VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
PROGRAMŲ SISTEMŲ KATEDRA

Ethereum blokų grandinės technologijos tinkamumas elektroniniam balsavimui

Ethereum blockchain for electronic voting

Bakalauro baigiamasis darbas

Atliko: 4 kurso 1 grupės studentas
Lukas Kairys (parašas)

Darbo vadovas: lekt. Andrius Adamonis (parašas)

Vilnius – 2017

TURINYS

Santrauka

Elektroninis balsavimas - tai sritis, kurioje vieningo, saugaus ir užtikrinto technologinio sprendimo dar nėra atrasta. Šio darbo tikslas yra ištirti decentralizuotos viešos transakcijų saugojimo sistemos (toliau „blockchain“) pritaikymą elektroniniame balsavime. Buvo iškelti pagrindiniai uždaviniai: išanalizuoti blokų grandinės technologijos savybes, ištirti bei aprašyti blockchain technologijos realizacijos Ethereum tinklo bei išmaniųjų kontraktų savybes, įvertinti blokų grandinės technologijos tinkamumą iškeltoms balsavimo taisyklėms bei sukurti programos modelį bei prototipą. Šiuo darbu autorius atrado sprendimą galintį patenkinti iškeltas elektroninio balsavimo taisykles. Galima teigti, jog Ethereum blockchain yra tinkama technologija užtikrinti keliamus saugumo bei panaudojamumo reikalavimus. Sukurtą modelį bei prototipą bus galima naudoti kaip gaires tolimesniems veiksmams.

Įvadas

Kasmet įvairaus masto rinkimams sunaudojama daugybė žmogiškųjų resursų, yra didelė tikimybė žmogiškosioms klaidoms bei rezultatų skaičiavimas užtrunka gana ilgai. Lietuvoje rinkimų laikotarpiu vis dažniau kalbama apie elektroninį balsavimą, jo aktualumą bei trūkumus, kurie stabdo inovacijas šioje srityje. Pasaulyje tik kelios šalys taiko ar bandė taikyti elektroninio balsavimo sprendimus, todėl ši sritis yra nauja ir galimybių naujovėms yra nemažai. Taigi, autorius nusprendė savo darbu išanalizuoti šią temą.

Elektroninio balsavimo analizei bei sprendimui įgyvendinti buvo pasirinkta blokų grandinės technologija dėl keleto esminių priežasčių. Blockchain naudojama kaip duomenų bazė, kuri yra globali ir atvira bei duomenys saugomi transakcijų pavidalu. Tai garantuoja duomenų nepakeičiamumą bei atvirumą. Taip pat kodas, aprašytas kontrakte, yra viešas ir vykdomas visų tinklo dalyvių. Tai užtikrina kontrakte įdėtų taisyklių vieningą interpretaciją, o tuo pačiu – taisyklėmis išpildomų sprendimų atvirumą ir saugumą.

Autorius teigia ir savo tyrime įrodys, kad blokų grandinės technologija yra tinkama elektroninio balsavimo įgyvendinimui. Elektroninis balsavimas pasižymi šiomis savybėmis: balsuoti gali tik užsiregistravę rinkėjai, vienas rinkėjas gali atiduoti ne daugiau kaip vieną balsą, balsavimas anonimiškas, negalimi balsų pakeitimai iš išorės jokio kito asmens apart rinkėjo. Autorius tai įrodys lygindamas dabartinį fizinį balsavimo procesą bei sukurtą sprendimą elektroniniam balsavimui kartu su pasirinkimo argumentais. Taip pat bus atliktas sprendimo vertinimas pagal aprašytas taisykles. Uždaviniai šiam tikslui pasiekti:

1. Ištirti bendrąsias blockchain technologijos savybes, aprašomas literatūroje.
2. Palyginti sprendimą, paremtą blockchain technologija, su sprendimu, paremtu centrine duomenų baze.
3. Išanalizuoti blockchain technologijos Ethereum realizacijos bei išmaniųjų kontraktų savybes.
4. Apibrėžti saugaus elektroninio balsavimo taisykles.
5. Aprašyti elektroninio balsavimo veikimo modelį, paremtą blockchain technologija, bei jį įvertinti pagal apibrėžtas taisykles.
6. Pademonstruoti elektroninio balsavimo veikimą, sukuriant programos prototipą, veikiantį Ethereum blockchain technologijos pagrindu.

Pagal iškeltus uždavinius sudarytas darbo tyrimo metodas. Metodą sudaro šie žingsniai:

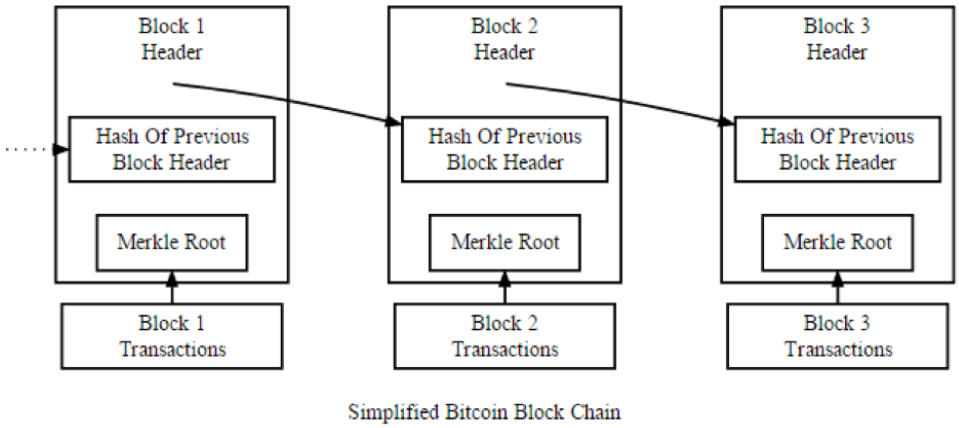
1. Mokslinės literatūros analizė. Atliekama literatūros analizė, kuri apibrėš pagrindinius pasirinktos technologijos bruožus.
2. Palyginimas su kitu technologiniu sprendimu. Remiantis ištirtomis savybėmis pirmame

žingsnyje, detaliai palyginami sprendimai.

3. Norint sukurti taikymo modelį bei prototipą, atliekama literatūros analizė konkrečios pasirinktos technologijos realizacijos bei vertinamos galimybes taikymui.
4. Išanalizuojamos taisyklės, kuriomis remiantis turėtų būti sukurtas veikimo modelis bei prototipas.
5. Išanalizavus, atliekamas procesų tarp dabartinio bei kuriamo sprendimo palyginimas bei argumentuojami kuriamo sprendimo pasirinkimai.
6. Aprašius veikimo modelį, atliekamas vertinimas pagal iškeltas taisykles bei reikalavimus, tam kad būtų galima įvertinti technologijos tinkamumą iškeltam taikymui.
7. Pagal sukurtą veikimo modelį, rašoma programa, kuri įgyvendins aprašytą modelį ar jo dalį.
8. Atliekamas bandymas parašytos programos, tikrinamas veikimas, atliekami kaštų skaičiavimai.

1. Blockchain technologija

Blockchain - decentralizuota transakcijų saugojimo sistema. Tai reiškia, kad sandoriai nėra fiksuojami jokio tarpininko. Nėra trečiosios šalies, pavyzdžiui, finansinės institucijos, kuri saugotų sandorių įrašus. Visas transakcijų sąrašas yra saugomas pas visus tinklo dalyvius. Specialistai teigia, jog joje gali būti saugomi duomenys apie lėšų pervedimus, išduotas paskolas ar nuosavybės informaciją [Ker15]. Pagrindinis šios technologijos privalumas - jog informacijos joje suklastoti ar sukeisti yra neįmanoma. Kiekvienas blokas, kuriame skaitmeninių įrašų pavidalu užfiksuotos naujausios transakcijos, jungiasi prie prieš tai įrašyto bloko chronologine tvarka ir taip sudaro blokų grandinę. Kiekvienas naujas blokas talpinamas tik į grandinės galą (žr. 1 pav.) ir savyje turi praėjusio bloko santrauką [MIC15]. Pagrindiniai šios technologijos saugumo aspektai: atvirumas, saugumas bei galimybė decentralizuoti duomenų saugojimą.



1 pav. Blokų grandinė

1.1. Decentralizacijos galimybės

Blockchain sistemą sudaro nepriklausomi serveriai - tinklo dalyviai, kurių kiekviename saugoma duomenų kopija. Šie kompiuteriai yra sujungti tinkle be jokio specialaus ryšio ir gali veikti iš bet kurios pasaulio vietos. Atlikdami matematines operacijas jie užtikrina, jog transakcija buvo atlikta teisingai. Patekus naujai transakcijai į vieną iš kompiuterių, ji yra paskleidžiama po tinklą. Tuomet tinklo dalyviai matematiškai patikrina transakciją, įtraukią į bloką ir priklausomai nuo taikomo konsensuso algoritmo atlieka matematinius skaičiavimus tam, kad galėtų patvirtinti visą naują duomenų bloką. Pirmas tinko dalyvis atradęs sprendimą, jį išsiunčia kitiems tinklo dalyviams, kurie patikrinę bloką ir patvirtinę įtraukia į savo blokų grandinę. Pasiekus sutarimą daugiau nei tam tikram kiekiui tinklo dalyvių, blokų grandinė laikoma teisinga. [Li16]. Pažeisti sistemą yra praktiškai neįmanoma, kadangi reikėtų atjungti visus kompiuterius tinkle. Kol yra bent vienas

veikiantis kompiuteris - veikia ir visa sistema. Taigi vis daugiau naujų kompiuterių prisijungiant prie sistemos yra plečiamas ir stiprinimas tinklas. Blokų grandinės specialistų nuomone, pagrindinis privalumas - visi vartotojai yra lygiateisiai ir nėra vienos valdančios dalies, kuri kontroliuotų ir būtų atsakinga už visus duomenis [Jef16].

1.2. Atvirumas

Kiekviena transakcija atlikta sistemoje yra sukuriama tinklo dalyvių, patvirtinama ir įrašomą į bendrą blokų duomenų grandinę. Realiu laiku galima stebėti tinkle atliktas transakcijas. Kiekvienas tinklo dalyvis gali matyti, kiek ir kokių yra atliktų transakcijų vieno dalyvio, bet negali jo identifikuoti realiame gyvenime [McC15]. Tai reiškia, jog visos transakcijos tampa atviros ir tiesiog nėra duomenų, kuriuos reikėtų vogti, kadangi viskas ir taip laisvai pasiekiama.

1.3. Apsauga

Apsauga ir patikimumas yra pagrįstas matematiniais skaičiavimais ir algoritmais. Technologija remiasi viešo rakto kriptografija. Kiekviena transakcija yra pasirašoma transakcijos kūrėjo privačiu raktu. Taip atsiranda galimybė greitai patikrinti duomenų autentiškumą, ar jie nebuvo modifikuoti siuntimo metu, naudojantis paskelbtu viešu raktu. Knygos „Mastering Bitcoin“ autorius teigia, jog siekiant sufalsifikuoti įrašus esančius blokų grandinėje, įsilaužėlis turėtų taip pažeisti kriptografiją, jog daugiau nei pusė kompiuterių tinkle priimtų neteisingą sprendimą ir patvirtintų šią transakciją [Ant14]. Šifravimo metodai naudojami siekiant užtikrinti informacijos konfidencialumą, vientisumą ir autentiškumą.

1.4. Konsensuso algoritmas

Norint decentralizuotai nuspręsti, kokie įrašai turėtų būti įtraukti į blokų grandinę, turi būti demokratinis būdas tą atlikti. Tam reikalingos taisyklės tarp dalyvių, kurios apibrėžtų, kaip tinkle bus balsuojama ir kokiu algoritmu remiantis bus priimami sprendimai. Pagrindinė problema yra ta, jog gali egzistuoti keletas skirtingų blokų grandinės šakų, kadangi kiekvienas kasėjas (angl. „miner“) tinkle gali turėti skirtingą paskutinį bloką, kurį nori įtraukti į bendrą blokų grandinę. Siekiant išspręsti šią problemą ir nuspręsti, kuris blokas yra validus, yra reikalingas konsensuso algoritmas. Reikalingas būdas, kuris leistų decentralizuotai priimti sprendimą, kuri šaka yra teisinga ir turėtų būti patvirtinta. Tai yra sudėtinga problema, kuri buvo iškelta anksčiau, kaip Bizantijos generolų problema. Kaip grupėje žmonių ar kompiuterių priimti vieningą sprendimą esant apribotiems šių

sąlygų:

1. Dalis tinklo dalyvių gali būti nepatikimi ir gali sukčiauti.
2. Bendravimo kanalas tarp dalyvių yra nesaugus.
3. Negali būti jokio centrinio taško, kuris priimtų sprendimus. Viskas turi būti atlikta taip, jog nereikėtų niekuo pasitikėti.

Aprašome keturis variantus pasiekti konsensusą esant šioms sąlygoms, kuriuos gali įgyvendinti blokų grandinės technologija.

1.4.1. Darbo įrodymo (Proof of work)

Šis algoritmas yra labai paprastas ir buvo kurtas su mintimi įrodyti, jog tikriausiai buvo atliktas didelis kiekis matematinių operacijų. Dažniausiu atveju ji įgyvendinama naudojant kriptografinę maišos funkciją. [ZXD16] Pats algoritmas bendruoju atveju veikia taip:

1. Turime dalį duomenų (pavyzdžiui transakcijų sąrašą).
2. Tuomet reikia ieškot antros duomenų dalies, kurią sujungus su pirma ir įvykdžius maišos funkciją yra gaunama tam tikrus reikalavimus atitinkanti reikšmė, kaip pavyzdžiui tam tikras skaičius iš eilės einančių nulių.
3. Tinkle pavykus vienam dalyviui atrasti šią reikšmę, jis paskleidžia rezultatą į tinklą [Mur16].
4. Kiti tinklo dalyviai privalo kartu patvirtinti šio bloko tikrumą. Transakcijos naujajame bloke yra validuojamos siekiant apsisaugoti nuo apgavystės bei suvienodinti visų tinklo dalyvių turimus duomenis.
5. Transakcijos, kurios buvo naudojamos skaičiavimuose yra patvirtintos ir šis naujas blokas įrašomas į blokų grandinę. [Pil15]

Visa algoritmo stiprybė yra tame, kad yra neįmanoma nuspėti, kokia antra duomenų dalis sugeneruos reikiamą maišos reikšmę, tad reikia atsitiktinai perrinkti visas galimas reikšmes iki kol bus gauta tinkama reikšmė. Vienas iš pagrindinių trūkumų šio algoritmo yra tai, jog jis yra lėtas. Priklausomai nuo realizacijų, vidutiniškai vieną bloką iškasti užtrunka apie 10 minučių. Tačiau norint būti visiškai tikriems, kad blokas yra įtrauktas ir galutinis, pavyzdžiui Bitcoin tinkle yra laukiama, kol bus sugeneruoti dar papildomi šeši blokai, kas reikš, jog blokas, esantis prieš kitus šešis sekoje, yra validus. Taigi, dėl šios priežasties norint pagrįstai patvirtinti transakcijų sąrašą, yra reikalinga iki valandos laiko. [Pil16]

Decentralizuotame tinkle gali nutikti taip, jog keli validūs blokai gali būti sugeneruoti skirtingų tinklo dalyvių atrandant riekiamą maišos reikšmę panašiu metu. Šiuo atveju gali būti sugeneruojamos kelios šakos tinkle. Tai labai retas atvejis, ir dažniausiai įvairiose realizacijose grandinė,

kuri būna ilgesnė, yra laikoma autentiška. Pavyzdžiui turime paskutinį validų bloką numeriu 80, kurį yra patvirtinę visi tinklo dalyviai. Atsitinka taip, jog trys dalyviai sugeneruoja tris naujus blokus 81a, 81b, 81c ir paskleidžia juos po tinklą. Tarkime tinklo dalyvis pamatęs 81b bloką pradeda formuoti 82b bloką. Tačiau netikėtai gauna 81a bloką. Dalyvis jį stebi, ir vis dar dirba ties 82b bloku. Tuomet jis gauna naują validų bloką 82a. Pagal šią ilgiausios grandinės taisyklę, kasėjas pakeičia trumpesnę grandinę (..80, 81b) į ilgesnę (..80, 81a, 82a) ir toliau dirba ties 83a bloku. Taip tinkle yra decentralizuotai išsprendžiami konfliktai. [ZXD16]

1.4.2. Įtakos tinkle (Proof of stake)

Šis algoritmas buvo pasiūlytas kaip alternatyva darbo įrodymo konsensuso algoritmui. Tikslas jo atsiradimui - trumpesnis blokų grandinės patvirtinimo laikas. Vietoje to, kad liepti tinklo dalyviams atlikti skaičiavimus beribėje erdvėje, įtakos tinkle algoritmas prašo vartotojų įrodyti turimą pinigų (įtakos) kiekį tinkle. [Pil15] Daroma prielaida, jog žmonės su daugiau pinigų tinkle bus mažiau linkę pulti tinklą bei bandyti pažeisti esančius duomenis. Parinkimas pagal turimą pinigų kiekį tinkle gali atrodyti nesąžiningas, kadangi vienas turtingiausias dalyvis tinkle yra dominuojantis ir gali priimti sprendimus. Yra pasiūlyta daugiau sprendimų, kurie atsižvelgia ir į kitus faktorius papildomai. Pavyzdžiui Peercoin tinklas papildomai vertina ir turimų pinigų amžių.[ZXD16]

Palyginimui su darbo įrodymo algoritmu, įtakos tinkle algoritmas sutaupo energijos ir yra daug efektyvesnis. Kita vertus, kadangi blokų tvirtinimo kaštai yra praktiškai verti nulio, tinklo atakos gali vykti kaip natūrali pasekmė.

Vietoje to, kad būtų dalinami blokai tolygiai pagal jų maišos funkcijų radimo greitį (jų kompiuterių skaičiavimo galią), įtakos tinkle algoritmas paskirsto blokus atitinkamai pagal turimą įtaką tinkle.

1.4.3. Paskirstytos įtakos tinkle (Delegated proof of stake)

Kaip ir įtakos tinkle algoritmas, šis algoritmas paskirsto prioritetą generuoti blokus pagal turimą kiekį pinigų tinkle. Pagrindinis skirtumas tarp šių algoritmų, jog paskirstytos įtakos tinkle konsensuso sprendimas paremtas galios perdavimu tinklo dalyvių išrinktiems kandidatams. Su ženkliai mažesniu dalyvių, kurie validuoja blokus, jie gali būti patvirtinti daug greičiau. Tai lemtų ir greitesnį transakcijų patvirtinimą. Papildomai tinklo dalyviai gali būti ramūs dėl nesąžiningų delegatų dalyvių, kadangi jie paprasčiausiai gali būti išbalsuoti.[ZXD16]

Algoritmo veikimo principas:

1. Tinklo dalyviai išrenka bet kokį kiekį dalyvių generuoti blokus.

2. Kiekvienas dalyvis turi vieną balsą, kurį gali skirti vienam iš išrinktų blokus generuojančių dalyvių.
3. Išrenkamas kiekis N išrinktų dalyvių, kurie gavo daugiausia balsavimo galios.
4. Kuomet akcininkai išrenka savo norimą kiekį balsuojančiųjų, jie turi taip pat ir balsuoti už tiek pat blokus generuojančių dalyvių.
5. Kiekviena kartą sugeneravus bloką, dalyviams yra sumokama už šią paslaugą.
   [Bit16]

1.4.4. Praktinė tolerancijos klaidoms (Practical byzantine fault tolerance)

Šis konsensuso algoritmas gali atlaikyti iki 1/3 žalingų blokų grandinės kopijų. Kitais žodžiais tariant, šis algoritmas užtikrina, kad mažiausiais 2*f + 1 (kur f - žalingų dalyvių skaičius) tinklo dalyvių turi priimti vienodą sprendimą prieš prijungiant transakcijas prie bendrojo įrašų sąrašo. Pritaikius šią formulę pavyzdžiui tinklui, kuriame transakcijas tvirtina 4 dalyviai, ši taisyklė maksimaliai galėtų toleruoti f=(4-1)/3=1 žalingą tinklo dalyvį. Jei egzistuoja du ar daugiau žalingų dalyvių, šis algoritmas negali užtikrinti duomenų integralumo bei vientisumo tarp tinklo dalyvių. Pavyzdžiui, norint toleruoti du žalingus dalyvius, reikėtų tinkle esančių vienetų skaičių padidinti iki 7. [blu16] Jei mažiau nei 3 vienetai yra prisijungę tinkle, blokų grandinė nustoja prijunginėti transakcijas į bendrą sąrašą. Taip yra dėl to, jog šis algoritmas negali užtikrinti duomenų vientisumo. Transakcijos bus toliau įrašinėjamos, kuomet bus daugiau nei 3 dalyviai prisijungę į tinklą. Šis atidėjimas sinchronizacijoje tarp tinklo dalyvių yra neišvengiamas ribojimas bet kokiame Praktinės tolerancijos klaidoms algoritme. [ZXD16]

1.5. Blockchain tipai pagal teisių struktūras

Blockchain realizacijos gali turėti skirtingas teisių struktūras. Pagrindiniai klausimai yra:

1. Kas gali rašyti į transakcijų sąrašą?
2. Kas gali skaityti duomenis iš transakcijų sąrašo?
3. Kas gali vykdyti konsensuso algoritmus duomenų integralumui ir teisingumui užtikrinti?

1.5.1. Privatus

Privatus blokų grandinės tinklas gali būti apibrėžiamas kaip tinklas, su apribota teise skaityti bei rašyti duomenis. Taip pat tik pasirinkta dalis dalyvių prižiūri bei vykdo konsensuso algoritmus ir užtikrina teisingus duomenis. [Jen17] Siekiant valdyti tas teises, jos yra saugomos centralizuotai vienoje organizacijoje. Skaitymo teisės gali būti viešos arba apribotos pasirinktinai. Tikėtina, kad

tokios aplikacijos bus naudojamos organizacijos viduje ir viešas duomenų skaitymas išvis nebus reikalingas. Kitais atvejais norint audituoti duomenis, išorinis skaitomumas gali būti reikalingas. [But15] Privačiame tinkle išlieka didelė rizika, jog duomenys gali būti pakeisti, jei tik didžioji dalis dalyvių pasiekia susitarimą ir kartu nusprendžia tai padaryti. [ZXD16]

1.5.2. Viešas

Viešame blokų grandinės tinkle nėra jokių ribojimų kas gali rašyti ar skaityti duomenis. Konsensuso algoritmą gali vykdyti bet kokie suinteresuoti tinklo dalyviai. [Jen17] Tai reiškia, jog bet kas pasaulyje gali siųsti transakcijas į sąrašą ir tikėtis, kad jos bus įrašytos, jei bus validžios. Šio tipo tinklai laikomi visiškai decentralizuoti. [But15] Vienas iš didžiausių trūkumų lyginant su privačiu ar konsorciumo tinklu, yra transakcijų patvirtinimo laikas. Tai lemia didelis kiekis dalyvių, kurie tvirtina transakcijas bei sudaro ilgesnį uždelsimą.[ZXD16]

1.5.3. Konsorciumo

Konsorciumo blokų grandinės tinklas yra toks, kur konsensuso procesą kontroliuoja išrinkta grupė tinklo dalyvių. [Pil15] Tai yra tarpinis variantas tarp viešo ir pilnai privataus tinklo. Pavyzdžiui turime konsorciumą iš 10 finansinių institucijų. Kiekviena iš jų prižiūri po vieną serverį tinkle. Tam, kad būtų blokas patvirtintas yra įvedama taisyklė, kiek tinklo narių turi patvirtinti bloką. Skaitymo teisės gali būti neapribotos arba apribotos suteikiant prieiga tik tinklo dalyviams. Taip pat gali būti sukuriami kiti keliai, kaip pavyzdžiui atskiri prieigos taškai (API), kurie leistų iš išorės pasiekti ribotą informaciją, ar kreiptis ribotą kiekį kartų. Tokie tinklai vadinami dalinai decentralizuoti. [But15]

1.6. Apriboti bei neapriboti tinklai

Blokų grandinės technologijos dar gali būti skirstomos į du tipus: apriboti bei neapriboti.

Neapriboto blokų grandinės tinklo dalyviai yra anonimiški arba dalyvauja su pseudonimais. Bet kas pasaulyje gali prisijungti prie tinklo bei rašyti, skaityti, tvirtinti transakcijas. Anonimiškumo leidimas tinkle sukelia riziką tinklo atakos pavojui, kuomet pažeidėjas įgauna didelę įtaką tinkle. [Bar16] Pavyzdžiui Bitcoin tinkle, bet koks dalyvis su reikšminga dalimi (daugiau nei 50% viso tinklo) matematinių skaičiavimų galios gali pakeisti įrašus transakcijų sąraše. Taip būtų pažeista visa sistema ir nebūtų galima atskleisti kaltininko. Kita bėda su šio tipo blokų grandinės tinklu yra jo plečiamumas. Augimo potencialas yra ribojamas duomenų kiekiu blokų grandinėje. Pagrindė problema ta, jog kiekviena transakcija turi būti patvirtinta kiekvieno tinklo dalyvio. Šiuo

metu Bitcoin blokų grandinės tinklo dydis yra apie 110 gigabaitų. Jei duomenų kiekis pasiektų Visa apdorojamų duomenų kiekį, per metus saugomas duomenų kiekis paaugtų po 8 terabaitus. [Bar16] Visi šie duomenys privalo būti saugomi kiekvieno tinklo dalyvio kompiuteryje. Tai lemia, jog šiame atvirame tinkle ateityje duomenų saugojimas bus dar brangesnis ir užtruks vis daugiau laiko. [XPZ16] Pagrindinis dalykas, dėl ko egzistuoja neapribotos blokų grandinės tinklai yra ta, jog dalyviai sutinka paskolinti savo kompiuterio galią bei gauti atlygį už konsensuso algoritmo vykdymą bei taip uždirbti pinigus. [Bar16]

Priešingai viskas vyksta apribotos prieigos blokų grandinės tinkle. Šio tipo tinkle visi dalyviai bei konsensuso algoritmo vykdytojai yra identifikuojami ir žinomi. Tinklo dalyviai yra pažymėti tam tikrame registre ir turi teisę pasiekti šį apribotą tinklą. Kitaip tariant, tinklo dalyviai turi turėti teisinį statusą realiame pasaulyje, norinti dalyvauti tinkle. Prisijungiant prie tinklo, dalyvis iškart įgauna skaitymo teisę, kadangi ši informacija dalyviams yra viešai prieinama. Visa teisių informacija gali būti saugoma blokų grandinėje taip pat. Apribotos prieigos tinklas yra puikus sprendimas finansinėms institucijoms. Jų natūralus poreikis turėti tam tikrą kontrolę transakcijų tvirtinimui ir įrašymui, siekiant sumažinti riziką. [XPZ16] Bankas JPMorgan išleido savo blokų grandinės versiją pavadinimu Quorum. Programuotojai iš viso pasaulio gali naudotis juo, skaityti duomenis, kurti išmaniuosius kontraktus, tačiau tik tam tikros kompanijos yra pakviestos tvirtinti bei turėti teises įrašyti transakcijas. [Lei17]

Tiesa, taip pat yra ir tarpinis variantas, vadinamas šalutine blokų grandine (side chain). Tai yra atskiras, apribotas ir privatus transakcijų sąrašas, valdomas tam tikros organizacijos ir periodiškai įrašantis tam tikrą dalį informacijos apie turimas transakcijas į viešą neapribotą blokų grandinės tinklą. [Bar16] Ši informacija būtų agreguojama, tad šalutinės blokų grandinės suteikia galimybę praplėsti galimą duomenų saugojimo kiekį, kurio negali patenkinti pagrindinis tinklas. [Yer17]

Renkantis šio ar kito blokų grandinės tinklo prieigos ribojimą, ar ne, reikia įsivertinti, kas yra svarbu: transakcijų apdorojimo laikas, kaina, kontrolė, lankstumas keisti tinklo taisykles.[XPZ16]

Atlikta analizė detaliai paaiškina blockchain technologijos veikimo principą, savybes bei galimybes. Blockchain technologinė specifika suteikia stiprų pagrindą elektroninio balsavimo realizacijai.

2. Palyginimas tarp centrinės duomenų bazės ir blockchain

Palyginimui pasirinkta sprendimas su blockchain technologija bei sprendimas su centrine duomenų baze, kad būtų galima išanalizuoti pagrindinius privalumus ir trūkumus šių skirtingų duomenų saugojimo sistemų. Centrinė duomenų bazė pasirinkta palyginimui, kadangi ji yra dažniausias bei dauguma atveju tinkamiausias pasirinkimas įvairioms sistemoms. Taip pat turi daug skirtumų lyginant su blockchain technologija. Norint įvertinti ir atrasti tinkamiausią elektroninio balsavimo technologinį sprendimą, atliksime palyginimą tarp šių dviejų technologijų.

2.1. Palyginimo kriterijai

Pasirinkti trys palyginimo kriterijai: duomenų apsauga, duomenų atstatymo galimybės, prieigos kontrolė. Pasirinkti kriterijai yra svarbūs elektroninio balsavimo technologijos pasirinkimui bei taikymui [BS]. Norint pasiekti kuo didesnį sistemos saugumą ir patikimumą yra būtina atidžiai įvertinti šiuos technologinius aspektus. Prie kiekvieno kriterijaus yra aprašyti argumentai jo pasirinkimui.

2.1.1. Duomenų apsauga

Programišiams gali pavykti įsilaužti į duomenų bazę ir pasiekti tam tikrus duomenis. Naudojant šifravimą, net ir neteisėtai pasisavinęs duomenis įsilaužėlis negalės jų nepastebimai pakeisti, suprasti jų prasmės ir ja pasinaudoti. Saugumo specialistai teigia, jog jautrią informaciją yra būtina šifruoti ir saugojant pačioje duomenų bazėje, ir persiunčiant ją tarp kliento ir serverio [Dav09].

2.1.1.1. Blockchain

Ši technologija paremta viešo bei privataus rakto kriptografija. Kiekviena transakcija yra šifruojama. Tik su privačiu raktu galima pasiekti transakcijos turinį ir ją atrakinti, o su viešu raktu greitai patikrinti jos autentiškumą. Kiekvienas tinklo dalyvis užsiima kasimu (angl. mining). Kasimas - tai paskirstyta vienodo sprendimo priėmimo sistema, skirta patvirtinti įvykusias transakcijas ir jas įtraukti į blokų grandinę [Ant14]. Kad transakcija būtų patvirtinta, ji turi būti pasirašyta transakcijos kūrėjo privačiu raktu. Tuomet ji bus patikrinta viešu raktu visų tinklo dalyvių. Tik tada ji bus įrašyta į blokų grandinę [Li16]. Kadangi visos transakcijos yra viešos, kriptografija apsaugo nuo sugadinimo bei melagingų transakcijų. Tiesa, yra sukurta sprendimų, kurie į blokų grandinę įrašo jau šifruotą informaciją, tad informacijos esančios transakcijoje nėra įmanoma suprasti be papildomų žinių. Taip pasitelkiant kriptografiją apsaugome ir nuo duomenų perskaitymo trečiųjų

šalių. [KMS16]

2.1.1.2. Centrinė duomenų bazė

Centrinės duomenų bazės turi keletą silpnybių duomenų saugomo atžvilgiu: dažniausiai duomenys bei atsarginės duomenų kopijos nėra šifruojamos. Tai reiškia, jog gavus prieigą prie duomenų kopijos, ar patekus į duomenų bazę piktavaliams, jie nesunkiai gali pasisavinti jautrią informaciją. Tačiau ir centrinės duomenų bazės turi įvairių technologijų užtikrinti duomenų validumą: įsitikinti, kad duomenų kūrėjas yra tikrai tas žmogus bei duomenys nebuvo pažeisti ar pakeisti piktavalio po jų sukūrimo. Tai atliekama naudojant šifravimą. Šifravimą duomenų bazėms galima taikyti keliais skirtingais lygiais: stulpeliams, lentelėms ar failams [DQ13]. Tokios galimybės leidžia pasiekti skirtingus saugomo lygius. Taigi pasitelkiant kriptografiją yra užtikrinama, kad įsilaužėlis negalėtų suprasti saugomų duomenų.

2.1.2. Duomenų kopijos ir atstatymas

Virtualūs duomenys gali būti sugadinti atsitikus įvairiems įsilaužimams, klaidingam sistemos veikimui ar netikėtam praradimui. Šiai problemai spręsti daromos atsarginės duomenų kopijos, skirtos atstatyti duomenis į pradinę būseną. Duomenų bazių specialistai teigia, jog duomenų kopijos turi būti atliekamos nuolatos bei įvykus nenumatytiems įvykiams, kaip netikėtam serverio išsijungimui ar vartotojo padarytos klaidos atveju [Gor14]. Naudojantis padarytomis duomenų kopijomis, turi būti įmanoma greitai atstatyti sistemą į buvusią būseną.

2.1.2.1. Blockchain

Blokų grandinės duomenų kopijos daromos nuolatos prisijungus naujam vienetui. Kiekvienas serveris laiko po atskirą ir pilną duomenų kopiją. Tai yra įmanoma dėl to, jog kiekvienai transakcijai labai paprastai gali būti patikrintas jos teisingumas ir autentiškumas, vietoje to, jog turėti centrinę sistemą, kuri tai prižiūrėtų. Sinchroniškumas užtikrinimas paprastai, kadangi kiekvienas serveris prijungtas į tinklą vienas kitą informuoja apie bet kokį pasikeitimą savo duomenų bazėje [GM15]. Dėl šios priežasties joks individualus serveris nėra kritinis. Jei jis būtų atjungtas nuo tinklo tam tikrą laiką, blockchain technologija užtikrina automatinį duomenų atstatymą iš kitų serverių.

2.1.2.2. Centrinė duomenų bazė

Dažniausiai įprastų duomenų bazių kopijos daromos periodiškai, saugant jos tuo metu esamą būseną. Kopija gali būti saugojama visiškai kitame serveryje, kitoje geografinėje vietoje. Kadangi šiuolaikinės įmonės duomenų bazėse saugo ypatingai svarbią informaciją, bet koks jos neveikimo laikas yra didelis nuostolis. Įvykus netikėtam įvykiui tokiu būdu atstatyti duomenis gali užtrukti tam tikrą laiko tarpą bei atstatymo procesas ribotų naudotojų atliekamus veiksmus sistemoje. [CGG14] Taip pat yra ir kitas duomenų kopijų realizavimo būdas vadinamas pasikeitusių duomenų kopija. Joje saugomi tik paskutiniai įrašai nuo paskutinės duomenų bazės kopijos. Taip stebint pasikeitimus ir juos nuolatos siunčiant tinkle į atsarginį serverį, esantį kitoje vietoje. Tačiau net ir šiuo atveju, nutikus klaidai yra prarandami duomenys, kurie tuo metu dar nebuvo pasiekę atsarginės duomenų bazės. [Hub16]

2.1.3. Prieigos kontrolė

Kiekvienoje duomenų bazėje yra būtina kontroliuoti jos pasiekiamumą bei prieigą prie duomenų. Siekiant užtikrinti saugumą, duomenų bazių valdymo sistemos yra realizavusios įvairiausius prieigos kontrolės algoritmus. Administratoriai turi užtikrinti tam tikrų vartotojų prieigą prie sistemos, stebėti jų atliktus veiksmus bei riboti jų teises norint leisti tik autorizuotus pakeitimus duomenų bazių sistemoje [GMB15].

2.1.3.1. Blockchain

Kadangi visi susijungę serveriai laiko pilną duomenų kopiją, visos transakcijos yra viešos. Tai reiškia, jog bet kas gali peržiūrėti duomenų bazės dabartinę būseną, pakeitimus, kuriuos atliko transakcija, bei skaitmeninį parašą, kuris leidžia susekti transakcijos kūrėjo buvusias transakcijas [McC15]. Blockchain atveju tiesioginės galimybės apriboti prieigos prie dalies duomenų nėra, tačiau pasitelkus kriptografiją duomenis galima šifruoti bei viešu raktu pasidalinti tik su tam tikrais asmenimis. Tinklo dalyviai gali būti apriboti rašymo arba skaitymo teisėmis tik visam tinklui.

2.1.3.2. Centrinė duomenų bazė

Įprastose duomenų bazėse pasiekiamumui kontroliuoti reikia centrinės vietos, kurioje galima laikyti sąrašą vartotojų, turinčių prieigą prie duomenų [Aks12]. Tai reiškia, jog visos užklausos skaityti bei keisti duomenis keliauja per centrinį serverį, kuris gali nuspręsti priimti ar atmesti šį veiksmą. Tai didelis privalumas, tačiau taip pat ir trūkumas. Dėl žmogaus klaidos: pamirštama

atsijungti, dėl nesaugiai laikomo slaptažodžio, gali būti prarasti dideli kiekiai duomenų, ar atitekti į piktavalių rankas.

Atliktas palyginimas pagal pateiktus kriterijus pabrėžė blockchain technologijos stiprybes duomenų atstatomumo bei apsaugos atžvilgiu. Duomenų prieigos reguliavime, sprendimas su centrine duomenų baze suteikia daugiau galimybių nei sprendimas su blockchain technologija, tačiau pasitelkus kriptografija šią silpnesnę vietą galima sustiprinti. Remiantis šiuo palyginimu, autorius teigia, jog blockchain technologija yra tinkamesnė elektroninio balsavimo sprendimo įgyvendinimui.

3. Ethereum blockchain technologija

Ethereum yra paskirstytos kompiuterių galios platforma, kuri išnaudoja blokų grandinės technologiją pirmiausia panaudotą Bitcoin platformoje. Tačiau ši platforma praplečia technologijos pritaikymą daug labiau nei tik kriptografinė valiuta. Tyrėjas Vitalik Buterin 2013 metų pabaigoje aprašė Ethereum teorinį modelį ir tikslą. Jis apibrėžė tai kaip: „blokų grandinė su visaverte ir išbaigta (Turing-complete) programavimo kalba, kuria naudojantis galima kurti kontraktus, kuriuos galima naudoti siekiant užkoduoti būsenos pasikeitimo funkcijas“. [Mur16] Ši techologija yra inovatyvi blokų grandinės taikymu paremta virtuali mašina, leidžianti saugoti būseną vartotojų sukurtuose kontraktuose. [Pil15] Platforma įneša daugybę praplėtimo galimybių į kriptografinę ekosistemą ir sukuria papildomus taikymus link sričių kaip atlyginimų išmokėjimas, vestuvių įrašai ar nekilnojamo turto registras. Vienas iš Ethereum programuotojų teigia, jog jiems pavyko sukurti blokų grandinę, kuri turi savyje integruotą programavimo kalbą, leidžiančią žmonėms kurti įvairiausias programas ant blokų grandinės infrastruktūros. Pagrindinė Ethereum sąvybė - išmanieji kontraktai. Ethereum yra kaip virtuali mašina prižiūrima visų dalyvių, esančių tinkle. Naudojantis išmaniaisiais kontraktais, programuotojai gali rašyti įvairiausias programas, kurios bus vykdomos internete. [Pil15] Šios platformos valiuta vadinama Ether, kuria yra apdovanojami tinklo dalyviai, tvirtinantys transakcijas bei vykdantys išmaniuosius kontraktus. Tinkle naudojamas darbo įrodymo konsensuso algoritmas, siekiant palaikyti duomenų vientisumą.

3.1. Išmanieji kontraktai

Išmanieji kontraktai - tai programos, vykdomos Ethereum blokų grandinės tinkle kiekvieno tinklo dalyvio. Taip yra užtikrinama, jog viskas vyksta decentralizuotai. Šių kontraktų autorius pasiūlė atlygį tinklo dalyviams už kontraktų vykdymą, naudojant savo kompiuterių galią. Atlygį pavadino kuru (angl. „gas“). Norint įvykdyti kontraktą, reikia paskirti tam tikrą kuro kiekį, kurį galima pirkti už Ether valiutą. [AH16] Išmanieji kontraktai gali būti sudėtingi, savyje saugoti būseną, ją keisti bei kviesti kitus kontraktus. Ethereum išmanieji kontraktai yra rašomi aukšto lygio programavimo kalbomis Solidity arba Serpent. Ši blokų grandinės technologija buvo sukurta taip, jog joje būtų galima saugoti būseną bei kontraktų kodą. Būsena Ethereum saugoma iš objektų pavadintų sąskaitomis, kurie identifikuojami naudojant jų 20 baitų adresus.

Yra dviejų tipų sąskaitos: nuosavybės išorėje sąskaita (angl. „externally owened account“) bei kontrakto sąskaita (angl. „contract account“). Nuosavybės išorėje sąskaita yra kaip paprasta sąskaita valdoma privačiu raktu ir savyje sauganti Ether balansą. Kontraktų sąskaitos turi balansą taip pat, tačiau dar turi ir kitus du laukus: kontrakto kodą bei savo duomenų saugyklą. Kontraktų

sąskaitos yra valdomos kodo, esančio jose. Kodas gali keisti būseną, tai yra saugoti bei redaguoti duomenis saugykloje. Duomenys saugomi rakto-reikšmės pagrindu. Nuosavybės išorėje sąskaitos gali kurti transakcijas, kurios įrašomos į blokų grandinę. Transakcijos gali būt dviejų tipų: pervedami pinigai į kitą sąskaitą (reikalingi gavėjo, siuntėjo adresai bei suma), kontrakto iškvietimo (reikalinga siuntėjo ir kontrakto adresai, suma bei papildomas duomenų laukas kontrakto funkcijos iškvietimui). Kontrakto iškvietimo transakcija leidžia iškviesti bet kokią viešą funkciją esančią Ethereum blokų grandinėje. Kontraktai negali įrašyti transakcijų, bet jie gali siųsti žinutes kitiems kontraktams, kurios prilygsta transakcijoms, tik kad yra inicijuojamos iš kontrakto kodo.

Skaičiuoti būsenos pokyčius kontraktuose naudojama Ethereum virtuali mašina (EVM). EVM sugebėjo išspręsti pagrindinę problemą, kaip išvengti nesibaigiančių ciklų vykdymo tinkle. Jei kontrakto kodas turėtų nesibaigiantį ciklą, tai sukeltų didžiules problemas tinkle, ir būtų sunaudojami didžiuliai kiekiai kompiuterių galios, o rezultatas vistiek nebūtų pasiektas. Begaliniams ciklams įveikti naudojamas kuras, kurio kiekis nurodomas kviečiant išmanųjį kontraktą. Kiekvieno kodo bito operacija EVM kainuoja tam tikrą kiekį kuro. Duomenų saugojimas yra pati brangiausia operacija, kadangi transakcija su būsenos pakeitimu yra saugoma blokų grandinėje amžiams. Jei vykdant funkciją kuras pasibaigia, transakcija pažymima kaip nesėkminga ir kuras nėra grąžinamas. Jei gautas kuras nebuvo sunaudotas, perteklius yra grąžinamas kontrakto funkciją iškvietusiam asmeniui. Kuro naudojimas yra būtinas paskatinti dalyvius vykdyti kontrakto kodą bei rašančius kontraktus, rašyti efektyvias programas.

Kontrakto rašymas yra kaip paprastos programos rašymas naudojant funkcijas, kintamuosius. Unikalus bruožas yra kontrakto kodo nepakeičiamumas. Kuomet jis yra įrašomas į blokų grandinę, jei kūrėjas nepasiliko sau galinių durų (tikrinimo ar siuntėjas yra kūrėjas ir tuo atveju įvykdomas specialus kodas), kodas tampa nebepakeičiamas. Kontrakto negalima ištrinti ir jis liks blokų grandinėje amžinai. Tai sukuria unikalią galimybę egzistuoti kontraktams, kurių pakeisti nebegali niekas ir programuotojas neturi jokių galių. Taip atsiranda galimybė visiškai atsiriboti nuo bet kokio priklausomumo centralizuotai sistemai. [Mur16]

Skaidrumas - dar viena svarbi kontraktų savybė. Bet kas gali pasižiūrėti į kontrakto kodą ir jei aprašyta logika yra tinkama, galima pradėti jį naudoti. Jei matoma, jog kontrakto kodas jūsų netenkina, jo nenaudojate. Šis atvirumas yra ir privalumas, ir trūkumas. Yra gerai, jog egzistuoja galimybė visiems suinteresuotiems asmenims naudotis kontraktu, įvertinti jo patikimumą. Tačiau, taip pat ši galimybė peržiūrėti kontrakto kodą išlieka ir bet kuriam kitam tinkle esančiam dalyviui, galbūt būsimam piktavaliui. [Sta16]

Išanalizavus Ethereum blockchain bruožus bei įvertinus galimybes, kurias suteikia išmanieji

kontraktai, daroma išvada, jog ši technologija gali būti panaudota elektroniniam balsavimui bei padaryti sprendimą skaidrų bei patikimą.

4. Elektroninis balsavimas

4.1. Naudojami terminai ir jų paaiškinimas

Šiame balsavimo aprašyme yra naudojami šie terminai su atitinkamomis reikšmėmis:

1. Balsuotojas arba Rinkėjas - žmogus turintis suteiktą teisę skirti balsą tam tikruose rinkimuose.
2. Balsuotojų registras - sąrašas žmonių, galinčių balsuoti.
3. Elektroninis balsavimas - rinkimai, kurie savo procese naudoja elektroninius būdus priimti balsus.
4. Nuotolinis elektroninis balsavimas - elektroninis balsavimas, kuris atliekamas iš prietaisų, nekontroliuojamų rinkimų administracijos.
5. Autentifikacija - patikrinimas pateiktų vartotojo asmens duomenų bei jo tapatybės.
6. Balsavimo lapelis - būdas, kuriuo balsuotojas gali išreikšti savo pasirinkimą.
7. Administratorius - rinkimų organizatoriaus išrinktas asmuo ar žmonių grupė, kontroliuojanti elektroninį rinkimų procesą.
8. Validuotojai - tam tikri organizaciniai vienetai esantys skirtingose vietose ir įgalioti prižiūrėti bei kontroliuoti administratoriaus darbą, padėti vykdyti rinkimus. Pavyzdžiui seimo rinkimų atveju - savivaldybės. Tai atliekama nuotoliniu būdu ir automatizuotai.
9. Stebėtojai - asmenys, stebintys rinkimų eigą bei užtikrinantys sąžiningą rinkimų vykdymą.

[Eur04]

4.2. Apibrėžimas

Elektroninis balsavimas - tai balsavimas, kurio metu naudojamos elektroninės priemonės balso paskyrimo ar skaičiavimo procese. Priklausomai nuo implementacijos, elektroninis balsavimas gali apimti dalį internetinių paslaugų, nuo duomenų perdavimo iki pilno internetinio balsavimo per balsuotojų asmeniškai naudojamus elektroninius prietaisus. Automatizavimo laipsnis gali varijuoti nuo paprastų darbų iki pilno sprendimo, kurį sudaro: vartotojo registravimas ir identifikavimas, balso skyrimas, balsų skaičiavimas, balsų šifravimas ir perdavimas į serverius, rinkimų valdymas. Ideali elektroninio balsavimo sistema turi atlikti visas šias užduotis laikydamasi įvairiausių reguliacinių standartų. Taip pat ji turi sėkmingai įgyvendinti šiuos aukšto lygio reikalavimus: saugumas, tikslumas, integralumas, privatumas, validumas, pasiekiamumas, kaštų efektyvumas, plečiamumas. [Buc04]

Elektroninis balsavimas gali būti dviejų tipų:

1. Elektroninis balsavimas, kuris yra prižiūrimas fiziškai valdžios atstovų ar nepriklausomų stebėtojų balsavimo vietoje, kurioje yra naudojami tam tikri elektroniniai prietaisai.

2. Nuotolinis elektroninis balsavimas, kuris vyksta internetu. Balsuotojas gali paskirti savo balsą iš namų ar darbovietės be prievolės apsilankyti rinkimų apylinkėje. [EEs]

Šiame darbe nagrinėsime tik nuotolinį elektroninį balsavimą, kuris suteikia rinkėjams galimybę balsuoti nuotoliniu būdu.

Nuotolinis elektroninis balsavimas suteikia galimybę greitam ir paprastam balso paskyrimui bei suskaičiavimui. Piliečiams, esantiems užsienyje, taip pat suteikiama galimybė paprastai balsuoti nuotoliniu būdu. Tai yra išskirtinis atvejis analizei, kadangi šis balsavimo atvejis yra vienas globaliausių ir patogiausių būdų naudoti, tačiau tuo pat metu ir keliantis daugybę teisinių, technologinių bei vykdymo iššūkių.

4.3. Balsavimo taisyklės

Norint užtikrinti patikimumą ir saugumą, elektroninis balsavimas turi atitikti įvairias taisykles bei reikalavimus. Svarbu, jog jų būtų laikomasi, su jomis būtų susipažinęs kiekvienas balsuojantis, o technologijos pasirinktos balsavimui leistų tai įgyvendinti. Europos konsulatas [Eur04] apibrėžia pagrindines 4 rinkėjo teises elektroniniam balsavimui:

1. Visuotinė rinkimų teisė. Visi žmonės turi teisę balsuoti ir dalyvauti rinkimuose, atsižvelgiant į jų amžių ir tautybę.
2. Lygybės rinkimų teisė. Kiekvienas balsuotojas gali skirti tik po vieną balsą.
3. Laisvų rinkimų teisė. Balsuotojas turi skirti savo balsą laisvai ir be jokios įtakos iš išorės ar balsavimo procese.
4. Slaptų rinkimų teisė. Balsuotojas turi teisę skirti balsą anonimiškai, jog nebūtų galima nustatyti ryšio tarp balsuotojo bei jo balsavimo lapelio.

Ženevos projekte [Gen03] buvo aprašyti pagrindiniai punktai, kuriuos turėtų tenkinti nuotolinis elektroninis balsavimas atsižvelgiant į Europos konsulato reikalavimus:

1. Balsai negali būti nei sugadinti, nei pakeisti.
2. Balsai negali būti atskleisti iki oficialaus balsų skaičiavimo.
3. Tik užsiregistravę asmenys gali balsuoti.
4. Kiekvienas balsuotojas turi vieną ir tik vieną balsą.
5. Balso slaptumas yra garantuotas. Jo niekada nebus galima susieti su balsuotoju.
6. Balsavimo sistema bus atspari DDOS („Denial of service attack“) atakoms.
7. Balsuotojas yra apsaugotas nuo tapatybės vagystės.

8. Skirtų balsų suma bus lygi gautų balsų sumai.
9. Yra įmanoma įrodyti, jog tam tikras pilietis balsavo.
10. Sistema nepriims balsų kitu laiku, nei balsavimo vyksmo laikas.
11. Sistemai bus galima atlikti auditą.

Pagal šiuos reikalavimus vertinsime sukurtą sistemos modelį.

5. Balsavimo procesas

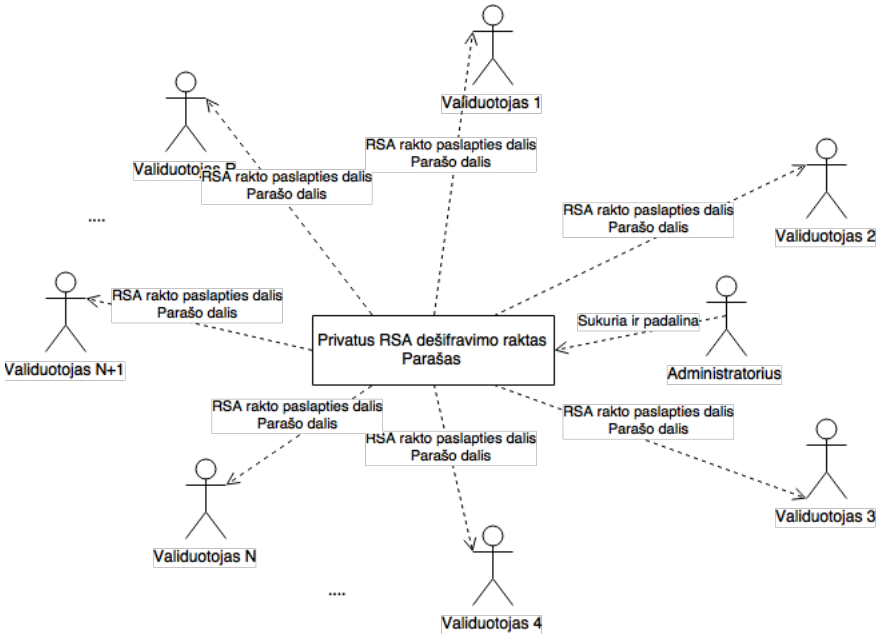
Teisės aktų registre aprašytas Lietuvos Respublikos Seimo (LRS) rinkimų įstatymas [Vyt92] apibrėžia esminius balsavimo eigos punktus bei procedūras. Pagal šį balsavimo procesą lyginsime mūsų elektroninį balsavimo sprendimą bei pateiksime argumentus pasirinktiems sprendimams.

5.1. Balsavimo pradžia ir pasiruošimas

5.1.1. LRS rinkimų įstatymo žingsniai

Rinkimų komisijos pirmininkas su komisijos nariais patikrina, ar balsadėžė yra tuščia, ją užantspauduoja. Tik įsitikinęs, jog patalpa įrengta pagal visus reikalavimus, apylinkės rinkimų komisijos pirmininkas išdalija rinkimų biuletenius ir rinkėjų sąrašus komisijos nariams, atidaro balsavimo patalpą, tuo skelbdamas rinkimų pradžią. Išdalintų rinkimų biuletenių skaičius įrašomas rinkimų apylinkės balsų skaičiavimo protokole.

5.1.2. Ethereum blockchain sprendimo atitikmuo



2 pav. Dešifravimo rakto ir parašo padalinimo schema

Šiame sprendime atskirsime pradžią ir pasiruošimą, kadangi jiems reikalingi atskiri žingsniai:

1. Pasiruošimas. Sprendimą (žr. 2 pav.) sudaro keletas validuotojų bei administratorius. Virtualiems balsavimo lapeliams pasirašyti bus naudojamas slenkstinis keletos dalių parašas [Guo04], kurio dalys padalinamos validuotojams. Taip pat sukuriama RSA privataus ir viešo rakto pora, kuri naudojama balsų šifravimui. Privatus raktas yra laikomas paslaptyje, kurios

dalys pagal slenkstinę Šamiro kriptografinę schemą [BL90] padalinamos validuotojams. Taip pat sukuriama pirmoji administratoriaus Ethereum paskyra, kuri turės teisę registruoti rinkėjus ir išduoti jiems balsavimo teisę bei antroji Ethereum paskyra, kuri turės teisę inicijuoti balsų skaičiavimą.

2. Pradžia. Inicijuojant balsavimą bei įrašant kontrakto kodą į blokų grandinę, kode yra nurodomi administratoriaus Ethereum paskyrų identifikatoriai, balsavimo pradžios ir pabaigos laikai, validuotojų parašo viešas raktas bei balsų šifravimo viešas raktas. Nuo šio momento kontraktas tampa viešas ir yra matomas blockchain tinkle.

5.1.3. Argumentai

Slenkstinis keletos dalių parašas padalintas validuotojams naudojamas tam, kad nebūtų centrinio taško, kuris galėtų suteikti teisę balsuoti. Šis balsavimo teisės suteikimas turės būti priimtas kolektyviškai pasirašius bent N skaičiui validuotojų.

RSA raktų pora yra būtina. Balsai bus šifruojami viešu raktu, kadangi ši informacija įrašoma į viešą blokų grandinės transakcijų sąrašą ir bus pasiekiama visiems. Naudojant privatų raktą, pasibaigus rinkimams administratorius gavęs iš bent N validuotojų paslaptis atskleis privatų raktą bei taip galės nutraukti balsavimą ir paskelbti dešifravimo raktą blockchain kontrakte. Taigi rinkimų metu nebus galimybės sužinoti kokie yra rezultatai.

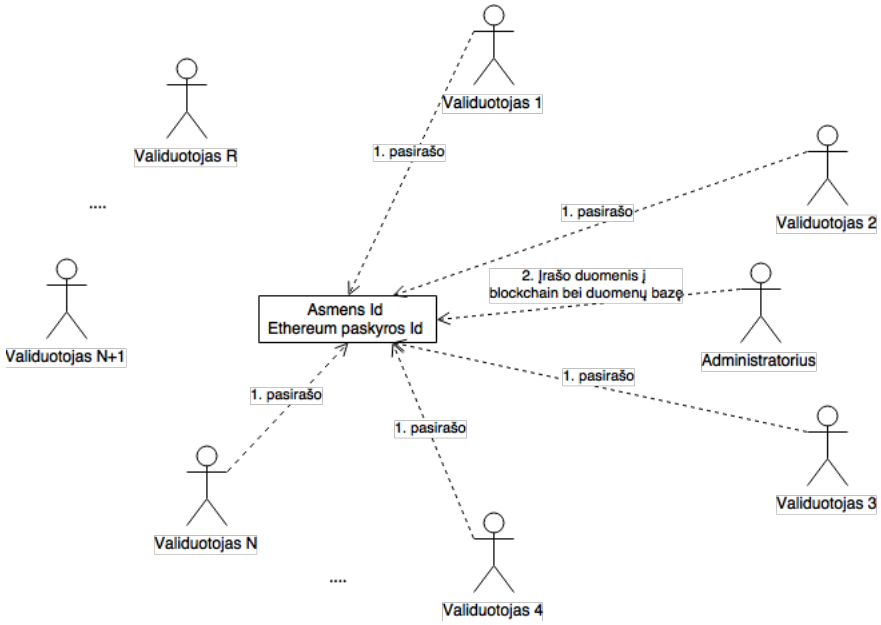
Kontraktas, įrašytas į blockchain, tampa viešas ir bet kas gali peržiūrėti jo veikimo principą bei taisykles. Tiesa, suprasti kodą pavyks tik technologiškai išsilavinusiam žmogui. Įrašyto kontrakto pakeisti nebegalima, tad balsuotojai gali būti užtikrinti, jog aprašytos balsavimo taisyklės nebus pakeistos rinkimų metu.

5.2. Rinkėjo asmenybės nustatymas

5.2.1. LRS rinkimų įstatymo žingsniai

Atvykęs į balsavimo patalpą, rinkėjas privalo pateikti komisijos nariui balsavimo pažymėjimą, dokumentą, patvirtinantį jo asmenybę. Tuomet jis pasirašo rinkėjų sąraše ir jam išduodamas rinkimų biuletenis.

5.2.2. Ethereum blockchain sprendimo atitikmuo



3 pav. Pasirašymų schema

Rinkėjo registraciją sudaro keletas etapų, kurie užtikrina rinkėjo identifikavimą bei jo registravimą ir balsavimo teisės suteikimą.

1. Rinkėjo identifikacija. Rinkėjas yra identifikuojamas tam tikroje išorinėje sistemoje, kurioje patikrinama, ar jis turi teisę balsuoti šiuose rinkimuose. Išorinė sistema turi užtikrinti patikimumą identifikuojant balsuotoją. Šiuo atveju asmuo identifikuojamas bei patikrinama ar pateiktas jo asmens kodas yra teisingas. Sistema patikrina amžių, bei sąrašą piliečių asmens kodų, kurie neturi teisės balsuoti. Pagal šiuos kriterijus rinkėjas yra prijungiamas prie sistemos arba ne.
2. Ethereum paskyros sukūrimas. Sistema sukuria Ethereum paskyrą ir rinkėjui suteikia dokumentą parsisiųsti, kuriame yra privatus raktas, užkoduotas vartotojo įvestu slaptažodžiu. Po atsisiuntimo dokumentas sistemoje yra automatiškai sunaikinamas.
3. Balsavimo teisės suteikimas ir rinkėjo bei balso atskyrimas (žr. 3 pav.). Šiame etape reikia suteikti vartotojui balsavimo teisę, gavus patvirtinimus iš bent N validuotojų. Administratoriaus serverio sistema siunčia sukurtos Ethereum paskyros adresą bei asmens identifikatorių validuotojams pasirašyti. Norint įrodyti, jog šiai paskyrai teisė balsuoti buvo suteikta validuotojų, turi būti naudojamas kontraktas, kuriam pateikus balsuotojo paskyros adresą bei tą patį adresą pasirašytą validuotojų, kontrakte būtų patikrinama viešu raktu, ar tai tikrai pasirašyta validuotojų. Iš administratoriaus nurodytos paskyros kviečiama kontrakto funkcija, kurioje atliekamas patikrinimas ir suteikiama teisė balsuoti. Taip pat atliekama transakcija

iš Administratoriaus paskyros į balsuotojo paskyrą pervedant tam tikrą kiekį (nurodytą „Rinkimų organizavimo kainų lentelė“) Ether valiutos, kuri leis kviesti balsavimo funkciją. Tuo pačiu metu sistema administratoriaus duomenų bazėje pažymi, jog šis asmuo jau yra gavęs balsavimo teisę ir išsaugo validuotojų pasirašytą asmens identifikatorių.

5.2.3. Argumentai

Kaip ir paprastam balsavime, taip ir elektroniniame balsavime, rinkėjas yra identifikuojamas pagal jo pateiktus įrodymus. Elektroninio balsavimo atveju, tai yra išorinė sistema, kurioje vartotojas patvirtina savo tapatybę.

Balsavimo teisės suteikimą atitinka du veiksmai elektroniniame balsavime: Ethereum paskyros sukūrimas bei Balsavimo teisės suteikimas. Šie du veiksmai vartotojui suteikia teisę balsuoti ir yra atitikmuo fiziniam balsavimo lapeliui. Paprastam balsavime rinkėjo bei balso atskyrimas įvyksta tuomet, kai yra pasirašoma ir įteikiamas balsavimo lapelis. Elektroninio balsavimo atveju, siekiant išvengti rinkėjo bei jo balso nustatymo, sistemoje nėra saugomas ryšys tarp rinkėjo identifikatoriaus bei sukurtos Ethereum paskyros identifikatoriaus.

Centrinę duomenų bazę, kurioje saugomi jau gavę balsavimo teisę asmens kodai, gali pasiekti visi validuotojai bei bet kuriuo metu patikrinti, ar asmens kodas jau gavęs balsavimo teisę. Tą atlikti galima prisijungus prie duomenų bazės bei pagal asmens kodą patikrinti, ar šis kodas jau gavo virtualų balsavimo lapelį (Ethereum paskyrą), ar ne. Tokiu būdu užtikrinama, jog teisė balsuoti bus vienam asmeniui suteikiama tik vieną kartą ir tas sprendimas bus decentralizuotai priimtas keleto validuotojų.

5.3. Balsavimas

5.3.1. LRS rinkimų įstatymo žingsniai

Gavęs balsavimo lapelį, balsuotojas eina į kabiną bei pažymėdamas kandidatą ant lapelio, skiria savo balsą. Jei buvo sugadintas balsavimo lapelis, rinkėjui paprašius, yra išduodamas naujas. Senas yra išsaugomas, ant jo yra pasirašoma rinkimų komisijos nario.

5.3.2. Ethereum blockchain sprendimo atitikmuo

Rinkėjas sistemoje išsirinkęs kandidatą, patvirtina savo sprendimą. Tuomet sistema balsą užšifruoja viešu kontrakte nurodytu raktu. Tai vyksta vartotojo naršyklėje. Užšifruotą balsą vartotojui leidžiama parsisiųsti bei išsisaugoti kaip tekstinį dokumentą.

Tuomet sistema sukuria transakciją, kurioje yra kviečiama kontrakto balsavimo funkcija. Kontrakte yra patikrinama, ar šiai paskyrai yra suteikta balsavimo teisė. Taip pat patikrinama, ar balsavimo laikas dar nėra pasibaigęs. Patikrinus šias sąlygas, sistema įrašo užšifruotą balsą bei rinkėjo paskyros identifikatorių. Jei yra gaunamas antras balsas iš to pačio rinkėjo, senasis yra perrašomas.

5.3.3. Argumentai

Kontrakte tikrinama logika dėl rinkėjo galimybės balsuoti bei yra saugomi balsai. Tokiu būdu apsisaugoma nuo balsavimo pažeidimų, kaip pakartotinio balsavimo, ar žalingo duomenų pakeitimo, kadangi visi pasikeitimai matomi blockchain tinkle bei transakcijų sąraše.

Balsuotojas atlikdamas balsavimą gali išsisaugoti užšifruoto balso kodą bei savo Ethereum paskyros identifikatorių, kurių pagalba balsavimo metu ar po balsavimo gali patikrinti užšifruoto balso kodą su esančiu Ethereum blockchain kontrakte. Taip pat pateikus šiuos duomenis skundus nagrinėjančiai institucijai, bus galima patikrinti, ar tikrai balsas nebuvo pakeistas.

5.4. Stebėjimas

5.4.1. LRS rinkimų įstatymo žingsniai

Stebėtojams turi būti suteiktos visos galimybės stebėti visą rinkimų eigą. Pastebėjus tam tikrus pažeidimus remiantis LRS įstatymais, jie turi teisę išreikšti pastabas ir pretenzijas, tačiau negali trukdyti proceso. [kom14]

5.4.2. Ethereum blockchain sprendimo atitikmuo

Komisija bei rinkėjai gali nuolatos matyti transakcijų skaičių blokų grandinėje bei vykstančias transakcijas. Iš šios informacijos galima suskaičiuoti užsiregistravusių rinkėjų skaičių bei kiek iš jų atidavė balsus. Taip pat galima stebėti bandymus neteisėtai balsuoti (atmestas transakcijas) bei apie tai informuoti atsakingus asmenis.

5.4.3. Argumentai

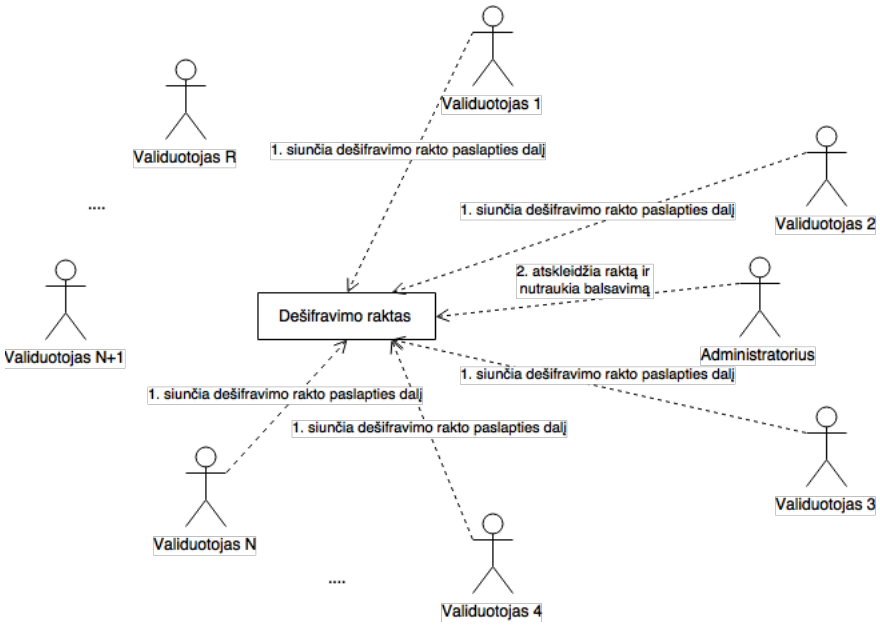
Rinkimų eigą galima stebėti dėl blokų grandinės atvirumo. Kadangi balsai šifruoti, balsavimo laikotarpiu matyti kiek koks kandidatas surinko balsų yra neįmanoma.

5.5. Rezultatų nustatymas

5.5.1. LRS rinkimų įstatymo žingsniai

Pirmiausia rinkimų komisijos pirmininkas suskaičiuoja nepanaudotus ir sugadintus balsavimo lapelius bei taip patikrina, ar nebuvo neteisėtai išduotų lapelių. Įsitikinus, kad balsadėžė nebuvo pažeista, ji yra atidaroma ir yra pradedami skaičiuoti balsai. Ši procedūra atliekama taip, jog visą procesą galėtų matyti visi balsų skaičiavime dalyvaujantys asmenys.

5.5.2. Ethereum blockchain sprendimo atitikmuo



4 pav. Dešifravimo rakto sukonstravimo bei balsavimo nutraukimo schema

Administratorius gavęs iš bent N validuotojų paslaptis atskleidžia privatų raktą (žr. 4 pav.). Pasibaigus balsavimo laikui, administratorius inicijuoja balsavimo pabaigą. Yra kviečiama kontrakto balsavimo pabaigos funkcija, kuriai yra pateikiamas dešifravimo raktas. Taip privatus dešifravimo raktas tampa visiems pasiekiamas. Administratoriaus sistema parsisiunčia balsus esančius kontrakte, juos dešifruoja bei suskaičiuoja rezultatus ir paskelbia viešai.

5.5.3. Argumentai

Šiuo atveju visi balsai tampa atviri ir bet kas gali patikrinti rezultatus. Turint privatų dešifravimo raktą, visi suinteresuoti asmenys gali perskaičiuoti balsus bei įsitikinti, jog jie buvo suskaičiuoti teisingai.

5.6. Prielaidos ir pasirinkimo sprendimai

Pasirinkimai buvo atlikti vadovaujantis tam tikromis prielaidomis, ar ribojimais dėl technologinių sprendimų.

5.6.1. Rinkėjo kompiuterio saugumas

Šiame darbe yra daroma prielaida, jog rinkėjas yra suinteresuotas ir pats gali užtikrinti, jog jo kompiuteris yra saugus ir nėra apkrėstas virusais. Jei kompiuteris yra nulaužtas programišių, didelė tikimybė, jog balsas gali būti pakeistas rinkėjui to nežinant.

5.6.2. Kitų žmonių įtaka balsuojant

Kadangi balsavimas gali vykti iš namų, šioje aplinkoje negalima užtikrinti, jog rinkėjas atiduoda balsą savo valia ir be kitų žmonių, stovinčių už nugaros, įtakos. Šiai problemai spręsti rinkėjui yra suteikiama galimybė pakeisti savo balsą visų rinkimų metu. Tačiau vartotojui gali būti liepta ištrinti ir sunaikinti savo Ethereum paskyros dokumentą, kas lems, jog šis sprendimas tampa nebeveiksmingas.

5.6.3. Administratoriaus elgsena

Darome prielaidą, jog administratorius yra visiškai patikima ir saugi institucija, kuria rinkėjai pasitiki. Tai gali būti tam tikra valstybinė organizacija, politinė partija, ar įmonės vadovybė, atsižvelgiant į balsavimo pobūdį. Kadangi visi veiksmai atliekami per administratoriaus bei validuotojų serverius, darome prielaidą, kad jie nėra užkrėsti virusais.

5.6.4. Ethereum paskyros duomenų praradimas

Ethereum paskyrą sudaro privatus raktas. Jis turi būti saugomas rinkėjo kompiuteryje. Iš administratoriaus puslapio parsisiųstas failas su privačiu raktu turi būti saugomas vartotojo iki tol kol bus atliktas balsavimas. Ištrynus jį nėra jokių galimybių atstatyti, ar suteikti vartotojui galimybę balsuoti antrą kartą.

5.6.5. Rinkimų vykdymo viešame Ethereum tinkle kaina

Kaip ir aprašyta darbe, transakcijų įrašymas bei kontraktų vykdymas Ethereum tinkle kainuoja pinigus. Buvo atliktas eksperimentas, kiek toks balsavimas su 100.000 balsuotojų galėtų kainuoti apytiksliai Ethereum viešame tinkle. Ethereum valiutos kursas dolerio atžvilgiu nuolat

kinta, tačiau šio darbo rašymo metu jis yra toks: 1 ETH yra vertas 91 USD. Skaičiavimai pateikti pirmoje lentelėje.

Vienetas: Transakcija	**Kaina (Ethereum kuras)**	**Kaina (Ethereum valiuta)**	**Kaina ($)**
Kontrakto įrašymas	679,829	0.1434 ETH	13.10 $
Balsavimo teisės paskyrimas	63,959	0.0134 ETH	1.22 $
Balso paskyrimas	196,033	0.0413 ETH	3.77 $
Stebėjimas	0	0 ETH	0 $
Balsavimo stabdymas	642,460	0.1355 ETH	12.38 $
Rezultatų suskaičiavimas	0	0 ETH	0 $
Viso administratoriaus kaina	1386,248	0.2923 ETH	26,7 $
Viso 1 balsuotojo kaina	196,033	0.0413 ETH	3.77 $
Viso 100,000 balsuotojų kaina	19,603,300,000	4130 ETH	377,000 $

1 lentelė. Rinkimų organizavimo kainų lentelė

Norint organizuoti šalies mąsto rinkimus, akivaizdu, jog tai finansiškai būtų labai brangu. Tačiau, kaip sprendimas, galėtų būti naudojamas privatus Ethereum tinklas, kuriame transakcijas tvirtinti galėtų tik organizacijos, organizuojančios rinkimus, kompiuteriai. Šiame darbe piniginis aspektas bei galimybė organizuoti rinkimus privačiame blockchain tinkle nėra analizuojami.

6. Sistemos vertinimas bei atitikimas taisyklėms

Sukurtą sistemos modelį vertinsime pagal Ženevos projekto reikalavimus, detaliai išdėstytus 4.3 skyriuje. Vertinimas pateiktas antroje lentelėje.

Atitikimas (%)	Reikalavimas	Paaiškinimas
99%	Balsai negali būti nei sugadinti, nei pakeisti.	Šiame sprendime balsai negali būti pakeisti kito asmens negu rinkėjas. Sugadinti balsų taip pat negalima. Pagrindinė sąlyga: nėra tam tikro dalyvio arba dalyvių grupės, turinčios daugumą Ethereum platformoje ir siekiančios pažeisti visą tinklą. Šiai problemai spręsti gali būti naudojamas privatus Ethereum blockchain tinklas.
100%	Balsai negali būti atskleisti iki oficialaus balsų skaičiavimo.	Naudojant privatų raktą atskleistą iš validuotojų paslapčių, administratorius gali inicijuoti balsų skaičiavimą ir tik tuomet balsai yra dešifruojami.
100%	Tik užsiregistravę asmenys gali balsuoti.	
100%	Kiekvienas balsuotojas turi vieną ir tik vieną balsą.	Taip pat yra suteikiama papildoma galimybė pakeisti savo balsą visų rinkimų metu.
100%	Balso slaptumas yra garantuotas. Jo niekada nebus galima susieti su balsuotoju.	Balsuotojo asmens duomenys yra visiškai atskirti nuo Ethereum paskyros identifikatoriaus, tad nebus jokios galimybės nustatyti kas balsavo.
100%	Balsavimo sistema bus atspari DDOS („Denial of service attack“) atakoms.	Tinklas yra atsparus DDOS atakoms, kadangi visos aplikacijos yra vykdomos ant kiekvieno serverio esančio tinkle, tad kol yra bent vienas veikiantis serveris, sistema bus pasiekiama. [TO16]
100%	Balsuotojas yra apsaugotas nuo tapatybės vagystės.	Tik žmogus, identifikavęs save per išorinę sistemą, gaus Ethereum paskyrą. Dėl šios priežasties pavogti tapatybės nėra įmanoma.
100%	Skirtų balsų suma bus lygi gautų balsų sumai.	Kiekviename etape galima skaičiuoti sumas: gavusių teisę balsuoti, balsavusių bei gautų balsų skaičių. Skiriami balsai patenka į blockchain kaip transakcijos kviečiančios kontrakto balsavimo funkciją. Kontraktas išsaugo balsą. Taigi, skirtų balsų suma bus lygi gautų balsų sumai.
100%	Yra įmanoma įrodyti, jog tam tikras pilietis balsavo.	Yra įmanoma įrodyti, jog piliečiui buvo suteikta balsavimo teisė pagal administratoriaus duomenų bazėje pažymėtus įrašus, kurie pasirašyti validuotojų.
100%	Sistema nepriims balsų kitu laiku, nei balsavimo vyksmo laiko.	Kontrakte nurodytas balsavimo pabaigos ir pradžios laikas, tad balsuoti kitu laiku nebus įmanoma.
100%	Sistemai bus galima atlikti auditą.	Sistemos auditą gali atlikti bet koks technologiškai išsilavinęs žmogus.

2 lentelė. Rinkimų organizavimo kainų lentelė

7. Elektroninio balsavimo prototipas

Veikimo modelį, aprašytą 5 skyriuje, sudaro trys dalys: administracinė dalis, vartotojo dalis bei blockchain balsavimo logikos išmaniaisiais kontraktais dalis. Prototipas kuriamas su tikslu įgyvendinti aprašytą modelį bei pademonstruoti veikimą Ethereum blockchain tinkle. Buvo nuspręsta aprašyti išmanų kontraktą bei realizuoti tik blockchain esančią dalį. Kontraktą buvo pasirinkta rašyti Solidity programavimo kalba. Kontraktą (žr. Priede nr. 1) sudaro:

1. Inicializavimo funkcija. Ji kviečiama kuriant kontraktą bei jai nurodomi parametrai: balsavimo pradžios laikas, balsavimo pabaigos laikas, balsų šifravimo viešas raktas, validuotojų viešas raktas bei administratoriaus paskyros, turinčios teisę nutraukti balsavimą, adresas. Funkcijoje papildomai nuskaitoma administratoriaus, kuriančio bei įrašančio šį kontraktą į blokų grandinę, paskyros adresas ir visa informacija yra išsaugoma blockchain kontrakto duomenų saugykloje.
2. Teisės balsuoti suteikimo funkcija. Funkcija įvykdoma tik jei ją kviečia administratoriaus paskyra su pateiktu balsuotojo adresu bei tuo pačiu adresu, pasirašytu validuotojų. Jei šios sąlygos tenkinamos, kontrakte išsaugoma teisė balsuoti bei padidinamas registruotų balsuotojų skaitliukas.
3. Patikrinimo, ar pasirašytas balsuotojo adresas validuotojų, funkcija. Įgyvendinta nebuvo, tačiau jos veikimas paprastas: viešu validuotojų raktu, patikrinti ar informacija buvo pasirašyta jų parašu.
4. Balsavimo funkcija. Funkcijoje patikrinama, ar besikreipianti Ethereum paskyra turi balsavimo teisę, ar laikas yra tarp balsavimo pradžios ir pabaigos laikų. Patenkinus šias sąlygas, yra išsaugomas pateiktas šifruotas balsas bei padidinamas prabalsavusiųjų skaitliukas.
5. Balsavimo užbaigimas. Ši funkcija priima balsų dešifravimo raktą, patikrina ar funkciją kviečia administratoriaus paskyra, galinti nutraukti balsavimą bei ar balsavimo laikas pasibaigęs. Jei šios sąlygos tenkinamos, dešifravimo raktas išsaugomas kontrakto atmintyje bei tampa viešas. Nuo šio momento visi gali dešifruoti balsus bei suskaičiuoti rezultatus.

Visi sprendimai funkcijoms įgyvendinti paremti 5 skyriuje aprašytu procesu bei veikimo modeliu.

Prototipo kontraktas buvo įdiegtas į testinę Ethereum aplinką bei kontrakto funkcijos kviečiamos naudojant standartinę Ethereum blockchain tinklo piniginės naudotojo sąsają (žr. Priede nr. 2). Remiantis šiuo prototipu buvo skaičiuojami rinkimų kaštai, nurodyti skyriuje 5.6.5. Taip pat atlikus bandymą, buvo įrodyta, jog modelio Ethereum dalis, aprašyta 5 skyriuje, gali būti realizuota ir veikti korektiškai. Šį prototipą galima naudoti tolimesniam sprendimo plėtojimui.

Rezultatai ir išvados

Šiuo darbu parodyta, jog Ethereum blockchain technologija suteikia daug privalumų elektroninių rinkimų įgyvendinimui. Tačiau turi ir keletą trūkumų, kuriuos detaliai išanalizuoti bei pateikti sprendimus autorius planuoja ateityje. Sukurtas modelis parodė, jog ši technologija gali būti pritaikoma ir atitinka beveik visas iškeltas elektroninio balsavimo taisykles. Pateikta analizė, sistemos modelis bei prototipas gali būti naudojami kaip pagrindas elektroninio balsavimo vystymui ir taikymui.

Darbo tikslui pasiekti buvo atliktos užduotys ir gauti rezultatai:

1. Atlikta saugomu analizė parodė, jog blokų grandinė išlieka stabili ir turi tik labai nedidelę teorinę galimybę būti pažeista įsilaužėlių.
2. Atliktas palyginimas tarp blokų grandinės sistemos bei centrinio serverio architektūros aiškiai pabrėžė blokų grandinės sistemos stipriąsias puses būtent atstatomumo ir duomenų saugumo atžvilgiu.
3. Išanalizuotos Ethereum blockchain technologijos bei išmaniųjų kontraktų savybės parodė, jog šios technologijos turi daugybę pritaikymo galimybių ir gali užtikrinti decentralizuotą sprendimų priėmimą bei kodo vykdymą, kuris yra reikalingas elektroniniam balsavimui.
4. Apibrėžtos balsavimo taisyklės, kuriomis vadovaujantis turėtų būti įgyvendintas elektroninis balsavimas.
5. Paruoštas sistemos modelis, kuris parodo, kaip elektroninis balsavimas galėtų veikti bei įgyvendinti iškeltas taisykles. Taip pat pateiktos prielaidos, kuriomis vadovaujantis buvo sukurtas modelis.
6. Buvo sukurtas prototipas, kurio pagalba galima atlikti elektroninio balsavimo imitaciją Ethereum blockchain tinkle.

Literatūra

[AH16] Luke Anderson ir Holz. New kids on the block: an analysis of modern blockchains. *Arxiv preprint arxiv:1606.06530*, 2016. URL: https://arxiv.org/pdf/1606.06530.pdf.

[Aks12] Prof. B. B. Meshram Akshay Patil. Database access control policies. *International journal of engineering research and applications (ijera)*, 2012. ISSN: 22489622. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.416.4856&rep=rep1&type=pdf.

[Ant14] Andreas M. Antonopoulos. *Mastering bitcoin: unlocking digital crypto-currencies*. O'Reilly Media, Inc., 1st leid., 2014. ISBN: 9781449374044.

[Bar16] Dylan Bargar. The economics of the blockchain: a study of its engineering and transaction services marketplace, 2016. URL: http://tigerprints.clemson.edu/cgi/viewcontent.cgi?article=3422&context=all_theses&sei-redir=1&referer=https%3A%2F%2Fscholar.google.lt%2Fscholar%3Fas_ylo%3D2016%26q%3Dripple%2Blabs%26hl%3Dlt%26as_sdt%3D0%2C5#search=%22ripple%20labs%22.

[Bit16] Bitshares.org. Delegated proof-of-stake consensus. Žiūrėta: 2017-04-26. 2016. URL: https://bitshares.org/technology/delegated-proof-of-stake-consensus/.

[BL90] Josh Benaloh ir Jerry Leichter. Generalized secret sharing and monotone functions. *Proceedings on advances in cryptology*. Springer-Verlag New York, Inc., 1990, p. 27–35.

[blu16] IBM bluemix. Testing consensus and availability. Žiūrėta: 2017-04-26. 2016. URL: https://console.ng.bluemix.net/docs/services/blockchain/etn_pbft.html.

[BS] Prashanth P. Bungale and Swaroop Sridhar. Requirements for an electronic voting system, -.

[Buc04] Thomas M. Buchsbaum. E-voting: international developments and lessons learnt, 2004.

[But15] Vitalik Buterin. On public and private blockchains. Žiūrėta: 2017-04-26. 2015. URL: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains.

[CGG14] J.J. CHEN, B.E. Garin ir Girkar. Zero and near-zero data loss database backup and recovery. US Patent App. 13/791,517. 2014. URL: https://www.google.com/patents/US20140258241.

[Dav09] Pinal Dave. Sql server - introduction to sql server encryption and symmetric key encryption tutorial with script, 2009.

[DQ13] Anwar Pasha Deshmukh ir Riyazuddin Qureshi. Transparent data encryption – solution for security of database contents. *Corr*, abs/1303.0418, 2013. URL: http://arxiv.org/abs/1303.0418.

[EEs] E-Estonia. I-voting. Žiūrėta: 2017-05-09. URL: http://e-estonia.com/component/i-voting/.

[Eur04] Council of Europe. Legal, operational and technical standards for e-voting: recommendation. *Council of europe publishing*, 2004. URL: http://www.eods.eu/library/CoE_Recommentaion%20on%20Legal,%20Operational%20and%20Technical%20Standards%20for%20E-voting_2004_EN.pdf.

[Gen03] Chevallier M. ITU E-Government Workshop Geneva. Internet voting: status; perspectives and issue, 2003.

[GM15] Andres Guadamuz ir Christopher Marsden. Blockchains and bitcoin: regulatory responses to cryptocurrencies. *First monday*, 20(12-7), 2015.

[GMB15] Marco Guarnieri, Srdjan Marinovic ir David A. Basin. Strong and provably secure database access control. *Corr*, abs/1512.01479, 2015. URL: http://arxiv.org/abs/1512.01479.

[Gor14] M. M. Gorman. *Database management systems*, 2014.

[Guo04] Lifeng Guo. Cryptanalysis of threshold-multisignature schemes, 2004.

[Hub16] Jeniffer Hubard. Back up and restore of sql server databases. Žiūrėta: 2017-04-26. 2016. URL: https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/back-up-and-restore-of-sql-server-databases.

[Yer17] David Yermack. Corporate governance and blockchains. *Review of finance*:rfw074, 2017.

[Jef16] Correspondent Jeff Ward-Bailey. How bitcoin's 'blockchain' could transform banking, voting, and data. *Christian science monitor*:N.PAG, 2016. ISSN: 08827729.

[Jen17] Christoph Jentzsch. Public vs private chain. Žiūrėta: 2017-04-26. 2017. URL: https://blog.slock.it/public-vs-private-chain-7b7ca45044f#.yt20dlz5f.

[Ker15] Sean Michael Kerner. Financial and tech titans form open-source blockchain project. *Eweek*:1, 2015. ISSN: 15306283.

[KMS16] Ahmed Kosba, Andrew Miller ir Elaine Shi. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. *Security and privacy (sp), 2016 ieee symposium on*. IEEE, 2016, p. 839–858.

[kom14] Lietuvos Respublikos vyriausiosioji rinkimų komisija. Stebėtojo atmintinė, 2014.

[Lei17] Matthew Leising. Post-bitcoin technology has geeks, giants, and hackers excited. Žiūrėta: 2017-04-26. 2017. URL: https://www.bloomberg.com/news/articles/2017-03-23/post-bitcoin-technology-has-geeks-giants-and-hackers-excited.

[Li16] Victor Li. Bitcoin's blockchain technology being used in business, finance and contracts. *Aba journal*:1, 2016. ISSN: 07470088.

[McC15] Bennett T. McCallum. The bitcoin revolution. *Cato journal*, 35(2):347–356, 2015. ISSN: 02733072.

[MIC15] PAUL VIGNAS MICHAEL J. CASEY. The next big thing. *Economist*, 415(8937), 2015. ISSN: 00130613.

[Mur16] Danny Murray. Distributed resource sharing using the blockchain technology ethereum. Disertacija. California State University, Sacramento, 2016. URL: http://csus-dspace.calstate.edu/bitstream/handle/10211.3/182265/Distributed_Resource_Sharing-Danny_Murray.pdf?sequence=1.

[Pil15] Marc Pilkington. Blockchain technology: principles and applications. *Browser download this paper*, 2015. URL: http://inpluslab.sysu.edu.cn/files/Paper/Summary/Blockchain_Thinking__The_Brain_As_A_Decentralized_Autonomous_Corporation.pdf.

[Pil16] Marc Pilkington. Blockchain technology: principles and applications. Žiūrėta: 2017-04-26. 2016. URL: http://inpluslab.sysu.edu.cn/files/Paper/Summary/Blockchain_Thinking__The_Brain_As_A_Decentralized_Autonomous_Corporation.pdf.

[Sta16] Josh Stark. Making sense of blockchain smart contracts. Žiūrėta: 2017-04-26. 2016. URL: http://www.coindesk.com/making-sense-smart-contracts/.

[TO16] Nikolaos Petros Triantafyllidis ir TNO Oskar van Deventer. Developing an ethereum blockchain application, 2016.

[Vyt92] Lietuvos Respublikos Aukščiausiosios tarybos pirmininkas Vytautas Landsbergis. Lietuvos respublikos seimo rinkimų įstatymas, 1992.

[XPZ16] Xiwei Xu, Cesare Pautasso ir Liming Zhu. The blockchain as a software connector. *Software architecture (wicsa), 2016 13th working ieee/ifip conference on*. IEEE, 2016, p. 182–191.

[ZXD16] Zibin Zheng, Shaoan Xie ir Hong-Ning Dai. Blockchain challenges and opportunities: a survey, 2016. URL: http://inpluslab.sysu.edu.cn/files/blockchain/blockchain.pdf.

Priedas nr. 1

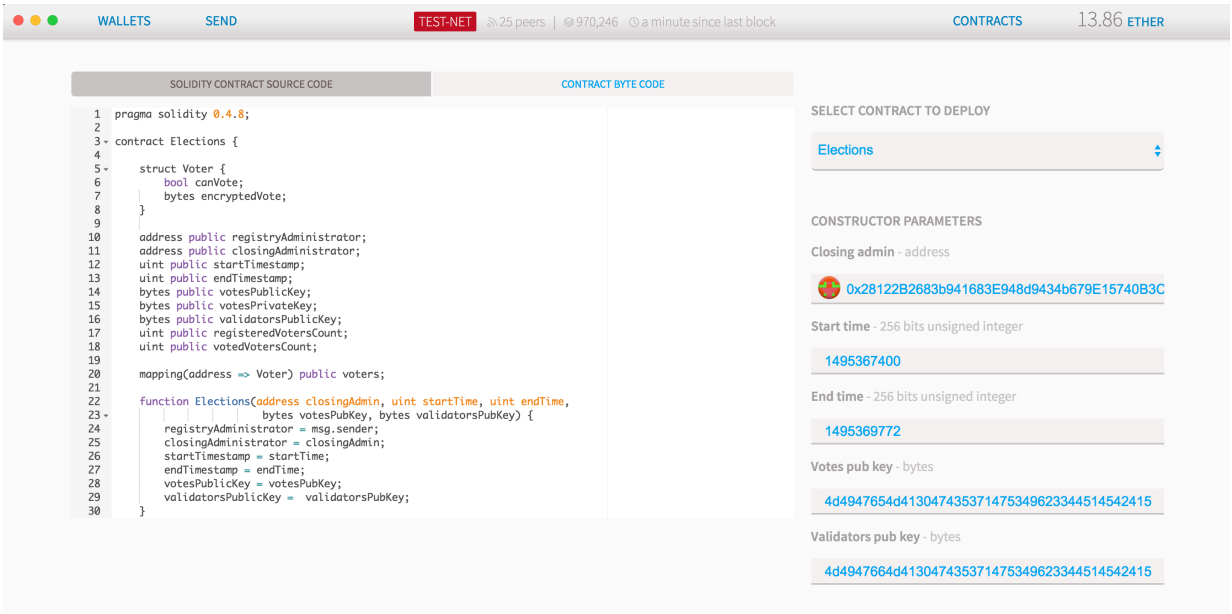
Solidity programavimo kalba parašytas elektroninio balsavimo kontraktas

```
pragma solidity 0.4.8;

contract Elections {

    struct Voter {
      bool canVote;
        bytes encryptedVote;
    }

  address public registryAdministrator;
  address public closingAdministrator;
  uint public startTimestamp;
  uint public endTimestamp;
  bytes public votesPublicKey;
  bytes public votesPrivateKey;
  bytes public validatorsPublicKey;
  uint public registeredVotersCount;
  uint public votedVotersCount;

  mapping(address => Voter) public voters;

  function Elections(address closingAdmin, uint startTime, uint endTime,
            bytes votesPubKey, bytes validatorsPubKey) {
    registryAdministrator = msg.sender;
    closingAdministrator = closingAdmin;
    startTimestamp = startTime;
    endTimestamp = endTime;
    votesPublicKey = votesPubKey;
    validatorsPublicKey =  validatorsPubKey;
  }

  function giveRightToVote(address voter, bytes signedVoterAddressByValidator)
    {
    if (msg.sender != registryAdministrator) {
      throw;
```

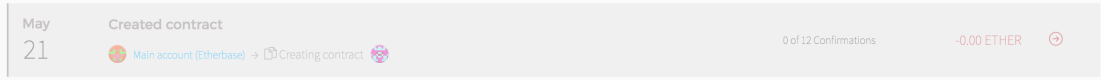
```
35      }
36      if (!isConfirmedByValidators(voter, signedVoterAddressByValidator)) {
37        throw;
38      }
39
40        voters[voter].canVote = true;
41        registeredVotersCount++;
42    }
43
44    function isConfirmedByValidators(address voter, bytes
       signedVoterAddressByValidator) private returns (bool) {
45      // TODO: check signature
46      return true;
47    }
48
49    function vote(bytes vote) {
50      Voter sender = voters[msg.sender];
51      if (!sender.canVote)
52        throw;
53
54      if(block.timestamp < startTimestamp || block.timestamp > endTimestamp)
55        throw;
56
57      sender.encryptedVote = vote;
58      votedVotersCount++;
59    }
60
61
62    function endVoting(bytes decryptionKey) {
63      if (msg.sender != closingAdministrator)
64        throw;
65      if((block.timestamp > startTimestamp && block.timestamp < endTimestamp))
66        throw;
67
68      votesPrivateKey = decryptionKey;
69    }
70
71  }
```

Priedas nr. 2

Elektroninio balsavimo prototipo demonstracija

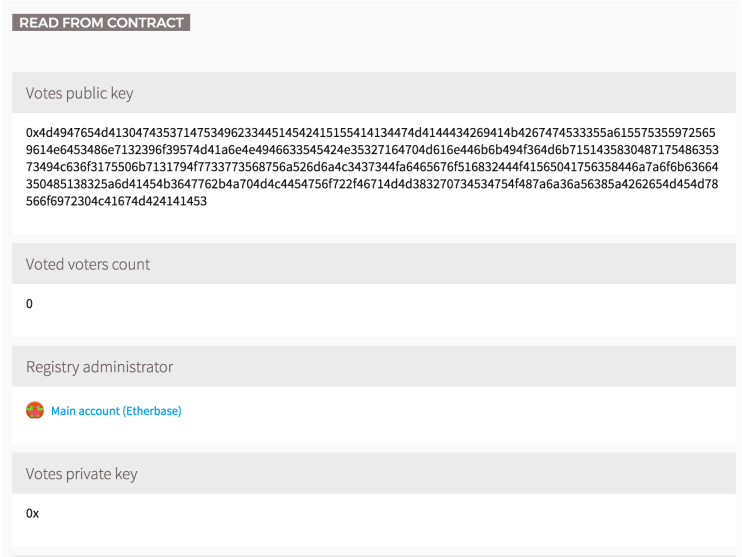


5 pav. Kontrakto sukūrimas

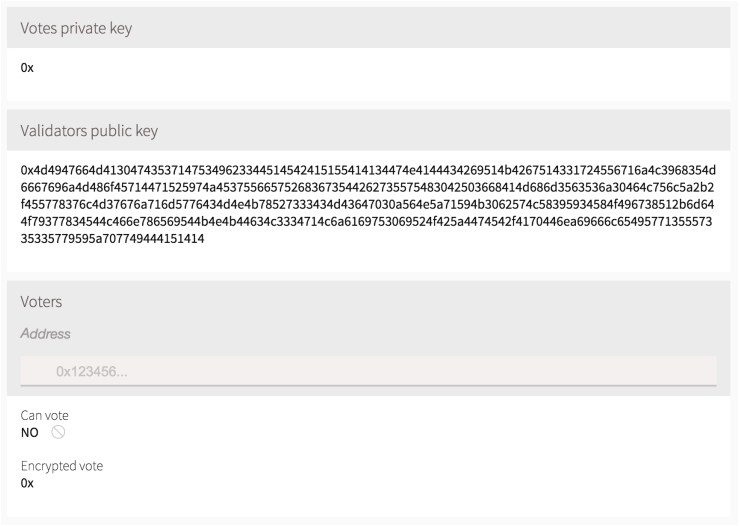


6 pav. Kontrakto sukūrimo transakcija

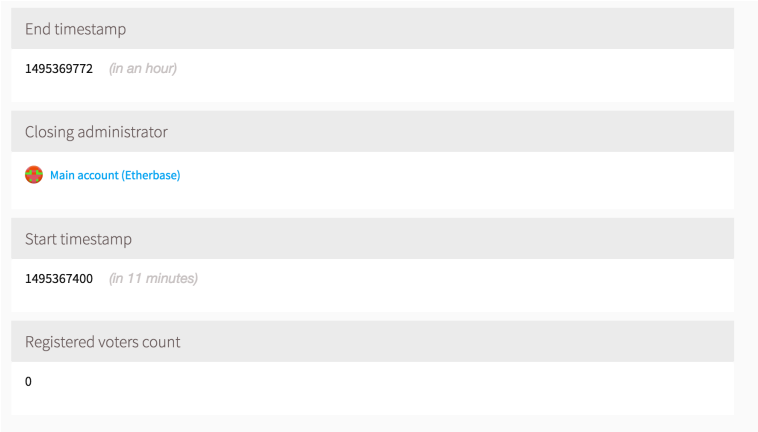
7 pav. Kontrakto sukūrimo transakcija tvirtinama tinklo



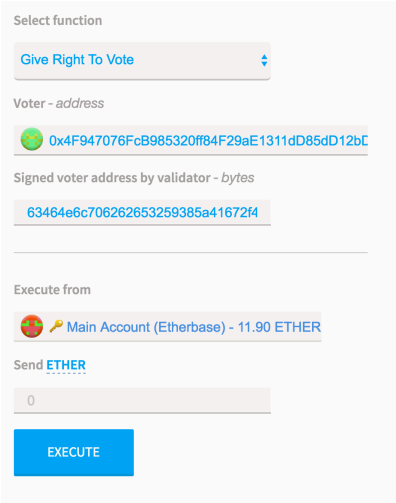
8 pav. Įrašytas kontraktas bei jo duomenys 1



9 pav. Įrašytas kontraktas bei jo duomenys 2

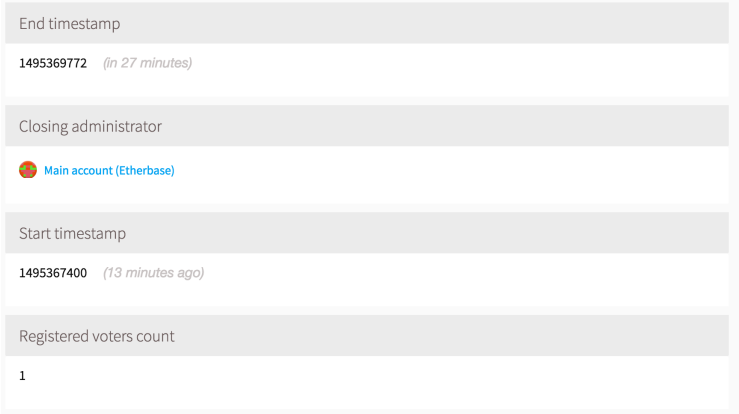


10 pav. Įrašytas kontraktas bei jo duomenys 3



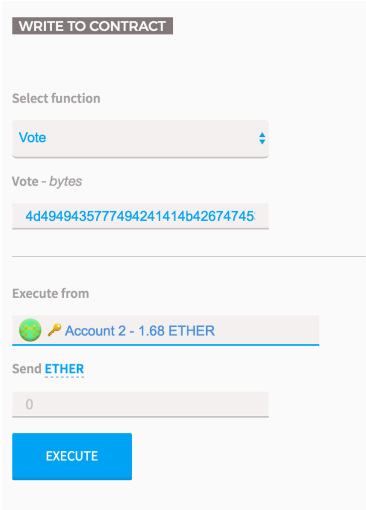
11 pav. Balsavimo teisės suteikimas

12 pav. Balsavimo teisės suteikimo transakcijos tvirtinimas

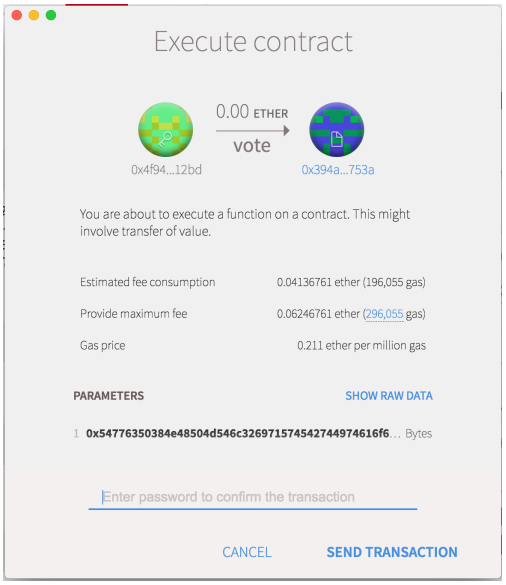


13 pav. Kontrakto duomenys po teisės suteikimo 1

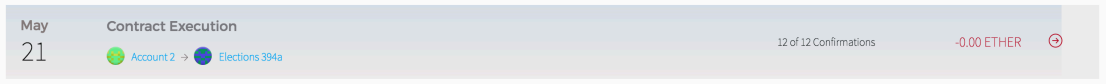
14 pav. Kontrakto duomenys po teisės suteikimo 2



15 pav. Balsavimas



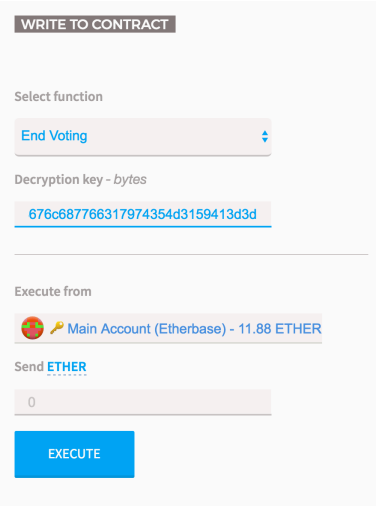
16 pav. Balsavimo transakcijos patvirtinimo langas



17 pav. Balsavimo transakcijos tvirtinimas

18 pav. Kontrakto duomenys po balsavimo 1

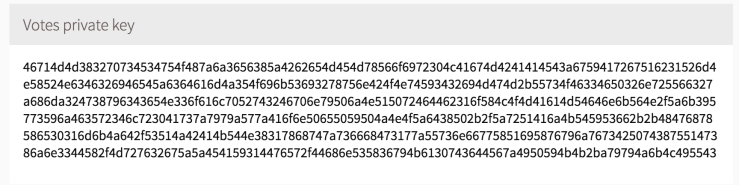
19 pav. Kontrakto duomenys po balsavimo 2



20 pav. Balsavimo užbaigimas

21 pav. Balsavimo užbaigimo kontrakto tvirtinimas

22 pav. Kontrakto duomenys po balsavimo užbaigimo 1



23 pav. Kontrakto duomenys po balsavimo užbaigimo 2