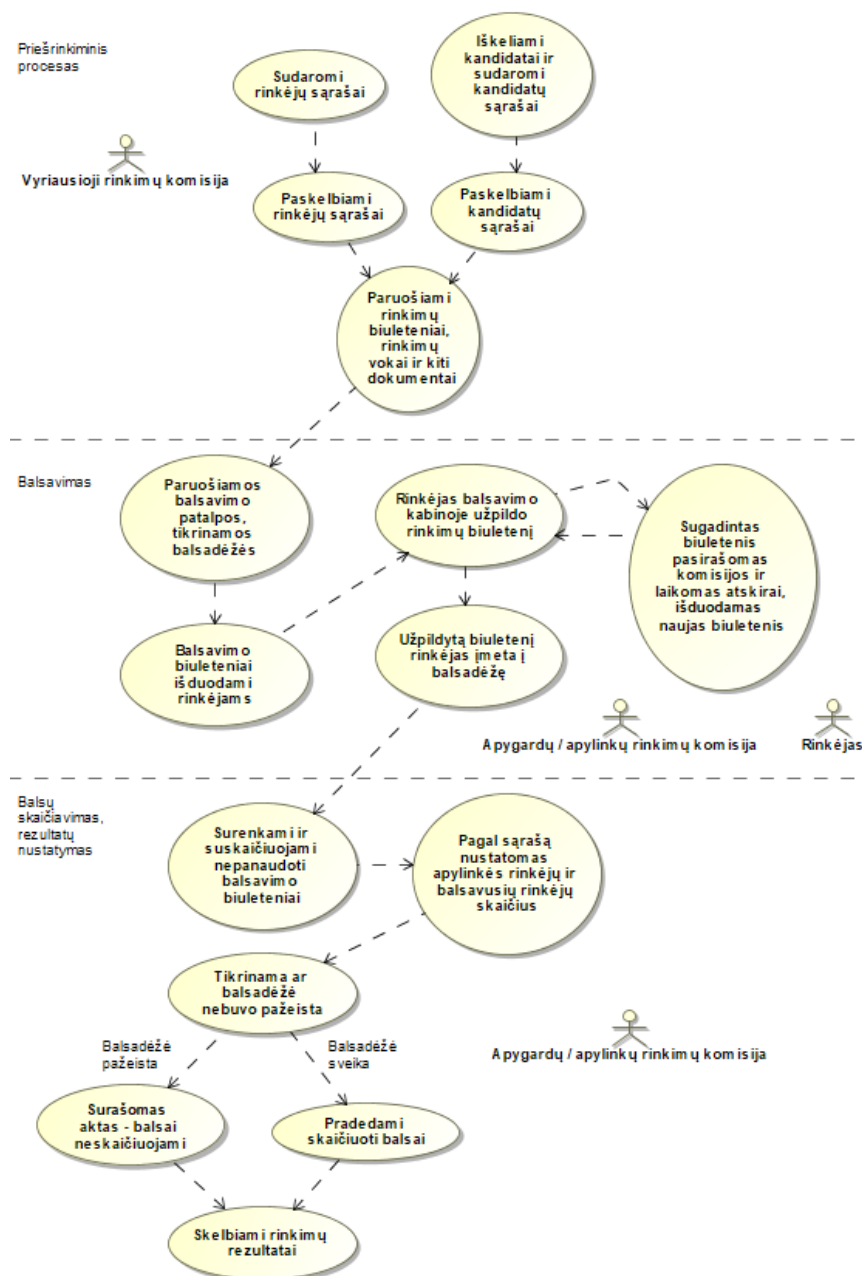
neleistų nustatyti ryšio tarp balso ir konkretaus rinkėjo. Tiek techninė, tiek programinė įranga turi būti patikimai apsaugota ir užkirsti kelią visiems nelegaliems veiksams; [2]

5. skaidrus rinkimų mechanizmas – informacija apie internetinį balsavimą turi būti išplatinta viešai, kaip ir šios sistemos funkcionavimas. Tokios sistemos turi būti įvertinamos nepriklausomų specialistų ir ekspertų. Rinkėjai turi turėti galimybę išbandyti ir priprasti prie internetinio balsavimo sistemos, prieš įregistruojant jų balsus. Turi būti sudaroma galimybė stebėtojams dalyvauti internetiniame balsavime bei rezultatų nustatymo metu, tiek, kiek numato įstatymai. Internetinio balsavimo sistemos turi būti skaidrios, kad nebūtų logiškai paaiškinamų abejonių dėl sistemų skaidrumo. [2]

Koncepcijoje minima, kad internetinio balsavimo procesas turi būti tiek saugus, tiek ir skaidrus, kad bet kuriame etape būtų galima įsitikinti proceso skaidrumu ir tikrumu. Taip pat techninė sistemos pusė turi būti visapusiškai įvertinta kompetentingų specialistų, o pati sistema apsaugota nuo visų žinomų ir įmanomų įsilaužimo ar klastojimo būdų. Vertėtų paminėti, kad koncepcijoje pripažįstama, jog internetinis balsavimas teismo gali būti pripažintas negaliojančiu, jei buvo pažeistas bent vienas iš anksčiau minėtų internetinio balsavimo principų. [2]

1.3. Popierinio balsavimo proceso schema

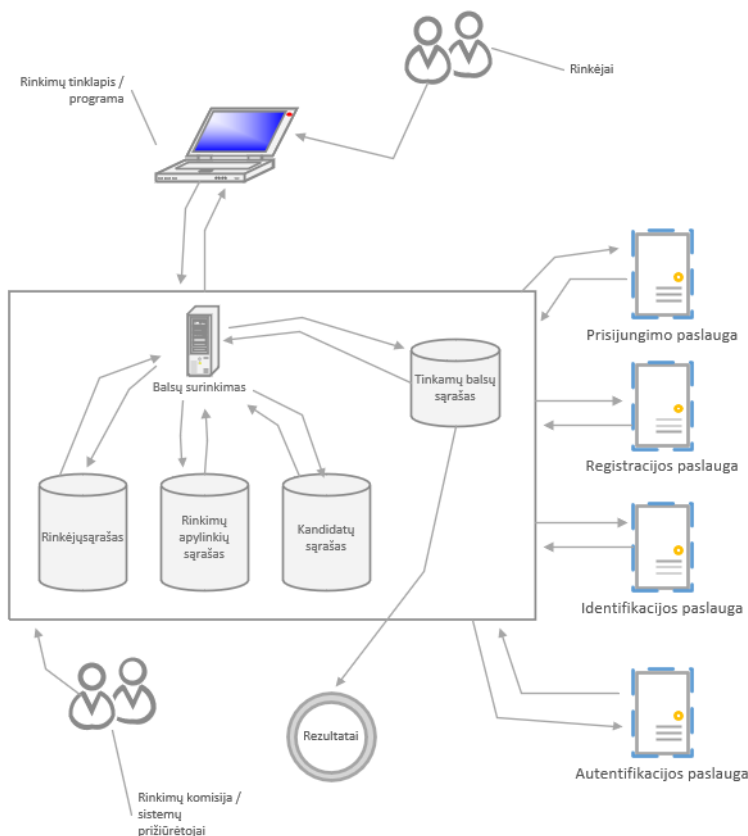
Įprastą popierinį balsavimą sudaro keletas veikėjų bei komponentų (žr. **1 pav.**). Priešrinkiminiame etape dalyvauja Vyriausioji rinkimų komisija. Šiame etape sudaromi rinkėjų ir kandidatų sąrašai, jie paskelbiami, paruošiami rinkimų biuleteniai, vokai ir visi kiti reikalingi dokumentai. Kitame balsavimo etape pagrindiniai veikėjai yra apygardų / apylinkių rinkimų komisija ir rinkėjas. Kaip galima matyti anksčiau minėtame paveiksle (žr. **1 pav.**), šiame etape yra paruošiamos rinkimų patalpos, tikrinamos balsadėžės. Atidarius balsavimo patalpas, rinkėjams yra išduodami balsavimo biuleteniai, rinkėjai atskirose, iš anksto paruoštose kabinose, gautus biuletenius užpildo ir meta į balsadėžę. Pasibaigus balsavimo laikui pereinama į trečiąją etapą – balsų skaičiavimą ir rezultatų nustatymą. Šiame etape dar kartą patikrinama balsadėžė, jeigu ji nėra pažeista, balsai skaičiuojami ir skelbiami rinkimų rezultatai. Priešingu atveju – balsai anuliuojami.



1 pav. Popierinio balsavimo schema

1.4. Elektroninio balsavimo proceso schema

Elektroniniame balsavime rinkėjai savo balsą dažniausiai atiduoda naudodamiesi asmeniniais kompiuteriais (arba mobiliaisiais telefonais). Norėdamas atiduoti balsą, rinkėjas turi prisijungti prie rinkimų sistemos, tam jis turi turėti prieigos teises. Rinkėjui teisės suteikiamos iš anksto, rinkimų komisijai jį registravus kaip rinkėją. Prisijungęs prie sistemos rinkėjas gali atiduoti savo balsą. Balsai, rinkėjų ir kandidatų sąrašai bei rinkimų apylinkių sąrašai dažniausiai yra saugomi duomenų bazėse, su kuriomis *bendruoja* rinkimų sistemos serveris. Abstrakti elektroninio balsavimo schema matoma 2 pav.



2 pav. Elektroninio balsavimo schema

1.5. Tradicinio balsavimo trūkumai ir blokų grandinių pritaikymo galimybės

Apžvelgus Lietuvos Respublikos Seimo rinkimų įstatymą [1] ir internetinio balsavimo koncepciją [2] galima pastebėti keletą vietų, keliančių susirūpinimą saugumu:

- rinkėjų ir kandidatų registracija – registruojant rinkėjus ar kandidatus gali pasitaikyti žmogiškų klaidų, taip pat sudarius šiuos sąrašus yra tikimybė, kad neautorizuoti žmonės peržiūrės arba pakeis esamą informaciją, taip sukeldami riziką rinkimų tikrumui, legalumui;
- rinkėjų ir kandidatų sąrašų perdavimas – perduodant rinkėjų sąrašus tiek popieriniu, tiek elektroniniu būdu (persiunčiant) atsiranda tikimybė, kad jie bus pakeisti arba pavogti, taip gali būti išgaunama informacija piktavalių, kurie pasinaudodami gauta arba pakeista informacija gali bandyti klastoti rinkimų rezultatus;
- balsadėžių tikrinimas ir antspaudavimas – kaip anksčiau buvo aprašyta, rinkimų dieną balsadėžės yra tikrinamos rinkimų komisijos ir komisijos pirmininko, tačiau nėra galimybės įsitikinti, kad šie asmenys nėra prigrasinti, papirkti arba kitaip paveikti priešišku rinkimams asmenų, taip paliekant galimybę klastoti rinkimų duomenis;
- balsavimo procesas – balsavimo procese, nors ir labai sunku, tačiau įmanoma apsimesti kitu asmeniu arba paveikti rinkėjo valią, taip keliant grėsmę rinkimų rezultatams. Atiduoti balsą antrą kartą yra praktiškai neįmanoma, todėl nėra galimybės rinkėjui pakeisti paveiktą balsą savo tikrąja valia;
- popierinių balsų biuletenių perdavimas (pervežimas) į skaičiavimo vietas – šio proceso, kaip ir rinkėjų ir kandidatų sąrašų perdavimo metu kyla tos pačios grėsmės;

- balsų skaičiavimo procesas – balsų skaičiuotojai gali padaryti žmogišką klaidą dėl nuovargio, išsiblaškymo ar kitų veiksnių, taip pat išlieka tikimybė, kad skaičiuotojai (arba skaičiavimo aparatai) yra paveikti priešiško asmenų.

Kaip galima matyti, tradiciniai rinkimai turi nemažą dalį saugumo grėsmių. Didžiąją dalį gali padėti išspręsti blokų grandinių naudojimas, dėl pagrindinių blokų grandinių principų: nekintamumas (angl. *immutability*) (kiekvienas blokas yra susietas vienas su kitu, todėl norint pakeisti informaciją tektų pakeisti visą tinklą), decentralizacija (angl. *decentralization*) (nėra vienos valdymo institucijos ar asmens, kuri prižiūrėtų sistemą), padidintas saugumas (angl. *enhanced security*) (kriptografijos naudojimas, maišos funkcijų naudojimas), paskirstytos knygos (angl. *distributed ledgers*) (knyga yra vieša, todėl visi naudotojai gali matyti ar informaciją yra bandoma pakeisti, ar viskas vyksta tvarkingai), sutarimas (angl. *consensus*) (naudojamas bendras sutarimo algoritmas, kurio pagrindu yra tvirtinami ir saugomi blokai, todėl blokų grandinėje saugoma tik ta informacija, kurią patvirtina naudotojai). Blokų grandinės balsavime gali būti taikomos:

- rinkėjų ir kandidatų identifikacijai ir autentifikacijai;
- rinkėjų ir kandidatų sąrašų sudarymui ir perdavimui;
- balsadėžės alternatyvai;
- balsadėžės alternatyvai ir automatiniam balsų skaičiavimui.

1.6. Elektroninių balsavimo sistemų ir jų saugos analizė

Elektroninės balsavimo sistemos – tai vienas iš patogių būdų surinkti rinkėjų balsus. Šios sistemos naudojamos nuo 1960 m. [3]. Vienos pirmųjų buvo iškirstų kortelių sistemos (angl. *punch card systems*), vėliau pradėtos naudoti optinio skenavimo sistemos (angl. *optical scanning systems*), tiesioginio įrašymo elektroninės sistemos (DRE) (angl. *direct recording electronic systems*) bei internetinis balsavimas. Yra valstybių, kurios priima elektronines balsavimo sistemas ir jas plačiai naudoja (pvz. Brazilija, Indija, Jungtinės Valstijos ir pan.), tačiau dar daugiau valstybių jomis abejoja ir naudoja tradicinį – popierinį, rankinį balsavimą. Vertėtų paminėti, kad elektroninės balsavimo sistemos, lyginant su tradiciniu balsavimu, yra žymiai pranašesnės savo efektyvumu, tačiau jos vis dar turi įvairių saugumo problemų, o tai kelia abejonių jų patikimumu ir tikslumu, todėl abejonės kelia grėsmę sąžiningam demokratiniam balsavimui [3].

1.6.1. Iškirstų kortelių balsavimo sistemos

Iškirstų kortelių balsavimo sistemose balsuotojai iškerta skylutes balsavimo biuleteniuose, naudodami specialų, pateiktą įtaisą, skirtą skylėms padaryti. Iškirdami skylės balsuotojai pareiškia kuriam kandidatui atitenka jų balsas. Užfiksavęs savo balsą, balsuotojas deda kortelę į specialų kompiuterį – balsų skaičiavimo mašiną, arba į specialią dėžę, skirtą biuleteniams surinkti, kurie vėliau yra skaičiuojami [3].

Šio tipo balsavimo sistemos buvo išrastos dar 1964 metais. Viena populiariausių iškirstų kortelių balsavimo sistemų tipo buvo – „Votomatic“ [4]. Šio tipo sistemose ant balsavimo kortelės buvo spausdinami tik numeriai su atitinkamomis vietomis, kur turėjo būti iškertamos skylutės. Instrukcijos su kandidatų vardais dažniausiai būdavo pritvirtintos prie balsavimo aparato. Balsavimo biuletenio vietos, skirtos padaryti skylutėms, lygiuodavosi įdėtos į balsavimo aparatą. Vertėtų paminėti, kad šio tipo balsavimo įrenginiuose gali būti netiksliai sulygiuojamas balsavimo aparatas ir biuletenis, dėl šios priežasties, balsuotojui nežinant, balsas galėjo būti įspaudžiamas kitam, nenorimam kandidatui.

Dar viena šio balsavimo tipo sistema – „Datavote“. Priešingai nei anksčiau aptarta, šio tipo balsavime kandidatų vardai ir visa reikalinga informacija būdavo atspausdinta tiesiai ant balsavimo biuletenio, šalia vietų, kuriose turi būti iškirstos skylės.

Šio tipo balsavimo sistemomis pradėta labai stipriai abejoti ir jų atsisakyti po 2000 metų JAV prezidento rinkimų. Pastebėta, kad 3,4 % balsuotojų, kurie balsavo Valvorto grafystėje (angl. *Walworth County*) (JAV apygarda Viskonsine), neatidavė savo balso už norimą kandidatą į prezidentus. [4] Taip atsitiko dėl netikslumų balsuojant iškirstų kortelių balsavimo sistemomis. Balsavimo biuleteniuose iškertant skylutes, likdavo kabėti popierėlio gabaliukas arba skylutės nebuvo pilnai išspaudžiamos, dėl to balsai, skaičiuojami specialių aparatų nebūdavo įskaičiuojami ir toks biuletenis būdavo užskaitomas kaip be balso pasirinktam kandidatui. Tariaama, kad dėl šių klaidų galėjo laimėti ne tas kandidatas, už kurį buvo balsuojama daugiausiai [4].

1.6.2. Optinio skenavimo balsavimo sistemos

Kalbant apie optinio skenavimo balsavimo sistemas, pirmiausia aktualu apžvelgti jų veikimo principą. Naudojant šio tipo balsavimą rinkėjai gauna specialius balsavimo biuletenius, kurie yra suprantami ir skaitomi specialaus balsų skaičiavimo aparato. Balsavimo lapuose yra nurodyti kandidatų vardai, prie kurių atspausdintas kvadratas, apskritimas arba neužbaigta rodyklė. Rinkėjas, pasirinkęs kandidatą už kurį nori balsuoti turi užpildyti figūrą (kvadratą arba apskritimą) arba užbaigti piešti rodyklę. Rinkėjų balsai skaičiuojami biuletenius sudedant į specialią mašiną, kuri aptinka ką balsuotojas pažymėjo ir duomenis įrašo į duomenų bazę. Balsams, įrašytiems į duomenų bazę yra atliekamas sumavimas ir gaunami balsų skaičiai, skirti kiekvienam kandidatui [3].

Vertėtų paminėti, kad gali būti naudojamos dvi skirtingos optinio skenavimo sistemos – optinė simbolių aptikimo (angl. *optical character recognition (OCR)*) sistema arba išmani simbolių aptikimo (angl. *intelligent character recognition (ICR)*) sistema. Šios sistemos detaliau aprašomos sekančiuose poskyriuose.

1.6.2.1. Optinė simbolių aptikimo sistema

Šio tipo sistemos dažniausiai naudojamos teksto (arba simbolių) nuskaitymui ir konvertavimui į kompiuteriui suprantamą formatą. Optinė simbolių aptikimo sistema (toliau – OCR) apdoroja nuskenuotą dokumentą ir naudodama specialią programinę įrangą atpažįsta simbolius, figūras arba tekstą (skaičius ir raides) [3]. Tokio tipo sistemos gali būti plačiai naudojamos norint perkelti rašytinus tekstus į kompiuterį, su galimybe vėliau juos koreguoti. Žinoma, vertėtų paminėti, kad OCR sistemos nėra labai tikslios ir neretai pasitaiko klaidų nuskaitytą tekstą, todėl yra reikalingas žmogiškas įsikišimas. Asmuo turi perskaityti tiek originalų tekstą, tiek nuskaitytą ir taip įsitikinti, kad viskas buvo nuskaityta ir perkelta teisingai, aptikus klaidas – jas ištaisyti. Todėl naudojant šią sistemą reikalingas dvigubas skaitymas, sistemos ir žmogaus.

1.6.2.2. Išmani optinė simbolių aptikimo sistema

Galima teigti, kad išmaniosios optinės skenavimo sistemos (toliau – ICR) yra tiesiog patobulintos OCR sistemos. ICR sistemos naudoja programinę įrangą, kuri pritaiko išmanius loginius testus nuskenuotiems duomenims. T. y., nuskenuoti tekstai yra patikrinami pagal rašybos ir gramatikos taisykles. Taip tekstas yra interpretuojamas ir nustatoma ar jis buvo nuskenuotas teisingai, nepaliekant loginių ir kitokių klaidų [3]. ICR sistemos įgyja didelį pranašumą prieš OCR sistemas,

kalbant apie ranka rašytų tekstų nuskaitymą. Išmanias optines simbolių nuskaitymo sistemas galima patikimiau naudoti įvairių formų nuskaitymui, kur tekstas dažniausiai yra ne spausdintas, o įrašomas ranka. Todėl galima patikimiau naudoti ir nuskaitant rinkimų biuletenius, kuriuose yra galimybė rinkėjams patiems įrašyti norimą kandidatą. Žinoma, nevertėtų pamiršti, kad ICR sistemos reikalauja greitesnių ir galingesnių kompiuterių, taip užtikrinant sistemos efektyvumą [3].

1.6.2.3. Optinio skenavimo sistemų klaidos

Nesunkiai galima pastebėti, kad optinio skenavimo sistemos nėra pačios patikimiausios ir šiuo atveju tai pagrįsti galima patirtimi. 2000 metų ir 2004 metų JAV prezidentų rinkimuose naudojant šio tipo balsavimo sistemas buvo susidurta su gana daug neatitikimų. Pvz., balsų skaičiavimo aparatas Floridoje nesuskaičiavo apie 31775 rinkėjų balsų, kadangi jie nenaudojo 2 numerio pieštuko arba mėlyno rašiklio pažymint norimą kandidatą, kaip buvo nurodoma instrukcijose. [5] Rinkėjai nupiešę žvaigždutes, apskritimus, arba pažymėję pasirinkimą simboliu „X“, naudojo rašiklius su rašalu, kurio nemato infraraudonieji jutikliai arba padarę klaidą, ją bandydavo ištaisyti užklijuodami arba užtušuodami pasirinkimą. Taip pat pasitaikė asmenų, kurie užpildydavo apskritimus prie visų kandidatų, o prie kandidato už kurį iš tiesų balsavo – palikdavo tuščią apskritimą, t. y., darydavo priešingai nei iš tiesų turėjo būti arba balsai nebuvo suskaičiuojami, nes rinkėjai naudojo gelinį rašiklį, o skaičiavimo aparatai buvo sukalibruoti nuskaityti tik anglies rašalą [5].

Nereikėtų pamiršti, kad aparatai netiksliai gali nuskaityti balsus ir dėl nešvarumų, dulkių. Taip pat gali pasitaikyti klaidų ir dėl popieriaus susiglamžymo. Vertėtų paminėti, kad gali pasitaikyti klaidų arba gedimų atminties kortelėse ar programinėje įrangoje, kuri skirta biuletenių nuskaitymui, balsų skaičiavimui.

1.6.3. Tiesioginio įrašymo elektroninės sistemos

Tiesioginio įrašymo elektroninėse sistemose (toliau – DRE), balsuotojai žymi savo balsą tiesiai į elektroninį įtaisą, naudodami liečiamą ekraną, mygtukus arba kitą panašų metodą. Jeigu balsavimai atliekami raštu, balsuotojui pateikiama klaviatūra, kad šis galėtų suvesti reikiamus duomenis [3]. Kaip jau buvo galima suprasti, tokio tipo balsavimo sistemose nėra reikalingi popieriniai balsavimo biuleteniai, balsuotojo balsai saugomi pačiame įtaise, kietajame diske, atminties kortelėje arba panašiam informaciją saugojančiame įrenginyje. Vertėtų paminėti, kad kai kurios sistemos saugo duomenis keliuose atminties įtaisuose, taip sukuriant atsarginę kopiją bei galimybę patvirtinti (sulyginti) balsus.

Balsavimo laikui pasibaigus, balsavimo duomenys keliama į centrinį kompiuterį. Duomenų perdavimui gali būti pasirenkami įvairūs būdai, nešiojami atminties įrenginiai, kompiuteriniai tinklai ir pan. Šis, centrinis kompiuteris, gavęs informaciją iš visų balsavimo vietų, atlieka balsų skaičiavimus [3].

Taip pat aktualu pažymėti, kad šios sistemos tikrai nėra tobulos ir joms kyla nemažai saugumo grėsmių. DRE tipo balsavimo sistemos priklauso nuo programinės įrangos, naudojamos balsavimo aparatuose bei balsų skaičiavimo mašinose, teisingumo (angl. *correctness*), tvirtumo (angl. *robustness*) ir saugumo (angl. *security*) [6]. Šio tipo balsavimo sistemose gali pasitaikyti, kad programinė įranga turi trūkumų arba yra užkrėsta virusų. Virusais dar galima traktuoti ir asmenis, kurie nori pakenkti vieniems kandidatams, o padėti kitiems. Tie asmenys gali būti rinkimų komisija, programinės įrangos kūrėjai arba balsavimo sistemų prižiūrėtojai. Neatmetama galimybė, kad jais

gali būti netgi asmenys, kuriantys operacinę sistemą, kuriai yra kuriama balsavimo sistemos programinė įranga, pavyzdžiui, asmuo į DRE balsavimo sistemą gali įdiegti programinę įrangą (kenksmingą kodą), kuri bus aktyvuojama rinkimų dieną ir pakeis rinkėjų balsus, taip suklaidinant rinkimų rezultatus. Naudojant kodo maskavimo metodus, tokio tipo ataką būtų labai sunku aptikti. Kodo maskavimas gali būti atliekamas pasinaudojant vienu ar keliais iš egzistuojančių metodų, pavyzdžiui [6]:

- pervadinimas (angl. *renaming*) – metodas pakeičia metodus ir kintamųjų vardus, naujieji vardai gali turėti neperskaitomų arba nematomų simbolių [6];
- pakavimas (angl. *packing*) – programa suspaudžiama, taip padarant programinį kodą neperskaitomu [6];
- netikro kodo įterpimas (angl. *dummy code insertion*) – įterpiamas perteklinis kodas, kuris neatlieka jokių veiksmų. Taip padaroma sunkiau perskaityti programinį kodą, taip pat pasinaudoti atvirkštine inžinerija [6];
- metaduomenų ir nereikalingo kodo pašalinimas (angl. *metadata and unused code removal*) – pašalinamas nereikalingas kodas bei metaduomenys, kurie gali suteikti daug naudingos informacijos apie programą, taip apsunkinant bandymus išsiaiškinti tikrąją programinės įrangos paskirtį.

Vertėtų nepamiršti, kad balsavimo sistemų gadinimas gali būti atliekamas tų pačių asmenų, kurie turi prižiūrėti DRE balsavimo įrangą. Tai yra grėsmė, kadangi šie fiziniai asmenys gali turėti prieigą prie įrangos jau po jos sertifikavimo ir patvirtinimo naudojimui. Tuomet jie gali įkelti kenksmingą programinį kodą ir taip pakenkti balsavimo baigčiai.

Šio tipo balsavimo sistemos nėra atsparios ir įvairiems virusams ar kitoms grėsmėms, tokioms kaip [6]:

- trojos arkliai (angl. *trojan horse*) – virusus sunku aptikti, gali pažeisti visus rinkimų rezultatus. Virusas gali būti įdiegiamas tiek DRE sistemų pardavėjų, tiek operacinės sistemos pardavėjų;
- komercinės paslaptys – dažniausiai dėl komercinių paslapčių nėra galimybės pilnai patikrinti programinės įrangos;
- netinkama konfigūracija – sistemos konfigūracijos pakeitimas gali atverti naujų skylių, taip sukuriant lengvą kelią įsilaužėliams;
- programinė įranga su klaidomis – kaip jau buvo aptarta, ne visuomet programinė įranga yra ištestuota teisingai, o tai gali lemti neteisingą balsavimą ar rinkėjo privačios informacijos atkleidimą.

1.6.4. Internetinis balsavimas

Niekas negalėtų ginčyti, kad internetas ir šiuolaikinės technologijos ne tik padeda žmonėms, bet ir labai stipriai pagreitina procesus, suteikia patogumo kasdienėms užduotims atlikti. Turbūt tai bene pati svarbiausia priežastis, kodėl buvo atkreiptas dėmesys į internetinį balsavimą. Kaip jau buvo minėta, internetinis balsavimas ne tik suteikia patogumo balsuotojams, kadangi rinkėjams nereikia išeiti iš namų, bet ir padeda sumažinti rinkimų kaštus, paspartinti rinkimų balsų skaičiavimus, lyginant su anksčiau aptartomis iškirstų kortelių balsavimo, optinio skenavimo arba tiesioginio įrašymo elektroninėmis sistemomis. Kalbant apie internetinį balsavimą, galima išskirti tris skirtingas šio balsavimo formas:

- internetinis balsavimas specialiose balsavimo vietose (angl. *polling site internet voting*) – rinkėjai pateikia savo balsus, pasinaudodami internetu naudodamiesi kompiuteriu ar kita specializuota įranga, kuri yra įrengta specialiose balsavimo vietose. Tokiu atveju tiek aparatūrinė, tiek programinė įranga yra prižiūrima rinkimų komisijos, o rinkėjų identifikacija gali būti vykdoma tradicinėmis priemonėmis [3].
- Internetinis balsavimas kioskuose (angl. *kiosk internet voting*) – kaip ir prieš tai aptrautame internetinio balsavimo atvejuje, taip ir šiame, tiek aparatūrinė, tiek programinė įranga yra prižiūrima rinkimų komisijos. Tačiau šiuo atveju rinkimų aparatai, kuriais rinkėjai balsuoja, yra įrengiami viešose vietose, tokiose kaip: prekybos centrai ir pan. Šiuo atveju, priešingai nei minėtame anksčiau, rinkimų komisija neatlieka rinkėjo identifikacijos [3].
- Nuotolinis internetinis balsavimas (angl. *remote internet voting*) – šiuo atveju, nei aparatūrinė įranga, nei aplinka, kurioje yra atliekami balsavimai, nėra prižiūrimi rinkimų komisijos. Galima pastebėti, kad dėl to šis balsavimas gali atrodyti ne toks saugus, tačiau pažymėtina, jog balsavimas gali būti atliekamas tik sistemose, kuriose rinkėjas gali patvirtinti savo tapatybę, o tai suteikia galimybę balsuoti tiesiai iš namų, darbo ar kitos aplinkos, kurioje yra interneto ryšys. Žinoma, būtent šis balsavimo būdas turi kitų, didelę riziką keliančių saugumo spragų [3].

Kalbant apie internetinio balsavimo saugą, svarbu pastebėti, kad didžiausia grėsmė kyla iš balsuotojų kompiuterių arba paprastai tariant, net dėl interneto. Nesunku suprasti, kad tikėtis, jog balsuotojų kompiuteriai nėra užkrėsti įvairių virusų yra tiesiog naivu. Taip pat yra sunku užtikrinti rinkėjų privatumą, pvz., šeimoje gali būti skirtingų politinių pažiūrų asmenų, kurie gali paveikti šeimos narių balsus fiziniu arba emociniu spaudimu. Taip pat, šiuo atveju yra sunku pažaboti balsų pirkimą, kadangi asmenys, perkantys balsus gali lengviau kontroliuoti už ką asmuo iš tiesų balsuoja.

Galima išskirti it kitas internetiniam balsavimui kylančias grėsmes:

- paslaugų atsisakymo (angl. *denial of service*) grėsmė – nutraukiama galimybė rinkėjams atiduoti savo balsą. Prieš tokio tipo atakas yra sunku apsisaugoti, taip pat sunku rasti kas jas atliko [6].
- Trojos arkliai, šnipinėjimo programos (angl. *spyware*), balsų pakeitimas arba stebėjimas – galimas balsų vogimas, rinkėjo privačios informacijos pasisavinimas. Galima apsaugoti individualius kompiuterius, tačiau apsaugoti viešai naudojamus yra labai sunku [6].
- Automatizuotas balsų pirkimas – pažeidžiami rinkimų rezultatai. Aptikti įmonę ar asmenį atliekantį šiuos veiksmus galima, tačiau tai gali būti organizuojama iš kitos šalies ar žemyno, tai apsunkina teisinius procesus, o kartais netgi nėra galimybės imtis priemonių prieš nusikaltėlį [6].
- Klastojimas (angl. *spoofing*) – suklautojami rinkėjų balsai, pažeidžiami rinkimų rezultatai [6].

1.7. Elektronini balsavimo sistemų saugos problemos, apsaugų prieš jas galimybės

1.7.1. Sudėtingų sistemų problemos

Kaip galima pastebėti, balsavimo sistemos nėra pačios paprasčiausios. Jas sudaro programinė arba aparatūrinė įranga, o neretai – ir programinė ir aparatūrinė įranga kartu. Šių sistemų programinę įrangą sudaro labai didelis kiekis kodo eilučių, taip pat, tarpusavyje įvairiai persipynusi aparatūrinė įranga ir visa tai turi komunikuoti be problemų. Būtent dėl to yra labai svarbu suprasti, kokios yra sudėtingų sistemų problemos, natūralūs įvykiai.

1.7.1.1. Natūralūs įvykiai

Kalbant apie elektorines balsavimo sistemas, galima suprasti, kad tai nėra labai paprastos sistemos. Nesvarbu ar tai būtų optinio skenavimo, ar internetinė, ar iškirstų kortelių balsavimo sistema, visos jos savyje turi sudėtingas sistemas. Vienose tai – programinis kodas, kitose – aparatūrinė įranga. Pagrindinė problema, kad kuo sudėtingesnė sistema, tuo tikimybė susilaukti nesusipratimų ir klaidų tampa vis mažiau išvengiama. O klaidos skirtingose sudėtingos sistemos vietose gali privesti prie visiškai nenusipėjimų ir didelį poveikį turinčių pasekmių [7]. Neretai sistemų klaidos atsiranda ne dėl iš anksto žinomų ir apgalvotų pažeidžiamumų, bet dėl to, kad sistema pradeda veikti visiškai priešingai, nei buvo tikimasi, dėl nežinomos priežasties.

Dar viena problema, kad neretai žmonės pervertina technologijų ir naujų sistemų patikimumą, tikisi, kad jos išspręs visas numatytas problemas, dėl kurių buvo sukurtos. Todėl visiškai nėra kreipiamas dėmesys į nenusipėjimus veiksmus ir pažeidžiamumus. Galėtume teigti, kad naujos technologijos tarsi užburia žmones, sukuria visiško saugumo iliuziją. Vertėtų pastebėti, kad sudėtingėjant sistemoms, jų klaidų tikimybė ne tik tampa natūraliu reiškiniu, bet ir yra neišvengiama, nesvarbu, ar tai visiškai nauja technologija, ar patobulinta, siekianti išspręsti tam tikras klaidas ir / ar spragas. Bene didžiausia sudėtingų sistemų problema, kad jos susidūrusios su klaidomis ar pažeidžiamumais nenustoja veikusios, tačiau grąžina visiškai nenusipėjimus rezultatus, kurie kartais gali būti net nepastebėti [7].

Turbūt vienintelis būdas išvengti klaidų sudėtingose sistemose yra prevencija, t. y., reikia testuoti visus įmanomus atvejus, tuos apie kuriuos žinoma ir tuos, apie kuriuos nežinoma nieko, tiksliau – netgi tas klaidas ar pažeidžiamumus, kurie dar net nėra išrasti [7].

1.7.2. Kriterijai nustatantys e. balsavimo sistemų patikimumą

Kaip jau buvo pastebėta, pereiti prie elektroninių balsavimo sistemų nėra taip paprasta. Kad ir koks stiprus noras būtų, ar kiek resursų ir dėmesio tam būtų skiriama, šioms sistemoms gali kilti daug įvairių grėsmių. Todėl prieš kuriant svarbu susidaryti teorinį kliūčių žemėlapi, nustatant kaip jas identifikuoti ir vertinti, taip palengvinant kūrimo procesą ir sustiprinant galimybę šių kliūčių išvengti. Būtent apie kriterijus, kuriais galima apibūdinti e. balsavimo sistemų patikimumą ir bus kalbama šiame poskyryje.

1.7.2.1. Neapskaityti balsai

Neapskaityti balsai (angl. *the residual votes*) – tai balsai kurie negali būti užskaityti rinkimuose [8]. Šių balsų atsiradimui gali būti keletas skirtingų priežasčių, pvz.: balsų atsiranda daugiau, nei iš viso yra balsuojančių asmenų, tai atsiranda dėl balsų klastojimo arba balsavimo ne vieną kartą. Taip pat, tai gali būti sugadinti balsai – kai rinkėjas neatiduoda savo balso nei vienam kandidatui arba atiduoda balsą keletui kandidatų. Kalbant apie visiškai demokratiškus balsavimus, yra labai svarbu užtikrinti, kad neapskaitytų balsų būtų kuo mažiau, kadangi balsų klastojimas atspindi klestinčią korupciją arba demokratijos nebuvimą, o rinkėjo pasirinkimas sugadinti savo balsą gali nulemti rinkimus netikėta linkme, kai bus atspindėta bloga balsavimo baigtis – rezultatas tenkinantis ne daugumos, o mažumos nuomonę.

1.7.2.2. Programavimo klaidos ir klastojimas

Dar vienas labai svarbus požymis, kurį reikia užtikrinti, norint turėti saugią balsavimo sistemą, tai programavimo klaidų nebuvimas ir negalėjimas klastoti balsų. Jau iš anksčiau nagrinėtų e. balsavimo sistemų buvo galima pastebėti, kad jos nėra sukurtos tobulai. Pasitaikydavo, kai balsai nebūdavo užskaitomi arba užskaitomi visiškai kitam kandidatui, taip pat kandidatai gaudavo daugiau balsų, nei iš tiesų rinkėjų už juos balsuodavo. Taigi, labai svarbu yra užtikrinti teisingai veikiančią programinę ir aparatūrinę įrangą, užtikrinant teisingą balsų skaičiavimą, kadangi, iš pažiūros nedidelės klaidos gali nulemti rinkimus klaidinga baigtimi.

Taip pat, yra labai svarbu užtikrinti, kad balsuotojai arba pašaliniai asmenys negalėtų paveikti balsavimo sistemų ir klastoti balsų. Nors su ankstyvosiomis elektroninio balsavimo sistemomis buvo į tai atsižvelgiama ir bandoma šią problemą spręsti sertifikuojant pagamintus, rinkimams skirtus aparatus, atliekant įvairius testavimus. Tačiau tai neužtikrina, kad rinkimų dieną ir rinkimų vietoje bus tie patys aparatai, kurie buvo pilnai ištestuoti ir sertifikuoti. [7] Reiktų atsižvelgti ir į tai, kad dažniausiai visi testavimai yra slepiami, t. y., visiškai nėra galimybės sužinoti, kokie testai ir kaip buvo atliekami. Tai gali reikšti, kad programinis kodas nėra tikrinamas nuodugniai, o aparatinė įranga patikrinama atliekant elementarius, kratymo, atsparumo karščiui, daužymo veiksmus. Nors tai gali padėti atrasti elementarias klaidas, tačiau tai visiškai nesuteikia galimybės užkirsti kelią neprognozuojamiems įvykiams [7].

1.7.2.3. Atstatymo galimybė

Elektroninio balsavimo sistemos turi ne tik būti atsparios įvairioms grėsmėms, bet ir turi būti numatyta situacija, kai sistema yra pažeidžiama ir ji turi savarankiškai atsistatyti. Tokios sistemos yra vadinamos atspariomis sistemomis. Tai reiškia, kad pažeidus sistemą, ji turi suprasti, kad buvo pažeista, apsisaugoti nuo to, sugrįžti į pradinę būseną ir tęsti darbą. Taip pat, turi būti numatyta galimybė atstatyti prarastus balsus. Nenumatant tokios galimybės tektų pakartoti rinkimus, o tai sumenkintų naudojamą elektroninę balsavimo sistemą, taip pat, sunaudotų daug papildomų kaštų, sukeltų nepatogumus ne tik kandidatams, rinkimų komisijai, bet ir patiems rinkėjams, tikėtina, kartojant rinkimus, sumažėtų ir rinkėjų, dalyvaujančių rinkimuose skaičius, mažėtų rinkėjų pasitikėjimas rinkimų sistema [9].

1.7.2.4. Patvirtinimo galimybė

Nepriklausomai nuo anksčiau aptartų kriterijų, dar vienas nemažiau svarbus kriterijus yra galimybė patvirtinti. Tai reiškia, kad kiekvienas asmuo turi turėti galimybę matyti ar jo balsas buvo suskaičiuotas tinkamai, t. y., ar tikrai buvo priskirtas tam kandidatui, kurį rinkėjas rinkosi. Jeigu yra pastebima klaida, balsuotojas turi turėti galimybę atlikti pakeitimus, taip priskirdamas savo balsą reikiamam kandidatui [9].

1.7.2.5. Keletas bendresnių kriterijų

Demokratijos užtikrinimas – elektroninės balsavimo sistemos turi užtikrinti, kad balsuoti bus galima tik už tikrus kandidatus, kurie turi teisę dalyvauti rinkimuose. Taip pat, balsai turi būti priimami tik iš asmenų, turinčių teisę balsuoti. Nevertėtų pamiršti, kad kiekvienas rinkėjas turi turėti galimybę atiduoti savo balsą tik vieną kartą. [9]

E. balsavimo sistemos, kaip jau buvo kalbėta, užtikrina patogumą rinkėjams. Tai neturėtų būti pamiršta ir toliau plėtojama. Balsavimas turi būti atliekamas greitai ir nereikalaujantis jokių papildomų, nestandartinių žinių iš balsuotojų, taip suteikiant galimybę balsuoti visiems rinkėjams, turintiems tam teisę, nepriklausomai nuo amžiaus ar turimų kompiuterinių žinių [9].

Dar vienas kriterijus, labai glaudžiai susijęs su aptartu anksčiau – mobilumas. Tai reiškia, kad rinkimai neturi būti pririšti prie vienos vietos. Rinkėjai turi galėti atlikti balsavimą jiems patogioje vietoje, kur yra internetinis ryšys [9].

1.7.3. Apsisaugojimo nuo pasitaikančių grėsmių pasiūlymai

Naudodamiesi kompiuterinėmis sistemomis naudotojai retai susimąsto apie saugumą ir įvairias grėsmes. Todėl prieš diegiant ir pradedant naudotis elektroninėmis balsavimo sistemomis, didelis dėmesys turi būti skiriamas rinkėjų švietimui apie galimas grėsmes ir galimybes, kaip nuo jų apsisaugoti, taip užtikrinant teisingus ir teisėtus, demokratiškus rinkimus. Keletas pasiūlymų, kurie galėtų padėti apsisaugoti nuo pačių populiariausių grėsmių pateikti toliau.

- Apsisaugojimas nuo žvejojimo (angl. *phishing*) atakų – bene vienintelis ir veiksmingiausias būdas padėti rinkėjams apsisaugoti nuo socialinės inžinerijos (dar kitaip socialinės žvejybos) (angl. *social phishing*) atakų, yra balsuotojų švietimas. Žinoma, visuomet turi būti atsižvelgiama į naujausius metodus, taip siekiant užkirsti kelią naujiems atakų variantams. Taip pat nereiktų pamiršti ir žvejybos atakos, kai yra klastojamos sistemos – sukuriamos identiškos sistemos, siekiant pavogti naudotojų duomenis. Nuo šio tipo atakos gali padėti apsisaugoti abipusė autentifikacija (naudotojo autentifikacija sistemai ir sistemos autentifikacija naudotojui). [9]
- Apsisaugojimas nuo sistemos vientisumą pažeidžiančių atakų – vienas senai naudojamų būdų – sertifikavimas, programinės įrangos kodo tikrinimas. Žinoma, šie veiksmai turi būti atliekami labai skrupulingai, apsvarstant visus įmanomus ir neįmanomus, žinomus ir nežinomus PĮ (programinės įrangos) pažeidžiamumus. Taip pat informacijos vientisumui užtikrinti gali būti naudojama kriptografija, taip pašalinant galimybę peržiūrėti informaciją tretiesiems, teisės tam neturintiems asmenims. Taip yra užkertamas kelias ne tik peržiūrėti, bet ir pakeisti keliaujančią informaciją. [9]
- Vienas iš būdų atgrasinti nusikaltėlius nuo atakų vykdymo – teisinės sistemos tobulinimas. Turi būti sukuriamos aiškos gairės, kaip turi būti vykdomas ne tik atakuotojų radimas, bet ir kokios bausmės jiems yra skiriamos, kaip traktuojami nusikaltimai informacinėje erdvėje, nusikaltimai prieš kompiuterines sistemas. [9]
- Turi būti tobulinimas internetinis tinklas. Reikia turėti aiškų veiksmų planą, kaip vykdomos paslaugos teikimo stabdymo (angl. *denial of service*) atakos šalinimas, kadangi prevencija prieš jas yra beveik neįmanoma. Taip pat, galima sukurti vadinamas medaus statines (angl. *honey spots*), taip įviliojant nusikaltėlius į spąstus, sutrukdant ne tik atakos įvykdymą, bet ir užtikrinant atakuotojų radimą. [9]

1.7.4. Blokų grandinių naudojimas e. balsavimo sistemose

Dar vienas būdas padidinti elektroninių balsavimo sistemų saugumą yra blokų grandinių technologijos. Šią technologiją galima apibūdinti kaip paskirstytą, nepakeičiamą ir nenuginčijamą viešą knygą (angl. *public ledger*). Blokų grandinių technologija turi keturis pagrindinius aspektus:

- viešoji knyga, nėra saugoma vienoje vietoje, ji saugoma keliose skirtingose vietose, todėl dingsta vieno taško (angl. *single point of failure*) saugumo grėsmė [10].
- Egzistuoja kontrolė, kuri yra paskirstyta ir užtikrina, kas gali atlikti naujus sandorius viešojoje knygoje [10].
- Kiekvienas naujas blokas tinkle yra glaudžiai susijęs su prieš tai buvusiu, taip sukuriant nekintantį tinklą ir užtikrinant negalėjimą klastoti buvusių transakcijų, užtikrinamas anksčiau vykdytų sandorių vientisumas [10].
- Prieš pridedant naują bloką į jau egzistuojantį tinklą, didžioji dalis mazgų (angl. *nodes*) turi priimti bendrą susitarimą [10].

Plačiau blokų grandinių technologija aprašyta 1.8 skyriuje.

1.8. Blokų grandinių technologijų, metodų ir karkasų analizė

Šiame skyriuje bus trumpai apžvelgta blokų grandinių technologija, metodai bei populiariausi karkasai, naudojami kuriant sistemas, paremtas blokų grandinių technologijomis.

1.8.1. Blokų grandinių technologijos

Kaip jau buvo minėta anksčiau, blokų grandinės – tai paskirstyta, nepakeičiama ir nenuginčijama vieša knyga. Kalbant šiek tiek detaliau – blokų grandinė susideda iš duomenų rinkinių, dar vadinamų blokais, kurie sujungti į bendrą grandinę. Blokas vaizduoja keletą transakcijų. Kaip buvo galima suprasti, blokų grandinė susideda iš daugybės blokų, taip sukuriant pilną visų transakcijų istoriją, t. y. – transakcijų knygą. Kiekvienas blokas turi būti patvirtintas, tai atliekama naudojant kriptografinės priemonės. [11]

Vertėtų paminėti, kad kiekvienas blokas susideda iš laiko žymės (angl. *timestamp*), praeito bloko maišos vertės (angl. *hash value*) ir atsitiktinio skaičiaus (angl. *nonce*), kuris naudojamas maišos funkcijai patikrinti [11], [12]. Būtent maišos funkcijos ir padeda užtikrinti blokų grandinių vientisumą, kadangi kiekvieno sekančio bloko maišos vertė yra unikali, tai reiškia, kad pakeitus vieną iš blokų, tai iš karto būtų pastebėta, nes maišos reikšmė neatitiktų. Taip pat svarbu suprasti, kad norint, jog blokas būtų pridedamas prie grandinės, bloko transakciją turi patvirtinti didžioji dalis mazgų, o pats blokas, kuriame yra transakcija, turi taip pat būti patvirtinamas. [11]

Galima išskirti du pagrindinius blokų patvirtinimo metodus, kuriais remiantis paskirstytas tinklas sutinka arba ne, pridėti naują bloką prie grandinės – darbo įrodymas (angl. *proof of work*) ir statymo įrodymas (angl. *proof of stake*) [13].

- Darbo įrodymas – mazgai (naudotojų įrenginiai) įrodo, kad paskyrė savo skaičiavimo resursus ir atliko darbą. T. y., mazgai skaičiuoja maišos funkcijas, kai randama tinkama maišos funkcija, ji perduodama į tinklą, o naujas blokas yra pridedamas prie grandinės [14]. Už atliktą darbą, mazgai gauna atlygius – dažniausiai kriptovaliutos forma.
- Statymo įrodymas – šiuo metodu tvirtinant blokus, reikia mažiau skaičiavimo resursų. Kiekvienas kriptovaliutos turėtojas, siūlo savo kriptovaliutas, kaip užstatą už galimybę tvirtinti blokus. Šie naudotojai vadinami validatoriais (angl. *validators*). Validatoriai kasti blokui išrenkami atsitiktinai, priešingai nei darbo įrodymo metode, kur yra remiamasi varžymusi – kas greičiau iškas bloką. Blokai tvirtinami kelių skirtingų validatorių ir kai pasiekiamas reikiamas patvirtinimų skaičius, blokas pridedamas prie grandinės. [15]

1.8.2. Blokų grandinių privalumai

Aptarus blokų grandinių technologiją, svarbu išskirti pagrindinius blokų grandinių privalumus, kurie yra:

- patikimumas – du subjektai turi pilną transakcijos kontrolę, tam nereikia jokių trečiųjų šalių, todėl transakcijos vykdymas tampa labai saugus [16].
- Vientisumas – transakcijos vientisumas priklauso nuo protokolo ir yra vykdomos tiksliai taip, kaip yra aprašytos [16].
- Skaidrumas – pakeitimai blokų grandinėje yra vieši ir visiems matomi, todėl bet kokie nepageidaujami pakeitimai gali būti aiškiai matomi ir, esant reikalui, atstatyti į pradinę būseną [16].
- Teisingi duomenys – duomenys blokų grandinėje yra vientisi, nuoseklūs ir nekintantys [16].
- Tvirtumas – blokų grandinės naudoja decentralizuotą tinklą. Tai leidžia užkirsti kelią vieno taško (angl. *central point*) klaidoms ir užkerta kelią atakoms [16].

1.8.3. Blokų grandinių sunkumai

Kaip ir visos naujos technologijos, taip ir blokų grandinių technologija turi keletą problemų (sunkumų), kuriuos dar reikia išspręsti. Vienos iš pagrindinių – tai transakcijų įvykdymo greitis, limituota informacijos vieta kiekviename bloke. Taip pat, priklausomai nuo naudojamo metodo, patvirtinimo veiksmai gali reikalauti didelio kiekio resursų ir energijos. Vertėtų paminėti, kad nors visa informacija yra užšifruota, tačiau gali pasitaikyti, kad naudojamas nesaugus šifravimo metodas, o tai gali lemti informacijos atskleidimą [16].

Dėl technologijos naujumo gali kilti papildomų sunkumų ją integruojant. Taip pat ne visos šalys šią technologiją priima, o tai gali kelti problemų jos plėtrai. Nors tai ir saugi technologija, yra žmonių, kurie į ją žvelgia skeptiškai ir dar nesiruošia jos pripažinti. Vis dar vyksta įvairios diskusijos dėl šios technologijos reguliavimo, o tai kelia abejonių, kaip turi būti kuriamos sistemos naudojančios blokų grandinių technologijas. [16] Bene karščiausia šių dienų tema yra kriptovaliutų reguliavimas (kaip žinome, jos naudoja blokų grandinių technologijas).

1.8.4. Blokų grandinių karkasai

Blokų grandinių technologija yra tik bendrinis technologijos pavadinimas. Pažvelgus šiek tiek giliau, egzistuoja daugybė blokų grandinių karkasų, kurie skiriasi savo tikslais ir pritaikymo galimybėmis. Todėl prieš kuriant kokią nors sistemą, svarbu apžvelgti karkasus ir pasirinkti tinkamiausią, norimai sistemai sukurti. Šiame poskyryje bus aptarti keli populiariausi blokų grandinių karkasai (Ethereum, Hyperledger, Corda).

1.8.4.1. Kas yra blokų grandinių karkasas?

Paprasčiausiai blokų grandinių karkasą galima apibūdinti kaip programinės įrangos sprendimą, kuris palengvina blokų grandinėmis paremtos sistemos kūrimą bei diegimą ir reikalauja tik nedidelės dalies pakeitimų [17].

1.8.4.2. Ethereum karkasas

Tai atviro kodo karkasas, kuriuo galima kurti virtualias ir decentralizuotas paslaugas, vadinamas decentralizuotomis programomis (toliau – DApps). Tokios programos veikia remiantis protingais kontraktais (angl. *smart contracts*) [18].

Ethereum virtuali mašina (angl. *Ethereum virtual machine (EVM)*) (toliau – EVM), tai kvazi turingo (angl. *quasi-Turing*) (kvazi – netikras, turingas – talpus) mašina, turinti EMV baido kodą [18]. Šio tipo mašinoje skaičiavimai ribojami dujų (angl. *gas*) mokesčiais. Joje galima vykdyti DApps, kurios yra suprogramuotos įvairiomis programavimo kalbomis. Paprasčiau tariant, tam, kad kiekvienai programavimo kalbai arba programai nereiktų kurti atskiro karkaso, jie visi veikia tame pačiame blokų grandinių tinkle.

Kaip jau buvo minėta, programos kuriamos šiuo karkasu naudoja protingus kontraktus – vykdomąją programą, kurioje aprašytos sąlygos ir taisyklės, pagal kurias atliekamas sandoris tarp dviejų subjektų [19]. Decentralizuotos programos – tai programos, kurios naudoja protingus kontraktus įvairiems tikslams pasiekti.

Svarbu paminėti, kad šio karkaso licencijos tipas gali būti tiek mokamas, tiek nemokamas.

1.8.4.3. Hyperledger karkasas

Hyperledger – tai atviro kodo technologija, kurią palaiko IBM ir Linux Foundation. Tai visame pasaulyje žinoma iniciatyva, apimanti bankininkystės, finansų, gamybos, tiekimo grandinės, daiktų interneto ir kitas technologijas [18].

Hyperledger blokų grandinės platformai yra sukurta daug skirtingų karkasų, pvz.: *Fabric* (Java, JavaScript programavimo aplinkos), *Sawtooth* (bet kuri programavimo aplinka), *Burrow* (solidity programavimo aplinka), *Iroha* (C++ programavimo aplinka), *Indy* (Python, Java, C#, node.js programavimo aplinkos) [18].

1.8.4.4. Corda karkasas

Corda blokų grandinių platforma iš pradžių buvo sukurta teisėtiems kontraktams ir kitoms patikintoms organizacijoms dalintis duomenis. Vis dėl to, tai leidžia sukurti daug įvairių programų, kurios veiktų viename tinkle [18]. Corda veikia Java virtualioje mašinoje (angl. *Java virtual machine (JVM)*) ir buvo sukurta R3 konsorciūmo, siekiant saugoti, stebėti ir sinchronizuoti finansinius susitarimus tarp dviejų reguliuojamų finansinių institucijų [18]. Plačiau, R3 konsorciūmas, tai finansinė institucija, vadovaujanti konsorciūmo partnerystei, kurią sudaro daugiau nei 100 pasaulyje pirmaujančių finansų institucijų [20]. Vertėtų paminėti, kad transakcijų informacija nėra viešinama visam tinklui, t. y., informacija yra prieinama tik mazgams, kurie dalyvauja transakcijoje. Pvz.: vykdant transakciją tarp A ir B, jie ir yra vieninteliai mazgai, kurie gaus informaciją [18].

1.9. Blokų grandinių technologijų naudojimo elektroninėse balsavimo sistemose analizė

Nors blokų grandinių technologija yra sąlyginai nauja, tačiau ji yra sulaukusi didelio dėmesio ir jau naudojama daugelyje įvairių sprendimų ir sistemų. Elektroninės balsavimo sistemos nėra išimtis. Taigi šiame skyriuje bus trumpai apžvelgtas blokų grandinių technologijos naudojimas elektroninėse balsavimo sistemose.

1.9.1. Projektai naudojantys blokų grandinių technologiją balsavimo sistemoms

Kaip jau buvo minėta, blokų grandinių technologijos per trumpą laiką sulaukė labai didelio dėmesio ir buvo pradėtos naudoti įvairiose srityse. Žemiau yra pateikta kelių projektų apžvalga, kurie naudoja blokų grandines balsavimui.

1.9.1.1. Luxoft sprendimas

Šis sprendimas sukurtas pritaikyti Zug mieste, Šveicarijoje. Luxoft Harding kompanija siekia sukurti blokų grandinę vyriausybės aljansui ir labiau išreklamuoti bei praplėsti blokų grandinių naudojimą viešose institucijose [21]. Zug miestas jau priima kriptovaliutą kaip apmokėjimo būdą už įvairias paslaugas, taip pat suskaitmenino blokų grandinių sprendimą e. balsavimui, įskaitant pačią platformą, programinę įrangą ir algoritmus, kurie yra sukurti *Hyperledger Fabric* karkaso pagalba. Integravus su Zug miesto Ethereum pagrįsta skaitmenine ID registracijos programa, gyventojai jau gali savo balsus atiduoti blokų grandinėse. Šios kompanijos sprendimas yra patalpintas trijuose skirtinguose debesijos duomenų centruose, taip paskirstyta sistema paskirsto ir saugumą, duomenų praradimo rizikas ir užtikrina sistemos tvirtumą. Duomenų centrai yra paskirstyti geografiškai, du yra Šveicarijoje ir vienas Airijoje. Svarbu paminėti, kad kompanija teigia naudojanti inovatyvią šifravimo technologiją, kuri padeda užtikrinti balsų anonimiškumą, apsaugo nuo suklastojimo ir užtikrina saugų auditą. [22]

1.9.1.2. Voatz sprendimas

Voatz kompanijos sukurtame sprendime rinkėjai save identifikuoja biometrinėmis priemonėmis, kas yra skiriamasis parašas, pvz.: pirštų antspaudas arba tinklainės nuskaitymas. Vertėtų paminėti, kad šis sprendimas yra sukurtas mobiliesiems įrenginiams ir užtikrina galimybę balsuoti nuotoliniu būdu, anonimiškumą ir galimybę įsitikinti, kad balsas buvo įskaitytas teisingai [21].

1.9.1.3. Polys programa

Polys yra Kaspersky Lab sprendimas, užtikrinantis saugumą, nekeičiamumą ir anoniminį balsavimą. Šis sprendimas yra skaidrus, kadangi bet kas gali peržiūrėti balsavimą einamuoju laiku internetinėje erdvėje ir stebėti ar nėra jokių pažeidimų. Taip pat suteikia galimybę parsisiųsti visą blokų grandinę ir įsitikinti, kad balsai nebuvo pakeisti, o balsuotojai gali matyti, kad jų balsas yra visiškai anoniminis. Balsavimas vyksta rinkėjui nusiuntus užšifruotą rinkimų biuletenį į blokų grandinę. Tai užtikrina anonimiškumą ir nepakeičiamumą. Skaičiuojant balsus, sistema suskaičiuoja visus balsus, taip pat, tai padaryti gali bet kas ir užtikrinti, kad balsai buvo suskaičiuoti teisingai [23].

1.9.1.4. Public Votes programa

Tai laisvai prieinama, paprasta balsavimo programėlė, kuri naudoja Ethereum blokų grandinę, kas leidžia užtikrinti skaidrią ir sąžiningą balsavimo sistemą. Nors visų rinkėjų balsai yra įrašomi į blokų grandinę, vertėtų paminėti, kad programėlė nėra visiškai decentralizuota. Taip yra todėl, kad buvo siekiama sukurti lengvai naudojamą programėlę žmonėms, kurie nėra susiję su Ethereum. Programėlė sukurta naudojant Meteor platformą su vienu protingu kontraktu, kuris yra skirtas patalpinti balsui į blokų grandinę ir pačiam balso pateikimui. Balsavimą šioje programėlėje gali sukurti bent kas, tik turi susimokėti mokestį Ethereum kriptovaliuta. Sukūrus balsavimą ir persiuntus reikiamą kiekį kriptovaliutos į nurodytą adresą, kontraktas yra įvykdomas ir rinkėjai gali pateikti savo balsus.

Pateikus balsą yra įvykdomas kontraktas ir balsas įrašomas į blokų grandinę, o naudotojas nukreipiamas į kitą puslapį, kuriame mato kaip yra pasiskirstę balsai. [22]

1.9.1.5. Follow My Vote programa

Follow My Vote – dar viena programėlė, skirta balsavimui ir pagrįsta blokų grandinių technologijomis. Tam, kad rinkėjas galėtų balsuoti, jam reikia parsisiųsti programėlę (programėlė yra sukurta tiek kompiuteriams, tiek telefonams ar planšetiniams kompiuteriams). Tuomet naudotojas turi pateikti identifikacinę informaciją, kurią patvirtina rinkimus organizuojantys asmenys. Patvirtinęs tapatybę, rinkėjas gauna rinkimų lapelį (biuletenį), kurį užpildęs pateikia ir taip nusiunčia į „rinkimų dėžę“ – blokų grandinę. Priklausomai nuo rinkimų organizatoriaus, rinkėjams gali būti suteikta galimybė balsuoti iš anksto arba pakeisti savo balsą, jei jie persigalvojo. Taip pat kiekvienas rinkėjas turi galimybę sekti savo balsą ir įsitikinti, kad jis įskaitytas teisingai. Vertėtų paminėti, kad balsų anonimiškumas yra garantuojamas [21] [24].

1.10. Estų balsavimo sistemos pavyzdys

Kalbant apie elektroninio balsavimo sistemas, vertėtų nepamiršti aptarti ir kaimynų estų garsiosios elektroninio balsavimo sistemos. Kaip žinoma, Estijoje elektroninis balsavimas yra naudojamas jau nuo 2005 metų, pagrindinės priežastys, kodėl tai yra įmanoma [25]:

- sukurtas teisinis pagrindas, leidžiantis naudoti skaitmeninį parašą;
- dauguma žmonių turi tapatybės korteles ar pasus, kurie suteikia galimybę saugiai identifikotis ir savyje turi skaitmeninį parašą, naudojamą rinkimuose.

Norint sėkmingai įvykdyti rinkimus, tam reikia pasiruošti, t. y., turi būti parengti rinkėjų ir kandidatų sąrašai. Būtina paminėti, kad elektroniniu būdu pateikti balsai yra skaičiuojami atskirai ir tik vėliau sumuojami su popieriniu būdu pateiktais balsais. Būtina atsiminti, kad to paties žmogaus elektroninis ir popierinis balsai negali būti skaičiuojami du kartus, tai privalo būti skaičiuojama kaip vienas balsas.

Estijoje elektroninis balsavimas trunka septynias dienas ir prasideda likus dešimt dienų iki rinkimų dienos. Skaitmeniniam parašui naudojamas asmens dokumentas (angl. *ID card*), mobilusis identifikatorius (angl. *Mobile-ID*) arba skaitmeninis asmens dokumentas (angl. *Digi-ID*). Nuo 2015 metų rinkimų organizatoriai turi užtikrinti galimybę balsuotojams pasitikrinti pateikto balso vientisumą [25].

1.10.1. Estų nacionalinės asmens tapatybės kortelės

Estų nacionalinės asmens tapatybės kortelės visuomenei buvo pristatytos 2002 metais. Tai privalomas tapatybės dokumentas, kuris suteikiamas visiems Estijos piliečiams ir nuolatiniais gyventojams nuo 15 metų. Dokumente yra nurodyti asmens duomenys: vardas, pavardė, lytis, asmens kodas, gimimo data, pilietybė, kortelės numeris, kortelės galiojimo data ir asmens nuotrauka. [26]

Aptariamai temai mus labiau domina informacija, kuri yra saugoma kortelėje integruotame luste. Šiame luste saugoma skaitmeninė, ant kortelės pateikta informacija, dvi 2048 bitų RSA raktų poros ir šių raktų sertifikatas [26]. Pirmoji raktų pora naudojama autentifikavimui ir sertifikatas susieja piliečio viešąjį raktą su jo vardu, asmens kodu ir vyriausybės išduotu elektroninio pašto adresu [26].

Antroji raktų pora naudojama skaitmeniniam pasirašymui ir sertifikatas susieja piliečio viešąjį raktą su jo vardu ir asmens kodu [26].

Kartu su asmens dokumentu piliečiams išduodami trys skirtingi kodai (PIN). Pirmasis kodas yra naudojamas norint autentifikuotis, antrasis – naudojant skaitmeninį parašą. Trečiasis kodas (PIN PUK) naudojamas jeigu pirmasis arba antrasis kodas buvo suvestas neteisingai tris kartus, norint atrakinti kortelę, šis kodas yra ilgesnis nei pirmasis ar antrasis. Tapatybės kortelės galioja penkerius metus, kadangi praėjus šiam laikotarpiui, sertifikatai tampa negaliojančiais. [26]

Piliečiams ir nuolatiniais gyventojams taip pat gali būti išduodami kitokio tipo skaitmeniniai identifikatoriai: digi-ID ir mobiil-ID. Digi-ID yra panaši kortelė į tapatybės kortelę, tačiau ji skirta tik internetiniam naudojimui, taip pat ant jos nėra spausdintos nuotraukos ir joje pateikiama mažiau asmeninės informacijos, tačiau ji vis tiek užtikrina autentifikacijos ir skaitmeninio parašo funkcionalumą. Nuo 2014 metų šią kortelę gali įsigyti ne tik nuolatiniai Estijos gyventojai. Tai suteikia ne Estijos gyventojams galimybę naudotis Estijos autentifikacijos ir skaitmeninio parašo funkcijomis internete. Mobiil-ID teikia panašų funkcionalumą kaip ir prieš tai aptarta kortelė, tačiau ši yra integruota į telefono SIM kortelę. Tai suteikia galimybę gyventojams autentifikuotis ir naudotis skaitmeniniu parašu naudojantis savo telefonu, be jokios papildomos įrangos. [26]

1.10.2. Internetinio balsavimo sistema

Estijos elektroninio balsavimo sistema naudoja gerai žinomą viešojo rakto kriptografijos koncepciją [26]. Paprastai tariant, elektroninis balsavimas dažniausiai naudoja vadinamą voko schemą (angl. *Envelope Scheme*). Toks pavadinimas ir principas yra kilę iš įprasto balsavimo, t. y., rinkėjo anoniminis balsas yra įdedamas į voką, o šis patalpinamas į dar vieną, išorinį, voką, kartu su rinkėjo vardu ir parašu. Elektroniniu būdu tai realizuojama labai panašiai – balsuotojas užšifruoja balsą ir kompiuterio atsitiktinai sugeneruotą skaičių, specialiu, rinkimams skirtu raktu, taip yra suformuojamas pirmasis vokas. Tuomet pasirašomas užšifruotas balsas, naudojant skaitmeninį parašą, tokiu principu sukuriamas antrasis, išorinis, vokas. [25] Visi vokai surenkami ir išrūšiuojami, taip pat patikrinama balsuotojų teisė balsuoti. Surandami visi pasikartojantys balsai (t. y., asmens kuris balsavo tiek elektroniniu, tiek popieriniu būdu). Kaip jau buvo minėta, balsai yra išrūšiuojami pagal rinkimų apylinkes, tuomet yra pašalinami skaitmeniniai parašai. Balsų skaičiavimo metu, anoniminiai ir sumaišyti balsai yra iššifruojami specialiu, rinkimams skirtu privačiuoju raktu.

Vertėtų paminėti, kad sistema nenaudoja įvairių sudėtingų technologijų, siekiant užtikrinti rinkėjo privatumą, priešingai, jie naudoja paprastą funkcijų atskyrimą. Tokiu principu nėra jokios aparatinės įrangos arba naudotojo, kuris vienu metu turėtų serverio privatumą ir balsavimo biuletenį su prisegtu skaitmeniniu parašu. Taip pat visi komponentai kuria audito žurnalus (angl. *audit log*). [26]

1.11. Analizės dalies išvados

1. Tradicinis popierinis balsavimas negarantuoja saugaus ir nesuklastoto balsavimo. Kyla grėsmė kandidatų ar rinkėjų sąrašų klastojimui, balsavimo procese atsiranda galimybė pažeisti balsadėžę (sugadinti antspaudą, papildyti balsadėžę netikrais balsais).

2. Dabartinės naudojamos elektroninio balsavimo sistemos turi didelių saugumo spragų. Balsuotojų kompiuteriai gali būti pažeisti, dėl to gali būti klastojami rinkimų rezultatai, pažeidžiamas asmens privatumas (balsas gali tapti neanoniminiu, ko yra reikalaujama).

3. Elektroninio balsavimo sistemos turi užtikrinti keturis pagrindinius principus – skaidrumą, privatumą, anonimiškumą, vientisumą.

4. Siūlomas sprendimas – blokų grandinių naudojimas elektroninio balsavimo sistemoje užtikrintų rinkėjų anonimiškumą (neliktų galimybės susieti konkretaus balso su konkrečiu, atviru tekstu, matomu rinkėju), užtikrintų skaidrumą (kiekvienas rinkėjas turėtų galimybę matyti, kur nukeliavo jo balsas ir ar jis buvo teisingai priskaičiuotas), užtikrintų vientisumą (blokų grandinės yra decentralizuotas tinklas, tai užkerta kelią jų pažeidimui ir balsų pakeitimui).

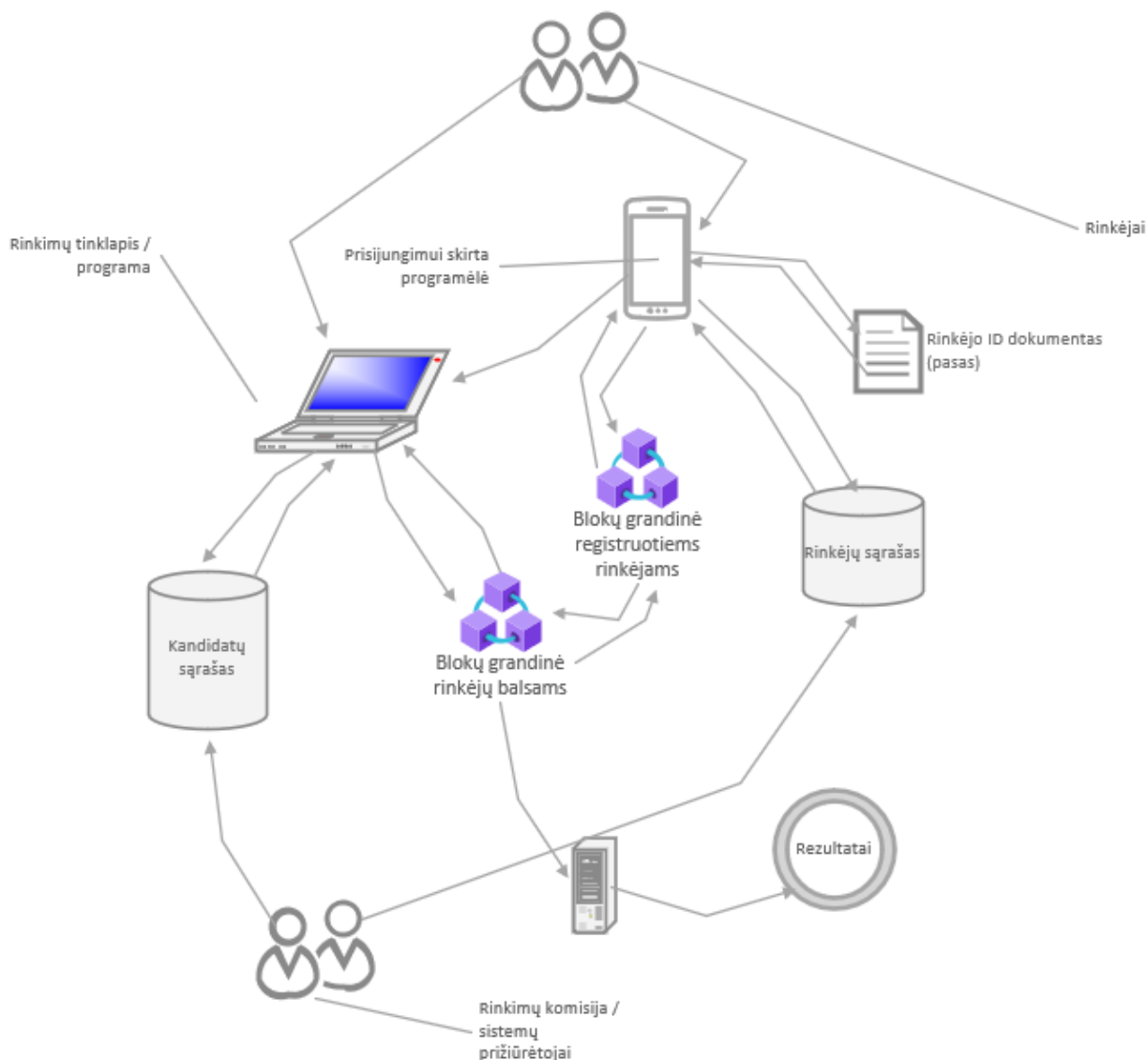
2. Elektroninės balsavimo sistemos pagrįstos blokų grandinių technologija architektūra

Šiame skyriuje pateikiama elektroninės balsavimo sistemos, pagrįstos blokų grandinių technologija architektūra. Siūlomas sprendimas užtikrintų tris pagrindinius elektroninėms balsavimo sistemoms keliamus reikalavimus – skaidrumą, privatumą ir anonimiškumą. Kuriamai sistemai nėra taikomas joks anksčiau sukurtas blokų grandinių karkasas. Sprendimui įgyvendinti kuriama nauja blokų grandinė, kuri yra specifiskai pritaikyta elektroniniam balsavimui ir padėsianti užtikrinti anksčiau minėtus elektroninėms balsavimo sistemoms keliamus reikalavimus.

Šis, toliau aprašomas, sprendimas pasirinktas ir sugalvotas siekiant pilnai decentralizuoti sistemą, taip atsisakant vienos duomenų talpyklos. Tai leis užtikrinti, kad duomenys nebūtų pakeičiami ir klastojami, taip pat sumažinti vieno taško klaidos tikimybę. Šis sprendimas užtikrina, kad būtų galima patikrinti duomenų tikrumą. Siūloma bloko grandinės bloko struktūra ir išmanieji kontraktai padės užtikrinti, kad rinkėjas galėtų atiduoti balsą tik vieną kartą, jis būtų nesuklastotas bei suteiks galimybę, esant poreikiui, rinkėjui peržiūrėti ar jo balsas buvo išsaugotas teisingai.

2.1. Vizija

Balsavimo sistemos, pagrįstos blokų grandinių technologija sprendimas vizualizuotas 3 paveiksle (žr. **3 pav.**). Siūlomo sprendimo vizijoje (žr. **3 pav.**) matomi įrenginiai, reikalingi rinkėjui, norinčiam pasinaudoti elektronine balsavimo sistema: asmens dokumentas (pasas), išmanusis telefonas ir / ar kompiuteris.



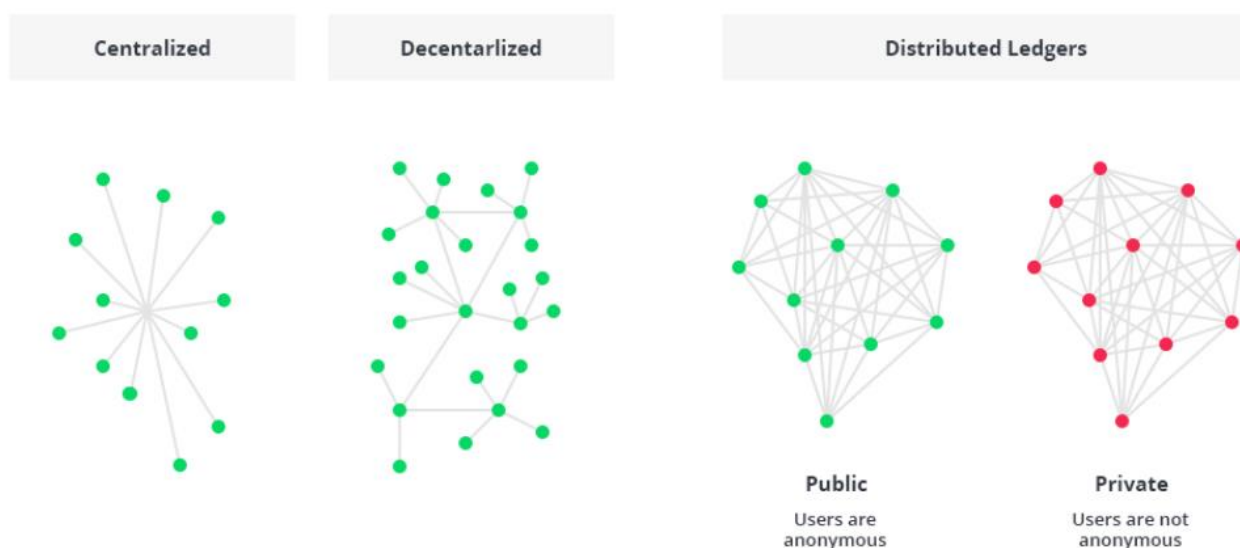
3 pav. Elektroninės balsavimo sistemos pagrįstos blokų grandinių technologija vizija

Naudotojas, norėdamas prisijungti (arba prisiregistruoti prie elektroninės balsavimo sistemos) iš pradžių išmaniuoju telefonu turi nuskaityti savo asmens dokumentą – pasą (taip nustatomas naudotojo vardas, pavardė, asmens kodas ir pirštų antspaudas), tuomet, naudodamasis įrenginyje įmontuotu pirštų antspaudų skaitytuvu nuskaityti savo piršto antspaudą. Nuskaityto piršto antspaudu duomenys elektroniniu būdu lyginami su esančiais asmens tapatybės dokumente, taip užtikrinant, kad prie sistemos jungiasi (arba registruojasi) tikrasis dokumento savininkas. Sistemai patvirtinus duomenis, rinkėjo vardas, pavardė bei asmens kodas tikrinami rinkėjų duomenų bazėje, tokiu būdu tikrinant ar rinkėjas turi teisę balsuoti. Atlikus šiuos veiksmus rinkėjas prijungiamas prie sistemos. Prisijungus prie balsavimo sistemos rinkėjui pateikiamas kandidatų sąrašas (iš VRK pateiktos kandidatų duomenų bazės). Rinkėjas, pasirinkęs kandidatą už kurį nori balsuoti, savo pasirinkimą išsaugo. Rinkėjo balsas yra įrašomas į blokų grandinę, sukuriant naują bloką joje. Pasibaigus balsavimui rezultatai gali būti dar kartą perskaiciuojami (pirmasis skaičiavimas yra vykdomas kuriant naują bloką grandinėje, kadangi kiekviename bloke yra saugomi rinkimų rezultatai einamuoju momentu) ir

pateikiami galutiniai rinkimų rezultatai. Vertėtų paminėti, kad rinkėjų ir kandidatų sąrašai yra paruošiami ir prižiūrimi rinkimų komisijos ir rinkimų sistemų prižiūrėtojų.

2.2. Elektroninės balsavimo sistemos, pagrįstos blokų grandinių technologija tinklo architektūra

Blokų grandinių technologija žymi dėl vienos iš ypatingų savybių – decentralizacijos. Centralizuota sistema yra sistema, kuri turi vieną centrinį serverį iš kurio valdomi visi prijungti mazgai. Decentralizuota paskirstyta sistema, yra tokia sistema, kuri neturi vieno centrinio serverio, o visi sistemos mazgai komunikuoja tarpusavyje. Dėl šios savybės sistema tampa mažiau pažeidžiama, kadangi nutrūkus komunikacijai tarp dviejų ar daugiau mazgų, sistema toliau funkcionuoja, nes komunikacija tarp kitų mazgų vis dar lieka aktyvi. Tačiau tinkamam sistemos įgyvendinimui reikia nemažo mazgų skaičiaus. (žr. 4 pav.)

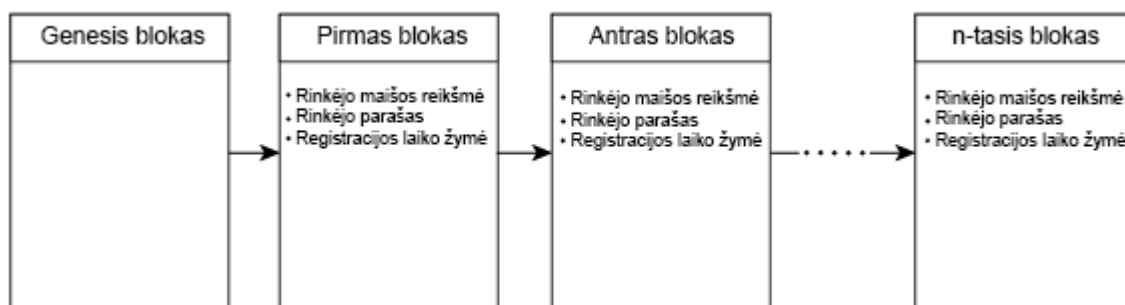


4 pav. Centralizacija, decentralizacija ir paskirstyti duomenys (angl. Centralized, Decentralized, and Distributed Ledger) [27]

Žvelgiant į elektroninio balsavimo sistemą, ji turėtų naudoti paskirstytą domenų technologiją (angl. *Distributed Ledgers Technology*), kadangi tokiu būdu būtų užtikrinamas tinkamas sistemos funkcionavimas bei būtų sumažinama tikimybė prarasti arba sugadinti duomenims, nes naudojant šį būdą duomenys talpinami ne vienoje vietoje, o visuose mazguose.

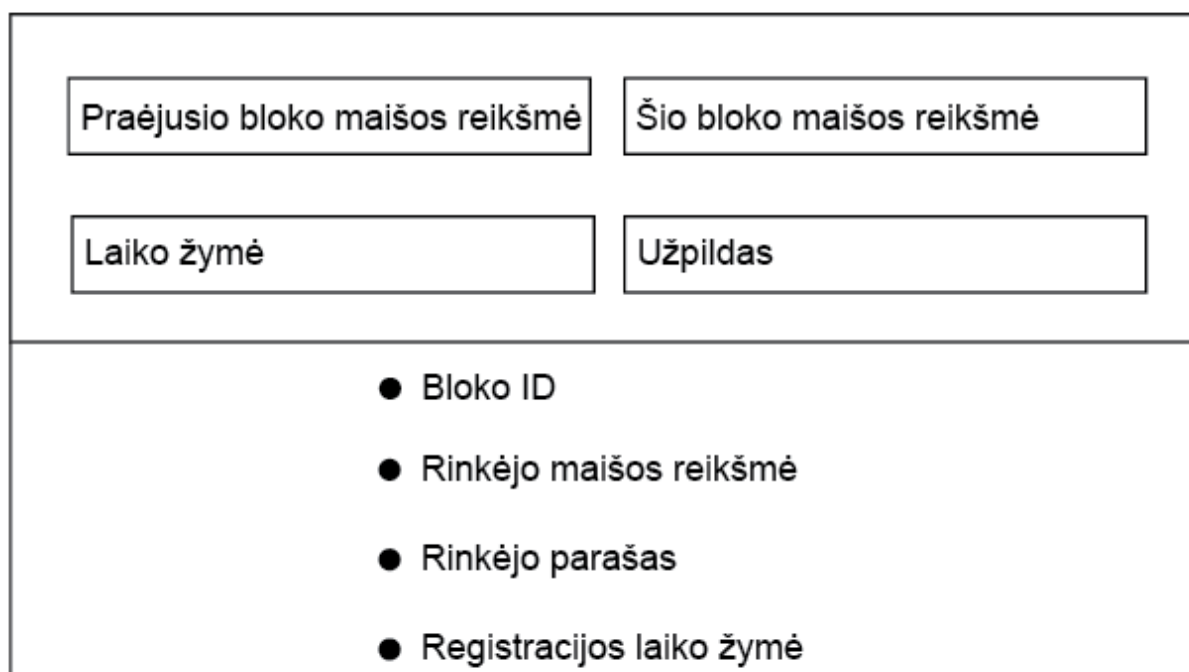
2.3. Elektroninės balsavimo sistemos, pagrįstos blokų grandinių technologijomis blokų grandinių ir blokų schemas

Kalbant apie rinkėjų blokų grandinę, siūlomame sprendime yra numatyta, kad bloke būtų saugomi registruotų naudotojų duomenys, tokie kaip: iš rinkėjo asmens duomenų (vardo, pavardės, asmens kodo, piršto antspauda informacijos) suformuotos maišos reikšmės, rinkėjo parašas bei registracijos laiko žymė. Visi blokai šioje blokų grandinėje yra identiškos struktūros, skiriasi tik juose patalpinti rinkėjų duomenys (žr. 5 pav.).



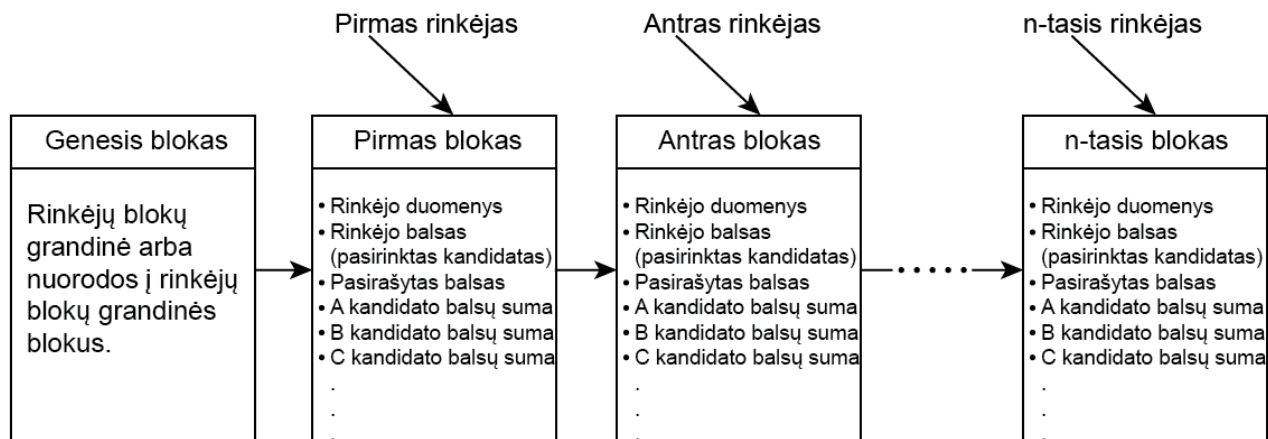
5 pav. Elektroninės balsavimo sistemos registruotų naudotojų blokų grandinės schema

Šios blokų grandinės bloko struktūra pavaizduota **6 pav.** Kaip matoma paveiksle, bloke yra saugomas bloko ID, rinkėjo maišos reikšmė (šios reikšmės saugojimas yra svarbus siekiant užtikrinti, kad rinkėjas savo balsą atiduotų tik vieną kartą), rinkėjo parašas bei registracijos rinkimų sistemoje laiko žyma.



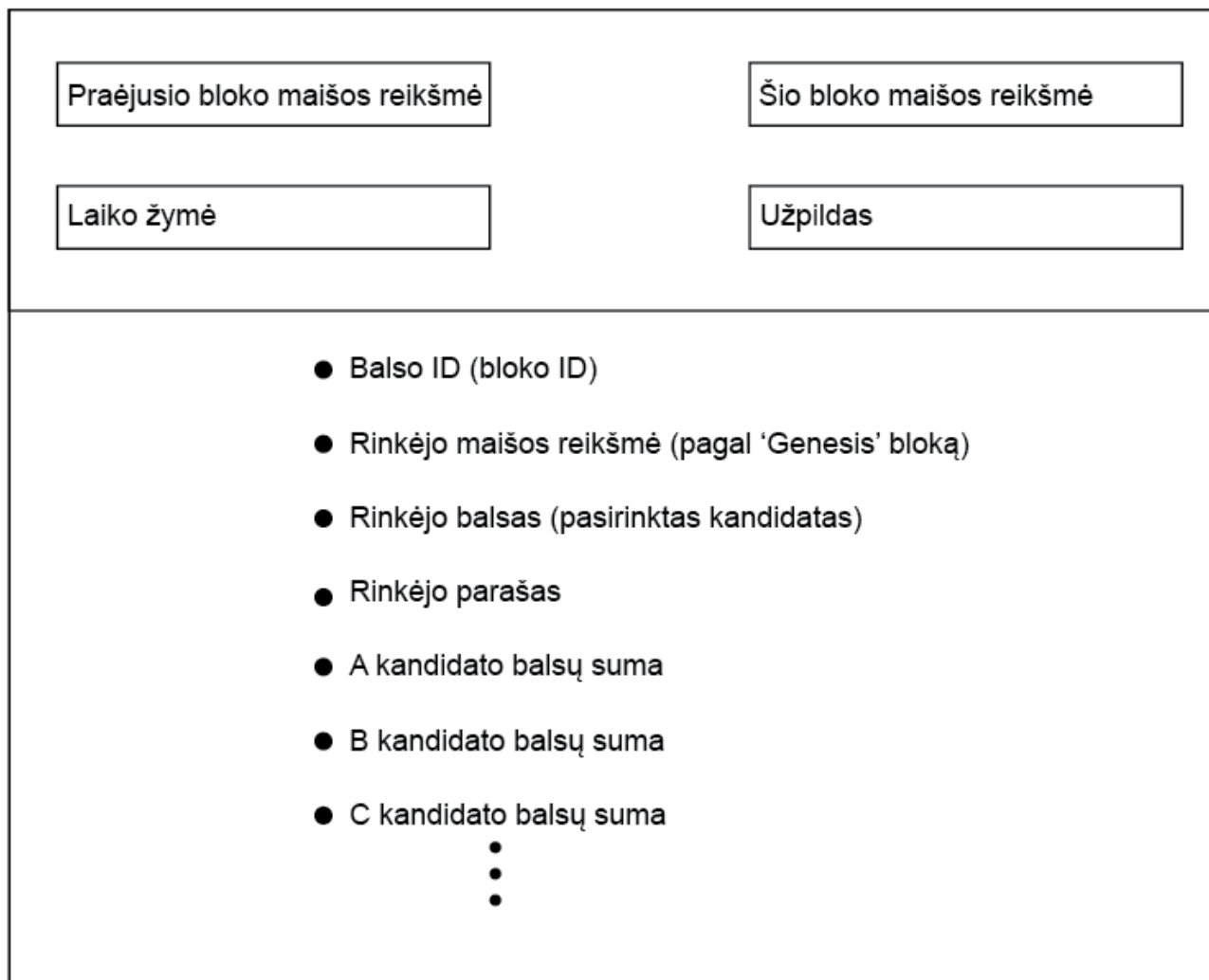
6 pav. Elektroninės balsavimo sistemos registruotų naudotojų blokų grandinės bloko schema

Siūlomo sprendimo balsų blokų grandinėje pirmasis blokas skirtas saugoti rinkėjų blokų grandinei arba nuorodoms į rinkėjų blokų grandinės blokus. Šios nuorodos leidžia greičiau rasti naudotoją registruotų naudotojų blokų grandinėje ir įsitikinti ar naudotojas turi teisę balsuoti bei yra užsiregistravę elektroninėje balsavimo sistemoje iki rinkimų dienos (rinkimų komisijos iš anksto nustatytais terminais). Kiekvienas sekantis blokas yra sudaromas kiekvienam balsui atskirai. Blokų grandinės schema pavaizduota **7 pav.**



7 pav. Elektroninės balsavimo sistemos balsų blokų grandinės schema

Kalbant apie blokų grandinės bloko struktūrą (išskyrus pirmąjį bloką), vertėtų paminėti, kad jame saugomas bloko / balso ID, rinkėjo maišos reikšmė (šios reikšmės saugojimas yra svarbus siekiant užtikrinti, kad rinkėjas savo balsą atiduotų tik vieną kartą bei esant reikalui, bloką būtų galima atvaizduoti rinkėjui, taip leidžiant įsitikinti, kad jo balsas buvo įrašytas teisingai), rinkėjo balsas ir rinkėjo pasirašytas balsas. Taip pat yra kiekvieno kandidato balsų skaičius atskirai, t. y. kuriant kiekvieną naują bloką, šis sąrašas yra atnaujinamas pridėdant naują rinkėjo atiduodamą balsą. Toks sprendimas leidžia pagreitinti balsų skaičiavimo procesą, nes galutiniai rezultatai bus paskutiniame blokų grandinės bloke. Žinoma, kadangi yra saugomi ir atskiri rinkėjų atiduodami balsai, visada galima rinkėjų atiduotus balsus patikrinti – perskaiciuoti ir įsitikinti, kad rezultatų sumos yra teisingos. Bloko struktūra pavaizduota **8 pav.**



8 pav. Elektroninės balsavimo sistemos balsų blokų grandinės bloko schema

2.4. Elektroninės balsavimo sistemos, pagrįstos blokų grandinių technologijomis veiklos diagramos

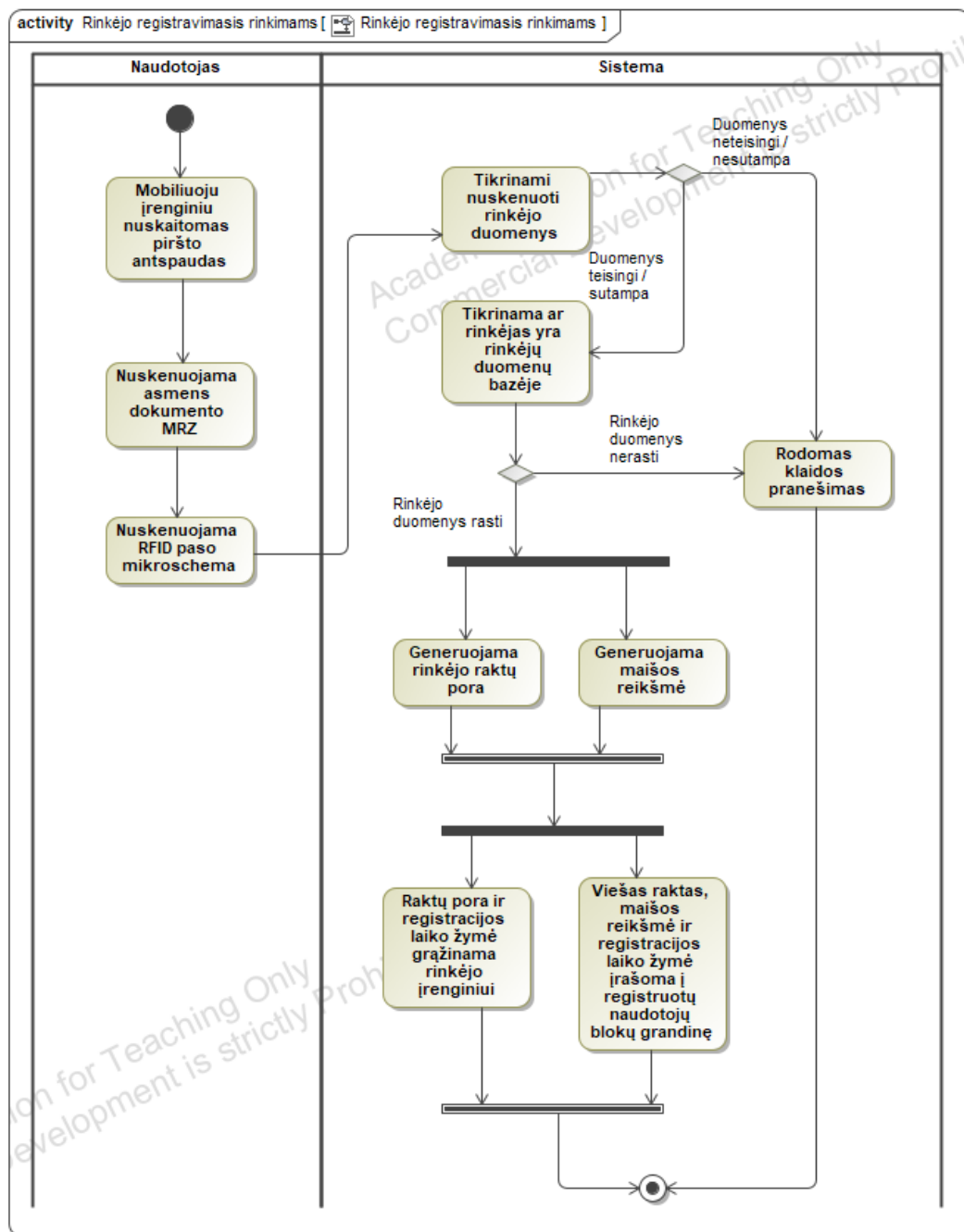
Šiame skyriuje pateikiamos ir aprašomos pagrindinių elektroninės balsavimo sistemos veiksmų veiklos diagramos. Tai leidžia geriau suprasti sistemos ir naudotojo atliekamus veiksmus bei jų įgyvendinimo idėją.

2.4.1. Rinkėjo registracija elektroninėje balsavimo sistemoje

Kaip jau buvo minėta, rinkėjui norint prisiregistruoti elektroninėje sistemoje yra reikalingas išmanusis telefonas, kurio pagalba nuskaitomas asmens tapatybės dokumentas ir asmens, atliekančio registraciją piršto antspaudas. Rinkėjui atlikus šiuos veiksmus sistema patikrina ar asmens, atliekančio registraciją, duomenys asmens dokumente yra teisingi. Jeigu duomenys neteisingi – grąžinamas klaidos pranešimas, jeigu teisingi – sistema tikrina ar asmuo turi teisę balsuoti rinkimuose. Šis patikrinimas vykdomas ieškant rinkėjo vardo, pavardės bei asmens kodo vyriausiosios rinkimų komisijos paruoštoje rinkėjų duomenų bazėje. Jeigu rinkėjo duomenys nėra randami – asmuo, atliekantis registraciją yra informuojamas, kad jis negali dalyvauti rinkimuose. Priešingu atveju – sistema rinkėjui generuoja elektroniniam parašui reikalingas raktų poras bei iš asmens duomenų sugeneruojama maišos reikšmė, kuri įrašoma į registruotų naudotojų blokų grandinę

kartu su registracijos laiko žyma. Taip pat į šį bloką įrašomas ir sugeneruotas rinkėjo viešasis raktas. Pilna raktų pora (viešas ir privatus raktai) bei registracijos laiko žymė yra grąžinami rinkėjui.

Vertėtų paminėti, kad registracija prie elektroninės balsavimo sistemos yra vykdoma iš anksto, o ne rinkimų dieną, vyriausiosios rinkimų komisijos numatytais terminais. (žr. **9 pav.**)

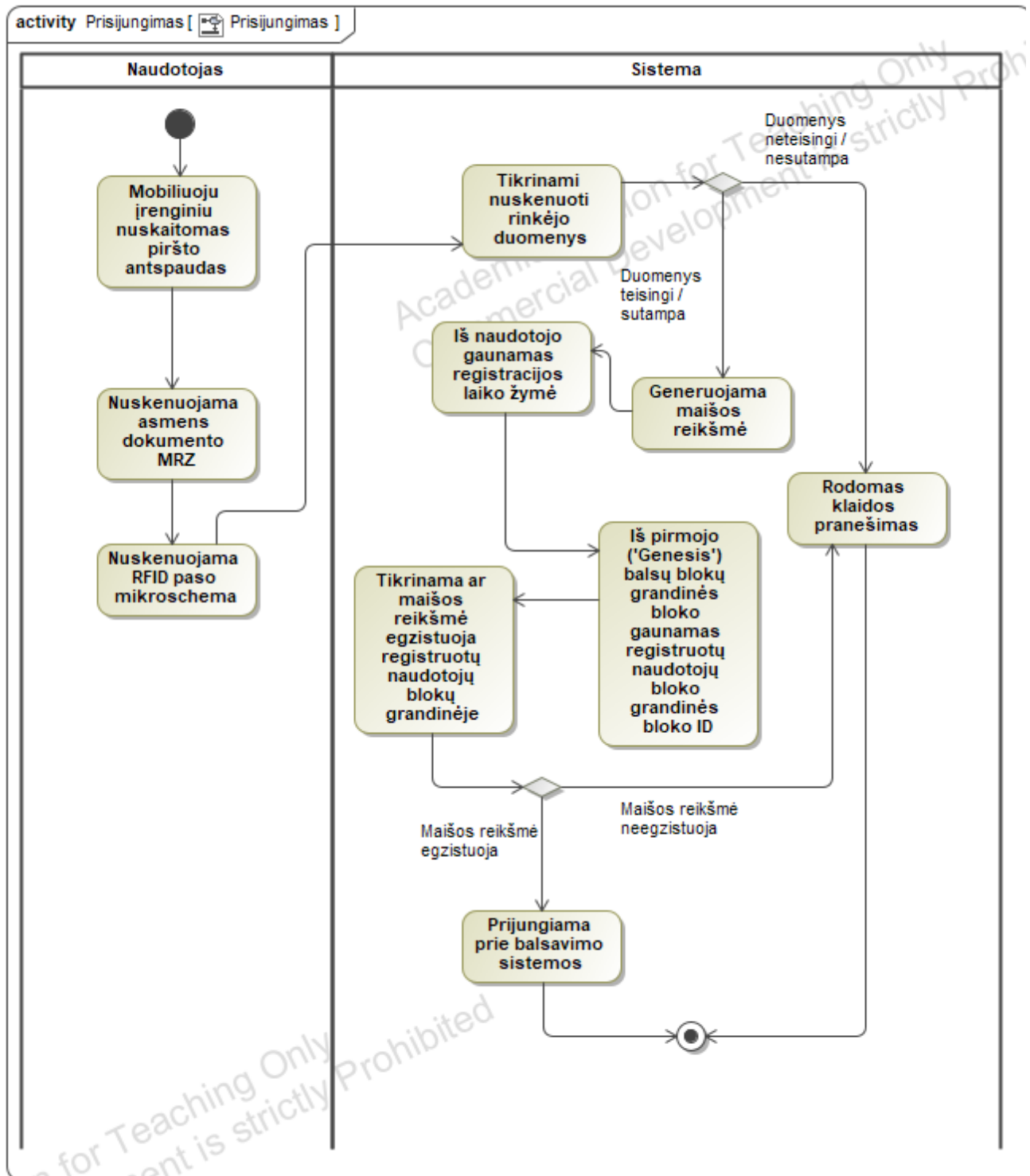


9 pav. Rinkėjo registravimosi elektroninėje balsavimo sistemoje veiklos diagrama

2.4.2. Rinkėjo prisijungimas prie elektroninės balsavimo sistemos

Rinkėjo prisijungimas prie elektroninės balsavimo sistemos vyksta labai panašiai kaip ir registracija. Naudotojas turi nuskaityti savo asmens dokumentą bei piršto antspaudą. Tuomet yra tikrinami rinkėjo duomenys. Jeigu duomenys neteisingi – rodomas klaidos pranešimas, priešingu atveju – iš asmens dokumento nuskaitytos informacijos sugeneruojama maišos reikšmė bei iš

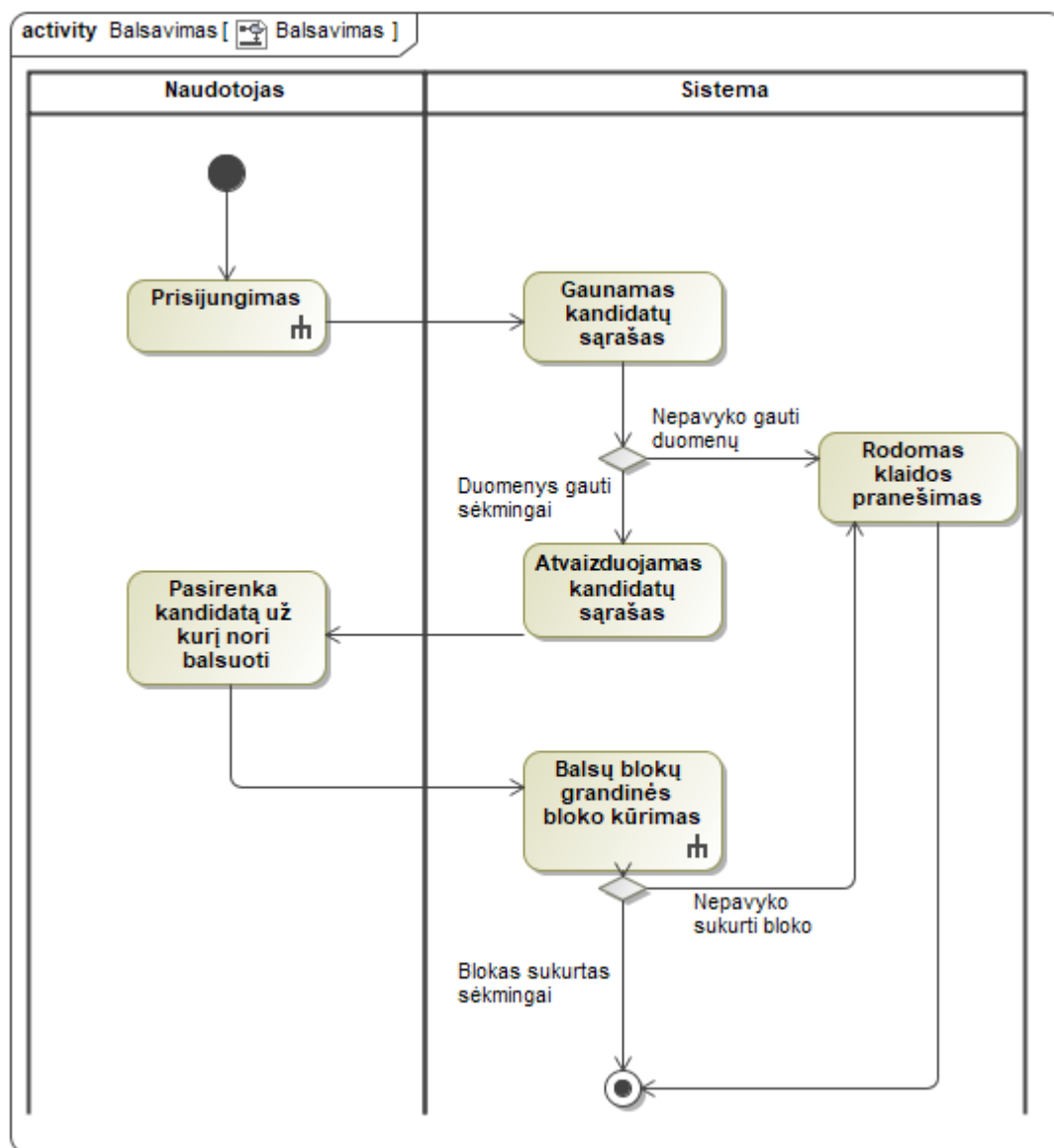
naudotojo gaunama registracijos sistemoje laiko žymė. Iš pirmojo (Genesis) balsų blokų grandinės bloko gaunamas registruotų naudotojų blokų grandinės bloko ID, kuriame reikėtų ieškoti naudotojo. Jeigu maišos reikšmė nėra randama registruotų naudotojų blokų grandinėje – išvedamas pranešimas, kad rinkėjas neturi teisės balsuoti. Jeigu maišos reikšmė randama – atidaromas balsui atiduoti skirtas langas. (žr. 10 pav.)



10 pav. Rinkėjo prisijungimo prie elektroninės balsavimo sistemos veiklos diagrama

2.4.3. Balsavimas elektroninėje balsavimo sistemoje

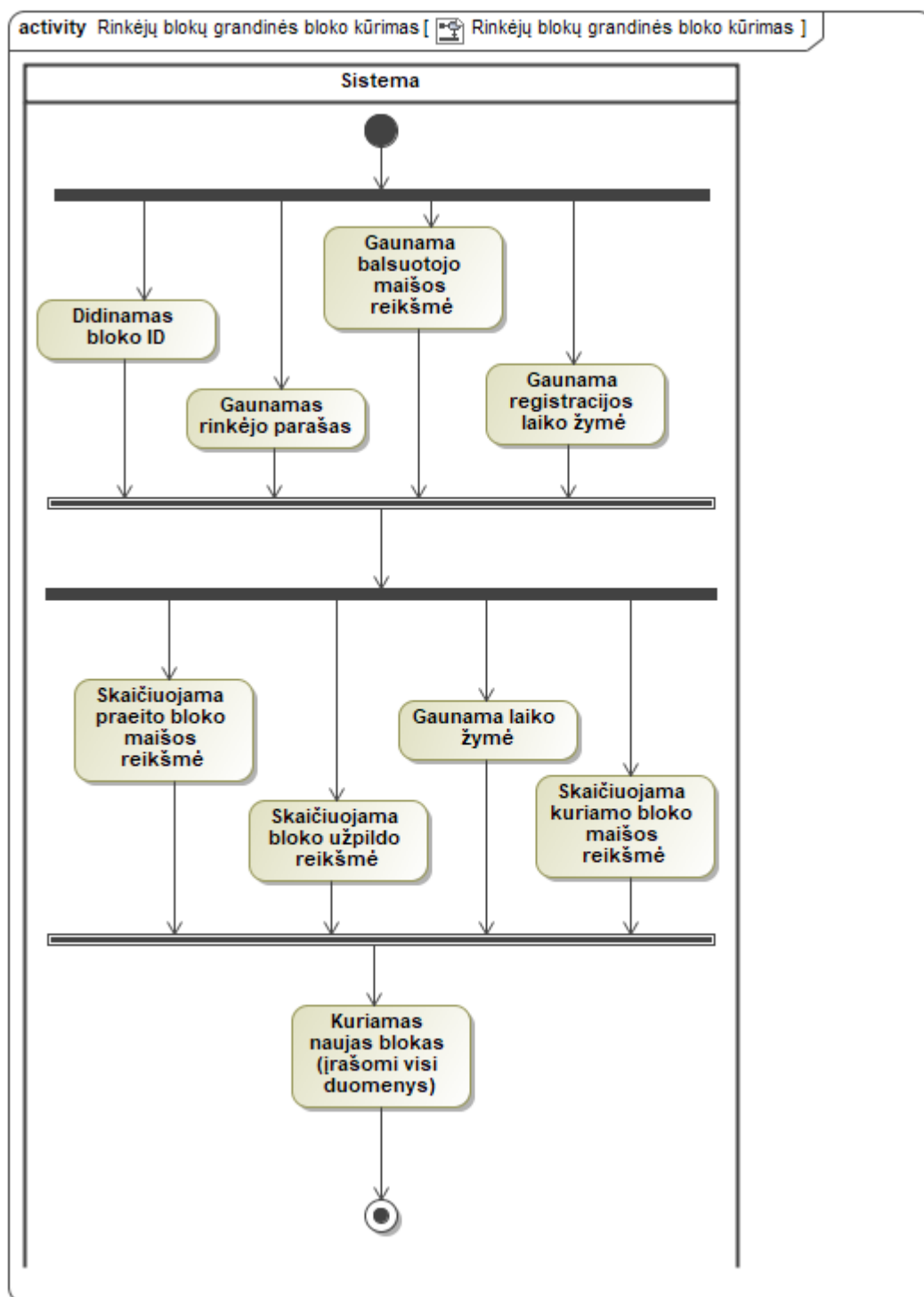
Rinkėjui sėkmingai prisijungus prie elektroninės balsavimo sistemos, sistema iš kandidatų duomenų bazės gauna kandidatų sąrašą, kurį atvaizduoja rinkėjui. Rinkėjas pasirenka kandidatą, kuriam nori atiduoti balsą ir savo pasirinkimą išsaugo. Tuomet sistema kuria naują bloką balsų blokų grandinėje (šis procesas aprašytas 2.4.6 skyrelyje). (žr. 11 pav.)



11 pav. Balsavimo elektroninėje balsavimo sistemoje veiklos diagrama

2.4.4. Rinkėjų bloko grandinės bloko kūrimas elektroninėje balsavimo sistemoje

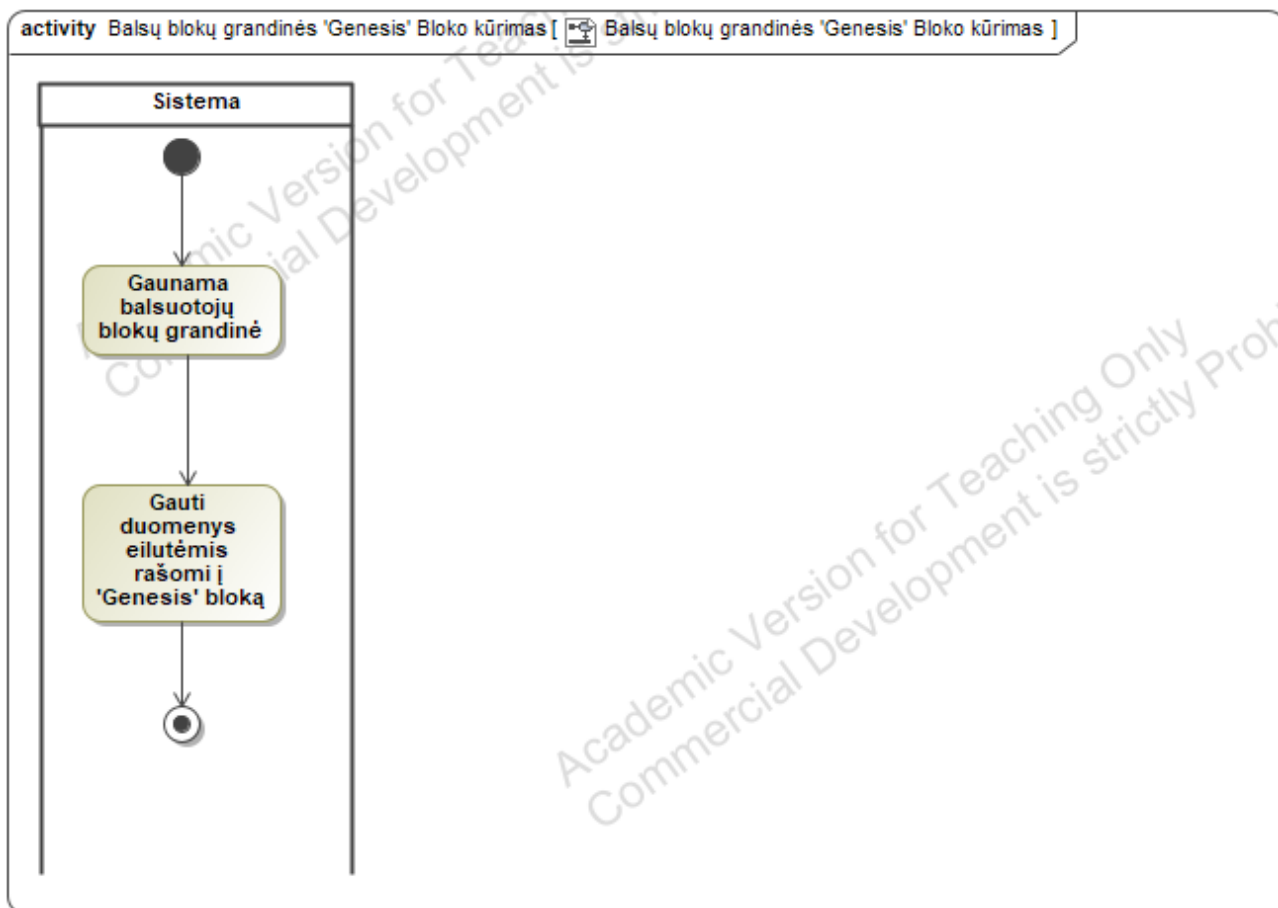
Rinkėjų bloko grandinės bloko kūrimui reikalingi šie duomenys: balsuotojo maišos reikšmė, rinkėjo parašas, registracijos laiko žymė. Iš pradžių sistema padidina bloko ID ir gauna anksčiau paminėtus duomenis. Turint šiuos duomenis, į bloką papildomai yra įtraukiama praėjusio bloko maišos reikšmė, suskaičiuojama bloko užpildo reikšmė, pridedama laiko reikšmė bei suskaičiuojama ir pridedama kuriamo bloko maišos reikšmė. Taip sukuriamas ir pridedamas naujas blokas blokų grandinėje. (žr. 12 pav.) Detalesnė blokų grandinės ir bloko struktūra yra pavaizduota ir aprašyta 2.3 poskyryje.



12 pav. Rinkėjų blokų grandinės bloko kūrimo elektroninėje balsavimo sistemoje veiklos diagrama

2.4.5. Balsų bloko grandinės pirmojo bloko kūrimas

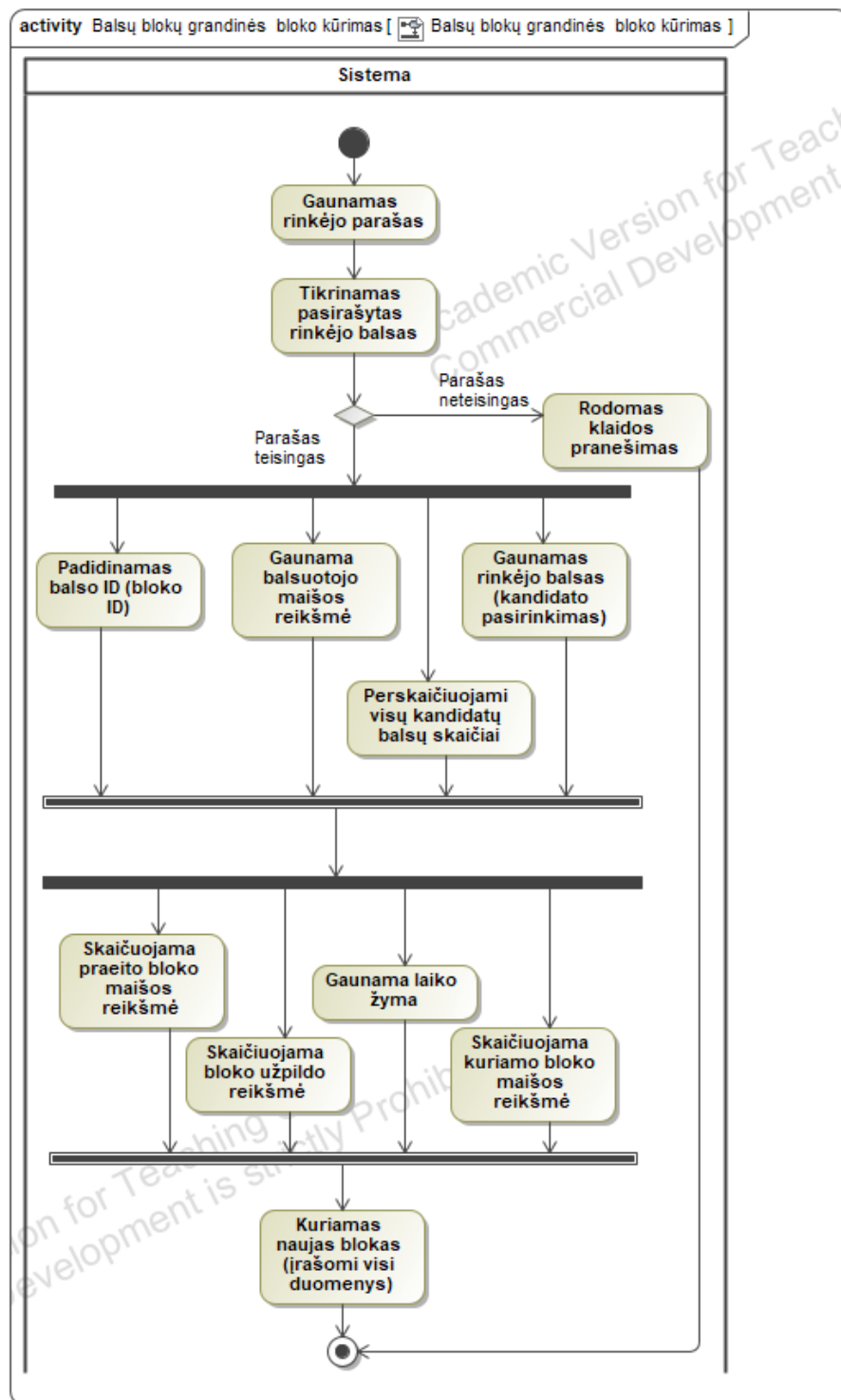
Pirmajame balsų bloko grandinės bloke yra talpinami sistemoje užsiregistravusių rinkėjų blokų grandinės blokų duomenys (arba nuorodos) (veiklos diagrama yra pateikiama 13 pav.).



13 pav. Pirmojo balsų bloko grandinės blokų kūrimo elektroninėje balsavimo sistemoje veiklos diagrama

2.4.6. Balsų bloko grandinės bloko kūrimas elektroninėje balsavimo sistemoje

Bloko kūrimas elektroninėje balsavimo sistemoje atliekamas apdorojant įvairius duomenis. Iš pradžių sistema gauna rinkėjo parašą ir patikrina rinkėjo pasirašytą balsą. Jeigu parašas neatitinka – rodomas klaidos pranešimas, jeigu parašas tinkamas, atliekami sekantys veiksmai: padidinamas bloko / balso ID, gaunama rinkėjo duomenų maišos reikšmė (skirta užtikrinti, kad rinkėjas atiduotų tik vieną balsą), atsižvelgiant į praėjusiame bloke esantį kiekvieno kandidato gautų balsų skaičių, rezultatai yra perskaičiuojami pridedant rinkėjo atiduotą balsą atitinkamam kandidatui, taip pat rinkėjo atiduodamas balsas yra įrašomas atskirai, kad būtų galima dar kartą perskaičiuoti rezultatus, jeigu kiltų įtarimų. Turint šiuos duomenis į bloką papildomai yra įtraukiama praėjusio bloko maišos reikšmė, suskaičiuojama bloko užpildo reikšmė, pridedama laiko reikšmė bei suskaičiuojama ir pridedama kuriamo bloko maišos reikšmė. Taip sukuriamas ir pridedamas naujas blokas blokų grandinėje. (žr. **14 pav.**) Detalesnė blokų grandinės ir bloko struktūra yra pavaizduota ir aprašyta 2.3 poskyryje.

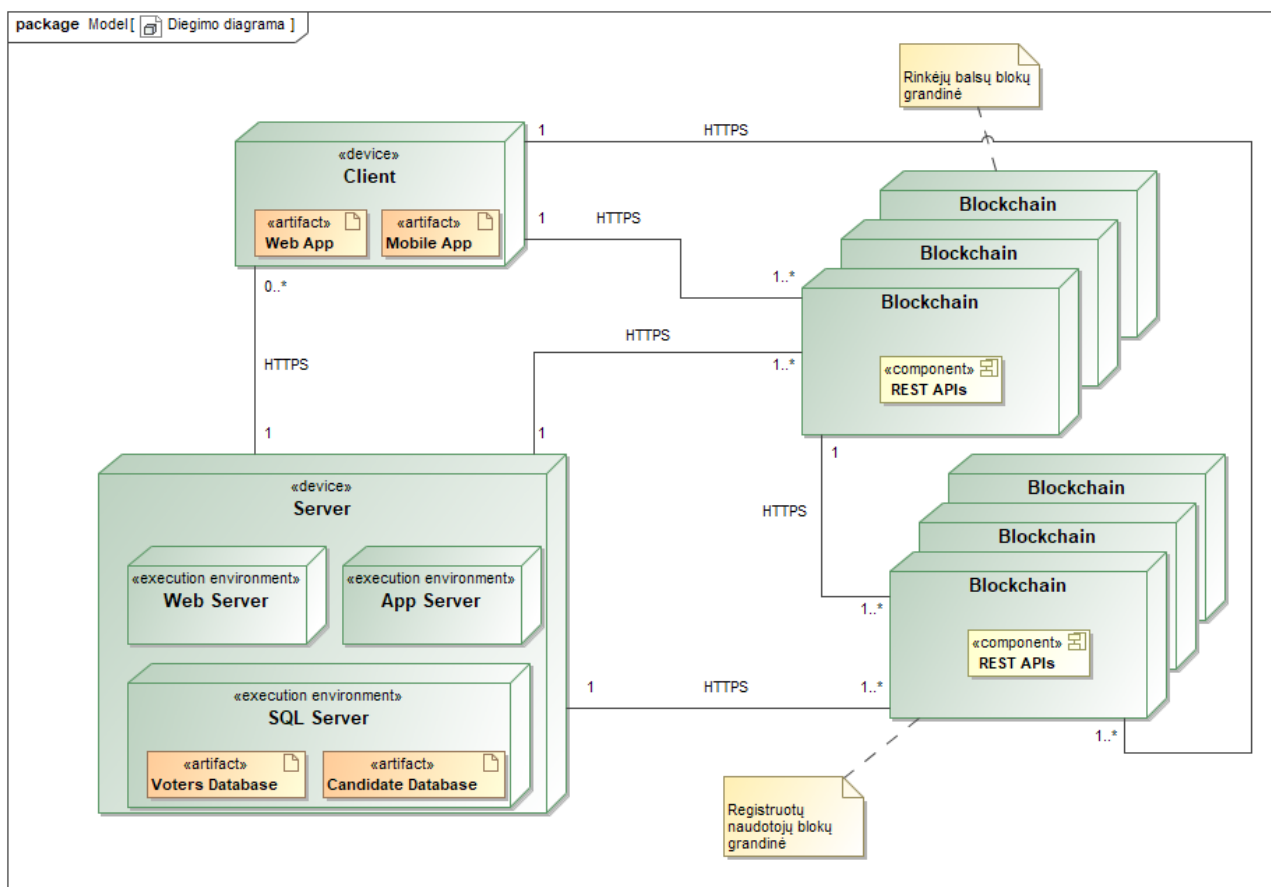


14 pav. Bloko kūrimo elektroninėje balsavimo sistemoje veiklos diagrama

2.5. Elektroninės balsavimo sistemos pagrįstos blokų grandinių technologijomis diegimo diagrama

Siūlomo sprendimo diegimo diagramoje (žr. 15 pav.) galima pastebėti, kad yra reikalingas serveris, kuriame veiktų rinkimų komisijos parengtos ir suformuotos rinkėjų ir kandidatų duomenų bazės. Kliento pusėje – mobilioji programėlė, kuri naudojama registracijai ir prisijungimui prie sistemos bei internetinė aplikacija (tinklapis), kuriuo naudodamasis rinkėjas atiduos balsą už norimą

kandidatą. Taip pat reikalingos dvi decentralizuotos paskirstytos blokų grandinės. Vienoje iš jų yra saugomi rinkėjų balsai ir kandidatų rinkimų rezultatai, kitoje – registruoti naudotojai (registruotų rinkėjų maišos reikšmės suformuotos iš vardo, pavardės, asmens kodo ir biometrinių duomenų).



15 pav. Elektroninės balsavimo sistemos, pagrįstos blokų grandinių technologijomis diegimo diagrama

2.6. Projektavimo dalies išvados

1. Projektuojant elektroninio balsavimo sistemą pastebėta, kad norint pagerinti skaidrumą, privatumą ir anonimiškumą, sistema turi naudoti paskirstytų duomenų technologiją.
2. Siekiant užtikrinti rinkėjų anonimiškumą, projektuojamos dvi atskiros blokų grandinės, pirmoji – nuasmenintiems rinkėjų duomenimis (maišos reikšmėms gautoms iš naudotojų duomenų), antroji – balsų saugojimui (nei vienoje blokų grandinėje nėra saugoma atvira naudotojo informacija).
3. Decentralizuota blokų grandinė padės užtikrinti balsų vientisumą ir nepakeičiamumą.
4. Siekiant sumažinti apsimetimo galimybę, rinkėjas, norėdamas prisijungti ir užsiregistruoti sistemoje turi naudoti mobilųjį telefoną, nuskaitydamas asmens dokumentą bei savo biometrinius duomenis.
5. Siekiant sukurti patikimą ir patogią sistemą buvo projektuojama nauja blokų grandinė, pritaikyta elektroniniam balsavimui.

3. Elektroninės balsavimo sistemos, pagrįstos blokų grandinių technologijomis prototipo realizacija

Pagal atliktą analizę ir parengtą elektroninės balsavimo sistemos, pagrįstos blokų grandinių technologijomis projektą buvo realizuotas šios sistemos prototipas. Šiame skyriuje aprašomos realizacijai naudotos priemonės ir įrankiai, parašytas prototipo programinis kodas (naudotojo sąsajos bei blokų grandinių), pagrindžiama kodėl projektuojama sistema yra saugesnės už naudojamas iki šiol.

3.1. Realizacijai naudotos priemonės

Programinė įranga:

- Visual Studio Code 1.72.0 – projekto kodo rašymui.
- Postman – 9.31.0 – API testavimu.

Programavimo kalbos:

- JavaScript – blokų grandinių ir API programavimui (pagrindinei sistemos logikai).
- Python – automatinių duomenų, skirtų testavimui, generacijai.

Bibliotekos:

- Crypto – biblioteka, skirta šifruotiems duomenims valdyti.
- Discovery-swarm – biblioteka, skirta prisijungti prie mazgų, naudojančių tą patį kanalą.
- Dat-swarm-defaults – biblioteka sukuria serverius, kurie padeda identifikuoti kitus potencialius mazgus.
- Get-port – biblioteka, naudojama laisvam prievadui serveryje rasti.
- Cron – biblioteka, naudojama suplanuotiems darbams vykdyti.
- Express – web karkasas, naudojama API kūrimui ir valdymui.
- Body-parser – biblioteka, leidžianti gauti duomenis iš ateinančios užklauso.
- Moment – biblioteka, kurios pagalba galima manipuluoti datomis.
- Crypto-js – kriptografijos standartų biblioteka.
- Level – biblioteka, skirta *key – value* duomenų bazės kūrimui ir valdymui.

Projekto valdymo priemonės:

- Nodejs – projektui reikalingų bibliotekų valdymas, JavaScript vykdymo aplinka.
- GitHub – projekto kodo saugojimui ir versijavimui.

Naudotos operacinės sistemos:

- Kali linux 2022.03 (Linux Rolling) – projekto kodo rašymas, testavimas.

Naudotojo sąsaja:

- ReactJS – sąsaja, skirta patogesnei prototipo demonstracijai ir testavimui.

3.2. Balsuotojų blokų grandinės architektūra ir komponentai

Balsuotojų blokų grandinei buvo kuriamos dvi atskiros programos. *VotersBlockchain* – pagrindinis paskirstytos blokų grandinės kodas ir *votersBlockchainManagement* – programa, skirta palengvinti darbą su blokų grandine bei projekto testavimu.

votersBlockchain programos kodo *block.js* faile aprašoma blokų grandinės bloko struktūra (bloko antraštės ir bloko kūno). *Chain.js* faile aprašytos pagrindinės funkcijos, skirtos valdyti blokų grandinę:

- *createDb* – sukuriamą lokali (*level*) duomenų bazė, skirta palengvinti testavimą, taip pat ją galima naudoti siekiant pagerinti sistemos greitaveiką;
- *getGenesisBlock* – sukuriamas pirmasis (*genesis*) blokų grandinės blokas;
- *getLatestBlock* – grąžinamas paskutinis sukurtas blokų grandinės blokas;
- *getChain* – grąžinama visa blokų grandinė;
- *validateChain* – tikrinama ar blokų grandinė nebuvo neteisėtai pakeista;
- *addBlock* – skirtas pridėti naujam blokui į blokų grandinę;
- *storeBlock* – naujai sukurtas blokas išsaugomas duomenų bazėje;
- *validateDB* – tikrinama ar blokų grandinės duomenų bazė nebuvo neteisėtai pakeista;
- *getDbBlockIndex* – grąžinamas pasirinktas (nurodžius indeksą) blokų grandinės blokas esantis duomenų bazėje;
- *getDbBlockHash* – grąžinamas pasirinktas (nurodžius maišos reikšmę) blokų grandinės blokas esantis duomenų bazėje;
- *getLastDBBlock* – grąžinamas paskutinis sukurtas blokų grandinės blokas esantis duomenų bazėje;
- *getBlock* – grąžinamas pasirinktas (nurodžius indeksą) blokų grandinės blokas;
- *generateNextBlock* – formatuojama informacija naujam blokui ir jis pridedamas į blokų grandinę;
- *insertNewBlock* – metodas, skirtas sukurti naują bloką ir patalpinti jį į blokų grandinę.

P2p.js yra pagrindinis programos failas. Paleidus programą sukuriamas atsitiktinis 32 bitų ilgio mazgo ID ir inicijuojama mazgų aptikimo biblioteka. Mazgų aptikimui paleidžiamas asinchroninis metodas, jame mazgui priskiriamas atsitiktinis prievadas, skirtas komunikacijai su kitais mazgais, tuomet ieškoma kitų mazgų, esančių tame pačiame kanale, jį radus – bandoma prisijungti. Šioje kodo dalyje taip pat realizuotas žinučių klausymosi kanalas. Gavus tam tikrą žinutės tipą (realizuoti ir galimi žinučių tipai tinkle yra aprašyti toliau darbe) yra imamasi konkrečių veiksmų, priklausomai nuo gautos žinutės.

- *REQUEST_BLOCK* – užklausa norint gauti bloką iš blokų grandinės su gauta indekso reikšme;
- *RECEIVE_NEXT_BLOCK* – užklausa norint gauti sekantį bloką grandinėje. Mazgas, gavęs šią žinutę siunčia žinutę kitiems mazgams su paskutinio bloko indekso reikšme +1, taip siekiant gauti ir papildyti savo turimą blokų grandinę naujai sukurtu bloku;
- *RECEIVE_NEW_BLOCK* – su šia žinute kartu gaunamas ir naujas blokas, kuris patalpinamas mazgo turimoje blokų grandinėje;
- *REQUEST_ALL_REGISTER_MINERS* – gavus šią žinutę išsiunčiamas mazgo turimas registruotų kasėjų (angl. *miners*) mazgų sąrašas kitiems mazgams;

- REGISTER_MINER – ši žinutė gaunama kartu su mazgo, kuris ją siunčia ID, tai yra prašymas jį užregistruoti pas save esančiame blokų kasėjų sąrašė;
- CREATE_NEW_BLOCK – gavus šią žinutę mazgas kuria naują bloką. Sukūrus naują bloką ir jį patalpinus savo blokų grandinėje, mazgas siunčia žinutę visiems kitiems mazgams (RECEIVE_NEW_BLOCK), kad šie siųstų užklausą ir prašytų gauti naują bloką, kurio nėra jų blokų grandinėje.

Šis metodas taip pat nuolatos stebi kanalą ir aptikęs, kad kuris nors mazgas atsijungė nuo tinklo jį pašalina iš kasėjų (angl. *miners*) sąrašo, taip užtikrindamas, kad nebus liepiama sukurti naujo bloko mazgui, kuris jau neegzistuoja tinkle.

Korektiškam sistemos veikimui realizuoti du pagrindiniai žinučių siuntimo metodai:

- writeMessageToPeers – metodas, skirtas siųsti žinutę visiems tinkle esantiems mazgams;
- writeMessageToPeerToId – metodas, skirtas siųsti žinutę konkrečiam mazgui, esančiam tinkle.

Siekiant užtikrinti, kad kasėjų sąrašas ir blokų grandinė visuomet būtų sinchronizuoti tarp visų mazgų, yra realizuoti du metodai, vykdomi kas penkias sekundes. Vienas siunčia žinutę visiems mazgams su tekstu – REQUEST_ALL_REGISTER_MINERS (žinutės reikšmė aprašyta aukščiau šiame skyriuje), kitas siunčia žinutę visiems mazgams – REQUEST_BLOCK, taip pat su šia žinute prideda prašomo bloko indeksą (t. y. paskutinio turimo bloko indeksas + 1) (žinutės reikšmė yra aprašyta aukščiau šiame skyriuje).

Siekiant užtikrinti, kad dėl tinklo problemų nedingtų kasėjai, kas septynias sekundes kartojamas pranešimas, kuriuo siekiama užsiregistruoti kasėjų sąrašė, taip pat kas septynias sekundes siunčiamas pranešimas REGISTER_API_IPS_AND_PORTS. Šis žinutės tipas plačiau aptartas *votersBlockchainManagement* programos aprašyme 3.2.1 skyrelyje.

Šioje programoje taip pat yra realizuota ir rest API užklausoms klausyti. Paleidus mazgo programinį kodą yra priskiriamas atsitiktinis prievadas. Programoje realizuotos šios užklausos:

- blocks – grąžina visą mazgo turimą blokų grandinę;
- getBlock – leidžia gauti bet kurį bloką siunčiant užklausą su norimo bloko indeksu;
- getDBBlockIndex – užklausa leidžia gauti bet kurį blokų grandinės bloką siunčiant norimo bloko indeksą, tačiau blokas grąžinamas iš lokalios *level* duomenų bazės;
- getDBBlockHash – užklausa leidžia gauti bet kurį blokų grandinės bloką siunčiant bloke saugomo rinkėjo duomenų maišos reikšmę, tačiau blokas grąžinamas iš lokalios *level* duomenų bazės;
- getLastDBBlock – grąžina paskutinį blokų grandinės bloką esantį duomenų bazėje;
- getLastBlock – grąžina paskutinį blokų grandinės bloką;
- getChain – grąžina visą saugomą blokų grandinę;
- insertNewBlock – užklausa, skirta sukurti naujam blokui blokų grandinėje, joje reikia siųsti blokui reikalingus duomenis.

3.2.1. Balsuotojų blokų grandinės valdymo programa

Kaip jau buvo minėta anksčiau, *votersBlockchainManagement* programa skirta lengviau naudotis ir testuoti sukurtą balsuotojų blokų grandinę, jos mazgus.

Pagrindinis programos kodas yra *management.js* faile. Paleidus programą ji, kaip ir blokų grandinės mazgo programa, susikuria atsitiktinį 32 bitų ilgio ID bei gauna atsitiktinį prievadą, skirtą komunikacijai su kitais mazgais. Sukūrus šiuos parametrus programa jungiasi prie nurodytų blokų grandinės mazgų tinklo. Priešingai nei anksčiau aprašyta programa, ši turi ir priima tik du mazgų siunčiamų pranešimų tipus:

- REGISTER_MINER – gavusi šią žinutę programa saugo visus mazgus, kurie registruojasi kaip kasėjai, tai yra reikalinga tam, kad būtų galima žinoti kam sistema turi priskirti bloko kūrimą;
- REGISTER_API_IPS_AND_PORTS – su šia žinute mazgas gauna visų mazgų API IP adresus ir prievadus, kuriais mazgai gali būti pasiekiami bei juos išsisaugo.

Tiek registruoti kasėjai, tiek jų API duomenys nuolatos tikrinami ir atsiradus naujam mazgui arba dingus mazgui, jie atitinkamai atnaujinami – mazgų duomenys pridedami arba pašalinami iš išsaugotų duomenų.

Kaip ir mazgų programos, taip ir valdymo programa turi du pagrindinius metodus, skirtus siųsti pranešimams kitiems mazgams – *writeMessageToPeers* ir *writeMessageToPeerToId*.

Ši programa kas penkias sekundes siunčia pranešimą REQUEST_ALL_REGISTER_MINERS visiems mazgams, taip tikrindama mazgų egzistavimą.

Valdymo programos pagrindinis tikslas yra bendras API, kuriuo galima pasiekti bet kurį mazgą, nežinant jų konkrečių IP adresų ir prievadų. Kalbant plačiau apie API, programoje yra realizuotos aštuonios pagrindinės užklausos:

- getChain – grąžina pilną sukurtą blokų grandinę. Kaip jau buvo minėta, ši programa turi pilną visų registruotų mazgų sąrašą bei jų komunikacijos duomenis, todėl siekiant paskirstyti apkrovą, blokų grandinė yra gaunama atsitiktinai pasirinkus mazgą iš turimo sąrašo. Tai užtikrina, kad kiekvieną kartą siunčiant užklausą, grandinė būtų gaunama vis iš naujo mazgo;
- getLastDBBlock – grąžina paskutinį bloką, esantį blokų grandinės duomenų bazėje. Ši užklausa mazgą pasirenka atsitiktinai;
- getCertainDBBlockIndex – grąžinamas pasirinkto indekso blokų grandinės blokas iš duomenų bazės. Ši užklausa mazgą pasirenka atsitiktinai;
- getCertainDBBlockHash – grąžinamas blokų grandinės blokas iš duomenų bazės, kuriame yra saugoma nurodyta maišos reikšmė. Ši užklausa mazgą pasirenka atsitiktinai;
- getLastBlock – grąžina paskutinį bloką, esantį blokų grandinėje. Ši užklausa mazgą pasirenka atsitiktinai;
- setRegistrationEndTime – užklausa, skirta nustatyti naudotojų registracijos laiko pabaigą. Po nustatyto laiko bandant registruotis sistemoje (sukurti naują bloką) to padaryti nepavyks;
- createVotingChainGenesisBlock – ši užklausa skirta sukurti pirmajam blokui balsų blokų grandinėje. Užklausos vykdyti nepavyks jeigu dar nėra pasibaigęs registracijos laikas;
- insertNewBlock – užklausa, skirta ir naudojama registruojantis balsavimo sistemoje. Su šia užklausa keliauja besiregistruojančio rinkėjo duomenys ir yra kuriamas blokas blokų grandinėje. Gavus šią užklausą programa duomenis stato į eilę, kurią apdoroja *cron* programa.

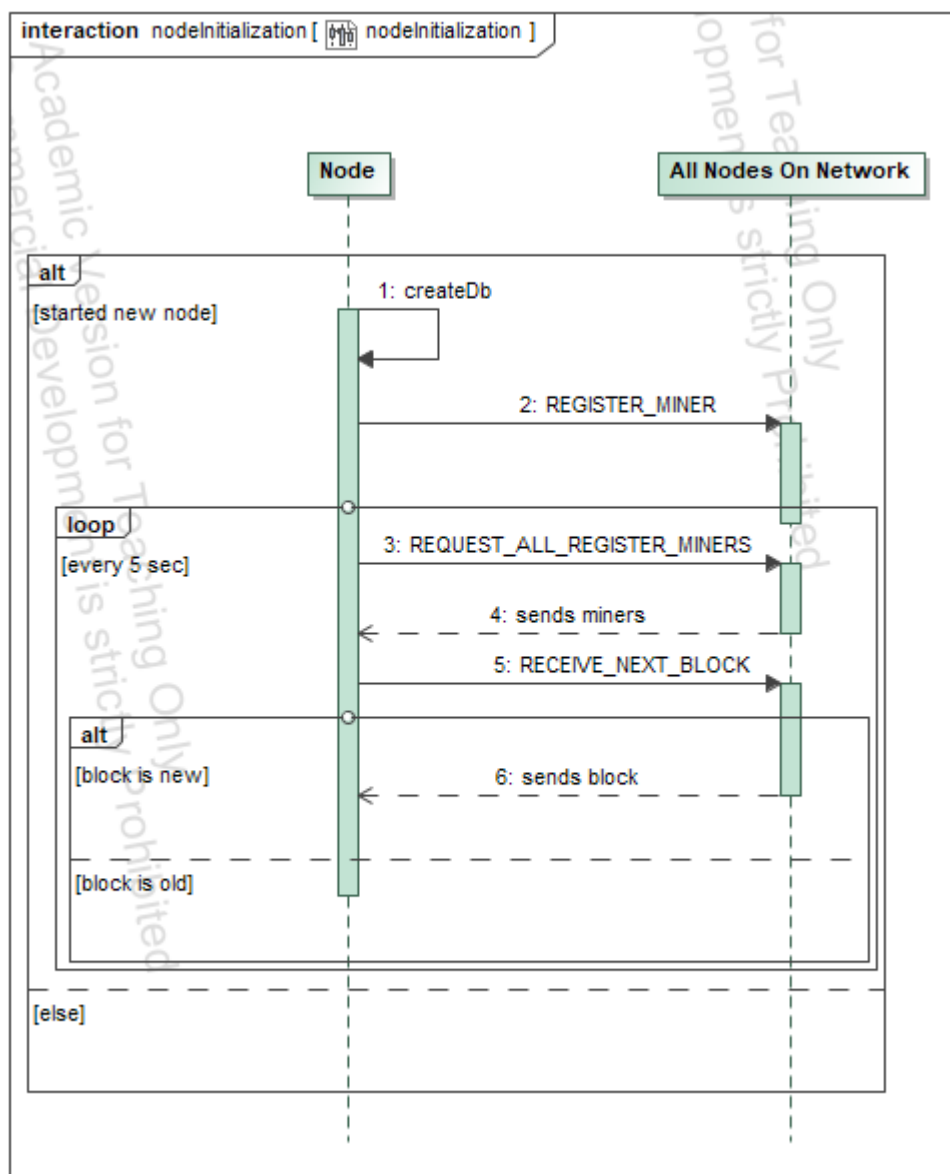
Cron programa – tai programa, kuria siekiama paskirstyti darbą tarp mazgų, taip pat užtikrinti, kad du skirtingi blokai nebus sukuriami su tuo pačiu indeksu, kadangi tai pažeistų blokų grandinės integralumą ir skirtingi mazgai turėtų skirtingas blokų grandines. Kaip jau buvo minėta, gavus

užklausa sukurti naują bloką, duomenys yra statomi į eilę, šią eilę ir apdoroja *cron* programa. Programa paleidžiama kas x sekundžių (x – parametras yra modifikuojamas, jį nustato programos kūrėjas). Programa ima duomenis patalpintus eilėje nuo pirmo ir siunčia mazgui, kad šis sukurtų naują bloką. Mazgai, kuriems siunčiama užduotis, taip pat imami iš eilės (iš registruotų kasėjų sąrašo), taip užtikrinant, kad nebūtų vieno mazgo, kuris yra atsakingas už blokų kūrimą ir išsprendžiant problemą – kas būtų jei vienas mazgas dingtų, o atsirastų kitas?

3.2.2. Balsuotojų blokų grandinės elgsenos modeliai

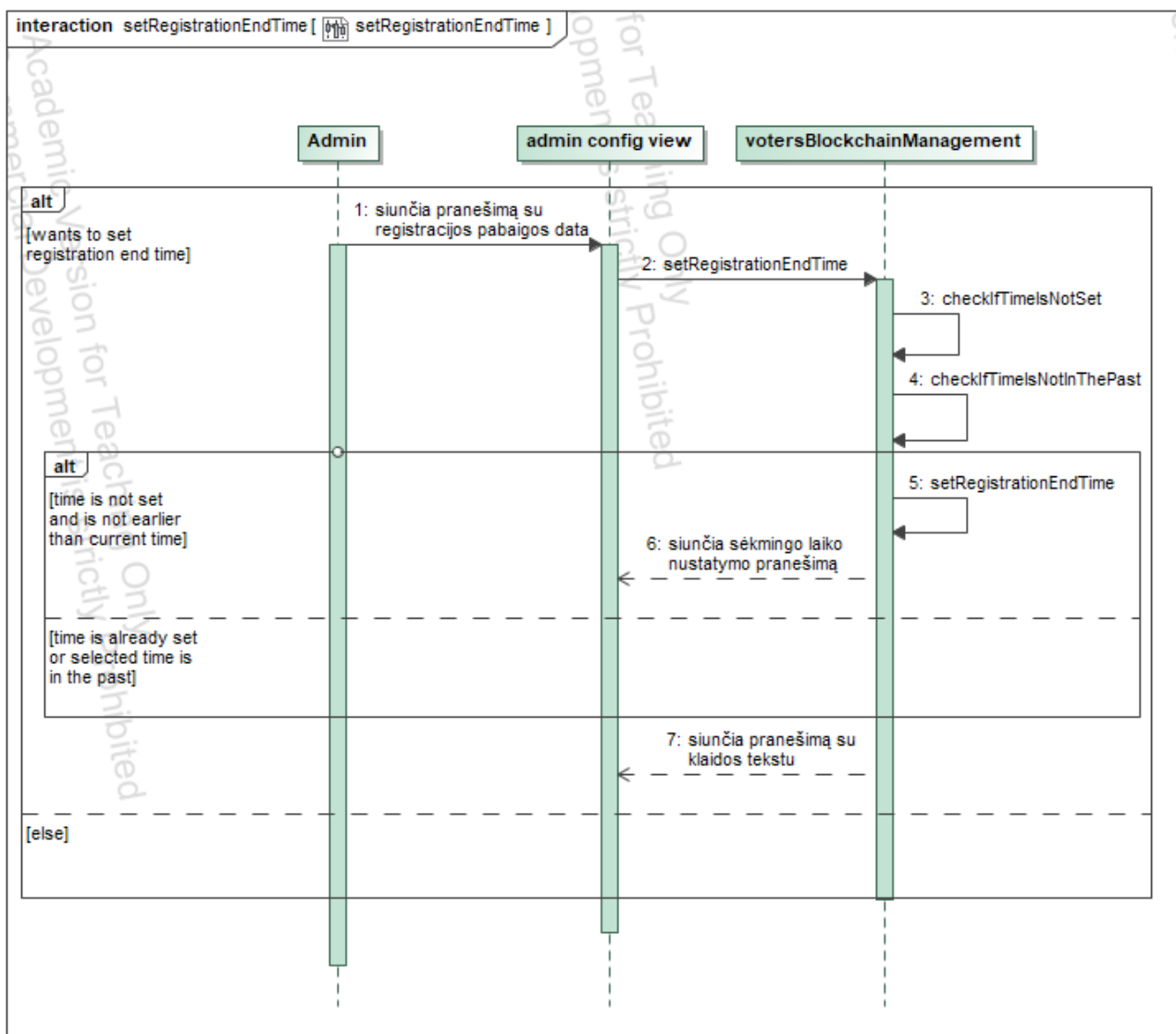
Detaliau analizuojant prototipo veikimą galima trumpai apžvelgti keletą pagrindinių elgsenos modelių, kurie padės detaliau suprasti sistemos veikimo principus.

16 pav. pateiktas mazgo paleidimo elgsenos modelis. Paleidus mazgą, šis iš pradžių sukuria lokalią duomenų bazę (joje saugoma blokų grandinės objekto kopija – kitaip tariant blokų grandinės kopija), tuomet naujai paleistas mazgas siunčia pranešimą visiems kitiems mazgams, kuriuo užsiregistruoja blokų kasėjų sąrašą. Atlikus registraciją pirminiai veiksmai yra atlikti, po to veikia 3-6 cikliniai veiksmai. 3 veiksmo mazgas prašo visų kitų mazgų, kad šie atsiųstų savo blokų kasėjų registracijos sąrašus, tam, kad šis visuomet būtų sinchronizuotas. 5 veiksmu siekiama sinchronizuoti turimą blokų grandinę su kitais mazgais, t. y. mazgas siunčia pranešimą, prašydamas kitų mazgų atsiųsti tam tikrą blokų grandinės bloką (paskutinio turimo bloko indeksas + 1). Cikliniai veiksmai kartojasi kas 5 sekundes visą mazgo gyvavimo laiką. Šis elgsenos modelis tinka ne tik balsuotojų blokų grandinei, bet ir balsų blokų grandinei, kadangi mazgų inicializavimas yra identiškas.



16 pav. Blokų grandinės mazgo paleidimo elgsenos modelis

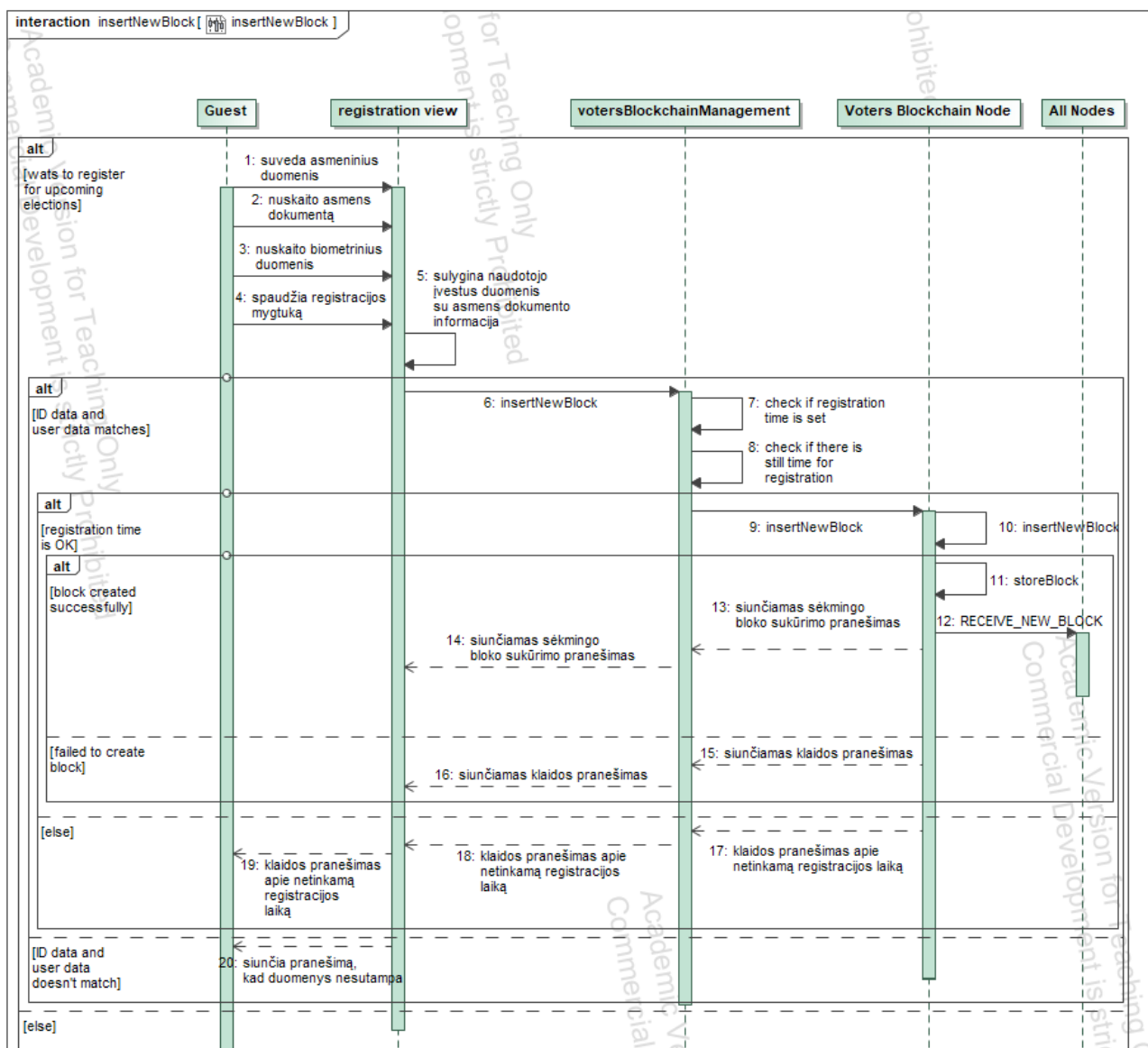
17 pav. galima matyti registracijos termino nustatymo elgsenos modelį. Jame matoma, kad administratorius pasirenka datą kada yra numatomas balsuotojų registracijos sistemoje galutinė data. Pasirinkti duomenys siunčiami balsuotojų blokų grandinės valdymo programai, kuri patikrina ar data jau nėra nustatyta, taip pat ar pasirinkta data nėra senesnė nei dabartinė data. Jeigu šie tikrinimai praeina be nesklandumų, galutinis terminas yra išsaugomas ir administratorius apie tai informuojamas. Priešingu atveju administratoriui grąžinamas pranešimas su klaidos tekstu.



17 pav. Registracijos termino nustatymo elgsenos modelis

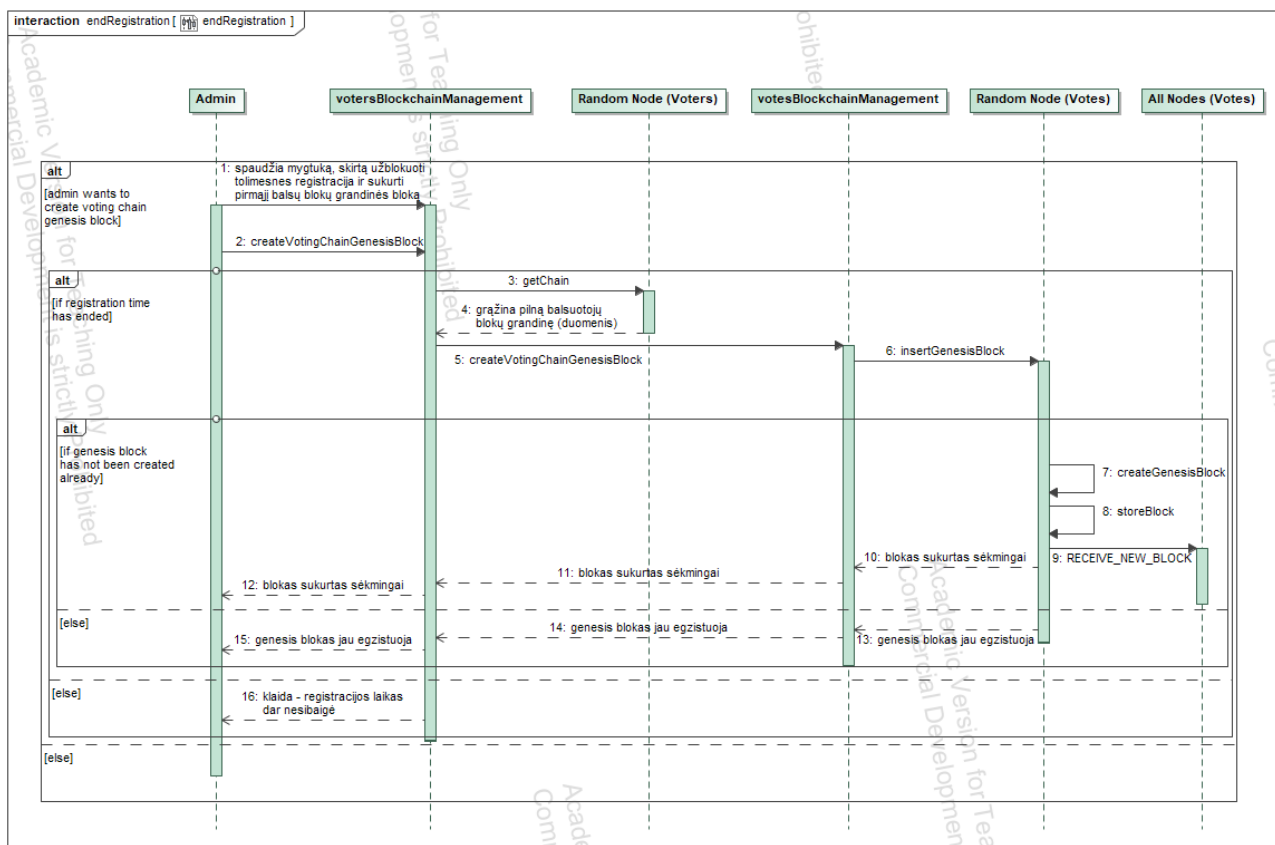
18 pav. pavaizduotas bloko kūrimo balsuotojų blokų grandinėje elgsenos modelis. Bloko kūrimas prasideda nuo naudotojo pateikiamų registracijai sistemoje reikalingų duomenų ir vieno mygtuko paspaudimu – patvirtinant užbaigia registraciją. Tuomet tikrinami naudotojo įvesti asmeniniai duomenys su duomenimis, esančiais naudotojo asmens dokumente. Jeigu duomenys nesutampa – naudotojas apie tai informuojamas ir jam tenka patikslinti informaciją ir bandyti registruotis dar kartą. Jeigu duomenys sutampa, darbą perima balsuotojų blokų grandinės valdymo programa. Ši iš pradžių patikrina ar naudotojas registruojasi tinkamu metu (t. y. ar registracijos pabaigos laikas nustatytas ir registracija vykdoma šiam laikui nepasibaigus), jeigu bandoma registruotis, kai registracija nėra galima – naudotojas apie tai informuojamas. Esant priešingai situacijai – registracijos laikui nepasibaigus – valdymo programa kreipiasi į atsitiktinį blokų grandinės mazgą ir liepia jam sukurti bloką su pateiktais duomenimis. Jeigu bloko nepavyksta sukurti dėl tam tikros klaidos – apie tai yra informuojama. Sėkmingai sukūrus bloką, jis papildomai yra išsaugomas lokaliaje duomenų bazėje, taip pat mazgas siunčia pranešimą visiems mazgams, kad šie prašytų atsiųsti naujai sukurtą bloką.

Taip pat, mazgas informuoja, kad blokas buvo sukurtas sėkmingai ir registracija sistemoje buvo sėkminga.



18 pav. Bloko kūrimo balsuotojų blokų grandinėje elgsenos modelis

19 pav. pateiktas registracijos draudimo (užbaigimo) elgsenos modelis. Administratorius, registracijos baigimui spaudžia tam skirtą mygtuką. Tuomet yra siunčiamas pranešimas balsuotojų blokų grandinei su pranešimu, skirtu inicijuoti balsų blokų grandinės pirmojo bloko kūrimą. Jeigu registracijos laikas dar nėra pasibaigęs, administratorius apie tai informuojamas, priešingu atveju valdymo programa atsitiktiniam mazgui siunčia pranešimą, kuriuo siekiama gauti pilną blokų grandinę. Gavus blokų grandinę, duomenys siunčiami balsų blokų grandinės valdymo programai. Ši programa atsitiktiniam mazgui persiunčia duomenis su pranešimu, skirtu inicijuoti ir sukurti balsų blokų grandinės pirmą bloką. Jeigu blokas jau yra sukurtas – siunčiamas klaidos pranešimas, priešingu atveju – mazgas sukuria bloką ir jį išsaugo. Taip pat bloką išsaugo ir lokaliaje duomenų bazėje. Atlikus šiuos veiksmus, mazgas siunčia pranešimą visiems kitiems mazgams, kad jie jo paprašytų naujai sukurtą bloką. Apie sėkmingą bloko sukūrimą informuojamas administratorius.



19 pav. Registracijos draudimo (užbaigimo) elgsenos modelis

3.3. Rinkimų balsų blokų grandinės architektūra ir komponentai

Balsų blokų grandinei, kaip ir balsuotojų blokų grandinei, buvo kuriamos dvi atskiros programos. *votesBlockchain* – programos kodas, skirtas blokų grandinės mazgams ir *votesBlockchainManagement* programa, kuria siekiama palengvinti blokų grandinės valdymą, demonstravimą ir testavimą.

Block.js faile aprašoma blokų grandinės bloko struktūra, o *chain.js* faile aprašytos pagrindinės funkcijos, skirtos valdyti blokų grandinę, jų yra 29:

- *createDb* – sukuriamą lokali (*level*) duomenų bazė;
- *getGenesisBlock* – grąžinamas pirmasis blokų grandinės blokas;
- *createGenesisBlock* – metodas, skirtas sukurti pirmajam blokų grandinės blokui (jis yra sudaromas iš balsuotojų blokų grandinės duomenų ir kuriamas registracijos laikui pasibaigus);
- *generateGenesisBlockData* – apdoroja gautus duomenis ir juos suformatuoja taip, kad būtų tinkami talpinimui į pirmąjį blokų grandinės bloką;
- *getLatestBlock* – grąžinamas paskutinis sukurtas blokų grandinės blokas;
- *getChain* – patikrinamas blokų grandinės vientisumas ir, jeigu integralumas yra nepažeistas, grąžinama visa blokų grandinė, priešingu atveju – klaidos pranešimas;
- *validateChain* – tikrinama ar blokų grandinė nebuvo neteisėtai pakeista;
- *addBlock* – patikrina blokų grandinės vientisumą ir prideda naują bloką;
- *storeBlock* – naujai sukurtas blokas išsaugomas duomenų bazėje;
- *validateDB* – patikrina ar blokų grandinės duomenų bazės integralumas nėra pažeistas;

- `getDbBlockIndex` – grąžinamas pasirinkto indekso blokų grandinės blokas, esantis duomenų bazėje;
- `getDbBlockHash` – grąžinamas blokų grandinės blokas su nurodyta rinkėjo duomenų maišos reikšme;
- `getLastDBBlock` – grąžinamas paskutinis blokų grandinės duomenų bazės blokas;
- `getBlock` – grąžinamas pasirinkto indekso blokų grandinės blokas iš atmintyje esančios grandinės;
- `getChainBlockHash` – grąžinamas blokų grandinės blokas iš atmintyje esančios grandinės, kuriame yra nurodyta rinkėjo maišos reikšmė;
- `getLastChainBlock` – grąžinamas paskutinis blokas iš atmintyje esančios grandinės;
- `generateNextBlock` – apdorojami / suformatuojami gauti duomenys, kad būtų galima juos talpinti į naują bloką;
- `insertNewBlock` – metodas, skirtas sukurti naują bloką ir patalpinti jį į blokų grandinę;
- `checkIfUserCanVote` – ieško gautų balsuotojo maišos duomenų (angl. *hash*) pirmajame balsų blokų grandinės bloke. Jeigu duomenys rasti – rinkėjas gali balsuoti, priešingu atveju – jam neleidžiama to daryti;
- `getUsersKey` – gaunamas rinkėjo viešas raktas iš pirmojo blokų grandinės bloko;
- `getUserVote` – iš visos blokų grandinės išrenkamas norimo rinkėjo atiduotas balsas;
- `checkIfUserAlreadyVoted` – patikrina ar rinkėjas jau balsavo, jeigu rinkėjas jau atidavė savo balsą, jam antrą kartą balsuoti neleidžiama. Jeigu rinkėjo balsas blokų grandinėje nerandamas, jam suteikiama galimybė balsuoti;
- `getLastBlockCandidatesResults` – metodas, skirtas gauti rinkimų rezultatams einamuoju momentu. Tai suteikia rinkimų stebėjimo galimybę ir realiu laiku matyti pirmaujantį kandidatą;
- `recalculateVotes` – metodas, skirtas patikrinti ar tikrai visi balsai buvo suskaičiuoti teisingai ir dar kartą juos perskaičiuoti;
- `recalculateVotesDB` – metodas, skirtas perskaičiuoti blokų grandinės, esančios duomenų bazėje, rezultatams;
- `changeCertainBlockVotersChosenCandidate` – metodas, skirtas testavimui. Juo pakeičiamas pasirinkto bloko rinkėjo pasirinktas kandidatas. Taip galima ištestuoti kaip reaguoja sistema į pažeistą blokų grandinės vientisumą;
- `getCandidates` – pirmojo indekso blokui skirtas metodas. Juo yra sugeneruojamas kandidatų sąrašas, kuris vėliau naudojamas balsų skaičiavimui ir talpinamas į kiekvieną bloką;
- `checkVotesCorrectCalculation` – patikrina ar balsai blokų grandinėje buvo suskaičiuoti teisingai;
- `addVotes` – gavus naują balsą, šiuo metodu perskaičiuojami kandidatų balsai ir rezultatai talpinami į naujai kuriamą bloką.

Kaip jau anksčiau aprašyta balsuotojų blokų grandinės programa, taip ir ši, turi vieną iš pagrindinių failų – *p2p.js*, kuris yra atsakingas už teisingą ir nenutrūkstamą komunikaciją tarp blokų grandinės mazgų. Programa veikia taip pat, kaip ir anksčiau aprašytoji (tik turi keletą papildomų funkcionalumų) – paleidus programą sukuriamas atsitiktinis 32 bitų ilgio mazgo ID ir inicijuojama mazgų aptikimo biblioteka. Tam paleidžiamas asinchroninis metodas, jame mazgui priskiriamas atsitiktinis prievadas, skirtas komunikacijai su kitais mazgais, tuomet ieškoma kitų mazgų, esančių tame pačiame kanale ir juos radus bandoma prisijungti. Čia realizuotas ir žinučių klausymosi kanalas.

Gavus tam tikrą žinutės tipą imamasi konkrečių veiksmų, priklausomai nuo gautos žinutės tikslo. Realizuotų priimamų žinučių tipai:

- `CREATE_GENESIS_BLOCK` – žinutė, kurią gavęs mazgas sukuria pirmąjį blokų grandinės bloką su gautais naudotojų duomenimis;
- `REQUEST_BLOCK` – užklausa norint gauti bloką iš blokų grandinės su gauta indekso reikšme;
- `RECEIVE_NEXT_BLOCK` – užklausa norint gauti sekantį bloką grandinėje. Mazgas, gavęs šią žinutę, siunčia žinutę kitiems mazgams su paskutinio bloko indekso reikšme +1, taip siekiant gauti ir papildyti savo turimą blokų grandinę naujai sukurtu bloku;
- `RECEIVE_NEW_BLOCK` – su šia žinute kartu gaunamas ir naujas blokas, kuris patalpinamas mazgo turimoje blokų grandinėje;
- `REQUEST_ALL_REGISTER_MINERS` – gavus šią žinutę išsiunčiamas mazgo turimas registruotų kasėjų (angl. *miners*) mazgų sąrašas kitiems mazgams;
- `REGISTER_MINER` – ši žinutė gaunama kartu su mazgo, kuris ją siunčia ID, tai yra prašymas jį užregistruoti pas save esančiame blokų kasėjų sąraše;
- `CREATE_NEW_BLOCK` – gavus šią žinutę mazgas kuria naują bloką. Sukūrus naują bloką ir jį patalpinus pas save blokų grandinėje, mazgas siunčia žinutę visiems kitiems mazgams (`RECEIVE_NEW_BLOCK`), kad šie siųstų užklausą ir prašytų gauti naują bloką, kurio nėra jų blokų grandinėje.

Šis metodas taip pat nuolatos stebi kanalą, ir aptikus, kad kuris nors mazgas atsijungė nuo tinklo, jį pašalina iš kasėjų (angl. *miners*) sąrašo, taip užtikrinant, kad nebus liepiama sukurti naują bloką mazgui, kuris jau neegzistuoja tinkle.

Šioje programoje taip pat yra du pagrindiniai žinučių siuntimo metodai:

- `writeMessageToPeers` – metodas, skirtas siųsti žinutę visiems tinkle esantiems mazgams;
- `writeMessageToPeerToId` – metodas, skirtas siųsti žinutę konkrečiam mazgui esančiam tinkle.

Kaip ir pirmoji aprašyta blokų grandinė, taip ir ši, turi du metodus, skirtus tinkamam blokų grandinių sinchronizavimui tarp mazgų. Šie metodai vykdomi kas penkias sekundes. Vienas siunčia žinutę visiems mazgams su tekstu – `REQUEST_ALL_REGISTER_MINERS` (žinutės reikšmė yra aprašyti viršuje), kitas siunčia žinutę visiems mazgams – `REQUEST_BLOCK`, taip pat su šia žinute prideda prašomo bloko indeksą (t. y. paskutinio turimo bloko indeksas + 1) (žinutės reikšmė yra aprašyta viršuje).

Bandant išvengti keliamų tinklo problemų, dėl kurių kasėjai gali dingti iš bendro mazgų tinklo, kas septynias sekundes kartojamas pranešimas, kuriuo siekiama užsiregistruoti kasėjų sąraše, taip pat kas septynias sekundes siunčiamas pranešimas `REGISTER_API_IPS_AND_PORTS`.

Balsų blokų grandinė, tiksliau kiekvienas paleistas mazgas, taip pat turi savo API. Užklausoms klausyti, paleidus programą priskiriamas atsitiktinis prievadas. Programoje realizuotos šios užklausos:

- `blocks` – gauti blokų grandinės blokams;
- `getBlock` – leidžia gauti bet kurį bloką, siunčiant užklausą su norimo bloko indeksu;

- `getUserVote` – grąžina bloką su konkretaus naudotojo pateiktu balsu;
- `recalculateVotesDBChain` – užklausa, skirta duomenų bazėje esančios grandinės rezultatų perskaičiavimui;
- `recalculateVotesChain` – užklausa, skirta atmintyje esančios blokų grandinės rezultatų perskaičiavimui;
- `getDBBlockIndex` – užklausa leidžia gauti bet kurį blokų grandinės bloką, siunčiant norimo bloko indeksą, tačiau blokas yra grąžinamas iš lokalsios *level* duomenų bazės;
- `getDBBlockHash` – užklausa leidžia gauti bet kurį blokų grandinės bloką, siunčiant rinkėjo duomenų maišos reikšmę, tačiau blokas yra grąžinamas iš lokalsios *level* duomenų bazės;
- `getLastDBBlock` – grąžinamas paskutinis blokas iš duomenų bazės;
- `getLastBlock` – grąžina paskutinį blokų grandinės bloką;
- `getChain` – skirta gauti pilnai blokų grandinei;
- `getChainBlockIndex` – grąžina pasirinkto indekso bloką iš atmintyje esančios blokų grandinės;
- `getChainBlockHash` – grąžina nurodyto rinkėjo (rinkėjo duomenų maišos reikšmės) bloką iš atmintyje esančios blokų grandinės;
- `canUserVote` – tikrinama ar rinkėjo, norinčio balsuoti, duomenys egzistuoja pirmajame blokų grandinės bloke;
- `getUsersKey` – randamas rinkėjo viešas raktas pirmame blokų grandinės bloke;
- `changeCertainBlockChosenCandidate` – užklausa, skirta testavimui. Ja galima pakeisti norimo bloko rinkėjo pasirinktą kandidatą;
- `getLastBlockCandidatesResults` – gaunami rinkimų rezultatai iš paskutinio blokų grandinės bloko;
- `checkIntegrity` – grąžina atsakymą, ar blokų grandinės vientisumas nėra pažeistas;
- `insertNewBlock` – užklausa, skirta sukurti naujam blokui blokų grandinėje, joje reikia siųsti blokui reikalingus duomenis.

3.3.1. Balsų blokų grandinės valdymo programa

Patogesniam blokų grandinės demonstravimui, testavimui bei valdymui yra sukurta *votesBlockchainManagement* programa.

Ši programa veikia taip, pat, kaip ir balsuotojų blokų grandinės valdymo programa, todėl visas veikimas nuo pradžių čia nebus aprašytas. Kadangi pagrindiniai skirtumai yra API dalyje, skyrelyje aprašyta tik ši dalis.

Šis API, kaip jau buvo minėta, yra bendras API, kuriuo galima pasiekti bet kurį mazgą, nežinant jų konkrečių IP adresų ir prievadų. Kalbant plačiau apie API, programoje yra realizuota dvidešimt pagrindinių užklausų:

- `getAllNodesInfo` – užklausa, skirta gauti visiems užregistruotiems mazgams. Skirtas vartotojo sąsajai – testavimui, kad būtų galima pasirinkti, kurio mazgo blokų grandinės bloką norima keisti, taip siekiant ją pažeisti;
- `getChainFromCertainNode` – ši užklausa taip pat yra skirta testavimui, ji leidžia pasirinkti konkretų mazgą (o ne atsitiktinį, kaip yra numatyta), iš kurio norima gauti blokų grandinę;

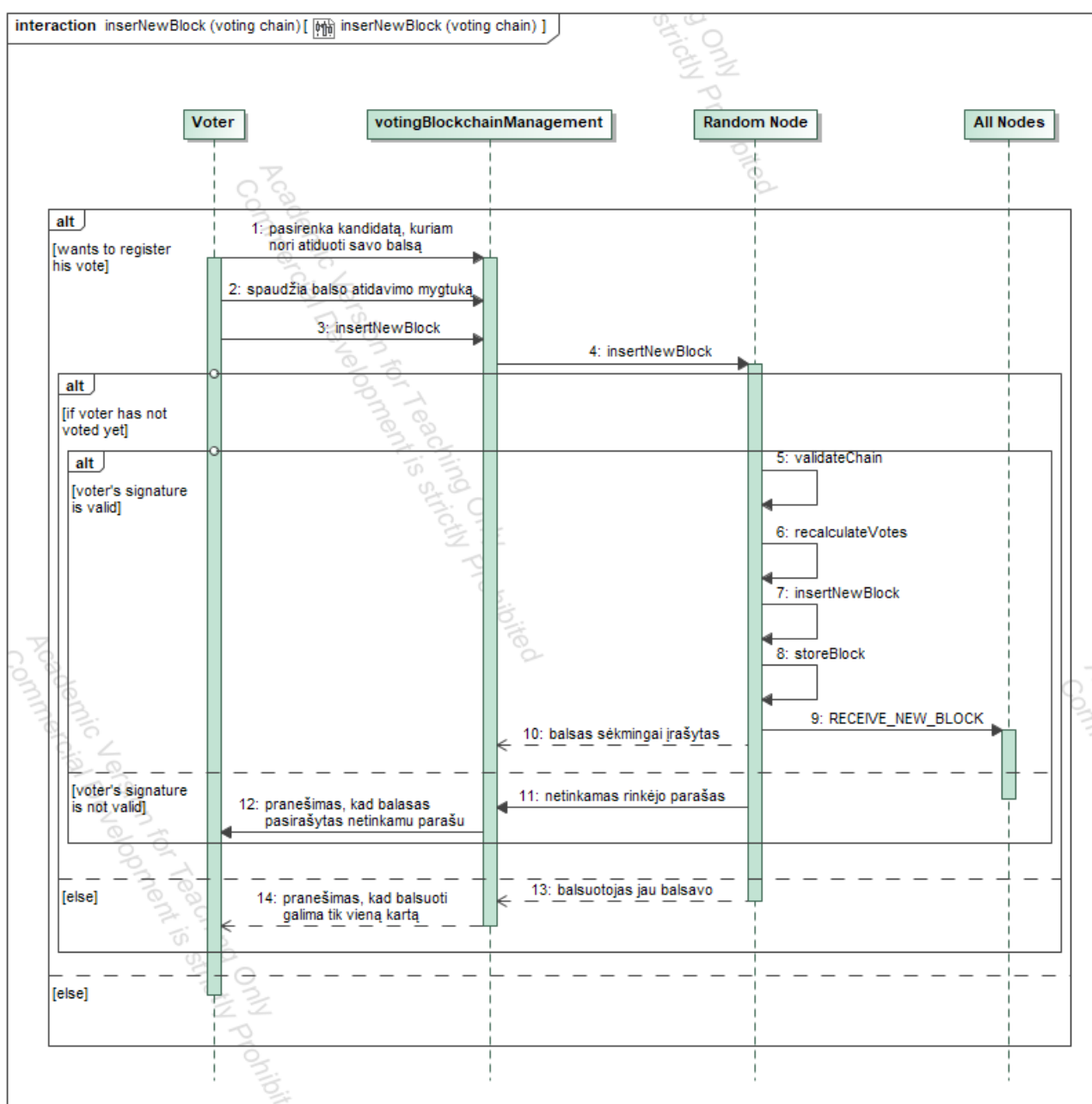
- `changeCertainNodeCertainBlock` – dar viena užklausa, skirta testavimui, kurios pagalba galima pakeisti pasirinkto mazgo pasirinktą bloką;
- `getChain` – grąžina pilną sukurto blokų grandinę. Kaip jau buvo minėta, ši programa turi pilną visų registruotų mazgų sąrašą bei jų komunikacijos duomenis, todėl siekiant paskirstyti apkrovą, blokų grandinę gaunama atsitiktinai pasirinkus mazgą iš turimo sąrašo, todėl kiekvieną kartą siunčiant užklausa, grandinė gali būti gaunama vis iš naujo mazgo;
- `getLastBlock` – grąžina paskutinį bloką esantį blokų grandinėje. Kaip ir prieš tai aprašyta užklausa, ši taip pat pasirenka mazgą atsitiktinai;
- `findUser` – siunčiama užklausa atsitiktiniam mazgui, siekiant patikrinti ar naudotojo duomenys egzistuoja pirmajame balsų blokų grandinės bloke;
- `getVotes` – gaunami rinkimų rezultatai iš paskutinio sukurto (atsitiktinio mazgo) blokų grandinės bloko;
- `checkIntegrity` – tikrinamas blokų grandinės integralumas;
- `setRegistrationEndTime` – užklausa, skirta nustatyti naudotojų registracijos laiko pabaigą. Po nustatyto laiko bandant registruotis sistemoje (sukurti naują bloką) to padaryti nepavyks;
- `recalculateVotesDBChain` – inicijuojamas duomenų bazėje esančios grandinės rezultatų perskaičiavimas. Mazgas pasirenkamas atsitiktinai;
- `recalculateVotesChain` – inicijuojamas atmintyje esančios grandinės rezultatų perskaičiavimas. Mazgas pasirenkamas atsitiktinai;
- `getLastDBBlock` – grąžinamas paskutinis blokas iš duomenų bazės. Mazgas pasirenkamas atsitiktinai;
- `getLastBlockChain` – grąžinamas paskutinis blokas iš atmintyje esančios blokų grandinės. Mazgas pasirenkamas atsitiktinai;
- `getCertainDBBlockIndex` – grąžinamas nurodyto indekso blokas iš duomenų bazės. Mazgas pasirenkamas atsitiktinai;
- `getCertainDBBlockHash` – grąžinamas nurodyto rinkėjo (duomenų maišos) balso blokas iš duomenų bazės. Mazgas pasirenkamas atsitiktinai;
- `getCertainChainBlockIndex` – grąžinamas nurodyto indekso blokas iš atmintyje esančios blokų grandinės. Mazgas pasirenkamas atsitiktinai;
- `getCertainChainBlockHash` – grąžinamas nurodyto rinkėjo (duomenų maišos) balso blokas iš atmintyje esančios blokų grandinės. Mazgas pasirenkamas atsitiktinai;
- `getUserVote` – užklausa, skirta gauti norimo rinkėjo balso bloką;
- `insertNewBlock` – užklausa skirta ir naudojama registruojantis balsavimo sistemoje. Su šia užklausa keliauja besiregistruojančio rinkėjo duomenys ir yra kuriamas blokas blokų grandinėje. Gavus šią užklausa, programa duomenis stato į eilę, kurią apdoroja *cron* programa;
- `createVotingChainGenesisBlock` – ši užklausa skirta sukurti pirmajam blokui balsų blokų grandinėje. Užklauskos vykdyti nepavyks, jeigu dar nėra pasibaigęs registracijos laikas.

Ši programa, kaip ir programa aprašyta 3.2.1 skyrelyje, turi savo *Cron* programą, kurios tikslas ir veikimo principas yra toks pats.

3.3.2. Balsų blokų grandinės elgsenos modeliai

Mazgų inicializavimas tiek balsuotojų blokų grandinėje, tiek balsų blokų grandinėje yra identiškas, todėl čia papildomai nėra dar kartą aprašomas mazgo paleidimo elgsenos modelis. Jį galima matyti 16 pav., o detaliau jis aprašomas - 3.2.2 skyrelyje.

20 pav. galima matyti blokų kūrimo balsų blokų grandinėje elgsenos modelį. Naudotojui pasirinkus kandidatą ir paspaudus mygtuką, skirtą įrašyti balsą blokų grandinėje, pranešimas su informacija siunčiamas balsų blokų grandinės valdymo programai. Programa tikrina, ar rinkėjo atiduotas balsas yra pasirašytas teisingu parašu. Jeigu parašas netinkamas – rodomas klaidos pranešimas, priešingu atveju, tikrinama ar rinkėjas dar nėra balsavęs. Jeigu balsuotojas jau yra balsavęs (blokas su balsuotojo informacijos maišos reikšme randamas balsų blokų grandinėje), rinkėjas yra informuojamas, kad jis jau balsavo ir antrą kartą to padaryti negalima. Jeigu rinkėjas dar nėra balsavęs, duomenys siunčiami atsitiktiniam mazgui. Mazgas, gavęs bloko kūrimo užklausą, patikrina ar blokų grandinės vientisumas nėra pažeistas, tuomet perskaičiuoja kandidatų balsus, pridėdamas rinkėjo balsą ir sukuria naują bloką. Sukurtą bloką taip pat įrašo į lokalią duomenų bazę ir siunčia pranešimą visiems mazgams, kad šie prašytų naujai sukurtą bloką. Apie sėkmingą bloko sukūrimą (informacijos įrašymą) siunčiamas informacinis pranešimas.

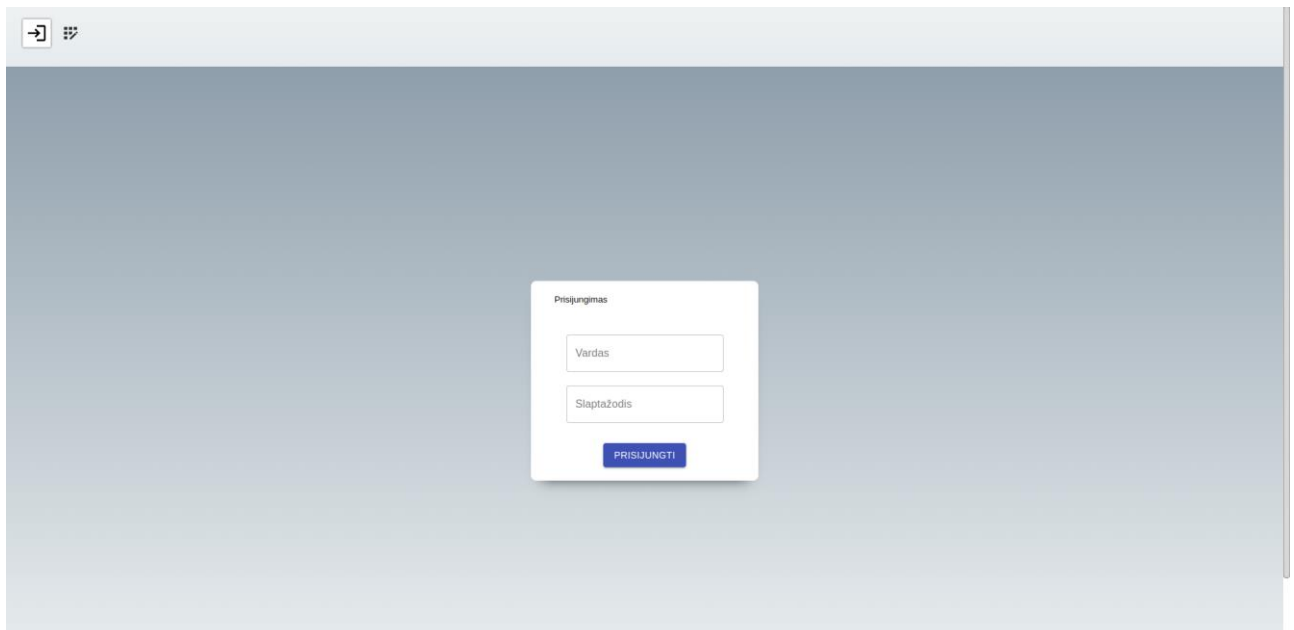


20 pav. Bloko kūrimo balsų blokų grandinėje elgsenos modelis

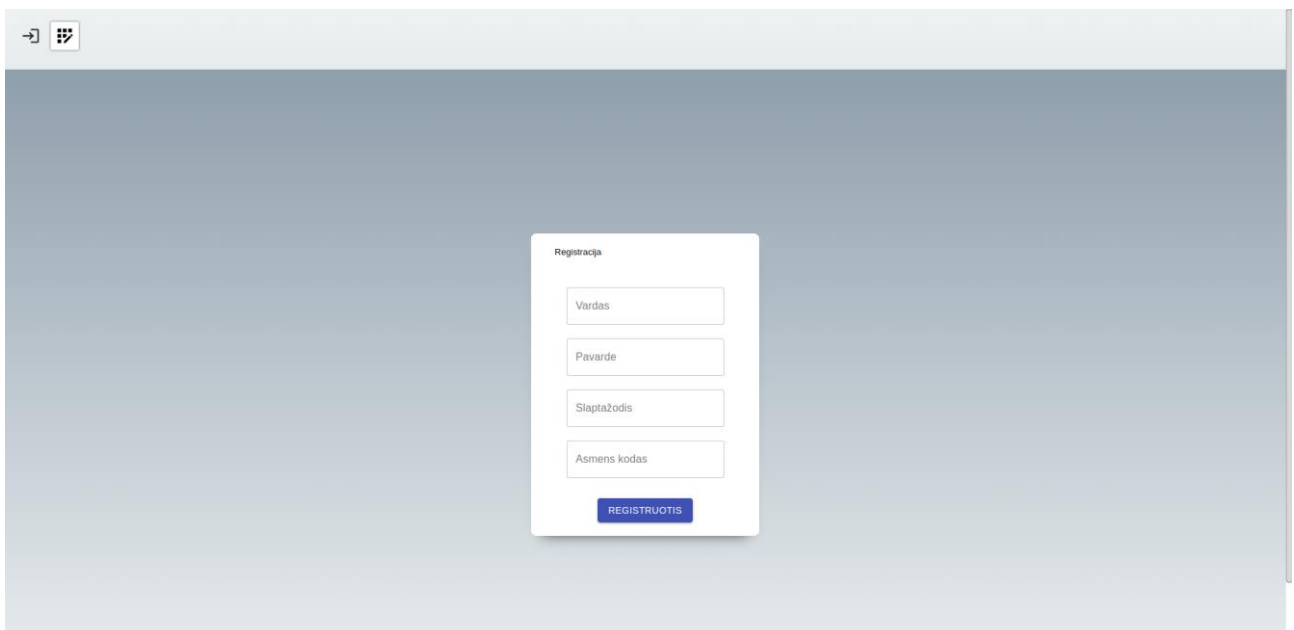
3.4. Testavimo ir demonstracijos naudotojo sąsaja

Siekiant patogiau testuoti ir demonstruoti el. balsavimo sistemos, pagrįstos blokų grandinių technologija realizuotą prototipą, pasinaudojant *ReactJS* karkasu, buvo sukurta naudotojo sąsaja. Šiame poskyryje pateikti pagrindiniai langai taip siekiant padėti detaliau įsivaizduoti sukurto sprendimo prototipą.

21 pav. ir **22 pav.** pavaizduoti prisijungimo ir registracijos langai. Jie skirti patikrinti ir pademonstruoti, kaip veikia naudotojų nuasmeninimas ir blokų kūrimas balsuotojų blokų grandinėje.

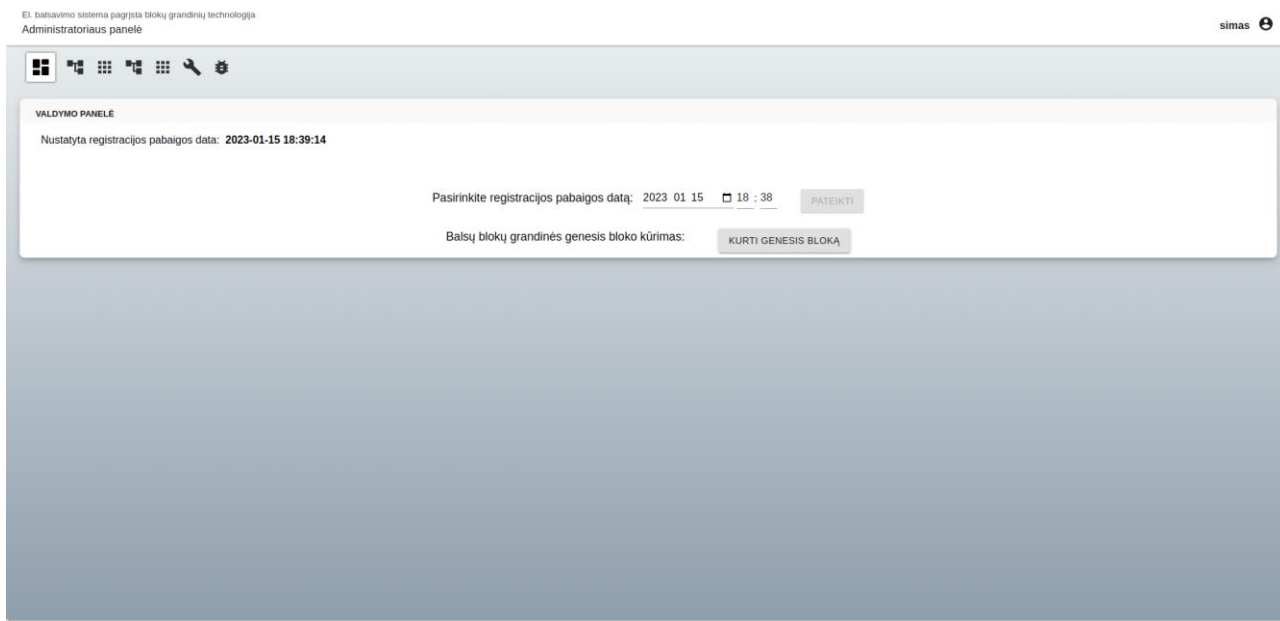


21 pav. Naudotojo sąsaja - Prisijungimas



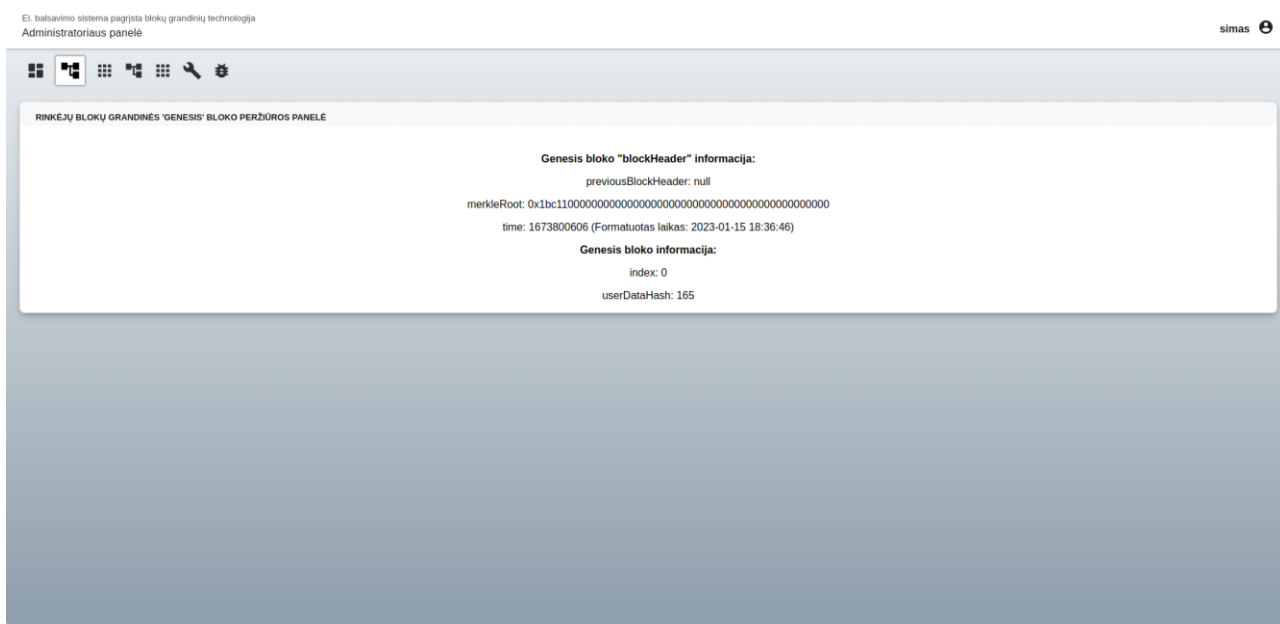
22 pav. Naudotojo sąsaja – Registracija

23 pav. pavaizduota administratoriaus panelė, kurioje administratorius gali nustatyti registracijos el. balsavimo sistemoje pabaigos datą. Pasibaigus registracijos laikui, administratorius gali sukurti balsų balsavimo blokų grandinės „Genesis“ (pirma) bloką.

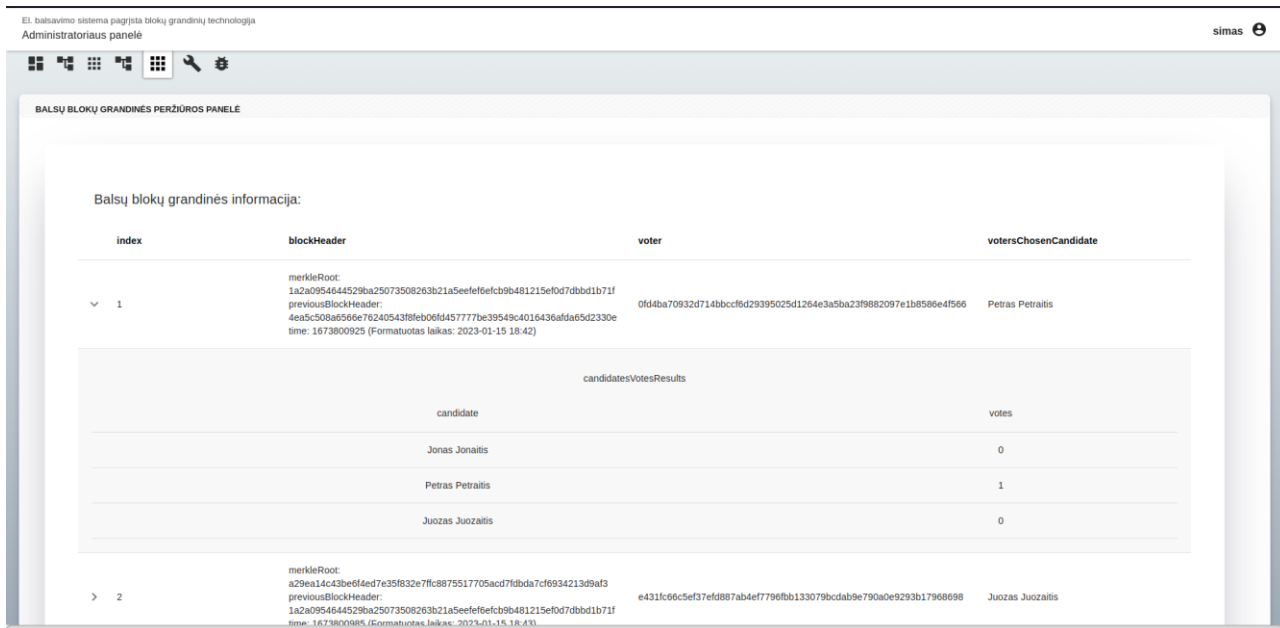


23 pav. Naudotojo sąsaja – Administratoriaus panelė (1)

24 pav. ir **25 pav.** pavaizduoti administratoriaus panelės, rinkėjų blokų grandinės peržiūros langai. **24 pav.** pateiktas pirmojo rinkėjų blokų grandinės peržiūros langas. **25 pav.** pavaizduotas likusių rinkėjų blokų grandinės blokų peržiūros langas, kuriame blokų informacija pateikiama lentelėje. Viena eilutė – vienas blokas.

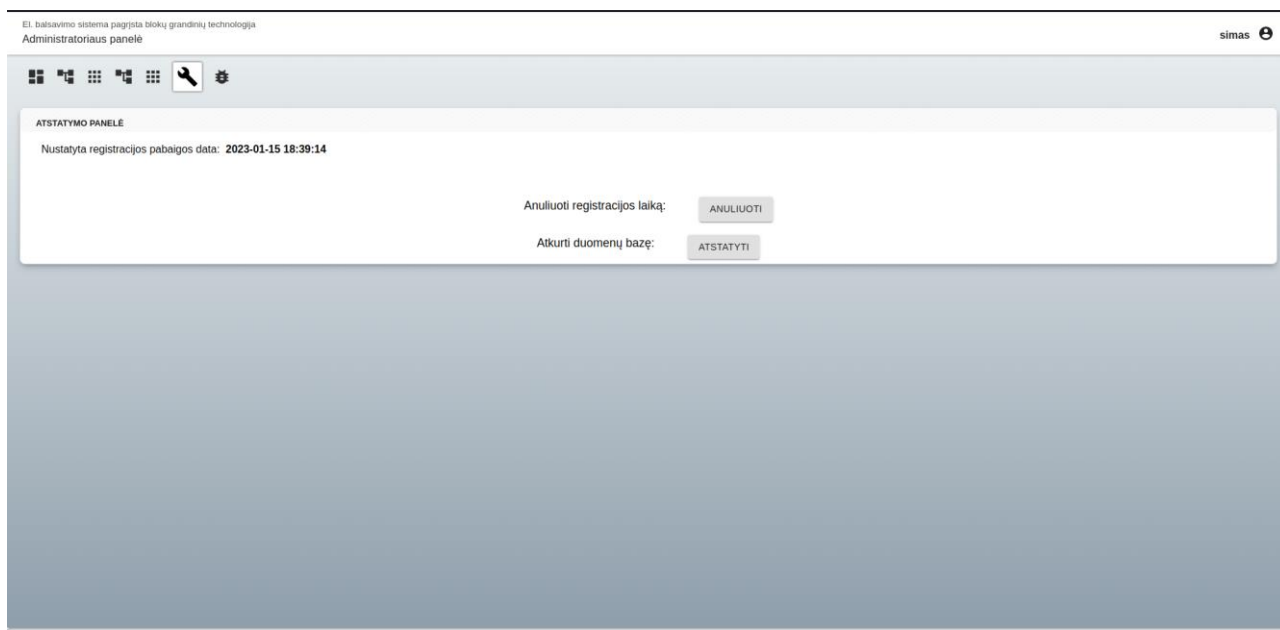


24 pav. Naudotojo sąsaja – Administratoriaus panelė (2)

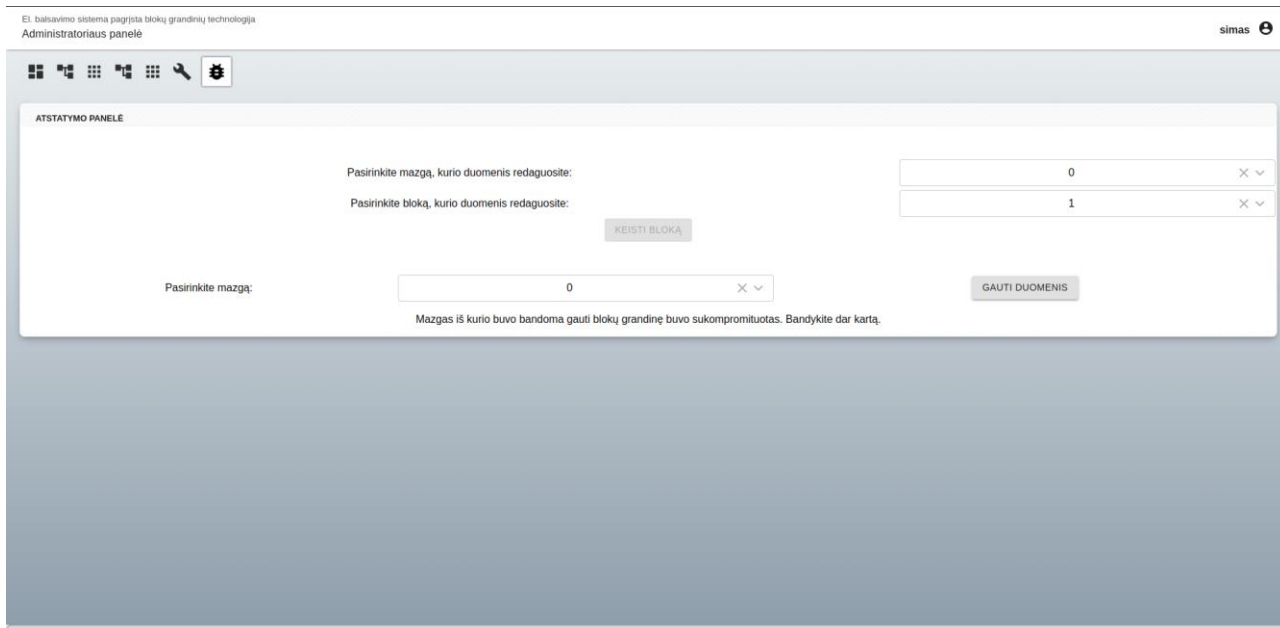


27 pav. Naudotojo sąsaja – Administratoriaus panelė (5)

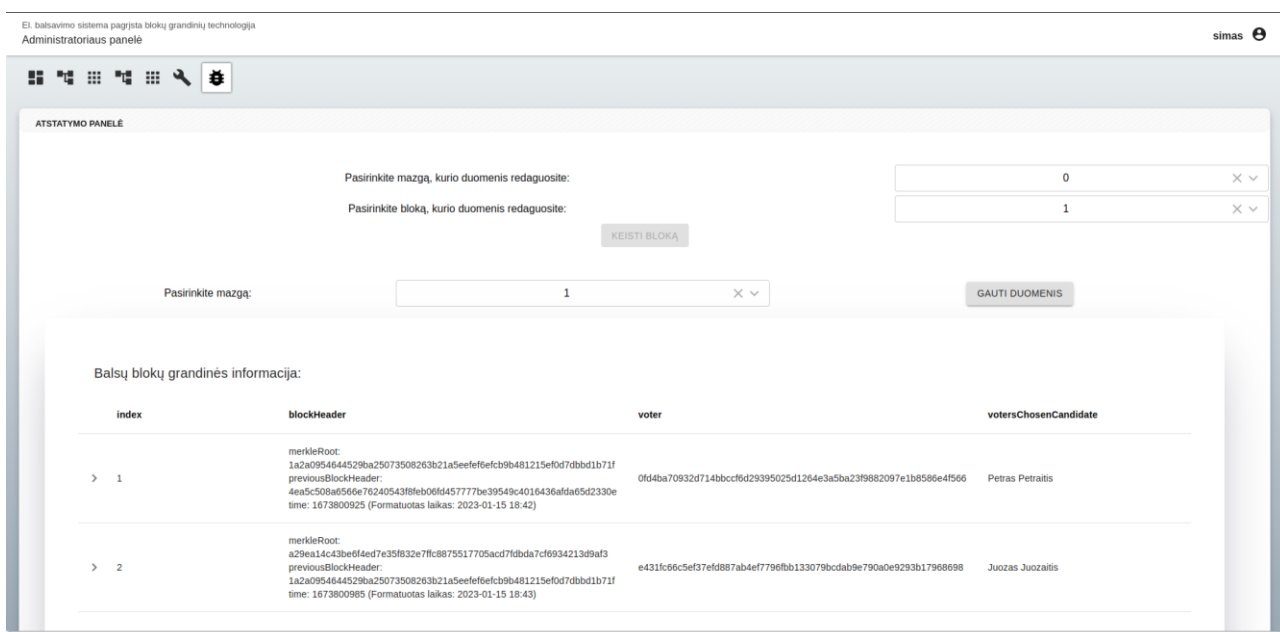
28 pav., 29 pav. ir 30 pav. pateikti administratoriaus panelės langai, kurie skirti sistemos demonstravimui ir testavimui. 28 pav. matomame lange atvaizduojami administratoriui skirti veiksmai, kuriais atkuriamas sistema – anuliuojamas registracijos laikas ir atkuriamas duomenų bazė į pradinę stadiją. 29 pav. ir 30 pav. matomi administratoriaus veiksmai, kuriais galima pakeisti pasirinktą balsų blokų grandinės bloką pasirinktame mazge, taip pažeidžiant visą blokų grandinę esančią tame mazge. Pasitikrinimui, kaip į tai reaguoja sistema, yra sukurtas veiksmas – galima pasirinkti norimą mazgą ir gauti jo blokų informaciją.



28 pav. Naudotojo sąsaja – Administratoriaus panelė (6)

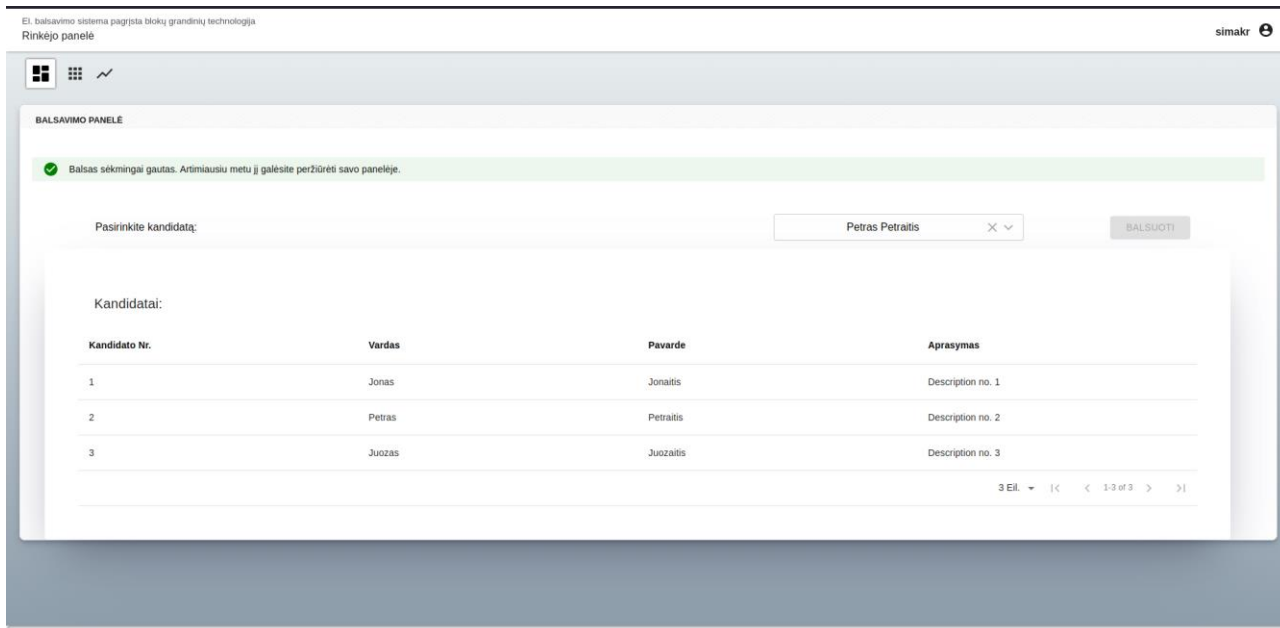


29 pav. Naudotojo sąsaja – Administratoriaus panelė (7)



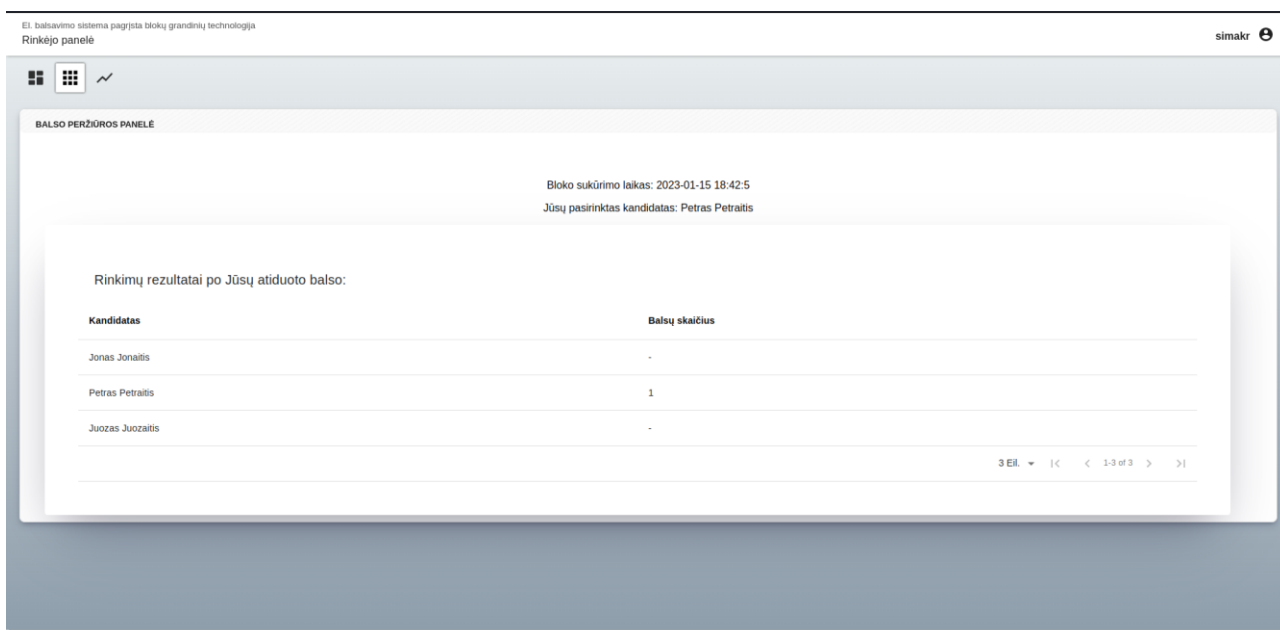
30 pav. Naudotojo sąsaja – Administratoriaus panelė (8)

31 pav. atvaizduota rinkėjo balsavimo panelė. Šioje vietoje rinkėjui pateikiama informacija apie kandidatus ir čia rinkėjas gali atiduoti savo balsą.



31 pav. Naudotojo sąsaja – Rinkėjo panelė (1)

32 pav. pavaizduotas rinkėjo panelės langas, kur rinkėjas gali paržiūrėti savo balso bloko informaciją (balsavimo datą, pasirinktą kandidatą ir bloke įrašytus rinkimų rezultatus po jo balso atidavimo).



32 pav. Naudotojo sąsaja – Rinkėjo panelė (2)

33 pav. pateiktas vaizdas, kaip atrodo rinkėjo panelės rinkimų rezultatų peržiūros langas einamuoju momentu. Rinkimų rezultatai gaunami iš paskutinio balsų blokų grandinės bloko.

RINKIMŲ REZULTATŲ PANELĖ

✓

Jei manote, kad Jūsų balsas nėra atvaizduojamas, patikrinkite "Balso peržiūros panelę" dėl detalesnės informacijos.

Rinkimų rezultatai einamuoju momentu:

Kandidatas	Balsų skaičius
Jonas Jonaitis	-
Petras Petraitis	1
Juozas Juozaitis	1

3 El. |< < 1-3 of 3 > >|

33 pav. Naudotojo sąsaja – Rinkėjo panelė (3)

3.5. Prototipo realizacijos dalies išvados

1. Realizuojant prototipą sukurtos dvi atskiros blokų grandinės – balsuotojų blokų grandinė ir balsų blokų grandinė.
2. Kiekvienai blokų grandinei sukurta atskira valdymo programa, skirta patogesniai prototipo testavimui ir demonstracijai (valdymui).
3. Siekiant vaizdžiai ir aiškiai parodyti prototipo veikimą ir realizaciją, pasinaudojant *ReactJS* karkasu buvo sukurta naudotojo sąsaja bei realizuoti pagrindiniai numatomi sistemos veiksmai.
4. Naudotojo sąsajoje sukurtas pasirinkto mazgo sukompromitavimo veiksmas, siekiant parodyti, kaip sistema reaguoja į mazgo blokų grandinės integralumo pažeidimą.

4. El. balsavimo sistemos, pagrįstos blokų grandinių technologija tyrimas

Šiame skyriuje pateikiamas kiekybinis ir kokybinis sukurtos elektroninės balsavimo sistemos, pagrįstos blokų grandinių technologija, tyrimas. Taip pat, sukurtas sprendimas trumpai aptariamas ir palyginamas su plačiai paplitusia ir naudojama, įprasta, MySQL duomenų baze.

4.1. Kokybinis tyrimas

Šioje tyrimo dalyje įsitikinama, kad sukurtas sprendimas atitinka iškeltus reikalavimus, t. y. užtikrina rinkėjų anonimiškumą, balsavimo skaidrumą ir vientisumą.

34 pav. galima matyti, kad balsų blokų grandinės pirmajame bloke saugomi nuasmeninti rinkėjo duomenys (rinkėjo duomenų maišos reikšmė). Taip pat, asmeninių duomenų nėra saugoma ir rinkėjo atiduoto balso bloke (žr. **35 pav.**).

```
GenesisBlock {
  blockHeader: BlockHeader {
    previousBlockHeader: null,
    merkleRoot: '4ea5c508a6566e76240543f8feb06fd457777be39549c4016436afda65d2330e',
    time: 1681949324
  },
  index: 0,
  voters: [
    {
      userDataHash: '0fd4ba70932d714bbccf6d29395025d1264e3a5ba23f9882097e1b8586e4f566',
      userSignature: '-----BEGIN PUBLIC KEY-----\n' +
        'MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDPiKaZhRc8xCn6n/+yBCcc9EqQ\n' +
        'mBuSsJVurEOCMYZNUiTRDu03PPV18tF53o7EnWo2oLwsCCq/6N10vJGPmnmwlyuf\n' +
        '5PD/AHzKwbU5sZ0KhfIuC7BvfBjLSXC9MsGvrmH/PVdTrjq3cQ+at7RfK60xj5jj\n' +
        'HsrFUCWWeTgQiGx3VwIDAQAB\n' +
        '-----END PUBLIC KEY-----\n',
      registrationTimestamp: 1681949300002
    },
    {
      userDataHash: 'e431fc66c5ef37efd887ab4ef7796fbb133079bcdab9e790a0e9293b17968698',
      userSignature: '-----BEGIN PUBLIC KEY-----\n' +
        'MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCZLGTkC5ucUiLrYectMGsU1AB4\n' +
        '+GRo/ijfuT07ZoViEl8utCGY53TnMmXeSqoFufMJx4ONlLDr8a5ggECHflrT2RJR\n' +
        'SMT2rkTmd2Dy4fr95Q25vILnKSKWDSXYK8Zx4nVPHan8Qvcr06D6PEE/iJRM1WQc\n' +
        'RXhCPBLCCufnAcMpbQIDAQAB\n' +
        '-----END PUBLIC KEY-----\n',
      registrationTimestamp: 1681949320004
    }
  ]
}
```

34 pav. Rinkėjo duomenų nuasmeninimas (1)

```
Block {
  blockHeader: BlockHeader {
    previousBlockHeader: '4ea5c508a6566e76240543f8feb06fd457777be39549c4016436afda65d2330e',
    merkleRoot: '3e4dda4e7cb91ba4780a12a1955ca741485b125eb42b031761f48166a03356d4',
    time: 1681949340
  },
  index: 1,
  voter: '0fd4ba70932d714bbccf6d29395025d1264e3a5ba23f9882097e1b8586e4f566',
  votersChosenCandidate: 'Jonas Jonaitis',
  votersSignature: '6a71f97e96018f27f9eab9642331c2f58f496488f428a695110fbf60b56ea3ba04c6f31f87e6591b928c25f1bdc5c6fbcc5dbb64e42965e0c08d9df40c6b\nf21b3a70aba425634087c70acf657b8b71e920a9d3830bf441b27b569e88f98f9d2df1598d6244848d69a5a1ae57429cd7b735e7cf6b841863ac3484de11f279a76a',
  candidatesVotesResults: [
    { candidate: 'Jonas Jonaitis', votes: 1 },
    { candidate: 'Petras Petraitis', votes: 0 },
    { candidate: 'Juozas Juozaitis', votes: 0 }
  ]
}
```

35 pav. Rinkėjo nuasmeninimas (2)

Balsavimo skaidrumas užtikrinamas taip, kad kiekvienas rinkėjas gali peržiūrėti savo balsą, t. y. gauti bloką kuriame yra įrašytas jo balsas. Tai atvaizduojama **36 pav.**

El. balsavimo sistema pagrįsta blokų grandinių technologija
Rinkėjo panelė simakr

BALSO PERŽIŪROS PANELĖ

Bloko sukūrimo laikas: 2023-04-20 3:09:0

Jūsų pasirinktas kandidatas: Jonas Jonaitis

Rinkimų rezultatai po Jūsų atiduoto balso:

Kandidatas	Balsų skaičius
Jonas Jonaitis	1
Petras Petraitis	-
Juozas Juozaitis	-

36 pav. Rinkėjo balso atvaizdavimas

Žinoma, vienas iš svarbiausių aspektų yra vientisumas. Įsitikinti, kad šis reikalavimas yra išpildytas, rankiniu būdu pakeičiama informacija pasirinktame blokų grandinės bloke. Tai padarius, bandoma gauti visą blokų grandinę ir stebima kaip į tai reaguoja sistema (žr. **37 pav.**).

Pasirinkite mazgą, kurio duomenis redaguosite:

Pasirinkite bloką, kurio duomenis redaguosite:

KEISTI BLOKĄ

Pasirinkite mazgą:

Pasirinkite visi mazgai

GAUTI DUOMENIS

Mazgas iš kurio buvo bandoma gauti blokų grandinę buvo sukompromituotas. Bandykite dar kartą.

Pasirinkti visi mazgai

1

37 pav. Mazgo blokų grandinės sukompromitavimas

Pateiktuose rezultatuose galima matyti, kad nėra įmanoma peržiūrėti blokų grandinės, kadangi sistema patikrinusi blokų grandinės integralumą aptiko pažeidimą. Todėl, siekiant išvengti netikslumų apie jį informuoja. Norint patobulinti metodą, galima būtų integruoti aptiktos pažeisto blokų grandinės mazgo priverstinį atjungimą nuo bendro tinklo arba priverstinį mazgo perkrovimą. Perkrovus mazgą, jis savyje pradėtų saugoti blokus iš naujo, nuo pradžių, kuriuos gautų siųsdamas užklausas į kitus tinkle egzistuojančius mazgus. Taip pat vertėtų apsvarstyti periodinį mazgų grandinių vientisumo patikrinimo realizavimą, taip iš anksto užkertant kelią pažeidimams, o galutinis naudotojas apie informacijos esančios mazge suklastojimą nežinotų.

Kalbant apie elektroninės balsavimo sistemos sprendimą, kuris yra realizuotas naudojant MySQL duomenų bazę, galima teigti, kad būtų sunku arba neįmanoma užtikrinti balsų vientisumo. Nors ir būtų galima sukurti tokią duomenų bazės struktūrą, kurioje būtų perskaičiuojamos ir saugomos prieš tai buvusių įrašų maišos reikšmės, tačiau DB būtų tik viena, t. y. būtų galima ne tik pakeisti įrašą duomenų bazėje, tačiau ir perskaičiuoti reikšmes bei pakeisti kitus įrašus. Priešingai – blokų

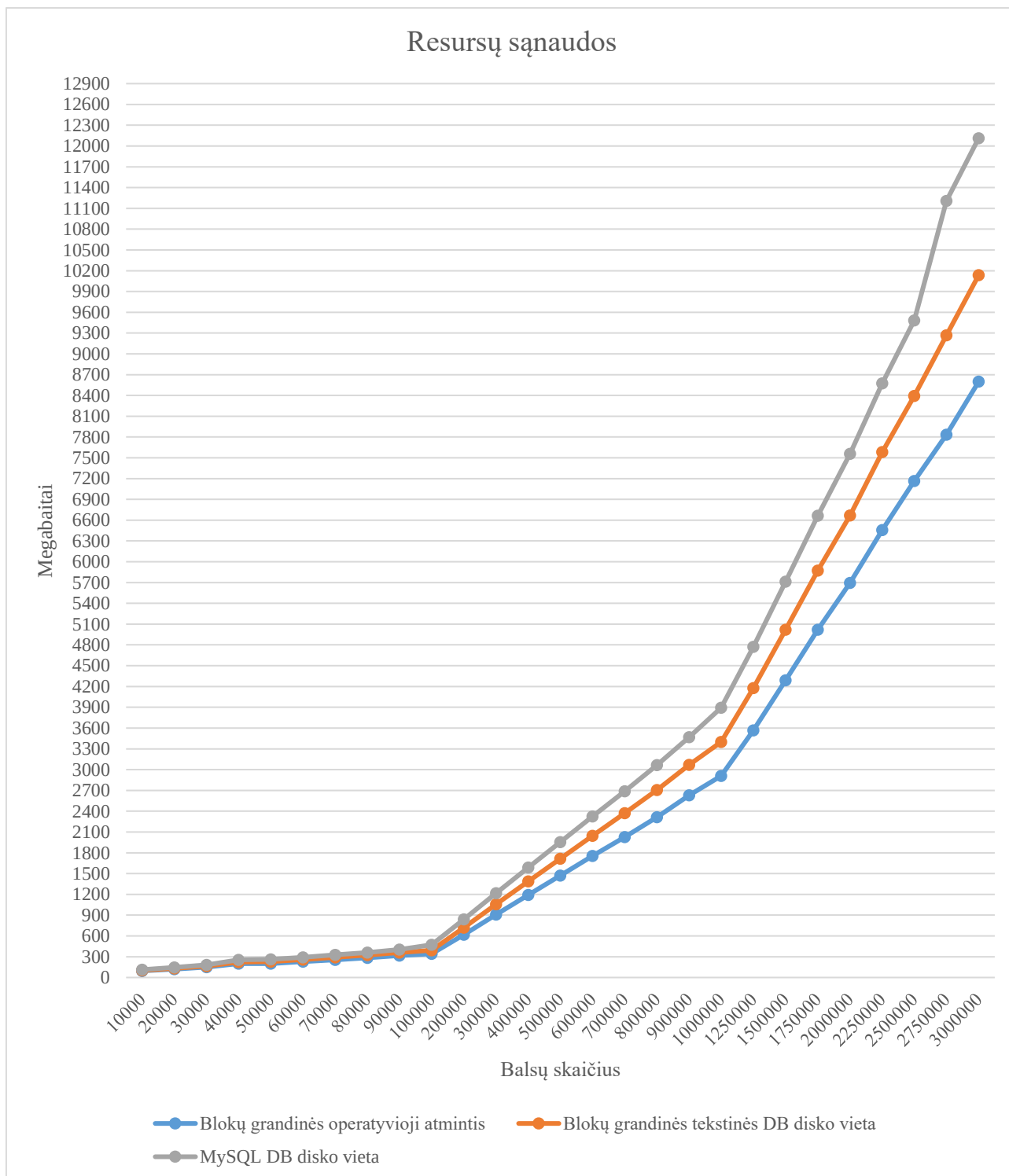
grandinės turi daug mazgų, kuriuose saugomi visi rezultatai, tokiu atveju yra praktiškai neįmano surasti, prisijungti ir pažeisti visus mazgus.

4.2. Kiekybinis tyrimas

Šio tyrimo metu, sukurto balsavimo sprendimo blokų grandinė užpildoma rinkėjų balsais nuo 10 tūkst. iki 3 mln. įrašų. Tuomet tikrinamas sunaudojamas operatyviosios atminties kiekis, tekstinei duomenų bazei sunaudojamas vidinės atminties kiekis, taip pat sparta atliekant tam tikrus veiksmus:

- atsitiktinio bloko (rinkėjo balso) parinkimas pagal bloko indeksą – lyginama tikrinant blokų grandinės integralumą ir to nedarant. Duomenys renkami iš tekstinės duomenų bazės ir blokų grandinės atmintyje atskirai.
- Atsitiktinio bloko (rinkėjo balso) parinkimas pagal rinkėjo maišos reikšmę – lyginama tikrinant blokų grandinės integralumą ir to nedarant. Duomenys renkami iš tekstinės duomenų bazės ir blokų grandinės atmintyje atskirai.
- Balsų perskaičiavimas – lyginama tikrinant blokų grandinės integralumą ir to nedarant. Perskaičiavimas atliekamas su tekstone duomenų baze ir blokų grandine, esančia operatyviojoje atmintyje atskirai.

Resursų sąnaudos buvo tiriamos blokų grandinę ir MySQL duomenų bazę (toliau – DB) pildant atsitiktinai generuojamais balsais bei stebint operatyviosios atminties sąnaudas ir tekstinei bei MySQL DB reikalingą vidinės atminties kiekį. Tyrimo rezultatai atvaizduoti **38 pav.**

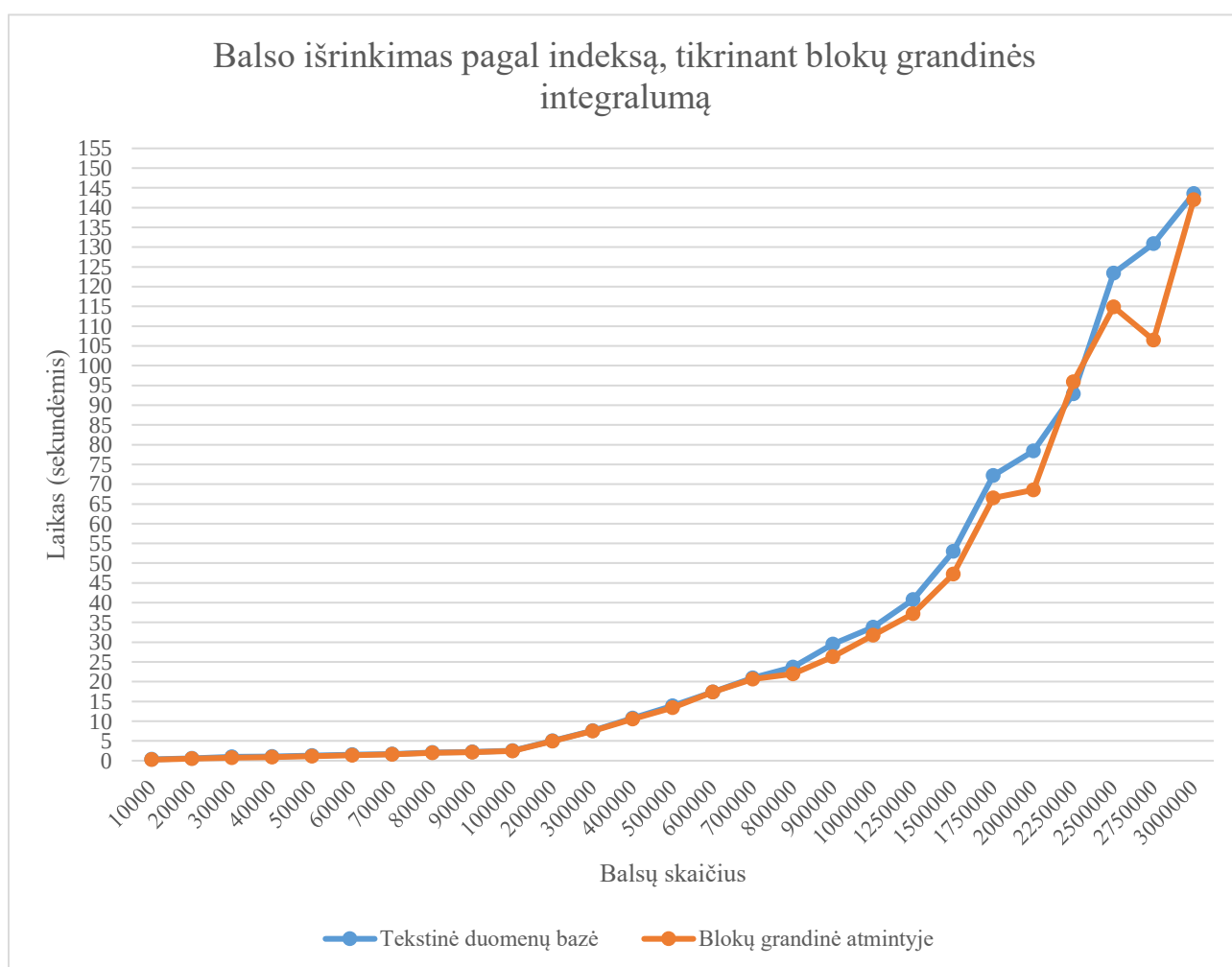


38 pav. Resursų sąnaudos

Minėtoje diagramoje galime matyti, kad tiek operatyviosios atminties, tiek disko sąnaudos auga stabiliai, lyginant su talpinamų balsų skaičiumi. Pagal esamą situaciją, 3 mln. rinkėjų balsų saugoti blokų grandinėje reikia apie 8 GB operatyviosios atminties. Žinant šiuolaikinius serverius, tai nėra bloga situacija, tačiau, esant reikalui, galima taikyti įvairius metodus ir sumažinti reikalingus resursus. Vienas iš pavyzdžių – kadangi blokų grandinė yra saugoma ir tekstinėje duomenų bazėje, taikyti operatyviosios atminties atlaisvinimą ir saugoti joje tik dalį paskutinių įrašų. O kitus įrašus, esant poreikiui, galima parinkti iš DB arba užkrauti į operatyviąją atmintį iš jos. Vertėtų pastebėti,

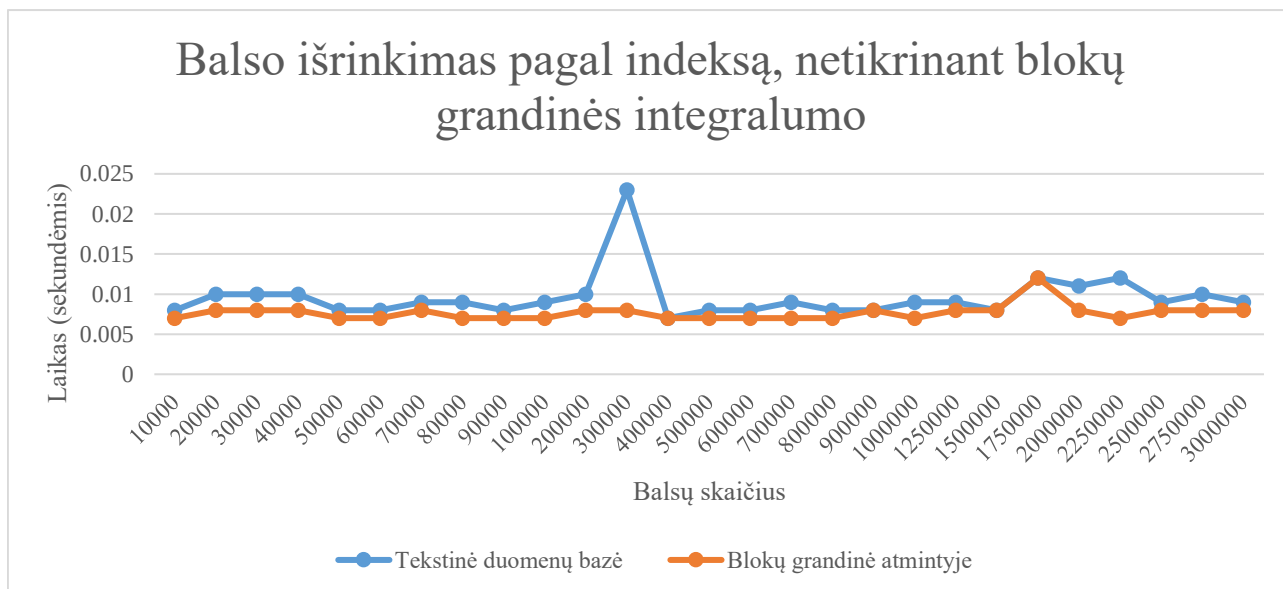
kad MySQL DB vidinės atminties sąnaudos yra didesnės, nei blokų grandinės tekstinės DB. Didesnis atotrūkis atsiranda, kai balsų skaičius viršija 100 tūkst. ribą. Reikėtų atsižvelgti į tai, kad įprastai sistemose būna naudojama tik viena duomenų bazė, taip pat daroma šios duomenų bazės atsarginė kopija. Šiuo atveju, sistemoje naudojant blokų grandinę, mazgų kiekis gali būti labai didelis, todėl sunaudojamos atminties kiekis ir vidinės atminties kiekis turėtų būti dauginamas iš mazgų skaičiaus. Atsižvelgiant į tai, bendros resursų sąnaudos augtų tolygiai, priklausomai nuo tinkle egzistuojančių mazgų kiekio, t. y., bendros visų mazgų resursų sąnaudos gali viršyti duomenų bazės resursų sąnaudas keliasdešimt ar net kelis šimtus kartų.

Kaip ir resursų tyrimas, taip ir visi sekantys tyrimai buvo atliekami didinant saugomų balsų skaičių blokų grandinėje. Diagramoje „Balso išrinkimas pagal indeksą, tikrinant blokų grandinės integralumą“ (žr. 39 pav.) galima matyti reikalingas laiko sąnaudas parinkti balsą pagal indeksą, tikrinant blokų grandinės integralumą.



39 pav. Balso išrinkimas pagal indeksą, tikrinant blokų grandinės integralumą

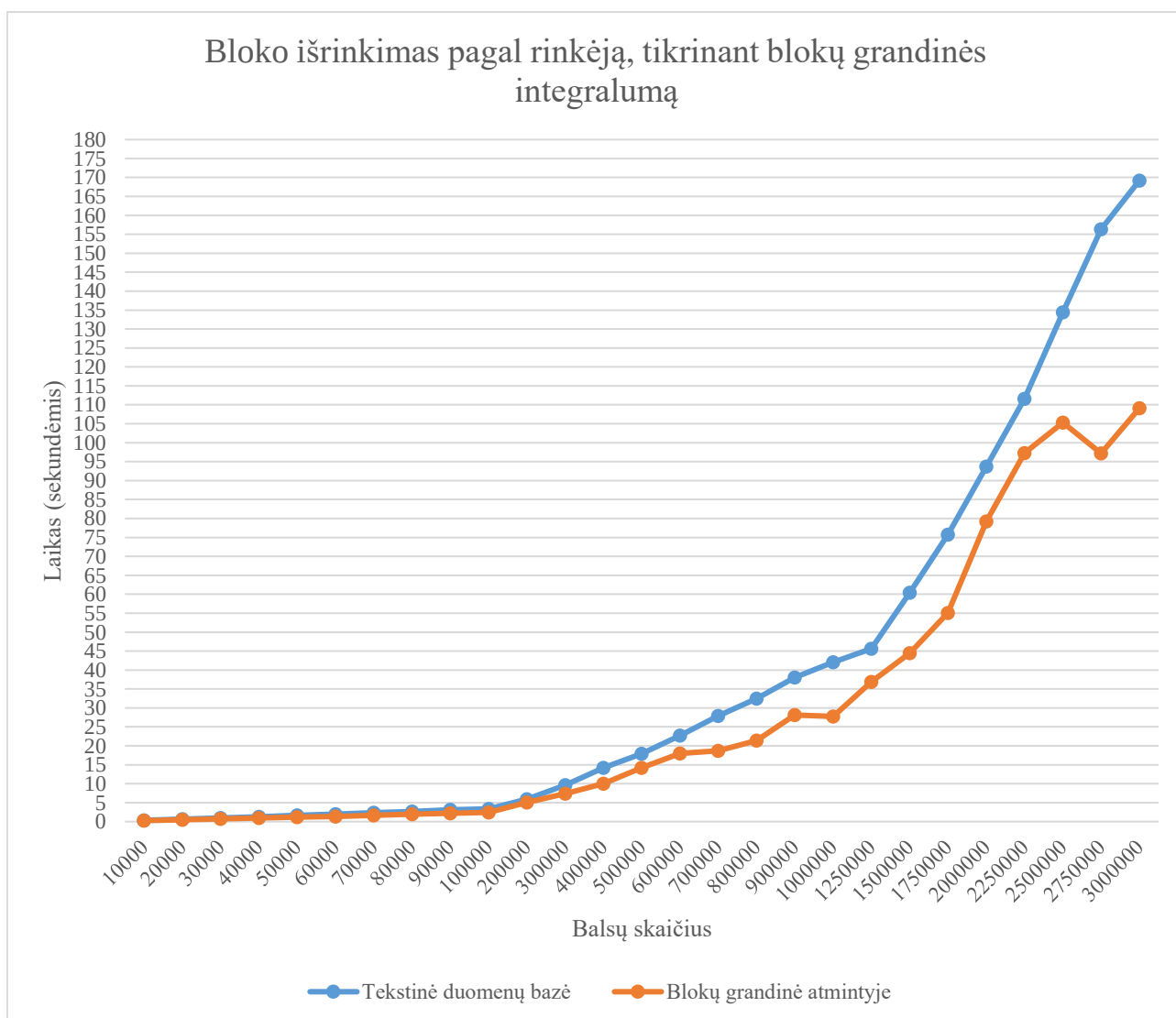
40 pav. matomos reikalingos laiko sąnaudos, siekiant parinkti balsą netikrinant blokų grandinės integralumo.



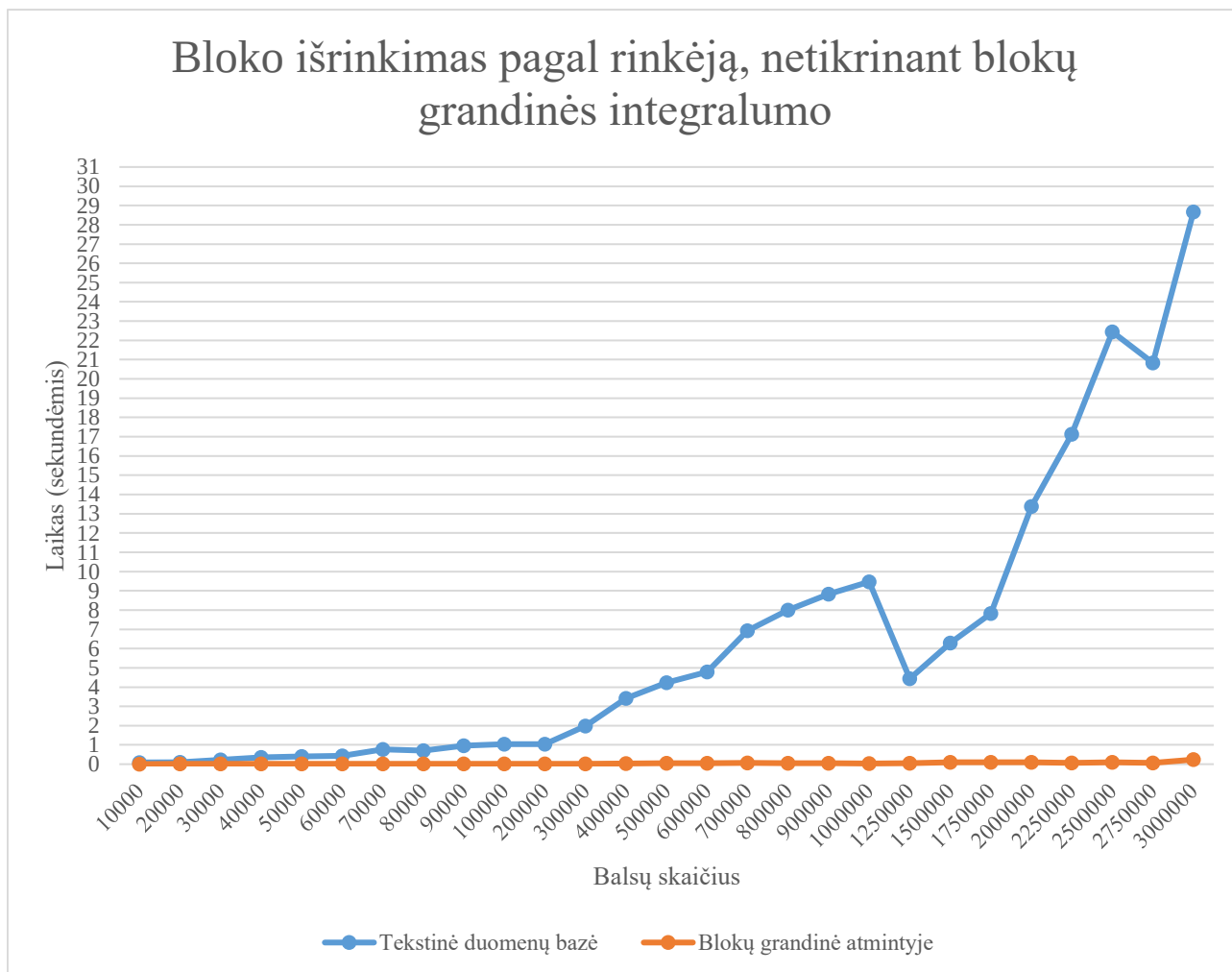
40 pav. Balso išrinkimas pagal indeksą, netikrinant blokų grandinės integralumo

Iš pateiktų diagramų galima matyti, kad balso paieškos laiko sąnaudos, tiek operatyviojoje atmintyje saugomoje blokų grandinėje, tiek tekstinėje duomenų bazėje, tikrinant ir netikrinant blokų grandinės integralumą yra labai panašios. Tačiau, kaip ir buvo galima numanyti, veiksmai su operatyviaja atmintimi atliekami greičiau, nei su tekstine duomenų baze. Didžiąją laiko sąnaudų dalį sudaro blokų grandinės integralumo tikrinimas, o ne balso paieška.

Dar vienas tyrimas buvo atliekamas skaičiuojant laiko sąnaudas, ieškant tam tikro rinkėjo balso (pagal rinkėjo duomenų maišos reikšmę). Tyrimas buvo atliekamas tiek tikrinant, tiek netikrinant blokų grandinės integralumą. Kaip ir paieška pagal indeksą, taip ir paieška pagal rinkėją buvo atliekama tiek su operatyviojoje atmintyje esančia blokų grandine, tiek su tekstine duomenų baze. Tyrimo rezultatai atvaizduoti **41 pav.** ir **42 pav.**



41 pav. Bloko išrinkimas pagal rinkėją, tikrinant blokų grandinės integralumą

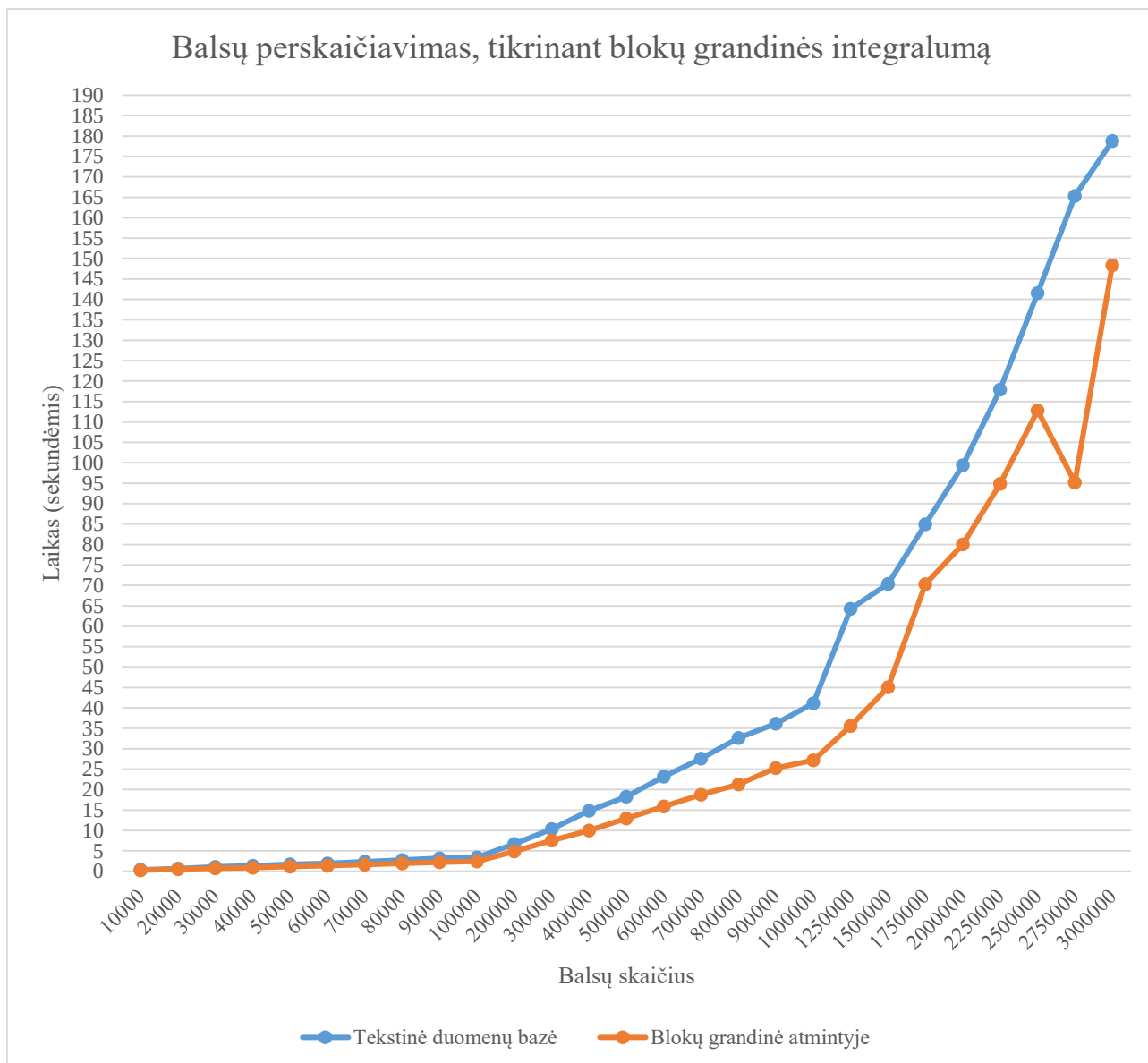


42 pav. Bloko išrinkimas pagal rinkėją, netikrinant blokų grandinės integralumo

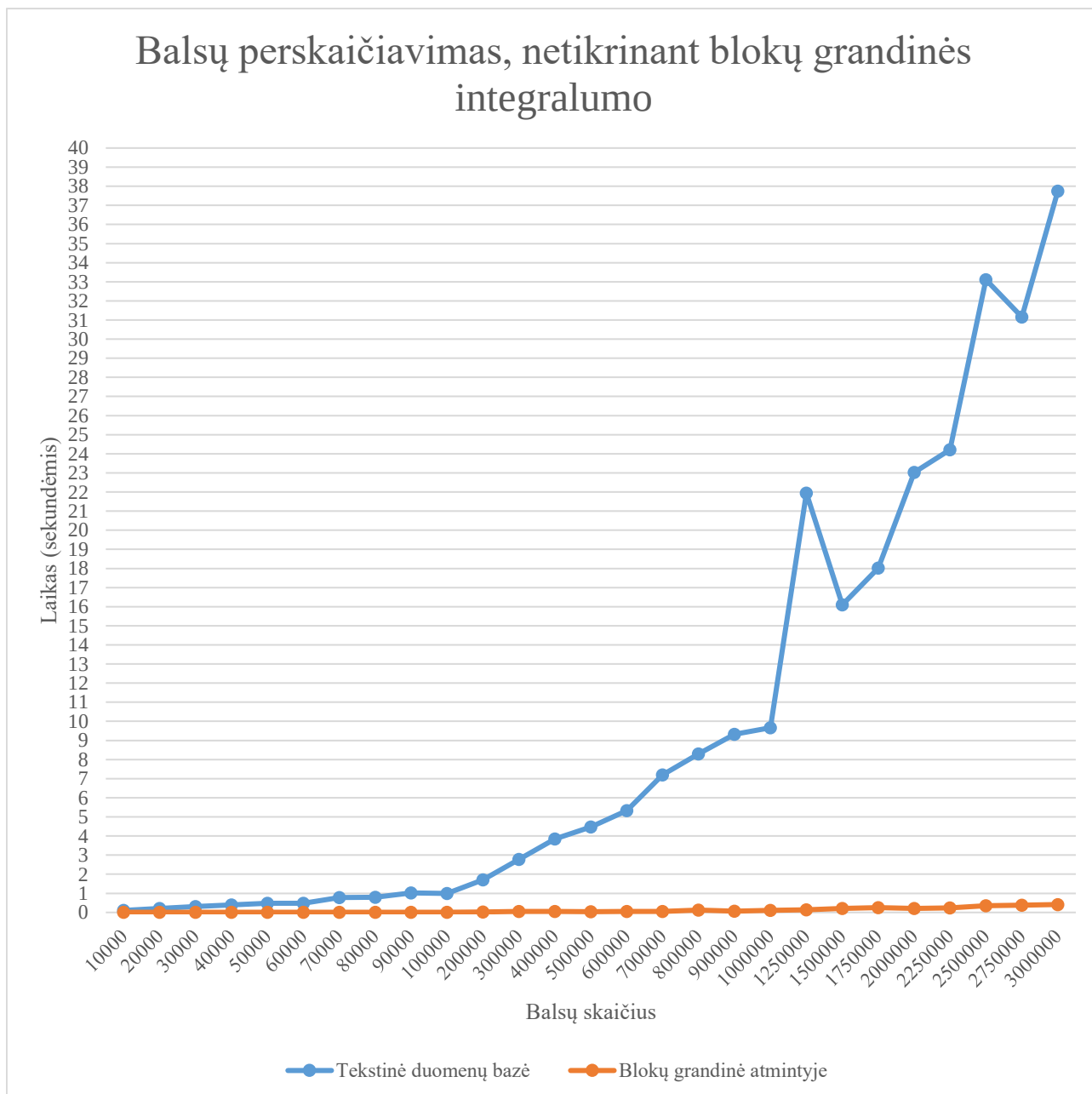
Šiuo atveju, priešingai nei ieškant rinkėjo balso pagal indeksą, galima matyti didesnę atotrūkį tarp paieškos operatyvioje atmintyje ir tekstinėje duomenų bazėje. Tačiau pasikartoja situacija, kai didžioji laiko sąnaudų dalis sudaryta iš blokų grandinės integralumo patikros, o ne balso paieškos.

Vertėtų paminėti, kad buvo ieškomi atsitiktiniai rinkėjų balsai, tačiau visi ieškomi balsai buvo sąlyginai blokų grandinės pabaigoje, taip siekiant gauti maksimalias galimas laiko sąnaudas, t. y. su prototipe realizuota paieška. Balso radimas netikrinant blokų grandinės integralumo ir balsui esant blokų grandinės pradžioje turėtų mažesnes laiko sąnaudas, nei yra atvaizduota diagramose. Vis dėl to, jeigu blokų grandinės integralumas būtų tikrinamas, laiko sąnaudos skirtųsi nežymiai, kadangi veiksmas priklausytų nuo blokų kiekio, o ne nuo bloko pozicijos grandinėje. Balsų paieška buvo atliekama tikrinant blokų grandinę iš eilės.

Dar vienas svarbus veiksmas, siekiant patikrinti ar paskutiniame bloke esantys balsai yra suskaičiuoti teisingai yra balsų perskaičiavimas. Šis tyrimo etapas taip pat buvo atliekamas su operatyvioje atmintyje esančia blokų grandine ir su tekstine duomenų baze, tikrinant blokų grandinės integralumą ir to nedarant. Rezultatai yra matomi **43 pav.** ir **44 pav.**



43 pav. Balsų perskaičiavimas, tikrinant blokų grandinės integralumą



44 pav. Balsų perskaičiavimas, netikrinant blokų grandinės integralumo

Rezultatai atskleidžia, kad veiksmai su atmintyje esančia blokų grandine yra atliekami greičiau, nei su tekstine duomenų baze. Žinoma, balsų perskaičiavimui galima taikyti kelis skirtingus metodus. Vienas iš jų – perskaičiuoti visus rinkėjų balsus, kaip tai buvo daroma aukščiau pateiktose diagramose. Esant užtikrintiems, kad balsų skaičiavimas sistemoje yra realizuotas teisingai ir patikimai, patikrinti blokų grandinės integralumą ir pasirinkti paskutinį blokų grandinėje esantį bloką. Pagal kurią elektroninės balsavimo sistemos, pagrįstos blokų grandinėmis metodu, kiekvienas rinkėjo balso blokas saugo perskaičiuotus einamuoju momentu esančius rinkimų rezultatus.

Iš atliktų tyrimų galima pastebėti, kad sukurtą metodą ir balsavimo sistemos prototipą būtų galima patobulinti pritaikant efektyvesnius paieškos metodus pvz.: paieškai pagal indeksą naudoti dvejetainę paiešką (angl. *binary search*). Bloko paiešką pagal rinkėją būtų galima atlikti iš pradžių atliekant

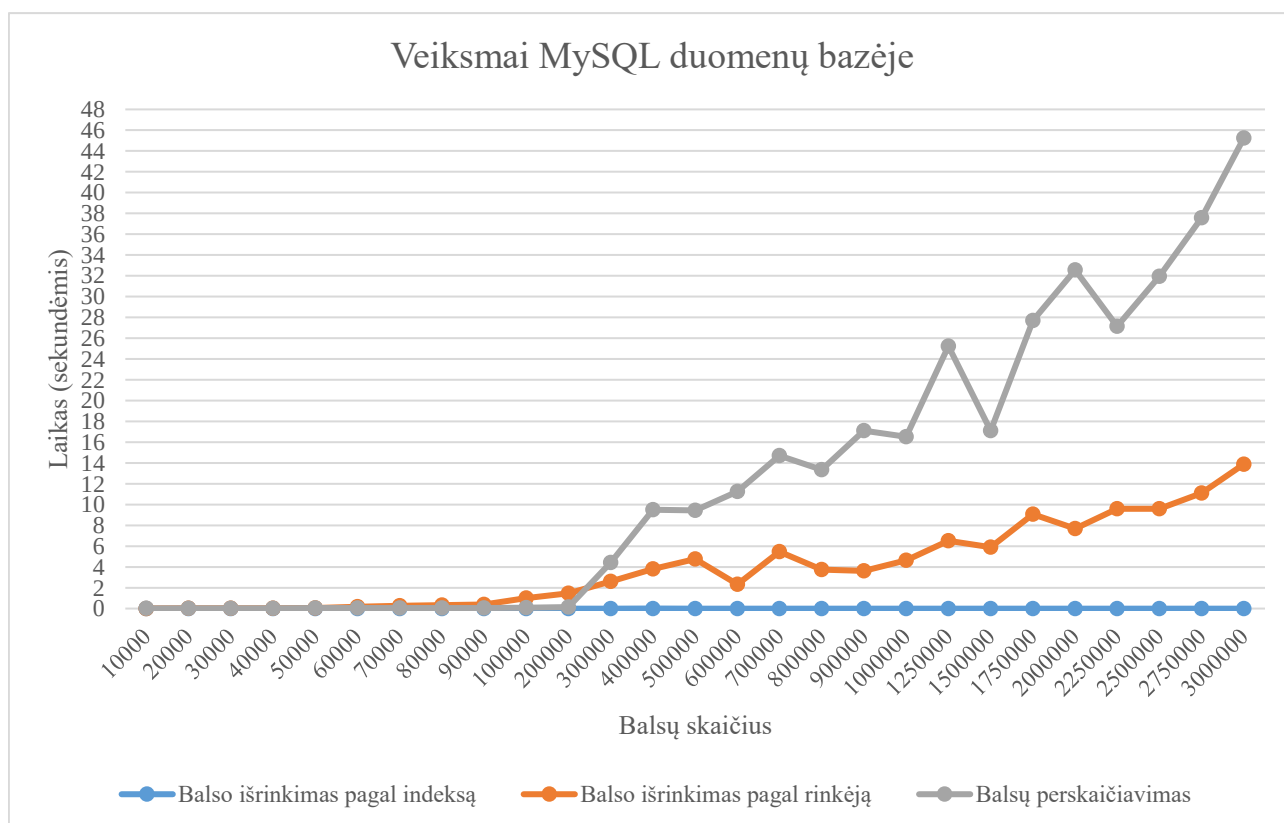
paiešką pagal laiką, taip sumažinant blokų aibę, kurioje reikia rasti rinkėjo maišos reikšmę. Žinoma, šiuo atveju turi būti žinomas ir pateikiamas rinkėjo balso pateikimo laikas.

Taip pat galima būtų pritaikyti blokų grandinės integralumo periodinį tikrinimą, tokiu atveju nereikėtų tikrinti blokų grandinės kiekvieną kartą, kai norima gauti tam tikro rinkėjo balso bloką. Šiuo atveju tekstinė duomenų bazė galėtų pasitarnauti siekiant atskirti tam tikrus veiksmus, atliekamus su blokų grandine. Pavyzdžiui, balsų paieškai, rezultatų tikrinimui ir panašioms veiksmams atlikti būtų galima naudotis tekstinėmis mazgų duomenų bazėmis, taip sumažinant apkrovą, kai yra įrašomi rinkėjų balsai, skaičiuojamos blokų grandinei reikalingos maišos reikšmės, tikrinami rinkėjų parašai.

Siekiant įvertinti ir geriau suprasti, kad blokų grandinės nėra pats efektyviausias ir greičiausiai veikiantis sprendimas, palyginimui rinkėjo balsų paieškos ir balsų perskaičiavimo operacijos buvo atliktos ir MySQL duomenų bazėje. Vertėtų paminėti, kad balsams saugoti buvo sukurta duomenų bazės lentelė, kurioje buvo 4 stulpeliai:

- id – balso id;
- voter – nuasmenintas rinkėjas (rinkėjo duomenų maišos reikšmė);
- votersChosenCandidate – pasirinktas rinkėjo kandidatas (rinkėjo balsas);
- signedData – balsas pasirašytas rinkėjo privačiu raktu.

Tyrimo rezultatai pateikti **45 pav.**

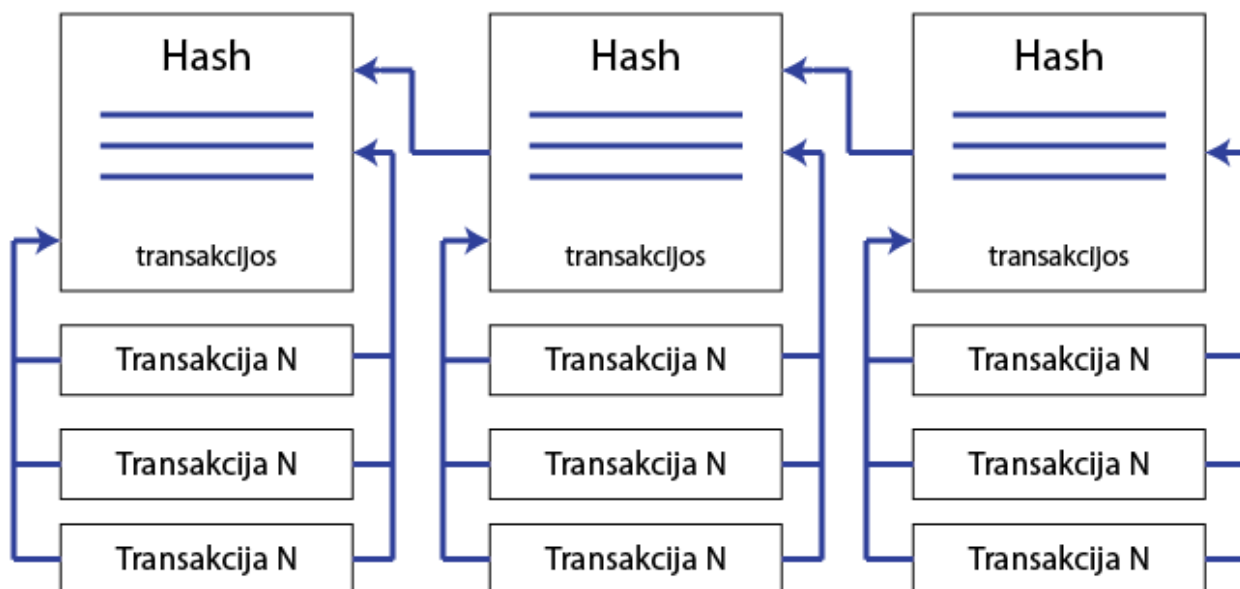


45 pav. Veiksmai MySQL duomenų bazėje

Kaip buvo minėta, veiksmas duomenų bazėje yra atliekamas greičiau, nei blokų grandinėje, tačiau elektroninės balsavimo sistemos sprendimo įgyvendinimas naudojant įprastą MySQL duomenų bazę kelia kitų rizikų, kurios aptartos **4.1** poskyryje.

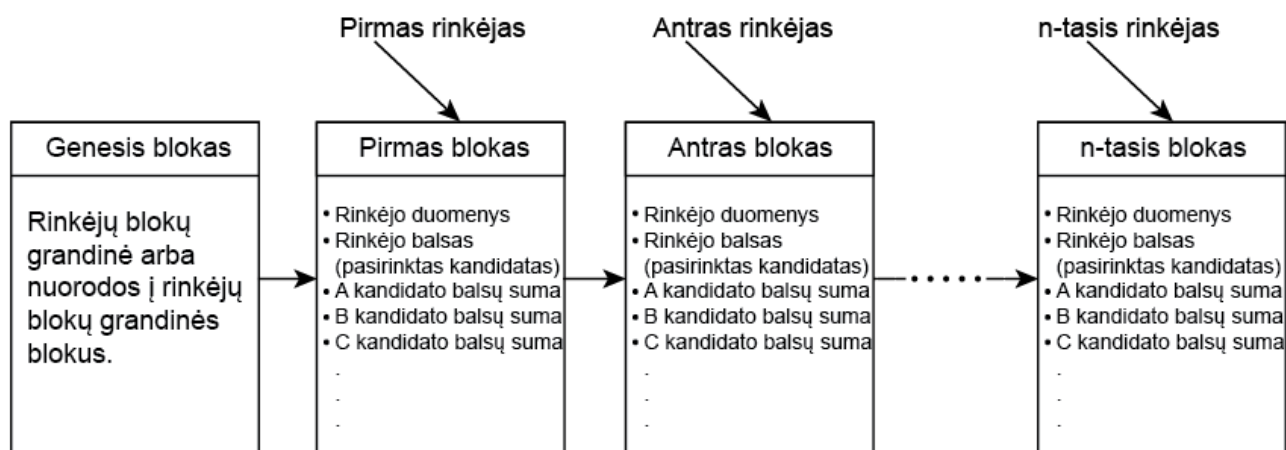
4.3. Prototipo blokų grandinės struktūros palyginimas su įprasta blokų grandinės struktūra

Įvairūs sprendimai, nepriklausomai ar tai būtų kriptovaliutos, balsavimo sistemos, ar kito tipo sistemos, pagrįstos blokų grandinėmis, jos visos dažniausiai turi vienodą blokų grandinės struktūrą. Kiekvienas blokas sudaromas iš n transakcijų skaičiaus. Tik užpildžius ir patvirtinus vieną bloką pradedamas pildyti sekantis, kurį sudaro identiškas transakcijų skaičius. Detalesnę struktūrą galima matyti **46 pav.**



46 pav. Standartinė blokų grandinės struktūra

Siūlomas sprendimas ir sukurtas prototipas ženkliai skiriasi savo blokų grandinės struktūra. Siūloma, kad kiekvieną bloką sudarytų atskiras rinkėjo atiduotas balsas ir einamieji rinkimų rezultatai. Tokiu būdu būtų sumažinamas kiekvieno bloko dydis, palengvinama rinkėjo atiduoto balso paieška – tai reikalinga siekiant turėti galimybę, kad rinkėjas įsitikintų, jog jo balsas buvo įrašytas teisingai. Vertėtų paminėti ir tai, kad siūlomo sprendimo atveju blokų grandinę sudarytų didesnis kiekis blokų. Detalesnę balsų blokų grandinės struktūrą galima matyti **47 pav.**



47 pav. Siūlomo sprendimo balsų blokų grandinės struktūra

Siūlomo sprendimo elektroninei balsavimo sistemai, pagrįstai blokų grandinių technologija, rinkėjų blokų grandinės ir balsų blokų grandinės plačiau aprašytos **2.3** poskyryje.

4.4. Tyrimo dalies išvados

1. Prototipo tyrimas leido nustatyti, kad bandant gauti bloką iš grandinės, kurios integralumas pažeistas, to padaryti nepavyks. Sistema informuos, kad grandinės integralumas yra pažeistas ir rinkimų rezultatai suklustoti. Priešingu atveju, naudojant MySQL duomenų bazę integralumo užtikrinti nepavyks.
2. Tyrimas buvo atliekamas pildant balsų blokų grandinę ir MySQL duomenų bazės lentelę įrašais nuo 10 tūkst. iki 3 mln. Vieno mazgo vidinės atminties sąnaudos yra mažesnės nei MySQL duomenų bazės vidinės atminties sąnaudos, tačiau blokų grandinė reikalauja sąlyginai didelio operatyviosios atminties kiekio.
3. Atsižvelgiant į tai, kad blokų grandinės tinkle mazgų kiekis gali būti labai didelis, bendros mazgų resursų sąnaudos augtų tolygiai mazgų skaičiui, t. y., blokų grandinės resursų sąnaudos gali viršyti duomenų bazės resursų sąnaudas keliasdešimt ar net kelis šimtus kartų.
4. Tyrimo metu nustatyta, kad didžiausias laiko sąnaudas atliekant veiksmus su blokų grandine sudaro blokų grandinės integralumo tikrinimas.
5. Prototipas reikalauja didelių operatyviosios atminties sąnaudų, tačiau blokų grandinė saugoma ir tekstinėje duomenų bazėje, vidinėje atmintyje, todėl siekiant pagerinti veikimą, būtų galima saugoti tik dalį blokų grandinės atmintyje, o visus reikiamus veiksmus atlikti su tekstine duomenų baze.
6. Tyrimo metu pastebėta, kad veiksmų atlikimas su tekstine duomenų baze užtrunka ilgiau nei su operatyviaja atmintimi, tačiau veiksmai su DB gali būti atliekami atskiru procesu, taip neapkraunant kitų blokų grandinės veiksmų.

Išvados

1. Apžvelgus Lietuvos Respublikos Seimo rinkimų procesą buvo nustatyti esminiai rinkimų reikalavimai, apibrėžta rinkimų organizavimo tvarka, rinkėjų ir kandidatų sudarymo tvarka, kandidatų kėlimas, rinkimų parengtinės veiklos, balsavimo ir balsų skaičiavimo procesas.
2. Atlikus tradicinių balsavimo būdų analizę, pastebėta, kad tradicinis, popierinis balsavimas neužtikrina saugaus ir nesuklastoto balsavimo. Šiuolaikinės elektroninės balsavimo sistemos negali užtikrinti keturių esminių principų – skaidrumo, anonimiškumo, privatumo ir vientisumo.
3. Suprojektuota elektroninė balsavimo sistema, pagrįsta blokų grandinių technologija. Sistemos projekte pateikta idėja, naudojanti dvi atskiras blokų grandines, viena – rinkėjų duomenims saugoti, antroji – veikianti kaip balsadėžė – balsams saugoti.
4. Siekiant sistemą visapusiškai pritaikyti elektroniam balsavimui buvo suprojektuota nestandartinė balsų blokų grandinė – kiekviename bloke saugoma ne tam tikras transakcijų skaičius, o vienas blokas – vieno balso principu veikianti blokų grandinė.
5. Prototipe buvo realizuotos dvi blokų grandinės – rinkėjų blokų grandinė ir balsų blokų grandinė. Blokų grandinėms sukurtos atskiros valdymo programos ir bendra naudotojo sąsaja, skirtos patogesniai sistemos testavimui ir demonstravimui.
6. Atlikus prototipo kokybinį tyrimą, nustatyta, kad sistema informuoja naudotoją, jeigu blokų grandinės mazgo integralumas buvo pažeistas.
7. Kiekybinis tyrimas parodė, kad blokų grandinės vidinės atminties sąnaudos yra mažesnės, nei MySQL duomenų bazės vidinės atminties sąnaudos. Tačiau atsižvelgiant į tai, kad blokų grandinės tinkle mazgų kiekis gali būti labai didelis, bendros mazgų resursų sąnaudos augtų tolygiai mazgų skaičiui, t. y., blokų grandinės resursų sąnaudos gali viršyti duomenų bazės resursų sąnaudas keliasdešimt ar net kelis šimtus kartų.
8. Kiekybinio tyrimo metu nustatyta, kad prototipas reikalauja didelio kiekio operatyviosios atminties. Atsižvelgiant į realizacijos principą, galimas problemos sprendimas yra saugoti tik dalį blokų operatyviojoje atmintyje, kadangi visa blokų grandinė yra papildomai saugoma tekstinėje duomenų bazėje.
9. Tyrimo metu pastebėta, kad didžiausias veiksmų su blokų grandine laiko sąnaudas sudaro integralumo tikrinimas t. y., vieno iš pagrindinių blokų grandinių principų užtikrinimas.

Literatūros sąrašas

1. [1] “Lietuvos Respublikos Seimo rinkimų įstatymas.” [žiūrėta 2022-03-28] Prieiga per: <https://e-seimas.lrs.lt/portal/legalActPrint/lt?jfwid=oizvyndl&documentId=TAIS.1536&category=TAD>
2. [2] “I-balsavimo koncepcijos modelis.” [žiūrėta 2022-03-28] Prieiga per: <https://e-seimas.lrs.lt/rs/legalact/TAP/TAIS.280219/>
3. [3] “Electronic Voting Systems —.” [žiūrėta 2021-11-19] Prieiga per: <https://aceproject.org/ace-en/topics/et/eth/eth02/eth02b/eth02b1>
4. [4] “Punch Card Voting Device | Wisconsin Historical Society.” [žiūrėta 2022-01-16] Prieiga per: <https://www.wisconsinhistory.org/Records/Article/CS2717>
5. [5] “Optical scanning machines are susceptible to miscounting U.S. voter ballots,” *VentureBeat*, Nov. 01, 2020. [žiūrėta 2022-01-16] Prieiga per: <https://venturebeat.com/2020/11/01/optical-scanning-machines-are-susceptible-to-miscounting-u-s-voter-ballots/>
6. [6] T. W. Lauer, “The risk of e-voting,” *Electronic Journal of e-Government*, vol. 2, pp. 177–186, 2004. [žiūrėta 2022-01-16] Prieiga per: <https://academic-publishing.org/index.php/ejeg/article/view/417>
7. [7] D. P. Moynihan, “Building Secure Elections: E-Voting, Security, and Systems Theory,” in *In: Public Administration Review* 64/5, 2004, pp. 515–528. [žiūrėta 2022-01-16] Prieiga per: <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1540-6210.2004.00400.x>
8. [8] “What Are Residual Votes? - Voting Machines - ProCon.org,” *Voting Machines*. [žiūrėta 2022-01-16] Prieiga per: <https://votingmachines.procon.org/questions/what-are-residual-votes/>
9. [9] A. Al-Ameen and S. Talab, “The Technical Feasibility and Security of E-Voting,” vol. 10, no. 4, p. 8, 2013. [žiūrėta 2022-01-20] Prieiga per: <https://www.iajit.org/PDF/vol.10%2Cno.4/4313.pdf>
10. [10] F. Þ. Hjálmarsson and G. K. Hreiðarsson, “Blockchain-Based E-Voting System,” p. 10. [žiūrėta 2022-01-20] Prieiga per: https://www.researchgate.net/profile/Mohammad_Hamdaqa/publication/327812253_Blockchain-Based_E-Voting_System/links/5ce1fff1458515712eb69dcd/Blockchain-Based-E-Voting-System.pdf
11. [11] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, “Blockchain,” *Bus Inf Syst Eng*, vol. 59, no. 3, pp. 183–187, Jun. 2017, doi: 10.1007/s12599-017-0467-3. [žiūrėta 2022-01-20] Prieiga per: <http://cs.unibo.it/~danilo.montesi/CBD/Articoli/2017Blockchain.pdf>
12. [12] “What is blockchain?,” *Journal of Accountancy*, Jul. 01, 2017. [žiūrėta 2021-11-19] prieiga per: <https://www.journalofaccountancy.com/issues/2017/jul/what-is-blockchain.html>
13. [13] S. Chandler, “Proof of stake vs. proof of work: key differences between these methods of verifying cryptocurrency transactions,” *Business Insider*. [žiūrėta 2022-01-16] Prieiga per: <https://www.businessinsider.com/personal-finance/proof-of-stake-vs-proof-of-work>
14. [14] “Proof of Work (PoW),” *Investopedia*. [žiūrėta 2022-01-16] Prieiga per: <https://www.investopedia.com/terms/p/proof-work.asp>
15. [15] “Proof of Stake Definition,” *Investopedia*. [žiūrėta 2022-01-16] Prieiga per: <https://www.investopedia.com/terms/p/proof-stake-pos.asp>
16. [16] B. Tavares, F. F. Correia, A. Restivo, J. P. Faria, and A. Aguiar, “A Survey of Blockchain Frameworks and Applications,” in *Proceedings of the Tenth International Conference on Soft*

- Computing and Pattern Recognition (SoCPaR 2018)*, vol. 942, A. M. Madureira, A. Abraham, N. Gandhi, C. Silva, and M. Antunes, Eds. Cham: Springer International Publishing, 2020, pp. 308–317. doi: 10.1007/978-3-030-17065-3_31. [žiūrēta 2022-01-16] Prieiga per: <https://arxiv.org/ftp/arxiv/papers/1903/1903.12553.pdf>
17. [17] “Best Blockchain Frameworks You Should Know About,” *Merehead*. [žiūrēta 2022-01-16] Prieiga per: <https://merehead.com/blog/blockchain-frameworks-you-should-know-about/>
 18. [18] M. Quasim, M. Khan, F. Algarni, A. Alharthy, and G. Alshmrani, “Blockchain Frameworks,” 2020, pp. 75–89. doi: 10.1007/978-3-030-38677-1_4. [žiūrēta 2022-01-16] Prieiga per: https://www.researchgate.net/profile/Mohammad_Quasim2/publication/339250474_Blockchain_Frameworks/links/5e6d2e3f299bf12e23c738e6/Blockchain-Frameworks.pdf
 19. [19] “Smart Contracts,” *Corporate Finance Institute*. [žiūrēta 2021-12-11] Prieiga per: <https://corporatefinanceinstitute.com/resources/knowledge/deals/smart-contracts/>
 20. [20] “R3 - CryptoMarketsWiki.” [žiūrēta 2022-01-16] Prieiga per: <https://crypto.marketswiki.com/index.php?title=R3>
 21. [21] U. Jafar, M. J. A. Aziz, and Z. Shukur, “Blockchain for Electronic Voting System—Review and Open Research Challenges,” *Sensors*, vol. 21, no. 17, Art. no. 17, Jan. 2021, doi: 10.3390/s21175874. [žiūrēta 2022-01-16] Prieiga per: <https://www.mdpi.com/1424-8220/21/17/5874>
 22. [22] K. Curran, “E-Voting on the Blockchain,” *The Journal of the British Blockchain Association*, vol. 1, pp. 1–6, Dec. 2018, doi: 10.31585/jbba-1-2-(3)2018. [žiūrēta 2022-01-16] Prieiga per: <https://jbba.scholasticahq.com/article/4451.pdf>
 23. [23] “POLYS.KASP.ENG_leaflet.pdf.” [žiūrēta 2022-01-16] Prieiga per: https://www.kaspersky.com/ihub/assets/POLYS.KASP.ENG_leaflet.pdf
 24. [24] “Blockchain Voting: The End To End Process,” *Follow My Vote*. [žiūrēta 2022-01-16] Prieiga per: <https://followmyvote.com/blockchain-voting-the-end-to-end-process/>
 25. [25] “13EMB_Priit_Vinkel.pdf.” [žiūrēta 2022-02-19] Prieiga per: https://www.venice.coe.int/files/13EMB/13EMB_Priit_Vinkel.pdf
 26. [26] D. Clarke and T. Martens, “E-voting in Estonia,” *arXiv:1606.08654 [cs]*, Jun. 2016, [žiūrēta 2022-02-19] Prieiga per: <http://arxiv.org/abs/1606.08654>
 27. [27] A. Lastovetska, “Blockchain Architecture Explained: How It Works & How to Build.” [žiūrēta 2022-05-01] Prieiga per: <https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture>