VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
PROGRAMŲ SISTEMŲ KATEDRA

Skaitmeninės tapatybės valdymas taikant blokų grandinę

Digital Identity Management using Blockchain

Bakalauro darbas

Atliko:	Jurgis Kargaudas	(parašas)
Darbo vadovas:	asist. Aurimas Šimkus	(parašas)
Darbo recenzentas:	lekt. Andrius Adamonis	(parašas)

Vilnius – 2018

Santrauka

Bus pridėta parašius visą darbą.

Summary

To be added when the whole thesis is finished.

Įvadas

Interneto paslaugos šiais laikais yra neatsiejama žmonių gyvenimo dalis. Norėdami individualizuoti turinį, sustiprinti taikomosios programos saugumą ar siekdami iš anksto išvengti kenkėjiškų tikslų turinčių asmenų ar sukurtų robotų, paslaugų tiekėjai siekia identifikuoti savo naudotojus. Interneto naudotojų skaičiui perkopus 4 milijardus [Min18], o kiekvienam naudotojui vidutiniškai turint po 7 skirtingas socialines paskyras [MM17], asmenų tapatybių valdymas, autentifikavimas ir autorizavimas tampa vis didesniu iššūkiu.

Tapatybių valdymas kelia problemų naudotojams. Bene didžiausi atsiradę keblumai: milžiniškas įsimintinų slaptažodžių kiekis bei sunkumai kontroliuojant savo asmens duomenų sklaidą skirtingose sistemose. Vidutiniškai interneto naudotojas turi 25 slaptažodžių reikalaujančias paskyras ir per dieną turi įvesti 8-is slaptažodžius [FH07]. Susidarius tokiai situacijai, per didelis įsimintinų slaptažodžių kiekis neretai priverčia naudotojus paaukoti saugumą dėl patogumo ir pradėti naudoti tą patį slaptažodį sirtingoms sistemoms [PM03; Sam99]. Naudotojas, turėdamas keletą paskyrų skirtingose sistemose, taip pat praranda dalį savo asmens duomenų kontrolės. Jam tenka pasitikėti taikomosios programos naudojamomis technologijomis ir metodais ir tikėtis, kad jie bus pakankamai saugūs ir stabilūs bei suteikti asmens duomenys nepasieks nepageidaujamų adresatų. Didėjant naudojamų paslaugų kiekiui, naudotojo skaitmeninės tapatybės duomenis turi vis daugiau taikomųjų programų ir bent vienai iš jų patyrus programišių įsilaužimą ar kitokią nesėkmę, jautrūs naudotojo duomenys gali būti paviešinti.

Taikyti skirtingi metodai skaitmeninės tapatybės valdymo internete problemoms spręsti. Šiais laikais vienas dažniausiai internete sutinkamų sprendimų yra vienkartinis prisijungimas (angl. *Single Sign-On*). Šis sprendimas leidžia naudotojui pasirinkti vieną tapatybės tiekėją (angl. *identity provider*) ir patikėti jam skaitmeninės tapatybės valdymą. Tokiu būdu naudotojui pakanka turėti tik paskyrą tapatybės tiekėjo sistemoje bei kreipiantis į paslaugas prisijungti per jį. Tačiau šis sprendimo būdas taip pat turi aiškių trūkumų: naudotojas negali prisijungti prie paslaugų, nepalaikančių pasirinkto tapatybės tiekėjo, jo pasiekiamumas tampa vieninteliu nesėkmės tašku (angl. *single point of failure*), naudotojas taip pat praranda dalį savo asmens duomenų kontrolės. Naršantis internete asmuo yra priverstas pasitikėti tapatybės tiekėjo gebėjimu perduoti tik naudotojo leistus asmens duomenis ir tik toms trečiosioms šalims, kurias jis patvirtina. Kaip rodo *Cambridge Analytica* incidentas [Gra18], net didžiosios kompanijos, tokios kaip *Facebook*, ne visada sugeba tai užtikrinti.

Blokų grandinė (angl. *blockchain*) yra nauja alternatyva skaitmeninės tapatybės valdymui. Ši technologija veikia kaip paskirstytų įrašų platforma (angl. *distributed ledger platform*), kurioje kiekvienas įrašas yra nekintamas, o visi užfiksuoti įrašai atspindi tikslią transakcijų istoriją nuo pat grandinės sukūrimo [Baa16]. Saugant tapatybės duomenis šioje grandinėje ir pritaikius reikiamą blokų grandinės pasiekiamumo lygį įrašų rašymui ir skaitymui, asmuo visada žinotų, kokia trečioji šalis gali pasiekti kokius tapatybės duomenis. Kadangi blokų grandinė yra decentralizuota, pritaikius ją skaitmeninių tapatybių valdyme taip pat būtų galima išvengti šioje srityje dažnos vienintelio nesėkmės taško problemos.

Šiame darbe blokų grandinės tinkamumas skaitmeninės tapatybės valdymui nagrinėja-

mas iš naudotojo perspektyvos. Pateikus esminius naudotojų poreikius identiteto valdymui, apžvelgiamas dabar naudojamų sistemų gebėjimas įgyvendinti šiuos reikalavimus. Įvertinus pagrindines neišspręstas naudotojams kylančias problemas, tiriama, kaip blokų grandinė gali padėti jas išspręsti, kokie tokio blokų grandinės panaudojimo skaitmeniniame tapatybės valdyme pranašumai, trūkumai bei priėmimo barjerai (angl. *adoption barriers*).

Darbo tikslas - išanalizuoti blokų grandinės tinkamumą skaitmeninės tapatybės valdymui.

Darbe keliami uždaviniai:

1. Išskirti naudotojų poreikius skaitmeninės tapatybės valdymo sistemoms.
2. Išnagrinėti dabartinius skaitmeninės tapatybės valdymo sprendimus ir jų gebėjimą įgyvendinti naudotojų reikalavimus.
3. Apibūdinti blokų grandinės technologiją ir jos savybes, leidžiančias spręsti naudotojų identifikavimo problemas.
4. Pateikti blokų grandinės panaudos atvejį skaitmeninės tapatybės valdymui ir sukurti jo veikimą demonstruojantį prototipą.
5. gal reiks įdėt esamus blockchain sprendimus
6. Įvertinti pateiktą sprendimą apibūdinant jo privalumus, trūkumus ir pritaikymo barjerus.
7. Palyginti pristatytą sprendimą su standartiniais naudotojų autentifikavimo ir autorizavimo būdais.

TURINYS

1. Skaitmeninės tapatybės valdymo apžvalga

1.1. Tapatybės patvirtinimo poreikis

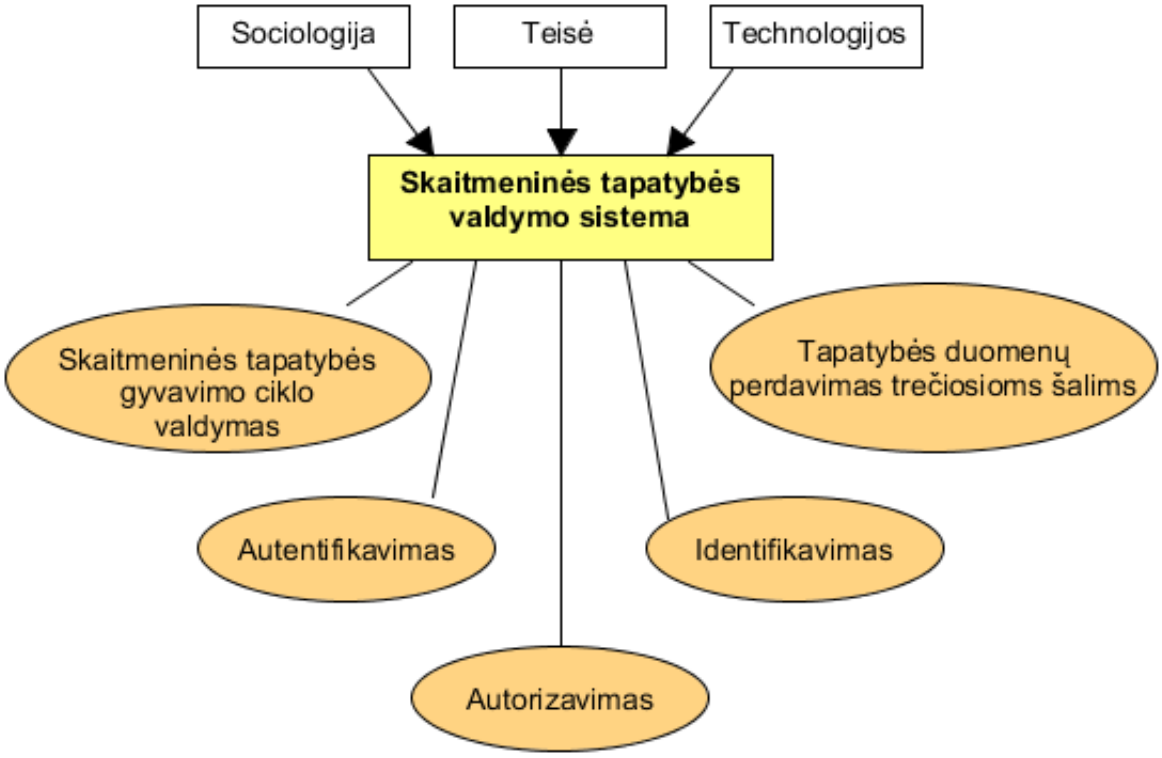
Šiais laikais naudotojo identifikavimas yra svarbi interneto taikomųjų programų dalis. Paslaugų tiekėjai identifikuoja savo naudotojus norėdami [Ral14]:

- registruoti (angl. *log*) naudotojų veiklą,
- užtikrinti, kad naudotojas iš tikrųjų yra asmuo, kuris sakosi esąs,
- suteikti dalį funkcionalumo tik autorizuotiems naudotojams,
- individualizuoti tinklalapio ar taikomosios programos turinį pagal naudotojo poreikius,
- sukurti paslaugos naudotojų bendruomenę,
- išvengti galimų anoniminių naudotojų atakų.

Dėl išvardytų priežasčių naudotojų identifikavimas atlieka svarbią rolę įvairiose taikomųjų programų srityse - elektroninėje valdžioje, elektroninėje komercijoje, verslo sumanume (angl. *business intelligence*), tyrimuose bei saugume (angl. *homeland security*) [GV09]. Kiekvienas paslaugų tiekėjas turi pasirinkti, kaip autentifikuoti, ir, jei reikia, autorizuoti naudotojus. Programos kūrėjas taip pat turi užtikrinti naudotojo suteiktų duomenų saugumą, o naudotojui tenka rūpintis skirtingų turimų paskyrų priežiūra ir savo duomenų sklaida tarp skirtingų sistemų. Minimus tapatybės atpažinimo skaitmeninėje erdvėje aspektus nagrinėja skaitmeninės tapatybės valdymo disciplina.

1.2. Skaitmeninės tapatybės valdymo samprata

Dėl nuolat vykstančios interneto ir jame esančių paslaugų plėtros tapatybių valdymo uždavinys pastaraisiais metais tapo itin svarbus [GV09]. Skaitmeninės tapatybės valdymo pagrindinis uždavinys yra kontroliuoti tapatybę ir su ja susijusius procesus, tokius kaip autentifikavimas, autorizavimas, prieigų kontrolė, tapatybės gyvavimo ciklo valdymas bei saugus tapatybės atributų perdavimas trečiosioms šalims [CY10; DP08]. Sprendžiant šį uždavinį, sukurta skirtingų skaitmeninės tapatybės valdymo sistemų. Šioms sistemoms įtaką daro kiti tapatybę nagrinėjantys mokslai (pvz. sociologija), taip pat jos gali atlikti keletą skirtingų funkcijų, susijusių su naudotojų tapatybe. Žemiau pateikiama diagrama, kurioje apibendrintas tapatybės valdymo sistemų kontekstas bei pagrindinės atliekamos užduotys:



1 pav. Skaitmeninių tapatybių valdymo sistemų kontekstas ir užduotys [GV09]

Paveiksle matomos disciplinos turi skirtingą poveikį tapatybių valdymo sistemoms. Sociologija padeda apibrėžti tapatybę ir jos atitikmenį skaitmeninėje erdvėje, teisės mokslas nusako tapatybės duomenų naudojimo reikalavimus, o esamos technologijos formuoja sistemos įgyvendinimo niuansus. Verta pastebėti, kad tapatybės valdymo sistema gali atlikti ne visas diagramoje nurodomas funkcijas, o tik dalį iš jų. Taip pat, 1-ame paveiksle bei visame darbe naudojamos skaitmeninės tapatybės valdymo sąvokos, tokios kaip *identifikavimas*, *autentifikavimas* ar *autorizavimas* neretai suprantamos skirtingai, o tai sukelia vieningos terminologijos trūkumą ir dėl jo kylančius neaiškumus [GV09]. Dėl to skyriuje „Sąvokų apibrėžimai“ pateikiami darbe naudojamų terminų aiškinimai.

1.3. Naudotojų poreikiai skaitmeninės tapatybės valdymo sistemoms

Skaitmeninės tapatybės valdymas yra plati sritis, kurią galima analizuoti iš skirtingų pusių: paslaugų tiekėjo, tapatybės tiekėjo ar naudotojo. Šiame darbe į skaitmeninių tapatybių valdymą žvelgta iš naudotojo perspektyvos - kaip skaitmeninio valdymo sistemos atitinka naudotojų poreikius bei lūkesčius. Išskirtos šios naudotojoms aktualios sistemų savybės:

- atpažinimo duomenų kiekis. Naudotojui vidutiniškai turint 25 paskyras, reikalaujančias slaptažodžių [FH07] bei naudojant nuo 2 iki 12-os el. paštų [GC07], jis tampa priverstas prisiminti vis daugiau slaptažodžių bei identifikatorių. Atsimintinų autentifikavimo duomenų kiekiui augant, naudotojai yra linkę aukoti saugumą dėl patogumo ir naudoti panašius slaptažodžius skirtingose sistemose [PM03; Sam99];

- saugumas. Privatumas yra žmogaus poreikis ir visa visuomenė nukentėtų nuo jo nebuvimo [MS07]. Suteikiant savo asmens duomenis internete naudotojai tikisi, kad jie bus patikimai saugomi ir nepasiekiami programišiams. Tapatybių valdymo sistemos turėtų būti budrios saugumo rizikoms bei viešai skelbti saugumui skirtas priemones ir atliktų saugumo analizių rezultatus, kad tiek naudotojai, tiek paslaugų tiekėjai galėtų pasitikėti tapatybių valdymo sistemomis [DD08];
- asmens duomenų kontrolė. Pasak Nyderlanduose atliktų tyrimų, naudotojai nesijaučia kontroliuojantys savo asmens duomenų internete [Baa16]. Dėl to naudotojai pradeda nepasitikėti taikomųjų programų kūrėjais, nes jie pilnai nežino, kokia informacija apie juos kaupiama ir kokioms sistemoms ji perduodama;
- patogumas (angl. *usability*). Naudotojams skaitmeninės tapatybės valdymas neretai yra tik pašalinis mechanizmas, reikalingas norint pasiekti paslaugą [DD08]. Dėl šios priežasties sistemos naudojimosi patogumas yra svarbus - kuo tapatybės valdymas yra labiau integruotas su asmens jau naudojamomis sistemomis, kuo mažiau jis reikalauja papildomo naudotojo įsitraukimo ir kuo suteikia geresnę naudotojo patirtį (angl. *user experience*), tuo labiau naudotojas bus linkęs pasirinkti šį identiteto valdymo sprendimą.

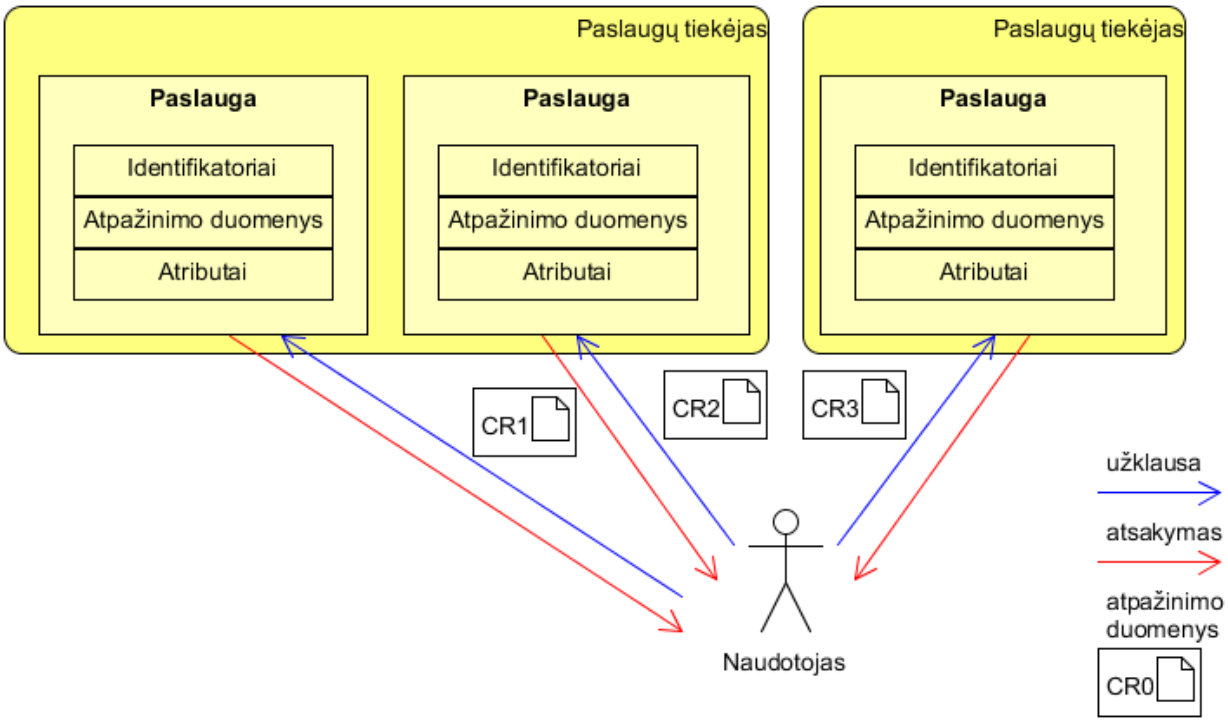
1.4. Skaitmeninės tapatybės valdymo modeliai

Naudojamų tapatybių valdymo sistemų architektūros bei veikimo principai yra skirtingi - S. Clauß ir M.Köhntopp savo tyrime pastebi, kad nėra vieningo standarto identiteto valdymo sistemoms [CK01]. Šiame skyriuje tiriami 3-ys dažniausiai naudojami identiteto valdymo modeliai. Tiriant kiekvieną modelį, pirmiausia apžvelgti jo bendri veikimo principai. Taip pat apžvelgtos paplitusios modelį įgalinančios technologijos (angl. *enabling technology*), nes modelio realizacijoje taikomi standartai ar protokolai gali turėti įtakos naudotojų poreikiams. Galiausiai, analizuotas modelio atitikimas naudotojų lūkesčiams, išvardytiems 1.3 skyrelyje.

1.4.1. Izoliuotas tapatybių valdymas

1.4.1.1. Modelis

Izoliuotame modelyje paslaugų tiekėjas yra ir tapatybės tiekėjas, nes visos su tapatybės valdymu susijusios operacijos yra atliekamos vieno serverio. Tapatybės duomenų saugojimas, autentifikavimas ir autorizavimas yra įgyvendinti paties paslaugų tiekėjo [CY10]. Kiekvienas naudotojas turi atskirus identifikatorius kiekvienai naudojamai paslaugai. Modelis grafiškai pavaizduotas žemiau esančiame paveiksle:



2 pav. Izoliuotas skaitmeninės tapatybės valdymas [CY10]

Pagal izoliuotą modelį, naudotojas turi savo paskyrą kiekvienoje naudojamoje sistemoje. Kiekvieną kartą autentifikuojant ar autorizuojant naudotoją, tai atlieka pats paslaugų tiekėjas, bendraudamas tiesiogiai su naudotoju (jo naršykle). Naudotojui prisijungus prie vieno tinklalapio ir gavus prieigos raktą, jis gali toliau naudotis šiuo tinklalapiu, tačiau prireikus pasinaudoti kita taikomąja programa, tapatybės atpažinimo veiksmai (autentifikavimas, autorizavimas) turi vėl būti atlikti naujoje sistemoje.

1.4.1.2. Realizacijos bei įgalinančios technologijos

Kadangi šis naudotojų autentifikavimo bei autorizavimo modelis naudojamas seniausiai, yra gana nemažai jį įgyvendinusių taikomųjų programų. Lietuvoje šį modelį naudoja „Tiketa“, „Bilietai.lt“, „Pigu.lt“, „Varle.lt“, pasaulyje - „Booking.com“, „Skycop“, „AirBnB“ bei kitos platformos. Verta pastebėti, kad dalis iš jų jau remiasi ne vien tik savo izoliuotu tapatybės valdymu, bet jau turi į savo sistemas integravę ir papildomų autentifikavimo būdų (pvz. prisijungimą per „Facebook“ ar „Google“).

Realizacijų technologiniai sprendimai dažniausiai nėra viešai prieinami. Šiame modelyje kiekvienas paslaugų tiekėjas yra ir tapatybės tiekėjas, tad nereikia apibrėžti protokolų, duomenų formatų ar kitų detalių, kurios formalizuotų bendravimą tarp pasikliaujančiosios šalies ir tapatybės tiekėjo - visa tai pats nusprendžia ir įgyvendina paslaugų tiekėjas.

1.4.1.3. Naudotojų poreikių įgyvendinimas

Nors izoliuotas tapatybių valdymas yra gana paprastas paslaugų tiekėjams, tačiau jis greitai tampa nebekontroliuojamu naudotojams [JP05]. Jis verčia naudotojus turėti paskyrą kiekvienai paslaugai, o tai lemia daugybės identifikatorių ir slaptažodžių valdymą. Tai sukelia „slaptažodžių nuovargį“ (angl. *password fatigue*), o tai veda prie tų pačių identifikatorių ir slaptažodžių pasirinkimo skirtingoms paslaugoms [DD08].

Izoliuotame identiteto valdyme programišiams sunkiau atlikti sukčiavimo (angl. *phishing*) ataką, nes naudotojas nebūna nukreipiamas į tapatybės tiekėjo puslapį. Tai pagerina šio modelio saugumą. Dėl to, kad paslaugų tiekėjas yra ir tapatybės tiekėjas, šiame modelyje galima išvengti duomenų perdavimo tarp skirtingų serverių - tokiu būdu sumažėja ir rizika, kad šiuos duomenis jų persiuntimo metu perims programišius. Tačiau, standartų duomenų formatams bei perdavimui nebuvimas gali paskatinti paslaugų tiekėjus nepažvelgti į tai atsakingai ir įgyvendinti bendravimą su naudotojo naršykle atmestinai.

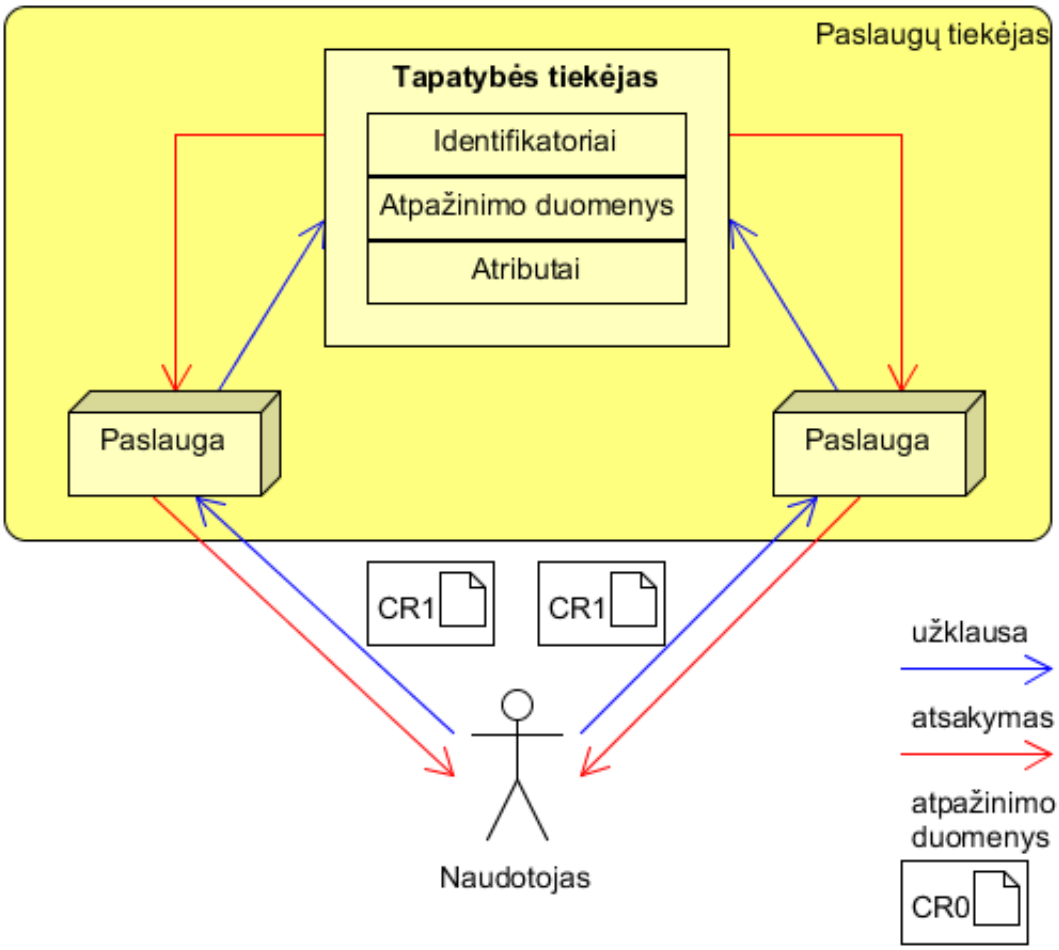
Naudotojų asmens duomenų kontrolė šiame modelyje priklauso nuo kiekvienos paslaugos. Asmenys atskirai suteikia savo duomenis kiekvienai paslaugai, dažniausiai paskyros sukūrimo metu. Jei paslauga informuoja apie duomenų panaudos atvejus (pvz. kam bus naudojamas el. pašto adresas), tuomet asmuo jausis labiau užtikrintas savo duomenų kontrole. Tačiau dėl šiame modelyje neišvengiamo duomenų suteikimo dideliam skirtingų paslaugų kiekiui, asmeniui tampa sunku prisiminti kiekvienos naudojamos platformos duomenų platinimo taisykles.

Izoliuotame tapatybės valdyme naudotojams tenka kartoti identifikavimo procesus (autentifikavimą, autorizavimą) tiek kartų, kiek paslaugų siekiama naudotis. Tai vargina naudotojus ir kuria blogą naudotojo patirtį. Tačiau, izoliuotas tapatybės valdymas pasižymi nuoseklia vartotojo sąsaja (dėl visų tapatybės valdymo procesų įgyvendimo tame pačiame paslaugų tiekėjo puslapyje), tad tai šiek tiek pagerina bendrą naudotojo patirtį.

1.4.2. Centralizuotas tapatybių valdymas

1.4.2.1. Modelis

Centralizuotame skaitmeninių tapatybių valdyme egzistuoja vienas tapatybės tiekėjas, į kurį kreipiasi visos paslaugos, esančios to paties paslaugų tiekėjo domene [JP05]. Kai paslaugų tiekėjui reikia autentifikuoti naudotoją (ar atlikti kitą tapatybės valdymo procesą), jis persiųs naudotojo pateiktus atpažinimo duomenis tapatybės tiekėjui, siekdamas pabaigti procesą [CY10]. Naudotojui šiame modelyje užtenka vienų atpažinimo duomenų, su kuriais jis gali prisijungti prie visų to paties paslaugų tiekėjo paslaugų. Modelio veikimas iliustruotas 3-iame paveiksle.



3 pav. Centralizuotas skaitmeninės tapatybės valdymas [CY10]

Centralizuotame modelyje paslaugų tiekėjo ir tapatybės tiekėjo funkcijos tampa atskirtos - tapatybės tiekėjas rūpinasi naudotojo identiteto valdymu, o paslaugų tiekėjas koncentruojasi į paslaugos vystymą. Tai sudaro patrauklesnes sąlygas naudotojui, tačiau taip pat sukuria vieno nesekmės taško (angl. *single point of failure*) sistemą. Tapatybės tiekėjo sistemai tapus nepasiekiamai, naudotojai nebegali naudotis nei viena paslauga tame pačiame domene.

1.4.2.2. Realizacijos bei įgalinančios technologijos

Centralizuotas modelis tinkamiausias naudoti darbuotojams įmonės ribose arba vieno paslaugų tiekėjo paslaugoms [JP05]. Pateikiami pavyzdžiai abiems šioms realizacijoms.

Viena iš įmonėse naudojamų realizacijų centralizuotam tapatybės valdymui - katalogų prieigos protokolas (angl. *Lightweight Directory Access Protocol*, toliau LDAP), naudojamas pasiekti ir palaikyti informaciją interneto tinkle [Kuk11]. Šis protokolas dažniausiai sujungiamas su aktyviąja direktorija (angl. *active directory*) ir leidžia laikyti kompanijos darbuotojų tapatybės informaciją vienoje vietoje. Taikomosios programos siunčia užklausas į LDAP serverį, kuriose nurodo norimą atlikti veiksmą (pvz. naudotojo autentifikavimą ar naudotojo atributų atnaujinimą). Informacija per LDAP perduodama LDAP duomenų apsikeitimo formatu (LDIF).

LDAP grįstas vienkartinis prisijungimas leidžia įmonės darbuotojams vieną kartą prisijungti prie tam tikros įmonėje naudojamos programos ir nebekartoti prisijungimo kreipiantis į kitą programą. Tačiau, tai galios tik toms programoms, kurios pasiekiamoms darbuotojams per vidinį intranetą [Kuk11]. Dėl šios priežasties LDAP grįstas centralizuotas tapatybės valdymas retai sutinkamas už įmonių intraneto ribų [Kuk11].

Centralizuotas tapatybės valdymas taip pat gali būti realizuotas ir ne įmonės ribose, jei konkretus paslaugų tiekėjas turi keletą paslaugų, skirtų naudotojams. Tokiu atveju jis gali turėti centralizuotą posistemę tapatybės valdymui, o naudotojui užtenka turėti vieną paslaugų tiekėjo paskyrą visoms įmonės paslaugoms. Tokios realizacijos pavyzdys - „Atlassian“ įmonės paslaugos. Naudotojui pakanka turėti vieną „Atlassian“ paskyrą ir jis gali naudotis skirtingais šio paslaugų tiekėjo produktais, tokiais kaip „Jira“, „Confluence“, „Bitbucket“ bei kitais. Vieną kartą prisijungus prie „Atlassian“ programos (pvz. „Jira“), naudotojas tampa autentifikuotas ir kituose „Atlassian“ tinklalapiuose.

1.4.2.3. Naudotojų poreikių įgyvendinimas

Iš naudotojo perspektyvos, centralizuotas modelis yra patogesnis nei izoliuotas. Naudotojui pakanka turėti vienus atpažinimo duomenis, kurie bus tinkami visoms konkretaus paslaugų tiekėjo programoms. Tačiau, norint pasiekti kito paslaugų tiekėjo paslaugą, naudotojo turima paskyra nebebus tinkama.

Centralizuotas tapatybės valdymas ne intranete gali patirti sukčiavimo (angl. *phishing*) ataką, jei paslaugų tiekėjas nukreipinėja naudotoją į tinklalapį kitame domene. Tačiau, kadangi paslaugų tiekėjas tapatybės valdymą realizuoja pats, jis gali leisti naudotojui vesti identifikavimo duomenis ir pačiame paslaugos puslapyje (o ne nukreipiant į kitą sistemą) arba nukreipti į tame pačiame domene esantį, paties paslaugų tiekėjo valdomą puslapį. Tai sumažina sukčiavimo jautrumo (angl. *phishing susceptibility*) galimybę.

Naudotojai neturi didelės asmens duomenų kontrolės centralizuotame tapatybės valdyme. Nors, skirtingai nei izoliuotame modelyje, jie suteikia duomenis mažesniam kiekiui taikomųjų programų (nebe kiekvienai programai, o kiekvienam paslaugų tiekėjui), tačiau tai vis dar nėra ideali situacija. Naudotojams vistiek reikia kontroliuoti visas skirtingų paslagų tiekėjų paskyras ir žinoti su jomis susijusias duomenų saugojimo bei platinimo taisykles. Taip pat, jeigu modelis taikomas ne įmonės intranete (kur duomenų apsikeitimui apibrėžtas formatas, pvz. LDIF), naudotojas nežino, kokiu būdu jo prisijungimo ar kiti duomenys bus perduodami iš vienos paslaugos į kitą.

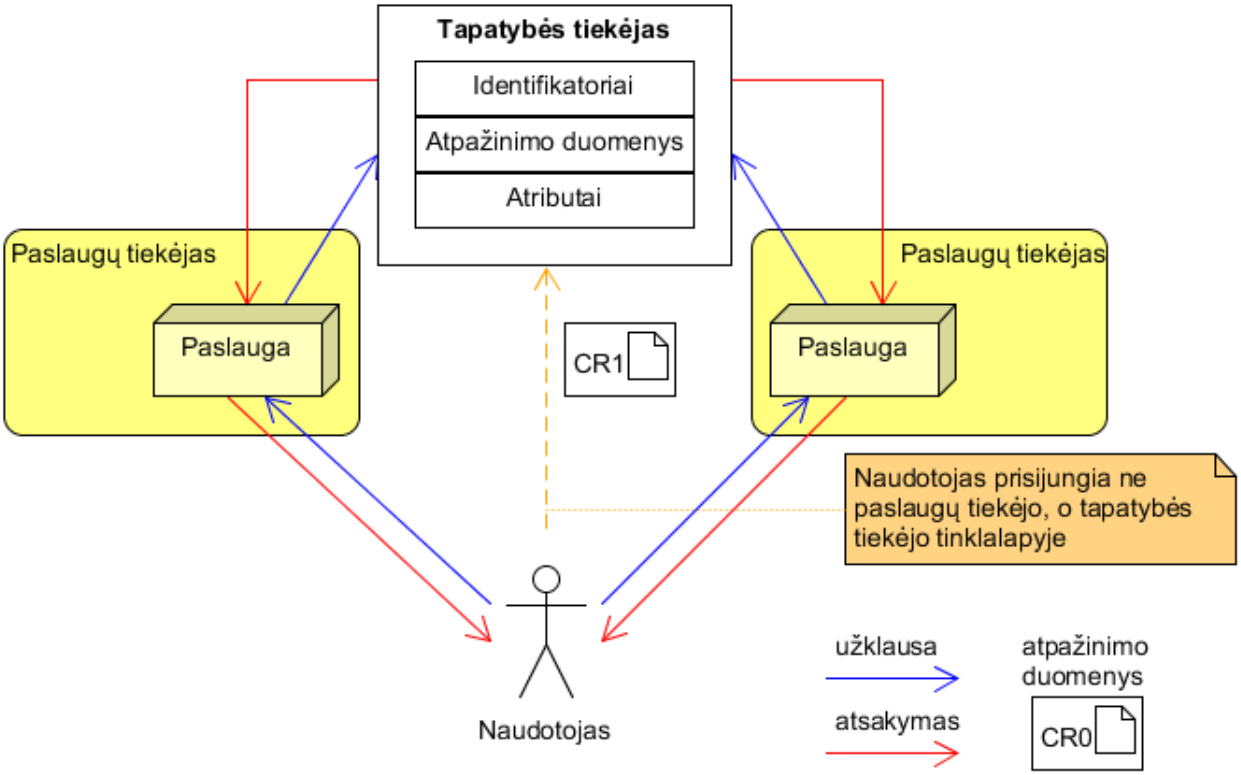
Centralizuotas tapatybės valdymo modelis sudaro palankias sąlygas gerai naudotojo patirčiai užtikrinti. Centralizuotas modelis, priklausomai nuo realizacijos, gali palaikyti vienkartinį prisijungimą, o tai leidžia naudotojui prisijungti vieną kartą ir tapti autentifikuotu visose paslaugų tiekėjo sistemose. Taip pat, kadangi tiek tapatybės valdymo, tiek paslaugų puslapiai yra valdomi paties paslaugų tiekėjo, gali būti užtikrintas vientisas tinklalapių stilius. Taigi, centralizuotą tapatybės valdymą įgyvendinę paslaugų tiekėjai gali sukurti patogias, naudotojams draugiškas (angl. *user-friendly*) sistemas.

1.4.3. Jungtinis tapatybių valdymas

1.4.3.1. Modelis

Ilgą laiką centralizuoto tapatybių valdymo pakako įmonėms turėti patogų, pačios įmonės prižiūrimą tapatybės valdymo sprendimą. Tačiau augant naudojamų taikomųjų programų bei integracijų su trečiųjų šalių aplikacijomis kiekiui, reikėjo sprendimo, leidžiančio identiteto valdymo uždavinius spręsti ne tik vienos organizacijos ribose. Todėl buvo pradėtas naudoti jungtinis (angl. *federated*) tapatybių valdymas.

Jungtinis (angl. *federated*) tapatybių valdymas yra aibė technologijų ir procesų, kurie leidžia sistemoms dalintis tapatybės informacija ir deleguoti tapatybės valdymo užduotis tarp skirtingų paslaugų tiekėjų [MR08]. Šis tapatybių valdymo modelis įgalina naudotojus turėti vienus atpažinimo duomenis, kuriuos gali naudoti skirtingų paslaugų tiekėjų tinklalapiuose. Žemiau pateikiama schema, vaizduojanti šio modelio architektūrą:



4 pav. Jungtinis skaitmeninės tapatybės valdymas [CY10]

Jungtiniame tapatybės valdyme tapatybės tiekėjas yra atskira sistema, su kuria turi integruotis paslaugų tiekėjas. Tapatybės duomenys bei su tapatybe susiję veiksmai (autentifikavimas, autorizavimas) yra deleguojami šiai sistemai. Naudotojas turi vieną identifikatorių, su kuriuo prisijungia tiesiogiai tapatybės tiekėjo puslapyje. Prisijungus šioje sistemoje, naudotojas tampa autentifikuotas visose paslaugose, kurios palaiko šį tapatybės tiekėją [MR08].

1.4.3.2. Realizacijos bei įgalinančios technologijos

Kadangi jungtiniame tapatybės valdyme tapatybės tiekėjas bei paslaugų tiekėjas yra skirtingų kūrėjų sistemos, duomenų apsikeitimui tarp jų sukurti technologiniai standartai. Trys šiuo metu labiausiai paplitę protokolai: *SAML*, *OAuth* bei *OpenID* [Kou17]. Šių technologijų apžvalga pateikiama 1-oje lentelėje.

1 lentelė. Jungtinio tapatybės valdymo technologijos

	SAML	**OAuth**	**OpenID**
Dabartinė versija	SAML 2.0	OAuth 2.0	OpenID Connect
Paskirtis	Autentifikavimas, autorizavimas, atributų perdavimas	Autorizavimas	Autentifikavimas
Duomenų perdavimas	HTTP, SOAP	HTTP, REST	HTTP, REST
Duomenų formatas	XML	JSON, JWT	JSON, JWT
Duomenų šifravimas	Yra	Yra	Yra
Tapatybės tiekėjo suteiktų duomenų validavimas	Viešo-privataus rakto infrastruktūra	Neapibrėžta (palikta realizacijai)	Viešo-privataus rakto infrastruktūra
Naudotojo sutikimas perduoti duomenis	Nėra	Yra	Yra
Mobiliųjų programėlių palaikymas	Nėra	Yra	Yra
Naudojančios organizacijos	Salesforce, PingFederate, Oracle Access Manager	Google, Amazon, GitHub	Google, Microsoft, Ping Identity

Kiekviena iš minimų technologijų šiandien yra gana plačiai naudojama internete - jų svarbą parodo ir didžiųjų kompanijų („Google“, „GitHub“, „Microsoft“) sprendimai pritaikyti jas savo programinėje įrangoje. Pagrindinis šių standartų skirtumas - jų panaudojimo apimtis. SAML pritaikytas visiems tapatybės valdymo veiksmams, OAuth skirtas naudotojui autorizuoti trečiąją šalį pasiekti jo atributus tapatybės tiekėjo platformoje, o OpenID skirtas naudotojų autentifikavimui.

1.4.3.3. Naudotojų poreikių įgyvendinimas

Šis tapatybių valdymo modelis yra gana patogus naudotojams. Jis išsaugo centralizuoto modelio privalumus bei išplečia jo funkcionalumą už vienos organizacijos ribų [Kou17]. Naudotojams užtenka turėti vienus atpažinimo duomenis, su kuriais gali prisijungti prie skirtingų paslaugų tiekėjų tinklalapių. Taip pat jungtinis tapatybės valdymas turi vienkartinį prisijungimą, kurį tinklalapyje matyti nori 77% interneto naudotojų [Res12]. Vienkartinio prisijungimo pagalba naudotojui užtenka vieną kartą prisijungti savo tapatybės tiekėjo puslapyje ir kreipiantis į visas šį tiekėją palaikančias paslaugas, jam iš naujo prisijungti nebereiks.

Asmens duomenų saugumas priklauso nuo bendravimo tarp paslaugų bei tapatybės tiekėjų, o šiame modelyje jis sudėtingesnis nei izoliuotame ar centralizuotame tapatybių valdyme, nes jungtinis valdymas paremtas tarpdomeniniu bendravimu [MR08]. Saugumas sustiprinimas persiunčia-

mus duomenis pasirašant taikant viešus ir privačius raktus bei užšifruojant. Tačiau, kol dauguma tinklalapių remiasi slapyvardžiu ir slaptažodžiu autentifikuojant naudotoją, šis modelis išlieka labai pažeidžiamas sukčiavimo (angl. *phishing*) atakoms [MR08].
Atliktas ne vienas tyrimas siekiant nustatyti jungtiniame tapatybės valdyme naudojamų protokolų saugumą [MVS16; SB12; SMS+12]. Pripažinta, kad sukurti automatinį protokolo saugumo analizės įrankį yra gana sunku dėl skirtingų galimų protokolų įgyvendinimo tėkmių [MVS16]. Todėl jungtiniame tapatybės valdyme naudojamų technologijų saugumas stipriai priklauso nuo konkrečių paslaugų bei tapatybės tiekėjų realizacijų detalių. Dažniausios atakos: prieigos rakto vagystės (angl. *token theft*), apsimetimas naudotoju, sesijų apkeitimas ir specifiniai XML formato išnaudojimai, tokie kaip parašų įvyniojimas (angl. *signature wrapping*) [MVS16; SB12; SMS+12]. Šios atakos dažniausiai įgyvendinamos taikant įprastus interneto programišių metodus: XSS (angl. *cross site scripting*, SQL įterpimą, puslapių apgavystes (angl. *phishing*) [MVS16].

Naudotojo duomenų kontrolė jungtiniame modelyje turi tiek privalumų, tiek trūkumų. Viena vertus, naudotojas savo asmens duomenis suteikia mažesniam kiekiui sistemų (tik tapatybės tiekėjams, vietoj visų paslaugų tiekėjų). Tačiau taip paslaugų tiekėjas tampa vieninteliu nesekmės tašku (angl. *single point of failure*) - programišiams įsilaužus į tapatybės tiekėjo sistemą, asmens paskyros visose paslaugose tampa prieinamos [PM03]. Taip pat, naudotojui gali būti sunku kontroliuoti savo duomenų sklaidą tarp tapatybės tiekėjo ir skirtingų paslaugų, ką rodo ir *Cambridge Analytica* incidentas [Gra18]. Nors OpenID Connect bei OAuth 2.0 standartai suteikia galimybes naudotojui išreikštinai patvirtinti, kokius duomenis jis sutinka perduoti trečiosios šalies paslaugai, kai jis pradeda ja naudotis (pavyzdys pateikiamas priede nr. 1), tačiau tapatybės tiekėjai ne visada tinkamai informuoja, kokie naudotojo veiksmai gali neišreikštai suteikti leidimą tapatybės tiekėjui perduoti duomenis kitai sistemai.

1.5. Skaitmeninės tapatybės valdymo modelių palyginimas

Apžvelgus skirtingas skaitmeninės tapatybės valdymo architektūras, 2 lentelėje pateikiamas modelių palyginimas. Skirtingi modeliai lyginti pagal 1.3 skyrelyje apibrėžtus naudotojų poreikius.

Atsižvelgus į palyginimo rezultatus, galima teigti, kad jungtinis tapatybės valdymas naudotojams yra parankesnis nei centralizuotas ar lokalizuotas valdymas. Šie modeliai verčia naudotojus kurti ir administruoti naujas paskyras nebandytose sistemose, prisiminti daugybę slapyvardžių bei slaptažodžių (ar silpninti saugumą naudojant tą patį slaptažodį) bei kartoti prisijungimo žingsnius, o tai įkyri naudotojams. Pasak kompanijos „Blue Research“ tyrimo, tinklalapiui prašant kurti naują paskyrą 54% interneto naudotojų teigia paliksiantys ar negrįšiantys į tokį puslapį, o 26% ieškos kito panašią paslaugą teikiančio tinklalapio, nereikalaujančio naujos paskyros.

Jungtinis tapatybės valdymas išsprendžia paskyrų kiekio bei prisijungimų skaičiaus, tačiau vis dar turi nemažų trūkumų. Pagrindiniai iš jų:

- vienintelio nesekmės taško situacija. Jungtiniame tapatybės valdyme tapatybės tiekėjas yra vienintelis nesekmės taškas (angl. *single point of failure*). Tapatybės tiekėjui tapus nepasiekiamam, asmuo internete nebegali naudoti visų paslaugų, prie kurių prisijungdavo per šį tapatybės tiekėją;

2 lentelė. Skirtingų tapatybės valdymo modelių palyginimas pagal naudotojo poreikius

		Izoliuotas	**Centralizuotas**	**Jungtinis**
Atpažinimo duomenys		Kiekvienai paslaugai	Kiekvienam paslaugų tiekėjui	Kiekvienam tapatybės tiekėjui
Patogumas	Prisijungimų kiekis	Tiek, kiek paslaugų	Tiek, kiek paslaugų tiekėjų	Tiek, kiek tapatybės tiekėjų
	Naudotojo patirties vientisumas	Yra	Yra	Nėra
Saugumas	Nukreipimai (angl. redirects)	Nėra	Galimi	Yra
	Vienas nesėkmės taškas	Nėra	Paslaugų tiekėjo tapatybės valdymo modulis	Tapatybės tiekėjas
	Technologiniai standartai	Paslaugos kūrėjo nuožiūra	Paslaugų tiekėjo nuožiūra	SAML 2.0, Oauth 2.0, OpenID Connect
Kontrolė	Naudotojo patvirtinimas duomenis perduodant kitai paslaugai	-	Nėra	Galimas (Oauth 2.0, OpenID Connect)
	Duomenų suteikimas tik jų prireikus	Tai realizavus paslaugos kūrėjui	Tai realizavus paslaugų tiekėjui	Dalinis (dar nenaudotai paslaugai prašant naudotojo patvirtinimo)
	Tapatybės duomenų keitimas	Kiekvienos paslaugos tinklalapyje	Kiekvieno paslaugų tiekėjo tinklalapyje	Kiekvieno tapatybės tiekėjo tinklalapyje

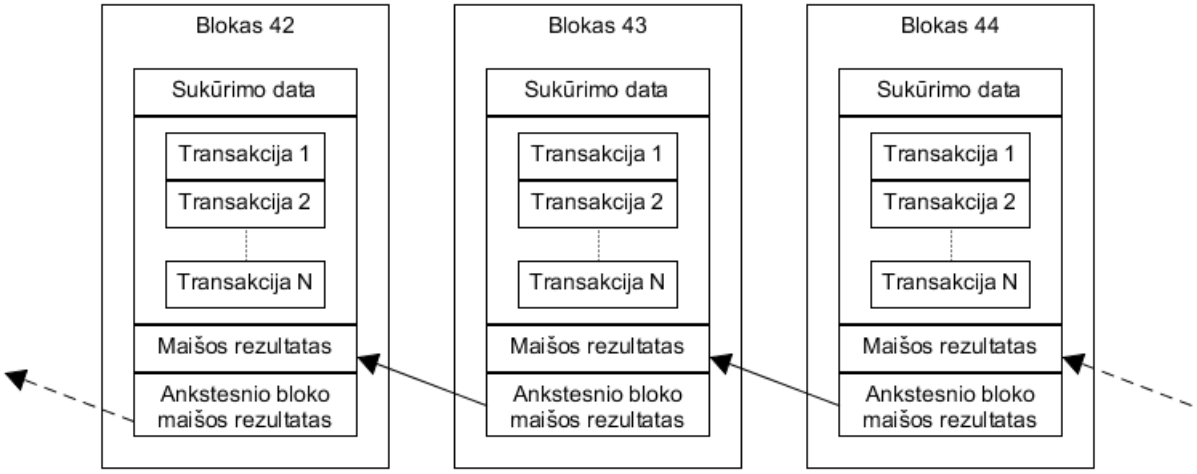
- naudotojų kontrolės trūkumas. Asmenys dažnai privesti suvesti daugybę tapatybės duomenų registruodamiesi, kurių nebūtinai reikia registracijos metu [SPM+11]. Po registracijos naudotojui belieka pasikliauti paslaugų bei tapatybės tiekėjais, kad jo duomenys nebus perduodami nepageidaujamoms trečiosioms šalims. Nors naudojamos technologijos, tokios kaip OAuth, išreikštinai prašo naudotojų sutikimo perduodant duomenis naujai paslaugai (žr. priedą nr. 1), tai atliekama tik pradedant naudotis tam tikra paslauga. Taip pat, *CambridgeAnalytica* incidentas [Gra18] rodo, kad šio sutikimo gali neužtekti. Visa tai veda prie to, kad naudotojai jaučiasi nekontroliuojantys savo asmens duomenų internete, norėtų lengviau keisti bei trinti juos, o dalį tapatybės valdymo sistemų naudoja tik todėl, kad neturi kitos išeities [Baa16];
- saugumo iššūkiai. Dėl naudojamų nukreipimų jungtinis tapatybės valdymas yra itin jautrus sukčiavimo (angl. *phishing*) atakoms, tačiau paslaugų tiekėjai dažniausiai vis dar remiasi naudotojų gebėjimu atpažinti netikrus programišių tinklalapius, nors to nerekomenduoja tyrimai [SPM+11]. Taip pat, jungtiniame tapatybės valdyme atsiranda vienas didelės vertės taikinys (angl. *single high value target*) - tapatybės tiekėjas. Įsilaužus į jo sistemą, naudotojų atpažinimo duomenys gali būti panaudoti daugybėje skirtingų paslaugų tiekėjų sistemų;
- pasitikėjimo trūkumas. Naudotojams jungtiniame tapatybės valdyme tenka pasikliauti tiek tapatybės tiekėjų, tiek paslaugų tiekėjų gebėjimu patikimai saugoti ir perduoti tapatybės duomenis. Norint naudotojų pasitikėjimo, sistemos turėtų būti skaidrios (angl. *transparent*) apie tai, kaip jos saugo, valdo tapatybės duomenis [Baa16]. Tačiau, kai technologijų specifikacijos palieka vietos nesaugiam protokolų įgyvendinimui [SB12], o paslaugų tiekėjai retai atskleidžia sistemos veikimo detales [Baa16], naudotojų pasitikėjimas senka.

Pateikti jungtinio tapatybės valdymo trūkumai rodo, kad tapatybės valdymo sritis vis dar yra tobulintina naudotojų atžvilgiu. Naudotojams trūksta didesnės tapatybės duomenų kontrolės, o dėl galimų saugumo iššūkių, vieno nesekmės taško situacijos ir neatskleidžiamų sistemų įgyvendinimo detalių, pasitikėti paslaugų bei tapatybės tiekėjais yra sunku. Toliau darbe apžvelgiama blokų

grandinės technologija, atkreipiant dėmesį į jos potencialą spręsti įvardytas problemas skaitmeniniame tapatybių valdyme: vieno nesėkmės taško situaciją bei kontrolės, skaidrumo ir pasitikėjimo trūkumą.

2. Blokų grandinės technologija

Blokų grandinė - tai vieno su kitu susijusių blokų grandinė, kurios blokuose saugomi nekeičiami įrašai [Nak08]. Šią technologiją galima apibūdinti kaip daugybę paskirstytų nekintamų skaitmeninių įrašų (angl. *immutable distributed ledger*), tarpusavyje susietų taikant kriptografiją (blokų grandinės pavyzdys pateikiamas 5 paveiksle). Technologija geriausiai žinoma dėl jos panaudojimo Bitcoin kriptovaliutoje. Šiame skyriuje apžvelgiami pagrindiniai blokų grandinės techniniai aspektai, savybės bei galimi skirtingi variantai.



5 pav. Supaprastintas blokų grandinės modelis

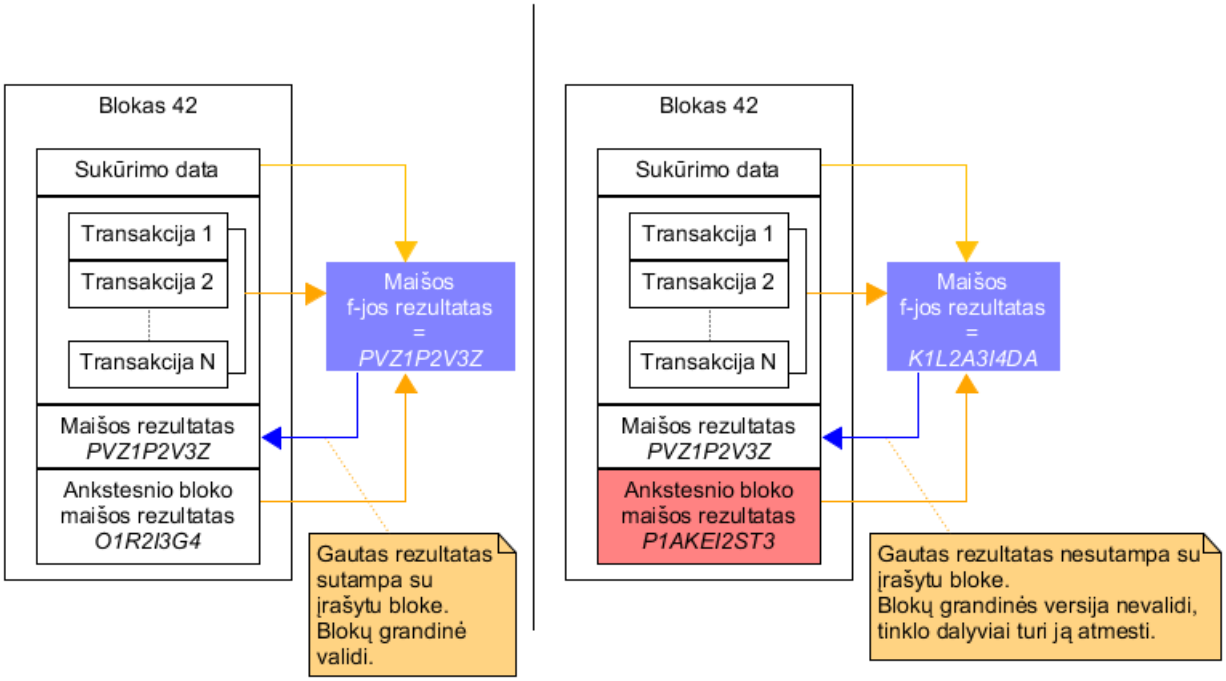
2.1. Nekintamumas

Blokų grandinėje kiekvienas blokas yra sudarytas iš šių dalių:

- transakcijų. Kiekviena transakcija yra duomenys, kuriuos norima saugoti blokų grandinėje. Šie duomenys gali būti bet kokia vertinga informacija: finansinės transakcijos, programinis kodas, asmens duoti sutikimai (angl. *consents*) ar kt. Kiekviena transakcija yra pasirašoma kūrėjo privačiu raktu. Vienas blokas gali turėti vieną arba daugiau transakcijų;
- bloko kriptografinės maišos funkcijos rezultato (angl. *hash*);
- ankstesnio (tėvinio) bloko kriptografinės maišos funkcijos rezultato;
- bloko sukūrimo laiko. Blokai grandinėje saugomi chronologiškai;
- kitų metaduomenų (pvz. bloko eilės numerio, blokų grandinės versijos, *nonce* darbo įrodymui).

Kiekvieno bloko maišos funkcijos rezultatas priklauso nuo jo transakcijų, prieš tai buvusio bloko maišos rezultato ir bloko metaduomenų. Jeigu betkurio bloko duomenys būtų pakeisti, tuomet maišos funkcija sugeneruotų kitokį maišos rezultatą ir būtų lengva patikrinti, kad naujai perskaičiuotas maišos rezultatas nesutampa su bloke esančiu rezultatu. Taip pat, kadangi kiekvienas blokas priklauso nuo prieš tai buvusio bloko, net ir pakeitus vieną iš pirmųjų blokų, pakeitimas

būtų pastebimas pridedant naujus blokus ir būtų galima suprasti, kad turima blokų grandinės versija yra nevalidi (žr. 6 pav.). Tokiu būdu kiekvienas blokų grandinės blokas patvirtina prieš tai buvusio bloko integralumą, taip pasiekiant blokų grandinės nekintamumą (angl. *immutability*), nes perrašyti įrašus blokuose nepastebėtam labai sunku [Nak08].



6 pav. Bloko grandinėje validavimas

2.2. Decentralizuotumas

Blokų grandinės sistema yra decentralizuota - nėra vieno centrinio serverio, kuris vienas turėtų visą blokų grandinę. Sistemą sudaro daugybė blokų grandinės mazgų (angl. *node*), kurie turi visą blokų grandinės kopiją. Šie mazgai yra atsakingi už naujų transakcijų validavimą, blokų su transakcijomis kūrimą, sukurtų blokų priėmimą į blokų grandinę ir pranešimus kitiems mazgams apie naują į grandinę priimtą bloką [Ant14]. Kiekvienas mazgas yra susietas su keletu kitu mazgų. Mazgas, kuris nori pridėti naują bloką (vadinamas *kasėju*), praneša apie jį kitiems mazgams, jie savo ruožtu žinią perduoda kitiems mazgams ir taip ilgainiui kiekvienas mazgas tinkle turi naujausią blokų grandinės versiją.

Kadangi nėra centrinės institucijos, kuri nuspręstų, ar siūlomas blokas yra tinkamas priimti į grandinę, sprendimą bendrai turi priimti visi tinklo dalyviai. Egzistuoja skirtingos taisyklės, vadinamos konsensuso strategijomis (plačiau apie juos 2.4 skyrelyje), kuriomis remdamiesi tinklo mazgai nusprendžia, ar pasiūlytas blokas yra validus. Šios taisyklės apibrėžia, kaip tinklo dalyviai turi įrodyti bloko validumą jį siūlydami į grandinę bei kaip patikrinti kito dalyvio pasiūlyto bloko validumą.

2.3. Skirtingi tipai

Priklausomai nuo tinklo dalyviams suteikiamų blokų grandinės skaitymo ir rašymo teisių, išskiriami trys pagrindiniai blokų grandinės tipai: vieša, konsorciumo bei privati. Tipų skirtumai pateikiami 3 lentelėje.

3 lentelė. Viešos, konsorciumo ir privačios blokų grandinės palyginimas [ZXD+17]

	Vieša	**Konsorciumo**	**Privati**
Konsensuso nustatymas	Visi kasėjai	Išrinkti tinklo dalyviai	Viena organizacija
Skaitymo teisės	Viešos	Gali būti viešos ar apribotos	Gali būti viešos ar apribotos
Centralizuotumas	Nėra	Dalinis	Yra
Efektyvumas	Mažas	Didelis	Didelis

Kadangi vieša blokų grandinė yra atvira visam pasauliui, visiems matomos ir joje išsaugotos transakcijos. Tai sudaro puikias salygas įrašų auditui, tačiau sumažina naudotojų privatumą. Siekiant išlaikyti tam tikrą privatumo lygį, viešoje grandinėje matomi tik transakcijas atlikusių asmenų vieši raktai [Nak08].

Privačios bei konsorciumo blokų grandinės yra tik dalinai decentralizuotos - jose blokų validavimą ir priėmimą į grandinę atlieka vienas ar dalis tinklo dalyvių. Šios grandinės privalumai: visi validuotojai yra žinomi, grandinės efektyvesnės dėl greičiau priimamų blokų, apribotos blokų skaitymo teisės suteikia didesnį privatumo lygį, o iškilus poreikiui, tinklo dalyviai gali pakeisti ar atšaukti įvykusias transakcijas [But15]. Konsorciumo ir privačios blokų grandinės labiau tinkamos įmonių vidiniam (ar jungtiniam, pvz. tarp kelių finansinių institucijų) naudojimui. Blokų grandinių karkasų sprendimus įmonėms siūlo IBM, Microsoft, Hyperledger [ZXD+17].

2.4. Konsensuso strategijos

Kadangi blokų grandinės sistema yra decentralizuota, nėra centrinės institucijos, kuri nuspręstų, ar naujai siūlomas pridėti į grandinę blokas yra validus (be transakcijų su falsifikuotais duomenimis). Todėl blokų grandinės tinkle taikoma konsensuso strategija, pagal kurią nusprendžiama, ar pridėti naują bloką į grandinę. Apžvelgiamos trys dažnai naudojamos strategijos: darbo, įtakos bei autoriteto įrodymo.

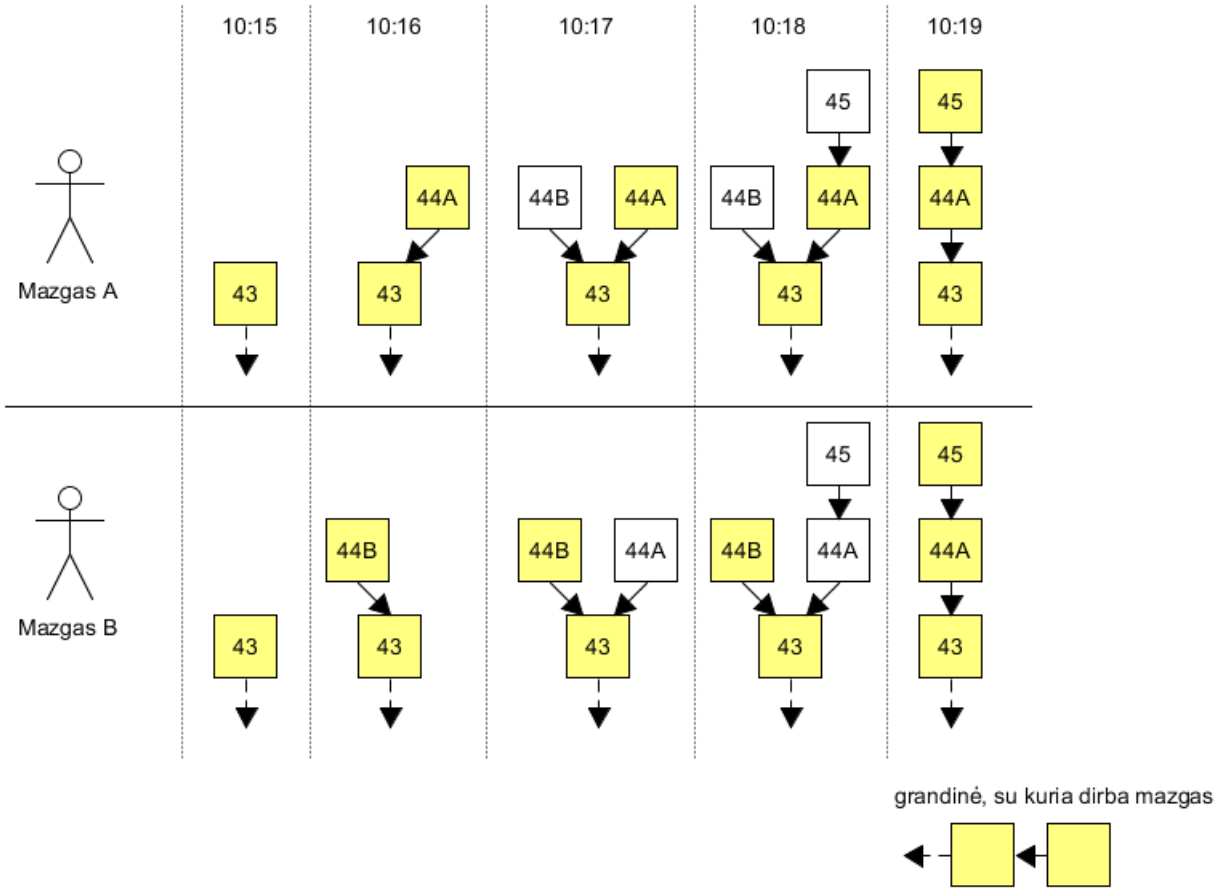
2.4.1. Darbo įrodymo (angl. *proof of work*)

Darbo įrodymo konsensuso strategija remiasi principu, kad daug pastangų ir resursų į bloko validumo įrodymą įdėjęs tinklo dalyvis nebus linkęs sukčiauti. Šioje strategijoje tinklo dalyvis, norėdamas pridėti bloką į blokų grandinę, turi išspręsti laikui ir resursams imlų matematinį uždavinį (užsiima *bloko kasimu*). Pirmas uždavinio reikšmę radęs tinklo dalyvis praneša apie ją kitiems,

kurie turi patvirtinti, ar ši reikšmė teisinga. Jei tai patvirtinta, tinklo dalyviai patikrina, ar naujojo bloko transakcijos yra validžios. Jeigu jos validžios, blokas pridedamas į grandinę [ZXD+17].

Darbo įrodymo matematinis uždavinys dažniausiai būna paremtas kriptografine maišos funkcija, kurios rezultatą lengvą validuoti, tačiau duomenis, sugeneravusius šį rezultatą, sunku surasti. Uždavinio tikslas - surasti šiuos duomenis. Tinklo dalyviai eikvoja didžiulius kiekius elektros energijos ir laiko, nes radimas būna paremtas duomenų perrinkimu (angl. *brute force*). Dėl šios priežasties rezultato ieškantiems *kasėjams* neretai būna įvesta paskatinimo sistema, kuri teisingą reikšmę radusį *kasėją* apdovanoja piniginiu atlygiu [Nak08].

Kadangi blokų grandinės tinklas yra decentralizuotas, įmanoma situacija, kad labai panašiu metu į grandinę skirtingų mazgų pridėti du validūs blokai. Taip dalis tinklo dalyvių gaus vieną mazgą, o dalis - kitą, o abu jie bus susieti su tuo pačiu prieš tai buvusiu bloku. Tokiu atveju, taikoma ilgiausios grandinės taisyklė (žr. 7 pav.). Mazgai dirba prie pirmiau gauto bloko, tačiau išsaugo kitą gautą bloką kaip šaką. Po to, kai bus gautas dar vienas blokas, jis bus susietas tik su viena iš šakų - taip ši šaka taps ilgesnė. Tuomet ilgesnė šaka paskelbiama aktyviąja grandine, visi su trumpesniąja šaka dirbę mazgai turi pereiti prie aktyviosios grandinės, o atmesto bloko (vadinamo *bloku-našlaičiu*) transakcijos grąžinamos į bendrą transakcijų sankaupą (angl. *transaction pool*) [Nak08]. Realiuose blokų grandinės taikymuose, dažnai laukiama keleto iš eilės einančių naujų blokų, kad būtų galima atmesti *bloką-našlaitį*. Pavyzdžiui, Bitcoin blokų grandinėje laukiama apytiksliai 6 blokų, kad *bloką-našlaitį* būtų galima atmesti [ZXD+17].



7 pav. Ilgiausios grandinės taisyklės taikymas

Pagrindinis šios konsensuso strategijos privalumas yra tas, kad dideli kasimo kaštai gali atgrasyti programišius nuo potencialių atakų. Tačiau, taip veltui išeikvojama daugybė elektros energijos - skaičiuojama, kad kasimas Bitcoin ir Ethereum blokų grandinėms kartu sudėjus per dieną sueikvoja elektros energijos, kurios vertė yra apie 1 milijoną dolerių [Eth14]. Taip pat, dėl ilgo uždavinio sprendimo laiko vieno bloko priėmimas į grandinę gali užtrukti - Bitcoin blokų grandinėje tai užima apie 10 minučių [ZXD+17].

2.4.2. Turto įrodymo (angl. *proof of stake*)

Turto įrodymo konsensuso strategija remiasi principu, kad daug blokų grandinės turto turintis kasėjas bus sąžiningas, nes išaiškinus jo nesąžiningumą jis rizikuoja prarasti savo turimą turtą [Baa16]. Šis algoritmas patiki sprendimą priimti tiems tinklo dalyviams, kurie įrodo kad turi daugiausia turto (pvz. blokų grandinės kriptovaliutos). Tai gali pasirodyti kaip nesąžiningas sprendimas, nes turtingiausias tinklo dalyvis gali būti vienvaldžiu sprendimų priėmėju. Dėl to blokų grandinės tinklai neretai taiko šios strategijos variantus: Peercoin papildomai vertina turto amžių, Blackcoin kitą patvirtintoją paskiria pagal atsitiktinę funkciją, kuri atsižvelgia ir į turimą turtą [ZXD+17].

Ši strategija leidžia nebeeikvoti didžiulių elektros kiekių, skirtingai nei darbo įrodymo strategija [Eth14]. Algoritmo efektyvumas taip pat sutaupo laiko ir blokai būna greičiau patvirtinami

ir pridedami į grandinę. Tačiau, dėl praktiškai nulinių bloko *kasimo* sąnaudų, galimos dažnesnės tinklo atakos [ZXD+17].

2.4.3. Autoriteto įrodymo (angl. *proof of authority*)

Autoriteto įrodymo strategija remiasi keletu tinklo dalyvių, kuriems suteikta teisė validuoti naujus blokus. Ši strategija nebėra tinkama visiškai decentralizuotai blokų grandinei, kurioje būtinas pilnas pasitikėjimo padalinimas [Hos17]. Tačiau ši strategija tinkama privačioms ar konsorciumo blokų grandinėms.

Šis konsensuso mechanizmas remiasi iš anksto išrinktais tinklo dalyviais, kurie bus atsakingi už blokų validavimą. Kiekvieną kartą pridedant naują bloką į grandinę, vienas iš išrinktų validuotojų patvirtins arba atmes pasiūlytą bloką. Siekiant sumažinti galimą kenksmingų patvirtintojų žalą, įvedamos taisyklės, neleidžiančios tam pačiam validuotojui patvirtinti keleto blokų iš eilės [Hos17].

Autoriteto įrodymo strategijoje validuotojams svarbu išlaikyti gerą reputaciją - susigadinus ją, validuotojas gali būti pašalintas iš tinklo. Šis konsensuso mechanizmas leidžia greitai ir su itin mažais ištekliais pridėti blokus, tačiau nėra tinkamas pilnai decentralizuotoms blokų grandinėms. Šią strategiją taiko Parity blokų grandinė [Hos17].

2.5. Pavojai ir trūkumai

Blokų grandinės technologija sukuria sąlygas decentralizuotai, nesuteikiant pasitikėjimo vienam ar keliems dalyviams, laikyti nekeičiamus duomenis. Tai atveria įvairių galimybių finansų, daiktų interneto, reputacijos sistemų, saugumo bei privatumo srityse [ZXD+17], tačiau ši technologija turi ir trūkumų. Pagrindiniai iš jų aptariami šiame skyriuje.

2.5.1. Daugumos ataka

Viešose blokų grandinėse dauguma (>50%) mazgų tinkle turi patvirtinti bloką, kad jis būtų priimtas į grandinę. Potencialus įsilaužėlis gali pateikti falsifikuotą blokų grandinės bloką (pvz. su netikromis transakcijomis), tačiau kol jis neturi daugumos skaičiavimo galios tinkle, šis blokas bus atmestas likusių dalyvių mazge (ir taps *bloku-našlaičiu* taikant ilgiausios grandinės taisyklę). Tačiau jeigu įsilaužėlis (ar keletas jų) turi daugumą skaičiavimo galios, jis gali dirbti su falsifikuota blokų grandinės versija greičiau negu likę dalyviai tinkle ir taip ilgiausia grandine, prie kurios pereis visi dalyviai, taps jo sukurta grandinė su falsifikuotais blokai [ZXD+17]. Ši ataka neištiko dviejų didžiausių blokų grandinių Bitcoin bei Ethereum, tačiau buvo įvykdyta prieš Verge blokų grandinę [Sed18].

2.5.2. Plečiamumas

Blokų grandinės plečiamumas matuojamas pagal du kriterijus: transakcijų pralaidumą ir saugojimo reikalavimus mazgams. Transakcijų pralaidumas, kuris priklauso nuo to, kaip greitai nauji

blokai su transakcijomi yra pridedami į blokų grandinę, susijęs su taikoma konsensuso strategija. Kuo taikoma strategija leidžia greičiau priimti naują bloką, tuo greičiau transakcijos bus patvirtintos. Bitcoin blokų grandinėje, taikančioje darbo įrodymo konsensusą, apdorojoma apie 7 transakcijas per sekundę [ZXD+17], kai Tendermint blokų grandinė, taikanti atsparumo klaidoms konsensusą, teigia galinti apdoroti tūkstančius transakcijų per sekundę [Ten17]. Dėl darbo įrodymo strategijos neefektyvumo blokų grandinės dažnai keičia ją į kitą konsensuso strategiją - Ethereum blokų grandinė ketina pereiti prie turto įrodymu grįsto konsensuso [Eth14].

Kita priežastis, dėl ko transakcijos tvirtinamos gana lėtai - blokai turi dydžio apribojimus. Dėl šių apribojimų, tik dalis susikaupusių transakcijų gali būti priimtos į naują bloką, o likusios turi laukti, kol pateks į kitą bloką. Tam spręsti pasitelktos šalutinės blokų grandinės. Jos dalį bloko duomenų iškelia į šalutinę grandinę, taip palikdamos daugiau vietos pagrindinės grandinės bloke. Tokį sprendimą priėmė Bitcoin blokų grandinė, į tinklą pristatydama SegWit protokolą, kuris iškelia skaitmeninių parašų duomenis į atskirą grandinę [Bit16].

Visos blokų grandinės dydis taip pat gali sukelti plečiamumo problemų. Šiuo metu Bitcoin blokų grandinė užima per 100 gigabaitų [ZXD+17]. Siekiant sumažinti šį kiekvienam mazgui reikiamą saugoti duomenų kiekį, siūlomi įvairūs sprendimai: mazgams neturėti seniausių blokų grandinės dalių (taip seni blokai su transakcijomis būtų iškeliami į atskirą duombazę) arba dalį blokuose esančios informacijos saugoti šalutinėje blokų grandinėje.

Rezultatai ir išvados

Literatūra

[Ant14] Andreas M. Antonopoulos. Mastering bitcoin : unlocking digital cryptocurrencies. 2014, p. 272. ISBN: 1449374042.

[Baa16] Djuri Baars. Towards Self-Sovereign Identity using Blockchain Technology. Disertacija, University of Twente, 2016. URL: http://essay.utwente.nl/71274/1/Baars%7B%5C_%7DMA%7B%5C_%7DBMS.pdf.

[Bit16] Bitcoin Wiki. Segregated Witness, 2016. URL: https://en.bitcoin.it/wiki/Segregated%7B%5C_%7DWitness (tikrinta 2018-05-02).

[But15] Vitalik Buterin. On Public and Private Blockchains - Ethereum Blog, 2015. URL: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (tikrinta 2018-05-02).

[Cam04] L.J. Camp. Digital identity. IEEE Technology and Society Magazine, 23(3):34–41, 2004. DOI: 10.1109/MTAS.2004.1337889. URL: http://ieeexplore.ieee.org/document/1337889/.

[CY10] Yuan Cao Yuan Cao ir Lin Yang Lin Yang. A survey of Identity Management technology. 2010 IEEE International Conference on Information Theory and Information Security:287–293, 2010. DOI: 10.1109/ICITIS.2010.5689468. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5689468.

[CK01] S Clauß ir M Køhntopp. Identity Management and its Support of Multilateral Security. Computer Networks, 37 (2):205–219, 2001.

[DD08] Rachna Dhamija ir Lisa Dusseault. The Seven Flaws of Identity Management: Usability and Security Challenges. IEEE Security & Privacy Magazine, 6(2):24–29, 2008-03. ISSN: 1540-7993. DOI: 10.1109/MSP.2008.49. URL: http://ieeexplore.ieee.org/document/4489846/.

[DP08] M. Dabrowski ir P. Pacyna. Generic and Complete Three-Level Identity Management Model. 2008 Second International Conference on Emerging Security Information, Systems and Technologies, p. 232–237. IEEE, 2008-08. DOI: 10.1109/SECURWARE.2008.18. URL: http://ieeexplore.ieee.org/document/4622588/.

[Eth14] Ethereum Foundation. Ethereum Wiki, 2014. URL: https://github.com/ethereum/wiki/wiki.

[FH07] Dinei Florencio ir Cormac Herley. A large-scale study of web password habits. Proceedings of the 16th international conference on World Wide Web - WWW '07, p. 657, New York, New York, USA. ACM Press, 2007. ISBN: 9781595936547. DOI: 10.1145/1242572.1242661. URL: http://portal.acm.org/citation.cfm?doid=1242572.1242661.

[GC07] Benjamin M. Gross ir Elizabeth F. Churchill. Addressing Constraints: Multiple Usernames, Task Spillage and Notions of Identity. CHI '07 extended abstracts on Human factors in computing systems - CHI '07, p. 2393, New York, New York, USA. ACM Press, 2007. ISBN: 9781595936424. DOI: 10.1145/1240866.1241013. URL: http://portal.acm.org/citation.cfm?doid=1240866.1241013.

[Gra18] Kevin Granville. Facebook and Cambridge Analytica, 2018. URL: https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html (tikrinta 2018-03-28).

[GV09] Uwe Glässer ir Mona Vajihollahi. Identity Management Architecture. 9:97–116, 2009. URL: https://link.springer.com/content/pdf/10.1007%7B%5C%7D2F978-1-4419-1325-8.pdf.

[Hos17] Adam Hose. Rolling your own Proof-of-Authority Ethereum consortium, 2017. URL: http://blog.enuma.io/update/2017/08/29/proof-of-authority-ethereum-networks.html (tikrinta 2018-05-01).

[JP05] Audun Jøsang ir Simon Pope. User Centric Identity Management. AusCERT Conference, 2005. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.60.1563%7B%5C&%7Drep=rep1%7B%5C&%7Dtype=pdf.

[Kou17] Sherif Koussa. Differentiating Federated Identities: OpenID Connect, SAML v2.0, and OAuth 2.0, 2017. URL: https://www.softwaresecured.com/differentiating-federated-identities-openid-connect-saml-v2-0-and-oauth-2-0/ (tikrinta 2018-04-22).

[Kuk11] Ado Kukic. Definitive guide to Single Sign-On (SSO), 2011. URL: https://resources.auth0.com/definitive-guide-to-single-sign-on/.

[Mic07] Microsoft Developer Network. Access Tokens, 2007. URL: https://msdn.microsoft.com/en-us/library/Aa374909.aspx (tikrinta 2018-04-07).

[Min18] Miniwatts Marketing Group. World Internet Users Statistics, 2018. URL: https://www.internetworldstats.com/stats.htm (tikrinta 2018-03-28).

[MM17] Jason Mander ir Felim McGrath. Global Web Index Social. Tech. atask., 2017. URL: https://cdn2.hubspot.net/hubfs/304927/Downloads/GWI%20Social%20Summary%20Q3%202017.pdf.

[MR08] E Maler ir D Reed. The Venn of Identity: Options and Issues in Federated Identity Management. IEEE Security and Privacy, 6(2):16–23, 2008. ISSN: 15407993. DOI: 10.1109/MSP.2008.50. URL: http://innovbfa.viabloga.com/files/IEEESecPriv%7B%5C_%7D%7B%5C_%7D%7B%5C_%7DVenn%7B%5C_%7Dof%7B%5C_%7DIdentity%7B%5C_%7D%7B%5C_%7D%7B%5C_%7D2008.pdf.

[MS07] Tewfiq El Maliki ir Jean-marc Seigneur. A Survey of User-centric Identity Management Technologies. International Conference on Emerging Security Information Systems and Technologies:12–17, 2007. DOI: 10.1109/SECURWARE.2007.6. URL: http://ieeexplore.ieee.org/xpls/abs%7B%5C_%7Dall.jsp?arnumber=4385303.

[MVS16] Christian Mainka, Rubde Vladislav Mladenov ir Jörg Schwenk. On the security of modern Single Sign-On Protocols – Second-Order Vulnerabilities in OpenID Connect, 2016. URL: https://arxiv.org/pdf/1508.04324.pdf.

[Nak08] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Disertacija, 2008. URL: www.bitcoin.org.

[PM03] Andreas Pashalidis ir Chris J. Mitchell. A taxonomy of single sign-on systems. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2727 LNCS:249–264, 2003. ISSN: 03029743.

[Ral14] Raluca Budiu. Login Walls Stop Users in Their Tracks, 2014. URL: https://www.nngroup.com/articles/login-walls/ (tikrinta 2017-06-10).

[Res12] Blue Research. Research Reveals Consumers Increasingly Interested In Social Login To Alleviate Online Registration Headaches | Janrain, 2012. URL: http://www.janrain.com/about/newsroom/press-releases/research-reveals-consumers-increasingly-interested-social-login/ (tikrinta 2017-05-27).

[Sam99] V Samar. Single sign-on using cookies for Web applications. Proceedings IEEE 8th International Workshops on Enabling Technologies Infrastructure for Collaborative Enterprises WET ICE99:158–163, 1999. ISSN: 10801383.

[SB12] San-Tsai Sun ir Konstantin Beznosov. The Devil is in the (Implementation) Details: An Empirical Analysis of OAuth SSO Systems. Proceedings of the 2012 ACM conference on Computer and communications security, p. 378–390, 2012. URL: http://delivery.acm.org/10.1145/2390000/2382238/p378-sun.pdf?ip=193.219.95.141%7B%5C&%7Did=2382238%7B%5C&%7Dacc=ACTIVE%20SERVICE%7B%5C&%7Dkey=1FA3353941FE8055.0BB7C649D41C6C66.4D4702B0C3E38B35.4D4702B0C3E38B35%7B%5C&%7D%7B%5C_%7D%7B%5C_%7Dacm%7B%5C_%7D%7B%5C_%7D=1524915309%7B%5C_%7D.

[Sed18] Kai Sedgwick. Verge Is Forced to Fork After Suffering a 51% Attack - Bitcoin News, 2018. URL: https://news.bitcoin.com/verge-is-forced-to-fork-after-suffering-a-51-attack/ (tikrinta 2018-05-02).

[SMS+12] Juraj Somorovsky, Andreas Mayer, Jörg Schwenk, Marco Kampmann ir Meiko Jensen. On Breaking SAML: Be Whoever You Want to Be. USENIX Security Symposium, 2012. URL: https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final91-8-23-12.pdf.

[SPM+11] San-Tsai Sun, Eric Pospisil, Ildar Muslukhov, Nuray Dindar, Kirstie Hawkey ir Konstantin Beznosov. What makes users refuse web single sign-on? Proceedings of the Seventh Symposium on Usable Privacy and Security - SOUPS '11:1, 2011. DOI: 10.1145/2078827.2078833. URL: http://dl.acm.org/citation.cfm?doid=2078827.2078833.

[Ten17] Tendermint. Tendermint - Blockchain Consensus, 2017. URL: https://tendermint.com/ (tikrinta 2018-05-02).

[ZXD+17] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen ir Huaimin Wang. Blockchain Challenges and Opportunities : A Survey. International Journal of Web and Grid Services, 2017. URL: https://www.researchgate.net/profile/Hong-Ning%7B%5C_%7DDai/publication/319058582%7B%5C_%7DBlockchain%7B%5C_%7DChallenges%7B%5C_%7Dand%7B%5C_%7DOpportunities%7B%5C_%7DA%7B%5C_%7DSurvey/links/59d86d50a6fdcc2aad0a2f2a/Blockchain-Challenges-and-Opportunities-A-Survey.pdf.

Sąvokų apibrėžimai

Atributas - charakteristika, susieta su esybe, pavyzdžiui fiziniu asmeniu. Galimi asmens atributai: gimimo data, vardas, ūgis, pirštų antspaudai [Cam04]. Atributas gali būti laikinas (pvz. adresas) arba nuolatinis (pvz. asmens kodas).

Identifikatorius - tai atributas, kuris vienareikšmiškai susiejamas su jį pateikiančiu asmeniu ir kurį sunku arba neįmanoma pakeisti. Fizinio asmens identifikatoriaus pavyzdys galėtų būti gimimo data (žmogus gali apie ją meluoti, tačiau gimimo datos pakeisti neįmanoma) [Cam04]. Skaitmeninio identifikatoriaus pavyzdys yra naudotojo elektroninio pašto adresas.

Atpažinimo duomenys (angl. *credentials*) - tai duomenys, skirti asmens autentifikavimui. Jie gali būti ir asmens atributai (pvz. biometriniai duomenys, tokie kaip pirštų antspaudai ar balsas), gali būti ir sugalvoti duomenys (pvz. slapyvardis ir slaptažodis). Dažniausiai internete naudojami atpažinimo duomenys yra identifikatoriaus (slapyvardžio ar el. pašto) ir slaptažodžio pora [MR08].

Identifikavimas - tai procesas, kurio metu asmuo susiejamas su jo identifikatoriumi [Cam04]. Identifikavimo pavyzdys yra asmens ir jo vardo susiejimas: *tu esi Jonas Jonaitis*.

Autentifikavimas - tai procesas, kurio metu patvirtinama sąsaja tarp tapatybės ir jos identifikatoriaus (t.y., įrodoma, kad asmuo iš tikrųjų yra tas, kas sakosi esąs) [Cam04; Kuk11]. Šiam patvirtinimui naudojami atpažinimo duomenys. Autentifikavimo pavyzdys: *tavo pateiktas slapyvardis ir slaptažodis patvirtina, kad tu esi Jonas Jonaitis*.

Autorizavimas - tai procesas, kurio metu leidžiama arba draudžiama asmeniui atlikti konkretų veiksmą, priklausomai nuo jo identifikatoriaus ar atributo [Cam04]. Pavyzdys: *kadangi tau yra daugiau nei 18 metų, tu gali nusipirkti energetinį gėrimą*.

Skaitmeninė tapatybė - abstrakti fizinės esybės reprezentacija, sudaryta iš aibės esybės nuolatinių ar laikinų atributų, kurie susiejami su fizine esybe [Cam04; GV09]. Fizinė esybė gali būti fizinis arba juridinis asmuo. Šiame darbe, jei nenurodyta kitaip, kalbama apie fizinio asmens skaitmeninę tapatybę.

Skaitmeninės tapatybės valdymas (angl. *digital identity management*) - tai veiksmų, skirtų kontroliuoti tapatybę ir su ja susijusius procesus, visuma [DP08]. Į tai įeina autentifikavimas, autorizavimas, prieigų kontrolė, tapatybės gyvavimo ciklo valdymas bei saugus tapatybės atributų perdavimas trečiosioms šalims [CY10].

Paslaugų tiekėjas (angl. *service provider*) - tai betkokia taikomoji programa, kuri suteikia naudotojui tam tikrą paslaugą ar norimą turinį. Galimi paslaugų tiekėjai yra interneto tinklapiai, susirašinėjimo programos ar kitos taikomosios programos, į kurias kreipiasi naudotojas [PM03; Sam99]. Paslaugų tiekėjas gali turėti vieną ar kelias paslaugas, kurioms reikia tapatybės valdymo funkcijų. Darbe paslaugų tiekėjas dar gali būti vadinamas pasikliaujančiąja šalimi (angl. *relying party*).

Tapatybės tiekėjas (angl. *identity provider*) - servisas ar taikomoji programa, skirta koordinuoti su tapatybe susijusius duomenis tarp naudotojų, jų naršyklių bei paslaugų tiekėjų [Kuk11]. Pagrindinės tapatybės tiekėjo funkcijos: infrastruktūros naudotojų tapatybės duomenims apdoroti sukūrimas ir užklausų iš paslaugų tiekėjų bei naudotojų apdorojimas [CY10].

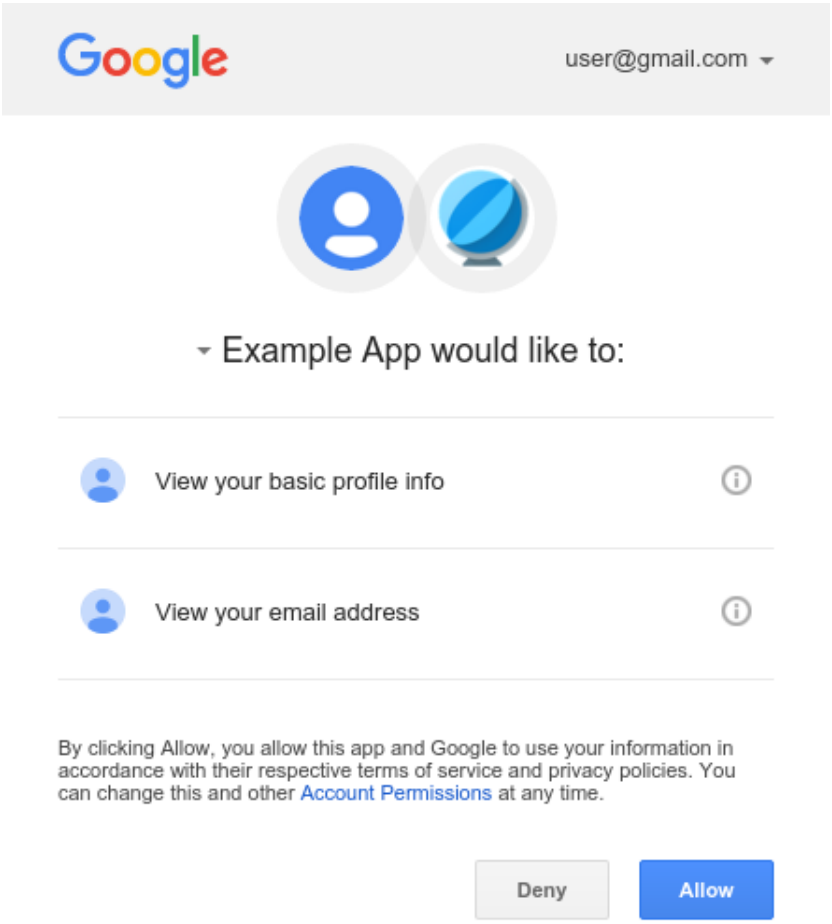
Prieigos raktas (angl. *token*) - tai objektas, identifikuojantis skaitmeninę tapatybę [Mic07].

Šis raktas būna išduodamas tapatybės tiekėjo ir skirtas identifikuoti naudotoją. Raktas būna prisegtas prie visų autentifikuoto naudotojo užklausų ir leidžia paslaugos tiekėjui žinoti, koks naudotojas kreipiasi.

Vienkartinis prisijungimas (angl. *single sign on*) - to be added.

Priedas nr. 1

OAuth prašymas naudotojui autorizuoti paslaugą



8 pav. Naudotojo sutikimas leisti Example App programai pasiekti jo Google paskyros duomenis