**MYKOLO ROMERIO UNIVERSITETAS**
**VIEŠOJO VALDYMO IR VERSLO FAKULTETAS**

**Valdas Rupšys**

# Blokų grandinės sistemų vaidmuo viešojo valdymo kibernetinio saugumo sprendimų įgyvendinime

**Magistro baigiamasis darbas**

**Vadovas**
**prof. dr. Tadas Limba**

VILNIUS, 2022

**MYKOLO ROMERIO UNIVERSITETAS**

**VIEŠOJO VALDYMO IR VERSLO FAKULTETAS**

# Blokų grandinės sistemų vaidmuo viešojo valdymo kibernetinio saugumo sprendimų įgyvendinime

**Kibernetinio saugumo valdymo magistro baigiamasis darbas**

**Studijų programa 6211LX066**

**Konsultantas**

**_____**

**2022**

**Vadovas**

**_____ prof. dr. Tadas Limba**

**2022**

**Recenzentas**

**_____**

**2022**

**Atliko**

**KSVvmis20-1 gr. stud.**

**_____ V. Rupšys**

**2022**

VILNIUS, 2022

# LENTELĖS

1 lentelė. Blokų grandinės tipai ..... 11
2 lentelė. Projektų charakteristikos ..... 50
3 lentelė. Projektų funkcionalumai ..... 51
4 lentelė. Projektų valdymas ..... 52
5 lentelė. Pojektų naudojimas ..... 53
6 lentelė. Projektų techninė architektūra ..... 54
7 lentelė. Projektų sąnaudos ..... 55
8 lentelė. Projektų nauda ..... 57

# PAVEIKSLAI

1 pav. Darbo struktūros loginė schema ..... 8
2 pav. Blokų grandinės veikimo procesas ..... 9
3 pav. Blokų grandinės atributai ..... 10
4 pav. Žemės nuosavybės registracijos procesas, kurį naudoja NRA (Sakartvelas) ..... 28
5 pav. Nekilnojamojo turto nuosavybės perdavimo procesas „ChromaWay“ (Švedija) ..... 30
6 pav. Tapatybės registravimo procesas „uPort“ projekte (Šveicarija, Cugas) ..... 32
7 pav. „Pensijų infrastruktūros“ projektas (Nyderlandai) ..... 35
8 pav. Išmaniųjų kuponų sistema „Stadjerpas“ (Nyderlandai, Groningenas) ..... 37
9 pav. Sertifikatų patikrinimo procesas „Blockcerts“ projekte (Malta) ..... 39
10 pav. Ekspertų vertinimų standartinio nuokrypio priklausomybė nuo ekspertų skaičiaus ..... 42
11 pav. Blokų grandinės startuoliai, įkurti 2009-2018 metais ..... 43
12 pav. Blokų grandinės startuolių tendencijos ..... 44
13 pav. Blokų grandinės startuolių skaičius pagal sektorius ..... 44
14 pav. Blokų grandinės startuolių pasiskirstymas pagal sektorius ..... 45
15 pav. Pritrauktas finansavimas 2009 m. – 2018 m. ..... 46
16 pav. Pritrauktos investicijos naudojantis įvairiais finansavimo instrumentais ..... 47
17 pav. Investicijų pasiskirstymas pagal skirtingus finansavimo instrumentus ..... 47

# TURINYS

**ĮVADAS** ..... **6**
**1. BLOKŲ GRANDINĖS TEORINIAI ASPEKTAI** ..... **9**
1.1 Blokų grandinės raidos ir evoliucijos analizė ..... 9
1.2 Blokų grandinės savybės ir probleminiai aspektai ..... 12
1.3 Blokų grandinės lūkesčiai ir prognozės ..... 16
1.4 Blokų grandinės teorinės įžvalgos ..... 18
**2. BLOKŲ GRANDINĖS VAIDMUO SKAITMENINĖS VALDŽIOS KONTEKSTE** ..... **23**
2.1 Blokų grandinė Europos Sąjungos viešojo valdymo kontekste ..... 23
2.2 Blokų grandinės vaidmuo transformuojant viešojo sektoriaus valdymą ..... 27
**3. BLOKŲ GRANDINĖS TECHNOLOGIJA PAREMTŲ PROJEKTŲ EMPIRINĖ ANALIZĖ** ..... **41**
3.1 Empirinio tyrimo metodologija ..... 41
3.2 Tyrimo duomenų analizė ..... 42
3.3 Horizontalus tyrimo atvejų palyginimas ..... 49
3.4 Atvejų tyrimo įžvalgos ..... 58
**IŠVADOS IR PASIŪLYMAI** ..... **62**
**LITERATŪRA** ..... **64**
**ANOTACIJA** ..... **71**
**ANNOTATION** ..... **72**
**SANTRAUKA** ..... **73**
**SUMMARY** ..... **74**
**PRIEDAI** ..... **75**

# ĮVADAS

**Temos naujumas ir aktualumas.** Pastebima, kad vis daugiau dėmesio skiriama galimam blokų grandinės technologijos pritaikymui viešajame sektoriuje. Blokų grandinės sistemos gali tapti nauja informacine infrastruktūra, palaikančia keitimąsi informacija tarp viešojo administravimo institucijų, piliečių ir įmonių. Viešojo sektoriaus kontekste buvo identifikuotos decentralizuotos informacinės infrastruktūros naudojimo atvejų grupės (Kounelis, 2017 ir Grech & Camilleri, 2017), kuriose, tikimasi, blokų grandinės technologija sukels perversmą arba bent jau ženkliai palengvins įvairių valdžios paslaugų gavimą ir funkcijas. Tos grupės apima, bet neapsiriboja, įvairių civilinių įvykių įrašų teikimą, valstybės registrų tvarkymą, elektroninį balsavimą, ekonomines operacijas, reguliacinę rinkos priežiūrą, mokesčių administravimą (įskaitant kovą su sukčiavimu ir mokesčių slėpimu), viešųjų pinigų perskirstymą, socialines išmokas bei pensijas.

Skaitmeninė valdžia yra pažangi viešojo administravimo mokslo koncepcija, e-valdžios paradigmos tęsėja. Pastarasis modelis iš principo tik skaitmenizavo viešojo sektoriaus administravimą, tuo tarpu skaitmeninės valdžios koncepcija siūlo naujų viešųjų paslaugų ir tų paslaugų teikimo modelių sukūrimą. Naujoji paradigma orientuota į vartotoją, reaktyvumą ir novatorišką viešųjų paslaugų teikimą. Blokų grandinė yra viena inovatyviausių skaitmeninių technologijų, į kurią turi būti atkreiptas dėmesys siekiant įgyvendinti naują valdžios politikos formavimo ir paslaugų teikimo paradigmą.

Kibernetinio saugumo kontekste atkreiptinas dėmesys į tris blokų grandinės sistemų savybes: 1) decentralizuoti ir paskirstyti tinklai (kiekviename mazge laikomas pilnas operacijų apskaitos archyvas); 2) negrįžtamumas ir nekintamumas (blokų grandinėje operacijų neina pakeisti/ištrinti, tik įrašyti); 3) registro atnaujinimai tinkle beveik realiu laiku (Killmeyer et al, 2017). Šios trys savybės leidžia sandorius atlikti saugiai ir patikimai, kas yra svarbu institucijoms tvarkant asmens ar jautrius duomenis. Blokų grandinės technologija įgalina paprastą ir efektyvų apskaitos tvarkymo metodą, kuris užtikrina įrašų vientisumą, konfidencialumą ir pasiekiamumą (Martinovic, 2017).

**Teorinis reikšmingumas.** Blokų grandinės technologiją, jos pritaikymą skaitmeninės valdžios įgyvendinimui, vaidmenį kibernetinio saugumo kontekste tyrė daugelis mokslininkų, tokių kaip D.Allessie, M.Sobolewski, L.Vaccari, F.Pignatelli, A.Anderberg, E.Andonova, M.Bellia, L.Cales, A.Inamorato dos Santos, I.Kounelis, I.Nai Fovino, M.Petracco Giudici, E.Papanagiotou, M.Sobolewski, F.Rossetti, L.Spirito, C.G.Reddicka, G.Purón Cidb ir S.Ganapati (2019), tačiau vis dar nepakankamai įvertintas blokų grandinės vaidmuo priimant kibernetinio saugumo sprendimus viešojo sektoriaus skaitmeninės valdžios įgyvendinime, nepakankamai atlikta empirinių tyrimų.

**Mokslinė problema.** Kaip blokų grandinės sistemų naudojimas keičia viešojo sektoriaus kibernetinio saugumo paradigmą?

**Darbo objektas:** blokų grandinės sistemos kibernetinio saugumo kontekste.

**Darbo dalykas:** blokų grandinės sistemų pritaikymas Europos šalių viešajame sektoriuje.

**Darbo tikslas:** ištirti blokų grandinės technologijos vaidmenį Europos šalių viešajame sektoriuje įgyvendinant skaitmeninės valdžios koncepciją kibernetinio saugumo aspektu, pateikti su šia sritimi susijusias rekomendacijas.

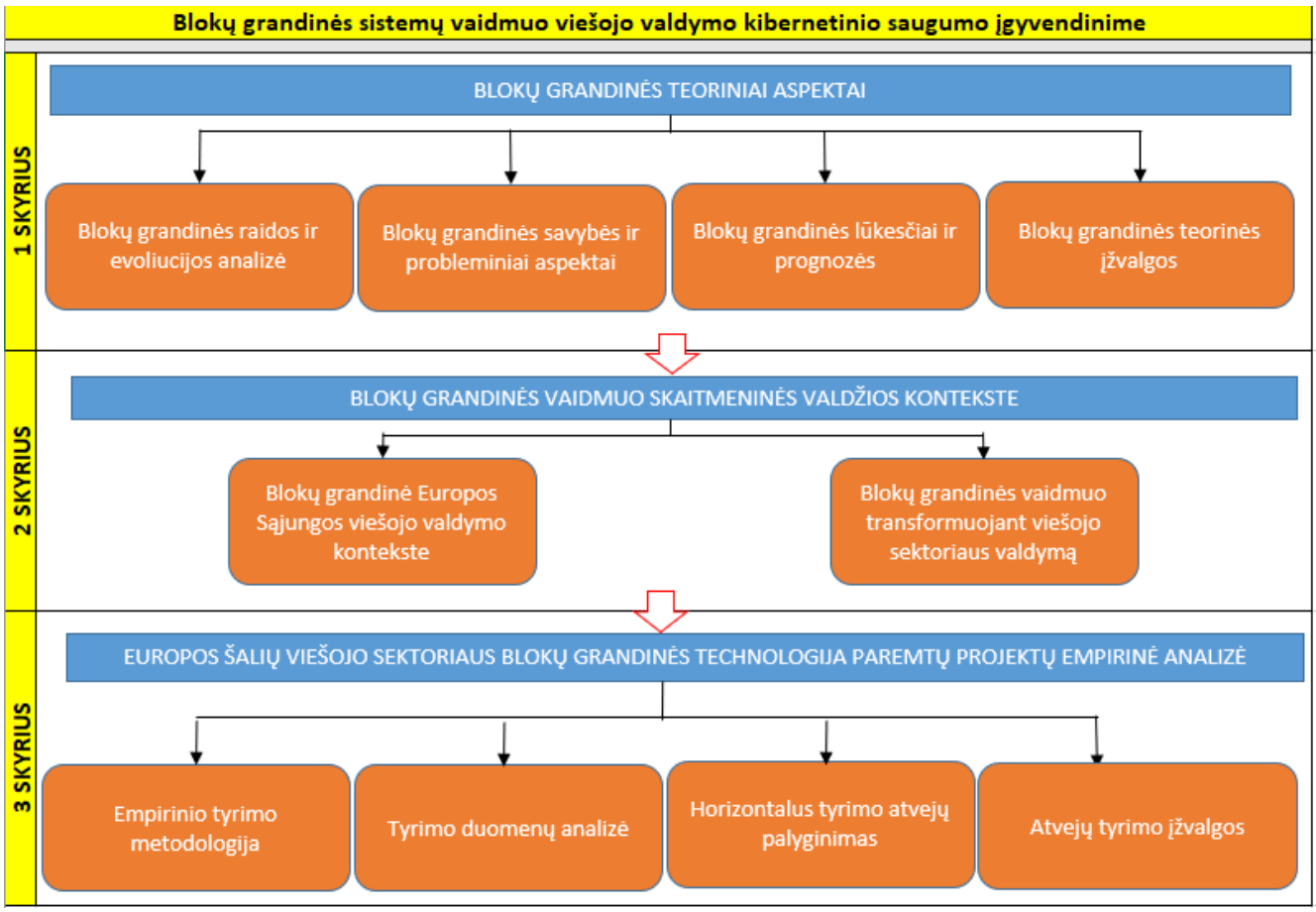
**Darbo uždaviniai:**

1. Aptarti blokų grandinės teorinį konceptą kibernetinio saugumo kontekste.
2. Įvertinti blokų grandinės sistemų vaidmenį ir pritaikymo galimybes viešojo sektoriaus perspektyvoje.
3. Išanalizuoti blokų grandinės naudojimą Europos šalių viešajame sektoriuje.

**Duomenų rinkimo šaltiniai ir analizės metodai.** Buvo remtasi mokslinės literatūros ir atvejo analize, atlikta ekspertų apklausa. Atliktos teorinė, lyginamoji, kokybinė turinio analizės bei daugybinių atvejų studija. Ekspertų nuomonė sužinota struktūruoto interviu forma. Mokslinės literatūros analizė taikyta siekiant išanalizuoti blokų grandinės teorinius aspektus per kibernetinio saugumo prizmę. Remiantis atvejo analizės metodu, siekta išanalizuoti blokų grandinės technologija paremtų projektų teikiamą naudą viešojo sektoriaus valdymui. Atliktas kokybinis 7 ekspertų nuomonės tyrimas, kuriuo siekta išsiaiškinti blokų grandinės naudojimo mastą bei ja paremtų projektų teikiamą naudą ir kuriamą pridėtinę vertę; pagrindines problemas, atsirandančias diegiant blokų grandinės projektus; išskirti kokybiškus blokų grandine paremtų projektų pavyzdžius.

**Darbo struktūra.** Magistro baigiamąjį darbą sudaro 3 dalys (žr. 1 pav.). Pirmoje dalyje analizuojami teoriniai blokų grandinės aspektai tokie kaip decentralizacija, skaidrumas, saugumas ir išmaniosios sutartys, taip pat apžvelgiami lūkesčiai, prognozės bei pateikiamos įžvalgos. Antroje dalyje nagrinėjama blokų grandinė skaitmeninės valdžios kontekste ES politikos lygmeniu bei viešojo sektoriaus valdymo transformacijos. Trečioje dalyje pateikiamas Europos šalių viešojo sektoriaus blokų grandinės technologija paremtų projektų empirinis tyrimas apžvelgiant technologijos naudojimą pasaulio ir Europos mastu bei atliekant horizontalų atrinktų projektų palyginimą, tokiu būdu įvertinant blokų grandinės vaidmenį transformuojant viešąjį sektorių. Darbo pabaigoje pateikiamos išvados ir pasiūlymai.

**Darbo praktinis reikšmingumas** pasireiškia išanalizuotais svarbiausiais blokų grandine paremtų projektų kokybiniais kriterijais, išskirta geraja praktika. Šia informacija galima pasinaudoti diegiant į kibernetinio saugumo bei efektyvumo gerinimą orientuotus blokų grandinės technologija paremtus projektus viešajame sektoriuje. Blokų grandine paremti projektai, diegiami viešajame sektoriuje su orientacija į kibernetinį saugumą bei efektyvumą yra mažai tyrinėta sritis, todėl gauti rezultatai gali būti pagrindas šios naujos srities plėtrai.




**1 pav. Darbo struktūros loginė schema**

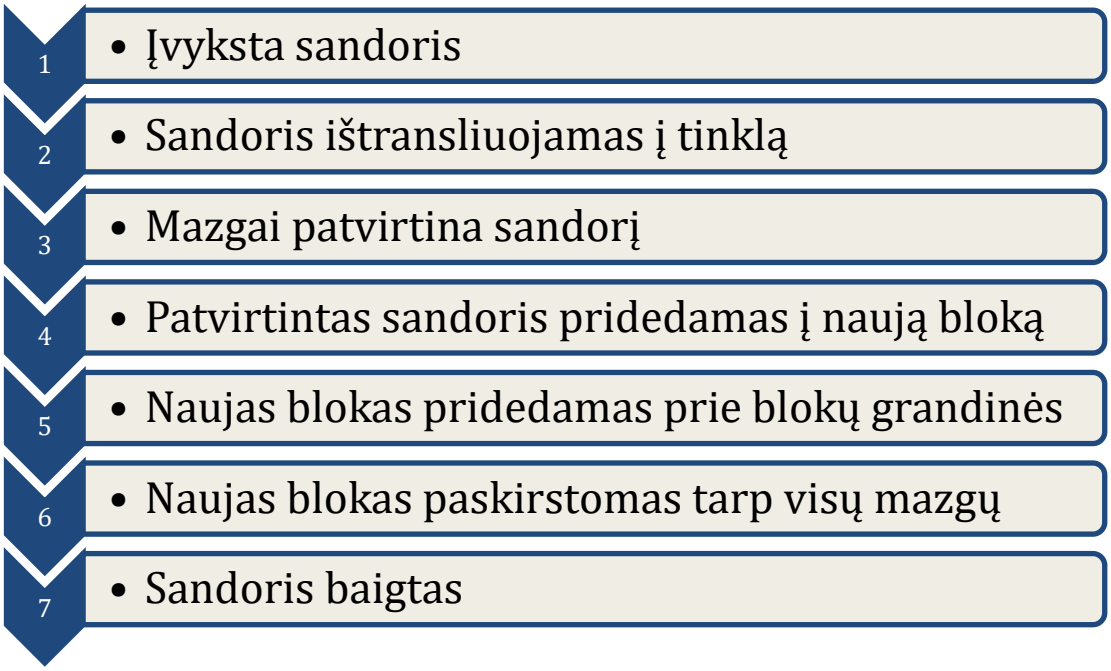
# 1. BLOKŲ GRANDINĖS TEORINIAI ASPEKTAI

## 1.1 Blokų grandinės raidos ir evoliucijos analizė

Blokų grandinė ir kitos paskirstytojo registro technologijos (PRT) - tai technologijos, leidžiančios patikimai keistis bet kokio tipo skaitmeniniais duomenimis lygiarangiu pagrindu, kai trečiųjų šalių ar tarpininkų yra mažiau arba jų iš viso nėra. Duomenys gali būti pinigai, draudimo polisai, sutartys, žemės nuosavybės teisės, medicininiai įrašai, gimimo ir santuokos liudijimai, prekių ir paslaugų pirkimas ir pardavimas arba bet kokio kito tipo sandoriai ar turtas, kurį galima paversti skaitmenine forma.

Blokų grandinė yra tik viena platesnės PRT šeimos dalis. PRT yra tam tikros duomenų bazių rūšys, kuriose duomenys įrašomi, jais dalijamasi ir jie sinchronizuojami paskirstytame kompiuterių ar dalyvių tinkle. Blokų grandinės technologija yra PRT pogrupis, kuriame naudojami kriptografiniai metodai duomenims įrašyti ir sinchronizuoti "blokų grandinėse". Kitaip tariant, visos blokų grandinės rūšys yra PRT, bet ne visos PRT yra blokų grandinės.

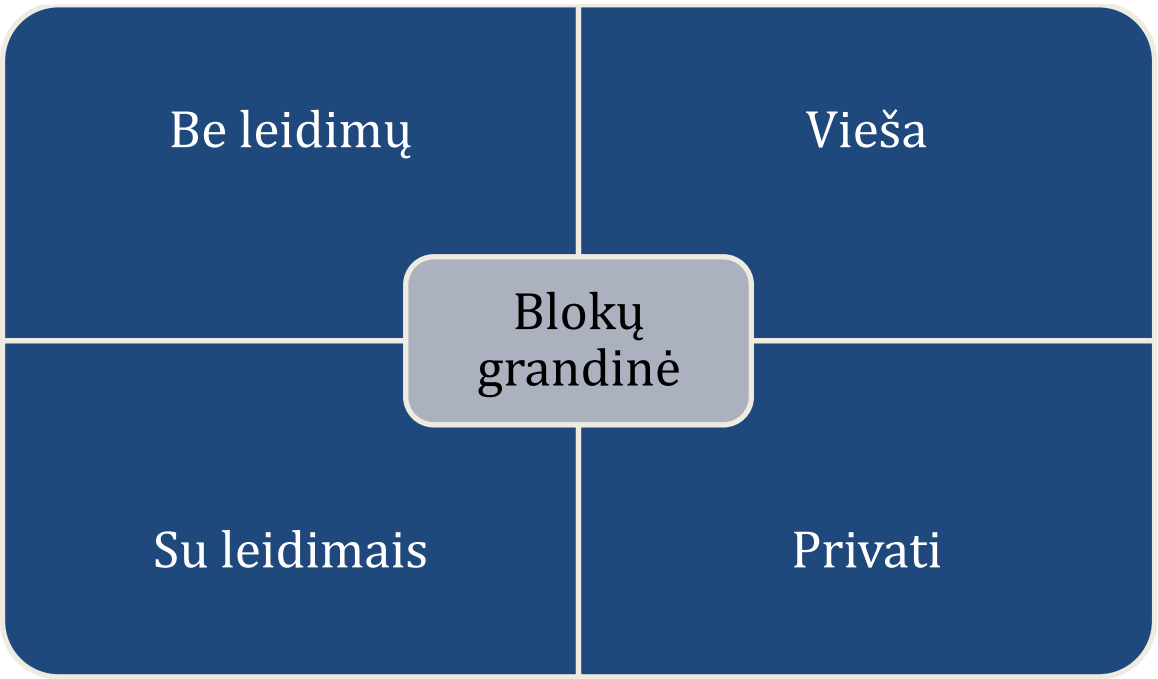
Blokų grandinė - tai duomenų bazė (registras), veikianti paskirstytame kelių mazgų arba kompiuterių tinkle, kuriame registruojami duomenų sandoriai (Wright ir De Filippi, 2015). Ji taip vadinama dėl ypatingo sandorių registravimo ir tikrinimo tarp šalių būdo (žr. 2 pav.). Šalis A prašo sandorio su šalimi B (pvz. pervesti pinigus, sudaryti sutartį arba dalytis įrašais). Šis sandoris perduodamas paskirstytam mazgų arba kompiuterių tinklui, kuris jį patvirtina pagal sutartą taisyklių rinkinį (konsensuso mechanizmą). Kai sandoris patvirtinamas, jis, kartu su kitais sandoriais, sujungiamas į naują "bloką" ir įtraukiamas į blokų grandinę.




**2 pav. Blokų grandinės veikimo procesas**

Visas procesas užtikrina, kad kiekvienas blokas būtų sukurtas taip, kad nenuginčijamai susietų jį su ankstesniuoju ir kitu bloku, taip sudarant blokų grandinę. Kiekvienas tinklo mazgas ar kompiuteris dalijasi unikaliu įrašu, sudarančiu blokų grandinę, jis nuolat atnaujinamas ir sinchronizuojamas. Tokiu būdu blokų grandinėje, tarsi duomenų bazėje arba registre, saugomi visų kada nors tinkle įvykdytų sandorių įrašai.

Egzistuoja daugybė skirtingų blokų grandinių su skirtingomis funkcijomis ir architektūromis. Jas galima išskirti pagal tai, kas gali skaityti, vykdyti ir tvirtinti sandorius. Kai blokų grandinę gali skaityti ir prie jos prisijungti bet kas, ji priskiriama "viešajai" arba "atvirai" kategorijai. Kai prieigą turi tik įgalioti subjektai, blokų grandinė laikoma "uždara" arba "privačia" (žr. 3 pav.).

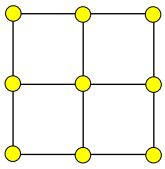
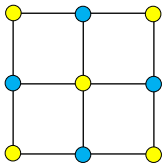
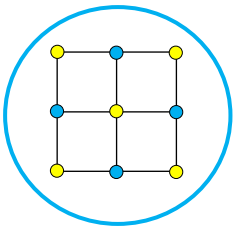
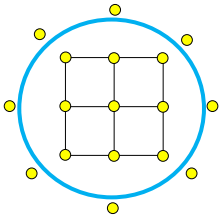



**3 pav. Blokų grandinės atributai**

Blokų grandinės gali būti skirstomos į "be leidimo" (angl. permissionless) arba "su leidimu" (angl. “permissioned”), priklausomai nuo to, kas gali siųsti sandorius ir kas gali juos patvirtinti. Jei sandorius gali siųsti ir tvirtinti bet kas, tokia blokų grandinė vadinama be leidimų. Jei tik autorizuoti dalyviai yra įgalioti vykdyti arba tvirtinti sandorius, arba ir viena, ir kita, tokia blokų grandinė vadinama su leidimais. Taip pat yra hibridinių blokų grandinių, kuriose derinami skirtingi aspektai (Peters ir Panayi, 2016; Danezis ir Meiklejohn, 2015).

Galima išskirti keturis pagrindinius blokų grandinių tipus: viešosios be leidimo, viešosios su leidimu, privačios su leidimu ir privačios be leidimo blokų grandinės (žr. 1 lentelę).

**1 lentelė. Blokų grandinės tipai**

| Blokų grandinės tipas | Paaiškinimas | Pavyzdys | Vizualizacija |
|---|---|---|---|
| Viešos blokų grandinės be leidimų | Šiose blokų grandinės sistemose bet kas gali dalyvauti blokų grandinės konsensuso mechanizme. Taip pat visi turintys interneto ryšį iš bet kurios pasaulio vietos gali sudaryti sandorius bei matyti visą jų žurnalą. | Bitcoin, Litecoin, Ethereum |  |
| Viešos blokų grandinės su leidimais | Šios blokų grandinės sistemos leidžia visiems turintiems interneto ryšį sudaryti sandorius ir matyti sandorių žurnalą, tačiau konsensuso mechanizme dalyvauja tik ribotas mazgų skaičius. | Ripple, privačios Ethereum versijos |  |
| Privačios blokų grandinės su leidimais | Šios blokų grandinės sistemos leidžia sudaryti sandorius bei žiūrėti sandorių žurnalą tik sistemoje dalyvaujantiems mazgams. Sistemos architektas arba savininkas sprendžia, kas gali dalyvauti sistemoje bei kurie mazgai gali dalyvauti konsensuso mechanizme. | Rubix, Hyperledger |  |
| Privačios blokų grandinės be leidimų | Šios blokų grandinės sistemos riboja kas gali sudaryti sandorius bei peržiūrėti sandorių žurnalą, tačiau konsensuso mechanizmas atviras visiems. | Exonum (dalinai) |  |

Geltoni taškai yra patvirtinantys mazgai, t. y. jie gali patvirtinti sandorius ir dalyvauti konsensuso mechanizme. Šviesiai mėlyni taškai yra tinklo dalyviai ta prasme, kad jie gali sudaryti sandorius, bet negali dalyvauti patvirtinimo mechanizme. Šviesiai mėlyni taškai nedalyvauja konsensuso mechanizme. Šviesiai mėlynas apskritimas reiškia, kad sandorių istoriją gali matyti tik apskritimo viduje esantys mazgai. Iliustracijos be apskritimo reiškia, kad visi, turintys interneto ryšį, gali matyti blokų grandinės sandorių istoriją.

## 1.2 Blokų grandinės savybės ir probleminiai aspektai

Blokų grandinės potencialas grindžiamas tam tikru pagrindinių savybių ir su jomis susijusių iššūkių deriniu: decentralizacija, atsparumu klastojimui, skaidrumu, saugumu, išmaniosiomis sutartimis (Tasca ir Tessone, 2018; Rauchs ir kt., 2018).

### 1.2.1 Decentralizacija

Blokų grandinė veikia per paskirstytą dalyvių tinklą. Todėl blokų grandinės (bent iš dalies) pakeičia kitus tarpininkus ar trečiąsias šalis, nuo kurių paprastai priklauso sandoriai. Vietoj to, pasitikėjimas tarp dalyvių užtikrinamas remiantis taisyklių rinkiniu, vadinamu konsensuso mechanizmu, kurio visi laikosi tikrindami, patvirtindami ir įtraukdami sandorius į blokų grandinę. Geriausiai žinomas konsensuso mechanizmas yra "darbo įrodymas" (angl. proof of work, PoW), kuris remiasi mazgų arba kompiuterių (vadinamų "kalnakasiais", angl. miners) skaičiavimo arba apdorojimo galia.

Tai, kad nėra centrinio subjekto, kontroliuojančio sistemą, blokų grandinių sistemoms suteikia didelį atsparumą. Nesant vieno gedimo taško (angl. single point of failure), sistemos beveik neįmanoma sukompromituoti, nes dėl didelio paskirstytų mazgų kiekio labai sunku vienu metu atakuoti visą tinklą.

Tačiau blokų grandinės turi apribojimų, susijusių su išplečiamumu ir našumu. Viešoji ir leidimo nereikalaujanti blokų grandinė gali apdoroti tik ribotą skaičių sandorių. Tačiau šią išplečiamumo problemą bando spręsti kiti už grandinės ribų esantys sprendimai. Darbo įrodymo procesas taip pat reiškia dideles energijos sąnaudas, nors dėl faktinių "Bitcoin" elektros energijos sąnaudų nėra sutarimo (Mccook, 2018; Mora et al., 2018; New York Times, 2018). Šiuo metu kuriami alternatyvūs sutarimo mechanizmai, pavyzdžiui, turimos dalies įrodymas (angl. proof of stake, PoS) ir kiti, kurie yra mažiau imlūs energijai.

Naujausi tyrimai rodo, kad blokų grandinių pasaulyje decentralizacijos teorija ne visada atitinka realybę. Duomenys apie didelę gavybos koncentraciją ar priklausomybę nuo riboto dalyvių skaičiaus (Gencer et al., 2018) arba didelio masto gavybos veiklos telkinius (Caccioli et al., 2016) rodo, kad tik nedaugelis blokų grandinės sistemų iš tikrųjų yra decentralizuotos. Tokios situacijos gali sudaryti sąlygas galimiems sąmokslams arba grupės dalyvių atakoms kontroliuojant didžiąją dalį skaičiavimo išteklių, dar kitaip vadinamoji "51% ataka".

Susirūpinimą dėl centralizacijos kelia ir privačios bei leidimų reikalaujančios blokų grandinės. Šiose sistemose dalyvių grupė, įmonės ar administratoriai iš anksto atrenka dalyvius arba suteikia jiems prieigą. Tai galima laikyti centralizuotu arba pusiau centralizuotu modeliu, kai dalyvių grupė išlaiko didelę kontrolę, dėl kurios gali būti priimami savavališki sprendimai ir patiriamos didelės sąnaudos, kaip šiandien vyksta kitose ne blokų grandinės sistemose (Crespigny, 2018).

### 1.2.2 Atsparumas klastojimui

Kita svarbi blokų grandinių savybė yra ta, kad jas labai sunku pakeisti ar ištrinti sandorių įrašus- tai įmanoma tik per "51 % ataką" arba bendru tinklo dalyvių sutarimu. Kiekvienas pakeitimas blokų grandinėje yra matomas visiems, todėl beveik neįmanoma padaryti pakeitimų, kad kas nors jų nepastebėtų. Viešieji ir privatieji raktai arba kriptografiniai parašai taip pat užtikrina sandorių vientisumą ir autentiškumą.

Šia prasme blokų grandinės įrašai yra atsparūs klastojimui. Neatšaukiamumo ir neklastojamumo savybės užtikrina, kad blokų grandinėje yra unikali įrašų versija, kuria gali dalytis visi grandinės dalyviai.

Vienas iš labiausiai diskutuotinų klausimų yra susijęs su galimais konfliktais tarp blokų grandinės ir Europos Sąjungos (ES) Bendrojo duomenų apsaugos reglamento (BDAR) teisės į duomenų ištrynimą, geriausiai žinomos kaip "teisė būti pamirštam" (Finck, 2018). Potencialus poreikis nustatyti ir susisiekti su visais reikiamais mazgais su prašymu ištrinti ar net ištaisyti duomenis ("teisė į pakeitimą") gali būti realiai neįgyvendinamas. Be to, bet kokie pakeitimai nuo klastojimo apsaugotoje duomenų bazėje gali pakirsti dalyvių pasitikėjimą pačia blokų grandine ir sukelti įtarimų dėl klastojimo ir kišimosi.

Svarbu pažymėti, kad atsparumas klastojimui nėra tas pats, kas "nekintamas" ar "nekeičiamas".

Nepaisant jos decentralizuoto pobūdžio, ši technologija vis tiek yra pažeidžiama grėsmių ir atakų, kurios hipotetiškai gali leisti atskiriems asmenims ar grupėms pakeisti įrašus ar pakeisti sandorius. Be to, priklausomai nuo taikomo konsensuso mechanizmo, blokų grandinės dalyviai iš tikrųjų gali balsuoti arba nuspręsti atlikti pakeitimus ar pakeisti įrašą (Coindesk, 2016; Quartz, 2016). Tai reiškia, kad atsparumas klastojimui turėtų būti suprantamas ne kaip “nepakeičiamas”, o kaip “sunkiai pakeičiamas” (Walch, 2017).

Neilgoje blokų grandinės gyvavimo istorijoje jau yra registruota sandorių įrašų arba tiesiog blokų grandinės keitimo konsensuso būdu atvejų. Vienas prieštaringiausių tokių buvo "DAO įsilaužimas", kai lėšų vagystė buvo atkurta bendruomenei priėmus sprendimą padalyti arba "šakoti" (angl. fork) pagrindinį įrašą. Šis atvejis sukėlė plačias diskusijas, ką reiškia pasitikėjimas blokų grandinės sistemose. Jis atskleidė valdymo svarbą, nes galiausiai blokų grandinės vis dar priklauso nuo tam tikro subjektų (kūrėjų, kalnakasių, naudotojų ir kitų dalyvių) rinkinio, kurie turi konkrečius vaidmenis ir gali įsikišti tam tikrais momentais, kai suvokiama (arba reikalaujama pagal įstatymus), kad būtų išspręstos problemos, atnaujinta sistema arba atšauktos nenumatytos pasekmės.

### 1.2.3 Skaidrumas

Registras arba blokų grandinė yra prieinama visiems dalyviams arba iš anksto nustatytam dalyvių rinkiniui. Privačiose arba uždarose blokų grandinėse prieiga prie įrašų gali būti ribojama tik tam tikriems

dalyviams, o viešosiose arba atvirosiose blokų grandinėse visi, turintys interneto ryšį su tinklu, turi tas pačias teises pasiekti ir (arba) atnaujinti registrą pagal taikomą konsensuso mechanizmą. Taigi visi sandoriai viešosiose arba atvirosiose blokų grandinėse yra skaidrūs ir matomi, o tai didina audito galimybes ir pasitikėjimą tinklu.

Tačiau dėl skaidrių duomenų viešojoje blokų grandinėje gali kilti problemų, kai tam tikra informacija neturi būti viešai prieinama arba ją vėliau tenka keisti dėl klaidų, netikslumų ar kitų duomenų įvedimo problemų (Finck, 2017; Hogan Lovells, 2017). Šiuo metu tai yra vienas iš labiausiai ginčytinų klausimų - vis dar neišspręstas skaidrumo ir privatumo kompromisas viešosiose arba atvirosiose blokų grandinėse.

Galimas sprendimas - konfidencialius, neskelbtinus ar asmeninius duomenis saugoti "ne grandinėje" arba kitose duomenų bazėse. Tai taip pat gali būti galimybė saugoti didesnius duomenų rinkinius, atsižvelgiant į daugumos blokų grandinių plėtros apribojimus. Šie duomenys būtų susieti su blokų grandine per maišos (angl. hash) nuorodą arba rodyklę, išlaikant prieigą prie originalių duomenų kitoje duomenų bazėje tik įgaliotoms šalims, arba naudojant blokų grandinės platformą su integruota už grandinės ribų esančia decentralizuota duomenų baze. Kita galimybė - naudoti hibridinę arba privačią blokų grandinę, kurios suteikia daugiau lankstumo konfigūruojant skirtingus prieigos prie asmeninės, neskelbtinos ar privačios informacijos lygius pagal individualų poreikį.

Kriptografiniai protokolai suteikia pseudoanonimiškumą, o ne visišką anonimiškumą (Van Wirdum, 2015). Viena vertus, sandoriai nesusiję su realiomis tapatybėmis ir yra atsitiktinai perduodami per lygiarangį tinklą (pvz. bet kas gali perduoti bitkoinus kitiems naudodamasis privačiais raktais be jokios asmeninės informacijos), kita vertus, sandoriai vis tiek gali būti deanonimizuojami taikant įvairius metodus, kurių pagalba gali būti nustatyta konkrečių duomenų subjektų tapatybė (Goldfeder et al., 2017; Coincenter, 2015).

Įvairiais eksperimentais ir moksliniais tyrimais bandoma spręsti minėtas problemas naudojant kriptografinius protokolus, kaip pavyzdžiui "nulinio žinojimo įrodymas", kurie gali būti papildomais šifravimo sluoksniais, siekiant užtikrinti sandorių privatumą. Jei blokų grandinės sistemos būtų tinkamai suprojektuotos pagal organizacijų poreikius, jomis potencialiai netgi būtų galima priimti decentralizuotus ir privatumą užtikrinančius sprendimus.

### 1.2.4 Saugumas

Vienas iš pagrindinių blokų grandinės privalumų - saugiai sekti ir tikrinti informaciją. Visi sandoriai žymimi laiko žymomis, t. y. tokie duomenys, kaip informacija apie mokėjimą, sutartį, nuosavybės perleidimą ir panašiai yra viešai susieti su tam tikra data ir laiku. Tai reiškia, kad niekas neturėtų galėti pakeisti to, kas buvo užregistruota ir pažymėta laiko žyma. Dėl to ypač naudinga

įvairioms šalims patikrinti, kada ir kas atliko konkretų sandorį, arba patvirtinti, kad duomenys egzistavo tam tikru laiko momentu.

Blokų grandinė remiasi viešojo ir privataus rakto kriptografija, kad būtų užtikrintas autentiškumas bei duomenų mainų ar sandorių vientisumas. Dalyviai turi atskirą tapatybę, pagrįstą viešųjų ir privačiųjų raktų deriniu: viešaisiais raktais plačiai dalijamasi su kitais tinklo dalyviais, o privatieji raktai laikomi paslaptyje. Pavyzdžiui, privačiu raktu užšifruotus pranešimus ar sandorius gali atidaryti tik gavėjai, turintys atitinkamą viešąjį raktą (kuriuo dalijasi siuntėjas). Arba, jei pranešimas užšifruotas viešuoju raktu, jį iššifruoti gali tik nurodytas gavėjas, naudodamas savo privatųjį raktą, tačiau tokioje sistemoje iškyla kita kibernetinio saugumo rizika- pats raktų valdymas (ENISA, 2016).

Elgdamiesi neatsargiai blokų grandinės dalyviai savo viešuosius ir privačiuosius raktus gali lengvai prarasti, lygiai taip pat kaip telefoną ar atsarginę duomenų kopiją (Wired, 2017a; Wired, 2017b). Daugelis žmonių pasikliauja trečiosiomis šalimis valdant savo raktus, tačiau tai sukelia papildomą riziką, jei į šias bendroves įsilaužiama (Fortune, 2017).

Dar niekam nepavyko įveikti viešųjų blokų grandinių kriptografijos ir decentralizuotos architektūros, nors kai kas teigia, kad tai gali pavykti su kvantine kompiuterija (Forbes, 2017b).

Kvantine informacija pagrįstos technologijos neabejotinai taps skaitmenine revoliucija, nes numatoma įspūdinga kvantinių kompiuterių skaičiavimo galia ir "neišsprendžiamų problemų" sprendimai gali būti lengvai rasti, tačiau kol kas kvantiniai skaičiavimai nėra pakankamai galingi grasinti blokų grandinės saugumui. Nėra ir aiškaus sutarimo, kada tai gali įvykti. Europos Komisijos Generalinio direktorato Jungtinio tyrimų centro apklausoje dėl kvantinių technologijų (Lewis et al., 2018 m.) pateikiamas vidutinis įvertis - 15 metų plius/minus 11,5 metų.

Todėl blokų grandinės bendruomenė turi būti aktyvi ir jau dabar ruoštis kitai kartai, kuri turi būti atspari kvantams. Akivaizdu, kad kvantinės kompiuterijos atsiradimas turės įtakos ne tik blokų grandinėms, bet ir visoms sistemoms, kurios remiasi susilpnėjusiais kriptografiniais algoritmais. Todėl jau dabar kuriamos naujos kartos kriptosistemos, paprastai vadinamos postkvantiniais kriptografiniais algoritmais, kurios gali būti naudingos naujos kartos kvantams atspariems registrams. Panašiai nereikėtų ignoruoti ir kitų naujųjų kvantinių technologijų (pavyzdžiui, kvantinių raktų paskirstymo protokolų) privalumų, nes tai taip pat gali padėti padidinti blokų grandinės sistemų saugumą.

### 1.2.5 Išmaniosios sutartys

Blokų grandinės technologija gali būti naudojama ne tik valiutos sandoriams, bet ir kitoms decentralizuotoms paslaugoms įgyvendinti. Viena iš pagrindinių priežasčių yra papildomos funkcijos, kurias galima įdiegti blokų grandinėje. Bene svarbiausia iš jų - išmaniųjų sutarčių naudojimas.

Išmaniosios sutartys - tai kompiuterinės programos, galinčios vykdyti šalių susitarimo sąlygas be žmogaus koordinavimo ar įsikišimo (Szabo, 1997; Buterin, 2015). Šie susitarimai gali būti įrašyti ir patvirtinti blokų grandinėje, kuri vėliau gali automatiškai vykdyti ir užtikrinti sutarties vykdymą, paprastai pagal "jei - tai" instrukcijas: “Jei" kažkas atsitinka (pavyzdžiui, jei išsinuomojate automobilį ir sumokate už jo trumpalaikį draudimą), "tada" atliekamos tam tikros operacijos arba veiksmai (automobilio durelės atsirakina ir pervedamas mokėjimas). Išmanioji sutartis suteikia galimybę dviem ar daugiau šalių atlikti patikimą sandorį be tarpininkų. Būdas, kuriuo sandoriai tikrinami ir įtraukiami į blokų grandinę, garantuoja, kad konfliktai ar netikslumai bus suderinti ir kad galiausiai bus tik vienas galiojantis sandoris (nebus dvigubų įrašų).

Išmaniosios sutartys išpopuliarėjo su "Ethereum" kriptovaliuta, kurioje naudojama atvirojo kodo "Ethereum Virtual Machine" (EVM) blokų grandine pagrįsta paskirstytųjų skaičiavimų platforma. Pagrindinis EVM tikslas - saugoti paskirstytą sandorių, atliktų naudojant Ethereum skaitmeninę valiutą eterį (ETH), įrašą. Išmaniųjų sutarčių funkcijas siūlo ir kitos platformos. Pagrindiniai principai išlieka tie patys, nors kai kuriais atvejais skiriasi įgyvendinimas ir išmaniųjų sutarčių tvarkymo būdai.

Tačiau kai kurie teigia, kad tai iš tikrųjų yra klaidingas pavadinimas, nes išmaniosios sutartys yra nei "išmaniosios" (galinčios išversti sudėtingus teisinius susitarimus į programinę įrangą), nei "sutartys" (neturinčios pagrindinių teisinių ar sutartinių nuostatų) (Orcutt, 2018). Išmaniosios sutartys šiuo metu įmanomos arba taikomos tik ribotomis ir griežtai apibrėžtomis sąlygomis, pavyzdžiui, kai nereikia spręsti ginčų. Atitinkami iššūkiai gali kilti nagrinėjant žmonių ir organizacijų galimybes kurti savo taisyklių sistemas ar išmaniąsias sutartis, kaip tam tikros automatizuotos privačios reguliavimo sistemos arba *lex cryptographica*, kurios gali išvengti jurisdikcijos taisyklių ir netolimoje ateityje veikti tarptautiniu mastu (De Filippi ir Hassan, 2016; De Filippi ir Wright, 2018; Quintais ir kt., 2019).

## 1.3 Blokų grandinės lūkesčiai ir prognozės

Nuo 2014 m. blokų grandinės technologijos populiarumui įtakos turėjo staigus finansų įstaigų susidomėjimas PRT. Blokų grandinės poveikio finansų sektoriui prognozės greitai užpildė atidžiai stebimą erdvę - nuo vertinimų, kad paskirstytojo registro technologijos iki 2022 m. gali sumažinti bankų infrastruktūros sąnaudas 15-20 mlrd. dolerių per metus (Santander, 2015), iki jų gebėjimo užtikrinti 5-10 mlrd. dolerių santaupų perdraudimo pramonei (PwC, 2016) arba iki 2027 m. sukaupti 10% pasaulio bendrojo vidaus produkto (BVP) (WEF, 2015). Dalis šio triukšmo buvo perkelta į bandomuosius projektus, skirtus tarptautiniams mokėjimams ir atsiskaitymams, prekybai vertybiniais popieriais, kapitalo skolinimui ar tapatybės valdymui ir kitiems naudojimo atvejams.

Tačiau kol buvo kuriamos geriau žinomos finansų sektoriaus taikomosios programos, vis dažniau pradėta kalbėti ir apie platesnį blokų grandinės potencialą kituose sektoriuose (Forbes, 2015; The

Economist, 2014). Nauji dalyviai - nuo pramonės iki akademinės bendruomenės, vyriausybių ir tarptautinių organizacijų - ėmė svarstyti, kaip ateityje blokų grandinė galėtų pakeisti pramonės, ekonomikos ir visuomenės dalis (Davidson et al., 2016).

Dabar daugiausia dėmesio skiriama tam, kaip panaudoti blokų grandinę kitose srityse kaip platesnės PRT šeimos dalį. Tai yra viena iš technologijų, kuri, kaip tikimasi, turės didelį poveikį per ateinančius 10-15 metų (OECD, 2016). Blokų grandinę galima būtų susieti su naujomis gamybos tendencijomis arba "ketvirtąja pramonės revoliucija", kuri apima kitas naujas technologijas, pradedant daiktų internetu ir baigiant dirbtiniu intelektu bei robotika ir naujomis medžiagomis arba pridėtine gamyba (OECD, 2017; Schwab, 2017; Craglia et al., 2018). Ateities scenarijai, paremti blokų grandine, taip pat pasižymi potencialiai giliais ekonomikos ir valdymo modelių pokyčiais, nukreiptais į decentralizuotus vertės mainus arba dar labiau įtraukią, skaidrią ir atskaitingą skaitmeninę ekonomiką (Casey ir Vigna, 2018; Mougayar, 2016; Tapscott ir Tapscott, 2016).

Pastaraisiais metais kriptovaliutos ir apskritai blokų grandinės technologija buvo tarp svarbiausių diskusijų pasaulio ekonomikos forumo veikloje ir renginiuose. Kasmetiniuose susitikimuose Davose, Šveicarijoje, vieši pareiškimai, specialios sesijos ir kiti renginiai blokų grandinės tema perėjo nuo įspėjamojo požiūrio prie pozityvesnių pastabų, nukreiptų į galimą platesnį poveikį įvairiuose sektoriuose. Pasaulio ekonomikos forumo Ketvirtosios pramonės revoliucijos centras, įsteigtas 2017 m., parengė nemažai rezultatyvių darbų, nuo "Blokų grandinės transformacijos žemėlapio" - dinamiškos žinių priemonės, padedančios suprasti pagrindines problemas, susijusias su blokų grandinės diegimu - iki "Blokų grandinė- tai daugiau nei beprasmis triukšmas" (WEF, 2018 m.) - skirtą padėti suinteresuotiesiems subjektams suprasti ar blokų grandinė yra tinkama jų verslo poreikiams. Taip pat buvo sudaryta Pasaulinė blokų grandinės taryba siekiant padėti formuoti pasaulinę technologijų politiką ir įmonių valdymo darbotvarkę šioje srityje. Tarybą sudaro 30 narių, tarp kurių yra ministrai ir įvairių reguliavimo agentūrų vadovai, vyriausieji vykdomieji pareigūnai, ir pagrindiniai technikos ir pilietinės visuomenės ekspertai.

Visgi didelė dalis blokų grandinės potencialo vis dar atrodo neišnaudota arba dar nėra visiškai išbandyta (Gartner, 2018a). Vis dar neišspręstos pagrindinės techninės problemos, tokios kaip viešųjų blokų grandinių išplečiamumas ir našumas, daugiausia susijęs su maža sandorių apimtimi; galimi slaptieji susitarimai ar koncentracija, kai dauguma dalyvių gali užvaldyti tinklą; didelis energijos suvartojimas diegiant dabartinius darbo įrodymo konsensuso mechanizmus; arba asmeninių, neskelbtinų ar konfidencialių duomenų apsauga blokų grandinėmis grindžiamose taikomosiose programose, kurios turi būti skaidrios ir atsparios klastojimui.

Tuo pat metu, kalbant apie ekonominį poveikį, naujausi tyrimai rodo nevienareikšmiškus rezultatus. Didžioji dauguma (77%) vyriausiųjų informacijos pareigūnų pripažino, kad jų organizacija nesidomi ar neplanuoja tirti ar kurti blokų grandinės sistemų, ir tik 1% nurodė, kad jų organizacijose

blokų grandinės diegiamos bet kokia forma (Gartner, 2018b). Be to, didelis procentas projektų yra nutraukiami arba nepasiekia reikšmingo masto (Deloitte, 2017). Kalbant apie pirminį virtualiosios valiutos siūlymą (angl. initial coin offering, ICO), daugiau kaip pusė projektų per keturis mėnesius tampa neaktyvūs (Benedetti ir Kostovetsky, 2018), o daugiau kaip 80 % 2017 m. buvo apkaltinti sukčiavimu (Satis Group, 2018).

Kai kas laikotarpį iki 2021 m. laiko "neracionaliu išsipūtimu", ir tik kitame "didesnių tikslinių investicijų" etape prognozuojama, kad iki 2026 m. blokų grandinės pridėtinė vertė verslui išaugs iki 360 mlrd. dolerių (Gartner, 2018c).

Tačiau greta nuogąstavimų dėl blokų grandinės poveikio, jos pridėtinės vertės ar konkrečių jos plataus pritaikymo būdų vis dažniau pasirodo ženklų, liudijančių apie įtikinamas jos taikymo ir potencialaus augimo galimybes.

## 1.4 Blokų grandinės teorinės įžvalgos

**Perspektyvos.** Blokų grandinė yra sparčiai besikeičianti sritis, dažnai pasižyminti didelių lūkesčių ir vykstančių eksperimentų mišiniu. Be šiame darbe nagrinėjamų temų, vis iškyla arba išryškėja nauji klausimai, kurie gali būti labai svarbūs siekiant suvokti kitą galimą blokų grandinės poveikį politikos, ekonomikos, socialiniu, techniniu, teisiniu ar aplinkosaugos lygmenimis.

Nors blokų grandinės technologija dinamiškai žengia į priekį, vis dar reikia papildomų žinių, kad būtų galima geriau suprasti ne tik jos esmę, bet ir plaukiojančias ribas, susijusias su jos potencialu. Tai padėtų geriau pasiruošti reaguoti į kai kurias neatidėliotinas problemas, su kuriomis politikos formuotojai susidurs rytoj, ne tik į tas, kurios jau pasirodė.

Be stiprių signalų, kurie buvo pastebėti analizuojant dabartines ir artimiausios ateities blokų grandinės perspektyvas konkrečiuose sektoriuose, ilgesnio laikotarpio perspektyvoje atsiranda ir silpnų signalų, kurie nurodo naujus veiklos aspektus. Mąstant apie būsimus blokų grandinės kelius, labai svarbu susikoncentruoti į kelis atrinktus signalus, siekiant iš anksto nepraleisti tokių signalų vertės ir to, ką jie atskleidžia.

**Pasitikėjimas ir valdymas.** Blokų grandinė gali iš naujo apibrėžti, ką reiškia "pasitikėjimas" tarp asmenų, grupių, institucijų ar organizacijų. Kai kurių nuomone, pasitikėjimą, tiksliau, nepasitikėjimą žmonėmis ir organizacijomis (laikomomis klystančiomis ir korumpuotomis), galėtų pakeisti pasitikėjimas blokų grandinės architektūromis, kurios galėtų vykdyti visus sandorius autonomiškai ir neutraliai. Tačiau mažai tikėtina, kad išnyks tarpininkai arba kad pasitikėjimas bus paprasčiausiai įtvirtintas per blokų grandinės techninius protokolus.

Vietoj to, blokų grandinė, kaip technologija, sudėtingai sąveikauja ekonominiu, kultūriniu, socialiniu, politiniu ir instituciniu lygiu (Catlow et al., 2018; Brekke, 2019). Pavyzdžiui, kalbant apie

išmaniąsias sutartis, dėl teisinės ir techninės kalbos spragų reikia (arba visada gali reikėti) teisininkų ir teisės ekspertų, turinčių ir bendrų, ir tikslių atitinkamų teisinių sistemų žinių, dalyvavimo ar įsikišimo (Khalil et al., 2017).

Nors tai susiję su sudėtingais ir brangiai kainuojančiais procesais, tačiau valdžios įsikišimo vis tiek gali prireikti siekiant nustatyti vienodas sąlygas dalyvauti visuomeninėje ir ekonominėje veikloje, priimti sprendimus dėl atsakomybės ir įsipareigojimų, užtikrinti taisyklių laikymąsi ir spręsti ginčus ar suteikti teisines garantijas ir apsaugą.

Kuriant ir diegiant blokų grandinės technologiją reikia daugiau diskusijų dėl pasitikėjimo sąlygų. Tradicinių tarpininkų ar trečiųjų šalių vaidmenų transformacija, kartu su asmenų, grupių ir organizacijų tarpusavio sąveikos pertvarka, ragina atidžiai išnagrinėti valdymo mechanizmus, kuriais bus valdomos ir sudaromos sąlygos tokioms blokų grandinėms. Pavyzdžiui, tai susiję su apibrėžimu, kuris nusako kas ką ir kada daro konkrečiame blokų grandinės tinkle (naudotojai, tvirtintojai, reguliuotojai) ir su atsakomybės bei atskaitomybės lygiais (Lapointe ir Fishbane, 2018).

**Decentralizuotas koordinavimas.** Apie blokų grandinę dažnai diskutuojama kaip apie naują institucinę decentralizuoto koordinavimo ir ekonominių bei socialinių sąveikų valdymą (Davidson et al., 2016; Bodó ir Giannopoulou). Žvelgiant iš šios perspektyvos, blokų grandinė konkuruoja su kitomis koordinavimo institucijomis- įmonėmis, rinkomis ir valdžios institucijomis.

Decentralizuotas valdymas gali pakeisti valdžios vykdomą sandorių kontrolę į pasidalijamąją kontrolę, paskirstytą tarp dalyvių. Pačių piliečių kontroliuojama tapatybė, automatinis teisės aktų taikymas per išmaniąsias sutartis arba vietovei neutralus, klastojimui atsparus balsavimas gali perkelti sprendimų priėmimą piliečiams ir padidinti jų suverenumą.

Blokų grandinė taip pat gali paskatinti labiau decentralizuotus, paskirstytus, bendradarbiavimu pagrįstus procesus ekonomikos organizavime. Jau esame matę panašių modelių griaunamąjį poveikį "platformų ekonomikos" arba "dalijimosi ar bendradarbiavimo ekonomikos" srityje (Esser et al., 2016; Bock et al., 2016; Codagnone et al., 2016). Šiuo atveju blokų grandinė galėtų paskatinti naujų inovacijų modelių kūrimą egzistuojančių įmonių sąskaita. Tačiau ji taip pat galėtų sudaryti sąlygas įvairiems vertės kūrimo šaltiniams, pajamų paskirstymui ir bendram asimetrinių santykių tarp ekonomikos subjektų subalansavimui.

Tarpininkavimas taip pat gali reikšti dinamiškesnių modelių skatinimą, kai daugybė skirtingų subjektų, individualių ar kolektyvinių, gali kurti, parduoti, pirkti savo skaitmeninį turtą arba gauti kompensaciją už jį.

Artimiausioje ateityje apribojimai gali būti susiję su naujo tipo ekonominėmis ir socialinėmis institucijomis, įgyvendinančiomis blokų grandinės taisyklių sistemas, pavyzdžiui, išmaniąsias sutartis, siekiant policentrinio ir bendro išteklių valdymo. Kai kas jau eksperimentuoja su decentralizuotomis

autonominėmis organizacijomis, kurios gali turėti išteklių, jais keistis ar prekiauti ir autonomiškai sąveikauti su kitais žmonėmis, įrenginiais, organizacijomis (Buterin, 2014; Mougayar, 2015).

**Kriptoekonomika.** Lygiagrečios arba nereguliuojamos ekonomikos, mažai susijusios su pagrindine ekonomika, proliferacijos nauda gali būti svarbesnė nei nusikalstamos veikos atvejai tokioje ekonomikoje. Blokų grandinė galėtų sudaryti sąlygas plisti tarptautinėms, neteritorinėms ir atviroms inovacijoms, verslininkams ir verslo operacijoms, apeinančioms bet kokią reguliavimo ar politinę priežiūrą, pavyzdžiui, "kriptoanarchijų" ar "kriptosecesijų" forma (Macdonald et al., 2016).

Vienas iš esminių pokyčių galėtų būti susijęs su žetonų (angl. token) sąvoka dabartiniuose ir būsimuose kriptoekonomikos scenarijuose. Neapsiribojant finansine konotacija, "valiuta", "žetonas" ar "skaitmeninis turtas" blokų grandinės sistemoje gali būti suprantamas kaip įvairios paskirties vertės vienetas, naudojamas tam tikruose verslo modeliuose ar ekonominėse sistemose (Mougayar, 2017). Įvairiose blokų grandinės sistemose žetonas suteikia specialią prieigą prie paslaugos ar produkto (pavyzdžiui, debesų saugyklos), suteikia balsavimo teisę ir (arba) atlygina dalyviams už jų laiką, darbą, recenzijas ar kitą indėlį, viską, kas susiję su tinklu.

Kriptografinės arba žetonais pagrįstos sistemos gali turėti įtakos asmenų, grupių, bendruomenių ir organizacijų tarpusavio sąveikos elgesio koordinavimui. Tai reiškia, kad tokios sistemos kelia klausimus apie galimą naują paskirstytąją ekonomiką ar rinką, kurioje įvairūs dalyviai siekia bendrų tikslų. Šiuo atžvilgiu besiformuojanti "kriptoekonomikos" sritis sujungia ekonomiką, informatiką ir elgsenos mokslus, kad būtų galima tirti individualių sprendimų priėmimą ir strateginę sąveiką tokiose ekosistemose.

**Savarankiška tapatybė.** Blokų grandinė galėtų pasiūlyti alternatyvius tapatybės valdymo arba savivaldumo principo įgyvendinimo mechanizmus, kurie leistų asmenims saugoti ir valdyti savo tapatybę ir įrašus blokų grandinėje.

Priklausomai nuo struktūros, blokų grandinės sistemos potencialiai galėtų suteikti galimybę priimti decentralizuotus ir privatumą užtikrinančius sprendimus. Blokų grandinės architektūros gali pasiūlyti bent jau pseudo-anonimizavimą, tačiau ne visišką anonimizavimą, todėl daugeliu atvejų, norint nuslėpti tam tikrą informaciją apie sandorius ar konfidencialius duomenis, reikia papildomų šifravimo ir (arba) paslėpimo sluoksnių (De Filippi, 2016). Taip pat galima suteikti leidimą naudotis duomenimis tik konkrečioms ar patikimoms šalims arba atšaukti prieigą tam tikru metu. Tai leistų greičiau ir saugiau valdyti tapatybės nustatymo procesus ir geriau kontroliuoti duomenų atskleidimą ir atrankinį dalijimąsi jais. Decentralizuoti sprendimai tokiems tikslams šiuo metu yra kuriami, kurie, tačiau, neapsieina be kritikos (Narayanan et al., 2012). Pavyzdžiui, šiuo metu vykdomi keli projektai ir iniciatyvos, kurių metu kuriami nauji piliečių kontroliuojami su savarankiška skaitmenine tapatybe režimai (Financial Times, 2017; Symons et al., 2017), pagrįsti paskirstytomis, atviromis ir modulinėmis architektūromis, skirtomis internetinei tapatybei ir duomenims konfidencialiai valdyti realiuoju laiku.

Svarbu toliau vertinti, kaip blokų grandinė galėtų veikti kartu su kitomis paskirstytomis tapatybės ir autentiškumo nustatymo sistemomis, t. y. elektroninių parašų, elektroninių antspaudų, laiko spaudų, elektroninių pristatymo paslaugų ir interneto svetainių autentiškumo patvirtinimo, kad būtų sudarytos sąlygos saugiam ir tarpvalstybiniam įmonių, piliečių ir valdžios institucijų elektroniniam bendravimui.

**Sąveika ir standartizavimas.** Nepriklausomai nuo to, kokie blokų grandinės sprendimai bus sukurti per ateinančius metus, svarbiausia, kad būtų kuriami interoperabilūs protokolai, kad skirtingi blokų grandinės produktai ir paslaugos nebūtų uždari ir galėtų bendrauti tarpusavyje.

Sąveikos siekiama pasitelkiant tarptautinio lygmens standartizavimo darbo grupes. Kai kurie teigia, kad toks standartizavimas bus labai svarbus siekiant suderinti jos taikymą ir sudaryti sąlygas jos pritaikymui įvairiose pramonės šakose. Kiti teigia, kad per ankstyvas sąveikos taikymas gali įgalinti dar neištestuotas technologijas ir (arba) įtakingų bendrovių sprendimus tokiu būdu užblokuojant naujus rinkos dalyvius.

Viena vertus, šiuo metu vykdomos standartizacijos iššūkiai yra susiję su dar tik besiformuojančiomis koncepcinėmis ir praktinėmis žiniomis apie blokų grandinę, kita vertus, jie yra susiję su blokų grandinės kūrėjų bendruomenių integracijos stoka, kuri yra linkusi būti labiau atskirta nuo šios veiklos arba užgožta didesnių technologinių ar komercinių narių.

Priklausomybės nuo platformos ar pardavėjo pavojų būtų galima sumažinti įtraukiant daugiau procesų, kurie praktiškai leistų naujiems ar mažesniems dalyviams prasmingai dalyvauti, atsižvelgiant į jų laiko, kapitalo ir žmogiškųjų išteklių ribotumą. Šiuo atžvilgiu dabartinės daugiašalės valdymo procedūros, taikomos rengiant standartus, galėtų būti toliau aptariamos ir tobulinamos, kad būtų laikomasi pagrindinių atvirumo, skaidrumo ir konsensuso principų.

**Duomenų tvarkymas ir valdymas.** Skaitmeninių duomenų tvarkymas tapo pagrindine daugelio įmonių ir pramonės šakų dalimi ir, tikėtina, ši tendencija artimiausioje ateityje dar labiau sustiprės.

Kas, kaip ir kokiais tikslais tvarko, saugo ir valdo duomenis, yra arba taps esminiais klausimais bet kuriai organizacijai. Blokų grandinė, kaip klastojimui atsparus registras, galėtų suteikti daugiau mechanizmų, užtikrinančių duomenų autentiškumą ir patikimumą (Lemieux, 2016).

Visgi blokų grandinė neturi sprendimų, kaip užtikrinti tikslumą, nuoseklumą ar duomenų galiojimą per visą jų gyvavimo ciklą. Pavyzdžiui, problemų gali kilti dėl į blokų grandinę įvedamų, apdorojamų ir joje saugomų duomenų kokybės, t. y. jei duomenys yra neteisingi, negaliojantys ar neišsamūs. Blokų grandinės technologija tik įrašo ir tikrina duomenis, kai jie įvedami ir bendru dalyvaujančių dalyvių ar mazgų sutarimu, be jokių garantijų ar faktų tikrumo patikrinimo.

Taip pat gali kilti problemų dėl blokų grandinės techninių architektūrų stabilumo ir tęstinumo. Pavyzdžiui, kyla rizika, kad ankstesnių blokų grandinės sistemų ("atšakų") įrašai gali būti nebepanaudojami, t.y. jų nebegalima išsaugoti, atnaujinti ar tvarkyti, todėl tai gali sukelti painiavą visame tinkle dėl teisėtos ir naujos įrašo versijos.

Organizacijos turi įvertinti savo išteklius, reikalingus patikimoms skaitmeninėms saugykloms kurti, ir užtikrinti papildomus techninius, politinius ir institucinius pajėgumus, kad būtų galima tinkamai saugoti archyvinius dokumentus, valdyti duomenis, suteikti prieigą prie jų ir apskritai juos išsaugoti.

# 2. BLOKŲ GRANDINĖS VAIDMUO SKAITMENINĖS VALDŽIOS KONTEKSTE

Blokų grandinės populiarumo augimas ir didėjantis dėmesys jai neliko nepastebėtas ES politikos lygmeniu. Iš pradžių daugiausia dėmesio buvo skiriama virtualioms valiutoms, tačiau blokų grandinės, kaip besiformuojančios naujos technologijos, potencialas įvairiuose sektoriuose pastaraisiais metais yra viešai Europos valdžios institucijų pripažintas ir skatinamas. Pavyzdžiui, buvo paskelbta nemažai kvietimų, mokslinių tyrimų programų ir finansavimo programų trečiosioms šalims, kuriose Europos Komisija remia eksperimentus ir inovacijas. Be to, nemažai EK tarnybų jau vykdo arba svarsto apie tiriamąją veiklą, naudojant blokų grandinę kaip galimą būdą pagerinti su politikos įgyvendinimu susijusius pagrindinius procesus, pavyzdžiui reguliuojamos informacijos prieinamumą, ataskaitų teikimą realiuoju laiku, tapatybių valdymą, notarinio patvirtinimo paslaugas ir prekių judėjimo stebėseną.

## 2.1 Blokų grandinė Europos Sąjungos viešojo valdymo kontekste

Europos komisijos (EK) politikos lygmeniu blokų grandinė laikoma viena iš proveržio technologijų, kurios potencialus poveikis finansų sektoriui gali būti didžiulis, bet taip pat ir toli už jo ribų (EK, 2017c). Tai reiškia, kad blokų grandinės technologijos gali transformuoti skaitmenines paslaugas, atsisakant centralizuotų platformų modelių, ir gali būti taikomos įvairiose srityse: e. sveikatos paslaugų, e. valdžios ir socialinių prekių teikimo, energetikos, tiekimo grandinių, daiktų interneto, finansų sektoriaus ir kitose srityse (EK, 2017d). Be to, tarptautinio vystymosi srityje blokų grandine užtikrinti sandoriai buvo įvardyti kaip vienas iš galimų skaitmeninių sprendimų, kurie gali padėti kovoti su skurdu, prisidėti prie tikslingesnės humanitarinės ir vystymosi veiklos ir jos susiejimo, taip pat padėti valdyti migraciją ir šalinti trūkumus daugelyje ES šalių partnerių (EK, 2017b).

Blokų grandinės technologijos diegimo privalumai yra skaidrumas ir galimybė atlikti auditą, kurie gali suteikti piliečiams daugiau galimybių kontroliuoti ir padėti sumažinti sukčiavimo ir atitikties užtikrinimo išlaidas valdžios institucijoms ir priežiūros institucijoms (EK, 2017d). Vis dėlto ES politikos lygmeniu taip pat nustatyta nemažai neišspręstų klausimų, įskaitant plėtros galimybes, valdymą, sąveikumą ir teisinius bei reguliavimo aspektus, pavyzdžiui, iššūkius tradicinėms civilinės ir sutarčių teisės sąvokoms ir taisyklėms (EK, 2017a).

Europos valdžios institucijos nagrinėja įvairias strategijas, kaip spręsti šias su blokų grandine susijusias problemas. 2018 m. vasario mėn., atsižvelgiant į Europos Parlamento (EP) remiamą FinTech horizontaliąją darbo grupę, pradėjo veikti ES blokų grandinės observatorija ir forumas. Juo siekiama

stebėti tendencijas, pokyčius ir panaudojimo atvejus, sutelkti ekspertines žinias, kad būtų galima spręsti sektorines ir tarpsektorines problemas, ieškoti bendrų sprendimų ir tarptautinių panaudojimo atvejų.

ES blokų grandinės observatorija ir forumas subūrė dvi temines darbo grupes (blokų grandinės politikos ir bendrųjų sąlygų bei naudojimo atvejų ir pereinamojo laikotarpio scenarijus), kurių kiekvieną sudaro apie 30 narių. Ji taip pat paskelbė keletą teminių ataskaitų, pavyzdžiui, apie blokų grandinių inovacijas Europoje (2018 m. liepos mėn.), blokų grandines ir BDAR (2018 m. spalio mėn.), blokų grandines valdžios institucijoms ir viešosioms paslaugoms (2018 m. gruodžio mėn.), blokų grandinių plėtrą, sąveikumą ir tvarumą (2019 m. kovo mėn.) ir blokų grandines ir skaitmeninę tapatybę (2019 m. gegužės mėn.).

Nuo 2018 m. balandžio mėn. 26 valstybės narės, Norvegija ir Lichtenšteinas pasirašė deklaraciją, kuria sukuriama Europos blokų grandinės partnerystė (EBP). Jos tikslas - bendradarbiauti kuriant Europos blokų grandinės paslaugų infrastruktūrą (angl. European Blockchain Services Infrastructure, EBSI), kad būtų remiamas tarptautinis skaitmeninių viešųjų paslaugų diegimas. Partnerystės tikslas - sukurti infrastruktūrą, kuria būtų galima naudotis, kad būtų remiamos skaitmeninės paslaugos, kurias diegia viešasis sektorius, o ilgainiui - ir privatūs subjektai. Ši plėtra taip pat grindžiama EK remiamu galimybių tyrimu, kuriuo siekiama įvertinti ES blokų grandinės infrastruktūros (EuroChain) sąlygas atviroje, novatoriškoje, patikimoje, skaidrioje ir ES teisės aktus atitinkančioje duomenų ir sandorių aplinkoje.

2018 m. lapkričio 20 d. Briuselyje vykusiame ES blokų grandinės apskritojo stalo susitikime EK ir Europos blokų grandinės partnerystė paskelbė sprendimą 2019 m. įsteigti Tarptautinę patikimų blokų grandinės programų asociaciją (angl. International Association for Trusted Blockchain Applications, IATBA). Idėja - suburti daugybę suinteresuotųjų subjektų iš pramonės, startuolių, vyriausybių, tarptautinių organizacijų ir pilietinės visuomenės, kurie aktyviai dalyvauja blokų grandinės ir PRT programose. Prie asociacijos stebėtojų teisėmis kviečiamos prisijungti vyriausybinės organizacijos, standartus nustatančios įstaigos ir tarptautinės organizacijos. Pagrindiniai jos tikslai yra:

- palaikyti dialogą su valdžios institucijomis ir reguliavimo institucijomis, kuris padės suvienodinti reguliavimo metodus blokų grandinės atžvilgiu pasauliniu mastu;
- skatinti atvirą, skaidrų ir įtraukų pasaulinį blokų grandinės ir kitų PRT infrastruktūrų bei taikomųjų programų valdymo modelį;
- remti sąveikumo gairių, specifikacijų ir visuotinių standartų rengimą ir priėmimą, kad būtų sustiprintos patikimos, atsekamos, į vartotoją orientuotos skaitmeninės paslaugos;
- parengti konkretiems sektoriams skirtas gaires ir specifikacijas, skirtas patikimų blokų grandinės ir PRT taikomųjų programų kūrimui ir spartinimui konkrečiuose sektoriuose (pvz., finansinių paslaugų, sveikatos, tiekimo grandinės, energetikos ir finansinės įtraukties).

Per pastaruosius dvejus metus EK taip pat remia standartizacijos pastangas Tarptautinėje standartizacijos organizacijoje (angl. International Organization for Standardization, ISO), Tarptautinėje telekomunikacijų sąjungoje (angl. International Telecommunication Union, ITU), Europos telekomunikacijų standartų institute (angl. European Telecommunications Standards Institute, ETSI) ir Europos elektrotechnikos standartizacijos komitete (angl. European Committee for Electrotechnical Standartization, CEN-CENELEC). Pastaroji grupė neseniai paskelbė straipsnį (CEN-CENELEC, 2018 m.), kuriame pateikta nemažai rekomendacijų prioritetinėmis temomis, pavyzdžiui, tvaraus vystymosi, skaitmeninės tapatybės, privatumo ir duomenų apsaugos, ir pabrėžiami konkretūs Europos naudojimo atvejai finansinių paslaugų ir turto valdymo, registrų paslaugų ir (arba) licencijų valdymo, asinchroninio ir (arba) paskirstytojo automatizavimo, duomenų apsaugos ir informacijos saugumo, tapatybės valdymo, lėšų rinkimo (naudojant kuponus), išmaniųjų energijos tinklų ir išmaniųjų namų ir (arba) miestų srityse.

2019 m. vasario mėn. EK Vidaus rinkos, pramonės, verslumo ir mažų ir vidutinių įmonių (MVĮ) generalinis direktoratas (angl. Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, DG GROW) paskelbė, kad Europos Sąjungos intelektinės nuosavybės tarnyba (angl. the European Union Intellectual Property Office, EUIPO) pradėjo Kovos su klastojimu blokatono forumą. Jame dalyvaus žmonės ir organizacijos, kurie apibrėš kovos su klastojimu naudojimo atvejį ir susijusį bandomąjį projektą ir galiausiai suformuos bei sukurs būsimą blokų grandine grindžiamą kovos su klastojimu infrastruktūrą. Šiuo tikslu forumas ketina sujungti privačias organizacijas, teisėsaugos institucijas ir piliečius, kad padėtų nustatyti autentiškas ir suklastotas prekes visoje platinimo grandinėje.

Šis forumas - tai 2018 m. birželio 22-24 d. Briuselyje surengto konkurso "EU Blockathon", kurio tikslas - išnaudoti blokų grandinės technologijos potencialą siekiant apsaugoti tiekimo grandines nuo klastočių, tęsinys. Renginio metu 11 programuotojų komandų 48 valandas dirbo kartu kurdamos įvairius kovos su klastojimu blokų grandinės sprendimus, skirtus vartotojams, teisėsaugos institucijoms, logistikos operatoriams ir įmonėms.

Anksčiau EUIPO aktyviai dalyvavo svarstant blokų grandinės poveikį intelektinei nuosavybei. Pavyzdžiui, 2017 m. spalio 27 d. Alikantėje ji surengė konferenciją "Blokų grandinė ir intelektinė nuosavybė ", kurioje buvo aptartos pagrindinės technologijos sąvokos, technologijos ir intelektinės nuosavybės sąveika ir trys praktinio naudojimo atvejai (tiekimo grandinės apsauga, muzikos įrašų valdymas ir BTC atsekamumas). Dalyvavo blokų grandinės ekspertai, nacionalinių intelektinės nuosavybės tarnybų, teisių turėtojų ir pilietinės visuomenės atstovai.

Tuo pat metu EP taip pat aktyviai dalyvauja anksčiau vykusiose ir tebevykstančiose diskusijose apie šios technologijos tarpsektorinį potencialą. 2018 m. vasarį Europos Parlamento mokslinių tyrimų tarnyba, ypač jos Mokslinių prognozių skyrius (angl. Scientific Foresight Unit, STOA), paskelbė ataskaitą "Kaip blokų grandinės technologija galėtų pakeisti mūsų gyvenimą", kuria siekiama paskatinti svarstymus ir diskusijas (Boucher et al., 2017). Pirmiausia joje pripažįstama, kad blokų grandinės

technologija yra sudėtinga, prieštaringa ir greitai kintanti, nors ja vis labiau domisi piliečiai, įmonės ir teisės aktų leidėjai visoje ES. Ataskaitoje nagrinėjamos aštuonios sritys, kuriose blokų grandinės, kaip teigiama, gali daryti didelį poveikį (valiutos, skaitmeninis turinys, patentai, e. balsavimas, išmaniosios sutartys, tiekimo grandinės, viešosios paslaugos ir decentralizuotos autonominės organizacijos), ir paaiškinama, kaip ši technologija galėtų būti plėtojama tose konkrečiose srityse, kokį poveikį ši plėtra galėtų turėti ir kokių galimų politinių klausimų reikėtų numatyti.

2018 m. spalio 3 d. EP priėmė rezoliuciją "Paskirstytojo registro technologijos ir blokų grandinės: pasitikėjimo be tarpininkavimo stiprinimas" (angl. Distributed Ledger Technologies and Blockchains: Building Trust with Disintermediation) (EP, 2018a) kurioje pabrėžiamas platus PRT grindžiamų taikomųjų programų spektras, kuris potencialiai galėtų paveikti visus ekonomikos sektorius, pavyzdžiui, energetikos, transporto, sveikatos priežiūros, tiekimo grandinių, švietimo, kūrybinių industrijų, finansinių paslaugų ir kt. Rezoliucijoje pateikiama teigiama jų galimo poveikio perspektyva, pavyzdžiui, pasitikėjimo ir skaidrumo didinimas, sandorių ir tarpininkavimo sąnaudų mažinimas, organizacinio efektyvumo didinimas ir piliečių įgalinimas kontroliuoti savo duomenis. Taip pat ypač pabrėžiama, kad ES turi galimybę tapti pasauline lydere PRT srityje ir būti patikima veikėja formuojant jos plėtrą ir rinkas visame pasaulyje, todėl blokų grandinėms ir PRT reikia inovacijoms palankios, įgalinančios ir skatinančios sistemos, kuri galėtų užtikrinti reguliavimo ir teisinį tikrumą ir garantuoti vartotojų, investuotojų ir aplinkos apsaugą. Be to, tokioje sistemoje turėtų būti laikomasi technologijų neutralumo ir verslo modelių neutralumo principo.

2018 m. gruodžio 13 d. EP priėmė rezoliuciją "Blokų grandinės: į ateitį orientuota prekybos politika" (angl. "Blockchain: A Forward-Looking Trade Policy") (EP, 2018b), kurioje visų pirma nagrinėjama, kaip blokų grandinės gali sustiprinti ir pagerinti ES prekybos politiką. Pavyzdžiui, joje pabrėžiama, kad blokų grandinės potencialiai galėtų padėti įgyvendinti prekybos ir darnaus vystymosi darbotvarkę, didinant pasitikėjimą žaliavų ir prekių kilme ir didinant gamybos procesų ir tiekimo grandinių skaidrumą, kai tai susiję su jų reguliavimo atitiktimi darbo, socialinėms ir aplinkosaugos teisėms, įskaitant konfliktinių iškasenų, neteisėtos prekybos kultūros vertybėmis, eksporto kontrolės ir korupcijos sritis.

Panašiai kaip ir ankstesnėje rezoliucijoje, šioje rezoliucijoje pabrėžiama, kad svarbu, jog ES pirmautų ir prisiimtų atsakomybę blokų grandinės srityje. Joje pabrėžiama, kad reikia vienodų sąlygų, kai kalbama apie pasaulinę konkurenciją, ir palankios plėtros ir reguliavimo aplinkos, kartu teigiama, kad teisės aktais nustatant technologiją, kuria grindžiamos taikomosios programos, būtų ribojamos inovacijos ir naujų taikomųjų programų kūrimas. Galiausiai rezoliucijoje EK ir valstybės narės raginamos imtis tam tikrų veiksmų, pavyzdžiui, pradėti ir prižiūrėti bandomuosius projektus, kad būtų patikrinta jų nauda; parengti blokų grandinės taikymo tarptautinėje prekyboje pagrindinių principų rinkinį (kad būtų užtikrintas pakankamas teisinio tikrumo lygis); atlikti pagrindinį vaidmenį blokų

grandinės standartizavimo ir saugumo procese, įskaitant, terminologiją, plėtrą ir technologijos diegimą prekybos ir tiekimo grandinės valdymo srityje.

## 2.2 Blokų grandinės vaidmuo transformuojant viešojo sektoriaus valdymą

Susidomėjimą blokų grandinės galimybėmis viešajame sektoriuje rodo kasmet didėjantis eksperimentinių projektų kiekis. Privalumai akivaizdūs- didesnis kibernetinis saugumas (duomenų vientisumo užtikrinimas, atsparumas klastojimui, skaidrumas), efektyvumo padidėjimas (mažesnis duomenų apdorojimo laikas ir sąnaudos) ir didesnis gyventojų pasitikėjimas viešuoju registrų tvarkymu. Kol kas blokų grandinė siūlo daugiau laipsniškų negu radikalių naujovių, kaip kartais vaizduojama, nors kai kurios iš jų turi didžiulį ekonominės naudos potencialą.

Kokio masto pokyčius įneš blokų grandinė į viešąjį sektorių, dar neaišku, nes ši technologija dar tik pradedama taikyti ir turi įveikti nemažai kliūčių, susijusių su plėtra, našumu ir konfidencialumu. Taip pat yra blokų grandinės diegimo atvejų, kai ji nesukuria aiškios pridėtinės vertės, palyginti su centralizuotomis sistemomis, arba ji nesukuria naujos paslaugos ar paradigminio pokyčio piliečių ir valdžios institucijų santykiuose.

### 2.2.1 Žemės ir nekilnojamojo turto sandoriai

Blokų grandinė - tai nauja bendrosios paskirties informacinė technologija, skirta registruoti ir atsiskaityti už sudėtingus sandorius (Davidson ir kt., 2016). Šios savybės turi konkrečios reikšmės viešojo administravimo ir valdymo kontekste.

Viešojo administravimo institucijose daugybė registrų, kuriuose kaupiami piliečių, mokesčių ar žemės nuosavybės įrašai, yra brangiai kainuojantys, juose gali būti žmogiškųjų klaidų, be to, juose yra vieno gedimo taško rizika.

Viešojo administravimo institucijos blokų grandinės technologiją galėtų naudoti paskirstytam dokumentų ir turto registravimui, vietoj dabar naudojamo centralizuoto būdo. Blokų grandinės technologijos nauda viešosioms paslaugoms apima galimybę teikti specialiai pritaikytas paslaugas konkretiems piliečiams, didesnį pasitikėjimą valdžios institucijomis, geresnį automatizavimą, skaidrumą ir galimybę atlikti auditą (Atzori, 2015, 2017; Norta, 2015; Swan, 2015; Van Zuidam, 2017).

Tokių įrašų, kaip gimimo liudijimas, žemės nuosavybės dokumentai ar teistumas, paskirstyta registracija ir keitimasis jais galėtų būti ypač naudingi piliečiams tose šalyse, kuriose centralizuota informacijos infrastruktūra yra mažiau išvystyta, nepatikima arba korupcinė.

Viename iš Europoje vykdomų blokų grandinės projektų, skirtų skaitmeninei valdžiai, Sakartvelo Nacionalinė registrų agentūra (NRA), bendradarbiaudama su "The Bitfury Group", naudoja blokų grandinės technologiją, kad savo piliečiams suteiktų skaitmeninį žemės nuosavybės teisės sertifikatą.

Šiuo metu šis bandomasis blokų grandinės projektas leidžia registruoti žemės nuosavybės teisių pirkimus ir pardavimus bei registruoti naujas žemės nuosavybės teises (nuo 2016 m. balandžio mėn. jų įregistruota daugiau kaip 100 000). Taip siekiama padidinti visuomenės pasitikėjimą su nuosavybe susijusia apskaita ir galiausiai padėti Sakartvelui kovoti su korupcija ir ginčais dėl turtinių pretenzijų (Eurasianet, 2017; The Bitfury Group, 2017). Tikimasi, kad ateityje sistema taip pat užtikrins turto sunaikinimo, hipotekos ir nuomos registravimą bei notarines paslaugas (Forbes, 2017a).

Šiame konkrečiame bandomajame projekte blokų grandinės sistema yra privati, atsižvelgiant į tai, kas gali patvirtinti sandorius, o tai reiškia, kad faktinį sandorių patvirtinimą atlieka grupė žinomų serverių arba mazgų, tačiau vėliau duomenys yra šifruojami, o sandoris patvirtinamas viešojoje Bitcoin blokų grandinėje, kuri visiems piliečiams suteikia skaidrumo. Šis projektas yra viešos ir privačios blokų grandinės derinimo pavyzdys.

Žemės nuosavybės teisės įgijimo ar keitimo procesą sudaro šie žingsniai (žr. 4 pav.):

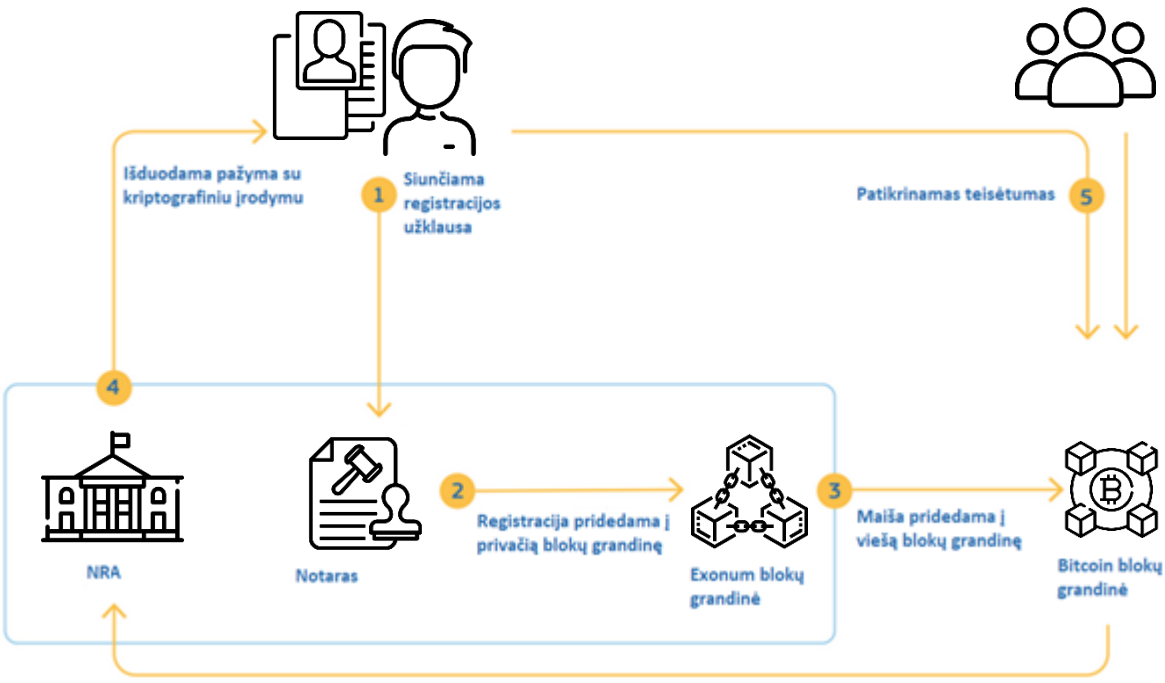
1. Pilietis gali inicijuoti prašymą tarnybai arba notarui įregistruoti arba patikrinti žemės nuosavybės teisės išrašą.

2. Notaras įregistruoja žemės nuosavybės teises privačioje "Exonum" blokų grandinėje.

3. Privačios "Exonum" blokų grandinės maišos kodai yra įtvirtinti viešojoje "Bitcoin" blokų grandinėje, kuri užtikrina visų sandorių vientisumą.

4. NRA suteikia piliečiui skaitmeninį jo turto sertifikatą, paremtą kriptografiniu išrašo originalumo įrodymu, paskelbtu "Bitcoin" blokų grandinėje.

5. Dabar bet kas gali patikrinti, ar žemės nuosavybės teisė yra teisėta ir galiojanti.




**4 pav. Žemės nuosavybės registracijos procesas, kurį naudoja NRA (Sakartvelas)**

Šis blokų grandinės diegimas teikia kiekybinės ir kokybinės naudos derinį:

- ženkliai sutrumpėja žemės nuosavybės teisių registravimo ir tikrinimo laikas: anksčiau šiems veiksmams atlikti reikėdavo nuo vienos iki trijų dienų, o naudojant blokų grandinę sandorio laikas sutrumpėja iki kelių minučių;
- didesnis žemės nuosavybės teisių registravimo proceso skaidrumas;
- didesnis piliečių pasitikėjimas NRA saugomų duomenų tikslumu;
- sistema tapo efektyvesnė, nes sertifikato patikrinimo laikas sutrumpėjo nuo kelių dienų iki kelių sekundžių;
- Žemės nuosavybės teisių registravimo paslaugos veiklos sąnaudos sumažėjo iki 90%.

Su naujos sistemos diegimu susijusios išlaidos yra daugiausia vienkartinės, susijusios su Exonum protokolo pritaikymu ir integracija su NRA ir notarais. Piliečiams netaikomi jokie papildomi mokesčiai. Pažymėtina, kad keletas senosios sistemos išlaidų išlieka (pavyzdžiui, centrinės skaitmeninių įrašų sistemos priežiūra), nes blokų grandinės sistema nepakeičia senojo sprendimo. Be to, piliečio inicijuoto prašymo patikrinimą notaras vis dar atlieka rankiniu būdu.

Kalbant apie pagrindines išvadas, pagrindiniai NRA blokų grandinės bandomąjį projektą skatinantys veiksniai yra didesnis skaitmeninių sertifikatų saugumas ir patikimumas. Sertifikatų patikra atliekama viešojoje blokų grandinėje, kurios nekontroliuoja joks dalyvis ar dalyvių grupė. Šis nepriklausomas ir nepaperkamas sluoksnis padeda kovoti su sukčiavimu ir užkirsti kelią ginčams dėl žemės nuosavybės teisių. Tačiau blokų grandinės sistema neužtikrina visiško institucijų (pvz. notaro) eliminavimo iš proceso ir nepakeičia esamų sistemų. Ji tik suteikia daugiau naujų funkcijų - papildomų garantijų piliečiams. Dėl šios priežasties ją integruoti į senąsias sistemas buvo palyginti lengva.

Šios blokų grandine pagrįstos sistemos lengvą įgyvendinimą ir sėkmę daugiausia lėmė Sakartvelo NRA organizacijos sėkmė ir savarankiškumas. Ši organizacija turi mažai biurokratijos ir remia inovacijas "iš apačios į viršų". Kiti pagrindiniai sėkmės veiksniai susiję su teisine nuostata, pagal kurią žemės nuosavybės duomenys yra vieši (kitose šalyse jie laikomi privačiais), taip pat su registracijos proceso automatizavimu ir piliečiams lengvai suprantama internetine sąsaja.

Kitas blokų grandinės sistemų taikymas viešajame administravime susijęs su nuosavybės ar nekilnojamojo turto sandorių procedūromis. Jų saugumas ir skaidrumas yra svarbūs dėl didelės turto vertės, tačiau atsiskaitymo procesas yra lėtas ir brangus dėl to, kad jam gresia įvairios rizikos ir apskritai trūksta pasitikėjimo šiuo metu veikiančiomis registravimo sistemomis.

2016 m. rugsėjį Švedijos kartografijos, kadastro ir žemės registravimo tarnyba kartu su banku "Landshypotek", SBAB, "Telia", "ChromaWay" ir "Kairos Future" (ChromaWay, 2017) sukūrė blokų grandine pagrįstą bandomąjį projektą, kuriuo siekiama iš naujo apibrėžti nekilnojamojo turto sandorius ir hipotekos dokumentus. Šiuo projektu bandoma spręsti tiek nekilnojamojo turto perleidimo sandorių šalių tarpusavio nepasitikėjimo problemą, tiek paspartinti sandorius.

Sprendime pristatoma visiškai nauja blokų grandine pagrįsta darbo eiga, kuri supaprastina ir užtikrina nuosavybės teisės perleidimo procesą. Pilietis prisijungia prie "ChromaWay" interneto puslapio, kuris suteikia prieigą prie "Esplix" - išmaniųjų sutarčių darbo eigos mechanizmo. Sistema palaiko sąsają su Švedijos žemės registru, kuris yra atsakingas už žemės nuosavybės teisių saugojimą. Blokų grandinė saugo tik sistemos būseną po kiekvieno darbo eigos žingsnio įvykdymo. Visas sandorio procesas, kuriuo grindžiamas nekilnojamojo turto perleidimas (dalyvaujant pirkėjui, pardavėjui, nekilnojamojo turto agentui, bankams ir žemės registrui), pavaizduotas 5 paveiksle.




**5 pav. Nekilnojamojo turto nuosavybės perdavimo procesas „ChromaWay“ (Švedija)**

Ši bandomoji blokų grandinė apibrėžiama kaip privati blokų grandinė su leidimais, kurioje anonimiškai saugomi įvairių dalyvių pateikti sandorių duomenys. Šiuo metu naudojama centralizuota tapatybės nustatymo sistema, kuria apibrėžiama, kas gali sudaryti sandorius ir matyti duomenis, o sandorius patvirtina žinomi mazgai. Nors projektas vykdomas jau kurį laiką, šis bandomasis projektas vis dar nėra integruotas į nekilnojamojo turto agentų aplinką. Be to, duomenų gavimas iš blokų grandinės dar nėra automatinis - dar reikia įveikti kai kurias technines kliūtis.

Mažesnės sandorių sąnaudos yra viena iš pagrindinių šio bandomojo projekto privalumų. Nekilnojamojo turto sandorių sudarymo laikas sutrumpėja nuo kelių savaičių iki kelių minučių ar valandų. Šiuo metu nekilnojamojo turto draudimo išlaidos gali siekti iki 10% pirkimo vertės. Naudojant "ChromaWay" sistemą šią sumą galima sumažinti iki 1%. Finansinę naudą lemia ir kiti teigiami padariniai, pavyzdžiui, sumažėjęs popierizmas ir sukčiavimo atvejų skaičius. Dar viena svarbi nauda gaunama dėl optimizuotos darbo eigos, kuri leidžia labiau pasitikėti šiais didelės vertės sandoriais ir potencialiai pagerinti rinkos veikimą bei padidinti turto likvidumą. Taip pat pabrėžiamas didesnis

atsparumas bet kokiems išorinių dalyvių atliekamiems saugojimo sistemos pakeitimams, atsižvelgiant į paskirstytą blokų grandinės platformos pobūdį.

Projekto išlaidos apima integravimo ir eksploatavimo išlaidas. Pirmiausia, norint įdiegti visoms suinteresuotoms šalims tinkamą sistemą, reikia daug pastangų, kad ji būtų integruota į senąsias sistemas ir sąveikautų su bankų sistemomis. Veiklos sąnaudos greičiausia bus didesnės, palyginti su centralizuotos duomenų bazės sprendimu (ChromaWay, 2017). Išlaidas didina nuolatinis konsorciumo duomenų bazės, kuri yra blokų grandinės protokolo dalis, replikavimas.

Apskritai tokio tipo bandomasis projektas rodo, kad blokų grandine grindžiamas automatizavimo potencialas gali padėti pasiekti didžiulį efektyvumo augimą atsiskaitant už daugiašalius sandorius ir mažinant tarp agentų esantį neapibrėžtumą. Pavyzdžiui, "ChromaWay" bandomajame projekte išmaniųjų sutarčių darbo eiga bent iš dalies pakeičia tradicinių notarų veiklą. Dabartinėje sistemoje notaras tikrina sandorio šalių tapatybę ir tikrina dokumentų bei parašų autentiškumą. Jis taip pat tikrina, ar šalių išsakyti teiginiai atitinka realaus pasaulio faktus ir laisvą valią. Naujojoje sistemoje šie elementai pateikiami automatiškai elektroniniu formatu.

Tačiau šis bandomasis projektas taip pat išryškina keletą kliūčių, kurios trukdo naudoti blokų grandinės technologiją sudėtingiems ir didelės vertės sandoriams, tokiems kaip nekilnojamojo turto perleidimo sandoriams. Pavyzdžiui, teikiant informaciją apie nekilnojamąjį turtą ir elektroninį naudotojų autentiškumo patvirtinimą paslauga vis dar priklauso nuo centralizuotų sistemų duomenų. Elektroninės tapatybės sistema turi būti pripažinta valdžios ir susieta su konkrečiais fiziniais ar juridiniais asmenimis. Taip pat kyla papildomų abejonių, ar be trečios patikimos šalies (pvz. notaro) galima užtikrinti elektroniniu būdu pateiktų duomenų tikrumą.

### 2.2.2 Tapatybės valdymas

Norint naudotis internetinėmis paslaugomis ar atlikti internetines operacijas, reikia, kad piliečiai atskleistų atitinkamą informaciją arba pateiktų tapatybės įrodymą. Paprastai iš piliečių reikalaujama pateikti finansinę ir asmeninę informaciją, kuri saugoma centralizuotose ar vyriausybės kontroliuojamose platformose arba duomenų bazėse. Daugelyje tokių duomenų bazių kyla rimtų saugumo problemų, apie kurias liudija žinios apie didelius pažeidimus, dėl kurių atskleidžiama naudotojų asmeninė informacija. Šiuo atžvilgiu, kas, kaip ir kokiais tikslais tvarko, saugo ir valdo tokius duomenis, yra naujausių ir tebevykstančių Europos reguliavimo iniciatyvų, įgyvendinamų pagal bendrosios skaitmeninės rinkos strategiją, pagrindas.

Blokų grandinės technologija galėtų padėti kurti naujus tapatybės ir prieigos valdymo sprendimus, nes būtų įdiegti decentralizuoti asmens tapatybės nuosavybės, valdymo, atstovavimo ir patvirtinimo modeliai. Kaip vieną tokio modelio naudojimo atvejų galima paminėti Šveicarijos Cugo savivaldybės

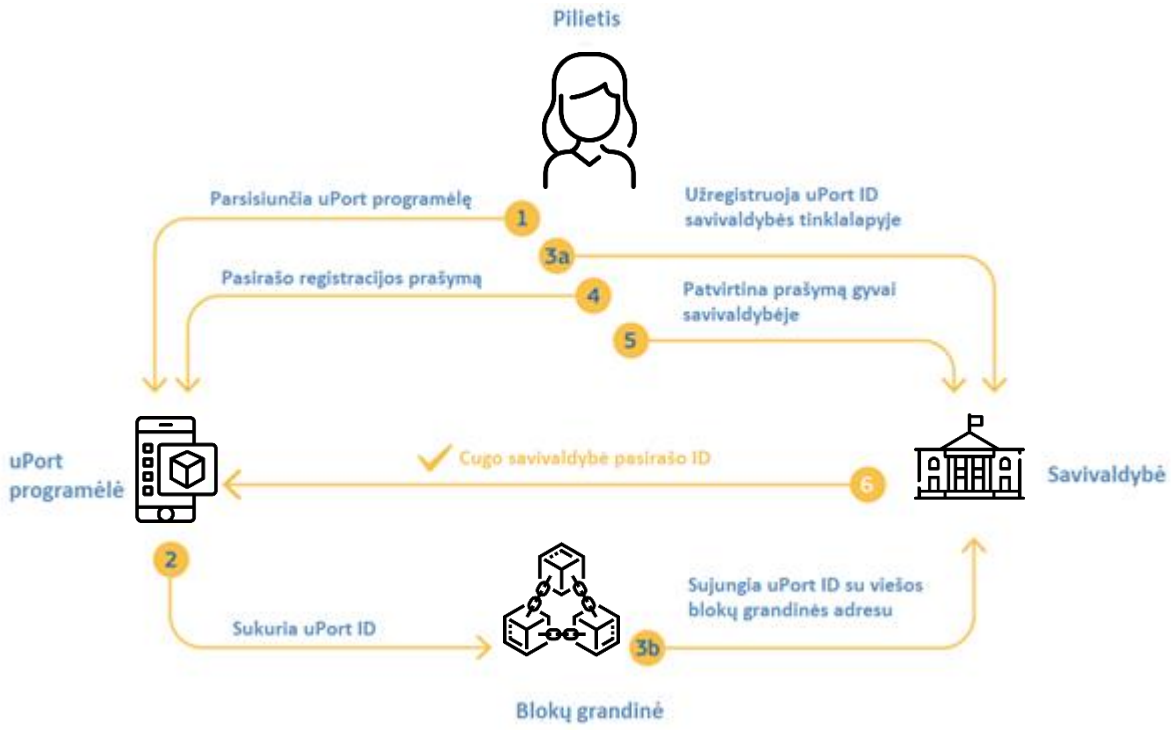
Ethereum sistemoje išduodamą skaitmeninę tapatybę pavadintą uPort. Šią tapatybę siekiama naudoti patikimoms ir savarankiškoms e. valdžios paslaugoms teikti, suteikiant piliečiams galimybę pasirinktinai atskleisti konkrečią informaciją konkrečioms įmonėms ir viešosioms paslaugoms.

Šiuo metu šiame ankstyvajame bandomajame etape, kuris prasidėjo 2017 m. lapkričio 15 d., teikiamas tik gyvenamosios vietos įrodymas, t. y. skaitmeninė, blokų grandine pagrįsta tapatybė, kurią patvirtino Cugo miesto Gyventojų kontrolė. Iki šiol užsiregistravo apie 300 iš 30 000 Cugo gyventojų, tačiau projekto tikslai yra  išsiplėsti ir į kitas vietos valdžios institucijų teikiamas viešąsias paslaugas tokias kaip apklausos, e. balsavimas, dviračių nuoma, knygų skolinimasis, mokesčių deklaravimas ir mokėjimai už automobilių stovėjimą.

Konsorciumas valdantis "uPort" taikomąją programą yra mišrios viešojo ir privačiojo sektorių struktūros, į kurią įeina "ConsenSys", "TI&M", Liucernos ekonomikos universiteto Cugo finansinių paslaugų institutas (IFZ) ir Cugo savivaldybė, dalis. Paslaugų ir technologijų plėtra priklauso nuo kitų viešųjų organizacijų, verslo ir uPort bei Ethereum atvirojo kodo bendruomenių.

Kaip veikia "uPort"? Programėlė sukuria unikalų ir nekeičiamą kriptografinį adresą blokų grandinėje ir susieja jį su vietine naudotojo pinigine, esančia išmaniajame telefone.

UPort tapatybės registravimo procesas pavaizduotas 6 paveiksle.




**6 pav. Tapatybės registravimo procesas „uPort“ projekte (Šveicarija, Cugas)**

1. Cugo gyventojai pirmiausia į mobilųjį telefoną atsisiunčia "uPort" programėlę;

2. Joje automatiškai sukuriama uPort tapatybė, kuri yra išmaniosios sutarties viešasis adresas Ethereum blokų grandinėje;

3. uPort ID užregistruojama Cugo savivaldybės interneto svetainėje, į kurią, kaip papildomą asmeninę informaciją, įrašo savo dabartinį Cugo asmens tapatybės numerį ir gimimo datą;

4. Naudojantis programėle, kriptografiškai pasirašomas registracijos prašymas, kuris siunčiamas į savivaldybę;

5. Einama į savivaldybę ir asmeniškai patvirtinamas prašymas;

6. Cugo savivaldybė kriptografiškai pasirašo ID ir automatiškai išsiunčia patvirtinimą į "uPort" programėlę.

Po šios procedūros "uPort" tapatybė pripažįstama kaip oficiali vyriausybės išduota tapatybė. Susiejimo procesą reikia atlikti tik vieną kartą. Šis bandomasis blokų grandinės projektas turi neabejotiną pridėtinės vertės potencialą.

Pirma, tikimasi sutaupyti veiklos sąnaudų, nes Cugo savivaldybė pereina nuo asmens duomenų saugojimo prie paprasto asmens tapatybės tikrinimo, kad galėtų teikti paslaugas.

Antra, tokio tipo blokų grandinės sistema gali sumažinti kibernetinių atakų riziką ir infrastruktūros išlaidas. Savarankiškos tapatybės sprendimas gali sumažinti poreikį įmonėms ir kitoms organizacijoms išlaikyti centralizuotas tapatybės informacijos saugyklas. Kai tapatybės nuosavybė ir jos patvirtinimas perduodamas piliečiams, sumažėja poreikis arba visai nebereikia serverių su centrinėmis duomenų bazėmis.

Galiausiai dėl naujų atestacijos formų piliečiai sutaupo laiko, kad galėtų naudotis paslaugomis. Jei paslaugų teikėjai, įmonės ir viešojo administravimo institucijos naudos uPort tapatybę, kad galėtų naudotis savo paslaugomis, tai gali padėti sutaupyti laiko, skirto konkrečioms tapatybėms kiekvienai iš šių paslaugų nustatyti ir tvarkyti. Taip pat būtų galima padidinti efektyvumą, kadangi paslaugoms nebereikėtų slaptažodžio ir jas būtų galima integruoti tarpusavyje, nes tapatybės nustatymo mechanizmai sutaptų.

Šio konkretaus bandomojo projekto išlaidos yra susijusios ir su kūrimu, ir su eksploatavimu. Nors projekto kūrimo ir valdymo išlaidos neatskleidžiamos, per 8 mėnesius sistemos integracijai buvo skirta apie 10 visos darbo dienos ekvivalentų. Kalbant apie eksploataciją, ateityje sistemai valdyti reikės tik savivaldybės tarnautojo. Tačiau sandorių kaina gali tapti svarbiu veiksniu, nes apskaičiuota, kad kiekvieno naujo vartotojo pridėjimas kainuos 105 JAV dolerius, jei bandomasis projektas bus perkeltas į pagrindinį Ethereum tinklą. Cugo mieste gyvena 30 000 gyventojų, kurių kiekvienam registracijai reikia transakcijos, tad išlaidos galėtų siekti 3 000 000 JAV dolerių. Kadangi pagrindiniame Ethereum tinkle išmaniųjų sutarčių siunčiami pareiškimai taip pat kainuoja brangiai, uPort tapatybės naudojimas gali pareikalauti papildomų išlaidų.

Apibendrinant, pagrindiniai projekto pliusai yra tai, kad "uPort" naudotojai gali pasirinktinai atskleisti informaciją šalims autentiškumui nustatyti ir taip geriau kontroliuoti savo tapatybę. Jie gali pasirinkti, kiek duomenų, kam ir kada juos atskleisti. Todėl iš esmės įmonės ir programėlės iš naudotojo

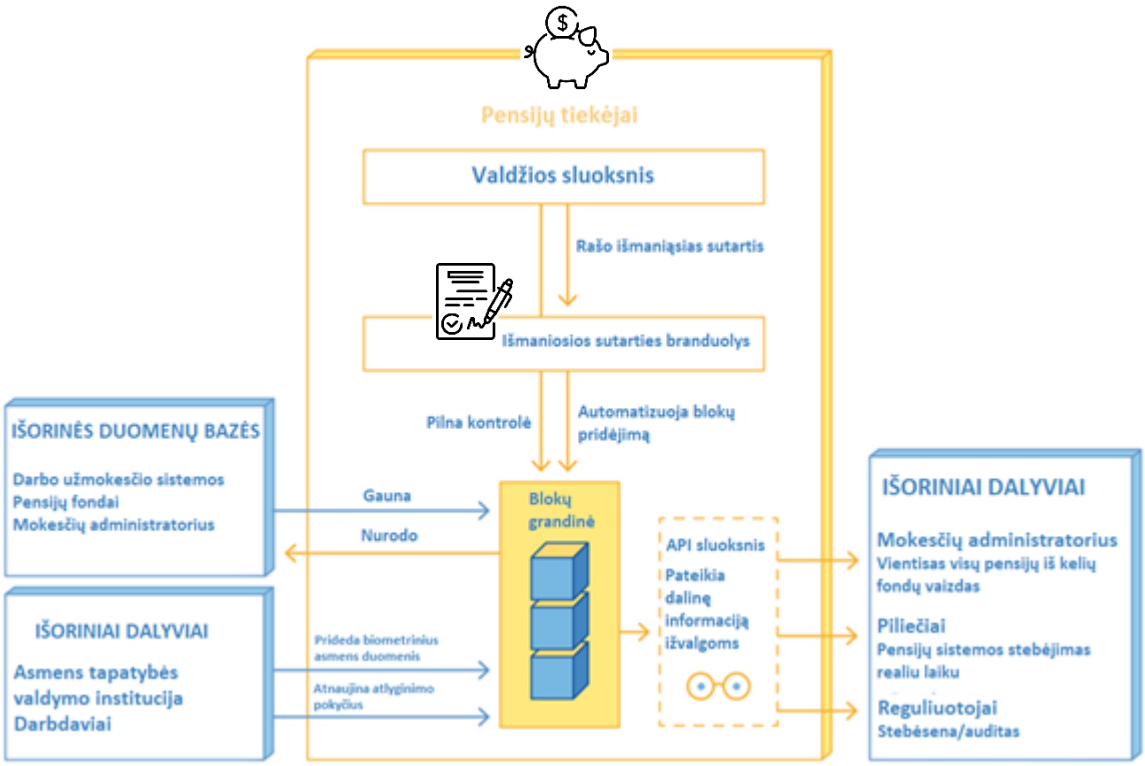
gauna tik minimalų asmens duomenų rinkinį, kaip numatyta BDAR. Be to, asmens duomenys saugomi saugiu, užšifruotu pavidalu mobiliajame įrenginyje. Atestatai visada siunčiami ne grandinėje ir juos autentifikavimui gali naudoti bet kuris paslaugų teikėjas ar viešoji įstaiga, todėl abi pusės padidina efektyvumą ir saugumą.

Cugo mieste vykdomas decentralizuotos tapatybės projektas "uPort" yra potencialaus blokų grandinės taikymo pavyzdys, leidžiantis piliečiams susikurti savarankišką tapatybę, kuri būtų patvirtinta ir pripažįstama valdžios. Projekte naudojamos išmaniosios sutartys, skirtos asmens duomenų valdymui ir kontroliuojamam dalijimuisi jais, ir tai yra puikus pavyzdys, kaip blokų grandinė gali būti naudojama siekiant suteikti piliečiams daugiau galių. Visgi, kaip ir šiuo atveju, decentralizuotai tapatybės sistemai vis tiek reikalinga lygiagrečiai egzistuojanti centralizuota, valstybei ar savivaldybei priklausanti sistema.

### 2.2.3 Viešųjų išmokų paskirstymas

Blokų grandinės sistemos gali užtikrinti didesnį viešojo finansavimo efektyvumą ir skaidrumą, ypač panaudojant paskirstytos registracijos, narystės valdymo, keitimosi informacija ir automatinio vykdymo naudojant išmaniąsias sutartis funkcijas. Veikdamos kaip decentralizuoti tinklai, blokų grandinės sistemos gali suteikti galimybę visiems dalyvaujantiems naudotojams (nuo viešojo administravimo institucijų ir privačių veiklos vykdytojų iki piliečių) valdyti savo sandorius.

Papildomas saugumas ir atskaitomybė, kuriuos užtikrina blokų grandinės sistemos, kaip klastojimams atsparūs įrašai, gali būti labai naudingi įvairioms valdžios sektoriaus paslaugoms, pradedant valstybės pagalba ir baigiant socialiniais pervedimais. Pavyzdžiui, vis sudėtingesnės profesinės karjeros, kai darbuotojai per savo gyvenimą turi kelis darbdavius ir darbo vietas, daro įtaką pensijų administravimui, nes būsimieji pensininkai dažnai dalyvauja keliose asmeninėse pensijų programose, kurias teikia įvairūs pensijų fondų teikėjai. 2018 m. APG ir PGGM, du didžiausi pensijų teikėjai Nyderlanduose, pradėjo bandomąjį projektą "Pensijų infrastruktūra", kuris yra bendruomenės pagrindu veikiantis pensijų administravimo blokų grandinės pavyzdys. Tikslas - įgyvendinti lankstesnę ir skaidresnę pensijų administravimo sistemą piliečiams, kartu pasiekiant gerokai mažesnes sąnaudas. Šiame bandomajame projekte dalyvauja įvairios suinteresuotosios šalys, įskaitant darbdavius, nacionalinę tapatybės tarnybą, mokesčių administratorių, darbo užmokesčio mokėtojus, pensijų fondus, paslaugų teikėjus ir piliečius. Apžvalga pateikta 7 paveiksle. Sistema teikia skirtingas funkcijas, atsižvelgiant į dalyvio vaidmenį. Pavyzdžiui, mokesčių institucijai ji suteikia vientisą konkretaus asmens įmokų, surinktų daugelyje pensijų fondų, vaizdą. Piliečiui ji realiuoju laiku suteikia informaciją apie jo pensijų sistemą ir pensijos likutį. Darbdaviai gali tiesiogiai vykdyti ir registruoti darbo užmokesčio pakeitimą. Reguliavimo institucijos neatlieka aktyvaus vaidmens, nors gali matyti kai kuriuos duomenis.




**7 pav. „Pensijų infrastruktūros“ projektas (Nyderlandai)**

Šiuo metu projektas yra koncepcijos įrodymo (angl.proof of concept) stadijoje, nes numatytos funkcijos dar yra neišbaigtos. Bandomasis atvejis pagrįstas APG darbuotojų pensijų fondu ir šiuo metu jame dalyvauja maždaug 5 000 naudotojų. Naudojama patobulinta Ethereum protokolo versija, kuri sukuria privačią blokų grandinės architektūrą. Tinklo mazgai yra žinomi mazgai, atstovaujantys infrastruktūroje dalyvaujančioms suinteresuotosioms šalims. Taigi, naudojamas blokų grandinės archetipas yra privatus su leidimais.

Šio blokų grandine pagrįsto bandomojo projekto nauda apima išlaidų taupymą pensijų administravimui, kuris tradiciškai reikalauja daug administravimo, patikrinimų, žmogiškojo darbo ir kopijavimo sudėtingoje aplinkoje su valdžios ir privataus sektoriaus sistemomis.

Dėl to patiriama daug išlaidų ir kyla duomenų sugadinimo rizika esamose duomenų bazėse. Apskaičiuota, kad naudojant blokų grandinę būtų galima sutaupyti 500 mln. eurų iš bendros, šiuo metu išleidžiamos 1 mlrd. eurų sumos. Šis bandomasis projektas taip pat gali padidinti efektyvumą, susijusį su paskirstytos duomenų bazės, kuri būtų pirminis ir vienintelis teisingos informacijos šaltinis visoms skirtingoms šalims, sukūrimu. Žvelgiant iš piliečių perspektyvos, sumažėja sandorių sąnaudos, nes informacija, nors ir paskirstyta, yra pasiekiama per vieną bendrą sąsają, pagrįstą asmeninės pensijos išmaniosiomis sutartimis. Šiuo metu apskaičiuota, kad vidutinės piliečių dalyvavimo pensijų fonduose išlaidos sudaro 80 EUR per metus, o siekiama jas sumažinti iki 15 EUR per metus.

Apibendrinant galima teigti, kad Nyderlanduose vykdomas “Pensijų infrastruktūros” bandomasis projektas skirtas visiems ekosistemos aspektams - nuo piliečių, kurie patys valdo savo pensijų sistemas,

iki automatinio mokesčių deklaravimo valdžios institucijoms. Bendros duomenų bazės ir darbo eigos automatizavimo funkcionalumas blokų grandinėje naudojamas siekiant užtikrinti didelį pensijų sistemos administravimo ir reguliavimo efektyvumą. Tačiau sistemos mastas ir sudėtingumas viršija dabartinius technologinius pasiekimus. Didelis sandorių kiekis, kuriuos reikia apdoroti naudojant išmaniąsias sutartis, yra didelis iššūkis. Nors visi dalyviai yra atstovaujami, šios infrastruktūros sudėtingumas reiškia, kad šis projektas vis dar yra labai ankstyvame savo gyvavimo ciklo etape.

Dar vienas blokų grandinės sistemų taikymas viešųjų išlaidų srityje yra susijęs su perskirstymo programų tikslingumu ir valdymu. Nuo 2016 m. Nyderlandų Groningeno savivaldybė, siekdama skatinti įtrauktį mieste, naudoja blokų grandinės infrastruktūrą, kad mažas pajamas turintiems žmonėms galėtų teikti paslaugas su nuolaida. Išmaniojoje sutartyje galima užprogramuoti išsamias išlaidų sąlygas, pavyzdžiui, reikalavimus atitinkančių gavėjų profilius, ribas, limitus ir įgaliotus paslaugų teikėjus. Tuomet šiuos išmaniuosius kuponus galima naudoti sporto klubuose, suteikiant galimybę lankytis baseinuose ar kino teatre arba subsidijuojant saulės baterijas namų savininkams.

Sistema veikia taip (žr. 8 pav.):

1. Pilietis kreipiasi į savivaldybę, nurodydamas savo vardą, pavardę, adresą ir asmens kodą;

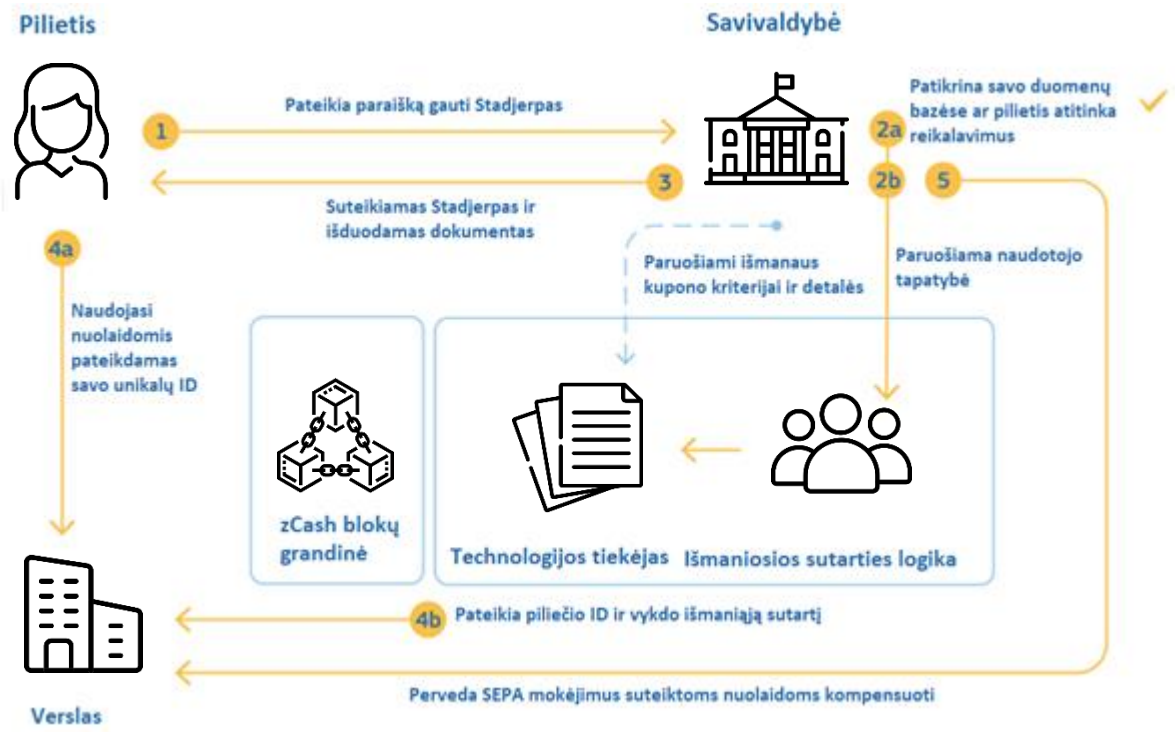
2. Savivaldybė patikrina, ar užsiregistravęs pilietis turi teisę gauti išmaniuosius talonus. Jei taip, savivaldybė blokų grandinėje nustato anoniminę naudotojo tapatybę, susietą su asmens duomenimis, saugomais už grandinės ribų;

3. Savivaldybė suteikia piliečiui pažymėjimą kartu su asmeniniu QR kodu, nurodančiu blokų grandine pagrįstos išmaniųjų kuponų sistemos ID;

4. Pilietis naudojasi dalyvaujančių įmonių paslaugomis, kurios nuskenuoja QR kodą, esantį ant pažymėjimo, kad aktyvuotų išmanųjį kuponą ir apskaičiuotų nuolaidą;

5. Po tam tikro laikotarpio savivaldybė įmonėms atlieka SEPA mokėjimus.

Programoje yra užsiregistravę daugiau kaip 20 000 piliečių ir paslaugų teikėjų, o kiekvieną mėnesį atliekama apie 4 000 išmaniųjų kuponų operacijų. Iš pradžių, kai 2015 m. buvo sukurta sistema, buvo naudojamas "Bitcoin" blokų grandinės protokolas. Tačiau dabar sistema perkelta į "Zcash", nes čia sandorių išlaidos yra gerokai mažesnės. Šiame blokų grandinės protokole sistema naudoja savo išmaniąsias sutartis. Saugomas kiekvienas sandoris, išskyrus tikrojo sandorio detales. Patvirtinimas atliekamas viešojoje blokų grandinėje, nors naudotojams, kurie gali sudaryti sandorius, suteikiami leidimai, todėl sistema yra viešoji blokų grandinė su leidimais.




**8 pav. Išmaniųjų kuponų sistema „Stadjerpas“ (Nyderlandai, Groningenas)**

Tikimasi, kad šis blokų grandinės diegimas turės daug teigiamų pasekmių, įskaitant viešųjų lėšų paskirstymo efektyvumo didinimą. Šis poveikis daugiausia pasireiškia viešosios atskaitomybės ir perskirstymo politikos požiūriu, nes programuojamieji išmanieji kuponai užtikrina, kad kiekvienas konkrečiam tikslui ir paramos gavėjui skirtas euras būtų išleistas tinkamai. Ji taip pat gali padidinti savivaldybės veiklos efektyvumą. Kadangi blokų grandinė sukuria viešą registrą tikrinimo ir audito tikslais, ji gali palengvinti automatinius mokėjimus. Tikimasi, kad savivaldybėje sumažės popierinių dokumentų ir žmonių darbo procedūrų poreikis.

Šie ir panašūs bandomieji projektai atskleidžia blokų grandinės sistemų potencialą valdant, nukreipiant ir skiriant socialines išmokas, dotacijas, subsidijas ar pagalbą, tokiu būdu užtikrinant, kad viešosios lėšos, rezervuotos konkrečiam tikslui, būtų skirtos tik šiam tikslui ir nukreiptos pageidaujamai naudos gavėjų grupei.

Išmaniosiomis sutartimis grindžiamo sprendimo privalumai - didesnė viešoji atskaitomybė ir galimybė atlikti viešųjų išlaidų auditą šioje srityje, nes iš anksto nurodoma, kad lėšos turi būti išleistos konkrečiose vietose, ir jų negalima nukopijuoti.

Be to, blokų grandinės naudojimas gali padidinti tokių programų saugumą, atsparumą ir informacijos skaidrumą. Jis pašalina vieno gedimo taško pažeidžiamumą, taip sumažindamas išorinės atakos riziką. Padidėja informacijos vientisumas, nes užpuolimo ar mazgo gedimo atveju duomenys vis tiek saugomi kituose mazguose. Taip pat padidėja duomenų patikimumas, nes sumažėja duomenų kopijavimas ir replikavimas tarp įvairių dalyvių, juos reikia įvesti tik vieną kartą. Be to, visiems dalyvaujantiems naudotojams užtikrinamas didesnis skaidrumas, nes kiekvienas sandoris yra įrašomas

ir vienpusiškai jo pakeisti neįmanoma. Dėl to reguliavimo institucijos gali atlikti visos sistemos apžvalgas be informacijos asimetrijos, kai viena sandorį sudaranti pusė žino daugiau negu kita.

### 2.2.4 Sertifikatai ir akreditacija

Žvelgiant į blokų grandinės taikymą švietimo srityje, ši technologija galėtų padėti aukštojo mokslo įstaigoms notariškai tvirtinti skaitmeninius sertifikatus ir diplomus. Tai būtų galima daryti didesniu mastu ir greičiu, skaidriau ir matomiau, o svarbiausia - iš karto pasitikėti pažymėjimais, kurie patvirtina į darbą pretenduojančio absolvento ar darbo ieškančio asmens gebėjimus. Galiausiai tai galėtų turėti įtakos studentų ir absolventų įsidarbinimo perspektyvoms ir profesinei karjerai.

Švietimo srityje sertifikatai ir diplomai naudojami patvirtinti, kad asmuo dalyvavo švietimo programoje ir (arba) pasiekė tam tikrus mokymosi rezultatus, kurie dažnai tikrinami taikant vertinimo praktiką. Pažymėjimai gali būti oficialūs (pvz. suteikiantys profesinę kvalifikaciją) arba neoficialūs (pvz., pažymėjimai, patvirtinantys lankomumą arba dalyvavimą mokymosi veikloje); jie taip pat gali būti įvairių formatų, pavyzdžiui, popieriniai arba skaitmeniniai. Akreditavimas švietimo srityje - tai procedūra, pagal kurią autoritetinga institucija (pvz. ministerija ar akreditavimo agentūra) suteikia organizacijai ar asmeniui teisę išduoti patikimą ir galiojantį sertifikatą ar pažymėjimą (diplomą), atitinkantį iš anksto nustatytus standartus ir kokybės užtikrinimo priemones.

Formos, kuriomis besimokantiesiems išduodami išsilavinimo pažymėjimai, keitėsi. Popieriniai sertifikatai turi tam tikrų apribojimų, kuriuos galėtų įveikti skaitmeninis ir blokų grandine registruojamas sertifikatas. Tarp jų, be kita ko, yra klastojimo rizika, pakeitimo išlaidos ir lėtas patikrinimas. Skaitmeninį, bet ne blokų grandinėje registruotą sertifikatą galima lengviau patikrinti ir atšaukti, tačiau jei jis neturi skaitmeninio parašo, jį taip pat galima suklastoti.

Net jei sertifikatas turi skaitmeninį parašą, jei šis parašas nėra pagrįstas atviru standartu, kurį galima visuotinai patikrinti, sertifikato tikrinimo procedūra gali būti užblokuota tam tikros programinės įrangos ekosistemų, o tai sumažina jo tinkamumą įvairiomis aplinkybėmis.

Savo ruožtu blokų grandinėje užregistruotą skaitmeninį sertifikatą gali patikrinti bet kuris asmuo, turintis prieigą prie blokų grandinės. Arba tai gali būti daroma naudojant automatinę atvirojo kodo tikrinimo sistemą, pavyzdžiui, "Blockcerts Universal Verifier". Šis atvirasis akademinių įrašų standartas naudojamas 2017 m. spalį Maltos vyriausybės pradėtame bandomajame projekte.

"Blockcerts", naudodamasis blokų grandinės infrastruktūra, daugiausia dėmesio skiria visiems vertės grandinės aspektams: sertifikatų kūrimui, išdavimui, peržiūrai ir tikrinimui (Inamorato dos Santos, 2017).

Procesą sudaro šie etapai (žr. 9 pav.):

1. Universitetas siunčia piliečiui prašymą atsisiųsti "Blockcerts" programėlę;

2. Pilietis įsidiegia programėlę ir pripažįsta universitetą kaip emitentą, kartu sukurdamas privatų ir viešąjį raktą;

3. Programėlė "Blockcerts" siunčia piliečio viešąjį raktą universitetui;

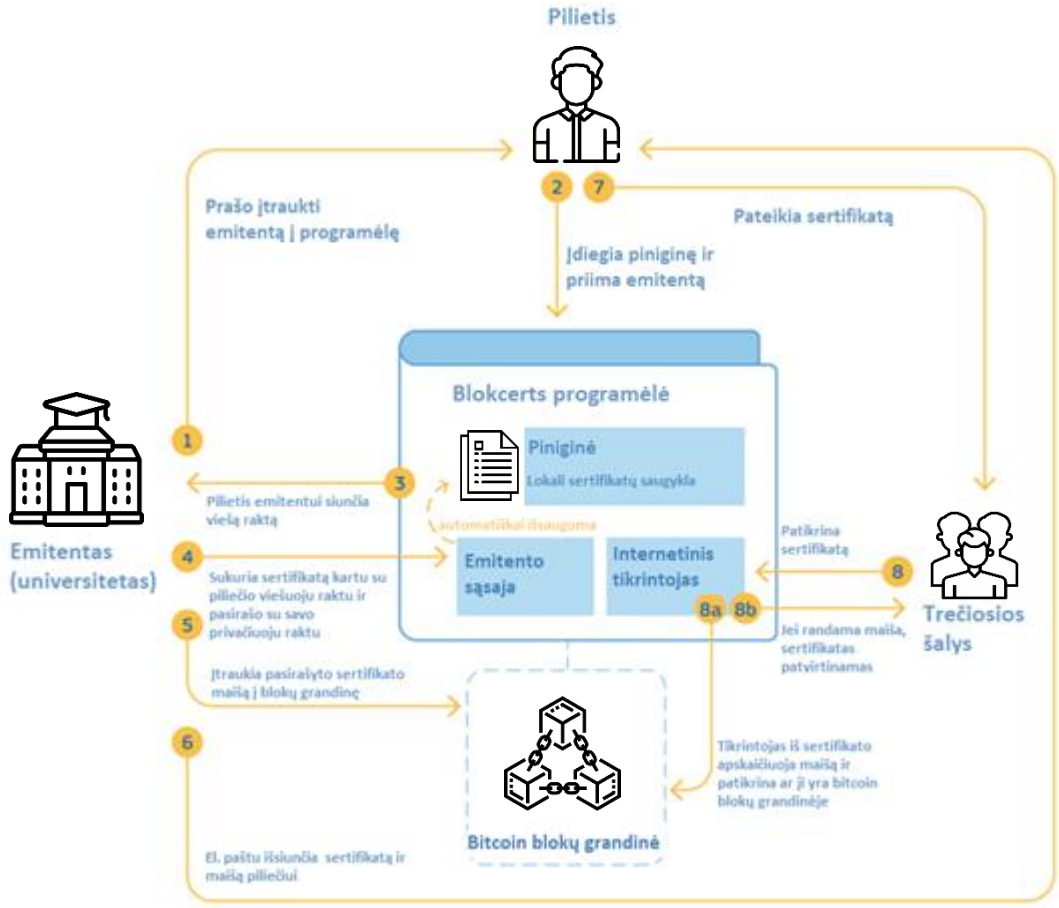
4. Universitetas sukuria skaitmeninį sertifikatą, įskaitant piliečio viešąjį raktą, "Blockcerts" emitento sąsajos programoje. Šis sertifikatas pasirašomas universiteto privačiuoju raktu;

5. Universitetas sertifikatą pakeičia maišos kodu "Blockcerts" emitento aplinkoje ir išsaugo maišos kodą "Bitcoin" blokų grandinėje;

6. Universitetas piliečiui el. paštu išsiunčia sertifikatą ir blokų grandinėje saugomą maišos kodą;

7. Pilietis gali pateikti sertifikatą ir internetinę nuorodą tretiesiems asmenims;

8. Trečiosios šalys įveda sertifikatą ir internetinės nuorodos adresą į "Blockcerts" internetinį tikrintuvą, kuris patikrina, ar sertifikato maišos kodas sutampa su "Bitcoin" blokų grandinėje įrašytu maišos kodu. Jei maišos kodas randamas, sertifikatas patvirtinamas. Tokiu būdu trečioji šalis gauna dokumento originalumo įrodymą.




**9 pav. Sertifikatų patikrinimo procesas „Blockcerts“ projekte (Malta)**

Apibendrinant galima pasakyti, kad blokų grandine pagrįstam sertifikatui ar diplomui patvirtinti nereikia jokių tarpinių šalių.

Net jei akredituota išduodančioji organizacija laikui bėgant išnyksta, šį sertifikatą vis tiek galima patikrinti. Taip pat blokų grandinėje skelbiamas tik sertifikato maišos kodas, o paties dokumento skelbti nereikia, taip išsaugant dokumento privatumą.

Galimybė vietoje patikrinti ir patvirtinti įgaliojimus, kurią suteikia blokų grandinė, gali sumažinti biurokratines procedūras, kurios kitu atveju švietimo įstaigoms, darbdaviams, absolventams ir darbo ieškantiems asmenims užimtų daug laiko. Tai taip pat gali sumažinti socialinės (ir švietimo) atskirties riziką asmenims, kilusiems iš konfliktų zonų, pavyzdžiui, tam tikroms migrantų ir pabėgėlių grupėms. Teoriškai blokų grandinės sistemos naudojimas gali leisti šiems asmenims išsaugoti ir tvarkyti savo tapatybę ir įrašus, pavyzdžiui, akademines pažymas, sertifikatus, diplomus, formaliojo ir neformaliojo mokymosi dokumentus. Be to, blokų grandinėje esančių tokių įrašų atsparumo klastojimui principas leidžia suinteresuotosioms šalims jais pasitikėti.

Jungtinės Karalystės Atvirojo universiteto susidomėjimas blokų grandine neapsiriboja vien skaitmeninių sertifikatų ir diplomų studentams išdavimu, bet ir siekia išsiaiškinti, kaip universitetas galėtų padėti absolventams gauti kuo didesnę naudą iš savo diplomų, kad pagerintų jų finansines ir socialines sąlygas, todėl daugiausia dėmesio skiriama mikroakreditavimui naudojant ženkliukus. Projekto esmė- suteikti studentams, kurie išklausė tam tikrą žinių modulį ar paskaitų grupę, virtualų “ženkliuką”, kuris įtraukiamas į blokų grandinę. Tokiu būdu potencialūs darbdaviai gali iš anksto ieškoti būsimų darbuotojų pagal tam tikrus gebėjimus arba nusamdyti juos, nelaukiant galutinio studento diplomo.

Iššūkis šiame projekte yra tas, kad šis potencialas taps realybe tik plečiant bendradarbiavimą. Turi bendradarbiauti visos suinteresuotosios šalys: studentai, aukštojo mokslo institucijos, valdžia ir privatusis sektorius. Todėl ES finansuojamu projektu QualiChain siekiama sukurti, išbandyti ir įvertinti decentralizuotą švietimo ir darbo kvalifikacijų saugojimo, dalijimosi ir tikrinimo platformą, daugiausia dėmesio skiriant blokų grandinės technologijos galimybėms.

Bendrieji švietimo bendruomenės tyrimų teiginiai blokų grandinės adresu rodo, kad švietimo sistemos gali tikėtis eros, kai studentai galės visiškai kontroliuoti savo duomenis, akademinius įrašus, sertifikatus, stenogramas, kursų darbus ir vertinimą. Tokia individuali savo duomenų kontrolė dažnai vadinama "savarankiška tapatybe". Tai reiškia, kad ilgainiui studentai nebebus priklausomi nuo įvairių paslaugų, kurias paprastai teikia aukštojo mokslo institucijos. Taigi, žvelgiant iš šios perspektyvos, tikimasi, kad aukštojo mokslo institucijos turės nuolat atsinaujinti, kad neatsiliktų nuo šio sparčiai besikeičiančio pasaulio, kurį lemia potencialiai perversmą galinčių sukelti technologijų, tokių kaip blokų grandinės, pažanga.

# 3. BLOKŲ GRANDINĖS TECHNOLOGIJA PAREMTŲ PROJEKTŲ EMPIRINĖ ANALIZĖ

## 3.1 Empirinio tyrimo metodologija

**Tyrimo tikslas** – identifikuoti ir pagal nustatytus kriterijus empiriškai įvertinti Europos šalių viešojo sektoriaus projektus, kurie naudoja blokų grandinės technologiją.

**Tyrimo uždaviniai:**

1. Įvertinti blokų grandinės naudojimo mastą pasaulio ir Europos šalyse.
2. Nustatyti blokų grandinės technologijos naudojimo teikiamą naudą skaitmeninės valdžios ir piliečių atžvilgiu.

Buvo atliekamas **kombinuotas tyrimas**, taikant **kokybinio ir kiekybinio tyrimo strategijas**.

**Tyrimo atranka.** Tyrimo imties sudarymui pasirinkta netikimybinė tikslinė atranka**.**

**Tyrimo imtis**- Europos šalių viešojo sektoriaus blokų grandinės technologija paremti projektai. Pasirinkta tokia **strategija** todėl, kad nesvarbu kuo užsiima įmonės, svarbu ar jos naudoja blokų grandinės sistemas savo sprendimuose.

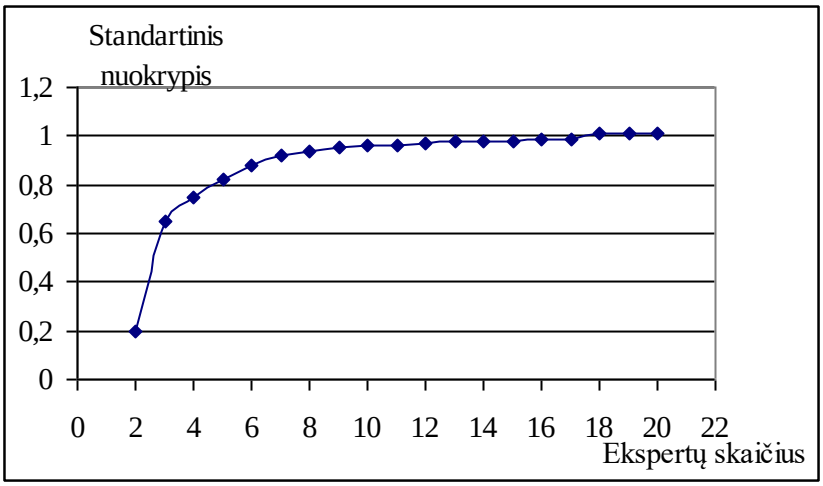
**Tyrimo etapai.** Pirmu etapu analizuojamos blokų grandinės sistemos įvairiais aspektais pasaulio ir Europos kontekste pasitelkiant viešai prieinamus informacijos šaltinius. Antru etapu nagrinėjami Europos šalių viešojo sektoriaus blokų grandinės technologija paremti projektai. Tyrimui atlikti pasirinkti mokslinės literatūros analizės ir struktūruoto interviu metodai.

**Tyrimo organizavimas.** Kadangi kokybinius ir kiekybinius ekspertinius vertinimus gali išreikšti individualūs ekspertai, organizacijų atstovai, organizacijų oficialūs požiūriai (ataskaitos, pranešimai, oficialūs dokumentai ir kt.), be to pakankamas ekspertų skaičius kiekybiniuose vertinimuose – 7–10 ekspertų, o kokybiniuose vertinimuose gali būti ir mažesnis (Baležentis, Žalimaitė, 2011, p. 30), todėl tyrimas buvo atliekamas apklausiant įvairių Europos šalių viešojo sektoriaus blokų grandine paremtų projektų atstovus arba analizuojant oficialius projektų dokumentus (angl. whitepaper) ir/arba pranešimus. Pirminis projektų kandidatų sąrašas buvo sudarytas remiantis viešai prieinamais šaltiniais: ekspertų tinklaraščiais, naujienų straipsniais, moksliniais straipsniais susijusiais su blokų grandine viešajame sektoriuje. Apribojus sąrašą iki Europoje įgyvendinamų projektų sąrašas sutrumpėjo iki septynių:

- Projektas „Exonum“ (žemės registras, Sakartvelas);
- Projektas „Blockcerts“ (akademiniai kredencialai, Malta);
- Projektas „Chromaway“ (nekilnojamojo turto sandoriai, Švedija);
- Projektas „uPort“ (decentralizuota tapatybė, Šveicarija);
- Projektas „Infrachain“ (valdymo sistema, Liuksemburgas);

- Projektas „Pensijų infrastruktūra“ (socialinės išmokos, Nyderlandai);
- Projektas „Stadjerspas“ (išmanieji kuponai, Nyderlandai).

Klasikinėje testų teorijoje teigiama, kad agreguotų sprendimų patikimumą ir priimančių sprendimą (šiuo atveju ekspertų) skaičių sieja greitai gęstantis netiesinis ryšys (žr. 10 pav.) ir yra įrodyta, jog agreguotų ekspertinių vertinimų moduliuose su vienodais svoriais nedidelės ekspertų grupės sprendimų ir vertinimų tikslumas nenusileidžia didelės ekspertų grupės sprendimų ir vertinimų tikslumui, todėl toks ekspertų skaičius yra priimtinas (Baležentis, Žalimaitė, 2011).




**Šaltinis:** Baležentis, Žalimaitė, 2011, p. 25; Libby, 1978.

**10 pav. Ekspertų vertinimų standartinio nuokrypio priklausomybė nuo ekspertų skaičiaus**

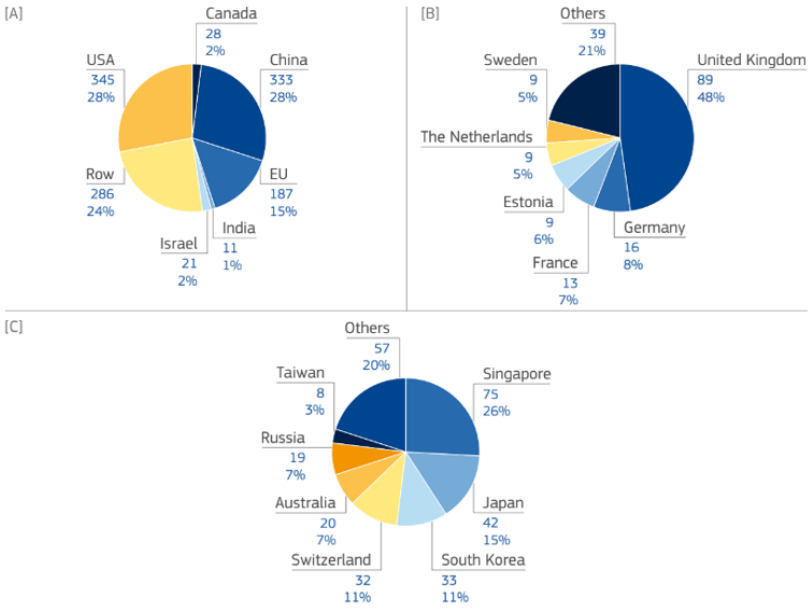
**Tyrimo reprezentatyvumas.** Dėl blokų grandinės technologijos naujumo ir specifinių pritaikymo galimybių tyrimas nėra statistiškai reikšmingas, nes blokų grandinės technologijos įsisavinimo lygis viešajame sektoriuje kol kas vyksta tik tarp inovatorių ir ankstyvųjų įsisavintojų (angl. early adopters), t.y. iki 16% visų potencialiai galinčių naudoti technologiją, pagal inovacijų difuzijos teoriją (Rogers&Shoemaker, 1971).

## 3.2 Tyrimo duomenų analizė

Blokų grandinė neapsiriboja tik finansinėmis programomis ir įgauna populiarumą daugelyje kitų sektorių. Tikimasi, kad tai bus viena iš technologijų, kurios padarys didžiulį poveikį per ateinančius 10-15 metų. Jos iškilimą liudija staigus blokų grandinės pradedančiųjų įmonių skaičiaus augimas ir jų finansavimo apimtys. Didžiulis finansavimas prasidėjo 2014 m. ir sparčiai auga iki šiol. Pirminiai monetų siūlymai (ICO) skatino blokų grandinės startuolių ekosistemos finansavimą, tuo pačiu didėjantys rizikos kapitalo srautai į šį sektorių reiškia ir didėjančią šios verslo srities brandą. Jaučiama stipri konkurencija tarp JAV ir Kinijos, o Jungtinė Karalystė kartu su Vokietija, Prancūzija, Nyderlandais ir

Estija atlieka svarbų vaidmenį Europoje. Šveicarija ir Singapūras taip pat pasižymi ypatingu dinamiškumu, po jų seka Japonija ir Pietų Korėja.

2018 m. gruodžio 31 d. duomenimis, daugiausia blokų grandinės įmonių buvo įsteigta JAV, po jų seka Kinija. ES šioje klasifikacijoje atsilieka - jos dalis pasaulinėje blokų grandinės įmonių ekosistemoje sudaro tik 15 % (žr. 11 pav., A skydelį).




Šaltinis: Venture Sources – Dow Jones

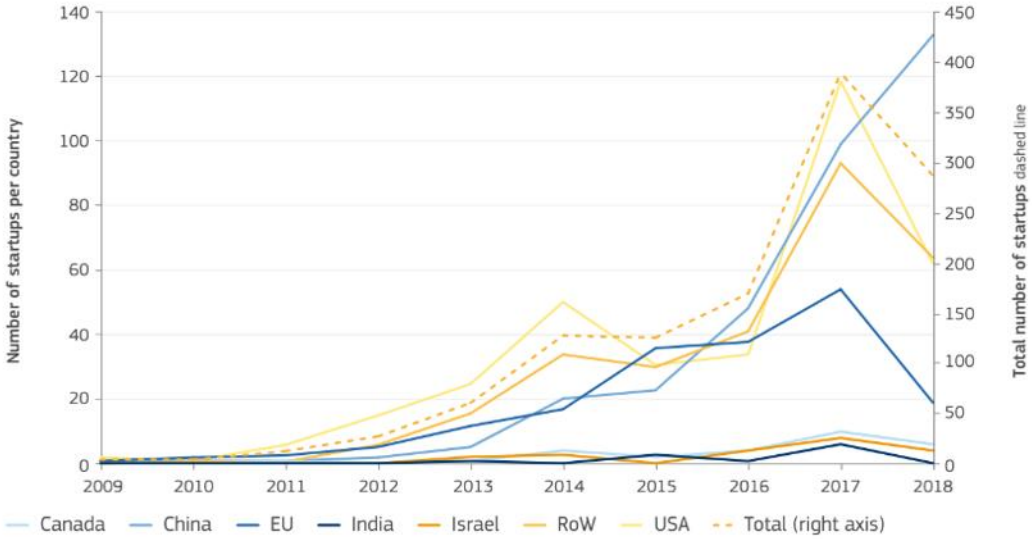
**11 pav. Blokų grandinės startuoliai, įkurti 2009-2018 metais**

**[A] Pasaulyje; [B] Europoje; [C] Likęs pasaulis (be A dalies)**

Skydelyje B pateikiamas bendras blokų grandinės pradedančiųjų įmonių skaičius ES valstybėse narėse. Jungtinėje Karalystėje veikia beveik pusė ES blokų grandinės pradedančiųjų įmonių, po jos eina Vokietija, Prancūzija ir Estija, kurių dalys atitinkamai sudaro 8 %, 7 % ir 6 %.

Skydelyje C pateikiamas naujų įmonių skaičiaus pasiskirstymas pagal likusį pasaulį išskyrus Kanadą, Kiniją, ES, Indiją, Izraelį ir JAV. Šiuo atžvilgiu Singapūras, Japonija, Pietų Korėja, Šveicarija, Australija ir Rusija išsiskiria tuo, kad jose veikia dviženklis skaičius blokų grandinės pradedančiųjų įmonių. Bene ryškiausias pastebėjimas, kuris matyti iš 11 paveikslo yra tas, kad apskritai blokų grandinės ekosistemos daugiausia klesti išsivysčiusios ekonomikos šalyse.

Naujų blokų grandinės pradedančiųjų įmonių atėjimo į rinką dinamika tarp pagrindinių pasaulio žaidėjų iliustruojama 12 paveiksle. Nuo 2010 m. iki 2017 m. visame pasaulyje kasmet sparčiai augo naujų startuolių, pradedančių veiklą blokų grandinės pramonėje, skaičius - vidutiniškai 40 % per metus (punktyrinė linija). Šis augimas ypač akivaizdus JAV, Kinijoje ir Europoje. 2018 m. tokių startuolių smarkiai sumažėjo visame pasaulyje išskyrus Kiniją, kurioje 2018 m. buvo užregistruota daugiau startuolių nei ankstesniais metais.



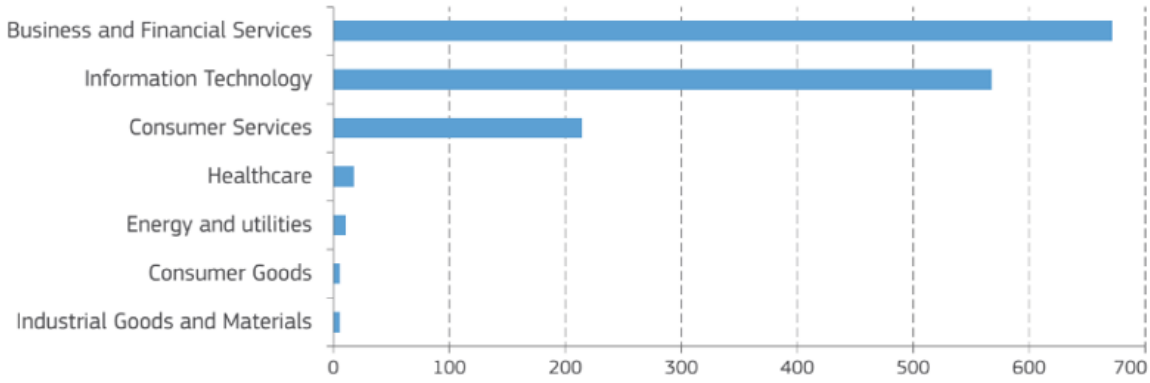

Šaltinis: Venture Sources – Dow Jones

**12 pav. Blokų grandinės startuolių tendencijos**

Nors ši mažėjimo tendencija 2019-2021 m. globaliu mastu nepasitvirtino, tačiau blokų grandinės startuolių skaičiaus pasiskirstymas pagal valstybes kinta gana intensyviai (stipriai didėja JAV, mažėja arba nežymiai didėja likusiame pasaulyje) todėl tai gali reikšti, kad pasauliniu mastu blokų grandinės startuolių atžvilgiu pramonė artėja prie prisotinimo taško.

Šią hipotezę patvirtina neseniai įvykęs perėjimas nuo sutelktinio finansavimo ir ICO prie reguliuojamų ir institucionalizuotų finansavimo formų, pavyzdžiui, rizikos kapitalo. Šis finansavimo struktūros pokytis rodo, kad (vis dar didėjančios) investicijos dabar daugiausia skiriamos jau įsteigtoms įmonėms, kad būtų finansuojamas sėkmingų projektų plėtros etapas.

Pasauliniame blokų grandinės startuolių vaizde pagal pagrindines ekonominės veiklos rūšis (13 pav.) ypač dominuoja du sektoriai: "Verslo ir finansinių paslaugų" (672 įmonės) ir "Informacinių technologijų" (568 įmonės).

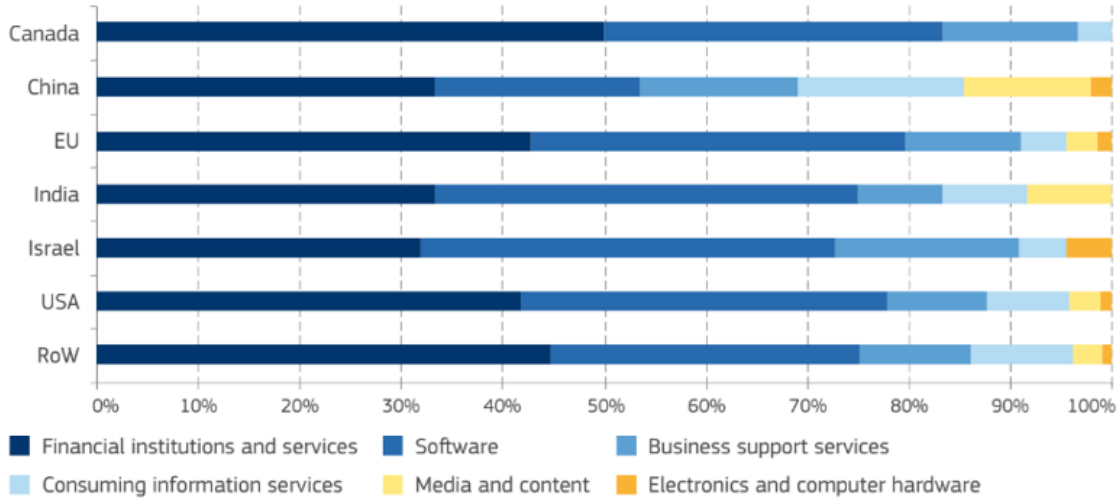



Šaltinis: Venture Sources – Dow Jones

**13 pav. Blokų grandinės startuolių skaičius pagal sektorius**

Pirmasis sektorius apima įmones, kurios užsiima mokėjimais ir sandorių apdorojimu, investicinėmis paslaugomis, duomenų valdymu, reklama ir rinkodara. Antroji grupė apima IT įmones, kuriančias programinę įrangą verslo taikomosioms programoms, vertikaliųjų rinkų taikomosioms programoms, tinklų valdymui, duomenų bazėms, taip pat poilsiui ir sveikatos priežiūrai. Blokų grandinės startuoliai taip pat priskiriami "Vartotojų paslaugų" sektoriui (215), kuriame teikiamos paslaugos, susijusios su internetinėmis bendruomenėmis, bendrąja žiniasklaida ir turiniu, apsipirkimo palengvinimu, taip pat švietimu, mokymu ir pramogomis.

14 pav. pateikiami pagrindinių pasaulio rinkos dalyvių blokų grandinės startuolių profiliai, pagrįsti išsamesne pramonės klasifikacija. Pramonės profiliai yra gana vienodi trijuose pagrindiniuose regionuose: JAV, ES ir likusiame pasaulyje.



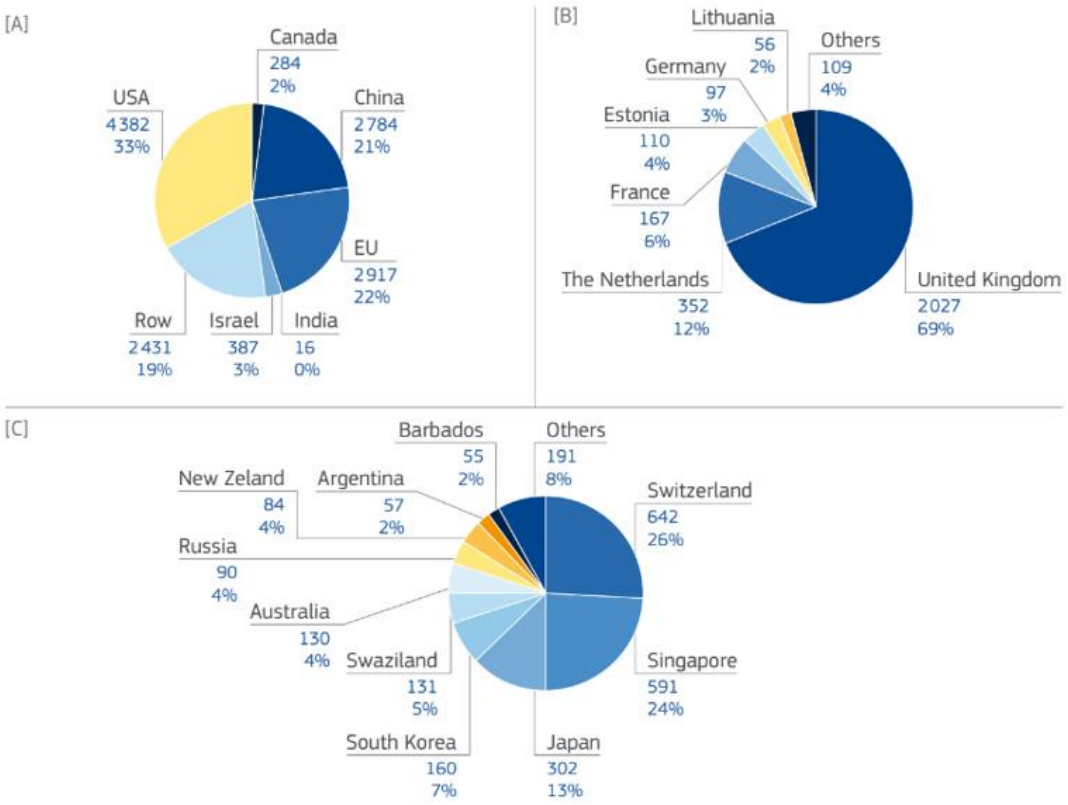

Šaltinis: Venture Sources – Dow Jones

**14 pav. Blokų grandinės startuolių pasiskirstymas pagal sektorius**

Daugiau nei 70% šių regionų startuolių kuria finansines paslaugas arba programinę įrangą. Dar 10% įmonių priskiriamos verslo paramos paslaugų sektoriui. Kinijoje, kuri pirmauja pagal startuolių skaičių, profilis yra įvairesnis ir labiau subalansuotas: apie 12% pradedančiųjų įmonių veikia žiniasklaidos ir turinio sektoriuje, o apie 16% - vartotojų informavimo paslaugų sektoriuje. Apskritai JAV ir ES blokų grandinės įmonės yra gana koncentruotos tik keliose pramonės kategorijose, orientuotose į programinės įrangos kūrimą, taip pat finansines ir verslo paslaugas, o Kinijos įmonės daugiau dėmesio skiria blokų grandinės taikomosioms programoms su vartotojais susijusiose srityse.

15 paveikslo A dalyje pavaizduotos pasaulinės sumos (mln. eurų), investuotos į blokų grandinės pradedančiąsias įmones tarp pagrindinių pasaulio žaidėjų 2009-2018 m. Daugiausia lėšų gavo JAV įmonės - iš viso 4,4 mlrd. ES įmonės gavo 2,9 mlrd. eurų investicijų, po jų rikiuojasi Kinijos pradedančiosios įmonės (2,8 mlrd. eurų). Apskritai per visą laikotarpį visų rūšių finansavimas, įskaitant rizikos šaltinių fondus, dotacijas ir ICO, visame pasaulyje viršijo 13,1 mlrd. eurų. Kituose regionuose

(likusiame pasaulyje, Kanadoje ir Izraelyje) įsisteigusioms bendrovėms tenka tik 23% pasaulinių investicijų į blokų grandinės pradedančiąsias įmones.




Šaltinis: Venture Sources – Dow Jones

**15 pav. Pritrauktas finansavimas 2009 m. – 2018 m.**

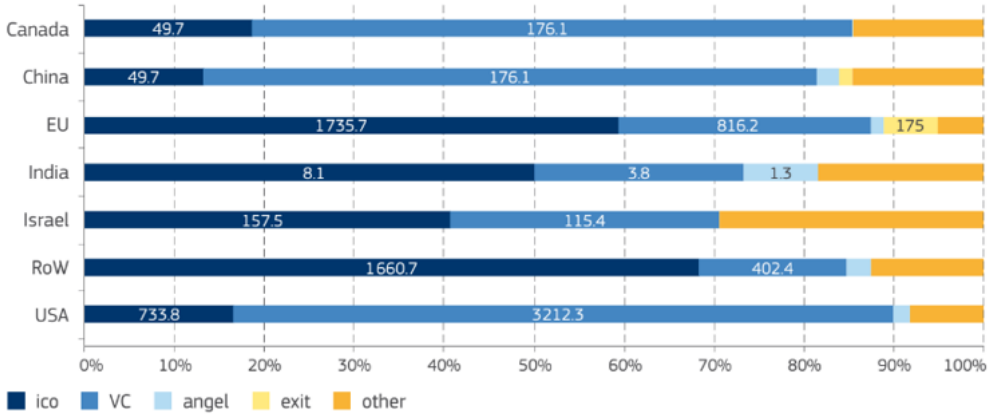
**[A] Pasaulis; [B] Europa; [C] Likęs pasaulis (be A dalies)**

Skydelyje B pateikiamas investicijų paskirstymas pagal ES valstybes nares. Jungtinės Karalystės dominuojantis vaidmuo yra dar akivaizdesnis nei 11 pav. pateikto blokų grandinės įmonių skaičiaus atveju. Jungtinėje Karalystėje įsteigtos įmonės gavo beveik 70% viso ES finansavimo. Toliau rikiuojasi Nyderlandai, kurių blokų grandinės pradedančiųjų įmonių finansavimas siekia 352 mln. eurų. Prancūzijos įmonės gavo 167 mln. eurų, po jų eina Estija ir Vokietija (atitinkamai 110 ir 97 mln. eurų).

Skydelyje C pateikiamos likusio pasaulio įžvalgos. Daugiausia lėšų pritraukė Šveicarijos, Singapūro, Japonijos, Pietų Korėjos, Svazilando ir Australijos blokų grandinės startuoliai (atitinkamai 642, 591, 302, 160, 131 ir 130 mln. eurų). Įdomu tai, kad tik šešios besivystančios šalys įtrauktos į sąrašą virš 50 mln. eurų ribos: Svazilandas, Estija, Rusija, Argentina, Lietuva ir Barbadosas, o tai patvirtina ankstesnį pastebėjimą, kad blokų grandinės technologija daugiausia kuriama ir finansuojama išsivysčiusiose šalyse.

16 paveiksle apžvelgiama finansavimo mechanizmų, pagal kuriuos investuojama į blokų grandinės startuolius, struktūra. Du didžiausi šaltiniai yra rizikos šaltinių fondai (6 634 mln. EUR) ir ICO (4 716 mln. EUR). Nemažai lėšų skyrė viešosios ir privačios dotacijos bei akceleravimo fondai (1 369 mln.

EUR). Atrodo, kad verslo angelų vaidmuo blokų grandinės bendrovėse yra labai mažas (257 mln. EUR). Pažymėtina, kad išėjimo iš investicijų į blokų grandinės įmones per įsigijimus, išpirkimus ar pirminius viešuosius siūlymus beveik nėra. Tai rodo, kad blokų grandinės technologijos rinkos vertės kūrimas vis dar yra ankstyvoje stadijoje.



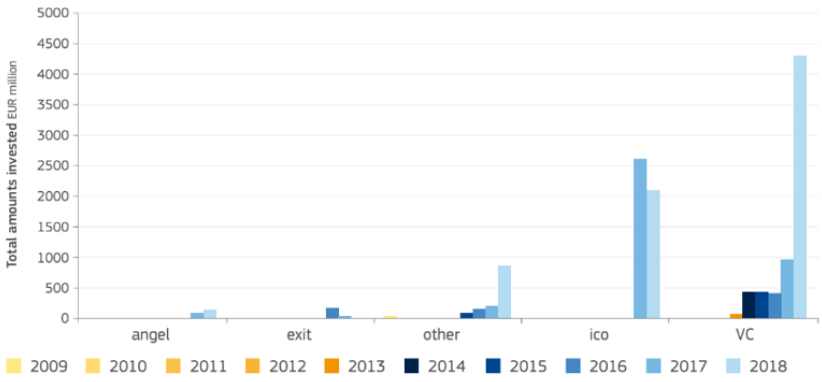

Šaltinis: Venture Sources – Dow Jones

**16 pav. Pritrauktos investicijos naudojantis įvairiais finansavimo instrumentais**

Vertinant šių dviejų dominuojančių šaltinių proporcijas įvairiuose geografiniuose regionuose, akivaizdu, kad JAV, Kanadoje ir Kinijoje, kur rizikos kapitalas sudaro 66-73% visų investicijų, yra svarbiausias. Kita vertus, Indijos, ES ir kitų pasaulio šalių blokų grandinės startuoliai daugiausia pasikliauja ICO, kuriems tenka 50-68 % viso finansavimo.

Rizikos kapitalo ir ICO vaidmenų pasikeitimas yra ryškiausias JAV ir ES skirtumas, susijęs su kapitalo pasiūla blokų grandinės startuoliams.

17 pav. pateikiama pasaulinių investicijų srautų į blokų grandinės startuolius dinamika pagal įvairias finansavimo priemones. Reguliarios investicijos į blockchain startuolius prasidėjo 2014 m. Iki 2016 m. pabaigos blokų grandinės įmonės gavo finansavimą daugiausia iš rizikos kapitalo, taip pat iš dalies iš dotacijų, nors bendras investicijų lygis buvo nedidelis. Nuo 2014 m. iki 2016 m. bendra investicijų suma kasmet augo 30-40% ir 2016 m. pasiekė 720 mln. eurų iš visų priemonių.




Šaltinis: Venture Sources – Dow Jones

**17 pav. Investicijų pasiskirstymas pagal skirtingus finansavimo instrumentus**

2017 m. investicijos į blokų grandinės startuolius išaugo iki 3,9 mlrd. eurų. ICO tais metais buvo svarbiausia priemonė (2,6 mlrd. EUR) ir pagrindinė pradedančiųjų įmonių ekosistemos varomoji jėga. ICO pats savaime tapo įgalintas blokų grandinės technologijos ir naudoja kriptovaliutas finansuoti visų rūšių pradedančiąsias įmones, kurios išleidžia savo žetonus.

2018 m. per ICO ir rizikos kapitalo fondus į blokų grandinės pradedančiąsias įmones toliau plaukė didelis finansavimas, kuris iš viso siekė 7,4 mlrd. eurų. Pažymėtina, kad tais metais taip pat gerokai išaugo dotacijų ir nuosavo kapitalo tipo finansavimas (968 mln. EUR). Tai rodo, kad kartu su rizikos kapitalu vyko akivaizdus perėjimas prie labiau institucionalizuotų, profesionalesnių ir taip pat labiau koncentruotų investuotojų dalyvavimo ir kontrolės formų blokų grandinės pramonėje. Įdomu tai, kad 2017-2018 m. vidutinė suma vienam rizikos kapitalo raundui smarkiai išaugo nuo 8 iki 15 mln. eurų, o vidutiniškai kiekvienas ICO abiem metais suteikė stabilias, bet didesnes sumas (atitinkamai 26 ir 28 mln. eurų).

**Apibendrinant pasaulines blokų grandinės tendencijas galima teigti, kad:**

-Blokų grandinės startuoliai pradėjo kurtis 2009 m. Po kelerių metų pasaulio investuotojai atkreipė dėmesį į blokų grandinės bendroves. Pirmosios didelės investicijos iš rizikos kapitalo fondų (412 mln. EUR) buvo gautos 2014 m.;

-Blokų grandinės technologijos populiarėjimą rodo tiek staigus blokų grandinės įmonių skaičiaus augimas, tiek joms skiriamo finansavimo apimtys;

-2014 m. pradėtas didžiulis finansavimas - 450 mln. eurų, jis sparčiai didėjo ir 2017 m. pasiekė 3,9 mlrd. eurų, o 2018 m. - daugiau kaip 7,4 mlrd. eurų. 2017 m. investuoto kapitalo suma išaugo neregėtu mastu dėl ICO sprogimo ir rizikos kapitalo investicijų, kurios ir toliau sparčiai auga.

-ICO - tai nauja finansavimo forma, kurią įgalino blokų grandinės technologija. Ji naudoja kriptovaliutas, kad finansuotų ankstyvojo etapo veiklą pradedančiųjų įmonių, kurios išleidžia savo ne nuosavybės žetonus. ICO buvo pradinė jėga, 2017 m. lėmusi didelį finansavimą blokų grandinės pradedančiųjų įmonių ekosistemai.

-Nors ICO yra ne kapitalo pritraukimo priemonė, skirta naujoms idėjoms išjudinti, tačiau didėjantis rizikos kapitalo srautas į šį sektorių reiškia didėjančią blokų grandinės projektų verslo brandą. Tikėtina, kad profesionalesnių ir institucionalizuotų investuotojų dalyvavimas turės įtakos tolesnei ekosistemos plėtrai, pradedant produktų ir platformų pasirinkimu ir baigiant strateginiais susivienijimais ir tarptautine konkurencija.

-Pasaulyje pagal blokų grandinės įmonių skaičių pirmauja JAV ir Kinija.

-Kai plačiau apžvelgiame tarptautinius žaidėjus, ypač dinamiškai blokų grandinės startuolių kūrimąsi skatina Šveicarija ir Singapūras, po jų seka Japonija ir Pietų Korėja.

-Besivystančių šalių dalyvavimas blokų grandinės technologijoje yra šiek tiek mažiau reikšmingas - tik 0,5 mlrd. eurų bendro finansavimo, kurio pagrindinis kapitalo šaltinis yra ICO.

## 3.3 Horizontalus tyrimo atvejų palyginimas

Tyrimo projektų imtis pasižymi dideliu heterogeniškumu. Daugiausia dėmesio buvo skiriama atskleisti bendrus modelius ir pagrindinius skirtumus tarp blokų grandine grįstų projektų, vykdomų viešajame sektoriuje. Tai buvo daroma lyginant projektus pagal iš anksto nustatytus kriterijus. Rezultatai pateikiami 2-8 lentelėse.

Visuose atvejuose pastebimas tiesioginis valdžios institucijų dalyvavimas projektuose. Vietos ir nacionalinės valdžios institucijos eksperimentuoja su tam tikromis konkrečiomis paslaugomis, pavyzdžiui, registracija, tikrinimu ir perdavimu (žemės nuosavybės teisės, asmens pažymėjimų tikrinimas ir tapatybės patvirtinimas arba išmokų paskirstymas). Šiomis konkrečiomis paslaugomis remiamos trys pagrindinės valdžios institucijų funkcijos:

-viešųjų registrų tvarkymas;

-socialinių pervedimų ir (arba) išmokų tvarkymas;

-patikrintos informacijos teikimas, siekiant palengvinti ekonominius sandorius.

Dauguma šių paslaugų yra skirtos piliečiams kaip galutiniams vartotojams, tačiau taip pat yra projektų, kuriuose daugiausia dėmesio skiriama pamatiniams blokų grandinių elementams. Šie decentralizuotos architektūros blokai, pavyzdžiui, vyriausybės patvirtinta decentralizuota tapatybė, gali būti naujos kartos viešųjų paslaugų, tokių kaip elektroninio balsavimo ar prieigos prie viešosios infrastruktūros suteikimo, įgalintojai.

Tyrimo apimties projektuose dalyvaujančios valdžios lygmuo yra įvairus, tačiau dominuoja nacionalinis. Projektai, kuriuose į konsorciumus įtrauktos vietos valdžios institucijos gyvavimo ciklas yra gana pažengęs ir jų taikymo sritis yra siauresnė. Tarptautiniai aspektai aiškiai išreikšti tik „Infrachain“ projekte. „Infrachain“ tikslas - sukurti Europos aukšto lygio etaloninį tinklą, sudarytą iš nepriklausomų mazgų, kuriuose galėtų būti talpinamos skirtingos blokų grandinės. Likusieji projektai yra vietinio arba nacionalinio pobūdžio, tačiau kai kuriais atvejais galima sukurti akivaizdžią pridėtinę vertę, jei sprendimas būtų išplėstas tarptautiniu mastu, kaip, pavyzdžiui, akademinių įgaliojimų tikrinimo atveju. Daugumos atvejų tyrimai rodo tarpsektorinius aspektus, t.y. paslaugos gali gali būti pritaikytos keletui sektorių, pramonės šakoms ar rinkoms. Pavyzdžiui, Cugo mieste sukurta decentralizuota tapatybė galėtų būti išplėsta ne tik viešajame sektoriuje. Ši struktūra leidžia teikti privačias paslaugas, tokias kaip nuoma, kur asmenys gali būti autentifikuojami naudojant "uPort" tapatybės sprendimą. Konkrečiuose veiklos sektoriuose plėtojantys specifines paslaugas yra "Chromaway" nekilnojamojo turto sandoriai ir "Exonum" žemės nuosavybės registras. Informacija apie buvimo vietą skaitmeninėse paslaugose sukuria vertę įvairiais būdais, pavyzdžiui bendruomenės elemento pridėjimas arba teikiamos paslaugos suasmeninimas. Blokų grandine grindžiamose sistemose buvimo vieta dažnai yra statinis elementas, kaip matyti 2 lentelėje.

**2 lentelė. Projektų charakteristikos**

| Projekto pavadinimas | Valdžia | Viešosios paslaugos | Tarp-tautinis | Tarpsektorinis | Vietovė | Programinis kodas |
|---|---|---|---|---|---|---|
| „Exonum“ žemės registras | Nacionalinė | Žemės sandorių registravimas ir tvirtinimas | Ne | Ne | Vietovė yra produktas | Atviro kodo |
| „Blockcerts“ akademiniai kredencialai | Nacionalinė | Sertifikatų tvirtinimas/Asmeninių dokumentų saugojimas | Taip | Verslas, švietimas | Vietovė yra statinė | Atviro kodo |
| „Chromaway“ nekilnojamojo turto sandoriai | Nacionalinė | Nekilnojamojo turto sandoriai | Ne | Ne | Vietovė yra produktas | Uždaro kodo |
| „uPort“ decentralizuota tapatybė | Vietinė | Gyv. vietos deklaravimas, e-balsavimas | Ne | Taip, platus pritaikymas daugeliui sričių | Vietovė yra statinė | Atviro kodo |
| „Infrachain“ valdymo sistema | Nacionalinė | Nėra | Taip | Taip, platus pritaikymas daugeliui sričių | Vietovė yra statinė | Atviro kodo |
| „Pensijų infrastruktūra“ | Nacionalinė | Pagerintas pensijų administravimas | Ne | Taip, platus pritaikymas daugeliui sričių | Vietovė yra statinė | Hibridinis: programinis kodas uždaras, standartai- atviri |
| „Stadjerspas“ išmanieji kuponai | Vietinė | Tikslinės naudos suteikimas mažas pajamas gaunantiems piliečiams | Ne | Taip, platus pritaikymas daugeliui sričių | Vietovė yra statinė | Hibridinis: atviro kodo blokų grandinės protokolas, tačiau uždaro kodo išmaniųjų sutarčių sluoksnis |

Dviejuose tyrime dalyvavusiuose projektuose, susijusiuose su žemės nuosavybės teise ir nekilnojamojo turto sandoriais, vieta gali būti laikoma produktu, tačiau ji apribota statiniais duomenimis. Nors blokų grandine paremtų projektų ekosistemoje yra iniciatyvų, kurios suteikia svarbesnį vaidmenį vietos informacijai blokų grandinės sistemose, nė vienas iš tyrime dalyvavusių projektų tiesiogiai naudotojo vietos duomenų neapdoroja. Keturi iš septynių projektų yra visiškai atviro kodo. Likusiuose projektuose naudojamas atviro kodo blokų grandinės protokolai, tačiau kuriama ir uždaro kodo programinė įranga, įgyvendinanti išmaniąsias sutartis.

Kiekvieno projekto atveju buvo tiriama, ar blokų grandinės platforma pakeitė viešojo valdymo organizacijos funkcijas ir (arba) perėmė vieną ar daugiau tokios organizacijos užduočių. Nė viename iš projektų nepastebėta, kad kurios nors viešojo valdymo institucijos įsitraukimo poreikis būtų eliminuotas. Teisybės dėlei reiktų paminėti, kad „Chromaway" projekte buvo išstumta notaro pozicija. Notarui nebereikia dalyvauti registruojant ir tvirtinant nuosavybės sandorių dokumentus, nes tai daroma

tiesiogiai išmaniosios sutarties darbo eigoje. Nepaisant šio atvejo, daugumoje projektų tapatybės patvirtinimo, dokumentų patikrinimo ar tinkamumo tikrinimo procedūros įvykdomos iki blokų grandinės protokolo. Dėl šių pokyčių sumažėja popierinių dokumentų ir sutaupoma laiko. Tyrime analizuoti projektai skiriasi pagal blokų grandinės pagalba įgyvendinamų funkcijų apimtį (3 lentelė).

**3 lentelė. Projektų funkcionalumai**

| Projekto pavadinimas | Ar iš proceso eliminuojamos institucijos? | Koks blokų grandinės funkcionalumas panaudotas? |
|---|---|---|
| „Exonum“ žemės registras | Ne. | Notarizacija |
| „Blockcerts“ akademiniai kredencialai | Dalinai: sumažėja darbo krūvis universitetų administracijai. | Notarizacija |
| „Chromaway“ nekilnojamojo turto sandoriai | Taip, eliminuojami notarai. Taip pat sumažėja darbo krūvis bankų bei žemės registrų sektoriui. | Bendra duomenų bazė/Išmaniųjų sutarčių automatizacija |
| „uPort“ decentralizuota tapatybė | Dalinai: sumažėja krūvis savivaldybei. | Notarizacija |
| „Infrachain“ valdymo sistema | Ne. | Notarizacija/Bendra duomenų bazė/Išmaniųjų sutarčių automatizacija |
| „Pensijų infrastruktūra“ | Dalinai: sumažėja darbo krūvis pensijų fondų valdytojams. | Notarizacija/Bendra duomenų bazė/Išmaniųjų sutarčių automatizacija |
| „Stadjerspas“ išmanieji kuponai | Dalinai: sumažėja krūvis savivaldybei. | Notarizacija/Išmaniųjų sutarčių automatizacija |

Dviejuose projektuose („Exonum“ ir „Blockerts“) blokų grandinė naudojama maišos kodams įrašyti, kurie savo esme yra šifruotos, laiko žymomis pažymėtos dokumentų ištraukos. Blokų grandine grindžiamas notarinis patvirtinimas leidžia patikrinti dokumento originalumą, kartu nurodant jo sukūrimo datą ir savininką. Iš vienos pusės ši elementari funkcija piliečiams teikia tik ribotą naudą, tačiau iš kitos pusės ji suteikia pridėtinės vertės, jei yra derinama su kitais elementais, tokiais kaip asmeniniai sertifikatai ir įgaliojimai. Dauguma projektų įgyvendina pažangesnes blokų grandinių funkcijas, o būtent- programuojamas išmaniąsias sutartis. Išmaniosios sutartys įgalina bendrą duomenų bazę ir keitimąsi informacija tarp skirtingų dalyvių („Pensijų infrastruktūra“), decentralizuotą tapatybės valdymą („uPort“), automatinį sandorių vykdymą ("Chromaway") arba naudojimąsi stebėsenos ir tinkamumo patikrinimo sistema („Stadjerspas“). Funkcionalumo tipas iš dalies daro įtaką paslaugos brandai. Tie projektai, kurie naudoja išmaniąsias sutartis bendroms duomenų bazėms arba darbo eigos automatizavimui, yra santykinai mažiau pažengę, tačiau to galima tikėtis, nes šios realizacijos turi suderinti skirtingus sudėtingos ir specifinės ekosistemos poreikius ir integruoti įvairių dalyvių anksčiau naudotas sistemas.

Konsorciumo vaidmenų sudėtis tyrimo projektuose labai skirtinga. Maždaug pusėje atvejų prie sprendimo įgyvendinimo prisideda atvirojo kodo programinės įrangos bendruomenė, tuo tarpu kituose projektuose pagrindinį sprendimo vystymo darbą atlieka technologijų tiekėjas (4 lentelė).

**4 lentelė. Projektų valdymas**

| Projekto pavadinimas | Konsorciumo sudėtis | Blokų grandinės modelis | Konsorciumo valdymas |
|---|---|---|---|
| „Exonum“ žemės registras | Vyriausybė; Atvirojo kodo bendruomenė; Techninio sprendimo tiekėjas | Privatus su leidimu ir viešas be leidimo | Centralizuotas |
| „Blockcerts“ akademiniai kredencialai | Vyriausybė; Atvirojo kodo bendruomenė; Techninio sprendimo tiekėjas | Privatus be leidimo | Hibridinis |
| „Chromaway“ nekilnojamojo turto sandoriai | Vyriausybė; Techninio sprendimo tiekėjas; Bankai | Privatus su leidimu | Hibridinis |
| „uPort“ decentralizuota tapatybė | Vyriausybė; Atvirojo kodo bendruomenė; Techninio sprendimo tiekėjas | Privatus be leidimo | Hibridinis |
| „Infrachain“ valdymo sistema | Vyriausybė; Techninio sprendimo tiekėjas; Verslas | Privatus ir viešas su leidimu | Decentralizuotas |
| „Pensijų infrastruktūra“ | Vyriausybė; Atvirojo kodo bendruomenė; Techninio sprendimo tiekėjas; Pensijų fondai | Privatus su leidimu | Hibridinis |
| „Stadjerspas“ išmanieji kuponai | Vyriausybė; Techninio sprendimo tiekėjas; Verslas | Privatus be leidimo | Centralizuotas |

Pats projektų konsorciumų valdymas dažniausiai yra centralizuotas arba mišrus. Centralizuotame modelyje paprastai vyriausybė turi didelę sprendimų priėmimo galią. Hibridinio modelio atveju keli stambūs dalyviai gali nukreipti konsorciumą tam tikromis kryptimis, dažnai su didele technologijų tiekėjo įtaka.

Blokų grandinės valdymo architektūrų pasirinkimas nėra vienareikšmis. Įdomu pastebėti tai, kad nė vienas projektas nėra paremtas vien tik vieša, be leidimų veikiančia blokų grandine. Visais atvejais yra tam tikras apribojimas: arba dėl to, kas gali sudaryti arba kas gali patvirtinti sandorius. Keturiais atvejais stebimas privačios su leidimais, kai patvirtinime dalyvauja ribotas žinomų mazgų skaičius, blokų grandinės elementų naudojimas.

Tyrimo metu dauguma projektų buvo konceptualiame arba bandomajame etape. Tik du projektai jau veikė pilnavertiškai ir teikė savo paslaugas gyventojams. Dabartinis naudojimas labai skiriasi priklausomai nuo projekto ir priklauso nuo gyvavimo ciklo etapo. Paprastai bandomųjų projektų naudotojų grupės neviršija kelių šimtų, tačiau jau veikiančių paslaugų atveju jie siekia kelis tūkstančius. Sakartvelo valdžios institucijos yra užregistravusios daugiau kaip 100 tūkstančių šifruotų žemės nuosavybės įrašų „Exonum“ blokų grandinėje. Groningeno savivaldybės kuponų sistema jau turi daugiau kaip 20 tūkstančių naudotojų.

Kaip matyti iš 5 lentelės, jau įgyvendinti ankstyvojo etapo projektai turi ribotą blokų grandinės sistemų apskaitos pralaidumo parametrą, t.y. kiek operacijų per sekundę (angl. transfer per second, abr. tps) gali apdoroti sistema.

**5 lentelė. Pojektų naudojimas**

| Projekto pavadinimas | Naudojamumas | Pralaidumas | Išplečiamumas | Branda |
|---|---|---|---|---|
| „Exonum“ žemės registras | Virš 100 tūkst. įrašų | Nežinoma | 5 tūkst. sandorių per sekundę | Pilnavertiškai veikiantis |
| „Blockcerts“ akademiniai kredencialai | Šimtai naudotojų | 7 sandoriai per sekundę | 7 sandoriai per sekundę | Ankstyvoji bandomoji stadija |
| „Chromaway“ nekilnojamojo turto sandoriai | Nežinoma | Nežinoma | 160 sandorių per sekundę | Koncepcijos patvirtinimo stadija |
| „uPort“ decentralizuota tapatybė | 300 naudotojų | Nežinoma | 7 sandoriai per sekundę | Ankstyvoji bandomoji stadija |
| „Infrachain“ valdymo sistema | Nežinoma | Priklauso nuo blokų grandinės | Priklauso nuo blokų grandinės | Ankstyvoji bandomoji stadija |
| „Pensijų infrastruktūra“ | 5 tūkst. naudotojų | Nežinoma | Nežinoma | Koncepcijos patvirtinimo stadija |
| „Stadjerspas“ išmanieji kuponai | 20 tūkst. naudotojų, 4 tūkst. sandorių per mėnesį | 7 sandoriai per sekundę | 7 sandoriai per sekundę | Pilnavertiškai veikiantis |

Tai nestebina, nes šiame etape pagrindinis tikslas yra sukurti veikiančią paslaugą bandomojoje aplinkoje. Į stabilumą ir sistemos masto didinimo galimybes atsižvelgiama vėlesniuose eksperimentavimo etapuose, kai pagrindinis tikslas yra prototipo optimizavimas eksploatacijai. Nors to neįmanoma patikrinti, deklaruojamas mastelio pokytis (suprantamas kaip maksimalus operacijų skaičius per tam tikrą laiko intervalą) dabartinėse aplinkose svyruoja nuo 7 iki 5000 operacijų per sekundę. Paprastai projektai, kuriuose naudojamos blokų grandinės su leidimais, mastelio keitimo apribojimų neturi. Mastelio keičiamumas dažnai laikomas blokų grandinių be leidimo įgyvendinimo kliūtimi, tačiau realybėje neatrodo, kad tai būtų pagrindinė kliūtis. Tyrimo projektai, savo sprendimuose naudojantys blokų grandinę be leidimų, turi sukurę būdus, kaip įveikti pralaidumo kliūtis. Pavyzdžiui „Blockcerts“ sandorius registruoja partijomis, o „Exonum“ šifruoja visą sistemos būseną, bet ne atskirus žemės nuosavybės dokumentus. Stadjerspas atveju dabartinis pralaidumas nėra kliūtis, nes numatytam subsidijuojamų paslaugų kiekiui atitinkamai numatytas išmaniųjų sutarčių kiekis.

Blokų grandine grindžiamų paslaugų techninės architektūros įvairiuose projektuose taip pat labai skiriasi. Visų tyrime dalyvavusių projektų architektūros sluoksnių apžvalga pateikiama 6 lentelėje.

**6 lentelė. Projektų techninė architektūra**

| Projekto pavadinimas | Naudotojo sąsaja | Kitos (ne PRT) sistemos | API sąsaja | PRT platformos konsensusas | Infrastruktūra |
|---|---|---|---|---|---|
| „Exonum“ žemės registras | Administravimo programa | Nekilnojamo turto registro sistema | Administratoriaus API nekilnojamo turto registrui | Privatus konsensusas ir atlikto darbo įrodymas | Žinomi mazgai ir Bitcoin blokų grandinė |
| „Blockcerts“ akademiniai kredencialai | Piniginė (programa) ir išdavėjo programinė įranga | Akademinių įstaigų sertifikatų duomenų bazės | Blokų grandinės API patvirtinimui ir paieškai | Atlikto darbo įrodymo konsensusas | Bitcoin blokų grandinė |
| „Chromaway“ nekilnojamojo turto sandoriai | Išmaniosios sutarties sąsaja (programa) | Švedijos nekilnojamo turto registras | Tarpmazginis API, Kliento API, Senoji API | Įgaliojimo įrodymo konsensusas | PostgreSQL ar kitos RDMS duomenų bazės kartu su žinomais mazgais |
| „uPort“ decentralizuota tapatybė | uPort (programa) | Savivaldybės internetinis puslapis | uPort Connect API | Turimos dalies įrodymo konsensusas | Maiša talpinama Ethereum blokų grandinėje, naudotojo duomenys saugomi lokaliai |
| „Infrachain“ valdymo sistema | - | - | - | Atlikto darbo įrodymo konsensusas | Ethereum protokolu grįsti mazgai |
| „Pensijų infrastruktūra“ | Programa | Darbo užmokesčio ir pensijų duomenų bazės | Nežinoma | Atlikto darbo įrodymo konsensusas | Maiša talpinama Ethereum blokų grandinėje su žinomais mazgais, sandorių talpinimo vieta nežinoma |
| „Stadjerspas“ išmanieji kuponai | QR kodas, naršyklė | Savivaldybės registrai | Administratoriaus API | Įgaliojimo įrodymo konsensusas | Mazgai naudojantys Zcash protokolą |

Vartotojo sluoksnyje yra virtualios piniginės, interneto portalai ir specialiai sukurtos programos. Dominuoja mobiliosios taikomosios programos, kurios paprastai pagerina galutinio vartotojo patirtį. Žvelgiant į ne paskirstytojo registro technologijų sistemas, visada naudojamas atskiras registras arba duomenų bazė. Visos diegimo sistemos turi ryšį su esamomis duomenų bazėmis- nuo darbo užmokesčio ar įgaliojimų duomenų bazių iki savivaldybių ar valstybinių registrų.

Blokų grandinės bandomuosiuose projektuose dažniausiai naudojama aplikacijų programavimo sąsaja (angl. Application Programming Interface, API), kad blokų grandinės sluoksnis būtų sujungtas su jau esamomis duomenų bazėmis arba su esamomis projekto dalyvių sistemomis. Sudėtingiausi blokų grandinės bandomieji projektai naudoja įvairias aplikacijų programavimo sąsajas, atliekančias skirtingas funkcijas.

Fizinis sandorių duomenų saugojimas labai priklauso nuo techninės blokų grandinės architektūros. Privačios blokų grandinės infrastruktūros dažnai leidžia dalyviams talpinti blokų grandinės mazgus ir dalyvauti konsensuse. Viešosiose blokų grandinės architektūrose fizinė saugomų sandorių duomenų vieta paprastai nėra žinoma.

Bandomuosiuose diegimuose pasitaiko įvairių konsensuso mechanizmų. Blokų grandinės architektūra (privati / vieša ir be leidimo / su leidimu) tik tam tikru mastu lemia kiek skaičiavimo požiūriu yra sudėtingas naudojamas konsensuso mechanizmas. Darbo įrodymas (angl. Proof-Of-Work) reikalauja daug energijos ir aparatinės įrangos, todėl kai kurie blokų grandinės be leidimų technologija paremti projektai („Stadjerspas‘, naudojantis „Zcash“ ) taip pat naudoja ir autoriteto įrodymo (angl. Proof-Of-Stake of Proof-Of-Authority) konsensuso mechanizmą. Visiškai privačios leidimais pagrįstos blokų grandinės diegimo priemonės ("Chromaway") taip pat naudoja šį konsensuso mechanizmą. Tarp žinomų mazgų gali būti diegiamas efektyvesnis konsensuso modelis, pavyzdžiui, PBFT (angl. Practical Byzantine Fault Tolerance, PBFT). Apskritai, vis daugiau tyrimų atliekama siekiant sukurti skaičiavimo požiūriu "lengvesnius" konsensuso mechanizmus pavyzdžiui, "Proof-Of-Stake", skirtus blokų grandinės diegimui be leidimų. Infrastruktūros sluoksnis, kuriame veikia konsensuso mechanizmas, priklauso nuo diegimo. Leidimais pagrįstose blokų grandinėse mazgai dažnai priklauso konsorciumo dalyviams, įskaitant valstybines institucijas. Be leidimų veikiančiose diegimo sistemose teoriškai bet kas gali įsteigti mazgą. Jei paslauga įtvirtina maišos kodus „Bitcoin“ blokų grandinėje, jie būtų saugomi visuose pilnaverčiuose Bitcoin mazguose, kurie pasiskirstę visame pasaulyje.

Informacijos apie tyrime dalyvavusių blokų grandinės bandomųjų projektų sąnaudas daugeliu atveju nebuvo įmanoma gauti dėl dviejų priežasčių. Pirma, kadangi daugybė viešųjų organizacijų tiria panašius bandomuosius projektus, noras dalytis išlaidų skaičiais yra ribotas, atsižvelgiant į strateginę svarbą būti pirmuoju iniciatoriumi. Antra, nepakankamas dėmesys sąnaudoms taip pat gali būti paaiškintas bandomųjų projektų pobūdžiu ir tikslais. Skirtingai nuo gamybos diegimo, eksperimentiniuose projektuose daugiausia dėmesio skiriama funkciniams maketams. Šiame etape nesvarstomas ekonominis ir techninis efektyvumas. Todėl, atsižvelgiant į minėtus veiksnius, buvo nustatytos tik įvairių sąnaudų kategorijos, kurios atsiranda kuriant paslaugas (7 lentelė).

**7 lentelė. Projektų sąnaudos**

| Projekto pavadinimas | Vienkartinės sąnaudos | Pasikartojančios sąnaudos |
|---|---|---|
| „Exonum“ žemės registras | Kūrimas, integravimas, adaptacija | Priežiūros ir veiklos sąnaudos, mokesčiai už sandorius |
| „Blockcerts“ akademiniai kredencialai | Kūrimas, integravimas | Mokesčiai už sandorius, programinio kodo palaikymas |
| „Chromaway“ nekilnojamojo turto sandoriai | Kūrimas, integravimas | Priežiūros ir veiklos sąnaudos |
| „uPort“ decentralizuota tapatybė | Kūrimas | Mokesčiai už sandorius, veiklos sąnaudos |

| | | |
|---|---|---|
| „Infrachain“ valdymo sistema | Techninė įranga | Nario mokestis (1-6 tūkst. eurų per metus), administravimo sąnaudos, mokesčiai už sandorius |
| „Pensijų infrastruktūra“ | Nėra duomenų | Nėra duomenų |
| „Stadjerspas“ išmanieji kuponai | Neatskleista, bet ne didesnės negu centralizuoto sprendimo | Mokesčiai už sandorius |

Kūrimo ir integracijos sąnaudos yra dvi pagrindinės vienkartinių sąnaudų rūšys. Be kūrimo, blokų grandine grindžiamoms paslaugoms taip pat reikalinga integracija su senosiomis sistemomis. Saugios ir automatizuotos sąsajos (aplikacijų programavimo sąsajos, API) su išorinėmis duomenų saugyklomis tai pat sudaro reikšmingą sąnaudų elementą. Plėtros sąnaudos apima blokų grandinės protokolo rašymą arba esamo atvirojo kodo sprendimo pritaikymą. Atvirojo kodo komponentų pritaikymas paprastai yra pigesnis, todėl ši galimybė dažniausiai ir pasirenkama. Be paskirstytojo registro technologijų sluoksnio sukūrimo, kiekviename projekte papildomai kuriamos specialios naudotojo sąsajos ir taikomosios programos. Tyrime analizuoti projektai nepatyrė didelių infrastruktūros išlaidų, nes bandomosiose aplinkose dalyvaujančių naudotojų skaičius ir blokų grandinės mazgų skaičius yra ribotas, tačiau operacinėms paslaugoms neabejotinai reikės didesnės ir patikimesnės infrastruktūros bei su tuo susijusių išlaidų. Infrastruktūros sąnaudos taip pat susijusios su blokų grandinės naudojimu, kuris priklauso nuo mazgų, dalyvaujančių konsensuso mechanizmuose, ir sandorių duomenų saugojimo pajėgumo. Taikomi įvairūs infrastruktūros teikimo modeliai. Paslaugoms, kurios daugiausia naudoja notarizavimo funkciją viešosiose leidimo nereikalaujančiose blokų grandinėse, iš esmės nereikia investuoti į specialią infrastruktūrą. Paslaugos, įgyvendinančios specifines funkcijas leidimų reikalaujančiose blokų grandinėse, pavyzdžiui, bendrai naudojamą duomenų bazę, greičiausiai reikės specialios infrastruktūros. Tačiau net ir šiuo atveju bus galima rinktis, ar diegti savo infrastruktūrą ar naudoti infrastruktūrą, teikiamą kaip paslaugą, pavyzdžiui, sukurtą pagal projektą „Infrachain“. Tyrime dalyvavusių projektų, kurie jau yra operaciniame lygmenyje, viešosios institucijos neturi specialios blokų grandinės infrastruktūros savo viduje, bet sudaro paslaugų teikimo sutartis su technologijų partneriais.

Sandorių mokesčiai yra būdingi leidimų nereikalaujančiose blokų grandinėse ir pastebimi visais keturiais šio archetipo tyrimo atvejais. Kai kuriuose projektuose reikia sumokėti blokų grandinės patvirtinimo išlaidas už kiekvieną naują naudotoją, o kituose- patvirtinimui siunčiamas tik vienas sandoris su visa sistemos būkle. Paslaugos, kurioms reikalingas kelių sandorių patvirtinimas viešojoje leidimų nereikalaujančioje blokų grandinėje ir priklauso nuo skaičiavimo požiūriu sudėtingo konsensuso mechanizmo, gerokai padidina aplinkosaugos sąnaudas.

Susisteminti kiekybines įžvalgas apie blokų grandine grindžiamų sprendimų teikiamą naudą yra gana sudėtinga. Nepaisant to, kai kurių sprendimų kokybiniai ir kiekybiniai aspektai, pasitelkus projektų komandų įverčius bei viešai prieinamą informaciją, pateikti 8 lentelėje.

**8 lentelė. Projektų nauda**

| Projekto pavadinimas | Kiekybinė nauda | Kokybinė nauda |
|---|---|---|
| „Exonum“ žemės registras | 400 kartų greitesnė išrašo registracija; > 90 % veiklos sąnaudų sumažėjimas | Padidėjęs skaidrumas ir duomenų patikimumas; didesnis atsparumas gedimams ir kibernetiniams incidentams |
| „Blockcerts“ akademiniai kredencialai | Mažesnės veiklos bei integracijos sąnaudos; efektyvumo padidėjimas | Patogiai saugomi bei pačių piliečių kontroliuojami duomenys; greitas ir pasirenkamasis dalijimasis; tapatybės bei privatumo apsauga; skaitmenizacija (jokių popierinių diplomų kopijų); padirbtų akademinių dokumentų (pažymų, diplomų, sertifikatų ir pan.) eliminavimas |
| „Chromaway“ nekilnojamojo turto sandoriai | ~1 mil. eurų per metus; > 95 % sumažėjęs sandorių laikas; >90 % sumažėjusi sandorių kaina; greitesnis nekilnojamo turto registracijos ir perdavimo procesas | Padidėjęs atsparumas sukčiavimui; padidėjęs pasitikėjimas rinkos veikla; didesnis aktyvų likvidumas |
| „uPort“ decentralizuota tapatybė | Mažesnės sąnaudos administravimui, įrašų laikymui, infrastruktūrai; padidėjęs administravimo efektyvumas | Pačių piliečių kontroliuojami duomenys; sumažinta kibernetinių atakų rizika |
| „Infrachain“ valdymo sistema | Nėra duomenų | Padidėjęs atsparumas, patikimumas, skaidrumas ir lankstumas |
| „Pensijų infrastruktūra“ | ~500 mil. eurų per metus; mažesnės sąnaudos įrašų laikymui bei sandoriams tarp piliečių; pensijų fondų ir administravimo efektyvumo padidėjimas | Padidėjęs skaidrumas, duomenų saugumas; pagerėjusi reguliuojamoji priežiūra |
| „Stadjerspas“ išmanieji kuponai | Mažesnės administravimo ir sandorių tarp piliečių sąnaudos; administravimo efektyvumo padidėjimas | Efektyvus perskirstymas; padidėjęs viešųjų lėšų auditabilumas |

Dažniausiai deklaruojama blokų grandine grindžiamų paslaugų nauda - procesų efektyvumas. Žmogaus atliekamo dokumentų registravimo ir tikrinimo proceso bei spausdintinių kopijų eliminavimas leidžia sutaupyti veiklos ir administravimo išlaidų. Daug greitesnis ir patikimesnis atsiskaitymas už sandorius sumažina pačių sandorių sąnaudas. Tai ypač gerai pastebima "Chromaway" projekto atveju. Galutinis nekilnojamojo turto sandorio laikas sumažėja nuo kelių savaičių iki kelių valandų, todėl sutaupoma labai daug lėšų, kurios kitu atveju būtų išleidžiamos hipotekos draudimui. Projektai, kuriais sukuriamos bendro naudojimo duomenų bazės, kaip "Chromaway" ar "Pensijų infrastruktūra", padeda išvengti begalinio tų pačių duomenų kopijavimo tarp skirtingų IT sistemų. Išmaniosios sutartys leidžia racionalizuoti įvairius verslo procesus, taigi sukurti efektyvumą mažinant neapibrėžtumą ir automatizuojant sandorius.

Projekto atstovų teigimu, blokų grandine grindžiama pensijų administravimo sistema Nyderlanduose „Pensijų infrastruktūra“ turėtų leisti sutaupyti 500 mln. JAV dolerių per metus sistemos administravimo išlaidų. Tai atitinka 50 % išlaidų sumažėjimą, palyginti su faktiniu lygiu. Projekte

"Chromaway" apskaičiuota grynoji nauda įgyvendinus išmaniąsias sutartis nekilnojamojo turto sandorių srityje - 100 mln. eurų per metus. Šią naudą iš dalies galima priskirti tiek viešosioms ir privačioms institucijoms tiek ir piliečiams. Projekto „Stadjerspas“ atveju naudą galima priskirti visai visuomenei, nes technologija pagerina viešųjų lėšų tikslingumą ir sumažina perskirstymo politikos išlaidas.

Blokų grandinės technologija taip pat teikia nemažai kokybinės naudos. Tai, kad įrašus apie sandorius paskirstytajame registre dalijasi keli mazgai, vienareikšmiškai didina kibernetinį saugumą ir atsparumą incidentams bei piktavališkam elgesiui. Blokų grandinės savybė, kad įrašai į ją gali būti tik įrašomi, bet neištrinami užtikrina neatšaukiamumą ir didina registro vientisumą bei audito atlikimo galimybes. Visas šias savybes tiesiogiai užtikrina pati technologija ir tikėtina, kad padidintų valstybinės apskaitos patikimumą. Tai, kad nėra centrinio tarpininko, kuris užtikrintų sandorių teisėtumą, yra dar vienas teigiamas poveikis. Jis perkelia procesų kontrolę pačiai ekosistemai. Pavyzdžiui, „uPort“ projekto naudotojai įgyja visišką savo asmeninių duomenų kontrolę ir gali pasirinktinai atskleisti juos bet kuriai trečiajai šaliai. Šifravimo metodai užtikrina dalijimosi asmens duomenimis ir jų saugojimo atitiktį Bendrajam duomenų apsaugos reglamentui. Galiausiai blokų grandine grindžiamos skaitmeninės paslaugos gali pagerinti naudotojų bendravimo su valdžios institucijomis patirtį. Pavyzdžiui, žemės nuosavybės teisės arba asmens dokumentus galima išduoti ir perduoti naudojantis mobiliąja programėle, nenaudojant popierinių kopijų ir vizitų į savivaldybę, Registrų centrą ar kitą valstybinę instituciją.

## 3.4 Atvejų tyrimo įžvalgos

**Aktyviai eksperimentuojama su visu blokų grandinės technologijos funkcionalumo spektru.**

Trys blokų grandinės savybės- notarizavimas, bendrai naudojama duomenų bazė ir darbo eigos automatizavimas - gali būti naudingos tiek valdžios institucijoms tiek piliečiams. Blokų grandinės notarizavimas leidžia patikrinti dokumento originalumą ir patvirtinti jo sukūrimo datą bei savininką. Decentralizuotas notarizavimas yra tik inkrementinė inovacija, todėl, jei ji pridedama prie esamų centralizuotų paslaugų, ji suteikia tik papildomą vertę. Tačiau kartu su kitomis naujovėmis, kaip lygiarangė failų sistema ir dalijimasis duomenimis, notarizavimas neša aiškią vertę piliečiams („Blockcerts“, „uPort“). Pažangesnės blokų grandinės funkcijos yra grindžiamos programuojamomis išmaniosiomis sutartimis. Išmaniosios sutartys įgyvendinamos skirtingiems tikslams, pavyzdžiui, bendrai naudojamai duomenų bazei, keitimuisi informacija (Pensijų infrastruktūra, Stadjerspas) arba daugiašalių sandorių automatizavimui ("Chromaway"). Pažangieji funkcionalumai turi didelę vertę, nes jie savaime yra „griaunamosios“ inovacijos. Jie iš esmės yra svarbūs visoms skaitmeninės valdžios atliekamoms funkcijoms efektyviai atlikti: duomenų valdymui, ekonominių sandorių palengvinimui, viešųjų lėšų perskirstymui ir reguliavimo kūrimui. Piliečiai, besinaudojantys išmaniosiomis sutartimis

grindžiamomis paslaugomis, taip pat naudojasi didesniu procesų efektyvumu, mažesniu neapibrėžtumu ar atsiskaitymo laiku.

**Blokų grandine grindžiamos notarinio tvirtinimo paslaugos yra santykinai labiau išvystytos.**

Įgyvendinamo funkcionalumo tipas turi įtakos projektų brandai. Projektai, kurie naudoja išmaniąsias sutartis, kad palengvintų bendrai naudojamų duomenų bazių naudojimą ar automatizuotų darbo procesų vykdymą, yra mažiau pažengę savo gyvavimo cikle, nes šios realizacijos turi suderinti skirtingus ekosistemos poreikius ir integruoti anksčiau naudotas sistemas. Kai kuriais atvejais pažangieji funkcionalumai jau gerai veikia techniškai, tačiau neatitinka teisinės bazės. Reguliavimo ir valdymo standartų trūkumas trukdo plėtoti „griaunančias“ paslaugas už koncepcinio ar ankstyvojo bandomojo etapo ribos. Projektai, kurie vykdo tik egzistavimo įrodymo (angl. proof of existence) patikrinimą, yra greičiau įgyvendinami. Jiems reikia mažiau integravimo pastangų ir gali būti naudojami jau esami programinės įrangos komponentai.

**Aukštesnio brandos lygio projektai paprastai turi labiau centralizuotą valdymą bei mažesnį suinteresuotų šalių kompleksiškumą.**

„Pensijų infrastruktūros“ projektas, kuris yra koncepcijos patvirtinimo etape, yra sudėtingiausias tyrimo pavyzdys. Jame dalyvauja kelių tipų suinteresuotosios šalys, su skirtingais veiklos tikslais ir skirtingomis anksčiau naudotomis duomenų bazėmis. „Stadjerspas“ kuponų sistema, „Exonum“ žemės nuosavybės registras ir „Blockcerts“ akademiniai pažymėjimai turi mažiau suinteresuotųjų šalių tipų. Projektai su labiau centralizuota valdymo struktūra yra pažangesni. Tikėtina, kad tai lemia hierarchiškesni sprendimų priėmimo procesai konsorciumuose, turinčiuose stiprų lyderį.

**Blokų grandine grindžiamos paslaugos aktyviai reaguoja į verslo poreikius. Jos taip pat turi aktyvius viešuosius veikėjus ir stiprius technologinius partnerius.**

Du imtyje esantys projektai jau teikia veikiančias paslaugas. Abiem atvejais yra stiprus technologinis partneris, užtikrinantis reikiamą integraciją su senosiomis sistemomis. Abu projektai yra ties dabartinėmis technologinėmis ribomis. Juose naudojamas bazinis blokų grandinės funkcionalumas-laiko žyma patvirtintas egzistavimo įrodymas. „Stadjerspas“ taip pat naudoja programuojamąjį sluoksnį, kuris leidžia nustatyti reikalavimus dėl konkrečių išmaniųjų kuponų. Be to, abu projektai turi aiškiai apibrėžtus verslo poreikius: registracija ir žemės nuosavybės teisių registravimas ir tikrinimas bei kuponų paskirstymas pagal konkrečius kriterijus naudos gavėjams.

**Blokų grandinės įgyvendinimas daugiausia grindžiamas atvirojo kodo programine įranga.**

Dauguma projektų remiasi jau patikrintais ir veikiančiais atvirojo kodo komponentais, nes dažnu atveju jie turi stiprias bendruomenes, sudarytas iš kūrėjų ir naudotojų. Atvirojo kodo elementams priskiriami blokų grandinės protokolai kaip "Zcash" arba "Bitcoin", taip pat ant protokolo esantis programinės įrangos sluoksnis kaip "Exonum" arba "Blockcerts". Atvirasis kodas yra vyraujantis projekto komandų pasirinkimas, nes jis pagreitina paslaugos kūrimą. Kai kuriuose projektuose atvirojo

kodo sprendimai derinami su uždaro kodo naudotojo aplinkos programinių sprendimu ir aplikacijų programavimo sąsaja (API), skirta senosioms sistemoms integruoti. Šiuos elementus teikia technologinis konsorciumo partneris. Kai kurios vyriausybės, dalyvaujančios blokų grandinės projektuose, skatina atverti sukurtus uždaro kodo elementus. Taip jos remia sukurtų sprendimų plėtrą į kitas platformas ir trečiųjų šalių taikomųjų programų kūrimą. Tokia strategija siekiama pagreitinti paslaugos adaptaciją ir prieinamumą.

**Blokų grandinė yra tik vienas sukurtos paslaugos sluoksnis, tačiau paslaugos kokybė paprastai priklauso ne nuo paskirstytojo registro technologijos sluoksnio.**

Blokų grandinė visada yra tik vienas iš kelių sistemos sluoksnių, o visuose projektuose naudojama centralizuota duomenų bazė, kurioje arba saugomi naudotojų duomenys, arba kuri tiekia sandorių duomenis į paskirstytąją sistemą. „Exonum“ ir „Stadjerspas“ projektuose naudojama centralizuota duomenų bazė sandorių duomenims saugoti. Blokų grandinės protokolas naudojamas tik maišos kodams, tačiau visa informacija apie sandorį saugoma centralizuotose duomenų bazėse. „Uport“ projekto atveju centralizuota duomenų bazė naudojama duomenų teikimui į paskirstytą sistemą, kai savivaldybė tikrina piliečio prašymo pagrįstumą ir susieja savo įrašus su „Uport“ adresu, vadinamu blokų grandinės tapatybe.

**Privatūs duomenys visada saugomi už grandinės ribų.**

Visuose projektuose privačių duomenų saugojimas yra kruopščiai suplanuotas. Kai naudojamasi leidimo nereikalaujančiomis arba viešosiomis blokų grandinėmis, privatūs duomenys saugomi už grandinės ribų centralizuotose saugyklose ("Exonum" atvejis) arba lokaliai naudotojo įrenginyje („Blockerts“ ir „uPort“ atvejai). Kai naudojama privati blokų grandinė su leidimais, privatūs duomenys iš esmės galėtų būti saugomi grandinėje užšifruota forma, tačiau didelių duomenų kiekių siuntimas tinklu paprastai yra neefektyvus dėl duomenų srauto pralaidumo apribojimų. Todėl kai kurie projektai ("Chromaway") papildomai naudoja išmaniųjų sutarčių platformą, kuri sujungia blokų grandinę su centralizuota duomenų baze ir registruoja visus įrašų pakeitimus.

**Sandorių pralaidumas nėra pagrindinė kliūtis.**

Stebimas akivaizdus skirtumas tarp leidimų reikalaujančių ir leidimų nereikalaujančių blokų grandinių atsižvelgiant į sandorių skaičių, kuriuos galima patvirtinti per tam tikrą laiko tarpą (angl transfer per second, abr. tps). Sandorių pralaidumas leidimo nereikalaujančios blokų grandinės protokoluose yra gerokai mažesnis (iki 7 tps) nei leidimų reikalaujančios blokų grandinės protokolų (160 - 5 000 tps). Projektai, kurie įtvirtina sandorius viešosiose leidimo nereikalaujančiose blokų grandinėse, sukūrė būdus, kaip sušvelninti pralaidumo apribojimus. Pavyzdžiui, jie vykdo sandorius partijomis arba maišos kodu šifruoja bendrą sistemos būseną. Projektai, kurie naudoja leidimų reikalaujančias blokų grandines, paprastai neturi jokių pralaidumo problemų, tačiau daugiausiai sandorių pralaidumo

reikalaujantys projektai („Pensijų infrastruktūra“) visgi susiduria su tam tikromis problemomis, susijusiomis su sandorių apdorojimu išmaniosiomis sutartimis.

**Blokų grandinės technologija nekelia grėsmės viešojo administravimo institucijų išlikimui.**

Didžioji dauguma analizuotų blokų grandinės technologija grindžiamų sprendimų papildo arba iš dalies pakeičia esamas viešąsias paslaugas. Papildantys sprendimai remiasi jau egzistuojančiais ir veikiančiais procesais („Exonum“ projektas). Iš dalies pakeičiantys sprendimai siūlo naujus paslaugų teikimo ar administracinės funkcijos organizavimo būdus. Pastaruoju atveju blokų grandinės technologija perima kai kurias viešųjų institucijų užduotis, pavyzdžiui tapatybės patvirtinimą arba tinkamumo paslaugos gavimui patikrą. Šie pokyčiai sumažina popierizmą ir sutaupo administravimui skiriamą laiką. Nė vienu iš paminėtu atvejų blokų grandinės technologija paremti sprendimai neeliminuoja viešosios institucijos veiklos. Galbūt tik „Chromaway“ yra vienintelis projektas, kuriame daroma prielaida, kad būtų galima atsisakyti notaro tarpininkavimo.

**Blokų grandine grindžiamų projektų įgyvendinimas reikalauja investicijų, tačiau diegimo sąnaudos nėra didesnės nei centralizuotų projektų atveju.**

Remiantis „Stadjerspass“ projekto, kuriame blokų grandine pagrįstas sprendimas buvo pasirinktas viešojo konkurso būdu, bendras diegimo išlaidų lygis yra tikrai konkurencingas. Blokų grandine grindžiamų paslaugų struktūra taip pat panaši į vienkartinių išlaidų struktūrą, kaip ir centralizuotų paslaugų. Kita vertus, projektai, kuriuose naudojamasi leidimo nereikalaujančiomis blokų grandinėmis, patiria naują sąnaudų elementą: mokesčius už sandorių patvirtinimą, mokamus nepastoviomis virtualiomis valiutomis (angl. cryptocurrencies). Naudojant sudėtingus ir daug energijos reikalaujančius konsensuso mechanizmus kelių sandorių patvirtinimui sukuriamos neproporcingai didelės veiklos sąnaudos.

**Blokų grandine grindžiamos paslaugos suteikia neabejotiną naudą ekosistemai.**

Pagrindiniai blokų grandinės technologijos teikiamos naudos viešajame sektoriuje veiksniai yra procesų efektyvumas ir sandorių duomenų skaidrumas. Sutrumpėjęs registracijos ir patikros laikas, greitesnis ir patikimesnis atsiskaitymas už sandorius ir popierinių kopijų atsisakymas galėtų potencialiai sutaupyti daug veiklos ir administravimo išlaidų. Blokų grandinės technologija taip pat suteikia nemažai kokybinių privalumų, didinančių kibernetinį saugumą bendrąja prasme: didesnis registro saugumas ir atsparumas bei duomenų vientisumo ir audito atlikimo garantijos. Centralizuotos patvirtinimo funkcijos panaikinimas taip pat suteikia strateginę naudą nevyriausybiniams ekosistemos dalyviams. Galiausiai, nors tai ne mažiau svarbu, blokų grandine grindžiamos paslaugos kartu su skaitmeninėmis naudotojų sąsajomis gali pagerinti bendravimo su valdžios institucijomis patirtį. Spausdintinių dokumentų ir vizitų į valdžios ar viešojo administravimo įstaigas, vien tik tam, kad būtų galima patvirtinti dokumentus arba gauti patvirtintas kopijas, atsisakymas- tai pavyzdiniai pokyčiai, kurių galima tikėtis ir kuriems neabejotinai pritartų ir piliečiai.

# IŠVADOS IR PASIŪLYMAI

1. Nors dar tik gimsta, blokų grandinės technologija siūlo daug žadančių naujovių sprendžiant nekintamus kibernetinės rizikos iššūkius, tokius kaip skaitmeninės tapatybės ir duomenų vientisumo išsaugojimą. Blokų grandinės potencialiai galėtų padėti pagerinti kibernetinę gynybą, nes ši technologija pasižymi projektiniu saugumu (angl. security by design) ir ja paremtos platformos gali apsaugoti duomenis, užkirsti kelią sukčiavimui pasitelkiant konsensuso mechanizmus, ir aptikti duomenų klastojimą remiantis pagrindinėmis blokų grandinės savybėmis: skaidrumu, galimybe atlikti auditą, duomenų šifravimu ir operaciniu atsparumu.

2. Blokų grandinės technologijos naudojimas teikiant viešąsias paslaugas kai kuriose srityse kuria neabejotiną pridėtinę vertę. Dvi pagrindinės su blokų grandine susijusios naudos grupės yra saugumas (duomenų vientisumo, nekintamumo ir nuoseklumo užtikrinimas) ir efektyvumas (sutrumpėjęs duomenų apdorojimo laikas ir mažesnės sąnaudos). Išmaniosios sutartys leidžia užtikrinti aukštą procesų automatizavimo lygį, o tai reiškia mažesnes administravimo sąnaudas ir saugojimo išlaidas, taip pat popierinių dokumentų tvarkymo atsisakymą. Žvelgiant iš piliečių perspektyvos, blokų grandinė, kartu su kitomis skaitmeninėmis decentralizuotomis technologijomis, gali panaikinti perteklinę biurokratiją, spausdintines kopijas ar apsilankymus viešojo administravimo institucijose nuotoliniu būdu valdomų mobiliųjų programėlių naudai. Dalis nepamatuojamos naudos, susijusi su piliečių sąveika su valdžios institucijomis, yra nepriklausomumo arba savarankiškumo įgijimas.

3. Priešingai nei dažnai vaizduojama, blokų grandinė kol kas nėra nei transformuojanti, nei griaunanti viešąjį sektorių. Nebuvo pastebėta jokių naujų verslo modelių sukūrimo ar naujos kartos paslaugų, nei tiesioginio kokių nors viešųjų institucijų, dalyvaujančių valdžios teikiamų paslaugų įgyvendinime, eliminavimo. Tikrai transformuojančios paslaugos, kuri įgalintų decentralizuotą balsavimą ar pilietinį valdymą tiesiogiai nedalyvaujant valdžios institucijoms, kol kas nėra. Visgi tyrime analizuotų blokų grandinės technologija paremtų projektų veiklos rezultatai leidžia pagrįstai tikėtis, kad blokų grandinė padidins viešojo sektoriaus valdymo efektyvumą ir skaitmeninės valdžios patikimumą bei sumažins sandorių sąnaudas ir neapibrėžtumą. Šią galimą naudą gautų administracija, piliečiai ir visa visuomenė.

**Pasiūlymai:**

- Blokų grandinės savybės nesuteikia neįveikiamos panacėjos visoms kibernetinio saugumo problemoms spręsti todėl, kaip ir su kitomis technologijomis, blokų grandinės diegimas privalo apimti tipinius kibernetinio saugumo standartus, tinklo kontrolės priemones, deramą kruopštumą, gerąją praktiką ir procedūras.

- Išankstinis standartizavimas ypač svarbus fundamentalioms paslaugoms, tokioms kaip viešojo administravimo modelio sistema ir decentralizuotas tapatybės valdymas, nes šie elementai sudaro galutiniam naudotojui teikiamų paslaugų pagrindą, tačiau siekiant išnaudoti visą šių paslaugų teikiamą naudą, būtina glaudžiau koordinuoti institucijų veiklą įgyvendinant ir eksploatuojant projektus. Pilnavertis įgyvendinimas turi būti racionalizuotas taikant bendras gaires, kad būtų užtikrinta saugumo, privatumo reikalavimų atitiktis ir techninė sąveika.
- Blokų grandine grindžiamų sprendimų nesuderinamumas su teisinėmis ir organizacinėmis sistemomis yra viena pagrindinių kliūčių, trukdančių išlaisvinti blokų grandinės transformacinį potencialą, todėl pagrindinis šios srities politikos tikslas turėtų būti paskirstytojo registro technologinės ir ekosistemos brandos kėlimas. Turėtų būti siekiama ne tik pritaikyti technologiją esamoms ekosistemoms, bet ir transformuoti esamus procesus, organizacijas ir struktūras, naudojant griaunamąjį blokų grandinės potencialą.

# LITERATŪRA

1. Atzori, M. (2015). *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?* Prieiga per internetą: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713

2. Atzori, M. (2017). *Blockchain Governance and the Role of Trust Service Providers: The TrustedChain Network.* doi: 10.2139/ssrn.2972837

3. Baležentis A. ir Žalimaitė M. (2011). *Ekspertinių vertinimų taikymas inovacijų plėtros veiksnių analizėje: Lietuvos inovatyvių įmonių vertinimas*. Vadybos mokslas ir studijos kaimo verslų ir jų infrastruktūros plėtrai, Nr. 3 (27).

4. Benedetti, H.E. ir Kostovetsky, L. (2018). *Digital Tulips? Returns to Investors in Initial Coin Offerings*. doi: 10.2139/ssrn.3182169

5. Bock, A.K., Bontoux, L., Nascimento, S. ir Szczepanikova, A. (2016). *The Future of the EU Collaborative Economy: Using Scenarios to Explore Future Implications for Employment.* Prieiga per internetą: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC102766/jrc102766 collaborative economy foresight final.pdf

6. Bodo, B. ir Giannopoulou, A. *The Logics of Technology Decentralization: the Case of Distributed Ledger Technologies*. Prieiga per internetą: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3330590

7. Boucher, P., Nascimento, S. ir Kritikos, M. (2017). *How Blockchain Technology Could Change Our Lives.* Prieiga per internetą: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf

8. Brekke, J.K. (2019). *Disassembling the Trust Machine: Three cuts on the political matter of blockchain* (daktaro disertacija). Prieiga per internetą: http://distributingchains.info/wp-content/uploads/2019/06/DisassemblingTrustMachine_Brekke2019.pdf

9. Buterin, V. (2014). *DAOs, DACs, DAs and More: An Incomplete Terminology Guide*. Prieiga per internetą: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide

10. Buterin, V. (2015). *A Next-Generation Smart Contract and Decentralized Application Platform.* Prieiga per internetą: https://github.com/ethereum/wiki/wiki/White-Paper

11. Caccioli, F., Livan, G. ir Aste, T. (2016). *Scalability and Egalitarianism in Peer-to-Peer Networks.* doi: 10.1007/978-3-319-42448-4

12. Casey, M.J. ir Vigna, P. (2018). *The Truth Machine: The Blockchain and the Future of Everything.* Niujorkas: Šv. Martyno leidykla.

13. Catlow, R., Garrett, M., Jones, N. ir Skinner, S. (2018). *Artists Re:Thinking The Blockchain.* Liverpulis: Liverpulio universiteto leidykla.

14. CEN-CENELEC. (2018). *Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies.* Prieiga per internetą: ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Sectors/ICT/Blockchain%20+%20DLT/FG-BDLT-White%20paper-Version1.2.pdf

15. ChromaWay. (2017). *Blockchain Land Registry Report 2017*. Prieiga per internetą: https://chromaway.com/papers/Blockchain_Landregistry_ Report_2017.pdf

16. Codagnone, C., Abadie, F. ir Biagi, F. (2016). *The Passions and the Interests: Unpacking the Sharing Economy*. Prieiga per internetą: https://ec.europa.eu/jrc/en/publication/eur-scientific-andtechnical-research-reports/passions-and-interests-unpacking-sharing-economy

17. Coincenter. (2015). *How Anonymous is Bitcoin?* Prieiga per internetą: https://coincenter.org/entry/how-anonymous-is-bitcoin

18. Coindesk. (2016). *Understanding The DAO Attack*. Prieiga per internetą: https://www.coindesk.com/understanding-dao-hack-journalist

19. Craglia, M. (2018). *Artificial Intelligence: A European Perspective*. Prieiga per internetą: https://publications.europa.eu/en/publication-detail/-/publication/ed2148f3-0288-11e9-adde-01aa75ed71a1/language-en/format-PDF/source-99349274

20. Crespigny, A.C. (2018). *How I Lost My Faith in Private Blockchains*. Prieiga per internetą: https://www.coindesk.com/how-i-lost-my-faith-inprivate-blockchains

21. Danezis, G. ir Meiklejohn, S. (2015). *Centrally Banked Cryptocurrencies.* doi: 10.14722/ndss.2016.23187

22. Davidson, S., De Filippi, P., ir Potts, J. (2016). *Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology.* doi: 10.2139/ssrn.2811995

23. De Filippi, P. (2016). *The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies*. Prieiga per internetą: http://peerproduction.net/issues/issue-9-alternative-Internets/peer-reviewed-papers/the-interplaybetween-decentralization-and-privacy-the-case-of-blockchain-technologies

24. De Filippi, P. ir Hassan, S. (2016). *Blockchain technology as a regulatory technology: From code is law to law is code.* Prieiga per internetą: http://firstmonday.org/ojs/index.php/fm/article/view/7113/5657

25. De Filippi, P. ir Wright, A. (2018). *Blockchain and the Law: The Rule of Code.* doi: https://doi.org/10.1016/j.joule.2018.04.016

26. Deloitte. (2017). *Evolution of blockchain technology Insights from the GitHub platform*. Prieiga per internetą: https://www2.deloitte.com/content/dam/insights/us/articles/4107_GitHub-blockchain/4107_Github-blockchain.pdf

27. EK. (2017)a. *Free flow of data and emerging issues of the European data economy*. Prieiga per internetą: https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-andemerging-issues-european-data-economy

28. EK. (2017)b. *Digital4Development: mainstreaming digital technologies and services into EU Development Policy*. Prieiga per internetą: https://ec.europa.eu/digital-single-market/en/news/digital4development-mainstreaming-digital-technologies-and-services-eu-development-policy

29. EK. (2017)c, d. *Review on the implementation of the Digital Single Market Strategy: A Connected Digital Single Market for All.* Prieiga per internetą: https://eur-lex.europa.eu/content/news/digital_market.html

30. ENISA. (2016). *Distributed Ledger Technology & Cybersecurity: Improving Information Security in the Financial Sector*. doi: 10.2824/80997

31. EP. (2018)a. *Distributed ledger technologies and blockchains: building trust with disintermediation*. Prieiga per internetą: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2018-0373&language=EN

32. EP. (2018)b. *Blockchain: a forward-looking trade policy.* Prieiga per internetą: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2018-0528&format=XML&language=EN

33. Esser, F. C., Abadie, F., Biagi, F., Martens, B., Bock, A.K., Bontoux, L., Nascimento, S. ir Szczepanikova, A., (2016). *The European Collaborative Economy: A Research Agenda for Policy Support*. Prieiga per internetą: http://publications.jrc.ec.europa.eu/repository/handle/JRC103256

34. Eurasianet. (2017). *Georgia: Authorities Use Blockchain Technology for Developing Land Registry*. Prieiga per internetą: https://eurasianet.org/georgia-authorities-use-blockchain-technology-developing-land-registry

35. Financial Times. (2017). *Reclaiming Europe's Digital Sovereignty.* Prieiga per internetą: https://www.ft.com/content/f096bcf6-87d5-4023-a9b5-73ae847076b2

36. Finck, M. (2017). *Blockchains and Data Protection in the European Union*. doi: 10.2139/ssrn.3080322

37. Finck, M. (2018). *Blockchain Regulation and Governance in Europe*. Kembridžas: Kembridžo universiteto leidykla.

38. Forbes. (2015). *Bitcoin's Value Isn't Currency, It's Technology*. Prieiga per internetą: https://www.forbes.com/sites/robertrosenkranz/2015/07/07/bitcoins-value-isnt-currency-its-technology/#179a405c1f11

39. Forbes. (2017)a. *The First Government To Secure Land Titles On The Bitcoin Blockchain Expands Project.* Prieiga per internetą: https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchainexpands-project/#5a9b2694dcdc

40. Forbes. (2017)b. *Why quantum computing's threat to bitcoin and blockchain is a long way off.* Prieiga per internetą: https://www.forbes.com/sites/amycastor/2017/08/25/why-quantum-computings-threat-to-bitcoin-and-blockchain-is-along-way-off/#1f3b295a2882

41. Fortune. (2017). *How Bitcoin Is Stolen: 5 Common Threats*. Prieiga per internetą: https://fortune.com/2017/12/08/bitcoin-theft/

42. Gartner. (2018)a. *Hype Cycle for Blockchain Technologies*. Prieiga per internetą: https://www.gartner.com/doc/3883991/hype-cycleblockchain-technologies

43. Gartner. (2018)b. *Blockchain Status 2018: Market Adoption Reality*. Prieiga per internetą: https://www.gartner.com/doc/3869693/blockchainstatus--market-adoption

44. Gartner. (2018)c. *Blockchain-Based Transformation*. Prieiga per internetą: https://www.gartner.com/doc/3869696/blockchainbased-transformation-gartner-trend-insight

45. Gencer, A.E., Basu, S., Eyal, I., Renesse, R. ir Van Sirer, E.G. (2018). *Decentralization in Bitcoin and Ethereum Networks.* Prieiga per internetą: https://arxiv.org/abs/1801.03998

46. Goldfeder, S., Kalodner, H., Reisman, D. ir Narayanan, A. (2017). *When the Cookie Meets the Blockchain: Privacy Risks of Web Payments Via Cryptocurrencies.* Prieiga per internetą: https://arxiv.org/abs/1708.04748

47. Grech, A. ir Camilleri, A. F. (2017). *Blockchain in Education*. Prieiga per internetą: http://nbnresolving.de/urn:nbn:de:0111-pedocs-150132

48. Inamorato dos Santos, A. (2017). *Blockchain in Education*. Prieiga per internetą: http://publications.jrc.ec.europa.eu/repository/handle/JRC108255

49. Khalil, F., Butler, T., OBrien, L. ir Ceci, M. (2017). *Trust in Smart Contracts Is a Process, as Well.* doi: 10.1007/978-3-319-70278-0-32

50. Killmeyer, J., White, M., ir Chew, B. (2017). *Will blockchain transform the public sector?* JAV, Teksaso valstija: Deloitte universiteto leidykla.

51. Kounelis, I., Di Gioia, R., Geneiatakis, D., Steri, G., Neisse, R., Karopoulos, G., ir Giuliani, R. (2017). *Blockchain in Energy Communities*. Prieiga per internetą: https://ec.europa.eu/jrc/en/publication/blockchain-energy-communities-proof-concept

52. Lapointe, C., ir Fishbane, L. (2018). *The Blockchain Ethical Design Framework*. Džordžtaunas: Džordžtauno universitetas.

53. Lemieux, V.L. (2016). *Trusting Records: Is Blockchain Technology the Answer?*. doi: 10.1108/RMJ-12-2015-0042

54. Lewis, A.M., Ferigato, C., Travagnin, M. ir Florescu, E. (2018). *The Impact of Quantum Technologies on the EU's Future Policies*. Prieiga per internetą: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC110412/quantum_computing_report_v5.4.pdf

55. Lovells, H. (2017). *A Guide to Blockchain and Data Protection*. Prieiga per internetą: https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf

56. Macdonald, T.J., Allen, D.W.E. ir Potts, J. (2016). *Blockchains and the Boundaries of Self-Organized Economies: Predictions for the Future of Banking. doi: 10.1007/978-3-319-42448-4*

57. Martinovic, I. (2017). *Blockchains for Governmental Services: Design Principles, Applications, and Case Studies*. Prieiga per internetą: https://www.ctga.ox.ac.uk/sites/default/files/ctga/documents/media/wp7_martinovickellosluganovic.pdf

58. Mcook, H. (2018). *The Cost & Sustainability of Bitcoin.* Prieiga per internetą: https://www.academia.edu/37178295/The_Cost_and_Sustainability_of_Bitcoin_August_2018_

59. Mora, C., Rollins, R.L., Taladay, K., Kantar, M.B., Chock, M.K., Shimada, M. ir Franklin, E.C. (2018). *Bitcoin emissions alone could push global warming above 2°C.* doi: 10.1038/s41558-018-0321-8

60. Mougayar, W. (2015). *An Operational Framework for Decentralized Autonomous Organizations.* Prieiga per internetą: http://start-upmanagement.org/2015/02/04/an-operational-framework-for-decentralized-autonomous-organizations

61. Mougayar, W. (2016). *The Business Blockchain: Promise, Practice and Application of the next Internet Technology*. Niujorkas: leidykla Wiley.

62. Mougayar, W. (2017). *Tokenomics – A Business Guide to Token Usage, Utility and Value.* Prieiga per internetą: https://medium.com/@wmougayar/tokenomics-a-business-guide-to-token-usage-utility-and-value-b19242053416

63. Narayanan, A., Toubiana, V., Barocas, S., Nissenbaum, H. ir Boneh, D. (2012). *A Critical Look at Decentralized Personal Data Architectures.* Prieiga per internetą: http://arxiv.org/abs/1202.4503

64. New York Times. (2018). *There Is Nothing Virtual About Bitcoin's Energy Appetite.* Prieiga per internetą: https://www.nytimes.com/2018/01/21/technology/bitcoin-mining-energy-consumption.html?mtrref=undefined

65. Norta, A. (2015). *Creation of Smart-Contracting Collaborations for Decentralized Autonomous Organizations. doi: 10.1007/978-3-319-21915-8_1*

66. OECD. (2016). *OECD Science, Technology and Innovation Outlook 2016.* Prieiga per internetą: http://dx.doi.org/10.1787/sti_in_outlook-2016-6-en

67. OECD. (2017). *The Next Production Revolution: Implications for Governments and Business*. Prieiga per internetą: http://dx.doi.org/10.1787/9789264271036-en

68. Orcutt, M., (2018). *States that are passing laws to govern smart contracts have no idea what they're doing.* Prieiga per internetą: https://www.technologyreview.com/s/610718/states-that-are-passing-laws-to-govern-smartcontracts-have-no-idea-what-theyre-doing/

69. Peters, G.W., ir Panayi, E. (2016). *Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money*. doi: 10.1007/978-3-319-42448-4

70. PwC. (2016). *Blockchain: The 5 Billion Opportunity for Reinsurers*. Prieiga per internetą: http://www.pwc.com/gx/en/industries/financial-services/publications/blockchain-the-5-billion-opportunity-for-reinsurers.htm

71. Quartz. (2016). *Everything you need to know about the Ethereum hard fork.* Prieiga per internetą: https://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork

72. Quintais, J.P., Bodo, B., Giannopoulou, A. ir Ferrari, V. (2019). *Blockchain and the Law: A Critical Evaluation*. Prieiga per internetą: https://stanford-jblp.pubpub.org/pub/blockchain-and-law-evaluation

73. Rauchs, M., Glidden, A., Gordon, B., Pieters, G., Recanatini, M., Rostand, F., Vagneur, K. ir Zhang, B., (2018). *Distributed Ledger Technology Systems: A Conceptual Framework*. Prieiga per internetą: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-10-26- conceptualising-dlt-systems.pdf

74. Rogers, F. ir Shoemaker, F. (1971). *Communication of innovations : a cross-cultural approach*. Free Press.

75. Santander. (2015). *The Fintech 2.0 Paper: rebooting financial services*. Prieiga per internetą: http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf

76. Satis Group. (2018). *Cryptoasset Market Coverage Initiation: Network Creation.* Prieiga per internetą: https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ

77. Schwab, K. (2017). *The Fourth Industrial Revolution.* Niujorkas: Crown Business.

78. Symons, T. ir Bass, T. (2017). *Me, My Data and I: The Future of the Personal Data Economy*. Prieiga per internetą: https://decodeproject.eu/publications/me-my-data-and-ithe-future-personal-data-economy

79. Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. JAV, Sebastopol: O'Reilly Media.

80. Szabo, N. (1997). *The Idea of Smart Contracts*. Prieiga per internetą: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html

81. Tapscott, D. ir Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Niujorkas: Penguin leidykla.

82. Tasca, P. ir Tessone, C. (2018). *Taxonomy of Blockchain Technologies. Principles of Identification and Classification*. Prieiga per internetą: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2977811

83. The Bitfury Group. (2017). *The Bitfury Group and Government of Republic of Georgia Expand Historic Blockchain Land-Titling.* Prieiga per internetą: https://medium.com/@BitfuryGroup/the-bitfury-group-and-government-of-republic-of-georgiaexpand-historic-blockchain-land-titling-4c507a073f6b

84. The Economist. (2014). *The trust machine: The promise of the blockchain.* Prieiga per internetą: https://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

85. Van Wirdum, A. (2015). *Is Bitcoin Anonymous? A Complete Beginner's Guide.* Prieiga per internetą: https://bitcoinmagazine.com/articles/is-bitcoin-anonymous-a-complete-beginner-s-guide-1447875283/

86. Van Zuidam, R. (2017). *Blockchain for dummies - 5 questions to Blockchain expert Rutger van Zuidam.* Prieiga per internetą: https://www.cityoftalent.nl/en/news/blockchain-for-dummies---5-questions-to-blockchain-expert-rutger-van-zuidam

87. Walch, A. (2017). *The Path of the Blockchain Lexicon (and the Law).* Prieiga per internetą: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2940335

88. WEF. (2015). *Deep Shift Technology Tipping Points and Societal Impact*. Prieiga per internetą: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

89. WEF. (2018). *Blockchain Beyond the Hype*. Prieiga per internetą: https://www.weforum.org/whitepapers/blockchain-beyond-the-hype

90. Wired. (2017)a. *I Forgot My Pin: An Epic Tale of Losing $30,000 in Bitcoin.* Prieiga per internetą: https://www.wired.com/story/i-forgot-my-pin-an-epic-tale-of-losing-dollar30000-in-bitcoin

91. Wired. (2017)b. *This man's lost bitcoin are now worth $75m – and under 200,000 tonnes of garbage.* Prieiga per internetą: http://www.wired.co.uk/article/bitcoin-lost-newport-landfill

Rupšys V. (2022). *Blokų grandinės sistemų vaidmuo organizacijų kibernetinio saugumo sprendimų įgyvendinime* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

# ANOTACIJA

Magistro baigiamajame darbe išanalizuotas ir įvertintas blokų grandinės technologijos vaidmuo transformuojant Europos šalių viešojo sektoriaus valdymą per kibernetinio saugumo prizmę. Pirmame skyriuje analizuojami teoriniai blokų grandinės aspektai tokie kaip decentralizacija, skaidrumas, saugumas ir išmaniosios sutartys, taip pat pateikiami lūkesčiai, prognozės bei pateikiamos įžvalgos. Antrame skyriuje nagrinėjama blokų grandinė skaitmeninės valdžios kontekste ES politikos lygmeniu bei viešojo sektoriaus valdymo transformacijos. Trečiame skyriuje pateikiama Europos šalių viešojo sektoriaus blokų grandinės technologija paremtų projektų empirinė analizė apžvelgiant technologijos naudojimą pasaulio ir Europos mastu bei atliekant horizontalų atrinktų projektų palyginimą, tokiu būdu įvertinant blokų grandinės vaidmenį transformuojant viešąjį sektorių.

**Pagrindiniai žodžiai:** blokų grandinė, skaitmeninė valdžia, kibernetinis saugumas, viešojo sektoriaus transformacija

Rupšys V. (2022). *The role of blockchain systems in the implementation of cybersecurity solutions for organisations* (master thesis). Vilnius: Mykolas Romeris University

## ANNOTATION

In the master thesis the role of blockchain technology in transforming the governance of the public sector in European countries through the prism of cybersecurity is analysed and evaluated. The first chapter analyses the theoretical aspects of blockchain such as decentralisation, transparency, security and smart contracts as well as expectations and forecasts. The second chapter examines the blockchain in the context of digital government at EU policy level and transformations in public sector governance. The third chapter presents an empirical analysis of blockchain technology-based public sector projects in European countries, providing an overview of the usage of the technology on a global and European scale and a horizontal comparison of the selected projects, thus assessing the role of blockchain in the transformation of public sector.

**Keywords:** blockchain, digital government, cybersecurity, public sector transformation

Rupšys V. (2022). *Blokų grandinės sistemų vaidmuo organizacijų kibernetinio saugumo sprendimų įgyvendinime* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

# SANTRAUKA

Paskirstytasis registras gali tapti nauja informacine infrastruktūra, palaikančia keitimąsi informacija tarp viešojo administravimo institucijų, piliečių ir įmonių, todėl buvo iškelta pagrindinė tyrimo problema- kaip blokų grandinės sistemų naudojimas keičia ES viešojo sektoriaus kibernetinio saugumo paradigmą? Darbo objektas- blokų grandinės sistemos kibernetinio saugumo kontekste. Šio darbo tikslas yra ištirti blokų grandinės technologijos vaidmenį Europos šalių viešajame sektoriuje įgyvendinant skaitmeninės valdžios koncepciją kibernetinio saugumo aspektu. Taip pat buvo iškelti ir darbo uždaviniai: aptarti blokų grandinės teorinį konceptą, įvertinti blokų grandinės sistemų vaidmenį kibernetinio saugumo kontekste, pristatyti blokų grandinės technologijos pritaikymo galimybes viešojo sektoriaus perspektyvoje ir išanalizuoti blokų grandinės naudojimą Europos šalių viešajame sektoriuje. Tyrimo metodika: mokslinės literatūros analizė, lyginamoji analizė, kokybinė turinio analizė, daugybinių atvejų studija.

Magistro baigiamojo darbo empirinio tyrimo tikslas buvo identifikuoti ir pagal nustatytus kriterijus empiriškai įvertinti Europos šalių viešojo sektoriaus projektus, kurie naudoja blokų grandinės technologiją. Išsikelti tokie uždaviniai: įvertinti blokų grandinės naudojimo mastą Europos šalyse bei nustatyti blokų grandinės technologijos naudojimo teikiamą naudą skaitmeninės valdžios ir piliečių atžvilgiu. Buvo atliekamas kombinuotas tyrimas, taikant kokybinio ir kiekybinio tyrimo strategijas. Tyrimo imties sudarymui pasirinkta netikimybinė tikslinė atranka**.** Tyrimo imtis- Europos šalių viešojo sektoriaus blokų grandinės technologija paremti projektai.

Blokų grandinė grindžiama ypatingu pagrindinių savybių deriniu: decentralizacija, atsparumu klastojimui, skaidrumu, saugumu ir išmaniosiomis sutartimis. Tokia sistema yra atspari trikdžiams, gedimams ar sabotažui, nes nėra centrinio subjekto, kontroliuojančio sistemą, tačiau nepaisant visų blokų grandinės galimybių, vis dar neišspręsta nemažai iššūkių, tokių kaip ribotas išplečiamumas, maža sandorių apimtis viešose blokų grandinėse, arba didelis energijos suvartojimas naudojant darbo įrodymo konsensuso mechanizmus.

Visgi kol kas blokų grandinė nėra nei transformuojanti, nei griaunanti viešąjį sektorių, kaip dažnai vaizduojama. Blokų grandinės sistemos nepakeičia esamų viešųjų institucijų sistemų. Blokų grandinę vis dar reikia integruoti su senosiomis sistemomis, kad būtų galima suteikti naujų papildomų funkcijų. Ši technologija taip pat vis dar priklauso nuo centralizuotų sistemų duomenų.

Magistro baigiamojo darbo pabaigoje pateikiamos išvados bei pasiūlymai dėl blokų grandinės technologijos naudojimo viešojo sektoriaus valdyme.

Rupšys V. (2022). *The role of blockchain systems in the implementation of cybersecurity solutions for organisations* (master thesis). Vilnius: Mykolas Romeris University

## SUMMARY

The distributed ledger has the potential to become a new information infrastructure supporting the exchange of information between public administrations, citizens and businesses, which is why the main research question was posed - how does the use of blockchain systems change the cybersecurity paradigm in the EU public sector? The subject of the paper is blockchain systems in the context of cybersecurity. The aim of this thesis is to investigate the role of blockchain technology in the public sector of European countries in the context of the implementation of the digital government concept from a cybersecurity perspective. The objectives of the thesis were: to discuss the theoretical concept of blockchain, to assess the role of blockchain systems in the context of cybersecurity, to present the applicability of blockchain technology in the public sector and to analyse the use of blockchain in the public sector of European countries. Research methodology: analysis of scientific literature, comparative analysis, qualitative content analysis, multiple case studies.

The aim of the empirical study of the master's thesis was to identify and empirically evaluate, according to defined criteria, public sector projects in European countries that use blockchain technology. The objectives were: to assess the extent of blockchain use on European scale and to identify the benefits of blockchain technology for digital government and citizens. A combined study was carried out using qualitative and quantitative research strategies. Non-probability purposive sampling was used to select the study sample. The sample is public sector blockchain technology-based projects in European countries.

Blockchain is based on a particular combination of key characteristics: decentralisation, tamper-proofing, transparency, security and smart contracts. Such a system is resilient to disruptions, failures or sabotage, as there is no central entity controlling the system, but despite the full potential of blockchain, a number of challenges are still outstanding, such as the limited scalability, the low transaction volumes in public blockchains, or the high energy consumption of the use of proof of work consensus mechanisms.

However, so far, blockchain is neither transformative nor disruptive to the public sector, as is often portrayed. Blockchain systems do not replace existing systems of public institutions. Blockchain still needs to be integrated with legacy systems to provide new additional functions. The technology is also still dependent on data from centralised systems.

The master thesis concludes with conclusions and proposals for the use of blockchain technology in public sector management.

# PRIEDAI

1 PRIEDAS. Tyrime panaudota anketa

Hello, I am a student of Mykolas Romeris University and I am a currently scanning for projects to complement my master thesis regarding DLT projects in Europe and the role of the blockchain in the cybersecurity field. I would like to invite you to share information about your project and help me widen my research scope. There is a 24 questions in the survey and it should take no more than 15 minutes. Thank you in advance!

1. What is the name of the project?

_____

_____

2. What level of goverment is involved in the project?
   - o National
   - o Local

3. Is your project internationalr?
   - o Yes
   - o No

4. Is your project cross-sector?
   - o Yes
   - o No

5. Do the project gather location data?
   - o Yes
   - o No

6. What type of software is used in the project?
   - o Open source
   - o Proprietary
   - o Hybrid

7. What institutions (if any) is disintermediated when using your solution instead of legacy system?

_____

_____

_____

_____

8.What blockchain functionalities is leveraged in your project?

- Notarization
- Smart contract automation
- Shared database

9. What is the composition of the consorcium of the project?

_____

_____

10. What architecture of the blockchain your project use?

- Private permissioned
- Private permissionless
- Public permissioned
- Public permissionless

11. What governance model of consortium is used in your project?

- Centralized
- Decentralized
- Hybrid

12. What is current usage of the project?

_____

_____

13. What is the current stage of your project?

- Proof of Concept / Demo
- Pilot / Beta Launch
- In-Production / Live
- Stalled / Aborted / Ended
- Other

14. What is current throughput of the project?

_____

_____

15. What is scalability of the project?

_____

_____

16. What user layer is used in the project?

_____

_____

17. What other (non-DLT) systems is used in the project?

_____

_____

18. What API layer is used in the project?

_____

_____

19. What consensus mechanizm is used in the project?

_____

_____

20. What infrastructure is used in the project?

_____

_____

21. What are non-recurring costs regarding the project?

_____

_____

22. What are recurring costs regarding the project?

_____

_____

23. What are quantitative benefits regarding the project?

_____

_____

24. What are qualitative benefits regarding the project?

_____

_____

*Thank you for taking the time to participate in this questionare.*