VILNIAUS UNIVERSITETAS

INFORMATIKOS INSTITUTAS

PROGRAMŲ SISTEMŲ BAKALAURO STUDIJŲ PROGRAMA

Blokų grandinių sistemos asmens duomenų saugojimui

Blockchain Systems for Storing Personal Data

Bakalauro baigiamasis darbas

Atliko: Dainius Simanavičius

Darbo vadovas: Asist., Dr. Vytautas Valaitis

Darbo recenzentas: Partn., Doc. Andrius Adamonis

Vilnius – 2020

Santrauka

Rašto darbe nustatytos pagrindinės tradicinių asmens duomenų saugojimo ir valdymo sistemų problemos: privatumas, saugumas, prieinamumas. Tiriamos blokų grandinės pritaikymo galimybės kuriant asmens duomenų saugojimo ir valdymo sistemas. Analizuojami tokių sistemų pranašumai ir trūkumai prieš šiuo metu egzistuojančius, tradicinius skaitmeninius ir realius sprendimus. Analizės metu pasiektos išvados, kad blokų grandinės technologija grįstos asmens duomenų saugojimo ir valdymo sistemos prieš tradicines sistemas turi tiek privalumų, tiek trūkumų. Privalumai: pritaikant decentralizaciją, nulinių žinių įrodymo metodą, decentralizuotus identifikatorius sukuriama savarankiška suvereni tapatybės valdymo sistema. Todėl išsprendžiamos tradicinėse sistemose kylančios problemos. Trūkumai: blokų grandinės technologijos pritaikymas asmeninių duomenų sektoriuje pakankamai naujas sprendimas, todėl prireiks nemažai laiko tokias sistemas integruoti į visuomenę. Antra, šios technologijos veikimo principas paprastam žmogui gan sunkiai suprantamas, todėl tai gali pakenkti tokių sprendimų populiarumui. Trečia, naudojant egzistuojančius blokų grandinės tinklus, kuriuose veikia darbo įrodymo (PoW) algoritmas (pavyzdžiui „Bitcoin“, „Ethereum“), gali nukentėti sistemos plečiamumo galimybės didėjant naudotojų skaičiui. Tai, jog blokų grandinės technologija grįstos asmeninių duomenų saugojimo ir valdymo sistemos ištaiso tradicinių sistemų trūkumus įrodo, jog atsižvelgiant į trūkumus toliau tobulinant ir plečiant blokų grandinės technologija grįstas asmeninių duomenų saugojimo ir valdymo sistemas, šios ateityje galės pakeisti šiuo metu įprastus, tradicinius sprendimus.

Raktiniai žodžiai: blokų grandinės technologija, asmeninių duomenų saugojimas, savarankiška suvereni tapatybė.

Summary

In this document, the author identifies that there are three main problems of traditional personal data storage and management systems: privacy, security, data availability. The author also researches possibilities of developing blockchain technology-based personal data storage and management applications, analyzes the advantages and disadvantages of such systems over traditional digital and real solutions. The analysis concludes that blockchain technology-based personal data storage and management systems have both advantages and disadvantages over traditional systems. Advantages: by applying decentralization, zero-knowledge proof method, decentralized identifiers, self-sovereign identity management systems are created. Therefore, the problems arising in traditional systems are solved. Disadvantages: the application of blockchain technology in the personal data sector is a relatively new solution and it will take a long time to integrate such systems into society. Second, the principle of operation of this technology is quite difficult for the average person to understand and this may undermine the popularity of such solutions. Third, the use of existing blockchain networks running a proof of service (PoW) algorithm (e.g., Bitcoin, Ethereum) may suffer from system scalability as the number of users increases. The fact that blockchain technology-based personal data storage and management systems address the problems of traditional systems demonstrates that taking into account the disadvantages in the further development and expansion of blockchain technology-based personal data storage and management systems, they might be able to replace currently used traditional systems.

Keywords: blockchain technology, storing personal data, self-sovereign identity

Turinys

Įvadas

Šiais laikais, kuomet gyvename „interneto amžiuje“, dauguma identifikacijos reikalaujančių paslaugų perkeliamos į internetinę erdvę ir žmonių, kurie turi prieigą bei naudojasi vis populiarėjančiomis internete teikiamomis paslaugomis, skaičius sparčiai auga, darosi vis svarbiau apsaugoti bei patogiai naudoti asmens duomenis. Tačiau kaip pastebima kitų autorių, tyrusių panašią temą darbuose - šiuo metu tapatybės valdymo sritis susiduria su problemomis keliose srityse. Asmens tapatybės vagystės ir duomenų pažeidimai nėra neįprasti reiškiniai ir dažnai būna nesaugios tapatybės valdymo praktikos rezultatas. Tapatybės valdymas dažnai yra centralizuotas, o tai kenkia subjektų privatumui. Paprasta visuomenė turi pasitikėti didelėmis korporacijomis ir vyriausybėmis, kad šios teisingai tvarkys jų asmens duomenis [Win17]. Kol fiziniame pasaulyje egzistuoja iš dalies tobulos sistemos asmens tapatybei nustatyti, kaip pavyzdžiui vairuotojo pažymėjimas, pasas ar asmens tapatybės kortelė, nėra lygiavertės sistemos, užtikrinančios mūsų asmens tapatybės patvirtinimo internetu, virtualioje aplinkoje [Jac16]. Tačiau atsiradus blokų grandinės technologijai vis dažniau imama galvoti apie šios technologijos pritaikymą asmens duomenų saugojimui bei valdymu: „Blokų grandinės technologija gali pasiūlyti būdą išvengti šios problemos pateikiant saugų sprendimą, nereikalaujant patikimos, centrinės valdžios.“ [Jac16]. Pradedamos kurti identifikavimo sistemos grįstos blokų grandinių technologija. Šiame darbe autorius analizuos tokių sistemų veikimo principą, lygins jas su tradiciniais sprendimais, nustatys ir pateiks blokų grandinių sistemų asmens duomenims saugoti privalumus ir trūkumus, pritaikymo galimybės.

Tyrimo Objektas

Blokų grandinės (angl. Blockchain) technologijos pritaikymo galimybės kuriant asmens duomenų saugojimo ir valdymo sistemas.

Darbo tikslas

Ištirti blokų grandinės pritaikymo galimybes kuriant asmens duomenų saugojimo ir valdymo sistemas, pranašumus ir trūkumus prieš šiuo metu egzistuojančius, tradicinius skaitmeninius ir realius sprendimus.

Uždaviniai

1. Išanalizuoti šiuo metu egzistuojančių, tradicinių asmens duomenų saugojimo/valdymo sprendimų esminius trūkumus;

2. Išanalizuoti blokų grandinės technologijos veikimo principą, struktūrą ir egzistuojančius tipus. Pateikti šios technologijos pritaikymo galimybes;
3. Išanalizuoti blokų grandinių technologija grįstų asmens duomenų saugojimo ir valdymo sistemų veikimo principą, pranašumus ir trūkumus lyginant su tradiciniais sprendimais;
4. Nustatyti ir pateikti blokų grandinės pritaikymo galimybes kuriant asmens duomenų saugojimo ir valdymo sistemas;
5. Eksperimento metu sukurti blokų grandinės technologija grįsto sprendimo prototipą;

Tyrimo metodas

Mokslinės literatūros atranka ir analizė, eksperimentas.

1. Tradicinių sprendimų trūkumai

Žmonės norėdami dalyvauti šiuolaikinės visuomenės veiklose, naudotis vis labiau populiarėjančiomis internetinėje erdvėje teikiamomis paslaugomis, turi kurti asmenines paskyras, registruoti savo asmeninius duomenis įvairiuose internetinėse svetainėse. Šiuo metu asmens duomenų valdymas nėra suverenus. Dažnas paslaugos naudotojas nesijaučia esantis savo asmeninių duomenų kontrolėje, kyla įvairių saugumo, privatumo ir prieinamumo problemų. Centrinėse duomenų bazėse saugomi naudotojų asmeniniai duomenys tampa patrauklūs ir vertingi programišiams (angl. hacker), dažnai tokius duomenis bandoma pavogti, panaudoti nelegaliems tikslams. Duomenų pažeidimai įvyksta beveik kiekvieną. dieną, atskleidžiant mūsų el. pašto adresus, slaptažodžius, kreditinių kortelių numerius, gyvenamąsias vietas, asmens kodus ir kitus privačius duomenis. Tačiau su problemomis susiduriama naudojant ne tik skaitmeninius sprendimus, bet ir realius dokumentus, tokius kaip vairuotojo pažymėjimą, pasą ir kt. Apie tai su kokiomis problemomis šiomis dienomis susiduriama naudojant tradicinius asmeninių duomenų saugojimo sprendimus plačiau aptarsime šiame skyriuje.

1.1. Saugumo problema

Sparčiai plečiantis internete teikiamų paslaugų kiekiui, dažnas žmogus naudojasi ne viena, bet keliomis, kartais net dešimtimis skirtingų paslaugų. Tai reiškia, kad naudotojas turi saugoti savo asmeninę informaciją, dažniausiai tai būna prisijungimo vardas, slaptažodis, gimimo data, visų skirtingą paslaugą teikiančių, paslaugos teikėjų serveriuose, kurie įprastai būna centralizuoti. Dėl perdėtų, kartojamų autentifikavimo, asmeninių duomenų saugojimo veiksmų atsiranda šių duomenų saugumo spragų. Tai patvirtina ir pastarųjų metų didžiausi duomenų nutekėjimo skandalai. 2019 metais daugiau nei 540 milijonų įrašų apie „Facebook“ naudotojus buvo viešai paviešinta „Amazon“ debesų kompiuterijos paslaugose [Sil19]. 2020 metais „Marriott International“ viešbučių tinklas paskelbė, kad naudojantis dviejų darbuotojų prisijungimo duomenimis buvo pavogti maždaug 5.2 milijono viešbučio lankytojų asmeninių duomenų – vardai, pavardės, gimimo datos, adresai, elektroniniai adresai ir kt. [Mih20]. Galima teigti, jog „šis į serverį orientuotas tapatybės valdymo modelis turi trūkumų. Paslaugų teikėjų požiūriu, valdyti ir autentifikuoti naudotojus tampa neišvengiamai sudėtinga. Slaptažodžiai ir asmens tapatybės informacija tradiciškai saugomi centralizuotame serveryje, o tai leidžia įsilaužėliams pasiekti savo kenkėjiškus tikslus pasisavinant, neteisėtai naudojant ar manipuliuojant šiais duomenimis. Todėl reikalaujama, kad paslaugų teikėjai sukurtų stipresnius mechanizmus, pridedant kelių veiksnių autentifikavimo prieigą ir stipresnį šifravimą, o tai dar labiau apsunkina sistemą.“ [LFA+18]. Tačiau saugumo problema egzistuoja ne tik

skaitmeninėje erdvėje, bet ir realybėje. Dokumentai su asmenine informacija, kuriuos kartu su savimi nešiojame beveik kiekvieną dieną gali būti pamesti arba pavogti, taip atsitikus visa dokumentuose esanti informacija prieinama bet kuriam dokumentą radusiam žmogui, o tai taip pat sukelia didelių saugumo problemų.

1.2. Privatumo problema

Gyvename tokiais laikais, kuomet asmeniniai duomenys žmonių gyvenime turi didelę prasmę, todėl atsidūrę netinkamose arba piktose rankose gali sumenkinti žmogaus reputaciją, patikimumą, sugriauti karjeros galimybes, sudaryti neigiamą arba neteisingą socialinį įvaizdį ir t.t Tampa aktualus asmeninių duomenų privatumas, kuris naudojant šiuolaikinius asmens duomenų saugojimo sprendimus vis dar gali būti nesunkiai pažeidžiamas. Gyvenime neretai susiduriame su situacijomis, kuriose turime įrodyti savo amžių, pavyzdžiui lankantis parduotuvėje ar einant į kino seansą. Dažniausiai savo amžiaus įrodymui naudojami dokumentai – pasas, asmens tapatybės kortelė arba vairuotojo pažymėjimas. Tačiau šiuose dokumentuose saugoma ir kita asmeninė informacija, tokia kaip vardas, pavardė, asmens kodas ir dokumento numeris. Dėl to kyla asmeninės informacijos privatumo problema, kadangi amžių tikrinanti šalis, kuriai šiuo atveju svarbi tik gimimo data, gauna prieigą prie visų dokumente esančių duomenų [Tyk19]. Ta pati asmeninių duomenų privatumo problema egzistuoja ir skaitmeninėje erdvėje. Šiais laikais vis labiau populiarėja patogų prisijungimą prie internete teikiamų paslaugų siūlantis jungtinio (angl. federated) tapatybės įrodymo būdas. Tapatybės įrodymo būdas vadinamas jungtiniu kai paslaugos tiekėjai ar organizacijos leidžia naudotojams naudoti tą pačią tapatybę skirtingose internetinėse paslaugose. Populiariausios šią vienkartinio prisijungimo paslaugą teikiančios organizacijos – „Facebook“ (Facebook Login) ir „Google“ (Google ID) . Tačiau nors ir siūlo patogesnį tapatybės įrodymo būdą, šios organizacijos gauna prieigą prie visų paslaugą naudojančių asmenų duomenų, dėl ko ir kyla privatumo problemų. Duomenų savininkas turi mažai arba išvis neturi savo asmeninių duomenų kontrolės, dažnai nežinoma kas su duomenimis daroma, su kuo jais dalinamasi [LFA+18]. Pavyzdžiui vienas daugiausiai dėmesio sulaukusių, pastarųjų metų skandalas, kuomet 2018 metais politiniais tikslais naudotojams nežinant buvo nutekinta apie 87 milijonai Facebook naudotojų asmeninių duomenų [BBC19].

1.3. Prieinamumo problema

Skaitmeninėje erdvėje naudotojų duomenys, kurių priežiūra patikėta įvairiems paslaugų tiekėjams, dažniausiai saugomi centriniame serveryje, kas gali sukelti duomenų prieinamumo problemą. Savaime arba dėl išorinių, dažniausiai programišių sukeltų veiksnių sutrikus centrinio

serverio veiklai, naudotojai nebegali pasiekti savo duomenų, jų valdyti ar pasinaudoti save identifikuojant. Prieinamumo problema aktuali ne tik skaitmeninėje erdvėje, tačiau ir realybėje. „ID4D“ pateiktais duomenimis[1] pasaulyje maždaug 1 milijardas žmonių neturi oficialių dokumentų įrodančių asmens duomenų teisingumą. Dėl šios priežasties žmogui gali kilti sunkumų norint pasinaudoti įvairiomis paslaugomis, įgyjant išsilavinimą, ieškant darbo ir kt.

[1] Projekto puslapis pasiekiamas internetiniu adresu https://id4d.worldbank.org/global-dataset

2. Blokų grandinės apibrėžimas

Šiomis dienomis plačiai ir daug kalbama apie blokų grandinės (angl. blockchain) technologiją, kuri savo svarba yra prilyginama interneto atsiradimui. Blokų grandinių technologija išpopuliarėjo maždaug prieš 11 metų, kai 2008 metais, žmogaus arba žmonių grupės (tiksliai nėra žinoma) pasivadinusio/-iais Satoshi Nakamoto dokumente pavadinimu „Bitcoin: A Peer-To-Peer Electronic Cash System" aprašė pirmąją kriptovaliutą „Bitcoin" (BTC), kuri oficialiai išleista 2009 metais, o jos veikimas buvo ir iki šiol yra grįstas blokų grandinės technologija [Nak08]. Blokų grandinės tinklas – tai paskirstyta (angl. distributed), decentralizuota, lygiarangių tinklų (angl. peer-to-peer, P2P) sistema, kurios duomenys negali būti ištrinti ir dažniausiai saugomi daugybėje tinklo mazgų išsidėsčiusių visame pasaulyje, taip užtikrinant didelį saugumą, todėl tokia sistema gali veikti be trečiųjų šalių, pavyzdžiui bankų, notarų, įsikišimo, visos operacijos atliekamos tiesiogiai tarp tinko dalyvių [SDP18, 1-2]. Šiame skyriuje plačiau apžvelgsime blokų grandinės technologijos veikimo principą, išanalizuosime jos struktūra ir aptarsime egzistuojančius tipus.

2.1. Blokų grandinės struktūra

Knygos „Blockchain For Dummies", kurioje skaitytojai supažindinami su blokų grandinės technologija, autorė Tiana Laurence išskiria tris pagrindines blokų grandinės struktūros dalis – blokas (angl. block), grandinė (angl. chain) ir tinklas (angl. network). Sujungus visas dalis, gauname blokų grandinės technologijos tinklą [Lau17, 10].

Blokas. Kiekvienas blokas esantis grandinėje yra sudarytas iš dviejų dalių – antraštės (angl. header), kurioje laikomi metaduomenys ir pagrindinės dalies (angl. body), kurioje laikomas transakcijų sąrašas. Bloko antraštėje saugomus metaduomenis sudaro prieš tai grandinėje einančio bloko maišos kodas (angl. hash), laikas (angl. timestamp), kada buvo sukurtas blokas, sunkumas, versija, „nonce" reikšmė ir Merkle šaknis (angl. Merkle Root) – visų bloke esančių transakcijų maišos kodų maišos kodas [Ant17, 197]. Pagrindinėje bloko dalyje saugomos transakcijos paprasčiausiai yra informacijos vienetai, saugantys reikalingus duomenis. Pavyzdžiui šiuo metu pagal rinkos kapitalizaciją didžiausios ir populiariausios kriptovaliutos „Bitcoin" blokų grandinės tinklo blokuose esančiose transakcijose saugoma pervedamos valiutos kiekis, siuntėjo ir gavėjo adresai, papildoma protokolo veikimui reikalinga informacija.

Pradžios blokas (angl. genesis block). Kaip ir nusako pavadinimas pradžios blokas tai pirmasis blokas grandinėje, kartais dar vadinamas blokas 0 arba blokas 1. Šis blokas ypatingas dėl tokios priežasties, jog prieš jį neegzistuoja joks kitas blokas, todėl bloko antraštėje esančiame ankstesnio

bloko maišos kodo vietoje nėra ką įrašyti. Dėl šios priežasties pradžios blokas grandinėje dažniausiai būna įrašytas blokų grandinės tinklo kūrimo metu, rankiniu būdu [Tec19].

Grandinė. Kaip jau buvo minėta, kiekvieno bloko antraštėje saugomas prieš tai blokų grandinėje einančio bloko maišos kodas. Tai reiškia, kad paėmus bet kokį tinklo bloką galėsime atsekti visus ankstesniuosius blokus užbaigiant pradžios bloku. Paprastai tariant, maišos kodas – tai virtualus piršto antspaudas. Šie virtualūs antspaudai, kurie matematiškai sujungia blokų grandinės tinklo blokus ir yra vadinamoji grandinė. Tam, kad suprastume kaip sukuriamas virtualiu piršto antspaudu dar vadinamas maišos kodas, turime išsiaiškinti kas yra ir kaip veikia maišos funkcijos. „Maišos funkcijos yra mažos kompiuterinės programos, kurios bet kokio tipo duomenis paverčia fiksuoto dydžio reikšme, nepriklausomai nuo pradinių duomenų dydžio. Maišos funkcijos vienu metu priima viena dalį įvesties duomenų ir sukuria maišos kodą atitinkantį įvesties duomenų bitus ir baitus. Maišos kodai gali turėti 0 įterptus kodo pradžioje tam, kad būtų suformuojamas reikiamas kodo ilgis. Egzistuoja daug maišos funkcijų, kurios skiriasi savo išvesties ilgiu. Svarbi grupė maišos funkcijų, kurios vadinamos kriptografinėmis maišos funkcijomis.“ [Dre17, 72]. Kriptografinė maišos funkcija SHA256, kuri sukuria beveik unikalią pastovaus 256 bitų arba 32 baitų reikšmę, yra vienas dažniausiai naudojamų funkcijų blokų grandinės tinkluose. Kriptografinės maišos funkcijos pasižymi šiomis savybėmis: yra deterministinės (angl. Deterministic) - tą pačią funkciją pritaikius tai pačiai įvesties reikšmei kelis kartus, rezultatas visada yra tas pats, pseudoatsitiktinės (angl. Pseudorandom) – funkcijos išvestis kinta nenuspėjamai, kad ir kiek mažai būtų pakeista įvestis, vienkryptės (angl. One-Way) funkcijos – žinant išvestį neįmanoma nustatyti įvesties, atsparios kolizijoms (angl. Collision Resistant) – beveik neįmanoma arba labai sunku rasti dvi ar daugiau išvesties reikšmes, kurios būtų identiškos [Lau17, 10, Dre17, 72-73].

Tinklas. Blokų grandinės tinklas veikia P2P tinklų principu, tai reiškia, kad visi tinklo naudotojai, kurie dažniausiai būna pasiskirstę po visą pasaulį, yra lygus, nėra jokių viršesnių, turinčių daugiau galimybių ar privilegijų, tinklo mazgų, todėl jie visi yra vienodai atsakingi už tinklo funkcionavimą. Blokų grandinės tinkle neegzistuoja joks serveris, jokios centralizuotos paslaugos ar hierarchijos. Tinklo mazgai dažniausiai saugo pilną visos grandinės informaciją, tvirtina naujai sukurtų blokų patikimumą. Tačiau tokie atliekami skaičiavimai blokų grandinės tinkle dažnai būna sunkūs, reikalaujantys daug resursų ir laiko, todėl naudotojai to nedaro už dyką, už atliktus skaičiavimus blokų grandinės algoritmas tinklo mazgus apdovanoja kriptovaliutos dalimi. Pavyzdžiui už atliktus skaičiavimo veiksmus „Bitcoin“ blokų grandinėje, tinklo mazgai apdovanojami „Bitcoin“ valiuta. [Ant17, 214; Lau17, 10-11]

2.2. Blokų grandinės veikimo principas

Kadangi blokų grandinės tinklas yra decentralizuota, lygiarangių tinklų sistema, kas reiškia, kad tinkle neegzistuoja joks centrinis serveris ar trečiosios šalys, kurios butų atsakingos už tinklo priežiūrą ar naujai pridėtų blokų tinkamumą ir teisingumą. Visi blokų grandinės tinklo dalyviai, kurie tinkle yra lygiaverčiai, patys sinchronizuoja blokų grandinę, tvirtina blokus ir juos prideda prie esamos grandinės. Tinklo dalyvių saugomos grandinės validumas ir vientisumas užtikrinamas naudojant konsensuso algoritmus (angl. Consensus algorithm). Tai yra taisyklės, kurios naudojamos norint surasti tinkamiausią sprendimą ar rezultatą paskirstytuose procesuose ar sistemose, kurį palaikytų visi sistemos ar proceso dalyviai. Egzistuoja ne viena konsensuso algoritmo variacija, kaip pavyzdžiui: „darbo įrodymas“ (angl. Proof of Work, PoW), „turto įrodymas“ (angl. Proof of Stake, PoS), „deleguotas turto įrodymas“ (angl. Delegated Proof of Stake, DPoS), „veiklos įrodymas“ (angl. Proof of Activity, PoA) ir kt. [AA19]. Šiame poskyryje aptarsime du labiausiai paplitusius konsensuso algoritmus – „darbo įrodymas“, kurį naudoja „Bitcoin“ [Nak08] ir „Ethereum“ [But14] kriptovaliutos ir „turto įrodymas“.

Naudojant „darbo įrodymas“ algoritmą, didelę svarbą turi „nonce“ kintamasis, kuris saugomas bloko antraštėje. Šio kintamojo reikšmė naudojama norint gauti skirtingus naujo bloko maišos kodo variantus. Tinklo dalyvis turi surasti tokia „nonce“ kintamojo reikšmę, kuri yra visiškai atsitiktinė, kad naujojo bloko maišos kodas, kuris kinta priklausomai nuo pasirinktos „nonce“ reikšmės, būtų mažesnis už tinklo nustatytą maišos kodą, kuris yra nustatomas pagal tuo metu tinklo dalyvių generuojamą skaičiavimo galią – kuo ji didesnė, tuo sunkiau surasti tinkamą „nonce“ reikšmę ir atvirkščiai, kuo dalyviu skaičiavimo galia mažesnė, tuo lengviau randama „nonce“ reikšmė. Pavyzdžiui „Bitcoin“ kriptovaliutos blokų grandinės tinkle nustatyta maišos kodo reikšmė būna tokia, jog tinklo dalyviai surastų tinkamą maišos kodo reikšmę per 10 minučių. [Nak08]. Tinklo dalyvis suradęs tinkamą „nonce“ kintamojo reikšmę apie tai praneša kitiems tinklo mazgams, kurie iš pradžių įsitikinę, jog bloko maišos kodas su jau nustatyta „nonce“ reikšme yra teisingas, prideda jį prie egzistuojančios grandinės. Tinklo dalyvis suradęs tinkamą „nonce“ reikšmę gauną atlygį – dažniausiai tai būna tinklo valiuta. Šis konsensuso algoritmas yra brangus ir pakankamai neefektyvus sunaudotų resursų atžvilgiu, kadangi vienam tinklo dalyviui radus tinkamą „nonce“ reikšmę, visi tinklo mazgai skaičiavimus pradeda iš naujo, tai reiškia, kad visos pastangos ir resursai (elektros energija, laikas, kompiuterinė įranga) išnaudoti ieškant grandinės bloko „nonce“ reikšmės tapo niekiniai, kadangi skaičiuojant naujų blokų „nonce“ reikšmes, senosios nesuteikia jokios naudos. Tačiau nors ir

neefektyvus resursų atžvilgiu, „darbo įrodymas“ išlieka vienu populiariausiu konsensuso algoritmų [Ant17, 228-231; SDP18, 131-133].

Kitas, taip pat populiarus konsensuso algoritmas - „turto įrodymas“. „PoS tai metodas, kuris naudojamas kriptovaliutų blokų grandinės tinkle norint pasiekti paskirstytąjį konsensusą. „Turto įrodymas“ prašo naudotojų įrodyti, kad jie valdo tam tikrą kiekį tinklo valiutos“ [Ant17, „Quick Glossary“ XXIX]. Šis algoritmas nuo „darbo įrodymas“ skiriasi tuo, jog tinklo mazgai nesivaržo tarpusavyje kas greičiau suras tinkamą „nonce“ reikšmę. Tinklo, kuriame naudojamas „turto įrodymas“, dalyviai turi „užstatyti“ norimą kiekį tinklo valiutos tam, kad galėtų tvirtinti naujus grandinės blokus. Tikimybė, jog tinklo dalyvis galės patvirtinti ir pridėti naują bloką į grandinę yra proporcingas „užstatytos“ valiutos kiekiui. Pavyzdžiui, jeigu tinklo mazgo „užstatytos“ valiutos suma sudaro 2% visame tinkle egzistuojančios valiutos, jis galės patvirtinti 2% naujai pridedamų blokų. Patvirtinus naujus blokus grandinėje, tinklo dalyvis atgauna savo „užstatytą“ valiutos kiekį po tam tikro laiko, kai įsitikinama, jog šio dalyvio į grandinę pridėti blokai yra teisingi/tikslūs. Konsensuso algoritmas „turto įrodymas“ veikia greičiau bei yra pigesnis už PoW algoritmą, kadangi skaičiavimai yra daug lengvesni, nereikalaujantys didelės skaičiuojamosios galios, veltui nešvaistomi resursai (elektros energija, laikas, kompiuterinė įranga). Taip pat, lyginant su PoW, PoS algoritmas suteikia didesnį saugumo lygį, kadangi norint pakenkti vertingam blokų grandinės tinklui, reikia valdyti didelę tinklo valiutos dalį, o ją įsigyti daug kainuoja, nes kuo daugiau perkama valiutos, tuo labiau kyla jos kaina [SDP18, 133-134].

2.3. Blokų grandinės tinklų tipai

Toshendra Kumar Sharma iš „Blockchain Council“ išskiria keturis blokų grandinės tinklų tipus: du pačius populiariausius ir dažniausiai sutinkamus - viešus (angl. public) ir privačius (angl. private), bei dar du papildomus - hibridinius (angl. hybrid) ir konsorciumo (angl. consortium) [Sha19a]. Pagrindinis ir didžiausias šių blokų grandinės tinklų tipų skirtumas yra tai, kas gali pasiekti, skaityti informaciją bei sukurti ar pridėti naujų blokų į grandinę.

Vieša blokų grandinė. Tai neapribota, nereikalaujanti leidimų transakcijų sistema [Sha19a]. „Kiekvienas, turintis prieigą prie interneto, gali prisijungti prie blokų grandinės tinklo platformos, kad taptų autorizuotu tinklo mazgu ir būtų blokų grandinės tinklo dalimi. Tinklo mazgui ar naudotojui, kuris yra viešosios blokų grandinės dalis, leidžiama pasiekti esamus ir ankstesnius įrašus, tvirtinti transakcijas arba atlikti „darbo įrodymus“ (angl. Proof of Work, PoW) naujai sukurtam grandinės blokui, taip „kasant“ tinklo valiutą. Pats paprasčiausias viešosios blokų grandinės tinklas yra naudojamas „kasant“ ir keičiant kriptovaliutas“ [Dat19]. Šio tipo blokų grandinėse neegzistuoja

naudotojas ar tinklo mazgas, kuris turėtų daugiau galimybių ar teisių už kitus, visi autorizuoti tinklo dalyviai yra lygus ir gali dalyvauti kuriant naujus blokus, skaitant ar tikrinant jau esamus. Viešos blokų grandinės yra atviros ir prieinamos visiems [Sha19a]. Šiuo metu egzistuojantys patys populiariausi viešos blokų grandinės tinklo pavyzdžiai – „Bitcoin“ [Nak08], „Ethereum“ [But14] ir „Ethereum“ išmaniesiems kontraktams [But14].

Privati blokų grandinė. Tai apribota, reikalaujanti leidimų, uždarame tinkle veikianti transakcijų sistema. Privati blokų grandinė dažniausiai nėra pilnai decentralizuota ir platinama kaip viešo tipo blokų grandinės tinklas. Šio tipo naudotojai - dažniausiai privatūs asmenys arba įmonės, kur tik atrinkti naudotojai turi prieigą prie blokų grandinės tinklo [Dat19]. Skirtingai negu viešose, privačiose blokų grandinėse egzistuoja tinklo kūrėjų parinktas naudotojas, kuris yra atsakingas už tinklo priežiūrą ir teisių, pasiekti ar įrašyti informaciją, suteikimą kitiems tinklo naudotojams. Visų autorizacijų, prieinamumo leidmų ir saugumo lygio nustatymas yra tinklą valdančios organizacijos rankose [Sha19a], todėl „privati blokų grandinė gali lengvai, jei nori, pakeisti blokų grandinės tinklo taisykles, sugrąžinti operacijas, modifikuoti likučius ir t.t“ [But15]. Šiuo metu egzistuojantys privačios blokų grandinės tinklo pavyzdžiai – Corda[2], Multichain[3], Hyperledger Sawtooth[4] [Sha19a].

Hibridinė blokų grandinė. Kaip ir nusako tipo pavadinimas, hibridinė blokų grandinė yra dviejų anksčiau minėtų tipų – privačios ir viešos blokų grandinės kombinacija. Hibridinė blokų grandinė vienu metu naudoja dviejų tipu bruožus, o tai reiškia, kad viena tinklo dalis gali būti privati, reikalaujanti leidimų, kai tuo tarpu kita tinklo dalis yra viešai prieinama. Pasirinkus tokį sprendimo būdą naudotojai ar tinklo mazgai gali nustatyti, koks naudotojas galės ar negalės matyti tam tikrus duomenis [Sha19a]. Taip pat hibridinė sistema pasižymi lankstumu, naudotojai nesunkiai gali sujungti privačias blokų grandines su keliomis viešomis. Privačioje hibridinio tinklo dalyje įvykusios transakcijos dažniausiai tikrinamos/patvirtinamose toje pačioje privačioje dalyje, tačiau naudotojai turi galimybę informaciją patalpinti ir viešoje tinklo dalyje [Dat19]. Taigi hibridinė blokų grandinė yra lygiai taip pat saugi kaip ir privačioji, tačiau naudotojams išlieka tokia pat skaidri kaip ir viešoji. Šiuo metu egzistuojantys hibridinio tipo pavyzdžiai - Dragonchain[5], XinFin[6].

[2] Projekto puslapis pasiekiamas internetiniu adresu https://www.corda.net/

[3] Projekto puslapis pasiekiamas internetiniu adresu https://www.multichain.com/

[4] Projekto puslapis pasiekiamas internetiniu adresu https://www.hyperledger.org/projects/sawtooth

[5] Projekto puslapis pasiekiamas internetiniu adresu https://dragonchain.com/

[6] Projekto puslapis pasiekiamas internetiniu adresu https://xinfin.org/

Konsorciumo blokų grandinė. Šio tipo blokų grandinė dažniausiai suprantama kaip privačios blokų grandinės atšaka. Pagrindinis dviejų tipų skirtumas yra tas, jog konsociumo blokų grandinė yra valdoma organizacijų grupės, kai tuo tarpu privačios blokų grandinės yra valdomos vienos organizacijos [Dra19]. Todėl pasirinkus šį sprendimą, daugiau nei viena organizacija gali dalintis informacija arba užsiimti „kasimu“. Šio tipo blokų grandinės dažniausiai naudojamos bankuose, valstybinėse organizacijose ir t.t. [Dat19].

2.4. Blokų grandinės panaudojimo galimybės

Dažniausiai blokų grandinės technologija yra tapatinama su kriptovaliutomis, ypatingai su plačiausiai žinomu „Bitcoin“, kadangi visas šios didelio populiarumo ir daug diskusijų sulaukusios kriptovaliutos veikimas yra pagrįstas blokų grandinės technologija. Tačiau toks požiūris, jog blokų grandinių technologija skirta tik pirkti, parduoti ar apskritai atsiskaityti kriptovaliutomis yra neteisingas. Šios technologijos galimybės yra daug didesnės. Tai atsispindi ir blokų grandinės pritaikymo galimybes tyrusių autorių darbuose [GR18, ZS18, Sha19b, Lem17]. Keletas pritaikymo atvejų plačiau:

- Elektroniniai balsavimai. Naudojant blokų grandinės technologiją, elektroniniai balsavimai tampa skaidrūs, tačiau nepažeidžia balsuotojų privatumo. Taip pat lengva įrodyti rezultatų tikrumą, kadangi į grandinę įrašyti blokai yra nekeičiami. Vienas iš egzistuojančių sprendimų, naudojančių blokų grandinės privalumus – „Follow my vote[7]“
- Medicina. Blokų grandinė naudojama pacientų sveikatos istorijos duomenims kaupti ir valdyti išlaikant didelį saugumą ir privatumą. Vienas iš egzistuojančių sprendimų, naudojančių blokų grandinės privalumus – „MedRec[8]“
- Nekilnojamo turto sektorius. Naudojant blokų grandinės technologiją galima sudaryti sandorius be trečiųjų šalių, kadangi yra pilnai pasitikima blokų grandinėje saugoma informacija. Tai sumažina nekilnojamo turto pirkimo, pardavimo ar nuomos sutarčių sudarymo laiką bei kaštus. Vienas iš egzistuojančių sprendimų, naudojančių blokų grandinės privalumus – „Propy[9]“.

[7] Projekto puslapis pasiekiamas internetiniu adresu https://followmyvote.com/

[8] Projekto puslapis pasiekiamas internetiniu adresu https://medrec.media.mit.edu/

[9] Projekto puslapis pasiekiamas internetiniu adresu https://propy.com/browse/

3. Blokų grandinės pritaikymas kuriant asmeninių duomenų sistemas

Pastaruoju metu žmonės vis rimčiau žiūri į asmeninius duomenis, pastebimi tradicinių, dažniausiai centralizuotų sistemų trūkumai, ieškoma patogių, bet tuo pačiu metu ir duomenų privatumą ir saugumą užtikrinančių asmeninių duomenų saugojimo ir valdymo sprendimų. Paskirstytos buhalterinės knygos technologija (angl. distributed ledger technology, DLT) yra būtent tai, kas leidžiantis tai padaryti. Tai suteikia galimybę kelioms institucijoms, organizacijoms ir vyriausybėms dirbti kartu, sukuriant decentralizuotą tinklą, kuriame duomenys saugomi keliose vietose, todėl tinklas tampa labiau atsparus klaidoms, o jame saugomi duomenys - klastojimui [TR18]. Decentralizuotos sistemos privalumai taip pat pastebimi ir aprašomi Bryan Pon, Chris Locke, Tom Steinberg leidinyje , „Private-Sector Digital Identity in Emerging Markets“: „Atviros, decentralizuotos sistemos įgalina asmenis turėti pilną savo tapatybės kontrolę, todėl kyla idėja apie „savarankiškas suverenias“ tapatybės sistemas. Šios sistemos naudoja paskirstytos buhalterinės knygos ir šifravimo technologijų derinius, siekiant sukurti nekintamus tapatybės įrašus. Asmuo susikuria tapatybės „talpyklą“, leidžiančią priimti asmenines savybes ar kredencialus iš neriboto skaičiaus organizacijų, įskaitant vyriausybę, tinklo ekosistemoje, kurioje gali dalyvauti bet kuri organizacija (pavyzdžiui išduoti kredencialus).“ [PLS16]. Šiuo metu jau egzistuoja sprendimų, kurie šiek tiek skiriasi technologiniais sprendimais, pritaikančių blokų grandinę asmeninių duomenų saugojimui. Šiame skyriuje aptarsime egzistuojančius pavyzdžius, jų veikimo principą, privalumus prieš tradicinius sprendimus.

3.1. Egzistuojantys blokų grandinės sprendimai

Šiame poskyryje aptarsime dviejų, „Sovrin“ ir „uPort“, asmeninių duomenų saugojimo ir valdymo naudojant blokų grandinės technologiją sprendimų veikimo principus. Šiuos sprendimus iš kitų daugelio šiuo metu sukurtų ar dar besikuriančių asmens duomenų saugojimo ir valdymo sprendimų autorius pasirinko dėl didelio šių sprendimų populiarumo, išbaigtumo, plačios ir laisvai prieinamos dokumentacijos. Poskyrio pradžioje autorius aptars bendrus analizuojamų sprendimų bruožus, o vėliau – skirtumus, analizuojant kiekvieno sprendimo veikimo principą atskirai.

Pirmiausia, blokų grandinės sprendimai, įskaitant tiek „Sovrin“, tiek „uPort“ veikia naudojant nulinių žinių įrodymą (angl. Zero-Knowledge Proof, ZKP). Tai metodas, kurį naudojant užtikrinamas asmeniniu duomenų privatumas, nes vienas subjektas gali įrodyti kitam subjektui, jog jis žino tam tikrą informaciją arba atitinka tam tikrus keliamus reikalavimus, neatskleidžiant jokios realios informacijos apie save. Paprasčiausias pavyzdys – sistemos, veikiančios nulinių žinių įrodymo

metodo pagrindu, naudotojas gali įrodyti, jog yra pilnametis, neatskleidžiant savo pilnos gimimo datos tikrinančiajai šaliai.

Antrasis nagrinėjamų sprendimų panašumas, jog tinkle dalyvauja ir tarpusavyje komunikuoja 3 skirtingų rolių naudotojai:

1. Kredencialų savininkai (angl. owners). Tai tinklo naudotojai, kurie asmeninėje skaitmeninėje piniginėje (dažniausiai tai yra mobilioji aplikacija), saugo kitų, patikimų tinklo naudotojų išduotus asmeninius kredencialus – patvirtintus asmeninės informacijos rinkinius (amžius, adresas, išsilavinimas ir t.t.) apie save, kuriuos vėliau, norėdami pasinaudoti kokia nors paslauga gali pateikti tapatybės tikrintojams [Tyk19]. Kredencialų savininkai pilnai kontroliuoja turimą informaciją, laisvai pasirenka kokią informaciją atskleisti ir su kuo ja dalintis [Win18]. Pilna savininko kontrolė dar vadinama savarankiška suverenia tapatybe (plačiau aptariama „Savarankiška suvereni tapatybė“ skyriuje), kurią užtikrina tiek „Sovrin“, tiek „uPort“ sprendimai.
2. Kredencialų išdavėjai (angl. issuers). Kredencialų išdavėjai – tai patikimi žmonės ar organizacijos, pavyzdžiui vyriausybė, bankai, draudimo įmonės, valstybinės įstaigos, tokios kaip vairuotojo pažymėjimo išdavėjos ir t.t., kurios kitiems tinklo naudotojams gali išduoti asmeninius kredencialus. Išduodami kredencialą, išdavėjai patvirtina/paliudija, jog kredencialuose pateikta naudotojo asmeninė informacija (pavyzdžiui vardas, amžius, adresas) yra tikra ir teisinga. Kredencialų naudingumas ir patikimumas visiškai priklauso nuo išdavėjo reputacijos ir patikimumo. Pavyzdžiui, pasų išdavimo įstaiga gali išduoti kredencialą, patvirtinantį, kad asmuo turi pasą su konkrečiu numeriu ir galiojimo data. Pasų išdavimo įstaiga kredencialą pasirašo naudodamasi savo privačiu raktu, todėl ateityje galima nesunkiai patikrinti, jog kredencialas yra tikras, jo saugoma informacija nepakeista ar kitaip nesuklastota [TR18, Tyk19].
3. Tapatybės tikrintojai (angl. verifiers). Dažniausiai tapatybės tikrintojai – paslaugos teikėjai, kuriems reikalinga asmeninė informacija apie paslaugos gavėją (šiuo atveju kredencialų savininką), tam, kad galėtų suteikti paslaugą. Tapatybės tikrintojai naudojasi blokų grandinės arba kitu decentralizuotu tinklu, tam kad nustatytų pateiktų kredencialų validumą. Pavyzdžiui, kredencialų savininkui pateikus patvirtinimą, jog jis yra tam tikro amžiaus, tikrinančioji šalis decentralizuotame tinkle patikrina kas išdavė ir pasirašė pateiktą kredencialą. Suradus kredencialų išdavėją, tapatybės tikrintojai turi visišką laisvę savarankiškai nuspręsti ar juo galima pasitikėti [Tyk19, Win18].

„Sovrin“ yra atviro kodo, viešas, apribotas (angl. permissioned), decentralizuotas asmens duomenų valdymo tinklas, sukurtas naudojant DLT. Tik patikimos institucijos, vadinamos valdytojomis (angl. steward) - tai gali būti bankai, universitetai, vyriausybės ir kt., gali valdyti mazgus dalyvaujančius konsensuso algoritmuose. Uždaro tinklo pasirinkimas nulemia tai, kad tinklo mazgams norint pasiekti bendrą sutarimą dėl tinkle būklės, nereikia atlikti brangaus darbo įrodymo (PoW) skaičiavimo, kas leidžia sumažinti energijos sąnaudas ir pagerinantį transakcijų pralaidumą. „Sovrin” tinkle naudotojas identifikuojamas naudojant decentralizuotus identifikatorius (plačiau aptariama „Decentralizuotas identifikatorius“ skyriuje), kurie valdomi asimetrine viešo ir privataus raktų pora. Privatumo tikslais naudotojas gali turėti tiek decentralizuotų identifikatorių, kiek jam reikia. Šie identifikatoriai tarpusavyje niekaip nėra susiję, todėl vienas identifikatorius gali būti susietas su išsilavinimo informacija, kitas su gyvenamojo adreso informacija, kitas dar su kita asmenine informacija, taip užtikrinamas naudotojo duomenų privatumas. Pagrindinis „Sovrin” tinklo elementas – tai paskirstytoji buhalterinė knyga, kurios mazguose (kuriuos prižiūri valdytojai) saugomi decentralizuoti identifikatoriai, su jais susiję viešieji raktai, kredencialų schemos ir t.t. Svarbu paminėti, kad naudotojų asmeniniai duomenys tinkle nesaugomi. Visi naudotojų duomenys saugomi jų pačių įrenginiuose esančiose skaitmeninėse piniginėse – taip sukuriama savarankiška suvereni tapatybė. Skaitmeninėje piniginėje saugomi ne tik asmeniniai duomenys, bet ir sugeneruotos kriptografinių raktų poros, kuriuos skaitmeninės piniginės programėlė padeda naudotojams valdyti. Visas bendravimas tarp tinkle esančių naudotojų veikia naudojantis skaitmeninės piniginės programa ir „Sovrin” tinklo sukurtais agentais (angl. agents) – tai saugūs tinklo galutiniai taškai (angl. endpoint), kurie veikia naudotojų vardu ir yra visuomet pasiekiami. Kadangi „Sovrin” tinko naudotojai visiškai kontroliuoti visus savo kredencialus – tik jie nusprendžia kas, kada ir kokią jų asmeninę informaciją galės matyti [DP18, FLK19, 451-453].

„uPort“ yra atvirojo kodo decentralizuotas asmens duomenų saugojimo ir valdymo karkasas, naudojantis išmaniuosius kontraktus (plačiau aptariama „Išmanusis kontraktas“ skyriuje) ir veikiantis Ethereum blokų grandinės tinkle. „uPort“ suteikia galimybę naudotojui saugoti savo asmeninius duomenis, siųsti ir prašyti kredencialų, pasirašinėti transakcijas, bei saugiai valdyti kriptografinius raktus. Pagrindinis naudotojui skirtas įrankis – „uPort“ mobilioji programėlė, kuri kiekvieno naudotojo registracijos metu sugeneruoja viešojo ir privačiojo raktų porą, į Ethereum tinklą įdiegia 3 kontraktus - valdymo (angl. controller), kuris skirtas saugomiems duomenis valdyti, tarpininko (angl. proxy), kurio paskirtis identifikuoti naudotoją (uPortID) ir atkūrimo (angl. recovery), kuris skirtas sugrąžinti naudotojo prieigą prie asmeninių duomenų, jei ši buvo prarasta. Visas duomenų valdymas

ir bendravimas su kitais sistemos naudotojais ar trečiosiomis šalimis vyksta per valdymo ir tarpininko kontraktus. Sistemos naudotojas gali turėti tiek identifikatorių (uPortID), kiek jam reikia, šie identifikatoriai tarpusavyje niekaip nėra susiję. Kiekvienas "uPort" sistemos identifikatorius yra atvaizduojamas į "uPort" registre saugomus duomenis. "uPort" registras – tai dar vienas išmanusis kontraktas. Bet kuris naudotojas gali kreiptis į registrą, tam, kad gautu duomenis, tačiau tik konkretus duomenų savininkas, su kurio uPortID yra susieti saugomi duomenis, gali juos modifikuoti. Dėl talpos dydžio sumetimų, duomenys registre saugomi JSON formatu, kuriame įrašyti asmeninių duomenų atributų maišos kodai. Patys duomenys saugomi IPFS (angl. InterPlanetary File System): paskirstytoje failų sistemoje, kurioje failą galima nuskaityti pagal jo maišos kodą. Dėl "uPort" registre saugomų duomenų, gali kilti problemų – nors duomenys ir užšifruoti, bet gali nutekėti metaduomenys apie konkrečius atributus arba santykiai su tapatybės teikėjais / pasitikinčiomis šalimis, dėl ko gali būti pažeistas privatumas. Dar viena problema – "uPort" sistemos plečiamumas. Kadangi naudojamasi Ethereum tinklu, plečiantis "uPort" sistemai ir didėjant tinklo naudotojų skaičiui, "uPort" gali nebesugebėti pasiūlyti pigių ir greitų transakcijų [DP18, FLK19, 453-454].

3.2. Decentralizuotas identifikatorius

Decentralizuotas identifikatorius (angl. Decentralized identifier, DID) – tai „globaliai unikalus identifikatorius, kuriam nereikalinga centralizuota registravimo institucija, nes identifikatorius yra registruojamas naudojantis paskirstytos buhalterinės knygos technologija (DLT) arba kita decentralizuoto tinklo forma." [RSS+20]. Plačiau tariant – „Decentralizuoti identifikatoriai (DID) yra naujo tipo identifikatoriai, leidžiantys patvirtinti, decentralizuotą skaitmeninę tapatybę. DID identifikuoja bet kurį subjektą (pvz., Asmenį, organizaciją, daiktą, duomenų modelį, abstraktų subjektą ir kt.), kurį DID valdytojas nusprendžia identifikuoti. Šie nauji identifikatoriai yra sukurti tam, kad DID valdytojas galėtų įrodyti jo valdymą ir būtų įgyvendinamas nepriklausomai nuo bet kokio centralizuoto registro, tapatybės teikėjo ar sertifikato institucijos. Decentralizuoti identifikatoriai yra nuorodos, kurios susieja DID subjektą su DID dokumentu, leidžiantį su juo patikimai sąveikauti." [RSS+20]. Decentralizuotas identifikatorius yra išreikštas tekstine reikšme, kuri susideda iš 3 dalių (žiūrėti 1 pav.):

1. Schemos identifikatorius. Visi DID turi pastovų schemos identifikatorių „did", kuris nurodo, kad tai yra decentralizuoto identifikatoriaus reikšmė.
2. Metodas. Metodo dalis nurodo mechanizmą, kaip atliekami kūrimo, skaitymo, atnaujinimo, trynimo veiksmai su DID ir su juo susietu DID dokumentu [Met19].
3. Identifikatorius metodo kontekste. Unikali reikšmė metodo kontekste.

1 pav. DID struktūra

„Sovrin“ įstaigos pirmininkas, taip pat „Internet Identity Workshop“ įkūrėjas ir organizatorius Phil Windley teigia, kad decentralizuoti identifikatoriai turi tenkinti tokias 4 pagrindines savybes [Win19], kurios taip pat paminėtos ir kitame šaltinyje [HGG20]:

- Decentralizuoti. DID turi veikti nepriklausomai nuo jokios centralizuotos registravimo institucijos. Dėl šios priežasties identifikatoriai gali būti kuriami ir atnaujinami nepriklausomai nuo vienos šalies ar subjekto kompetencijos, padidinant atsparumą cenzūrai [Win19, HGG20].
- Pastovūs. „Pastovumas užtikrina, kad identifikatorius visada nurodo tą patį subjektą. Todėl DID yra privatesni ir saugesni nei identifikatoriai, kuriuos galima priskirti iš naujo, pvz., domeno vardas, IP adresas, el. pašto adresas arba mobiliojo telefono numeris. Pastovumas yra labai svarbus naudotojo kontrolei ir savarankiškam suverenumui.“ [Win19].
- Kriptografiškai patvirtinami. Decentralizuoti identifikatoriai yra susieti su kriptografiniais raktais, todėl kontroliuojantis subjektas gali naudoti susietus raktus nuosavybės teisei įrodyti. Dėl šios savybės, šalys, apsikeitusios DID, gali viena kitą autentifikuoti ir užšifruoti savo bendravimą. [Win19, HGG20, Tyk19].
- Išsprendžiami. Decentralizuoti identifikatorius yra išsprendžiamas, taip gaunant su juo susietą DID dokumentą. Sprendimas tai DID dokumento susieto su konkrečiu identifikatoriumi paieškos veiksmas, naudojant metodą, kurį nurodo DID metodo komponentas. Apibendrinant galima sakyti, kad DID infrastruktūra veikia kaip visuotinė, decentralizuota rakto-vertės talpykla, kurioje raktai yra decentralizuoti identifikatoriai, o vertės - DID dokumentai. [Win19].

DID dokumentas – tai „Duomenų, apibūdinančių DID subjektą, rinkinys, įskaitant mechanizmus, tokius kaip viešieji raktai ir pseudonimiški biometriniai duomenys, kuriuos DID subjektas gali naudoti savo tapatumui patvirtinti ir įrodyti savo ryšį su DID. DID dokumente taip pat gali būti kitų atributų ar tvirtinimų, apibūdinančių subjektą. Šie dokumentai yra grįsti grafinių

duomenų struktūra, kurie paprastai išreiškiami naudojant [JSON-LD], tačiau gali būti išreikšti naudojant kitus suderinamus, grafinių duomenų struktūra grįstus formatus.“ [RSS+20].

3.3. Savarankiška suvereni tapatybė

Savarankiška suvereni tapatybė (angl. self-sovereign identity, SSI) – tai tapatybė, kurios informaciją valdo ir prižiūri pats tapatybės savininkas ar organizacija. SSI gali būti sudaryta iš įvairios informacijos kaip pavyzdžiui: asmens gimimo datos, vardo, pavardės, asmens kodo, pilietybės, išsilavinimo informacijos, asmens kredito informacijos ir t.t. Ši tapatybė nepriklauso nuo jokios centrinės valdžios ir niekada negali būti atimta. Savarankiškos suverenios tapatybės informacija dažniausiai laikoma skaitmeninėje piniginėje ir tik pats savininkas sprendžia kas ir kokią informacijos dalį gali matyti. Norint pasinaudoti kokiomis nors paslaugomis, žmogus nebeturi suteikti savo asmeninės informacijos paslaugos tiekėjams, kad jie ją saugotų, tapatybės įrodymui pilnai užtenka skaitmeninės piniginės su joje esančia informacija [Sov18a, Sov18b, Tyk19]. Kadangi savarankiškos suverenios tapatybės informacija saugoma individualiai kiekvieno asmens skaitmeninėje piniginėje, o ne centrinėje duomenų bazėje, išvengiama keletas pagrindinių šiuo metu egzistuojančių sistemų problemų:

1. Norint neteisėtai pasisavinti kitų asmenų informaciją, programišiai turi įsilaužti ne į vieną centrinę duomenų bazę, bet į kiekvieno asmens įrenginį atskirai. Tai padaryti yra daug sudėtingiau, kadangi užimtų daug laiko ir kompiuterinių resursų [Tyk19].
2. Dėl duomenų decentralizacijos, įmonės ar kiti paslaugos tiekėjai nebeturi kaupti naudotojų asmens duomenų savo centrinėse duomenų bazėse, taip sumažinant duomenų valdymo, priežiūros kaštus ir panaikinat riziką susijusią su paslaugos naudotojų asmens duomenų vagystėmis ar nutekėjimais [Tyk19].

Šaltiniuose [Win17, DJJ17], kuriose tiriamos skaitmeninės tapatybės panaudojimo galimybės, išskiriamos 10 savybių, kuriomis pasižymi savarankiška suvereni tapatybė:

1. Asmens tapatybė nepriklauso nuo jokios centrinės valdžios
2. Tapatybės savininkas turi pilną savo informacijos kontrolę;
3. Tapatybės savininkas bet kada gali pasiekti savo duomenis;
4. Sistemos ir algoritmai yra skaidrūs;
5. Tapatybė galioja tiek ilgai, kiek to nori tapatybės savininkas;
6. Tapatybės informacija ir su ja susijusios paslaugos prieinamos iš bet kur;
7. Tapatybės naudojamos tiek plačiai, kiek leidžia galimybės;
8. Tapatybės informacija prieinama tik su savininko leidimu;

9. Veiksmui atlikti naudojami tik tam veiksmo atlikimui reikalingi duomenys;
10. Turi būti užtikrinamas tapatybės duomenų saugumas;

Apibendrinant, savarankiška suvereni tapatybė yra privati, saugi ir prieinama iš bet kur (kitaip tariant – nešiojama (angl. portable)) [Tyk19].

3.4. Išmanusis kontraktas

Išmanusis kontraktas – tai į blokų grandinę įrašyta programa, kuri pasikreipus jai tinkle priskirtu adresu, automatiškai, pagal iš anksto nustatytas taisykles leidžia saugiai apsikeisti, pasidalinti skaitmeninėmis vertybėmis (kriptovaliutomis, asmens duomenimis ir t.t.). Dėl saugumo ir automatinio veikimo išmanieji kontraktai suteikia galimybę atsisakyti trečiųjų šalių dalyvavimo įvairiuose skaitmeninių vertybių apsikeitimo sandoriuose. Šiuo metu vieni populiariausių – "Ethereum" tinkle veikiantys išmanieji kontraktai, naudojantys tinklo mazguose įdiegtą „Ethereum" virtualią mašiną (angl. Ethereum Virtual Machine, EVM), kurioje vykdomas EVM baitų kodas. Nors "Ethereum" išmaniąsias sutartis galima kurti naudojant tiesiogiai baitų kodą, tačiau tai daryti yra gan sunku ir nepatogu, todėl yra sukurta aukštesnio lygio programavimo kalbų: "Serpent", "Vyper", "Bamboo" ir šiuo metu populiariausia – "Solidity", kurios ženkliai palengvina išmaniųjų kontraktų kūrimo procesą [But14; Ant18, 127-131].

3.5. Blokų grandinės technologija grįstų sprendimų privalumai ir trūkumai

Skyriuje „Tradicinių sprendimų trūkumai" autorius pateikė esmines problemos, kylančias naudojant tradicinius asmeninių duomenų saugojimo ir valdymo sprendimus. Nustatytos duomenų saugumo, duomenų privatumo ir duomenų prieinamumo problemos. Šiame skyriuje autorius išanalizavo egzistuojančių blokų grandinės technologija grįstus sprendimus, apibrėžė savarankišką suverenią tapatybę ir decentralizuotus identifikatorius, todėl galima apibrėžti blokų grandinės technologijos privalumus ir trūkumus lyginant su tradiciniais asmens duomenų saugojimo ir valdymo sprendimais. Apibendrinti rezultatai pateikiami 1 lentelėje, o plačiau aprašyti skirsniuose „Privalumai" ir „Trūkumai"

1 lentelė. Blokų grandinės technologija grįstų asmeninių duomenų saugojimo ir valdymo sistemų privalumai ir trūkumai gauti lyginant su tradicinėmis sistemomis

Kriterijus	Trūkumas	Privalumas	Priežastis
Privatumas		X	Naudotojų asmeninių duomenų privatumas blokų grandinės technologija

			grįstose sistemose užtikrinamas naudojantis nulinių žinių įrodymo metodu (ZKP). Taip pat suteikiama galimybė naudotojams sugeneruoti tiek skaitmeninėje piniginėje valdomų identifikatorių, kiek pats naudotojas galvoja, kad jam yra reikalinga, norint išskaidyti asmeninę informaciją, taip dar labiau padidinant saugomų asmeninių duomenų privatumą.
Saugumas		X	Decentralizuotas tinklas suteikia galimybę lengvai sukurti savarankišką suverenią tapatybės valdymo sistemą. Tai reiškia, kad asmeniniai naudotojų duomenys laikomi jų pačių įrenginiuose, taip ženkliai sumažinant duomenų vagysčių galimybes, kadangi norint pasinaudoti svetimais duomenimis nebeužtenka gauti prieigą prie vienos centrinės vietos, į kiekvieno asmens įrenginį turi būti įsilaužiama atskirai.
Duomenų prieinamumas		X	Duomenų prieinamumą užtikrina blokų grandinės technologijos savybės – decentralizacija ir skaitmeninė prieiga. Priešingai negu centralizuotose sistemose, duomenų kopijos saugomos daugybėje tinklo mazgų, todėl net ir sutrikus vieno ar kelių tinklo mazgų veiklai, saugomi duomenys ir toliau išlieka prieinami veikiančiuose tinklo mazguose. Taip pat dėl per nuotolį išduodamų ir patvirtinamų kredencialų

			suteikiama galimybė asmenims, iki šiol neturėjusiems galimybės, lengviau įrodyti savo asmens duomenų tikrumą
Pritaikymas visuomenėje	X		Blokų grandinės technologijos pritaikymas asmeninių duomenų sektoriuje pakankamai naujas sprendimas, todėl prireiks nemažai laiko tokias sistemas integruoti į visuomenę.
Populiarumas	X		Šios technologijos veikimo principas paprastam žmogui gan sunkiai suprantamas, todėl tai gali pakenkti tokių sprendimų populiarumui.

3.5.1. Privalumai

Didžiausias ir pagrindinis blokų grandinės technologija grįstų sprendimų privalumas – išsprendžiamos tradicinėse sistemose kylančios problemos. Kaip tai yra padaroma autorius apžvelgs šiame poskyryje.

Saugumas. Naudojant blokų grandinės technologiją, saugumas pasiekiamas pakeičiant tradicinius centralizuotus serverius, dažnai talpinančius visą naudotojų asmeninę informaciją vienoje vietoje, decentralizuotu tinklu, kuris suteikia galimybę lengvai sukurti savarankišką suverenią tapatybės valdymo sistemą. Tai reiškia, kad asmeniniai naudotojų duomenys laikomi jų pačių įrenginiuose, taip ženkliai sumažinant duomenų vagysčių galimybes, kadangi norint pasinaudoti svetimais duomenimis nebeužtenka gauti prieigą prie vienos centrinės vietos, į kiekvieno asmens įrenginį turi būti įsilaužiama atskirai.

Privatumas. Naudotojų asmeninių duomenų privatumas blokų grandinės technologija grįstose sistemose užtikrinamas naudojantis nulinių žinių įrodymo metodu, garantuojančiu, jog trečiosioms šalims yra pateikiami tik konkrečiam tikslui, pašalinių detalių neatskleidžiantys, reikalingi duomenis. Taip pat suteikiama galimybė naudotojams sugeneruoti tiek skaitmeninėje piniginėje valdomų identifikatorių, kiek pats naudotojas galvoja, kad jam yra reikalinga, norint išskaidyti asmeninę informaciją, taip dar labiau padidinant saugomų asmeninių duomenų privatumą.

Duomenų prieinamumas. Duomenų prieinamumą užtikrina blokų grandinės technologijos savybės – decentralizacija ir skaitmeninė prieiga. Priešingai negu centralizuotose sistemose, duomenų kopijos saugomos daugybėje tinklo mazgų, todėl net ir sutrikus vieno ar kelių tinklo mazgų veiklai, saugomi duomenys ir toliau išlieka prieinami veikiančiuose tinklo mazguose. Taip pat dėl per nuotolį išduodamų ir patvirtinamų kredencialų suteikiama galimybė asmenims, iki šiol neturėjusiems galimybės, įrodyti savo asmens duomenų tikrumą

3.5.2. Trūkumai

Analizės metu pastebimi ir blokų grandinės technologijos pritaikymo asmeninių duomenų saugojimo ir valdymo trūkumai. Pirmiausia – blokų grandinės technologijos pritaikymas asmeninių duomenų sektoriuje pakankamai naujas sprendimas, todėl prireiks nemažai laiko tokias sistemas integruoti į visuomenę. Antra, šios technologijos veikimo principas paprastam žmogui gan sunkiai suprantamas, todėl tai gali pakenkti tokių sprendimų populiarumui. Trečia, naudojant egzistuojančius blokų grandinės tinklus, kuriuose veikia darbo įrodymo (PoW) algoritmas (pavyzdžiui „Bitcoin“, „Ethereum“), gali nukentėti sistemos plečiamumo galimybės didėjant naudotojų skaičiui.

3.6. Pritaikymo galimybės

Blokų grandinės technologija grįstos asmens duomenų saugojimo ir valdymo sistemos galėtų pakeisti tradicinius sprendimus ir būti plačiai pritaikytos pagerinant teigiamą naudotojo patirtį, neapsiribojant pateiktais pavyzdžiais:

- Internetiniai pirkimai. Kiekvieną kartą naudotojui pateikus užsakymą internetu, prašoma užpildyti konkrečią informaciją, pavyzdžiui: vardą, el. pašto adresą, telefono numerį, adresą ir t.t. Šis procesas dažnai kartojamas kiekvieno pirkimo metu ar naudojantis skirtingais paslaugos teikėjais. Naudojant blokų grandinės technologija grįstus sprendimus išvengiama šių procesų pakartotinio naudojimo. Naudotojas savo asmeninius duomenis gali saugoti ir saugiai pateikti tiesiai iš skaitmeninės piniginės esančios jo asmeniniame įrenginyje.
- Bankinis sektorius. Naudotojui norint pasinaudoti banke teikiamomis paslaugomis neretai reikia pateikti nemažai dokumentų, pavyzdžiui: pasas, pajamas patvirtinantys dokumentai ir t.t. Šių dokumentų patikrinimas užtrunka nemažai laiko, kuris kartais skaičiuojamas savaitėmis. Blokų grandinės technologija paremtas sprendimas galėtų šį laiką ženkliai sumažinti, kadangi visa informacija susijusi su dokumentų validumu gali iškarto būti patikrinta visuomet prieinamame decentralizuotame tinkle.
- Sveikatos paslaugos.

3.7. Pasiūlymai

Išanalizavus egzistuojančių blokų grandinės technologija grįstų sprendimų veikimo principus, privalumus ir trūkumus šiame poskyryje autorius pateikia asmeninius pasiūlymus kuriant tokias asmeninių duomenų saugojimo ir valdymo sistemas.

Blokų grandinės sprendimas tūrėtų naudoti nulinių žinių įrodymo metodą (ZKP). Asmeniniais duomenimis turi būti dalinamasi atskleidžiant kuo mažiau pašalinės asmeninės informacijos, taip užtikrinant duomenų privatumą. Pavyzdžiui lankantis kino teatre, kuriame taikoma studentų nuolaida, klientas vietoj studento pažymėjimo, kuriame šiuo konkrečiu atveju pateikiama perteklinė, paslaugos tiekėjui neaktuali informacija (vardas, pavardė, studijų programa), turėtų galimybę įrodyti studento statusą paprastu, universiteto patvirtintu/pasirašytu teiginiu – „Yra studentas“, kurio validumas gali būti patikrintas blokų grandinės tinkle suradus informaciją patvirtinusio universiteto viešąjį raktą ir įsitikinus parašo validumu. Panašūs teiginiai turėtų egzistuoti ir norint įrodyti savo amžių, pavyzdžiui – „Yra pilnametis“ arba „Yra vyresnis negu 21 metų“.

Jokia asmeninė informacija neturi būti tiesiogiai saugoma blokų grandinės tinkle, asmeniniai duomenys, išduoti kredencialai saugomi tik naudotojo asmeniniuose įrenginiuose, kaip pavyzdžiui mobilusis telefonas ir valdomi naudojant tam skirta saugią skaitmeninės piniginės programą. Taip užtikrinant, jog sukuriama savarankiška suvereni tapatybė – duomenų savininkas turi visiškai pilną jų kontrolę.

Autorius siūlo naudoti uždarą blokų grandinės tinklą, kuriame mazgus prižiūri patikimos institucijos ar organizacijos, tokios kaip bankai, vyriausybės ir t.t., taip sutaupoma energijos, greičiau įvykdomos transakcijos. Institucijos, kurioms patikėtas mazgų valdymas, turėtų būti reitinguojamos, pagal atliekamų veiksmų validumą, taip užtikrinant pasitikėjimą tinkle.

4. Blokų grandinės technologija grįsto sprendimo prototipas

Rašto darbe išanalizavus tradicinių asmens duomenų saugojimo sistemų keliamas problemas bei remiantis egzistuojančių blokų grandine grįstų sprendimų pavyzdžiais, autorius sukūrė tradicinių sistemų keliamas problemas sprendžiantį, blokų grandinės technologija grįstą galimo sprendimo prototipą. Viena pagrindinių sistemos dalių, kurios prototipą autorius plačiau aptars šiame skyriuje – mobilioji skaitmeninės piniginės aplikacija, kuri skirta patogiai ir saugiai valdyti saugomus asmeninius duomenis.

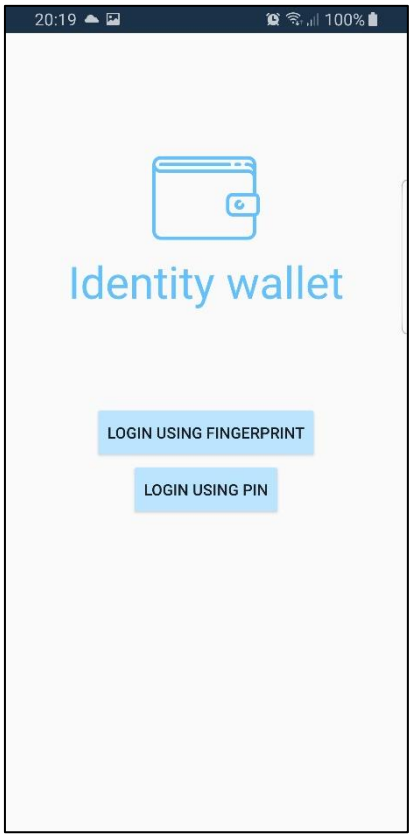
Autoriaus sukurtame programėlės prototipe įgyvendintos tokios funkcijos:

- Prisijungimas naudojant naudotojo sukurtą kodą arba biometrinius duomenis (žiūrėti 3 pav.).
- Registracija blokų grandinės tinkle. Pirmą kartą įsijungus mobiliąją skaitmeninės piniginės programėlę naudotojui sugeneruojama viešojo ir privataus raktų pora. Viešasis raktas patalpinamas blokų grandinės tinkle, kuriame jis susiejamas su decentralizuotu identifikatoriumi, kuris priskiriamas naudotojui.
- Sugeneruotos raktų poros automatinis valdymas. Mobiliosios aplikacijos prototipas naudotojui priskirtas raktų poras tvarko automatiškai, be naudotojo įsikyšimo, taip pagerinant naudotojo patirtį, bei sumažinant klaidos tikimybę.
- Kredencialų saugojimas. Visa naudotojo asmeninė informacija saugoma lokaliai pačiame įrenginyje, todėl jam suteikiama pilna asmeninių duomenų kontrolė. Naudotojo kredencialai, autoriaus sukurtame skaitmeninės piniginės prototipe, atvaizduojami sąrašo stiliumi, todėl informacija aiškiai suprantama, ja paprasta naudotis (žiūrėti 4 pav.).
- Kredencialų pateikimas QR kodu. Tam, kad skaitmenine pinigine būtų patogu naudotis, autorius įgyvendino informacijos pateikimo QR kodu funkcionalumą. Naudotojui paspaudus ant norimo panaudoti kredencialo skaitmeninėje pinginėje esančiame kredencialų sąraše (žiūrėti 4 pav.) sugeneruojamas QR kodas (žiūrėti 5 pav.), kuriame pateikiama su kredencialu susijusi informacija. Informacijos struktūros pavyzdys pateiktas JSON formatu (žiūrėti 2 pav.).

```
{
  "Owner": "did:pvz:asdfghjkl123456789own",
  "Sign": "awPgaegMRHAzorz93BOHn9dmodeA5hky3Qirm53U3lY1i99+L0EQjONQO1w0vlu18
    +g2Ddgk2okrgML/H+w0LGXCmg3YWVWs2240mQyS
    +tNFX66Fere7O5YSDcbqTIOTHaBKPsiyAfVTLRoeLRZ3COnafoDViH9vhUVmOg5ADrpn",
  "Credentials": [
    {
      "CredentialId": 1,
      "Timestamp": "1590403244",
      "Owner": "did:pvz:asdfghjkl123456789own",
      "Issuer": "did:pvz:asdfghjkl123456789iss",
      "Attribute": "IsStudent",
      "Value": "True",
      "Sign": "nprDA5gOmVUhv9HiVDofanOC3ZRLeoRLTVfAyisPKBaHTOITqbcDSY5O7ereF66XF
        Nt+SyQm0422sWVWY3gmCXGL0w+H/LMgrko2kgdD2g+81ulv0w1OQNOjQE0L
        +99i1Yl3U35mriQ3ykh5Aedomd9nHOB39zrozAHRnjJ17xc="
    }
  ]
}
```

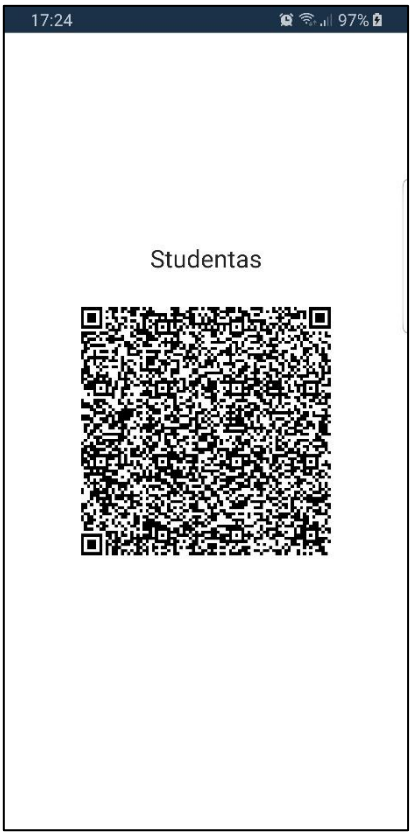

2 pav. QR kode pateikiamų duomenų struktūra

- QR kodo skenavimas. Funkcionalumas sukurtas patogiai nuskaityti kitų tinklo naudotojų pateiktus duomenis. QR kodo skenavimo funkcija naudotojas gali pasinaudoti paspaudęs pagrindinio lango apatiniame dešiniame kampe esantį mygtuką (žiūrėti 4 pav.)
- Kredencialų validumo patikrinimas naudojantis blokų grandinės tinkle saugoma informacija. Duomenų parašo patikrinimo metu blokų grandinės tinkle ieškomi reikalingi decentralizuoti identifikatoriai, su jais susiję viešieji raktai.



3 pav. Prisijungimo langas

4 pav. Pagrindinis langas



5 pav. Sugeneruotas QR kodas

Tam, kad autoriaus sistemos prototipas sėkmingai atliktu pagrindines asmeninių duomenų saugojimo, valdymo ir dalinimosi funkcijas, blokų grandinės tinkle turi būti saugoma tokia informacija:

- Decentralizuotas identifikatorius priskirtas tinklo naudotojui registracijos metu ir su identifikatoriumi susietas viešasis raktas. Saugomų duomenų struktūros pavyzdys JSON formatu (žiūrėti 6 pav.):

```
{
  "DID": "did:pvz:asdfghjkl123456789own",
  "PubKey": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
}
```

6 pav. DID ir viešojo rakto saugojimo struktūra

- Naudotojui išduotų ir jam priklausančių kredencialų identifikatoriai ir jų validumas. Autorius pasirinko tokį sprendimą, kadangi taip visiškai išvengiama asmeninių duomenų talpinimo blokų grandinės tinkle. Saugomų duomenų struktūros pavyzdys JSON formatu (žiūrėti 7 pav.):

```
{
  "CredentialId": 1,
  "Owner": "did:pvz:asdfghjkl123456789own",
  "Issuer": "did:pvz:asdfghjkl123456789iss",
  "Valid": true,
  "TimeStamp": "1590403244"
}
```


7 pav. Kredencialų validumo įrodymo struktūra

Rezultatai

Atlikus mokslinės literatūros ir egzistuojančių blokų grandinės technologija grįstų asmens duomenų saugojimo ir valdymo sprendimų analizę - pasiekti tokie rezultatai:

1. Skyriuje „Tradicinių sprendimų trūkumai“ argumentuotai pateikti šiuo metu egzistuojančių asmens duomenų saugojimo ir valdymo sprendimų esminiai trūkumai (saugumas, privatumas, prieinamumas), juos pagrindžiant realiai pavyzdžiais;
2. Poskyriuose „Blokų grandinės veikimo principas“, „Blokų grandinės struktūra“, „Blokų grandinės tinklų tipai“ išanalizuoti ir pateikti blokų grandinės technologijos veikimo principas, struktūra ir tipai. Poskyryje „Blokų grandinės panaudojimo galimybės“ apžvelgtos šios technologijos pritaikymo galimybės;
3. Skyriuje „Blokų grandinės pritaikymas kuriant asmeninių duomenų sistemas“ išanalizuotas blokų grandinės technologijos pritaikymas asmens duomenų saugojimo ir valdymo sistemoms kurti, pateikti privalumai ir trūkumai lyginant su tradiciniais sprendimais (žiūrėti 1 lentelėje);
4. Poskyriuose „Pritaikymo galimybės“ ir „Pasiūlymai“ nustatytos ir pateiktos blokų grandinių asmens duomenų saugojimo ir valdymo sistemų pritaikymo galimybės, autoriaus pasiūlymai tokių sistemų kūrimui;
5. Sukurtas ir skyriuje „Blokų grandinės technologija grįsto sprendimo prototipas“ aprašytas blokų grandinės technologija grįsto sprendimo prototipas;

Išvados

Atlikto darbo metu padarytos tokios išvados:

1. Šiuo metu naudojamų tradicinių asmens duomenų saugojimo ir valdymo sistemų analizės metu gauti rezultatai parodo, kad šios sistemos, kurios veikia centralizuotai, susiduria su tokiomis esminėmis problemomis:
    - Saugumo problema.
    - Privatumo problema.
    - Prieinamumo problema.
2. Tradicinėse asmens duomenų saugojimo ir valdymo sistemose kylančioms problemoms spręsti pradedamos kurti blokų grandinės technologija grįstos sistemos.
3. Blokų grandinės technologija grįstos asmens duomenų saugojimo ir valdymo sistemos prieš tradicines sistemas turi tiek privalumų, tiek trūkumų. Privalumai: pritaikant decentralizaciją, nulinių žinių įrodymo metodą, decentralizuotus identifikatorius sukuriama savarankiška suvereni tapatybės valdymo sistema. Todėl išsprendžiamos tradicinėse sistemose kylančios problemos. Trūkumai: blokų grandinės technologijos pritaikymas asmeninių duomenų sektoriuje pakankamai naujas sprendimas, todėl prireiks nemažai laiko tokias sistemas integruoti į visuomenę. Antra, šios technologijos veikimo principas paprastam žmogui gan sunkiai suprantamas, todėl tai gali pakenkti tokių sprendimų populiarumui. Trečia, naudojant egzistuojančius blokų grandinės tinklus, kuriuose veikia darbo įrodymo (PoW) algoritmas (pavyzdžiui „Bitcoin“, „Ethereum“), gali nukentėti sistemos plečiamumo galimybės didėjant naudotojų skaičiui.
4. Tai, jog blokų grandinės technologija grįstos asmeninių duomenų saugojimo ir valdymo sistemos ištaiso tradicinių sistemų trūkumus įrodo, jog atsižvelgiant į trūkumus toliau tobulinant ir plečiant blokų grandinės technologija grįstas asmeninių duomenų saugojimo ir valdymo sistemas, šios ateityje galės pakeisti šiuo metu įprastus, tradicinius sprendimus.

Šaltiniai

[AA19] Shikah J. Alsunaidi and Fahd A. Alhaidari, „A Survey of Consensus Algorithms for Blockchain Technology“, 2019 International Conference on Computer and Information Sciences (ICCIS), 2019,
[žiūrėta 2020-04-23]. Prieiga per internetą:
<https://ieeexplore.ieee.org/abstract/document/8716424 04-23>

[Ant17] Andreas M. Antonopoulos, „Mastering Bitcoin: Programming the Open Blockchain (O'Reilly 2nd edition)“, 2017, 197-231p.

[Ant18] Andreas M. Antonopoulos,, „Mastering Ethereum: Building Smart Contracts and DApps“, 2018, 127-131p.

[BBC19] BBC, „Facebook 'to be fined $5bn over Cambridge Analytica scandal'“, 2019,
[žiūrėta 2020-04-30]. Prieiga per internetą:
<https://www.bbc.com/news/world-us-canada-48972327>

[But14] Vitalik Buterin, „Ethereum White Paper A Next Generation Smart Contract & Decentralized Application Platform“, 2014,
[žiūrėta 2020-04-19]. Prieiga per internetą:
<https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf>

[But15] Vitalik Buterin, „On Public and Private Blockchains“, 2015,
[žiūrėta 2020-04-19]. Prieiga per internetą:
<https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>

[Dat19] Dataflair Team, “Types of Blockchains – Decide which one is better for your Investment Needs”, 2019,
[žiūrėta 2020-04-19]. Prieiga per internetą:
<https://data-flair.training/blogs/types-of-blockchain/>

[DJJ17] Uwe Der, Stefan Jähnichen, Jan Sürmeli, „Self-sovereign Identity – Opportunities and Challenges for the Digital Revolution“, 2017,

[žiūrėta 2020-04-30]. Prieiga per internetą:
<https://arxiv.org/ftp/arxiv/papers/1712/1712.01767.pdf>

[DP18] Paul Dunphy, Fabien A. P. Petitcolas, Innovation Centre, VASCO Data Security, „A First Look at Identity Management Schemes on the Blockchain“, 2018,
[žiūrėta 2020-05-05]. Prieiga per internetą:
https://arxiv.org/ftp/arxiv/papers/1801/1801.03294.pdf

[Dra19] Dragonchain, “What Different Types of Blockchains are There?”, 2019,
[žiūrėta 2020-04-19]. Prieiga per internetą:
<https://dragonchain.com/blog/differences-between-public-private-blockchains/>

[Dre17] Daniel Drescher, “Blockchain Basics: A Non-Technical Introduction in 25 Steps”, 2017, 72-73p.

[FLK19] Michael Friedewald, Eva Lievens, Stephan Krenn, Samuel Fricker, Melek Önen, „Privacy and Identity Management. Data for Better Living: AI and Privacy“, 2019, 453-454p.

[GR18] Julija Golosova, Andrejs Romanovs. „Overview of the Blockchain Technology Cases.“ 2018 59th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS).
[žiūrėta 2020-04-30]. Prieiga per internetą:
<https://ieeexplore.ieee.org/abstract/document/8552978>

[HGG20] Kim Hamilton-Duffy, Ryan Grant, Adrian Gropper, W3C, „Use Cases and Requirements for Decentralized Identifiers“, W3C Working Draft 25 April 2020,
[žiūrėta 2020-04-05]. Prieiga per internetą:
<https://www.w3.org/TR/did-use-cases/>

[Jac16] Jacobovitz, Ori. „Blockchain for identity management.“ The Lynne and William Frankel Center for Computer Science Department of Computer Science. Ben-Gurion University, Beer Sheva (2016),
[žiūrėta 2020-04-29]. Prieiga per internetą:
<https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf>

[Lau17] Tiana Laurence, „Blockchain For Dummies“, 2017, 10-11p.

[Lem17] Victoria L. Lemieux, „Blockchain and distributed ledgers as trusted recordkeeping systems.“, Future Technologies Conference *(FTC)*. Vol. 2017, [žiūrėta 2020-04-30]. Prieiga per internetą: <https://www.researchgate.net/profile/Victoria_Lemieux/publication/317433591_Blockchain_and_Distributed_Ledgers_as_Trusted_Recordkeeping_Systems_An_Archival_Theoretic_Evaluation_Framework/links/593aa6450f7e9b3317f4d860/Blockchain-and-Distributed-Ledgers-as-Trusted-Recordkeeping-Systems-An-Archival-Theoretic-Evaluation-Framework.pdf>

[LFA+18] Shu Yun Lim, Pascal Tankam Fotsing, Abdullah Almasri, Omar Musa, Miss Laiha Mat Kiah, Tan Fong Ang, Reza Ismail, „Blockchain technology the identity management and authentication service disruptor: a survey.“, International Journal on Advanced Science, Engineering and Information Technology , 2018, [žiūrėta 2020-04-30]. Prieiga per internetą: <https://www.researchgate.net/profile/Reza_Ismail4/publication/328919940_Blockchain_Technology_the_Identity_Management_and_Authentication_Service_Disruptor_A_Survey/links/5c0e5c89299bf139c74dddc2/Blockchain-Technology-the-Identity-Management-and-Authentication-Service-Disruptor-A-Survey.pdf>

[Met19] Metadium, “Decentralized Identifiers: the easy guide”, 2019, [žiūrėta 2020-05-01]. Prieiga per internetą: <https://medium.com/metadium/decentralized-identifiers-the-easy-guide-fb96429e8b24>

[Mih20] Carrie Mihalcik, „Marriott discloses new data breach impacting 5.2 million guests“, 2020, [žiūrėta 2020-04-30]. Prieiga per internetą: <https://www.cnet.com/news/marriott-discloses-new-data-breach-impacting-5-point-2-million-guests/>

[Nak08] Satoshi Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System“, 2008, [žiūrėta 2020-04-19]. Prieiga per internetą: <https://nakamotoinstitute.org/bitcoin/>

[PLS16] Bryan Pon, Chris Locke, Tom Steinberg, „Private-Sector Digital Identity in Emerging Markets“, United Kingdom: Caribou Digital Publishing, 2016, [žiūrėta 2020-05-05]. Prieiga per internetą: <https://www.cariboudigital.net/wp-content/uploads/2019/01/Caribou-Digitial-Omidyar-Network-Private-Sector-Digital-Identity-In-Emerging-Markets.pdf>

[RSS+20] Drummond Reed, Manu Sporny, Markus Sabadello, Dave Longley, Christopher Allen, W3C, „Decentralized Identifiers (DIDs) v1.0. Core architecture, data model, and representations“, W3C Working Draft 8 April 2020, [žiūrėta 2020-05-01]. Prieiga per internetą: <https://www.w3.org/TR/did-core/>

[SDP18] Bikramaditya Singhal, Gautam Dhameja, Priyansu Sekhar Panda, „Beginning Blockchain“, 2018, 131- 134p.

[Sha18] Toshendra Kumar Sharma, „How To Pick The Best Consensus Algorithm For Blockchain?“, 2018, [žiūrėta 2020-04-23]. Prieiga per internetą: <https://www.blockchain-council.org/blockchain/how-to-pick-the-best-consensus-algorithm-for-blockchain/>

[Sha19a] Toshendra Kumar Sharma, „Types Of Blockchain In The Market: Which One Is Better“, 2019, [žiūrėta 2020-04-18]. Prieiga per internetą: <https://www.blockchain-council.org/blockchain/types-of-blockchain-in-the-market-which-one-is-better/>

[Sha19b] Toshendra Kumar Sharma, „Top 10 Promising Blockchain Use Cases“, 2019, [žiūrėta 2020-04-30]. Prieiga per internetą: <https://www.blockchain-council.org/blockchain/top-10-promising-blockchain-use-cases/>

[Sil19] Jason Silverstein, „Hundreds of millions of Facebook user records were exposed on Amazon cloud server“, 2019, [žiūrėta 2020-04-30]. Prieiga per internetą:

<https://www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/>

[Sov18a] Sovrin, „Sovrin™: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust“, 2018,
[žiūrėta 2020-04-30]. Prieiga per internetą:
<https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf>

[Sov18b] Sovrin, „What is self-sovereign Identity?“, 2018,
[žiūrėta 2020-04-30]. Prieiga per internetą:
<https://sovrin.org/faq/what-is-self-sovereign-identity/>

[Tec19] TecraCoin, “What is Genesis Block and why Genesis Block is needed?”, 2019,
[žiūrėta 2020-04-21]. Prieiga per internetą:
<https://medium.com/@tecracoin/what-is-genesis-block-and-why-genesis-block-is-needed-1b37d4b75e43>

[Tyk19] Tykn, „Identity Management with Blockchain: The Definitive Guide“,
[žiūrėta 2020-04-29]. Prieiga per internetą:
<https://tykn.tech/identity-management-blockchain/>

[TR18] Andrew Tobin, Drummond Reed, „The Inevitable Rise of Self-Sovereign Identity“, 2018,
[žiūrėta 2020-05-01]. Prieiga per internetą:
<https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf>

[Win17] Van Wingerde, Marvin, „Blockchain-enabled self-sovereign identity“, Master’s thesis, Tilburg University, School of Economics and Management, 2017,
[žiūrėta 2020-04-30]. Prieiga per internetą:
<https://www.researchgate.net/profile/Marvin_Van_Wingerde2/publication/326914271_BLOCKCHAIN-ENABLED_SELF-SOVEREIGN_IDENTITY_An_exploratory_study_into_the_concept_Self-Sovereign_Identity_and_how_blockchain_technology_can_serve_the_fundamental_basis/links/5b6c10bb299bf14c6d97a85b/BLOCKCHAIN-ENABLED-SELF-

SOVEREIGN-IDENTITY-An-exploratory-study-into-the-concept-Self-Sovereign-Identity-and-how-blockchain-technology-can-serve-the-fundamental-basis.pdf>

[Win18] Phil Windley, „Verifiable Credential Exchange“, 2018, [žiūrėta 2020-05-01]. Prieiga per internetą: <https://www.windley.com/archives/2018/12/verifiable_credential_exchange.shtml>

[Win19] Phil Windley, „Decentralized Identifiers“, 2019, [žiūrėta 2020-05-01]. Prieiga per internetą: <https://www.windley.com/archives/2019/02/decentralized_identifiers.shtml>

[ZS18] Kaspars Zīle, Renāte Strazdiņa, „Blockchain use cases and their feasibility.“ Applied Computer Systems 23.1, 2018, [žiūrėta 2020-04-30]. Prieiga per internetą: <https://content.sciendo.com/view/journals/acss/23/1/article-p12.xml>

Santrumpos

SSI (angl. Self-sovereign identity) - Savarankiška suvereni tapatybė;

DID (angl. Decentralized Identifier) – decentralizuotas identifikatorius;

PoW (angl. Proof-of-Sork) – „darbo įrodymo“ algoritmas;

PoS (angl. Proof-of-Stake) – „turto įrodymo“ algoritmas;

ZKP (angl. Zero-Knowledge Proof) – nulinių žinių įrodymo metodas;

P2P (angl. Peer-to-Peer) – lygiarangių tinklų sistema;

DLT (angl. Distributed Ledger Technology) – paskirstytosios buhalterinės knygos technologija;

BTC – „Bitcoin“ valiuta;

ETH – „Ethereum“ valiuta;