MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

LINVIDA URBAITĖ

BLOKŲ GRANDINĖS TECHNOLOGIJOS ENERGETIKOS SEKTORIUJE: KIBERNETINIO SAUGUMO IŠŠŪKIAI IR GALIMYBĖS

Magistro baigiamasis darbas

Vadovas:

Prof. Dr. Mindaugas Kiškis

Vilnius, 2024

MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

BLOKŲ GRANDINĖS TECHNOLOGIJOS ENERGETIKOS SEKTORIUJE: KIBERNETINIO SAUGUMO IŠŠŪKIAI IR GALIMYBĖS

Kibernetinio saugumo valdymo magistro baigiamasis darbas

Studijų programa 6211LX066

Vadovas

_____ Prof. Dr. Mindaugas Kiškis

2024 05 03

Recenzentas

_____

2024

Atliko

KSVvmis22-1 gr. stud.

_____ L. Urbaitė

2024 05 03

Vilnius, 2024

TURINYS

LENTELĖS

PAVEIKSLAI

SANTRUMPOS/PAAIŠKINIMAI

BC (angl. Blockchain) **–** blokų grandinė.

B2B – verslas verslui (B2B), dar vadinamas B-to-B, yra verslo sandorių forma, pavyzdžiui, susijęs su gamintoju ir didmenininku arba didmenininku ir mažmenininku. Verslas verslui reiškia verslą, kuris vykdomas tarp įmonių, o ne tarp įmonės ir individualaus vartotojo.

Fotovoltinė sistema – saulės energijos sistema, kuri saulės šviesą paverčia elektra**.** Ji naudoja saulės baterijas, kad gautų saulės šviesą ir paverstų ją tinkama elektros energija gyvenamosioms, komercinėms ir pramoninėms reikmėms.

Hash – funkcija, konvertuojanti raidžių ir skaičių įvestį į užšifruotą fiksuoto ilgio išvestį.

Konsorciumas – laikinas ir sutartimis paremtas dviejų ar daugiau teisiškai ir ekonomiškai savarankiškų ir tokiomis išliekančių bendrovių susivienijimas, siekiant kartu imtis bendro projekto, verslo, derėtis ar įgyvendinti sandorį.

Merkle tree – „merkle“ medis yra būdas tvarkyti ir struktūrizuoti didelius duomenų kiekius, kad būtų lengviau juos apdoroti. Kriptovaliutos ir blokų grandinės atveju „Merkle“ medis naudojamas sandorių duomenims struktūrizuoti mažiau išteklių reikalaujančiu būdu.

P2P (angl. Peer -to- peer) **–** tinklo modelis, kuriame keitimasis resursais vyksta tiesiogiai tarp vartotojų.

REC (angl. Renewable Energy corporation) – atsinaujinančios energijos korporacija.

XML (angl. Extensible Markup Language**)** – W3C rekomenduojama bendros paskirties duomenų struktūrų bei jų turinio aprašomoji kalba. Pagrindinė XML kalbos paskirtis yra užtikrinti lengvesnį duomenų keitimąsi tarp skirtingo tipo sistemų, dažniausiai sujungtų internetu.

papiNet – pasaulinis komunikacijos XML standartas popieriaus ir miško produktų pramonei. PapiNet palengvina verslo procesų automatizavimą pramonėje, todėl verslo partneriams lengviau susitarti dėl duomenų apibrėžimų ir formatų.

EFET (angl. European Federation of Energy Traders) – Europos energijos prekybininkų federacija yra Europos energijos prekybininkų asociacija didmeninės elektros ir dujų rinkose. EFET buvo įkurta 1999 m. reaguojant į elektros ir dujų rinkų liberalizavimą Europos Sąjungoje.

EV(angl. Electrical Vechiles) – elektrinės transporto priemonės.

PV(angl. Photovoltaics) – yra šviesos pavertimas elektra naudojant puslaidininkines medžiagas, turinčias fotovoltinį efektą – reiškinį, tiriamą fizikoje, fotochemijoje ir elektrochemijoje. Fotovoltinis efektas komerciškai naudojamas elektros gamybai ir kaip fotosensorius.

ĮVADAS

Temos aktualumas 2022 metais kovo mėnesį Jungtinis tyrimų centras pateikė ataskaitą apie „*Blockchain sprendimus, skirtus energijos perėjimui*“ ir patvirtina, kad blokų grandinė turi didelį potencialą, būti naudojama energijos bendruomenėje kaip „decentralizuotas varomasis centras“, o tai iš esmės pakeistų energetikos sektorių (Jungtinis tyrimų centras, 2022).

Alexander Freier 2024 metais išleido knygą: „Blockchain energetikos sektoriuje. Pažangi technologija, skirta kovoti su pasauline klimato kaita?“. Nuo 2019 m. jis tiria galimybes įgyvendinti blokų grandinėmis pagrįstus sprendimus energetikos sektoriuje, taip pat jų potencialą naudoti kaip klimato technologijas. Atsinaujinantys energijos šaltiniai tapo pagrindiniu pasaulinio aplinkos valdymo srities tyrimų objektu. Atsižvelgiant į tai, naujomis techninėmis naujovėmis siekiama įveikti iššūkius, kylančius dėl nepastovios atsinaujinančios energijos gamybos ir trūkstamų saugojimo pajėgumų. „Blockchain“ – paskirstytos knygos technologija, naudojanti kriptografiją, tapo svarbi vis labiau decentralizuotos ir skaitmenizuojamos pasaulinės energetikos infrastruktūros sudedamoji dalis.

Blokų grandinių technologija taikoma finansų sektoriuje, vyriausybės sektoriuje, daiktų internete (IoT), kibernetinio saugumo programose, debesų saugykloje, išmaniajame nuosavybės valdyme, notaruose, nekilnojamajame turte, išmaniuosiuose kontaktuose, tapatybės valdyme, išmaniuosiuose miestuose, medicininių vaizdų vandenženkliuose ir transporto tinkluose (Alrammal, M.; Abu-Amara, F.; Ismail, Z.; Nadeem, 2023). Pranešama, kad transakcijų integravimas į „blockchain“ technologiją pagerina skaidrumą, sumažina kibernetines grėsmes ir padidina pasitikėjimą viešuoju sektoriumi (Lannquist, A.; Raycraft, R.D., 2022).

Šiuolaikinės BC programos apima platų naudojimo spektrą nuo mažo sudėtingumo, pvz., mokėjimų kriptovaliuta, iki sudėtingesnių programų, tokių kaip išmaniosios sutartys. „Blockchain“ tiekimo grandinė gali pasiūlyti stebėjimo funkciją labai sudėtingoje aplinkoje. Kadangi blokų grandinės technologija ir toliau populiarėja, didelio masto viešosios identifikavimo sistemos, tokios kaip pasų kontrolė ir dokumentų autentifikavimas, yra keletas revoliucinių BC technologijos panaudojimo būdų (Gad ir kt.2022.; Gans ir kt 2022.; Haque ir kt.2021).

„Blockchain“ technologija pastaruoju metu pritraukia daug dėmesio tiek akademinių tyrimų, tiek pramonės srityse, įskaitant energetikos pramonę. „Blockchain“ yra vertinama kaip novatoriška technologija, galinti pagerinti įprastą verslo būdą, ypač tuos, kuriems nereikalingas tarpininkas (A Simaremare, I Aditya, F Haryadi ir H Indrawan, 2020, p. 1).

Decentralizuota „blockchain“ technologija vis labiau pripažįstama kaip žaidimų keitiklis visiems centralizuotiems dalykams, įskaitant tradicinę centralizuotą energiją. Tuo tarpu energetikos sektoriuje vyksta transformacija iš tradicinės centralizuotos energijos tiekimo sistemos į paskirstytą energijos šaltinį (Q. Wang, R. Li, L. Zhan, 2021).

Vokietija ir daugelis Europos šalių šiuo metu yra pereinamojo laikotarpio energetikos įkarštyje. Atsinaujinantys energijos šaltiniai yra svarbi jos dalis. Demontuojamos atominės ir anglimi kūrenamos elektrinės, statomi vėjo ir saulės parkai. Be to, vis daugiau privačių namų ūkių gamina energiją patys. Tai keičia energijos tiekimą iš centrinio į decentralizuotą tinklą.

Paryžiaus susitarime atsižvelgiama į šį didėjantį sudėtingumą ir raginama taikyti daugiapakopius metodus siekiant sumažinti išmetamųjų teršalų kiekį. „Blockchain“ technologija gali atlikti pagrindinį vaidmenį, jei ji bus tinkamai taikoma skirtingose klimato rinkose (Alexander Frier, 2024).

Šiais neramiais ir netaikiais laikais svarbu užtikrinti energetikos sektoriaus saugumą ir efektyvumą. Didėjant kibernetinei rizikai iš įvairių šalių bei nusikalstamų grupuočių, siekiant sustiprinti gynybą ir atsaką, būtina sukurti veiksmingą kibernetinio saugumo kultūrą ir struktūrą. Visoms energetikos sektoriaus bendrovėms reikalinga standartizuota kibernetinės rizikos matavimo ir vertinimo sistema ir skaidrios paslaugų teikimo atkūrimo po atakos procedūros. Didžiausias prioritetas teikiamas ypatingos svarbos turtui, kuris turi įtakos vartotojų galimybei gauti elektros energiją. Iki šiol energetikos sektoriuje trūko pasauliniu mastu nuoseklių kibernetinio saugumo standartų. Norint padidinti atsparumą ir taip padidinti pasitikėjimą bei paspartinti energetikos pertvarką, skubiai reikia dalintis informacija ir taikyti tvirtą kibernetinio saugumo, atitikties ir rizikos politiką.

Technologijų plėtra konkrečioje pramonės šakoje reikalauja ir reguliavimo, ir politikos reformų. Atsižvelgiant į tai, šiame darbe nagrinėjami tarptautiniu mastu funkcionuojantys blokų grandinės technologijos modeliai energetikos pramonėje, pavyzdžiui, inovacijos prekybai (naudojant „išmaniąsias sutartis“) ir investicijoms bei skatinant lygiavertę (P2P) energijos gamybą (R. Karim, I. Sifat, 2022, p. 110).

Didžiausias Japonijos energijos tiekėjas sukūrė įmonę „Trende“, kuri bandė pradėti saulės energijos gamybą ir leisti P2P pirkti saulės energijos technologijas per „blockchain“ (Martin, 2018).

JAV įsikūrusios bendrovės „TransActive Grid“, „PowerLedger“ ir „Singularity“ iš Australijos, „Ideo CoLab“ ir kt. yra keletas pradedančiųjų energetikos pramonės įmonių, kurios efektyviai naudoja „blockchain“ technologiją (J. Wang, Q. Wang, N. Zhou, Y. Chi, 2017).

Mokslinė problema – ar blokų grandinės technologijos taikymas energetikos sektoriuje gali užtikrinti saugumą ir efektyvumą?

Tyrimo objektas – blokų grandinės technologija energetikos sektoriuje.

Tyrimo tikslas – ištirti blokų grandinės taikymo ypatumus ir galimybes, pranašumus ir trūkumus energetikos sektoriuje. Pateikti kibernetinio saugumo galimybes ir iššūkius taikant blokų grandinę bei pateikti rekomendacijas.

Tyrimo uždaviniai:

1. Išanalizuoti blokų grandinės technologijos struktūrą, veikimo principą ir reikšmę šiandieninėje sistemoje.

2. Ištirti „Blockchain“ technologijos taikymą energetikos sektoriuje.

3. Išanalizuoti kibernetinį saugumą blokų grandinės taikyme energetikos sektoriuje.

4. Išanalizuoti ir palyginti blokų grandinės taikymo atvejus energetikos sektoriuje Europoje ir visame pasaulyje.

5. Ištirti ekspertų požiūrius į blokų grandinės technologiją, taikymą, diegimo tikėtiną poveikį ir galimas problemas energetikos sektoriuje. (Nustatyti ir pateikti blokų grandinės pritaikymo galimybes).

6. Pateikti rekomendacijas ir pasiūlymus.

Moksliniai tyrimo metodai:

1. Mokslinės literatūros šaltinių analizė, sisteminimas ir apibendrinimas.

2. Statistinių duomenų analizė ir interpretacija.

3. Atvejų analizė.

4. Ekspertinio tyrimo metodas – ekspertų interviu.

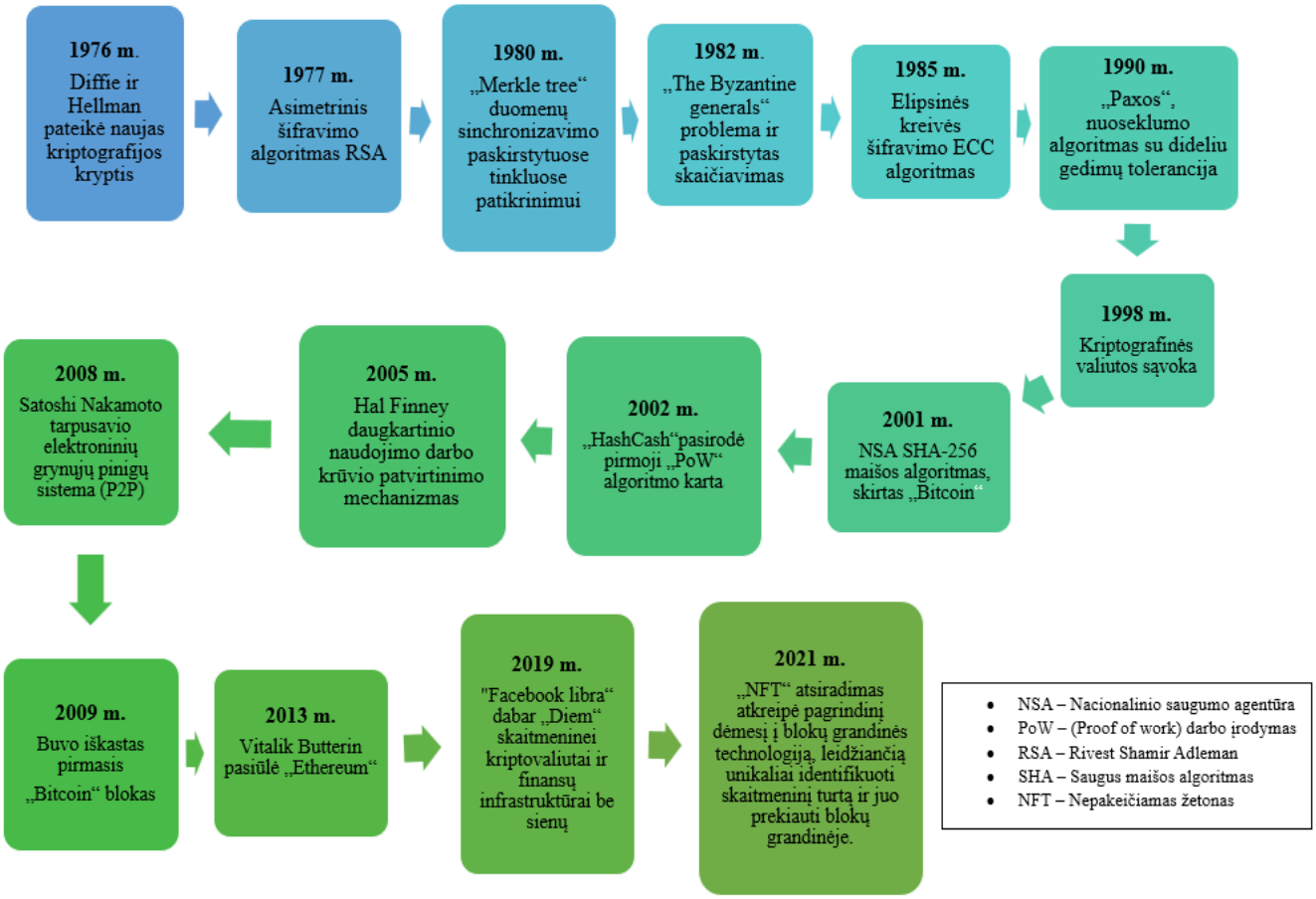
Tyrimo struktūra. Darbą sudaro 4 dalys. Pirmoje dalyje nagrinėjami blokų grandinės teoriniai aspektai: analizė ir raida, samprata ir kibernetinis saugumas. Antroje dalyje analizuojama blokų grandinės taikymas energetiniame sektoriuje. Apžvelgiami kibernetinio saugumo klausimai. Trečioje dalyje aprašomi pasirinkti tyrimo metodai. Ketvirtoje dalyje atliekama atvejų analizė, energetikos įmonės pasirinkusios blokų grandinės technologijos taikymą. Nagrinėjami ekspertų interviu gauti duomenys, interviu atsakymams susisteminti naudojamas Microsoft Excel paketas. Darbo pabaigoje pateikiamos išvados ir rekomendacijos.

Temos ištirtumo lygis. Alexander Freier (2024) parašė knygą „Blockchain in energy sector“, Vani Rajasekar, K. Sathya (2023) apžvelgė „Blockchain“ naudingumą atsinaujinančios energijos srityje, Andoni, M., Robu, V., Flynn ir kt. (2019) tyrė apie blokų grandinės technologijos iššūkius ir galimybes energetikos pramonėje. Wang Q ir kt. (2020) daugiausia rašė apie „blockchain“ technologijos naudojimą plečiant atsinaujinančius energijos šaltinius, siekiant sumažinti iškastinės energijos poreikį. Kirli, D, Couraud, B, Robu ir kt. (2022) sutelkė dėmesį į konkrečią sritį: išmaniųjų sutarčių taikymą energijos blokų grandinėse ir parodė šios technologijos privalumus ir trūkumus keliais naudojimo atvejais, susijusiais su energetikos pramone. Li, H, Xiao, F, Yin, L, Wu, atliko blokų grandinės technologijos naudojimo prekyboje energija, kaip vienos konkrečios energijos blokų grandinės taikymo, apžvalgą. Europos sąjunga iniciavo įvairius tyrimus. Vokietijos energetikos sektorius taip pat vykdė kelis metus, blokų grandinės pritaikymą šiame sektoriuje. A. Goudz ir M. Jasarevic aprašė knygoje : „Einsatz der Blockchain-Technologie im Energiesektor“. Lietuvoje buvo tiriama P. Danieliaus (2019) „Blokų grandinės technologija grindžiamo taikomojo modelio decentralizuotam elektros energijos skirstymui sukūrimas“.

1. „BLOCKCHAIN“ TECHNOLOGIJOS TEORINIAI ASPEKTAI

1.1 „Blockchain“ istorija

Daugelis technologijų, kuriomis remiasi „blockchain“, buvo kuriamos dar gerokai prieš pasirodant bitkoinui. Viena iš šių technologijų yra Merkle medis, pavadintas kompiuterių mokslininko Ralfo Merkle vardu. Merkle savo 1979 m. daktaro laipsnyje aprašė viešojo rakto platinimo ir skaitmeninių parašų metodą, vadinamą „medžio autentifikavimu“. Galiausiai jis užpatentavo šią idėją kaip skaitmeninių parašų teikimo būdą. Merkle medis suteikia duomenų struktūrą, atskiriems įrašams patikrinti (R. Sheldon, 2021). 1 paveiksle yra išskirti pagrindiniai blokų grandinės etapai.



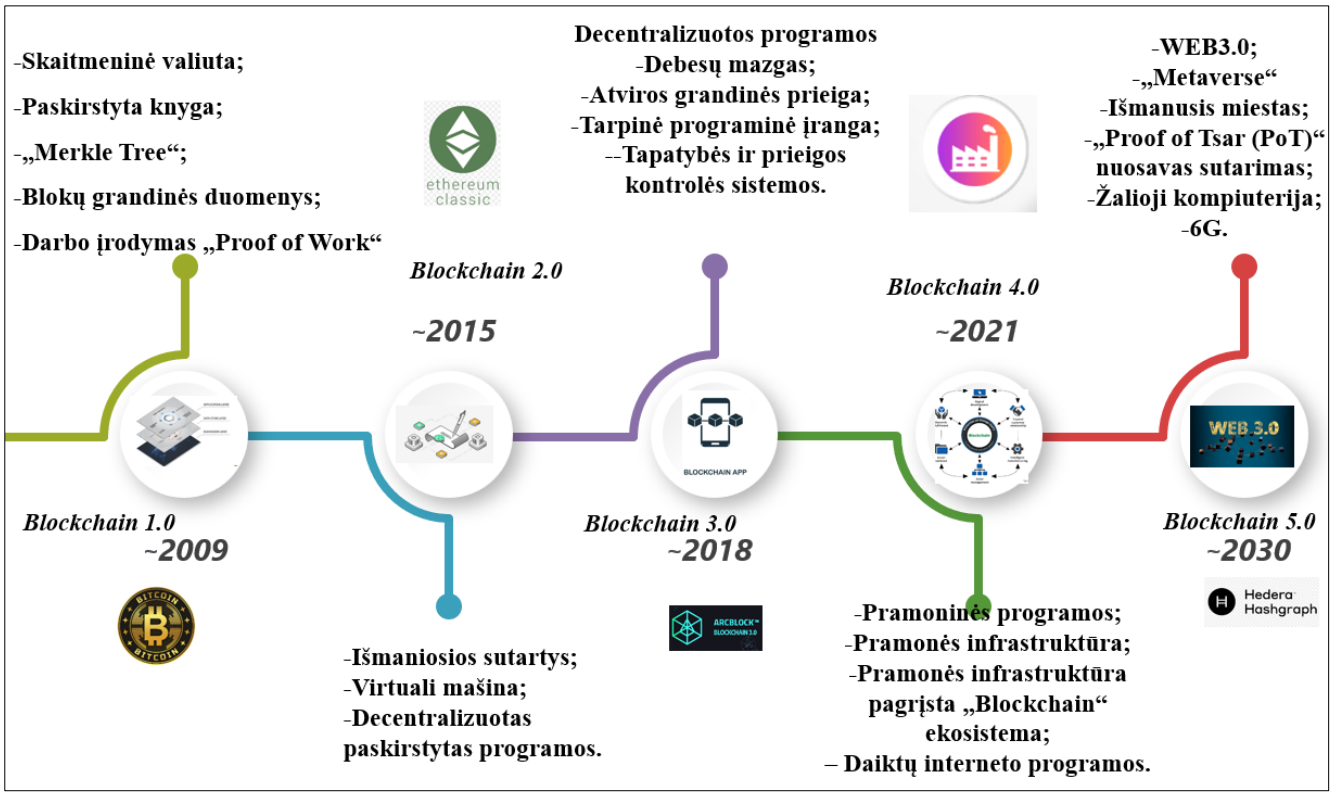
Šaltinis: sudaryta autorės pagal Mourtzis, D.; Angelopoulos, J.; Panopoulos, N. (2023).

1 pav. Istorinė blokų grandinės raida: pagrindiniai etapai

1982 m. kriptografas Davidas Chaumas pasiūlė technologiją, panašią į blokų grandinę. Stuartas Haberis ir W. Scottas Stornetta 1991 m. paskelbė tolesnius darbus apie kriptografiškai saugias blokų grandines. Jie norėjo įdiegti mechanizmą, kuris apsaugotų nuo dokumentų laiko žymų klastojimo. 1992

m. Haberis, Stornetta ir Dave'as Bayeris patobulino architektūrą naudodami Merkle medį, kuris gali sujungti daugybę dokumentų sertifikatų į vieną bloką. Nuo 1995 m. dokumentų sertifikatų maišos buvo skelbiamos kas savaitę „New York Times“ pavadinimu „Surety“. Satoshi Nakamoto sukūrė pirmąją blokų grandinę 2008 m. Nakamoto žymiai patobulino architektūrą įtraukdamas sudėtingumo parametrą, kad būtų pastovus blokų įtraukimo į grandinę tempas, ir taikydamas į „Hashcash“ panašų požiūrį į laiko žymų blokus be jų pasirašymo (Debatosh Pal Majumder, 2022, p.22).

2 paveiksle galite pamatyti evoliucinę blokų grandinės transformaciją, iliustracijoje taip pat nustatytos chronologinės ribos.



Šaltinis: sudaryta autorės pagal Mourtzis, D.; Angelopoulos, J.; Panopoulos, N. (2023).

2 pav. Nuo „Blockchain“ 1.0 iki „Blockchain 5.0“

1.2 Kas yra blokų grandinė ir kaip ji veikia?

Dabartinę blokų grandinės technologiją sugalvojo Satoshi Nakamoto.

„Blockchain“ yra technologija, skirta decentralizuoti operacijas ir tenkinti kibernetinio saugumo poreikius. Tai nuolat augančios paskirstytos duomenų bazės tipas, kuriame galima saugiai talpinti svarbią informaciją, tokią kaip išmaniosios sutartys, piniginės operacijos (kriptovaliuta) ir susiję duomenys (Abou Chacra, S., Sireli, Y. and Cali, U., 2018).

Blokas yra struktūrinis duomenų įrašas, kuriame iš esmės gali būti bet kokios operacijos su duomenimis ir kuris yra apsaugotas nuo manipuliavimo (Norbert Pohlmann, 2022).

Prieš įtraukiant į grandinę naują bloką, reikia atlikti laiko žymos ir maišos apdorojimo procesus; taigi blokų grandinės duomenys gali būti atsekami ir yra skaidrūs visiems, kurie dalyvauja blokų grandinėje. Iš esmės „blockchain“ taip pat gali būti laikoma paskirstyta, bendrai naudojama duomenų baze (Mourtzis, Dimitris, John Angelopoulos, Nikos Panopoulos, 2023).

Kiekvienam įrašui, kuris įtraukiamas į grandinę, suteikiamas unikalus skaitmeninis parašas, sukurtas kriptografine maišos funkcija arba algoritmu, tai veikia kaip skaitmeninis pirštų atspaudas. Be maišos, kiekvienas blokų grandinės blokas taip pat apima ankstesnio bloko maišą, laiko žymą ir duomenis apie darbo patikrinimo algoritmą (taip išgaunami ir tikrinami nauji blokai). Taip sukuriama blokų grandinė. Dėl šios priežasties blokų grandines taip pat sunku sugadinti, nes jei kas nors pasikeičia bet kuriame bloke (net jei tai tik taško ištrynimas), tai pakeičia bloko maišą (unikalus identifikatorius), o tai sulaužo bloką (Hirsh, Sandra, Alman, Susan Webreck, 2020, p. 3).

„Blockchain“ technologija yra duomenų saugojimo ir perdavimo būdas. Tai paskirstyta knygų sistema, leidžianti saugiai, skaidriai ir nekintamas operacijas tarp dviejų ar daugiau šalių. „Blockchain“ veikia sukurdama blokų grandinę, kurioje yra kiekvienos operacijos duomenys, kurie vėliau dalijami visiems tinklo dalyviams. Dėl to niekam praktiškai neįmanoma sugadinti duomenų ar jais kaip nors manipuliuoti. Dėl savo gebėjimo užtikrinti saugius ir patikimus sandorius, blokų grandinės technologija gali būti naudojama viskam, nuo finansinių paslaugų iki sveikatos priežiūros įrašų.

Nuo 1990-ųjų pradžios blokų grandinė buvo naudojama kaip būdas apsaugoti skaitmeninius dokumentus nepasikliaujant trečiosiomis šalimis. Pirmosios kartos blokų grandinių naudojimo atvejai daugiausia buvo susiję su nedideliais mokėjimais ir atlygio uždirbimu vaizdo žaidimuose. Tačiau 2015 m., pristačius išmaniųjų sutarčių blokų grandinės platformą, jos vaidmuo įvairiose pramonės šakose gerokai išsiplėtė.

Naudojant blokų grandinę gamintojams neįmanoma suklastoti, kas buvo tiekėjas medžiagų, pirkėjas gali matyti visą kelią savo prekes ir būti užtikrintas, kad prekė pagaminta iš kokybiškų medžiagų.

1.2.1 Blokų struktūra

Pagrindinė bloko struktūra blokų grandinėje paprastai apima šiuos komponentus:

1. Bloko numeris: tai unikalus kiekvieno bloko grandinės bloko identifikatorius, nurodantis jo vietą grandinėje.

2. Laiko žyma: tai data ir laikas, kai blokas buvo sukurtas ir įtrauktas į blokų grandinę.

3. Operacijų sąrašas: kiekviename bloke yra patikrintų ir prie bloko pridėtų operacijų sąrašas.

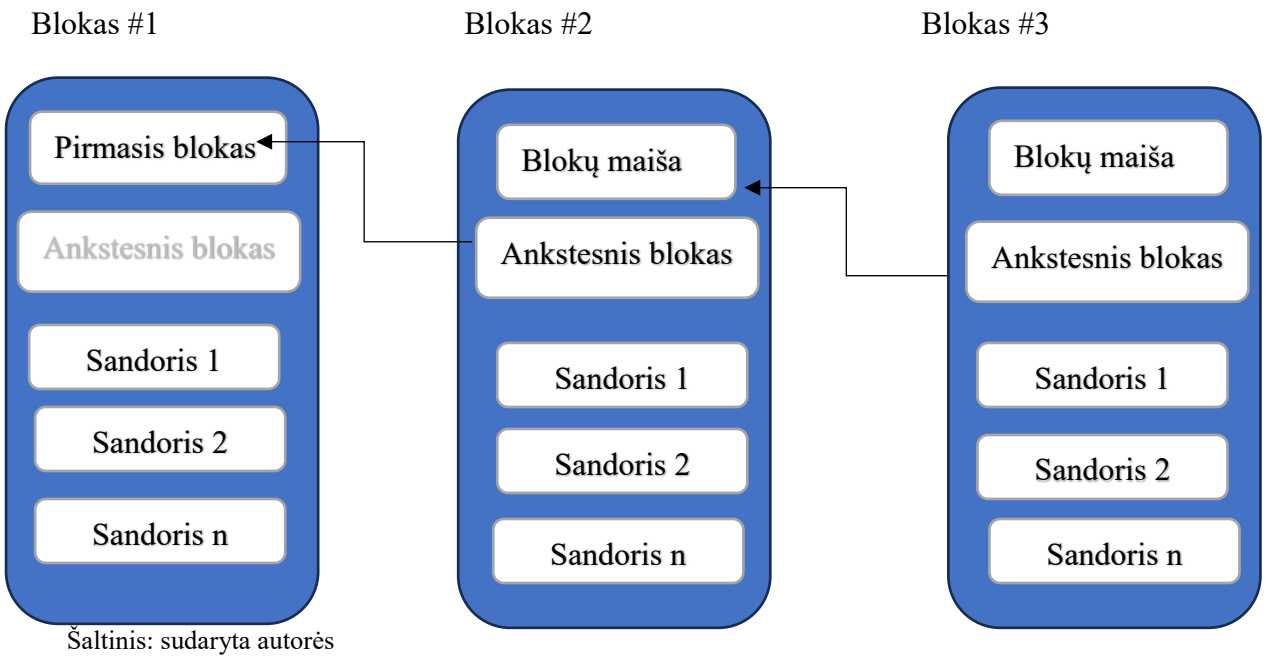
4. Ankstesnio bloko maiša: tai nuoroda į ankstesnio bloko maišą grandinėje, susiejant dabartinį bloką su ankstesniu.

5. „Nonce“: yra atsitiktinis skaičius, naudojamas kasybos procese, kuris yra būtinas norint sukurti tinkamą bloko maišą.

6. „Block Hash“: tai unikalus identifikatorius, sugeneruotas bloko duomenims taikant kriptografinius algoritmus, užtikrinančius jo vientisumą ir saugumą. Šie komponentai kartu sudaro bloko struktūrą blokų grandinėje, sukurdami saugų ir nekintamą operacijų įrašą.

Kaip naudojama maišos funkcija: pranešimo parašas paprastai neviršija 256 bitų ir transformuoja didelį informacijos rinkinį į nedidelį (tai neleidžia grįžti prie pradinio rinkinio). Pavyzdžiui, funkcija SHA-256 bus naudojama norint gauti 256 bitų (Dominique Guegan, 2017).

Naudojant „blockchain“, kiekvienas blokas turi tam tikrą duomenų kiekį ir yra susietas su ankstesniu bloku (žiūrėti 3 pav.). Kiekviename bloke, be duomenų, taip pat yra antraštė, susidedanti iš kelių bloko metaduomenų dalių. Blokai saugomi kaip failai. Jie indeksuojami atskiru indekso failu, esančiu už grandinės ribų, kartu su kita sistemai naudinga informacija. Pavyzdžiui, „Bitcoin“ turi blkindex.dat failą, kuriame yra blokinių failų indeksas. Blokų duomenys saugomi faile blk000n.dat, kur 000n yra bloko numeris. Nuoroda į kitą bloką ir vietoje to informacijos indeksavimas atskirame faile, tai reiškia, kad ankstesnio bloko duomenų keisti nereikia, norint pridėti tašką į kitą bloką. Duomenų laikymas be pakeitimų yra pagrindinė blokų grandinių savybė. Žinome, kad norint, kad blokų grandinės būtų naudingos, jose saugomi duomenys turi būti fiksuoti ir nekeičiami (Akira Summers, 2022, p.5).



Šaltinis: sudaryta autorės

3 pav. Blokų sandara

1.2.2 Kriptografija

Šiuolaikinė kriptografija – tai mokslo šaka, sprendžianti elektroninės informacijos saugos problemas. Kadangi kasmet vis daugiau informacijos siunčiama elektroninėmis ryšio priemonėmis, labai svarbu užtikrinti jos saugumą, nes elektroninė informacija (toliau – informacija) dažniausiai perduodama nesaugiais kanalais, pavyzdžiui, interneto ryšiu ir gali būti pasiekiama beveik visiems (Kriptografijos teorija, 2008).

„Blockchain“ naudoja kriptografiją, kad patikrintų operacijas, apdorotų mokėjimus ir užtikrinti atskirų dalyvių saugumą, kuris palaiko pasitikėjimą sistema. Blokų grandinė paprastai remiasi dviem kriptografinėmis schemomis: skaitmeniniais parašais ir kriptografinėmis maišos funkcijomis (Ryan, R., ir Donohue, M., 2017).

Kriptografija yra disciplina, skirta pranešimų apsaugai (konfidencialumo, autentiškumo užtikrinimui ir vientisumui) naudojant raktus. Ši technika yra senovinė ir kilusi iš senovės. Ilgą laiką tai buvo laikoma menu, o mokslu tapo tik XX a. Tai buvo masinis naudojimas kompiuterių, kurie demokratizavo jo naudojimą. Yra keletas kriptografijos algoritmų tipų: klasikinė kriptografija (lengvai iššifruojama), simetrinis kriptografijos algoritmas (su slaptu raktu), asimetrinės kriptografijos algoritmai (su viešaisiais arba privačiais raktais). Pastaruoju atveju viešasis raktas leidžia šifruoti, o privatus raktas – iššifruoti (Dominique Guegan, 2017).

Asimetriškas šifravimas ir „Hash“ yra plačiai naudojami blokų grandinės technologijoje. Asimetriškas šifravimas, pagrįstas viešųjų ir privačių raktų pora, yra svarbiausias dalykas siekiant užtikrinti vartotojų tarpusavio operacijų saugumą.

Asimetrinė kriptografija reiškia kriptografijos tipą, kai naudojamas raktas šifruoti duomenis skiriasi nuo rakto, kuris naudojamas duomenims iššifruoti. Tai taip pat žinoma kaip viešojo rakto kriptografija. Jis naudoja tiek viešuosius, tiek privačius raktus užšifruoti ir atitinkamai iššifruoti duomenis. Naudojamos įvairios asimetrinės kriptografijos schemos, įskaitant RSA, DSA ir „ElGammal“ (Imran Bashir 2018).

Kriptografinė maišos funkcija generuoja mažus skaitmeninius „pirštų atspaudus“, kurių kiekvienas yra unikalus į funkciją įvestam duomenų rinkiniui, leidžia greitai palyginti didelius duomenų rinkinius ir suteikia saugų būdą patikrinti, ar pagrindiniai duomenys nebuvo pakeisti. Taip pasiekiamas sutarimas sistemoje, nereikia lyginti kiekvieno dalyvio knygos eilutės po eilutės. Bet kuriam įvesties duomenų rinkiniui yra tik viena išvestis (Ryan, R., ir Donohue, M. 2017).

Maišos šifravimas naudojamas daugeliui svarbių procesų, kurie užtikrina bendrą blokų grandinės saugumą. Maišos naudojimas naudojamas transakcijų tikrinimui per kasybą; blokų grandinės įrašų nekintamumo išlaikymui; taip pat specialioms programoms, pvz., užtikrinant išmaniųjų sutarčių duomenų konfidencialumą ir duomenų apsaugą. Be to, maiša taip pat naudojama viešiesiems raktams

konvertuoti į blokų grandinės adresus. Maišos funkcija *H* yra transformacija, kuri suspaudžia savavališko ilgio įvestį iki fiksuoto ilgio, kuris vadinamas maišos reikšme.

Maišos funkcijos naudojamos blokų grandinės adresų generavimui, būtinam blokų sujungimui (HashPrev) ir Merkle maišos reikšmės apskaičiavimui, siekiant patikrinti visų bloko operacijų vientisumą (Norbert Pohlmann, 2022).

Apibendrinant, kriptografija yra svarbi blokų grandinės technologijos sėkmei.

1.2.3 Blokų grandinės tipai

Blokų grandinę galima skirstyti į keturias rūšis:

1.**Vieša**. Šioje blokų grandinėje visi sistemoje saugomi duomenys yra matomi visiems mazgams. Blokų grandinė prasideda nuo „genezės“ (kilmė, atsiradimas) bloko, o visi blokai yra sujungti per kriptografinę maišos funkciją. Kiekviename bloke yra antraštė ir operacijų serija, o kiekvienoje antraštėje yra ankstesnio bloko nuorodų. Taigi, jei kas nors nori sugadinti bet kurį bloką, jis turi pakeisti visas antraštes, nukreipiančias į ankstesnį mazgą, todėl ši funkcija blokų grandinę daro nekintamą ir atsparią klastojimui (D. Li, Z. Luo, B. Cao, 2022).

2. **Privati** yra centralizuota blokų grandinė. Skirtingai nuo viešosios blokų grandinės, privataus tipo savarankiškai valdo vienas subjektas. Norint pasiekti sandorius, kiekvienas dalyvis turi turėti atitinkamus leidimus. Privati yra labiau apsaugota ir kontroliuojama nei viešoji blokų grandinė ir dažniausiai naudojama elektroniniame balsavime, tiekimo grandinės valdyme ir kt. (Hyperledgerand R3 Corda, Ripple16).

3. **Hibridinė** blokų grandinė sujungia tiek viešųjų, tiek privačių blokų grandinių elementus, leidžiančius derinti atvirą dalyvavimą ir kontroliuojamą prieigą. Tai suteikia galimybę lanksčiai pritaikyti skaidrumo ir saugumo lygį, atsižvelgiant į konkrečius naudojimo atvejus ir reikalavimus. „Dragonchain“ yra labiausiai paplitęs hibridinės blokų grandinės pavyzdys.

4. **Konsorciumo** yra specializuota privačios blokų grandinės kategorija, kurioje kelios organizacijos kontroliuoja ir valdo blokų grandinę, o ne tik viena organizacija. Taigi ji turi panašius privalumus kaip ir privati blokų grandinė. Kadangi tai yra bendradarbiaujantis tinklas, jis yra produktyvesnis ir efektyvesnis tiek kolektyviai, tiek individualiai. Konsorciumo blokų grandines paprastai naudoja bankai, vyriausybinės organizacijos ir kt. 1 lentelėje parodyta konsorciumo blokų grandinė. „Consortiumblockchain“ pavyzdžiai yra „Energy Web Foundation“, R3 ir kt. (M. Pratyusa ir P. Chittaranjan, 2021).

1 lentelė. Blokų grandinės tipai

	Vieša	Privati	Hibridinė	Konsorciumo
Prieiga	Atvirai prieinama	Tik patvirtintiems dalyviams	Tik patvirtintiems dalyviam	Tik patvirtintiems dalyviams
Asmeniniai duomenys	Pseudonimų naudojimas	Priskirtas	Priskirtas	Priskirtas
Naujų blokų formavimas	Decentralizuota kalnakasiams naudojant išteklius	Centralizuotai per atskirus atvejus	Priklausomai nuo formos	Priklausomai nuo formos
Konsensuso mechanizmas	„Proof-of-Work“ darbo įrodymas	„Proof-of-Stake“ arba „Proof-of-Authority“	Proof of Work (PoW) algoritmas. proof of stake (PoS) algoritmas. Practical Byzantine Fault Tolerance (PBFT)	Priklausomai nuo formos
IT – saugumas	Labai aukštas, nėra vieno gedimo taško, manipuliuoti neįmanoma	Galimi centrinių veikėjų įsikišimai, vienas gedimo taškas	Aukštas saugumo lygis	Priklausomai nuo formos
Energijos sąnaudos	Aukštos	Žemas	Priklausomai nuo formos	Priklausomai nuo formos
Skaidrumas	Aukštas per atvirą operacijų istoriją	Tik pasirinktai dalyvių grupei	Skaidresnė nei privati	Tik pasirinktai dalyvių grupei
Sistemos pokyčiai	Mažas lankstumas	Aukštas lankstumas	Atnaujinimas sudėtingas	Konsorciumo viduje būtinas sutarimas
Jau atliktų sandorių pakeitimai	Neįmanoma	Galima per centrinę instituciją	Galima.	Galimas (pvz., daugumos sprendimu)
Sandorių greitis	Žemas („Proof-of-Work“ metu)	Greitas	Didelė sparta	Greitas, nei atviro tipo.
Kriptovaliuta	Dažniausiai būtinas kaip naujų blokų formavimosi skatinimo mechanizmas	Neprivaloma	Neprivaloma	Neprivaloma

Šaltinis: Sudaryta autorės pagal „Bundestago“ Vokietijos parlamento pateikta informacija

1.2.4 Konsensuso modeliai

Bloko saugumas ir patvirtinimas yra svarbi užduotis, kurią pasiekia tam tikras mechanizmas, vadinamas konsensuso algoritmais (S. Mojtaba, H. Bamakan, A. Motavali, A. Bondarti, 2020).

Konsensusas yra žmonių ar subjektų grupės susitarimo dėl konkretaus sprendimo ar veiksmo procesas. Blokų grandinėje konsensusas naudojamas siekiant užtikrinti, kad visi tinklo mazgai susitartų dėl esamos tinklo būsenos ir operacijų autentiškumo (Xiong ir kt., 2022). Tai labai svarbu norint išsaugoti blokų grandinės saugumą ir vientisumą. Skirtingos blokų grandinės platformos naudoja skirtingus algoritmus, tokius kaip darbo įrodymas, statymo įrodymas arba įgaliojimų įrodymas, kad tinklo mazgai pasiektų sutarimą (Hussein, Z., Salama, M.A. & El-Rahman, 2023).

Apskritai konsensuso algoritmai yra gyvybiškai svarbi „blockchain“ technologijos dalis ir atlieka svarbų vaidmenį užtikrinant blokų grandinės tinklų saugumą, decentralizavimą ir mastelio keitimą. Skirtingi sutarimo algoritmai turi keletą kompromisų, o algoritmo pasirinkimas gali turėti reikšmingų rezultatų blokų grandinės tinklo turtui ir veikimui (Hussein, Z., Salama, M.A. & El-Rahman, 2023).

Yra keletas skirtingų konsensuso modelių, kurių kiekvienas turi savo privalumų ir kompromisų. Kai kurie populiarūs konsensuso modeliai yra darbo įrodymas (Proof of Work), statymo įrodymas (Proof of Stake), deleguotasis statymo įrodymas (Delegated Proof of Stake) ir praktinis Bizantijos atsparumas gedimams (Practical Byzantine Fault Tolerance). Kiekvienas iš šių modelių turi savo būdą užtikrinti, kad visi tinklo mazgai susitartų dėl blokų grandinės būsenos, ir kiekvienas iš jų turi skirtingus reikalavimus dalyvauti konsensuso procese. Konsensuso modelis yra esminis bet kurios blokų grandinės sistemos komponentas, nes jis lemia tinklo saugumą, mastelio keitimą ir decentralizavimą. Skirtingi konsensuso modeliai gali būti tinkamesni įvairių tipų blokų grandinėms, atsižvelgiant į tokius veiksnius kaip dalyvių pasitikėjimo lygis, norimas decentralizacijos lygis ir sistemos energijos vartojimo efektyvumas.

„Proof of Work“ (PoW) – darbo įrodymo modelyje vartotojas paskelbia kitą bloką, pirmiausia išspręsdamas daug matematinių skaičiavimų reikalaujantį galvosūkį. Šio galvosūkio sprendimas yra jų atliktas „įrodymas“, jų duomenų blokas laikomas galiojančiu ir pridedamas prie visų blokų grandinės kopijų, taip pasiekiant konsensusą (D.Yaga, P. Mell, N. Roby, K. Scarfone, 2018, p.17).

„Proof of Stake“ (PoS) – statymo įrodyme, tikrintojas investuoja į sistemoje esančias monetas. Monetų savininkai gali periodiškai sukurti naujus blokus. Kad kiti mazgai atpažintų blokus kaip galiojančius, užuot atlikę aritmetines užduotis, jie turi tik įrodyti nuosavybės teisę (D. Hornsteiner, S.Hasenleithner, V. Pesendorfer, 2020, p. 14).

Vietoj maišos koeficiento, vartotojo statymas yra labai svarbus. Kuo didesnė dalis, tuo didesnė tikimybė, kad vartotojas bus pasirinktas patvirtinti kitą bloką. Kitaip tariant: kiekvienas, kuris sutinka įnešti į tinklą kuo daugiau monetų, padidina savo galimybes gauti atlygį. Statymo įrodymo mechanizmas naudoja atsitiktinį algoritmą, kad sudarytų sutarimą blokų grandinės tinkle. Taip ištraukiamas dalyvis,

kuris turi teisę sukurti bloką. Paprasčiau tariant, kiekvienas žetonas yra laimėjimo bilietas. Vadinasi, vartotojai, kurių statymas didesnis (= daugiau bilietų), taip pat turi didesnę tikimybę būti atrinktiems (BTC-ECHO GmbH, 2023).

„Proof-of-Authority“(POA) – šis sutarimo mechanizmas gali būti vertinamas kaip „Proof-of-Stake“ variantas, kai statymas yra tikrintojo tapatybė. POA remiasi (palyginti nedideliu) iš anksto patvirtintų tikrintojų paskyrų arba „institucijų“, turinčių teisę patvirtinti operacijas ir pridėti naujų blokų, skaičiumi. Įgaliojimo mazgai privalo atlikti išankstinės atrankos procesą, atskleisti savo tapatybę ir užsiregistruoti viešoje notarų duomenų bazėje bei laikytis kelių taisyklių, kad išliktų patikimi. Kadangi už tai yra atlyginama ir jie gauna energijos tinkle, jie turi paskatą išlikti patikimi ir vengti atakų. POA protokolai pasirodė ypač populiarūs privačiose (įmonių) blokų grandinėse, įskaitant energijos programas (pvz., „Energy Web Foundation“ blokų grandinės sistema). Taip yra dėl didelio operacijų greičio, kurį galima pasiekti POA pagrįstose sistemose ir daug mažesnių pridėtinių išlaidų bei energijos sąnaudų nei pvz., PoW sistemose. Tačiau nedidelis autoritetingųjų mazgų skaičius gali būti laikomas prieštaraujančiu decentralizacijos principams, kuriais grindžiamos blokų grandinės, todėl tai yra mažiau tinkama alternatyva viešoms, leidimo neturinčioms blokų grandinėms (Desen Kirli, Benoit Couraud, Valentin Robu ir kiti, 2022).

„Delegated Proof of Stake“ (DPoS) – tai naujovė, palyginti su standartiniu PoS, kai kiekvienas mazgas, turintis dalį sistemos, gali deleguoti patvirtinimą sandorį į kitus mazgus balsuojant. Jis naudojamas „BitShares“ blokų grandinėje (Imran Bashir, 2018, p. 38). Šis metodas nereikalauja tiek daug energijos suvartojimo.

„Practical Byzantine Fault Tolerance“ (PBFT) – praktinis Bizantijos gedimų tolerancija (PBFT) yra sutarimo algoritmas paskirstytoms sistemoms. Tai leidžia sistemoms pasiekti sutarimą, nepaisant klaidingų ar kenkėjiškų mazgų. PBFT turi lyderio mazgą, vadinamą pirminiu, kuris siūlo naują operacijų bloką kitiems mazgams. Patvirtinus bloką, kiti mazgai siunčia atsakymą į pirminį. Jei mazgų kvorumas sutinka, blokas prisijungia prie blokų grandinės (Tectum, 2023).

Naudinga biurokratinių gedimų aptikimo technika sprendžia priešiškų tinklo mazgų problemą. Išsklaidytas tinklo įrenginys gali būti įgalintas pasiekti susitarimą, nepaisant tam tikrų mazgų, kurie sugenda arba pateikia klaidingą informaciją, nes virtualus blokas naudoja kopiją (biurokratinių trūkumų pašalinimo techniką). PBFT stengiasi pasiūlyti tvirtą logiką, atkartojantį tas funkcijas net ir esant kenksmingiems mazgams. Pirminis mazgas (arba lyderis) ir daugybė pagalbinių mazgų paeiliui išdėstomi mikro paslaugose su statymu (arba atsarginėmis kopijomis). Bet kuris tinkamas sistemos mazgas turi galimybę perjungti iš tarpinio į pagrindinį pagrindinio mazgo gedimo atveju. Visos patikimos vietos gali dalyvauti pagal daugumos taisyklę (Zeel Dabhi, & Aishwarya, 2023).

PBFT siekia išspręsti problemas taupydamas energiją, tai yra nesinaudodamas įvairiais matematiniais skaičiavimais. PBFT taip pat ketina užtikrinti sandorio baigtinumą, kai dėl sandorių

susitariama (arba užbaigiama), priešingai nei PoW, jiems nereikia kelių patvirtinimų. Be to, kadangi visi tinklo mazgai dalyvauja priimant sprendimus (atsakydami į užklausą), tai lemia mažą atlygio dispersiją. Tačiau PBFT yra linkęs būti pažeidžiamas „Sybil“ atakų ir jis netinkamai keičiamas dėl didelių ryšio išlaidų (Bela Shrimali, Hiren B. Patel, 2022).

„Proof of History“ (PoH) – istorijos įrodymas (PoH) yra naujas „Solana Labs“ sukurtas konsensuso mechanizmas, kuris naudoja kriptografinę funkciją, vadinamą „Verifiable Delay Function“ (VDF), kad generuotų kiekvieno bloko grandinės bloko laiko žymas. Užtikrindama šių laiko žymų nekintamumą ir autentiškumą, VDF sukurtas taip, kad būtų sunku uždelsti ir atminti, todėl užpuolikams sunku manipuliuoti laiko žymomis. Tada VDF sugeneruota laiko žyma įtraukiama į kiekvieną blokų grandinės bloką, suteikiant patikrinamą ir nekeičiamą operacijų eilės įrašą. PoH mechanizmas pirmiausia naudojamas „Solana Blockchain“ tinkle, sukurtas taip, kad būtų keičiamas ir galėtų apdoroti tūkstančius operacijų per sekundę. Sumažinus saugyklos kiekį ir pralaidumą, reikalingą „blockchain“ palaikymui, PoH gali pagerinti Solana tinklo efektyvumą ir greitį, taip pat užtikrinti saugų ir patikrinamą operacijų įrašą (Blockchain Council, 2024).

Apibendrinant galima pasakyti, kad konsensuso algoritmai yra labai svarbūs decentralizuotų sistemų veikimui, o nuolatiniai šios srities tyrimai ir plėtra yra reikšmingi decentralizuotų technologijų pažangai ir plačiam pritaikymui. Tinkamo konsensuso algoritmo pasirinkimas konkrečiam naudojimo atvejui, gali labai paveikti sistemos veikimą ir saugumą.

1.3 Blokų grandinės privalumai ir trūkumai

Kaip ir kiekviena technologija blokų grandinių sistema, turi privalumų ir trūkumų.

„Blockchain“ technologija suteikia daug privalumų, įskaitant padidintą saugumą, skaidrumą, decentralizaciją ir nekintamumą. Tačiau taip pat kelia iššūkių, tokių kaip mastelio keitimo problemos, energijos suvartojimo problemos, reguliavimo sudėtingumas ir techniniai sudėtingumai.

Šios technologijos pritaikymas verslui turi daug privalumų. Toliau pateikiami pagrindiniai **privalumai**:

- *Efektyvumas* ir mažesnės transakcijų mokesčių sąnaudos: blokų grandinės technologija sumažina skaičiavimo ir verifikavimo laiką, todėl sandoriai vyksta greičiau ir pigiau. Šį pranašumą aptaria Don Tapscott savo knygoje „Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World“.
- *Atsekamumas* – BC sukuria negrįžtamą audito seką, leidžiančią lengvai atsekti pakeitimus tinkle.
- *Skaidrumas* – blokų grandinė užtikrina operacijų skaidrumą ir nekintamumą, nes visų operacijų negalima pakeisti ar ištrinti.

- *Saugumas* naudojant „blockchain“ technologiją, kiekviena operacija yra įrašoma ir patikrinama tinkle dėl sudėtingų kriptografinių operacijų. Informacijos autentiškumas užtikrinamas sudėtingais matematiniais algoritmais.
- *Atsiliepimai* dar vienas „blockchain“ technologijos pranašumas įmonėms yra grįžtamasis ryšys. Kadangi technologija yra visiškai atsekama per visą turto gyvavimo ciklą, turto gamintojai ir dizaineriai gali lengvai sekti turtą ir pritaikyti turto valdymą produktuose, kad jis būtų efektyvesnis. Atsiliepimai suteikia informacijos apie įrengimą, priežiūrą, siuntimo grąžinimą ir eksploatacijos nutraukimą (Niranjanamurthy, M., Nithya, B.N. & Jagannatha, S, 2019)

Trūkumai:

Dėl blokų grandinės pobūdžio ji visada bus lėtesnė, nei centralizuotos duomenų bazės. Kai apdorojama operacija, „blockchain“ turi atlikti visus tuos pačius veiksmus, kaip ir įprasta duomenų bazė, tačiau ji taip pat turi papildomas naštas:

- *Parašo patvirtinimas* kiekviena „blockchain“ operacija turi būti pasirašyta skaitmeniniu būdu naudojant viešąją ir privačią kriptografijos schemą. Tai būtina, nes sandoriai tarp mazgų plinta lygiaverčiu būdu, todėl jų šaltinio negalima įrodyti kitaip. Šių parašų generavimas ir tikrinimas yra sudėtingas skaičiavimo būdas.
- *Sutarimo mechanizmai* paskirstytoje duomenų bazėje, pvz., „Blockchain“, reikia dėti pastangas siekiant užtikrinti, kad tinklo mazgai pasiektų sutarimą.
- *Dėl pertekliaus* kalbama ne apie atskiro mazgo našumą, o apie bendrą skaičiavimo kiekį, kurio reikia „blockchain“. Nors centralizuotos duomenų bazės apdoroja operacijas vieną (arba du kartus), blokų grandinėje kiekvienas tinklo mazgas jas turi apdoroti atskirai. Taigi daug daugiau dirbama siekiant to paties galutinio rezultato.
- *Didelis energijos suvartojimas* „Bitcoin Blockchain“ tinklo kalnakasiai bando 450 tūkst. trilijonų sprendimų per sekundę, siekdami patvirtinti operacijas, naudodami didelę kompiuterio galią.
- *Kaina* „blockchain“ leidžia sutaupyti operacijos sąnaudas ir sutaupyti laiko, tačiau reikalauja didelio pradinio kapitalo (Niranjanamurthy, M., Nithya, B.N. & Jagannatha, S, 2019)

Aptariant surinktą informaciją – pagrindinis blokų grandinės pranašumas yra skaidrumas, efektyvumas, saugumas ir atsekamumas. Tačiau „blockchain“ susiduria su iššūkiais, įskaitant mastelio keitimo problemas, didelį energijos suvartojimą ir reguliavimo neapibrėžtumą.

1.4 Blokų grandinės reikšmė šiandieninėje sistemoje

Tikimasi, kad pasaulinė „blockchain“ rinka iki 2026 m. pasieks 67,4 mlrd. Daugiau nei 40 milijonų žmonių visame pasaulyje aktyviai naudojasi „blockchain“ technologija (Blockchain Council,

2024). 2 lentelėje, galima pamatyti, kaip plačiai yra taikoma blokų grandinė įvairiuose sektoriuose nuo vyriausybės iki logistikos. Daugiausia taikymo atvejų yra mažmeninėje prekyboje ir logistikoje.

2 lentelė. Blokų grandinės taikymas įvairiuose segmentuose.

Pramonės segmentas	Blokų grandinės taikymas
Vyriausybė/viešasis sektorius	• Balsavimas • Mokesčiai • Konkurso procesai
Finansinės paslaugos	• Užsienio valiutos • Įmonių skolos/obligacijos • Prekybos platformos • Mokėjimo pervedimas
Pramonės sektorius	• Gamybos procesai • Daiktų internetas (Iot) įrenginių valdymas • Paslaugų pramonė
Mažmeninė prekyba	• Lojalumo taškai • Tapatybės valdymas • Pasitikėjimo pramonė • Kapitalo turto valdymas • Akredityvai
Draudimo liudijimas	• Pretenzijų apdorojimas • P2P draudimas • Nuosavybės vardai • Pardavimas ir pasirašymas
Prabangus verslas	• Prabangos prekės
Tvarios ir žiedinės tiekimo grandinės	• Tvarus tiekimo grandinės valdymas (SSCM)
Tiekimo grandinė ir logistika	• Maisto tiekimo grandinė • Vaisių tiekimo grandinė • Tekstilės ir drabužių tiekimo grandinė • Žemės ūkio tiekimo grandinė • Automobilių tiekimo grandinė • Krovinių logistika • Statybos tiekimo grandinė

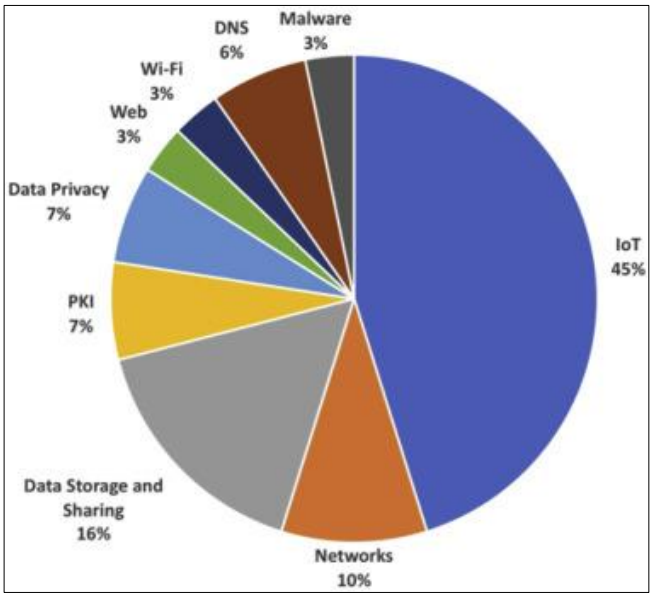
Šaltinis: sudaryta autorės

1.5 Kibernetinis saugumas blokų grandinės technologijoje

Kibernetinė sauga – tai politikos krypčių, metodų, technologijų ir procesų rinkinys, kuris veikia kartu siekiant apsaugoti kompiuterinių išteklių, tinklų, programinės įrangos programų ir duomenų konfidencialumą, vientisumą ir prieinamumą nuo atakų. Kibernetinės gynybos mechanizmai egzistuoja

programos, tinklo, pagrindinio kompiuterio ir duomenų lygiu. Yra daugybė įrankių, tokių kaip ugniasienės, antivirusinė programinė įranga, įsibrovimo aptikimo sistemos (IDS) ir apsaugos nuo įsibrovimo sistemos (IPS), kurios veikia branduoliuose, kad išvengtų atakų ir aptiktų saugumo pažeidimus (Berman ir kt., 2019).

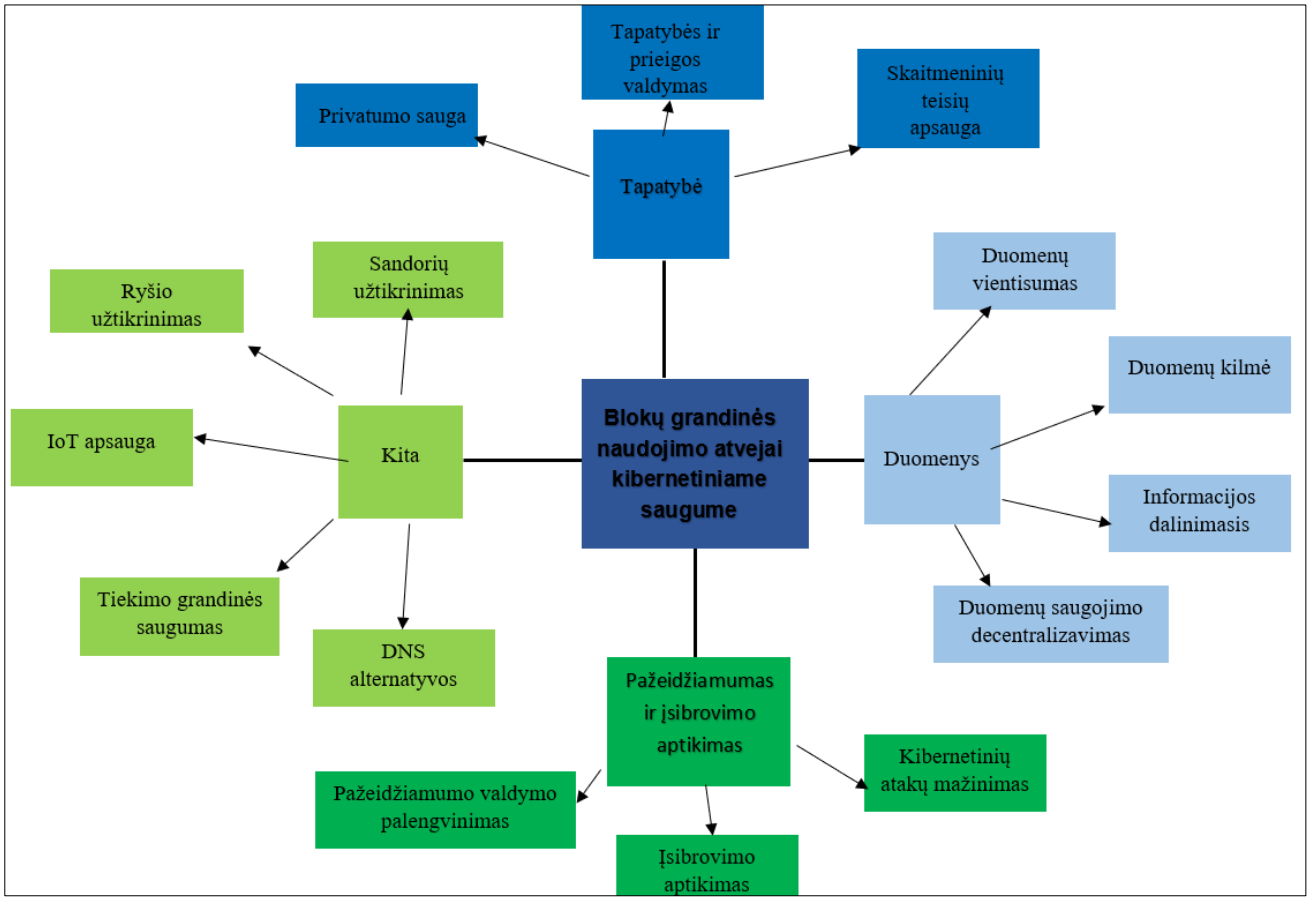
Norint, kad „blockchain“ technologija būtų naudojama saugiai ir patikimai ilgalaikėje perspektyvoje, reikia atsižvelgti į komunikacijos, saugumo ir patikimumo aspektus. Pasižiūrėkime į 4 paveikslą.



Šaltinis: P. J. Taylor, T. Dargahi, A. Dehghantanha ir kiti, 2020

4 pav. Blokų grandinės kibernetinio saugumo programos

Kaip ištyrė Paul J. Taylor ir kt., kad beveik pusė (45 %) visų blokų grandinės kibernetinio saugumo programų tyrimų yra susiję su daiktų interneto įrenginių saugumu. Duomenų saugojimas ir naudojimas yra antra populiariausia tema – 16 proc. Tyrimai apima blokų grandinės programas, skirtas ieškoti užšifruotų debesyje pagrįstų duomenų ir užkirsti kelią failų pavadinimų ir jame esančių duomenų klastojimui. Tinklai yra trečia pagal dažnumą tema, kurie sudaro 10% ir dažniausiai yra susiję su tuo, kaip „blockchain“ gali užtikrinti virtualių mašinų saugumą ir autentiškumą. Duomenų privatumas ir viešojo rakto infrastruktūra yra ketvirta dažniausiai pasitaikanti tema, kiekviena jų sudaro 7 proc. „Blockchain“ programos leidžia galutiniams vartotojams tam tikru būdu autentifikuoti kitą subjektą ar paslaugą, kad jiems nereikėtų pasikliauti pažeidžiamu centriniu informacijos serveriu. Penkta dažniausia tema yra apie domenų vardų sistemas (DNS) ir tai, kaip blokų grandinė gali veiksmingai priglobti DNS įrašus paskirstytoje aplinkoje, kad būtų išvengta kenkėjiškų pakeitimų ir paslaugų atsisakymo atakų. „Wi-Fi“, žiniatinklis ir kenkėjiškos programos, sudaro po 3 proc (P. J. Taylor, T. Dargahi, A. Dehghantanha ir kiti, 2020). Apžvelkime 5 paveiksle BC naudojimo atvejus kibernetiniame saugume.



Šaltinis: sudaryta autorės pagal Liu, M., Yeoh, W., Jiang, F., & Choo, K. K. R. 2022

5 pav. Blokų grandinės technologijos naudojimo atvejai kibernetiniame saugume

„Privatumo apsauga reiškia duomenų saugojimą paskirstytoje knygoje naudojant blokų grandinės technologijas, siekiant apsaugoti duomenų privatumą ir užkirsti kelią duomenų nutekėjimui, ypač socialinėje žiniasklaidoje, „blockchain“ pagrindu veikiančioje tinklo aplinkoje vartotojams nereikia pasitikėti jokia trečiąja šalimi, taip sumažinant privatumo nutekėjimo riziką.

Skaitmeninių teisių apsauga. Skaitmeninės teisės žiniasklaidos savininkams kelia didelį susirūpinimą dėl jų pažeidžiamumo dėl sukčiavimo ar atakų internete. „Blockchain“ įrašo kiekvieną operaciją paskirstytoje knygoje ir jos yra nekintančios, o tai reiškia, kad galima sekti skaitmeninį turinį. „Blockchain“ veiksmingai užkerta kelią neteisėtam žiniasklaidos duomenų naudojimui ir saugiai apsaugo žiniasklaidos savininkų teises.

Tapatybės ir prieigos valdymas. Tradicinis autentifikavimas dažnai priklauso nuo trečiųjų šalių ir yra linkęs į vieną gedimą. Pastaraisiais metais daug tyrimų buvo skirta blokų grandinės taikymui tapatybės ir prieigos valdymui, įskaitant autorizavimą ir autentifikavimą. Cui ir kt. sukūrė hibridinį blokų grandinės modelį, kad realizuotų abipusį mazgo tapatybės autentifikavimą pagal skirtingus komunikacijos scenarijus. Pasirodė, kad ši schema turi visapusišką saugumą ir aukštą našumą.

Ryšio užtikrinimas. Kaip decentralizuotas tinklas, blokų grandinė gali užmegzti didelio masto saugų ryšį tarp subjektų, o tai ypač tinka naudoti nepilotuojamuose orlaiviuose (UAV) arba transporto

tinkluose. Paskirstyta blokų grandinės sistema išvengia vieno gedimo taško, o ankstesni sandoriai ir ryšiai yra apsaugoti nuo klastojimo.

Daiktų interneto saugumas. Pažeisdami įrenginius su netinkamomis saugos funkcijomis, kibernetiniai užpuolikai gali gauti prieigą prie visos daiktų interneto sistemos.

Tiekimo grandinės saugumas. „Blockchain“ yra laikomas vienu iš įmanomų sprendimų vis didėjantiems iššūkiams, susijusiems su tiekimo grandinės saugumu. Be „blockchain“ atsekamumo ir nekintamumo, ši technologija užtikrina patikimas P2P operacijas, kurios nėra jautrios kibernetiniams nusikaltėliams manipuliuoti ar pažeisti. *DNS alternatyvos.* Pagrindinė tradicinės domeno vardų tarnybos funkcija yra sutelkta į serverį, kuris yra pažeidžiamas dėl talpyklos sugadinimo, DDoS atakų ir DNS užgrobimo. „Blockchain“ ir domeno vardo paslaugos derinys yra novatoriškas požiūris į šiuos saugumo iššūkius kuriant decentralizuotas, saugias ir patogias pavadinimų sistemas be patikimų šalių. Dvi populiarios esamos „blockchain“ pagrindu veikiančios DNS alternatyvos yra „Namecoin“ ir „Blockstack“. Kiekvienas sistemos mazgas gali veikti kaip DNS serveris, kuriame vartotojai gali atlikti domeno vardo registraciją, perdavimą ir duomenų peržiūrą. Dėl domeno vardų paslaugų decentralizavimo įsibrovėliai negali manipuliuoti arba pavogti centrinių įrašų.

Sandorių užtikrinimas. „Blockchain“ vis dažniau naudojama siekiant užtikrinti saugią prekybos aplinką ir užtikrinti elektroninių įrašų, ypač jautrių duomenų sveikatos priežiūros ir finansų sektoriuose, saugumą. Wangas ir Jonesas teigė, kad „blockchain“ pagrįstas elektroninių sveikatos įrašų valdymas gali saugiai kontroliuoti dokumentų prieinamumą, perkelti įrašus ir stebėjimo įrašus.

Pažeidžiamumo valdymo palengvinimas. Rotas ir Bleikas atskleidė, kad blokų grandinės kodo generavimas naudojant automatinę išmaniųjų sutarties kodų analizę ir sintezę padeda išvengti pažeidžiamumų ir klaidų.

Įsibrovimo aptikimas. „Blockchain“ gali būti naudojama kenkėjiškam elgesiui aptikti įvairiose tinklo aplinkose. Aleksandras ir Vangas integravo aptikimo variklį ir blokų grandinę, kad būtų sukurta decentralizuota ugniasienės sistema, galinti padidinti kibernetinį saugumą.

Kibernetinių atakų mažinimas Pasak Ma ir kt., „blockchain“ įrodė, kad gali atsispirti kenkėjiškai vidinių vartotojų veiklai, išorinėms DDoS atakoms ir „Sybil“ atakoms.

Duomenų saugojimo decentralizavimas. Tradicinės centralizuotos duomenų saugyklos trūkumas yra tas, kad sėkmingai įsibrovęs užpuolikas sukelia didelio masto vartotojo duomenų nutekėjimo incidentus. Tai gali sukelti katastrofiškų pasekmių, ypač jei duomenų nutekėjimas yra jautrūs finansų ar medicinos srities duomenys. Blokų grandinės metodas gali pakeisti tradicinius trečiųjų šalių duomenų saugojimo tiekėjus, todėl išvengiama trečiosios šalies keliamos rizikos.

Duomenų kilmė yra svarbi nustatant duomenų kokybę, patikimumą, pakartotinį duomenų naudojimą ir skaitmeninę teismo ekspertizę.

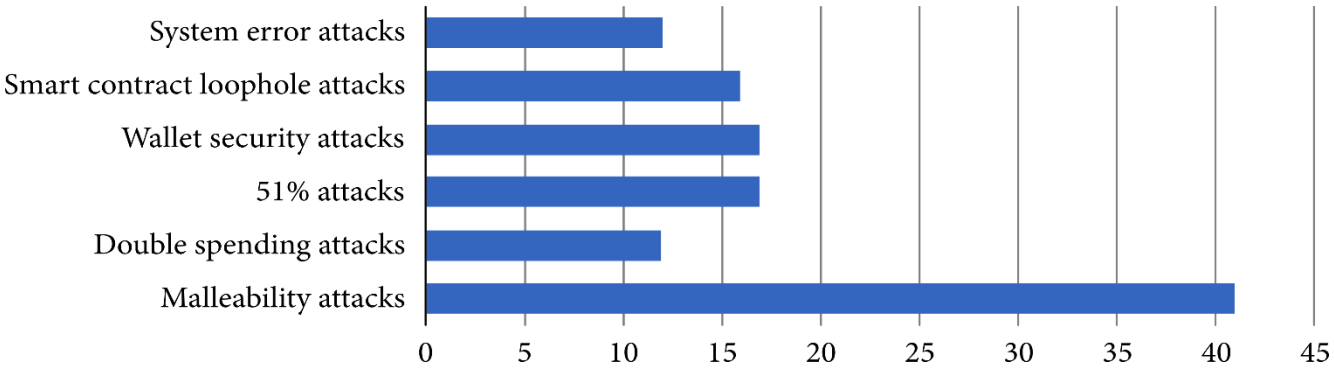
Dalijimasis informacija. „Blockchain“ pagrįsta duomenų dalijimosi sistema gali apsaugoti konfidencialius duomenis ir tinklo infrastruktūrą nuo atakų.

Duomenų vientisumas. Pasak Mylrea ir Gourisetti, blokų grandinė padeda spręsti sudėtingas problemas, susijusias su energijos operacijų duomenų vientisumo užtikrinimu ir taip sumažina duomenų klastojimo riziką (Liu, M., Yeoh, W., Jiang, F., & Choo, K. K. R. 2022).“

1.5.1 Kibernetinio saugumo iššūkiai su „Blockchain“

Tobulėjant technologijoms, kibernetinis saugumas įgavo didžiulę reikšmę atliekant tyrimus. Kibernetinio saugumo problemos eksponentiškai auga skirtinguose verslo pasaulyje veikiančiuose sektoriuose. Didelės įmonės daugiau dėmesio skiria tam, kada įvyks kibernetinė ataka, o ne tai, ar bus ataka. Įmonės ragina vyriausybes kovoti su kibernetinio saugumo atakomis, nes šios kibernetinio saugumo problemos sukelia didžiulius finansinius nuostolius. Tyrimas atskleidė, kad kibernetinės atakos turėjo didelį poveikį įmonėms, o 61% mažų ir vidutinių įmonių patyrė kibernetines atakas. Panašiai ir kitas tyrimas atskleidė, kad kibernetinio saugumo pavojai, tokie kaip duomenų pažeidimai ir konfidencialių duomenų atskleidimas, didėja dėl didėjančio debesų technologijų ir internetinių programų naudojimo (S. Mahmood**,** M. Chadhar, ir S. Firmin, 2022).

Pavyzdinių tyrimų, kuriuose pranešama apie BC kibernetinio saugumo iššūkius kiekvienai temai, pavyzdinis vaizdas parodytas 6 paveiksle. 80 % į imtį įtrauktų tyrimų atskleidžia, kad „Malleability attacks“ plastiškumo atakos (kriptografinės atakos) yra labiausiai paplitusios blokų grandinėje. Toliau pateikiamos piniginės saugumo atakos ir 51 % atakos, kaip dažniausi BC kibernetinio saugumo iššūkiai, atitinkamai po 33 %. Kitos svarbios kibernetinio saugumo atakos, apie kurias pranešta BC, yra išmaniųjų sutarties spragų atakos, dvigubų išlaidų atakos ir sistemos klaidų atakos.



Šaltinis: Human Behavior and Emerging Technologies, 2022

6 pav. Kibernetinio saugumo iššūkiai BC

3 lentelėje pateikiama atakų klasifikacija, kad susidarytų bendras vaizdas su kokiais kibernetiniais iššūkiais tenka susidurti, kai yra naudojama blokų grandinė.

3 lentelė. Kibernetinio saugumo atakų klasifikacija blokų grandinėje

Atakos	Nustatytos temos
„Malleability attacks“ (Kriptografinės atakos, plastiškos atakos)	Tinklo įsilaužimai Serverio pažeidimai Debesų platformos įsilaužimai Neteisėti sandoriai Stebėjimo problemos Sistemos parametrų keitimas Trūkumas skaičiavimo efektyvumo Cenzūra ir nusikalstami išpuoliai Įgaliojimo įrodymas (POA atakos) Telefono pasiklausymas Paslaugos atsisakymas (DoS atakos) Paskirstytas atsisakymas teikti paslaugą (DDoS atakos) Žmogus viduryje (MitM) arba „Sybil“ ataka Savanaudiška kasyba
Dvigubos išlaidų atakos	Pavogta kriptovaliuta Tinklo kasybos maišos greičio valdymas
51% atakos	Auksinis pirštas Piniginės saugumo atakos Įsilaužimas į vartotojų slaptažodžius ir programinės įrangos klaidos Sukčiavimas
Piniginės saugumo atakos	Privataus rakto saugumo atakos Informacijos vagystė, datos pažeidimai ir praradimai Manipuliavimo informacija ir autentifikavimo problemos Prastas prieigos valdymas naudojant išmaniąją sutartį Išmaniosios sutarties kodo klaida / programos pažeidžiamumas
Išmaniosios sutarties spragų atakos	Išmaniosios sutarties manipuliavimas trūkumais Kodu pagrįstos atakos Trūkumas integravimo ir priežiūros sistemų
Sistemos klaidų atakos	Sąveikos problemos Laikui jautrių operacijų vėlavimas

Šaltinis: Human Behavior and Emerging Technologies, 2022

Kairiajame stulpelyje pavaizduotos šešios standartizuotos „Blockchain“ kibernetinių atakų klasės. Nusikaltėliai kelia grėsmę blokų grandinėms keturiais pagrindiniais būdais: sukčiavimu, nukreipimu, „Sybil“ ir 51% atakomis. Ne visos BC yra vienodos. „Blockchain“ architektūros labai skiriasi, ypač kai kalbama apie tai, kaip skirtingos struktūros ir komponentai sukuria saugumo kompromisus.

2. BLOKŲ GRANDINĖS TAIKYMAS ENERGETINIAME SEKTORIUJE, ANALIZĖ

Šiame skyriuje analizuojamas energetikos pramonės skaitmeninimas ir apžvelgiama dabartinė energetikos pramonės plėtra ir technologijų padėtis. Mikrotinklų pažanga ir blokų grandinės technologijos pritaikymas energijos prekybos sektoriuje gali sukurti tvirtą ir tvarią energetikos infrastruktūrą.

„Blockchain“ technologija taip pat susilaukė nemažo dėmesio energijos rinkoje, kur BC jau prisidėjo prie naujos koncepcijos, vadinamos energijos internetu (IoE), kuri įgalina skaidrius, decentralizuotus energijos vartotojų tinklus, įskaitant energijos prekybos platformas. Buvo keletas sėkmingų blokų grandinės pritaikymų energetikos pramonėje, kur šios technologijos teikiami patobulinimai paskatino energijos perėjimą ir žiedinės ekonomikos iniciatyvas, pavyzdžiui, naujus sprendimus, skirtus elektriniam e. mobilumui, energijos demokratizavimui, P2P energijos prekybos platformoms, išmanioji apskaita, išmaniųjų tinklų valdymas, žaliųjų sertifikatų išdavimo automatizavimas ir prekyba anglies dvideginiu ir kt. Iš esmės, kaip pabrėžė Wang ir Su, „blockchain“ gali suteikti tris pagrindinius privalumus energetikos sektoriui: (1) decentralizuota prekyba energija ir energijos tiekimas, (2) efektyvus, automatizuotas energijos ir saugojimo srautų valdymas naudojant išmaniąsias sutartis ir (3) saugūs įrašai apie visą verslo veiklą energetikos pramonėje (Juszczyk, Oskar, ir Khuram Shahzad, 2022).

„Blockchain“ technologija energetikos sektoriuje naudojama pirkimo ir pardavimo sandoriams tarp energijos gamintojų ir vartotojų vykdyti. Blokų grandinės technologija leidžia sudaryti energijos pirkimo ir pardavimo sandorius per kelias sekundes. Sumažėja energijos pirkimo kaštai, dėl tiesioginių pardavimų be partnerių. Todėl galutiniams vartotojams ateityje bus mažesnės energijos sąnaudos.

Elektros, pagamintos iš decentralizuotų atsinaujinančių energijos šaltinių, procentas didėja dėl aplinkosaugos problemų, mažėjančių sąnaudų ir padidėjusio, kai kurių atsinaujinančių energijos šaltinių technologijų, pvz., vėjo ir saulės, efektyvumo. Didesnio kiekio atsinaujinančių energijos išteklių integravimas į tinklą ir rinką yra sudėtingas uždavinys elektros rinkos dalyviams. Kad tai būtų įmanoma pasiekti, turi būti apibrėžtos naujos politikos kryptys, leidžiančios integruoti naujas technologijas, pvz., energijos blokų grandinės programas, kurios gali padidinti efektyvumą ir saugumą, kartu padedant pritaikyti didelius su pertrūkiais atsinaujinančių šaltinių kiekius. Todėl komunalinės paslaugos ir tinklų operatoriai, priklausomai nuo šių šaltinių, turi apsvarstyti, kiek energijos būtų galima pagaminti, ypač esant dideliam poreikiui, atsižvelgiant į orų prognozes ir kitus veiksnius. Ateities energetikos sektoriui reikės naujų duomenimis pagrįstų energetikos sistemų, kurias palaiko pažangi duomenų analizė ir „blockchain“ technologija, nes energijos prognozavimo sistemos ir energijos blokų grandinės programos

padidina decentralizuotų ir paskirstytų energijos išteklių rinkos ir tinklo integravimo galimybes (Chacra, S.A., Sireli, Y. and Cali, U. 2021).

Palyginti su tradicinėmis energetikos technologijomis, blokų grandinės taikymas energetikos srityje turi šiuos techninius pranašumus: energijos blokų grandinės technologija padeda sukurti paskirstytą energijos prekybos ir tiekimo sistemą. Blokų grandinės technologija palaiko decentralizuotas energijos tiekimo sistemas ir supaprastintas daugiasluoksnes sistemas, kuriose energijos gamintojai, skirstymo sistemos operatoriai, perdavimo sistemos operatoriai ir tiekėjai gali tiesiogiai sujungti gamintojus ir vartotojus, kad galėtų atlikti sandorius visuose lygiuose per „blockchain“ tinklą (Qiang Wang, Min Su, 2020).

2.1 Skaitmeninimas energetikos pramonėje

Elektros energijos sistemos visame pasaulyje sparčiai keičiasi. Daugiau nei šimtmetį šios sistemos daugiausia rėmėsi centralizuotomis iškastinio kuro gamyklomis, gaminančiomis elektrą ir besiplečiančiais tinklais, kad ji būtų tiekiama galutiniams vartotojams. Komunalinės paslaugos turėjo aiškų tikslą: tiekti elektros energiją labai patikimai ir už mažą kainą. Tačiau dabar vyriausybės turi naujų ambicijų dėl elektros energijos sistemų. Daugelis reikalauja, kad šios sistemos būtų labai priklausomos nuo nepastovios vėjo ir saulės energijos, kai kurios taip pat siekia, kad būtų daug elektrinių transporto priemonių (EV), kurios gali įtempti tinklus. Dar labiau apsunkina reikalus, kad klientai montuoja savo įrangą – nuo saulės panelių iki baterijų ir išmaniųjų prietaisų – būtina sukontroliuoti jų gamybą ir elektros energijos suvartojimą. Komunalinėms įmonėms stengiantis išlaikyti patikimas paslaugas, pasiekti naujus politikos tikslus ir susidoroti su vis didėjančiu sudėtingumu, novatoriai renkasi numanomą sprendimą – blokų grandinės technologiją (Livingston, D., Sivaram, V., Freeman, M., & Fiege, M., 2018).

2018 metų pabaigoje Europos Sąjunga (ES) susitarė dėl 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyvos (ES) 2018/2001 dėl skatinimo naudoti energiją iš atsinaujinančių šaltinių (RED II direktyva). [1], kuris nustato bendrą atsinaujinančios energijos vartojimo tikslą – 32 proc. iki 2030 m.

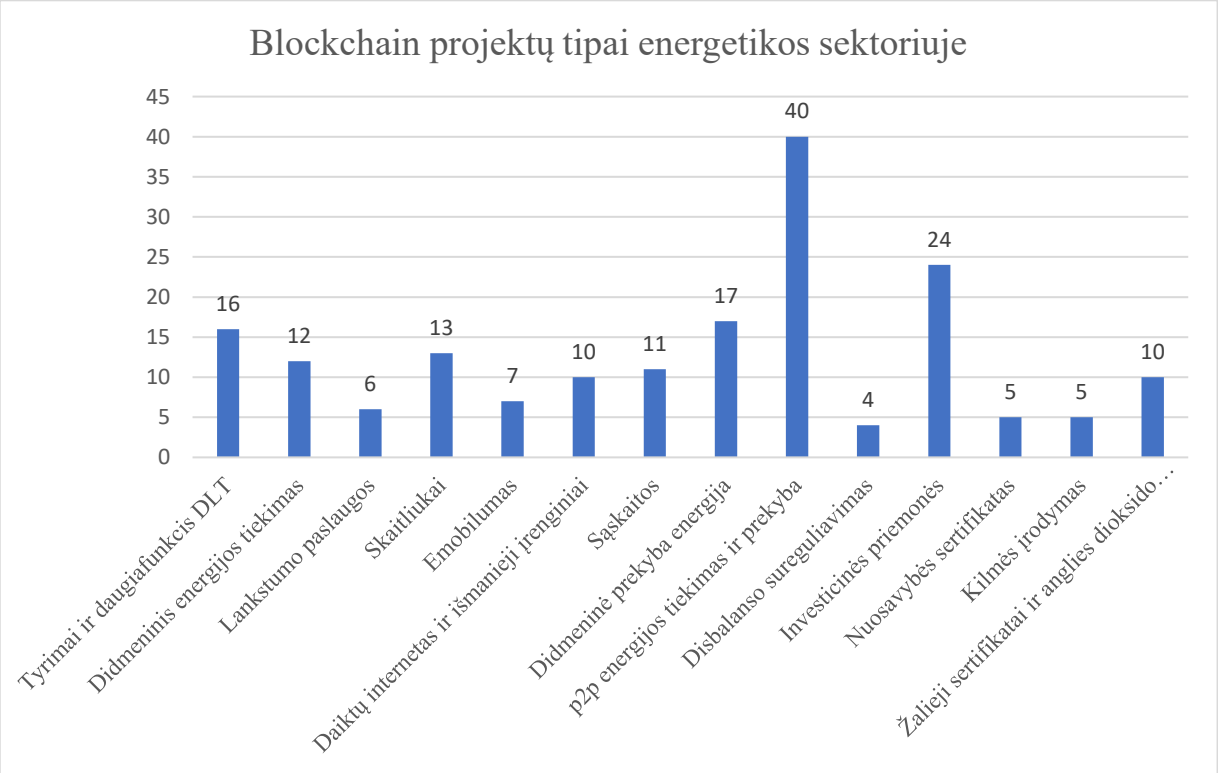
2.2 Blokų grandinės plėtra energijos pramonėje

Perspektyviausios „Blockchain“ taikymo sritys energetikos sektoriuje.

- Išmanioji apskaita;
- Decentralizuota energijos prekyba ir tiekimas;
- Kilmės sertifikatas;
- Elektromobilumas;

- Išmanūs skaitliukai;
- Išmanusis tinklas;
- Atsinaujinančios energijos sistemos *Kaip veikia fotovoltinė sistema* (Goudz, A., Jasarevic, M. 2020).

Kaip rodo Europos Komisijos Jungtinio tyrimų centro (JRC) ataskaita, žiūrėti 7 paveikslą: visų pirma, energetikos sektoriuje yra 16 mokslinių tyrimų iniciatyvų ir daugiafunkcinių blokų grandinės platformų. Yra 17 įmonių, veikiančių „blockchain“ didmeninės prekybos energija srityje, o 11 veikia BC didmeninės energijos tiekimo sektoriuje, o kai kurios užsiima ir viena, ir kita veikla. 6 įmonės siūlo lankstumo paslaugas ir 4 atsiskaitymo už disbalansą produktus. Be to, 13 įmonių aktyviai veikia blokų grandine pagrįsto išmaniojo matavimo srityje, o 10 siūlo daiktų interneto ir išmaniųjų įrenginių sprendimus. Tačiau didžioji dalis įmonių ir iniciatyvų (iš jų 40, trečdalis viso pasaulio) yra orientuotos į P2P energijos tiekimą ir prekybą. Jų tikslas yra išbandyti ir parduoti naujas tinklo valdymo ir verslo programas, kurias žada pasiūlyti „blockchain“. Pavyzdžiui, 11 įmonių siūlo „blockchain“ atsiskaitymo paslaugas. Kitas pavyzdys – verslo modeliai ir investicinės priemonės, tokios kaip pradiniai monetų pasiūlymai, skaitmeninių žetonų, kuriuos investuotojai išperka į naujas sutelktinio finansavimo įmones, išleidimas, pritaikomi ir energetikos sektoriuje. Šioje srityje yra 24 iniciatyvos. Visų pirma, nuosavybės sertifikavimo ir kilmės įrodymo rinkos segmentuose dirba 5 įmonės, o 10 siūlo blokų grandinėmis pagrįstus sprendimus žaliųjų sertifikatų ir anglies dioksido kreditų valdymui (Joint Research Centre, 2022).



Šaltinis: EC

7 pav. Blokų grandinės tipai energetiniame sektoriuje

Blokų grandinės technologija energetikos sektoriuje gali būti naudojama įvairiems tikslams, pavyzdžiui, palengvinti tarpusavio prekybą energija, gerinti tinklo valdymą ir efektyvumą, sudaryti sąlygas skaidriai ir decentralizuotai sekti energijos sandorius bei stiprinti kibernetinio saugumo priemones.

„Blockchain“ technologija pakeitė energijos prekybą ir tarpusavio sandorius energetikos sektoriuje. Naudojant „blockchain“, tokius sandorius kaip prekyba energija galima atlikti beveik akimirksniu, todėl nebereikia tarpininkų.

Kokie privalumai integravus blokų grandinę energetikos sektoriuje:

• **Efektyvi prekyba energija**: „blockchain“ leidžia tiesiogiai prekiauti energija be tradicinių tarpininkų. Tai leidžia greičiau, efektyviau veikti, sumažinant išlaidas ir padidinti skaidrumą.

• **Atsiskaitymas realiuoju laiku** : naudojant „blockchain“, už energijos sandorius galima atsiskaityti realiu laiku, taip užtikrinant greitesnį mokėjimą ir sumažinant administracinius vėlavimus. Tai padidina rinkos likvidumą ir suteikia galimybę greitai gauti lėšų.

• **Padidintas skaidrumas** : „blockchain“ suteikia skaidrią ir nekintamą visų energijos operacijų knygą, leidžiančią dalyviams atsekti ir patikrinti energijos kilmę. Tai padidina pasitikėjimą ir atskaitomybę rinkoje.

• **Decentralizuotos energijos sistemos** : „blockchain“ įgalina decentralizuotas energijos sistemas, leisdamas asmenims arba organizacijoms tiesiogiai keistis atsinaujinančios energijos pertekliumi tarpusavyje. Tai skatina atsinaujinančios energijos gamybą vietos lygmeniu ir sumažina priklausomybę nuo centralizuotų elektros tinklų.

• **Išmaniojo tinklo technologija** : „blockchain“ gali būti integruota su išmaniojo tinklo technologija, kad būtų galima automatizuoti elektros energijos apskaitą, atsiskaitymą ir paskirstymą. Tai pagerina tinklo valdymo efektyvumą ir sumažina veiklos sąnaudas.

• **Atsinaujinančios energijos sertifikatai : „Blockchain“ automatizuoja atsinaujinančios energijos sertifikatų** (REC) gamybą ir keitimąsi energetikos sektoriuje. REC įrodo, kad tam tikras elektros energijos kiekis buvo pagamintas iš atsinaujinančių šaltinių, skatinant švarios energijos iniciatyvas.

BC technologija teikia keletą privalumų tiekimo grandinės valdymui energetikos sektoriuje:

• **Didesnis skaidrumas** : „blockchain“ gali pateikti **skaidrią ir nekintamą** operacijų knygą, užtikrinančią, kad visi tiekimo grandinės dalyviai turėtų prieigą prie tikslios ir naujausios informacijos.

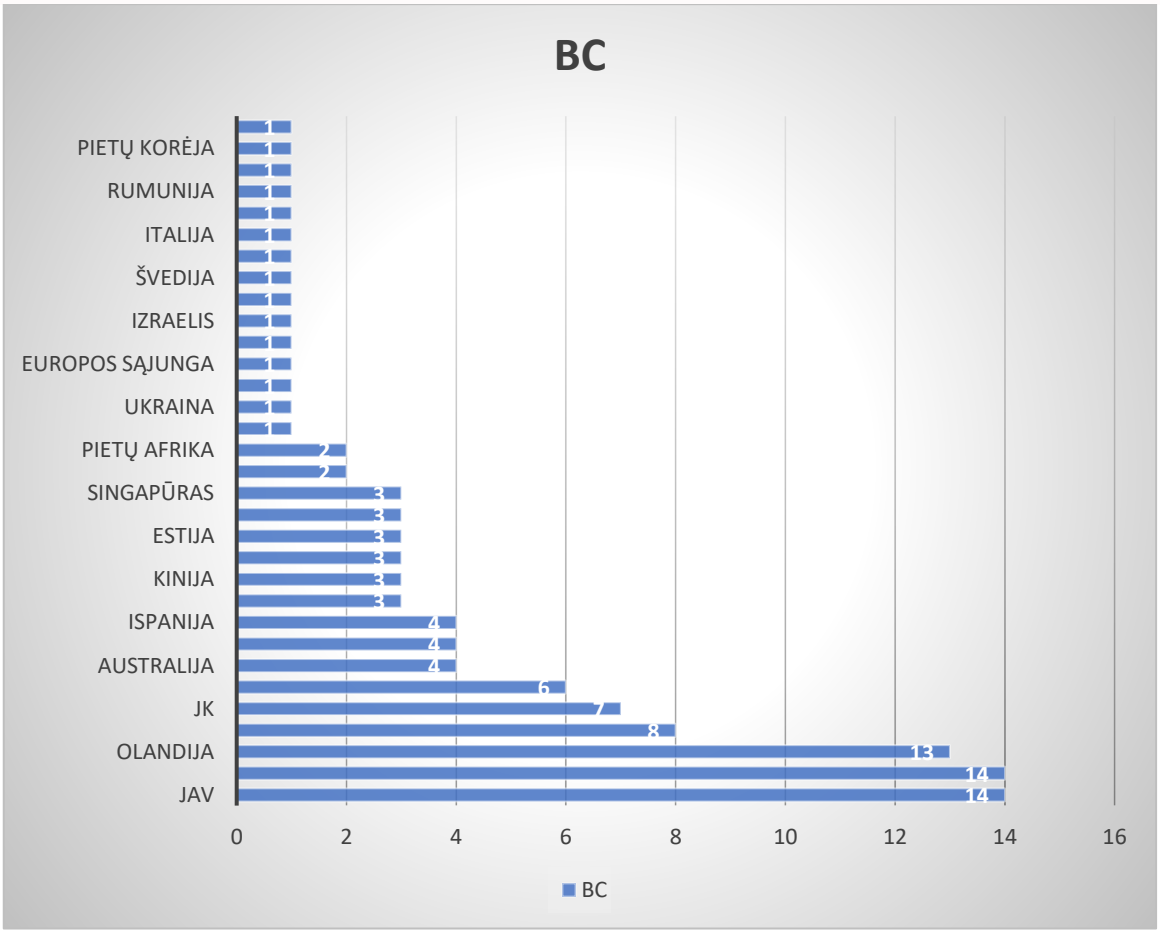
• **Patobulintas atsekamumas** : naudojant blokų grandinę, energijos išteklių kilmę ir judėjimą galima lengvai sekti ir patikrinti. Tai leidžia užtikrinti geresnę atskaitomybę ir padeda nustatyti bet kokius tiekimo grandinės neefektyvumus ar kliūtis.

• **Efektyvus atsiskaitymas** : „blockchain“ leidžia greičiau ir efektyviau atsiskaityti už sandorius, sumažinant rankinio popierizmo ir tarpininkų poreikį. Tai supaprastina tiekimo grandinės procesą ir sumažina išlaidas.

• **Saugus keitimasis duomenimis** : „blockchain“ užtikrina, kad duomenys būtų saugiai saugomi ir dalijamasi įvairioms tiekimo grandinės suinteresuotosioms šalims. Dėl decentralizuoto blokų grandinės pobūdžio ji yra labai atspari klastojimui ar neteisėtai prieigai.

• **Padidintas automatizavimas** : **išmaniosios sutartys** , kurios yra savaime vykdomos sutartys su iš anksto nustatytomis taisyklėmis, užkoduotomis blokų grandinėje, gali automatizuoti įvairius tiekimo grandinės valdymo aspektus. Tai sumažina žmogiškųjų klaidų skaičių ir padidina efektyvumą.

Siekdamas suprasti blokų grandinės potencialo mastą energetikos sektoriuje, Europos Komisijos Jungtinis tyrimų centras atliko susijusių pramonės iniciatyvų energetikos sektoriuje kraštovaizdžio analizę. Ši analizė aiškiai parodė, kad pramonės subjektai energetikos srityje rimtai investuoja į blokų grandinės technologijos bandomuosius projektus ir bandymus. Pagrindinis analizės tikslas buvo apibrėžti šios srities naudojimo atvejų taksonomiją. Buvo nustatytos keturios pagrindinės blokų grandinės naudojimo atvejų klasės energetikos sektoriuje ir aprašytos kituose poskyriuose. Taksonomiją sudaro įvairių tipų naudojimo atvejai, iš viso 117 iniciatyvų (žr. 8 pav.), daugiausia Europos Sąjungoje (65), JAV (14) ir Šveicarijoje (9), o likusios yra išsibarsčiusios visame pasaulyje. Daugiau nei pusė jų, t. y. 67, yra dislokuoti bent koncepcijos įrodymo lygmeniu (Joint Research Centre, 2022).



Šaltinis: sudaryta autorės pagal Joint Research Centre, 2022.

8 pav. Energijos blokų grandinės iniciatyvų paskirstymas pagal šalį

4 lentelėje pateikiamos įmonės naudojančios BC energetikos sektoriuje. Blokų grandinė naudojama išmaniajame tinkle, kuri apima: energijos prekybą, energijos rinką ir t.t „LO3 Energy“ kartu su „Siemens“ sukūrė bandomąjį mikrotinklelį, naudodama „blockchain“ technologiją. Gyventojai, turintys saulės baterijas, gali parduoti perteklinę energiją atgal savo kaimynams, sudarydami tarpusavio sandorį, kuris pasinaudoja blokų grandinės pranašumais.

4 lentelė. Įmonės naudojančios blokų grandinę energijos reikmėms

Išmaniojo tinklo energijos sektorius	Galima nauda	Platforma	Blokų grandinės įgyvendinimo metai	Šalis
Energijos prekyba	Išlaidų sumažinimas	-Enerchain (Ponton) -Interbit (BTL)	2018 2017	Vokietija Kanada
Energijos rinka	- Mokėjimų apdorojimo išlaidų sumažinimas - Sąskaitų skaidrumas - Daugiau energijos tiekimo galimybių	-Drift -Grid+	2017 2018	JAV
P2P rinka	- Paskirstyto energijos šaltinio ekonomikos plėtra - Daugiau energijos tiekimo galimybių - Sumažinti perdavimo tinklo apkrovą	- Brooklyn Microgrid projektas (LO3 Energy) - Jouliette (Alliander ir Spectral)	2017 2018	JAV Olandija
Pasiūlos ir paklausos valdymas	- Pasiūlos ir paklausos grandinės balansavimas	-TenneT - Electron	2018 2016	Olandija
Elektromobilių įkrovimas	- Elektros transporto priemonių įkrovimo ir iškrovimo koordinavimas	-„Share & Charge (Motion Werk) -eMotorWerks	2016 2017	JK JAV
Tinklo stebėjimas ir saugumas	- Tinklo valdymo ir saugumo gerinimas	-„Keyless Signature Infrastructure (Guardtime)	2008	Estija
NT rinka	-Efektyvumo ir skaidrumo gerinimas	-Solar Coin Ideo CoLab	2015 2018	Andora JAV

Šaltinis: Shekh S. Uddin, Rahul Joysoyal, Subrata K. Sarker, S.M. Muyeen, Md. Firoj Ali ir kiti, 2023

Pirmiausia pastebėta, kaip plačiai yra taikoma blokų grandinė energetikos sektoriuje, dažniausiai ji yra naudojama „peer to peer“ prekybai, lietuviškai tiksliau būtų *vartotojas-vartotojui.* Kitas įdomus

atvejis KSI blokų grandinė yra laiko žymėjimo metodas, leidžiantis įrodyti savo duomenų egzistavimą ir vientisumą neatskleidžiant jų turinio . Ją sukūrė Estijos kibernetinio saugumo įmonė „Guardtime“.

2.3 „BLOCKCHAIN“ projektų tipai

2.3.1 Išmanieji skaitliukai

Vienas iš svarbiausių išmaniojo tinklo komponentų yra išmanieji skaitikliai – elektroniniai prietaisai, registruojantys realiu laiku suvartojamos ir pagamintos elektros energiją namų ūkyje ar pramonėje ir siunčiantys duomenis elektros energijos pardavėjui stebėti atsiskaitymus. Taigi išmanieji skaitikliai atlieka pagrindinį vaidmenį išmaniajame tinkle, nes jie gali suteikti naudingos informacijos apie suvartojimą ir vartotojų profilį, o tai gali padėti prognozuoti apkrovą ir sumažinti apkrovos piką (Blockchain in the Energy Sector JRC technical report, 2021).

Sujungę išmaniųjų energijos skaitiklių rodmenis su nekintama duomenų saugykla, kurią įgalina blokų grandinė, vartotojai gali ne tik labiau pasitikėti atsiskaitymu už elektrą realiu laiku, bet ir atverti duris jiems pritaikyti savo naudojimą pagal esamas energijos kainas, sąveikaujant su vietinėmis energijos rinkomis skaidriai ir saugiai. „Blockchain“ technologija viso šio proceso metu labai palengvina elektronines atsiskaitymo sistemas dėl sklandaus mokėjimų apdorojimo ir patikimų duomenų įrašų, todėl visos operacijos gali būti atliekamos automatiškai ir be centralizuotos šalies. Skaitiklių duomenų gamintojai pagaliau gali turėti savo duomenis ir dalytis jais su savo sandorio šalimi, kad atsiskaitytų. Šias operacijas taip pat lengva sekti ir stebėti. Be to, visą mainų istoriją galima atsisiųsti iš „blockchain“ platformos ir naudoti periodiškai apmokėti sąskaitas.

2.3.2 Išmaniosios sutartys

Išmaniosios sutartys, susijusios su išmaniaisiais skaitikliais tinkle, yra įdiegtos blokų grandinėje. Ji užtikrina saugias operacijas leisdama tik autentišką duomenų perdavimą tarp išmaniųjų skaitiklių ir priežiūros mazgų ir praneša, jei įvyko neteisėtas ir piktybiškas duomenų klastojimas.

Naudojant blokų grandinės technologiją ir išmaniąsias sutartis, energijos tinklus galima efektyviai valdyti. Išmaniosios sutartys siunčia signalus sistemai, kad suformuluotų taisykles, kaip inicijuoti operacijas. Tokie procesai yra pagrįsti iš anksto nustatytomis išmaniųjų sutarčių taisyklėmis, užtikrinančiomis, kad visi energijos ir saugojimo srautai būtų valdomi automatiškai, o tai padeda subalansuoti pasiūlą ir paklausą. Trečia, „blockchain“ gali saugiai įrašyti visus energijos srautus. Energijos blokų grandinė saugo energijos sandorių duomenis vienoje blokų grandinėje, užtikrindama paskirstytą visų energijos srautų ir verslo veiklos saugumą (Qiang Wang, Min Su, 2020).

Pagrindinės sutarties funkcijos – vartotojų registracija, gamintojų įkeltos kainos, vartotojų užantspauduoti pasiūlymai, sistemų suderinimas, išmaniųjų skaitiklių nuskaitymas, sandorių likučio atsiskaitymas, premijų ir nuobaudų skatinimas. Sutartyje taip pat numatytos papildomos funkcijos užsakymo būsenos užklausai pagal ID arba adresą (G. Mingxing, Z. Ke, W. Su, X. Jinlei, ir kt., 2023).

Aiškinant plačiau kaip veikia išmaniosios sutartys: be kriptovaliutų operacijų, blokų grandinėje taip pat gali būti saugomas programinės įrangos kodas, vadinamas išmaniosiomis sutartimis, kuris vykdomas, kai įvykdomos iš anksto nustatytos sąlygos. Išmanioji sutartis yra įterpta į blokų grandinę, panašiai kaip kriptovaliutos operacija (tai yra dažniausiai naudojamas blokų grandinės atvejis). Konkrečiai, sukompiliuotas kodas ir konkrečios informacijos dalys, pvz., funkcijų, kurias reikia vykdyti, sąrašas yra siunčiamos iš piniginės į blokų grandinę. Tada šis kodas ir informacija turi būti įtraukti į bloką, kuris pridedamas prie knygos (nors ir sutarimo mechanizmas), tada išmaniosios sutarties kodas bus vykdomas, kad būtų nustatyta pradinė išmaniosios sutarties būsena . Panašiai kaip ir valiutos operacijos, kriptografinė maiša decentralizuotai apsaugo išmaniąją sutartį nuo bandymų ją pakeisti ar sugadinti. Kai jos kodas yra saugomas blokų grandinėje, išmaniąją sutartį galima palyginti su programinės įrangos procesu, kuris bus paleistas susidarius konkrečioms sąlygoms (pvz., tam tikram energijos suvartojimui ar gamybai). Praktiškai išmaniojoje sutartyje įterpto kodo vykdymas yra įdiegtas virtualioje aplinkoje, kurią fiziškai priglobia visi blokų grandinę sudarantys mazgai, tarsi jie būtų vienas kompiuteris (Desen Kirli, Benoit Couraud, Valentin Robu ir kiti, 2022).

2.3.3 „The Peer to peer“ prekyba

P2P protokolas „Hyperledger Fabric“ sukurtas naudojant „google RPC“ (gRPC). Jis naudoja protokolo buferius, kad nustatytų pranešimų struktūrą. Pranešimai perduodami tarp mazgų, kad būtų galima atlikti įvairias funkcijas. „Hyperledger Fabric“ yra keturi pagrindiniai pranešimų tipai: atradimas, operacija, sinchronizavimas ir sutarimas. Aptikimo pranešimais keičiamasi tarp mazgų paleidžiant, kad būtų galima rasti kitus tinkle esančius lygius. Operacijų pranešimai naudojami operacijoms įdiegti, iškviesti ir užklausoms pateikti, o sutarimo pranešimais keičiamasi konsensuso metu. Sinchronizavimo pranešimai perduodami tarp mazgų, kad būtų galima sinchronizuoti ir atnaujinti blokų grandinę visuose mazguose (Imran Bashir, 2018).

Kad vyktų P2P prekyba elektra, kiekvienas dalyvis turėtų investuoti į kompiuterį su blokų grandinės mazgu. Tada blokų grandinės tinklas valdys ir registruos visas operacijas (Basden ir Cottrell, 2017).

Norėdami pradėti prekybą energija, vartotojai iš pradžių turi pasirašyti P2P prekybos paslaugų platformos prenumeratos sutartį. Pasibaigus varžytynių procesui ir nustačius prekybos sumą bei kainą, energija gaminama iš vienos šalies, perduodama, vėliau suvartojama antrosios (Abou Chacra *ir kt.* ,

2018). Galutinio proceso metu atsiskaitoma už energijos kiekį. Tikra P2P prekyba vyksta tada, kai gamintojai prekiauja energija ir mokėjimais tiesiogiai vieni kitiems, neturėdami centrinės įstaigos, tokios kaip komunalinė įmonė. Tai pavyktų pirmiausia tiesiogiai prijungus visas vartotojų svetaines, o tada įdiegus „blockchain“ technologiją, kad būtų galima prekiauti. „Blockchain“ valdoma P2P energijos prekyba leidžia pirkėjams siūlyti reikiamą energijos kiekį iš konkretaus gamintojo už tam tikrą kainą, kurią jie gali nurodyti sutartyje. Išmanioji sutartis suaktyvinama tik tada, kai pardavėjas sutinka įvykdyti pirkėjo sąlygas (Abou Chacra *ir kt.* , 2018).

Taigi gamintojai gali tiesiogiai parduoti energijos perteklių netoliese esantiems vartotojams, skatindami decentralizuotos švarios energijos gamybos augimą ir prisidėti prie tvarumo tikslų.

2.3.4 Elektromobiliai

Riba tarp elektros energijos ir transporto sektorių nyksta dėl didėjančio elektromobilių populiarumo. Tačiau šios transporto priemonės vis dar susiduria su didelėmis kliūtimis, ypač atgraso pirkėjus nuo elektromobilių – viešosios įkrovimo infrastruktūros trūkumas. „Blockchain“ tinklai, leidžiantys privatiems įkrovimo infrastruktūros savininkams sklandžiai parduoti įkrovimo paslaugas elektromobilių savininkams, galėtų pagerinti elektromobilių patrauklumą ir įsisavinimą. Pavyzdžiui, Kalifornijos startuolis „eMotorWerks“ ir Vokietijos komunalinių paslaugų remiamas startuolis „MotionWerk“ Kalifornijoje bendradarbiavo su bandomuoju projektu, skirtu sukurti elektromobilių įkrovimo rinką. Ši iniciatyva leistų namų ūkiams, turintiems įkroviklius, išnuomoti juos elektromobiliams (Livingston, D., Sivaram, V., Freeman, M., ir Fiege, M., 2018).

2.3.5 Tinklo valdymas, išmanusis tinklas

Išmanusis tinklas užtikrina didesnį elektros energijos tiekimo saugumą. Tačiau ši koncepcija padidina esamos elektros pramonės sudėtingumą. Blokų grandinės integravimas į išmanųjį tinklą leidžia bendruomenei palaikyti sandorius sistemoje bendru sutarimu. Sandoriai atliekami su išmaniosiomis sutartimis. Operacijų istorija saugoma blokų grandinėje ir kopijuojama į visus pilnus mazgus. „Blockchain“ suteikia išmaniųjų sutarčių ir operacijų duomenų nekintamumą, apribodama įrašo keitimą arba trynimą (A. Agung ir G. Agung, R. Handayani, 2022).

Prekyboje elektra svarbiausia yra tikrinimas, ar energijos sandoris yra tikslus ir skaidrus, nes dabar prekyba energija yra monopolizuota centrinės valdžios ar stambių korporacijų. Daugeliu atvejų vyriausybinėmis agentūromis ar didelėmis korporacijomis galima pasitikėti, tačiau jas gali neutralizuoti įsilaužėliai ar kitos atakos.

5 lentelė. Tradicinio išmaniojo tinklo ir blokų grandinės pagrindu veikiančio išmaniojo tinklo valdymo ir veikimo palyginimas

„Smartgrid“ domenai	**Tradicinis išmanusis tinklas**	**Blockchain pagrįstas išmanusis tinklas**
Gamyba	• Didžioji dalis neatsinaujinančių energijos šaltinių. • Dažnai dideliu mastu iš centrinio šaltinio.	• Platformą gali naudoti visi energijos šaltiniai • Mikrotinklo gamintojai gali prisidėti prie atsinaujinančios energijos rinkos.
Perdavimas ir paskirstymas	• Vartotojai negali gauti nuolatinės informacijos apie energijos suvartojimą • Ribota kontrolė dėl paklausos ir pasiūlos informacijos srauto trūkumo • Didelis paskirstymo atstumas prisideda prie didelių paskirstymo nuostolių • Galios sandorių procedūros gali būti šiek tiek sudėtingos ir nesaugios	• Vartotojai gali gauti energijos suvartojimo ataskaitą reguliariai, tiksliai ir greitai • Energijos paskirstymas yra labai kontroliuojamas • Skatinama vietinė gamyba ir platinimas ir labai sumažinami paskirstymo nuostoliai • Supaprastintos ir labai saugios sandorių procedūros
Vartojimas	• Vartotojai neturi įtakos išmaniojo tinklo valdymui, kontrolei ir veikimui	• Vartotojai gali dalyvauti išmaniojo tinklo valdyme, eksploatacijoje ir valdyme kaip mikrotinklo gamintojai
Operacija	• Klientai dažnai turi ribotą energijos tiekėjo pasirinkimą • Valdomas rankiniu būdu ir yra pažeidžiamas netyčinių ar kenkėjiškų atakų • Sistemos atnaujinimai ir priežiūra atliekami rankiniu būdu • Klientai dažnai turi popierinę arba skaitmeninę sutartį • Centriniu būdu valdomas dažnio ir įtampos valdymas – sudėtinga valdyti naudojant kelis paskirstytus generatorius • Linkęs į nesėkmes ir gali sukelti elektros energijos tiekimą	• Klientai turi keletą energijos tiekėjų, iš kurių daugelis gali būti atsinaujinantys šaltiniai • Automatizuota ir savikontrolės sistema, sumažinanti biurokratiją • Automatiškai aptinka klaidas ir savarankiškai šalina trikdžius • Klientai turi išmaniąją sutartį • Automatinis dažnio ir įtampos valdymas gali būti atliekamas tiek lokaliai, tiek centralizuotai • Sistemai įtakos neturi, kai kurie sugedę arba nereaguojantys mazgai
Paslaugų teikėjas	• Neįgalioti asmenys / valdžios institucijos gali gauti prieigą prie neskelbtinų duomenų • Pažeidžiamas kibernetinių grėsmių • Neskelbtina informacija iš įvairių suinteresuotųjų šalių gali nutekėti neatsekus šaltinio	• Išmanioji sutartis užtikrina, kad tik tinkami subjektai turėtų prieigą prie atitinkamų duomenų • Labai apsaugota ir sunkiai nulaužiama sistema • Duomenų šifravimas ir Merkel maiša paskirstytame tinkle užtikrina maksimalų saugumą
Rinkodara	• Stebima centralizuoto valdymo būdu • Kainų nustatymas, atsiskaitymas ir kitos operacijos valdomos centralizuotai	• Decentralizuotas, bet gali būti ir pusiau centralizuotas • Galima naudoti išmaniąją sutartimi pagrįstą decentralizuotą ir automatizuotą kainų nustatymą, atsiskaitymą ir kitas operacijas

Šaltinis: sudaryta autorės pagal JRC

5 lentelėje matyti, kad blokų grandinės naudojimas duomenų ir išmaniojo tinklo valdymui yra naudingas kuriant diversifikuotą platformą, kurioje atitinkamos suinteresuotosios šalys turi vienodą įtaką bendram infrastruktūros veikimui.

Išmanusis tinklas yra naujos kartos tinklas, sukurtas susiliejus su IT technologijomis. Jei dėl kibernetinės atakos bus pažeistas išmanusis tinklas, maitinimo šaltinis, gali būti padaryta didžiulė žala, pavyzdžiui, elektros energijos tiekimo nutraukimas visoje šalyje. Tiesą sakant, kibernetinių atakų grėsmė didėja, o kibernetinio saugumo grėsmė išmaniajam tinklui nėra nereikšminga (Kim, Seong-Kyu, and Jun-Ho Huh, 2018).

2.4 Blokų grandinės technologijos diegimo energetikos sektoriuje iššūkiai

Naudojimo atvejų įgyvendinimas neapsiriboja blokų grandinės ir išmaniųjų sutarčių nustatymu. Diegiant reikia atsižvelgti į daugelį veiksnių, tokių kaip leidimai, mazgų arba operacijų skaičius per sekundę, kurie turi įtakos įgyvendinimui. Prieiga prie duomenų (gaunamų iš skaitiklių) tai potenciali kliūtis, nes blokų grandinės veikia naudojant pačius klasikinius interneto protokolus, o ne visi skaitikliai palaiko interneto ryšius. Tai akivaizdžiai kelia dar vieną svarbią problemą – stabilaus interneto ryšio poreikis, kad sistema tinkamai veiktų. Tačiau tai yra reikalavimas, kuris apskritai bus vis dažnesnis skaitmenizuojant energetikos sistemą – internetas taps svarbia paslauga, reikalinga tinklui valdyti. „Blockchain“ platformų (ypač išmaniųjų sutarčių) stadija yra dar viena kliūtis diegti sudėtingus automatizavimus, nes kai kurios funkcijos vis dar kuriamos. Kitas sudėtingas veiksnys sąveika su esamomis sistemomis. Šiandien didžiausias iššūkis yra integracija su senomis sistemomis, siekiant rinkti rodmenis ir sistemos duomenis. Dėl šios priežasties energijos bendruomenės naudojasi logika ir „blockchain“ pasaulių integracijomis (JRC technical report, 2021).

Teisiniai iššūkiai

„Blokų grandinės pagrindu veikiančios prekybos energija potencialas šiuo metu susiduria su daugybe teisinių kliūčių. Energetikos pramonės įstatymas (EnWG) su sudėtingais pranešimo ir patvirtinimo reikalavimais bei sutarčių projektavimo reikalavimais prekybai energija dar nėra pritaikytas tiesioginei prekybai energija tarp galutinių vartotojų. Kiti naudojimosi energija prekybos platformoje reikalavimai ir įpareigojimai, be kita ko, kyla iš Elektros tinklo mokesčių potvarkio (StromNZV), Elektros mokesčio įstatymo (StromStG), įskaitant susijusį įgyvendinimo reglamentą (StromStV) ir Atsinaujinančių energijos šaltinių įstatymo (EEG). Kadangi šiuo metu ir tikriausiai ateityje pavieniai galutiniai vartotojai negali patenkinti energetikos teisės aktų reikalavimų prekybai energija, todėl blokų grandinėmis pagrįstose energijos prekybos platformose tikriausiai taip pat reikės komercinių tarpininkų.

Duomenų apsaugos požiūriu pagrindinė problema yra ta, kad privačioje blokų grandinėje saugomus duomenis gali peržiūrėti visi dalyviai, net jei šie duomenys yra asmeniniai. Todėl asmens duomenų tvarkymui blokų grandinėje reikalingas pateisinimas, pavyzdžiui, veiksmingas sutikimas (6 str. 1 d. 1 p. a p.), BDAR 7 str.). Be to, dėl techninio saugumo nuo manipuliavimo, vieną kartą išsaugoti ir galbūt neteisingi duomenys gali būti ištrinti arba pakeisti tik taikant konsensuso mechanizmą. Dėl to nukentėjusiųjų teisių įgyvendinimas (BDAR 12 str. ir toliau) gali būti gerokai apsunkintas, o gal net neįmanomas. Taip pat kyla abejonių, kas atsakingas už decentralizuotą platformą, kaip apibrėžta BDAR 4 straipsnyje Nr. 7“ (Roland Stempelmann, 2021).

Teisė būti pamirštam 17 str. BDAR. Viena „blockchain“ ypatybių – nekeičiami saugomi duomenys – prieštarauja asmens duomenų teisės aktų nuostatoms, pagal kurias asmens duomenys turi būti sunaikinti, kai jie pasieks savo paskirtį arba kai asmuo prašo „teisės būti pamirštam“ str. 17 BDAR.

Visi šie iššūkiai rodo, kad naudojant blokų grandinės technologiją energetikos sektoriuje, svarbu atidžiai įvertinti ir spręsti su BDAR susijusius klausimus.

Apibendrinant galima pasakyti, kad sėkmingas blokų grandinės integravimas energetikos sektoriuje priklauso nuo daugelio technologinių ir infrastruktūrinių iššūkių įveikimo. Tai apima pažangių matavimo infrastruktūrų sukūrimą, sąveikumo problemų sprendimą, blokų grandinės platformų mastelio ir realaus laiko apdorojimo apribojimų šalinimą ir techninio sudėtingumo kliūčių įveikimą.

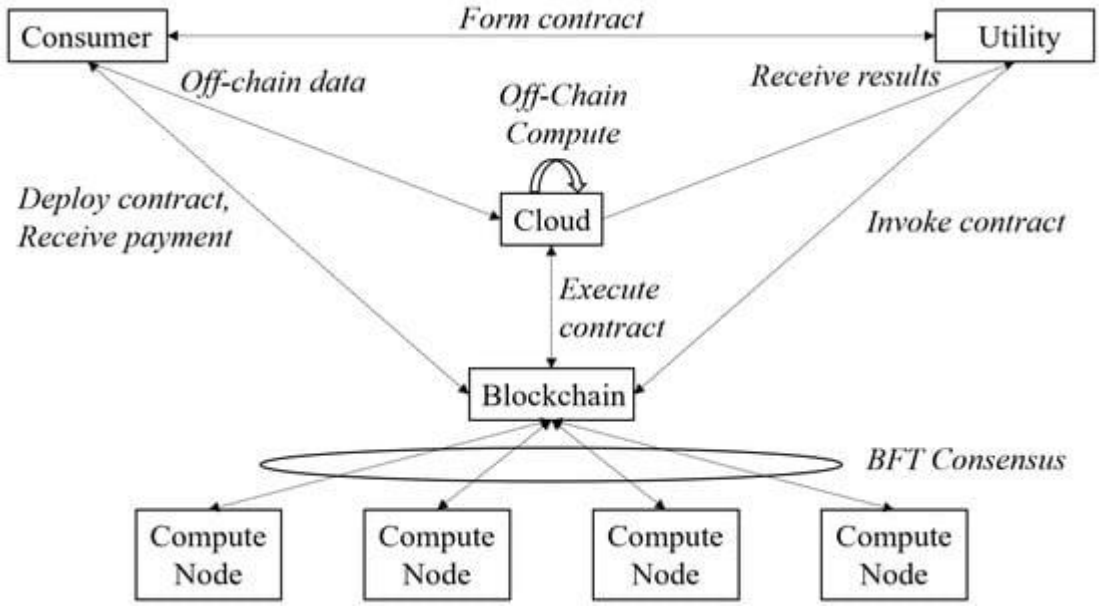
2.5 Kibernetinis saugumas energetiniame sektoriuje

Visi duomenys, kuriais keičiamasi „blockchain“ yra užšifruoti, todėl jų pakeisti ar nulaužti beveik neįmanoma. Dėl šių savybių jis yra ypač galingas sprendimas, galintis prisidėti prie ypatingos svarbos energetikos infrastruktūros kibernetinio saugumo, tiekimo grandinės valdymo, transaktyviųjų energijos sistemų ar vietinių energijos rinkų bei paskirstyto koordinavimo tarp tinklo subjektų gerinimo. Blokų grandinėms būdingos funkcijos – decentralizavimas, nekintamumas ir šifravimas – yra esminiai modernaus ir saugaus elektros tinklo projektavimo kriterijai (Pacific Northwest National Labaratory, 2019).

„Blockchain“ užtikrina, kad privatūs duomenys išliktų nekintantys ir saugūs, pagerina skaidrumą ir leidžia vartotojams turėti ir valdyti savo duomenis. Skaitmeninės tapatybės gali būti saugomos platformoje su privačiu raktu, kuris suteikia prieigą tik patvirtintam vartotojui. Tai sumažins duomenis pažeidimo riziką ir užkirs kelią neteisėtai prieigai prie gamintojų ir komponentų duomenų energetikos sektoriuje (Dr. Zoya Pourmirza, 2023).

„Tyrimai, skirti privatumo apsaugai, yra pagrįsti užtikrinimu, kad duomenų prašytojas galėtų pasiekti tik tuos duomenis, kuriuos savininkas aiškiai leidžia jam pasiekti, be to, prašytojas gautų tik

anonimizuotas suvestines ataskaitas. Prieiga prie pačių neapdorotų duomenų nesuteikiama, užtikrinant, kad savininko privatumas nebūtų pažeistas dėl nelaimingų atsitikimų, piktų kėslų ar išorinio įsiskverbimo į prašytojo IT sistemas. 9 paveikslas yra geras tokio požiūrio pavyzdys.



Šaltinis: Honari K ir kt., 2023

9 pav. Privatumą išsauganti duomenų prieiga per išmaniąsias sutartis

9 paveiksle komunalinė programa nori pasiekti vartotojų duomenis. Vartotojas saugiai saugos savo duomenis ne grandinėje esančioje duomenų bazėje (manoma, kad ji yra debesies pagrindu). Komunalinė įmonė ir vartotojas derėsis dėl SC (Smart Contract), kuriame bus nustatyti duomenys, kuriuos reikia pateikti, ir kompensacija vartotojui. Vartotojas pateikia šią sutartį su BC. Priemonė gali iškviesti SC, suaktyvindama (trečiosios šalies) debesies pagrindu vykdomą ne grandinės skaičiavimą, apimantį vartotojo duomenis. Tik šio skaičiavimo rezultatas grąžinamas į komunalinę įmonę o vartotojui sumokami pinigai (Honari K ir kt., 2023). “

Gai ir kt. pasiūlė blokų grandinę kovai su nesąžiningu energijos naudojimu, ryšio trukdžiais ir duomenų centrų atakomis.

1. Nekintamumas ir duomenų vientisumas: blokų grandinės naudojimas užtikrina nekintamumą ir duomenų vientisumą. Kai duomenys įrašomi į blokų grandinę, jų negalima keisti ar sugadinti, užtikrinant didelį pasitikėjimą ir užkertant kelią neteisėtiems pakeitimams. Pavyzdžiui, kriptografinė maišos funkcija (pvz., SHA-256) naudojama nekintamumui ir duomenų vientisumui užtikrinti.

2. Konsensuso mechanizmas: blokų grandinėje naudojamas sutarimo mechanizmas užtikrina operacijų tarp dalyvaujančių mazgų susitarimą ir galiojimą. Šis mechanizmas padeda išvengti atakų, pvz., dvigubų išlaidų, ir užtikrina sistemos vientisumą. Darbo įrodymo arba Bizantijos gedimų tolerancijos (BFT) algoritmai užtikrina blokų grandinės duomenis.

3. Šifravimas ir privatumas: šifravimo metodai taikomi slaptiems duomenims, įskaitant skaitmenines tapatybes, energijos operacijas ir asmeninę informaciją apsaugoti. Tai padeda užtikrinti

privatumą ir konfidencialumą, todėl neįgaliotoms šalims sunku pasiekti arba manipuliuoti duomenimis. Elipsinės kreivės kriptografija (ECC) su homomorfiniu šifravimu suteiks saugią ir patikimą aplinką saugumui ir privatumui užtikrinti.

4. Autentifikavimas ir prieigos kontrolė: tapatybės ir prieigos valdymo sistema įgyvendina tvirtus autentifikavimo mechanizmus ir vaidmenimis pagrįstą prieigos kontrolę. Tai užtikrina, kad tik įgalioti vartotojai, turintys atitinkamus vaidmenis, galėtų pasiekti konkrečias funkcijas ir duomenis, taip sumažinant neteisėtos prieigos riziką. Elipsinės kreivės skaitmeninio parašo algoritmas (ECDSA) su kelių faktorių autentifikavimu (MFA) ir vaidmenimis pagrįstu prieigos valdymu (RBAC) naudojamas stipriam autentifikavimui ir prieigos kontrolei.

5. Saugus ryšys: saugūs ryšio protokolai naudojami duomenų perdavimui apsaugoti mikrotinklo sistemoje. Tai apsaugo nuo slaptos informacijos pasiklausymo ir neteisėto perėmimo. Saugiam ryšiui galima naudoti „Transport Layer Security“ (TLS) arba „Secure Socket Layer“ (SSL) protokolus.

6. Atspari infrastruktūra: „Microgrid“ sistema suprojektuota su atleidimo ir gedimų tolerancijos mechanizmais, užtikrinančiais energijos tiekimo prieinamumą ir patikimumą. Šis atsparumas padeda sušvelninti galimų atakų ar gedimų poveikį ir palaiko nepertraukiamą energijos paskirstymą.

7. Auditas ir stebėjimas: sistema apima audito ir stebėjimo mechanizmus, kad būtų galima greitai aptikti saugumo incidentus ir į juos reaguoti. Prieigos įvykių, operacijų ir sistemos veiklos žurnalai saugomi blokų grandinėje, todėl galima atsekamumą ir atskaitomybę. Galima įdiegti realiojo laiko stebėjimo įrankius ir anomalijų aptikimo algoritmus, kad būtų galima nustatyti galimas saugumo grėsmes.

8. Teisės aktų laikymasis: sistema užtikrina, kad būtų laikomasi atitinkamų reglamentų ir standartų, susijusių su duomenų apsauga, privatumu ir prekyba energija. Naudodama blokų grandinės technologiją, sistema pateikia skaidrius ir audituojamus įrašus, kurie gali padėti laikytis teisės aktų.

9. Grėsmių mažinimas: naudojant „blockchain“ technologiją, sumažėja centralizuotų atakų rizika, nes dėl paskirstyto tinklo pobūdžio kenkėjiški veikėjai gali sunkiau pažeisti sistemą. Be to, kriptografijos metodų ir saugių protokolų integravimas padeda sumažinti įvairias saugumo grėsmes.

Ši sistema gali įveikti kibernetinio saugumo problemas, kurios padės atremti žinomas grėsmes ir suteiks saugią ir patikimą elektros energijos gamybos ir paskirstymo sistemą (Khubrani MM, Alam S, 2023).

6 lentelėje pateikti kibernetinių atakų pavyzdžiai prieš išmaniuosius tinklus.

6 lentelė. Kibernetinio saugumo atakų prieš išmaniuosius tinklus ir mikrotinklus pavyzdžiai

Pavyzdys	Šalis, metai	Atakos tipas	Detalės
Ukrainoje nutrūko elektros tiekimas	Ukraina 2015 m.	DDoS	2015 m. gruodį grupė užpuolikų panaudojo DDoS ataką, kad perkrautų trijų Ukrainos elektros skirstymo įmonių serverius, dėl kurių nutrūko elektros tiekimas, daugiau nei 225 000 klientų kelias valandas liko be elektros.
Dragonfly 2.0	Pasaulinis 2013 m.	APT	„Dragonfly 2.0“ yra kenkėjiškų programų kampanija, kuri nuo 2013 m. buvo nukreipta į energijos tinklus ir kitą svarbią infrastruktūrą visame pasaulyje. Kampanijos užpuolikai naudojo įvairius metodus, kad gautų prieigą prie energijos tinklų valdymo sistemų, įskaitant sukčiavimo ir vandens telkinių atakas.
Johanesburgo miesto išpirkos reikalaujančios programos	pietų Afrika 2019 m.	Ransomware	2019 m. Johanesburgo miestas Pietų Afrikoje patyrė išpirkos reikalaujančių programų ataką, kuri paveikė jo elektros tinklą, dėl kurio visame mieste nutrūko elektros tiekimas. Užpuolikai pareikalavo 4„ Bitcoin“ išpirkos, kurią miestas atsisakė sumokėti
Enel ransomware ataka	Italija 2020 m.	Ransomware	2020 m. energetikos milžiną „Enel“ nusitaikė gyvatė ir „Netwalker“ išpirkos programa.
Kolonijinio vamzdyno puolimas	Jungtinės Valstijos 2021 m.	Ransomware	Kolonijinis vamzdynas, tiekiantis daugiau nei pusę JAV Rytų pakrantės naftos, 2021 m. gegužę patyrė išpirkos reikalaujančios programos ataką, dėl kurios jis buvo priverstas nutraukti veiklą. „Colonial Pipeline“ galiausiai sumokėjo 4,4 milijono USD Bitcoin išpirką, kurios paprašė užpuolikai, grupė, pasivadinusi „DarkSide“.
„SolarWinds“ įsilaužimas	Pasaulinis 2020 m.	Tiekimo grandinės ataka	Nustatyta, kad „SolarWinds Orion“ programinė įranga (versijos 2019.4–2020.2.1 HF1) buvo pažeista 2020 m. gruodžio mėn. dėl sudėtingos tiekimo grandinės atakos, kuri paveikė daugybę JAV vyriausybinių organizacijų ir komercinių įmonių. Manoma, kad užpuolikai yra valstybės remiama gauja iš Rusijos, užkrėstos programinės įrangos dėka galėjo pasiekti privačią informaciją ir sistemas.

Šaltinis: Sudaryta autorės pagal Khubrani, Mousa Mohammed ir Shadab Alam. 2023

Iš šios lentelės pateiktų duomenų matome, kad energetikos sektorius yra kritinė infrastruktūra, kuriai sutrikus, galima patirti didelių nuostolių, žmonės gali likti be elektros energijos, o vyriausybės patirti didelių nuostolių, todėl svarbu apsaugoti energetikos sektorių.

2.5.1 Kibernetinės atakos prieš blokų grandinę energetiniame sektoriuje

Kibernetinės atakos prieš blokų grandinės technologiją energetikos sektoriuje kelia didelę grėsmę energijos tiekimo ir prekybos procesų saugumui ir vientisumui. Štai keletas galimų kibernetinių atakų, kurios gali būti nukreiptos į blokų grandinę energetikos sektoriuje:

1. 51 % ataka: blokų grandinės tinkle, jei užpuolikas valdo daugiau nei 50 % tinklo skaičiavimo galios, jis gali manipuliuoti transakcijomis, atšaukti operacijas, ar net neleisti patvirtinti naujų sandorių.

2. „Sybil Attack“: šio tipo ataka apima kelių netikrų tapatybių sukūrimą, kad būtų galima valdyti didelę tinklo mazgų dalį. Taip elgdamasis užpuolikas gali sutrikdyti sutarimo mechanizmą ir potencialiai manipuliuoti blokų grandine.

3. Paskirstyta paslaugos trikdymo (DDoS) ataka: užpuolikas gali pradėti „DDoS“ ataką prieš blokų grandinės mazgus arba tinklus energetikos sektoriuje, sukeldamas paslaugų sutrikimus ir neleisdamas teisėtiems vartotojams pasiekti blokų grandinės.

4. Išmaniųjų sutarčių pažeidžiamumas: išmaniosios sutartys yra savaime vykdomos sutartys, kurių sutarties sąlygos yra tiesiogiai įrašytos į kodą. Užpuolikai gali išnaudoti išmaniųjų sutarčių spragas vogti lėšas, manipuliuoti sandoriais ar trikdyti operacijas.

5. Kenkėjiškos programos ir sukčiavimo atakos: užpuolikai gali panaudoti kenkėjiškas programas arba sukčiavimo atakas, kad gautų neteisėtą prieigą prie vartotojų privačių raktų arba kredencialų, leidžiančių jiems kontroliuoti arba pavogti blokų grandinėje saugomą kriptovaliutos turtą.

6. Vidinės grėsmės, gali piktnaudžiauti savo privilegijomis, kad galėtų klastoti duomenis, manipuliuoti sandoriais arba trikdyti operacijas iš vidaus.

Apibendrinat ištirtą informaciją, energetikos įmonės ir blokų grandinės kūrėjai, siekdami sumažinti šias kibernetines grėsmes, turėtų įdiegti patikimas saugumo priemones, tokias kaip šifravimas, kelių veiksnių autentifikavimas, reguliarūs saugumo auditai ir nuolatinis tinklo veiklos stebėjimas. Be to, darbuotojų ir vartotojų mokymas apie geriausią kibernetinio saugumo praktiką ir reguliarių mokymų vedimas gali padėti išvengti sėkmingų kibernetinių atakų prieš blokų grandinės technologiją energetikos sektoriuje.

3. BLOKŲ GRANDINĖS TAIKYMAS ENERGETIKOS SEKTORIUJE TYRIMO METODOLOGIJA

Blokų grandinės technologijos energetikos įmonėse kaip tyrimo objekto pristatymas.

Išanalizavus literatūrą, buvo parengtas tyrimo logikos planas, kurio buvo laikomasi vykdant tiriamąją darbo dalį.

Tyrimo tikslingumo pagrindimas. Mokslinės literatūros analizė atskleidė (Alexander Freier, 2024, Shekh S., 2023, Anak Agung ir kt., 2022), kad „blockchain“ energetikos sektoriuje yra analizuojama tiek Europoje, tiek pasauliniu mastu. Nors yra autorių, kurie nagrinėja „blockchain“ energetikos sektoriuje, tačiau trūksta tikslių sukurtų platformų nagrinėjamų atvejų. Per paskutinius keletą metų akcentuojama, kad blokų grandinės technologijos ir jos reikšmė įmonėse kiekvienais metais auga, tačiau šios srities analizių Lietuvoje neatlikta. Dėl šios priežasties blokų grandinės technologijos energetiniame sektoriuje įgyja didesnį aktualumą ir reikalauja išskirtinio dėmesio. Pirmajam tyrimui atlikti buvo pasirinkta kokybinis tyrimas, kurios instrumentu buvo pasirinkta atvejo studijos analizė. Buvo pasirinktos trys įmonės („Powerledger“, „Acciona Energia“ ir „Ponton GmbH“), kurios naudoja blokų grandinę, kasdieninėje veikloje. Ekspertinis tyrimas – interviu pasirinktas dėl to, kad viešai prieinama informacija yra nepakankama, objektyviai įvertinti esamą situaciją, o ekspertai yra savo srities profesionalai, todėl jų vertinimai konkrečiais atvejais yra labiau pagrįsti nei išorės ekspertų.

Tyrimo tikslas – ištirti blokų grandinės taikymo ypatumus ir galimybes, pranašumus ir trūkumus energetikos sektoriuje. Pateikti kibernetinio saugumo galimybes ir iššūkius taikant blokų grandinę.

Tyrimo organizavimo metodika. Teorijai empiriškai patikrinti (Kardelis, 2002) ir teorinėms įžvalgoms pagrįsti, atliekamas kombinuotas tyrimas, taikant kokybinio ir kiekybinio tyrimo strategijas. Kokybinis tyrimas pasirinktas dėl teikiamų minimalių materialinių sąnaudų, galimybės tiriamą reiškinį nagrinėti platesniu aspektu, gauti įvairiapusę informaciją ir stebėti reiškinio vystymosi dinamiką. Kokybinio metodo strategija yra probleminės situacijos atviro, nestruktūrizuoto pobūdžio analizė, ir taikoma, siekiant tyrimą atlikti natūralioje aplinkoje, ir gauti detalų vaizdą apie tiriamą reiškinį (Tidikis, 2003). Atliekant tyrimą nėra formuluojamos hipotezės, o ieškoma naujų teiginių remiantis pirminiais šaltiniais, t.y. tyrimo eiga atvira naujoms idėjoms (angl. k. Open mind). Taip apibūdinama induktyviai grindžiamoji kokybinio tyrimo strategija, kurios metu reiškinys yra konceptualizuojamas iš naujo interpretuojant duomenis ir juos siejant su asmenine tyrėjo patirtimi (Bitinas, Rupšienė, Žydžiūnaitė, 2008). Kokybinis tyrimas įvertina tai, kad požiūriai ir praktikos skiriasi, nes nesutampa subjektyvios perspektyvos ir su jomis susiję socialiniai, biografiniai kontekstai (Flick, 2014).

Atvejo studijos analizė blokų grandinės taikymo energetiniame sektoriuje yra svarbi siekiant suprasti šios technologijos potencialą ir įvertinti naudą energetikos srityje. Kadangi atvejo analizės

tikslas yra ištirti „reiškinį jo realiame kontekste“ (Yin, 2011, p. 17). Šis metodas plačiai naudojamas verslo tyrimuose ir apima išsamią vieno atvejo analizę (Bryman & Bell, 2015).

Siekiant pateikti kaip blokų grandinė naudojama energetiniame sektoriuje pasirinktos organizacijos pavyzdį ir atskleisti su pokyčių įgyvendinimu susijusius atliekamus organizacijos veiksmus, pasirinktas atvejo studijos metodas, kaip geriausiai atspindintis vykstančius procesus organizacijos viduje neatsiejant nuo konteksto. Atvejų analizė apima su įmone susijusi informacija žiniasklaidoje ir įmonių tinklalapius, įmonių vidaus dokumentai (WhitePapers), šią informaciją interpretuojant remiantis mokslinės literatūros ir juridinių dokumentų analize.

Kokybinio interviu pagrindas – atviri klausimai, į juos tikimasi gauti kiek įmanoma platesnius, išsamesnius, atviresnius atsakymus, suformuluotus ir pateiktus paties tyrimo dalyvio, atspindinčius jo perspektyvą.

Ekspertinis tyrimas. Taikant ekspertinio tyrimo metodą atliekami šie žingsniai: 1. Sudaromas ekspertinio tyrimo planas; 2. Parenkamas ekspertų apklausos metodas ir parengiami būtini dokumentai; 3. Atrenkami ekspertai; 4. Atliekama ekspertinio tyrimo procedūra; 5. Analizuojami ekspertinio tyrimo duomenys, pašalinamos klaidos ir prieštaravimai; 6. Interpretuojami rezultatai; 7. Pateikiami oficialūs ekspertinio tyrimo rezultatai ir išvados. Rinkos tyrimuose taikomi ir kiekybiniai, ir kokybiniai tyrimo metodai, taip pat jų deriniai. Šie tyrimo metodai dažnai papildo vienas kitą (T. Belevičienė ir S. Jonušauskas, 2011). Ekspertais pasirinkti trys kibernetinio saugumo specialistai ir du IT technologijų specialistai, kurių funkcijos tiesiogiai susijusios su informatika, saugumu ir „blockchain“. Pagrindžiant pusiau struktūrizuoto interviu metodo taikomumą, šis metodas pasirinktas tikslingai, siekiant detaliau paaiškinti blokų grandinės pritaikymą praktiškai kibernetiniame saugume.

Kiekybinis antrinių statistinių duomenų analizės metodas. Nagrinėta literatūra ir duomenys pagrindė faktą, kad blokų grandinė plačiai naudojama technologija ir kiekiai kiekvienais metais auga.

Tyrimo imtis. Taikyta netikimybinė tikslinė atranka. Tikslingai pasirinktos įmonės: „Powerledger“, „Acciona Energia“ ir „Ponton GmbH“.

Pusiau struktūrizuotam interviu tyrimo imties sudarymo būdai: kritinė atranka: Imties vienetai buvo atrenkami pagal tyrėjo nustatytą kriterijų(-us). Kritinė atranka taikoma tada, kai imties vienetai iš populiacijos atrenkami laikantis tyrėjo nustatytų kriterijų. Šiuo atveju buvo išskirta keli kriterijai:

1. Turėtų išsilavinimą kompiuterių moksle arba kibernetiniame saugume;
2. Turėtų darbo patirties mažiausiai 5 metus;
3. Turėtų patirties su saugumu internete;
4. Išmanytų blokų grandinę (šis kriterijus koreguotinas, nes pradėjus ieškoti ekspertų, buvo išsiaiškinta, kad mažai yra specialistų išmanančių „blockchain“). Tyrimui atrenkami visi minėtus tris kriterijus atitinkantys atvejai. Kritinės atrankos būdas yra labai veiksmingas, taip surenkami kokybiški duomenys.

Tyrimo planas. Siekiant užtikrinti sėkmingą tyrimo įgyvendinimą, sudarytas detalus tyrimo planas, kuriame pateikiamas tyrėjo veiksmų ir veiklos eiliškumas, padėjęs efektyviai organizuoti tyrimo procesą bet pagrįsti tyrimą metodologiškai.

Tyrimo dizainą sudaro trys pagrindiniai etapai:

Pirmasis etapas – atliekama atvejų analizė siekiant pateikti kaip blokų grandinė naudojama energetiniame sektoriuje pasirinktos organizacijos pavyzdį ir atskleisti su pokyčių įgyvendinimu susijusius atliekamus organizacijos veiksmus, pasirinktas atvejo studijos metodas, kaip geriausiai atspindintis vykstančius procesus organizacijos viduje neatsiejant nuo konteksto. Atliekama kokybinė įmonių turinio analizė, renkama įvairiausi duomenys apie įmones ir jų veiklą. Taip pat, taikyta ir kiekybinė antrinių statistinių duomenų analizė.

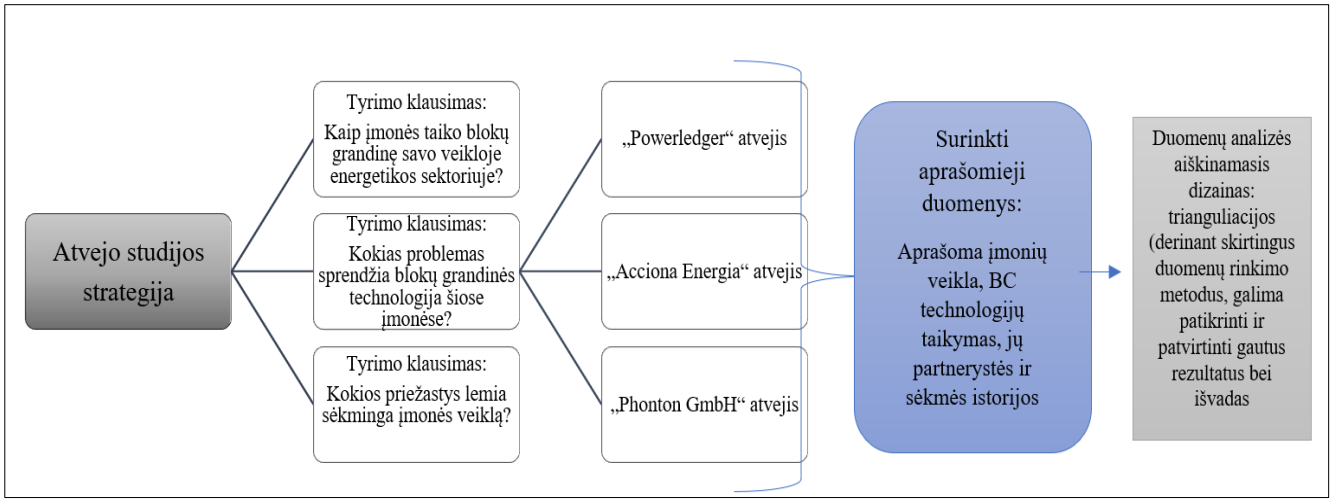
Antrame etape pusiau struktūrizuotas ekspertų interviu. Gauti duomenys yra analizuojami naudojant, kokybinio turinio (anglų k. Content) metodą.

Trečiame etape empiriškai tikrinami gauti duomenys, analizuojami gauti rezultatai.

4. BLOKŲ GRANDINĖS TECHNOLOGIJOS IR KIBERNETINIO SAUGUMO, ENERGETINIAME SEKTORIUJE ANALIZĖ

4.1 Blokų grandinės technologija energetikos įmonėse atvejų analizė, taikymo ypatumai ir iššūkiai

Atvejo analizė yra naudinga magistriniame darbe, nes ji leidžia integruoti teorines žinias su praktiniais pavyzdžiais, gilintis į konkrečią temą ir suteikti praktinių rekomendacijų verslo veiklai tobulinti.



10 pav. Atvejo studijos strategija

Atvejo studijos analizė blokų grandinės taikymo energetiniame sektoriuje yra svarbi siekiant suprasti šios technologijos potencialą ir įvertinti naudą energetikos srityje.

Pasirinkau atlikti atvejų analizes, kad atsakyčiau į tyrimo klausimus iškilusius nagrinėjant mokslinę literatūrą:

1. Kaip įmonės taiko blokų grandinę savo veikloje energetikos sektoriuje?
2. Kokias problemas sprendžia blokų grandinės technologijos šiose įmonėse?
3. Kokios priežastys lemia sėkminga įmonės veiklą , naudojant „Blockchain“?

4.1.1 „Powerledger“

7 lentelė. „Powerledger“ pagrindinė informacija

Interneto svetainė	https://powerledger.io
Industrija	Programinės įrangos kūrimas
Įmonės dydis	68 darbuotojų
Būstinė	Šveicarija ir Australija
Tipas	Privati
Įkurta	2016 m
Specialybės	Blockchain, energija, technologijos, saulės energija, EV, SaaS ir programinė įranga
Pajamos	$32 mln.

„Powerledger“ yra sparčiai augantis technologijų startuolis, kuris sukūrė pirmąją pasaulyje „blockchain“ energetikos ir aplinkosaugos prekių prekybos platformą, kad energijos rinkos būtų efektyvesnės. Sulaukė pasaulinio pripažinimo už savo technologijas, įskaitant 2018 m. laimėjimą sero Richardo Bransono tarptautiniame „Extreme Tech Challenge“ renginyje. „Powerledger“ patentuota programinė įranga šiuo metu naudojama keliose šalyse, įskaitant Australiją, Tailandą, Indiją, Japoniją ir JAV. Australijos bendrovė „PowerLedger“ pristatė galimybę pasirinkti tinkamą atsinaujinančios energijos šaltinį pagal savo pageidavimus. Jie naudoja „blockchain“ technologiją , kad padėtų patvirtinti duomenis vartotojams.

Taigi, dabar klientai gali pasirinkti, kokio energijos šaltinio nori, pavyzdžiui, vėjo, saulės ar vandens ir atitinkamai pirkti iš tiekimo. Naudojant blokų grandines supaprastintas patikrinimas, kilmė ir sekimas. Tokiu būdu galima sumažinti klientų laiką naudojant „PowerLedger“ platformą, kurioje klientai gali greitai patikrinti šaltinį ir pakeisti tiekimą iš tos pačios platformos pagal savo pageidavimus.

2023 m. liepos 31 d. „Powerledger“ pristatė savo viešą „blockchain“, pagrįstą „Solana“ kodu, tačiau pritaikydama „Powerledger“ energijos rinkoms ir kitoms paskirstytoms energijos programoms. Naujoji „Powerledger“ blokų grandinė siūlo mažų mokesčių ir didelio pralaidumo derinį, reikalingą

aukšto dažnio mažiems sandoriams paskirstytose energijos rinkose apdoroti, pavyzdžiui, tarpusavio prekybai energija ir sekimui (Powerledger Lightpaper, 2023).

Ką siūlo „Powerledger“:

Procesus. „Powerledger“ blokų grandinė siūlo trumpesnius nei sekundės patvirtinimo laikus ir gali apdoroti dešimtis tūkstančių operacijų per sekundę, užtikrindama sklandžią jūsų decentralizuotų programų (DApps) vartotojo patirtį.

Mažas operacijų sąnaudas.

Lengvesnis mastelio keitimas. Skirtingai nuo perpildytų tinklų, „Powerledger“ architektūra leidžia decentralizuotoms programoms (DApps) lengvai keisti mastelį, kad būtų patenkinti milijonai vartotojų, nepakenkiant našumui.

Į kūrėjus orientuoti įrankiai. „Powerledger Blockchain“ suteiks gausų kūrėjo įrankių, bibliotekų ir API integracijų rinkinį, kad paspartintų jūsų decentralizuotų programų (DApp) kūrimo kelionę.

Blockchain decentralizuotoms ir paskirstytoms energijos rinkoms. „Powerledger“ viešoji blokų grandinė leidžia kurti ir išplėsti energetikos projektus visame pasaulyje, apdorojant daugiau nei 50 000 operacijų per sekundę. Ši keičiamo dydžio technologija yra greita, skaidri ir saugi. „Powerledger“ „blockchain“ technologija palengvina saugią prekybą ir sumažina atsiskaitymo riziką, taip pat suteikia nekintamą ir patikrinamą audito seką.

„Powerledger Energy Blockchain“

„Powerledger“ naudoja „blockchain“ technologiją, kad sukurtų decentralizuotą, saugią ir skaidrią platformą. Be to, „Powerledger“ grandinė pradėjo veikti 2023 m. ir dabar palaiko platformos funkcijas – „xGrod“, „uGrid“, „Vision“, „PPA Vision“ ir „TraceX“.

Sparčiai tobulėjant „blockchain“ technologijai, „Powerledger“ savo viduje eksperimentuoja su įvairiomis pažangiomis pirmojo sluoksnio blokų grandinėmis. Kaip buvo numatyta originaliame dokumente, „Powerledger“ perėjo iš konsorciumo „Ethereum“ pagrindu veikiančios blokų grandinės į viešąją „blockchain“, skirtą energijos ir aplinkosaugos atributų prekybos programoms. 2023 m. liepos 31 d. „Powerledger“ pristatė savo viešą blokų grandinę, pagrįstą Solana kodu, tačiau pritaikydama „Powerledger“ energijos rinkoms ir kitoms paskirstytoms energijos programoms. Naujoji „Powerledger“ blokų grandinė siūlo mažų mokesčių ir didelio pralaidumo derinį, reikalingą aukšto dažnio „mikro“ sandoriams paskirstytose energijos rinkose apdoroti, pavyzdžiui, tarpusavio prekybai energija ir sekimui. „Powerledger Energy Blockchain“ yra pritaikyta atvira Solana blokų grandinė. „Solana“ dizainas yra greitesnis ir mažiau energijos reikalaujantis, nei esamos darbo patikrinimo blokų grandinės, nes jame naudojami „Proof-of-History“ ir „Proof-of-Stake“ (PoS) konsensuso mechanizmai. Solana PoS dizainas reiškia, kad „Powerledger“ turi pakviesti tikrintojus ir dalyvauti gali tik tie, kuriuos patvirtina „Powerledger“. Taip pat atsižvelgiame į kiekvieno tikrintojo naudojamos energijos kilmę, įskaitant atsinaujinančius energijos šaltinius. Dėl statymo patvirtinimo ir istorijos patvirtinimo protokolų

efektyvumo, leidžiančio užtikrinti didelį operacijų pralaidumą, „Powerledger“ blokų grandinė, palyginti su kitais pirmojo sluoksnio protokolais, žymiai pagerino energijos vartojimo efektyvumą kiekvienos operacijos pagrindu. Žvelgiant iš techninės perspektyvos, veiksmingo vieno bloko grandinės sluoksnio pasirinkimas buvo palankesnis dėl jo suderinamumo išlaikymo, suderinamumo su kitomis tos pačios grandinės programomis (Powerledger Whitepapers, 2023).

Nuo platformos perėjimo prie operacijų mokesčiais pagrįsto modelio, POWR yra vienintelė vietinė kriptovaliuta, likusi „Powerledger“ grandinėje. Tačiau, kadangi jis išleistas kaip ERC-20 prieigos raktas „Ethereum“ blokų grandinėje, POWR pirmiausia turi būti sujungtas iš „Ethereum“ į „Powerledger“, kad jį būtų galima naudoti. POWR naudojamas apmokėti operacijų mokesčius „Powerledger Energy Blockchain“. Tiek 1 lygmens blokų grandinės mokesčiai, tiek programėlių operatorių nustatyti konkrečios programos mokesčiai yra mokami POWR. Žetonas taip pat gali būti naudojamas statant. POWR turėtojai gali deleguoti savo žetonus kruopščiai atrinktiems „Powerledger“ grandinės tikrintojams ir uždirbti dalį jų pasirinkto delegato sukaupto atlygio. Bendra „POWR“ pasiūla yra 1 milijardas, o cirkuliuojanti atsarga šiuo metu siekia beveik 430 milijonų žetonų. Žetonui nenurodytas joks tiekimo apribojimas.

„Powerledger“ viešoji blokų grandinė gali pasigirti dideliu mastelio keitimu, galinti apdoroti dešimtis tūkstančių energijos operacijų per sekundę, todėl ji idealiai tinka valdyti tarpusavio sandorius didelėse energijos bendruomenėse.

Šį sausį 2024 m. Indijoje Karnatakos elektros reguliavimo komisija paskelbė viešai komentuojamo reglamento projektą, leidžiantį prekiauti energija, naudojant „blockchain“ technologiją. Įvedus šias taisykles, Karnataka taps trečiąja Indijos valstija po Utar Pradešo ir Delio, kurioje bus leidžiama prekyba elektros energija. Šios taisyklės yra pagrindinis žingsnis link decentralizuotos energetikos ateities, paremtos blokų grandinės technologija. „Blockchain“ ruošiasi tapti gyvybiškai svarbiu komponentu, skatinančiu perėjimą prie decentralizuotos energijos gamybos ir vartojimo.

Trečiosios kartos blokų grandinės galia.

Kadangi tvarumas tampa svarbia pasauline tema, ankstyvosios blokų grandinių kartos, kuriose sandoriai taiko didelius operacijų mokesčius ir lėtesnį patvirtinimo laiką, dažnai kritikuojamos dėl neveiksmingumo ir labai reikalingo mastelio trūkumo. Be to, „darbo įrodymo“ konsensuso mechanizmas, palaikantis ankstyvąsias „blockchain“ kartas, sunaudoja daug daugiau energijos. Trečiosios kartos blokų grandinės, tokios kaip **„Solana“** ir **„Powerledger“,** siūlo laimėjimus, nes jie gali atlikti dešimtis tūkstančių operacijų, palyginti su ankstesnių kartų blokų grandinėmis, už daug mažiau energijos ir vienos operacijos sąnaudų. „Powerledger“ viešoji blokų grandinė, pagrįsta Solana projektu, yra atviras tinklas su statymo įrodymo ir istorijos įrodymo konsensuso mechanizmu, pasižymintis itin mažais sandorių mokesčiais, dideliu energijos vartojimo efektyvumu. Galimybė

apdoroti dešimtis tūkstančių operacijų per sekundę, todėl ji tampa pagrindine technologija, palaikančia įmonės platformą.

Powerledger blokų grandinės taikymas lygiaverčių (P2P) energijos prekyboje.

Sandorių įrašų tvarkymas siekiant skaidrumo. Dėl decentralizuoto tarpusavio prekybos energija pobūdžio, vis svarbiau užtikrinti, kad įrašai būtų tvarkomi viešu ir nekintamu būdu. Kiekviena operacija, palengvinta naudojant Powerledger sprendimą, įrašoma į blokų grandinę. Kiekviename įraše yra „blockchain“ operacijos ID, pirkėjo viešosios piniginės ID, sandorio suma, kaina už kWh ir galiausiai visa sandorio suma. Tai reiškia, kad visos suinteresuotosios šalys gali peržiūrėti kiekvieną sandorį būdamos užtikrintos, kad įrašai yra nepakeisti ir nekintami, o tai sukuria pasitikėjimą p2p energijos prekybos rinkomis**.**

Patobulintas PPA matomumas naudojant išmaniąsias sutartis.

„Powerledger“ blokų grandinė leidžia vartotojams siųsti tinkintus energijos pirkimo sutarties (PPA) pasiūlymus vieni kitiems. Šie pritaikymai gali būti pagrįsti pirkėju, pardavėju, kaina ir trukme. „Blockchain“ užtikrina, kad šios sutartys būtų registruojamos nekeičiamai, todėl jas lengviau sekti ir sukurti geresnį EEPS matomumą energijos bendruomenėse.

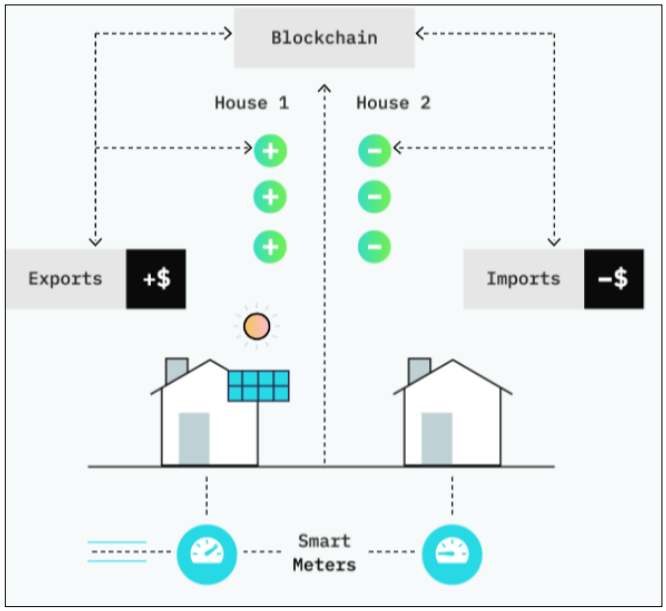
Dinamiškas kainų fiksavimas ir duomenų tikslumas. Naudodami įmonės energijos prekybos platformą, vartotojai gali patys nustatyti pirkimo ir pardavimo kainas tarpusavio prekybai savo bendruomenėje. Šie kainų nustatymai įrašomi blokų grandinėje kartu su kiekvieno vartotojo piniginės ID. Tai reiškia, kad naudotojo sukelti kainų pokyčiai tiksliai fiksuojami operacijų įrašuose, užtikrinant, kad duomenys būtų be neatitikimų.

„xGrid“

„xGrid“ leidžia mažmeninės elektros energijos pardavėjų klientams prekiauti saulės energija visame tinkle. „xGrid“ suteikia galimybę namų ūkiams ir įmonėms parduoti energiją, pagamintą iš saulės baterijų, kitiems energijos vartotojams, prijungtiems prie to paties elektros tinklo. Tai galima padaryti su klientais, turinčiais tą patį elektros energijos tiekimą arba per skirtingas komunalines paslaugas. „Blockchain“ sistema visa tai stebės. Sistemos esmė yra energijos prekybos variklis, leidžiantis mažmenininkams, komercinėms įmonėms ar elektros energijos įmonėms įvairiais būdais konfigūruoti prekyvietę.

„uGrid“

„uGrid“ leidžia sekti energiją ir prekiauti įterptiniuose tinkluose ir mikrotinkluose. Jis gali būti naudojamas prekybos centruose, daugiabučių kompleksuose, biurų pastatuose ir senelių namuose, kuriuose yra individualus arba bendrai valdomas energetinis turtas. Jei gyvenate daugiabučiame name arba valdote ir kuriate nekilnojamąjį turtą pragyvenimui, gali būti sudėtinga užtikrinti, kad visi būtų patenkinti ir sistema sugebės viską teisingai apskaičiuoti. „Powerledger“ platforma, tai atlieka paprastai ir skaidriai, naudodama blokų grandinę. 11 paveiksle pavaizduota kaip veikia „uGrid“.



Šaltinis: PowerLedger

11 pav. „uGrid“

Platforma leidžia gyventojams tarpusavyje prekiauti saulės energija ir užsidirbti pinigų savo stogo plote. Tai reiškia, kad gyventojai gali pirkti iš artimiausių žmonių, išsaugodami investicijas, pelną ir atsinaujinančių išteklių naudą bendruomenėje.

„Vision“

Energijos vartotojai vis labiau domisi tam tikros švarios energijos, pvz., saulės, vėjo ar žaliojo vandenilio, naudojimu. Tai reiškia, kad skaidrumas yra labai svarbus ir taip pat būtina patikrinti žaliosios energijos kilmę, kai ji juda tinkle. „Powerledger's Vision“ platformos funkcija leidžia galutiniams vartotojams pasirinkti energijos derinį pagal suvartojamos energijos tipą, šaltinį, vietą ir kiekį. Vizija įrodo energijos kilmę ir leidžia atsekamumą, ypač prekiaujant atsinaujinančia energija tarp namų ūkių ar įmonių. „Vision“ yra platforma, leidžianti vartotojams pasirinkti saulės, vėjo, hidroenergiją ar biomasę. Be to „Vision“ užtikrina reikiamą matomumą ir atsekamumą, kad būtų galima patikrinti ar žalias vandenilis, turi atsinaujinančių energijos šaltinių. Būdama nulinės anglies dioksido sertifikavimo sistemos įkūrėja, „Powerledger“ yra įsipareigojusi teikti tvirtą ir tarptautiniu mastu pripažintą kilmės schemą.

„TraceX“

„TraceX“ yra skaitmeninė rinka, kurioje naudojama „blockchain“ technologija, kad būtų galima efektyviai tvarkyti prekybą energijos atributų sertifikatais (EAC), tokiais kaip atsinaujinančios energijos sertifikatai (REC), kilmės garantijos (GO), anglies dioksido kreditai ir kiti aplinkosaugos instrumentai. Įmonė yra „EnergyTag“ narė – pramonės vadovaujama iniciatyva, kuria siekiama apibrėžti ir sukurti valandinių elektros energijos sertifikatų rinką, veikiančią pagal esamas sertifikatų schemas. „Powerledger“ platforma gali naudotis gamintojai, kurie turi sertifikatus parduoti arba komunalinės paslaugos ir organizacijos, kurios nori pirkti sertifikatus, kad įvykdytų reguliavimo

įsipareigojimus arba savanoriškus tvarumo tikslus. Brokeriams ir prekybininkams „TraceX“ yra labai efektyvus būdas valdyti savo klientų atsinaujinančios energijos sertifikavimo poreikius. Sumažina atsiskaitymo riziką. Išvengiant dvigubo naudojimo, REC yra apsunkinami pradiniame registre, kai jie importuojami į „TraceX“. Įrašoma „blockchain“ knygoje, suteikiant tvirtą audito seką.

Įmonė išskiria 8 lentelėje šiuos privalumus blokų grandinės naudojant kasdieninėje veikloje.

8 lentelė. Blokų grandinės technologijos privalumai

Decentralizacija	• „Blockchain“ palengvina tarpusavio prekybą energija, nereikalaujant centralizuotų tarpininkų, o tai leidžia vartotojams ir gamintojams tiesiogiai sudaryti sandorius vieni su kitais. • Decentralizacija sumažina priklausomybę nuo centralizuotų komunalinių paslaugų ir suteikia asmenims galimybę dalyvauti energijos rinkoje, todėl padidėja energetinė nepriklausomybė ir atsparumas.
Didesnis tikslumas	Naudojant blokų grandinę, išmaniosios sutartys gali būti naudojamos automatizuoti energijos prekybos ir atsiskaitymo procesus, sumažinant rankinio įsikišimo poreikį ir didinant efektyvumą.
Mažesnė klaidų ir sukčiavimo rizika	**Kibernetinio saugumo** grėsmės šiandienos tarpusavyje sujungtose energijos sistemose yra didelis iššūkis. „Blockchain“ decentralizuotas, apsaugotas nuo klastojimo operacijų įrašas gali sumažinti saugumo pažeidimų ir sukčiavimo riziką. „Blockchain“ paskirstyta architektūra užtikrina, kad operacijų įrašai būtų atkartojami ir sinchronizuojami keliuose mazguose, todėl piktavaliams veikėjams labai sunku keisti ar manipuliuoti duomenimis. Tai suteikia didesnį saugumą visoms dalyvaujančioms šalims,

	sumažina finansinių ir reputacijos praradimų riziką.
Mažesnės veiklos sąnaudos	Supaprastinant energijos sandorius ir sumažinant administracines išlaidas, „blockchain“ valdoma P2P prekyba padidina efektyvumą ir sumažina energijos tiekėjų ir vartotojų veiklos sąnaudas.
Mastelio keitimas didelėms energijos operacijoms	„Powerledger“ trečios kartos blokų grandinė pasižymi dideliu mastelio keitimu ir gali tvarkyti dešimtis tūkstančių energijos operacijų per sekundę, todėl ji tinka didelių energijos bendruomenių P2P sandoriams.
Detalus skaitiklių duomenų integravimas	„Powerledger Blockchain“ kiekvienam vartotojui integruoja išsamią skaitiklio informaciją. Tai apima esminę informaciją, tokią kaip skaitiklio serijos numeris, tikslios vietos koordinatės (platuma ir ilguma), turto tipas, generavimo tipas (kuro tipas) ir generavimo kategorija. Integravus šiuos su skaitikliu susijusius duomenis su operacijų įrašais, vartotojai gali gauti išsamų savo skaitiklio turto duomenų vaizdą, todėl lengviau suprasti ir analizuoti blokų grandinėje įrašytas operacijas. Šis išsamus vaizdas padeda patikrinti sandorius, todėl jie tinkami energetiniam auditui.

Šaltinis: Powerledger

Išvada

Sparčiai augant paklausai atsinaujinantiems ištekliams, energetikos kraštovaizdis pereina nuo centralizuoto prie paskirstyto. „Powerledger“ blokų grandinėmis paremta energijos prekybos platforma leidžia energijos bendruomenėms pasiekti didesnį skaidrumą ir atskaitomybę vykdant tarpusavio prekybą energija. Naudodamiesi išsamiais operacijų įrašais ir išmaniųjų sutarčių funkcijomis, dalyviai

gali sekti ir patikrinti kiekvieną savo energijos sandorių aspektą, taip skatindami pasitikėjimą rinka. Įmonės direktorė Dr. Green teigia, kad jos įmonė naudoja blokų grandinę, kad geriau apsisaugotų nuo kibernetinių atakų.

Apibendrinant atliktą atvejo analizę, pavyko atsakyti į visus iškeltus tyrimo klausimus pradžioje. „TraceX“ leidžia stebėti energijos kilmę ir kelionę nuo gamintojo iki vartotojo, „uGrid“ padeda valdyti mikrogrupių energijos mainus, o „Vision“ suteikia išsamią informaciją apie energijos vartojimą ir efektyvumą. Šios programos padeda optimizuoti energijos tiekimą, mažinti išmetamųjų teršalų kiekį bei skatinti tvarumą. „Powerledger“ pavyko pasiekti didesnį tikslumą, mažesnę klaidų ir sukčiavimo riziką, mažesnes veiklos sąnaudas, įveikti mastelio keitimą. Pasiteisinę konsensuso modeliai : „Proof-of-History“ ir „Proof-of-Stake“.

4.1.2 „Acciona Energía “

9 lentelė. „Corporación Acciona Energías Renovables, SA“ pagrindinė informacija

Interneto svetainė	https://www.acciona-energia.com/
Industrija	Energija ir komunalinės paslaugos
Įmonės dydis	10 001+ darbuotojas
Būstinė	Alkobendas, Madrido bendruomenė
Tipas	Privati
Įkurta	2001 m.
Specialybės	Atsinaujinantys energijos šaltiniai, inžinerija, vėjo energija, fotovoltinė energija, klimato kaita, tvarumas, inovacijos, viešieji darbai, koncesijos, nekilnojamasis turtas, vandens valymas, statyba, cirkuliacijos inžinerija, grandinės inžinerija,
Pajamos	€524 mln.

„Acciona“ yra Ispanijos įmonė, **visame pasaulyje veikianti 65 šalyse, penkiuose žemynuose**. **„Acciona, SA“** yra Ispanijos daugianacionalinis konglomeratas, skirtas infrastruktūros (statybos, vandens, pramonės ir paslaugų) ir atsinaujinančios energijos plėtrai bei valdymui. Bendrovė per dukterinę įmonę „Acciona Energía“ per metus pagamina 21 teravatvalandę atsinaujinančios elektros energijos. Įmonė specializuojasi saulės, vėjo ir hidroelektrinių jėgainių veikloje.

Įmonė buvo įkurta 1997 m., susijungus *Entrecanales y Tavora* ir *Cubiertas y MZOV*. Įmonės būstinė yra Alkobendo mieste, Madrido bendruomenėje, Ispanijoje. Įmonės JAV pagrindinė būstinė yra Čikagoje, Ilinojaus valstijoje.

„Acciona Energía“ siūlo daug paslaugų ir yra viena iš rimčiausių tirtų mano įmonių. Nuo 2015 m. ji pirmauja „Ekologiškiausių pasaulio komunalinių paslaugų“ reitinge, kurį paskelbė „Energy Intelligence“.

„ACCIONA“ sukūrė blokų grandinėmis pagrįstą registrą, kad apsaugotų savo pačių sukurtų energijos optimizavimo platformų intelektinę nuosavybę. Per šią sistemą įmonė gali apsaugoti visus savo inovatyvius technologinius sprendimus, suteikiančius konkurencinius pranašumus valdant atsinaujinančius išteklius.

Įmonė yra blokų grandinės naudojimo energetikos srityje pradininkė. Bendrovė naudoja „blockchain“ technologiją, kad patvirtintų atsinaujinančios energijos kilmę ir saugojimo procesus. Su šia nauja programa „ACCIONA“ garantuoja visų savo viduje sukurtų platformų nuosavybę, įskaitant ir šias 10 lentelėje pateiktas platformas.

10 lentelė. Platformos sukurtos blokų grandinės pagrindu

ATHERMIS®	Termografinio tikrinimo programinė įranga, leidžianti aptikti ir analizuoti fotovoltinius modulius didelėse fotovoltinėse gamyklose.
ADOSA STORAGE®	Atsinaujinančių išteklių energijos gamybos įrenginių saugojimo sistemų analizės ir modeliavimo įrankis.
GREENCHAIN®	„Blockchain“ pagrindu sukurta platforma, užtikrinanti atsinaujinančių energijos šaltinių atsekamumą klientams realiu laiku.
STORE ⁻ CHAIN®	„Blockchain“ sistema, kuri tikrina energijos atsekamumą ir realiu laiku atlieka saugojimo procesų stebėjimą įmonės atsinaujinančios energijos gamybos jėgainėse.
WINDBRAIN®	Programinė įranga, galinti aptikti vėjo turbinų veikimo anomalijas (diagnozuoti), kuriant prevencinės priežiūros metodus ir O&M optimizavimo metodus.

GreenH2chain	Leidžia realiuoju laiku sekti ir tikrinti vandenilio gamybą, užtikrinti, kad būtų laikomasi aplinkosaugos standartų, o suinteresuotosioms šalims suteikiamas patikimas informacijos šaltinis.

Šaltinis: Acciona SA

„Acciona Energía“ inovacijų direktorius Belénas Linaresas sakė: „Atsinaujinančios energijos kilmės atsekimas yra nuolat didėjanti paklausa, susijusi su žaliosios energijos įmonių sutarčių rinkos augimu, o „blockchain“ technologija gali labai palengvinti šią paslaugą klientams bet kurioje šalies dalyje.

Pagal „Storechain“ projektą „Acciona Energía“ panaudojo „blockchain“ technologiją, kad atsektų energijos kaupimą baterijose iš dviejų atsinaujinančių energijos šaltinių Ispanijoje – vėjo jėgainės Barasoaine ir Tudela fotovoltinės gamyklos (Powertechnologie 2018).

„ACCIONA“ naudoja blokų grandinę savo energijos valdymo programinei įrangai apsaugoti. Bendrovė saugo visą intelektinę nuosavybę savo pačios sukurta optimizavimo programine įranga, kuri yra konkurencinis pranašumas veiklos efektyvumo srityje.

Įmonė pristatė pirmąjį energetikos sektoriaus sertifikatą, garantuojantį šaltinio kodų apsaugą įmonės viduje. Tai pasiekiama naudojant unikalius raidinius ir skaitmeninius (maišos) kodus, kurie apima patikimą datos registraciją ir perduodami patikimoms trečiosioms šalims per blokų grandinę.

Šis sprendimas atlieka labai reikalingą vaidmenį programinės įrangos apsaugai, kuri pagal Ispanijos įstatymus paprastai nėra patentuojama. Be to, norint, kad programinė įranga būtų visiškai apsaugota, būtina paskelbti pirminį kodą, kad būtų įrodyta nuosavybės teisė į intelektinės nuosavybės registrą, todėl jis būtų prieinamas trečiosioms šalims.

Naujoji „ACCIONA“ blokų grandinės sistema buvo teisiškai pripažinta ir patvirtinta, todėl įmonei visiškai priklauso jos sukurta programinė įranga. Tai prisideda prie grupės inovacijų ir skaitmeninės transformacijos procesų stiprinimo.

KAIP TAI VEIKIA pavaizduota 12 paveiksle. Pirma, iš dokumento, kuriame yra „ACCIONA“ programinė įranga, sugeneruojamas unikalus raidinis ir skaitmeninis kodas (hash), atitinkantis skaitmeninį pirštų atspaudą. Tada ši maiša su sukūrimo data ir laiku išsaugoma registro platformoje ir siunčiama į tris skirtingas blokų grandinės platformas, kurios akredituoja ir sertifikuoja procesą. Originalus šaltinio kodo dokumentas yra saugomas ACCIONA ir yra patikimai susietas su sugeneruota maiša (Acciona, 2020).

Šaltinis: Acciona, 2020.

12 pav. Programinės įrangos veikimo principas

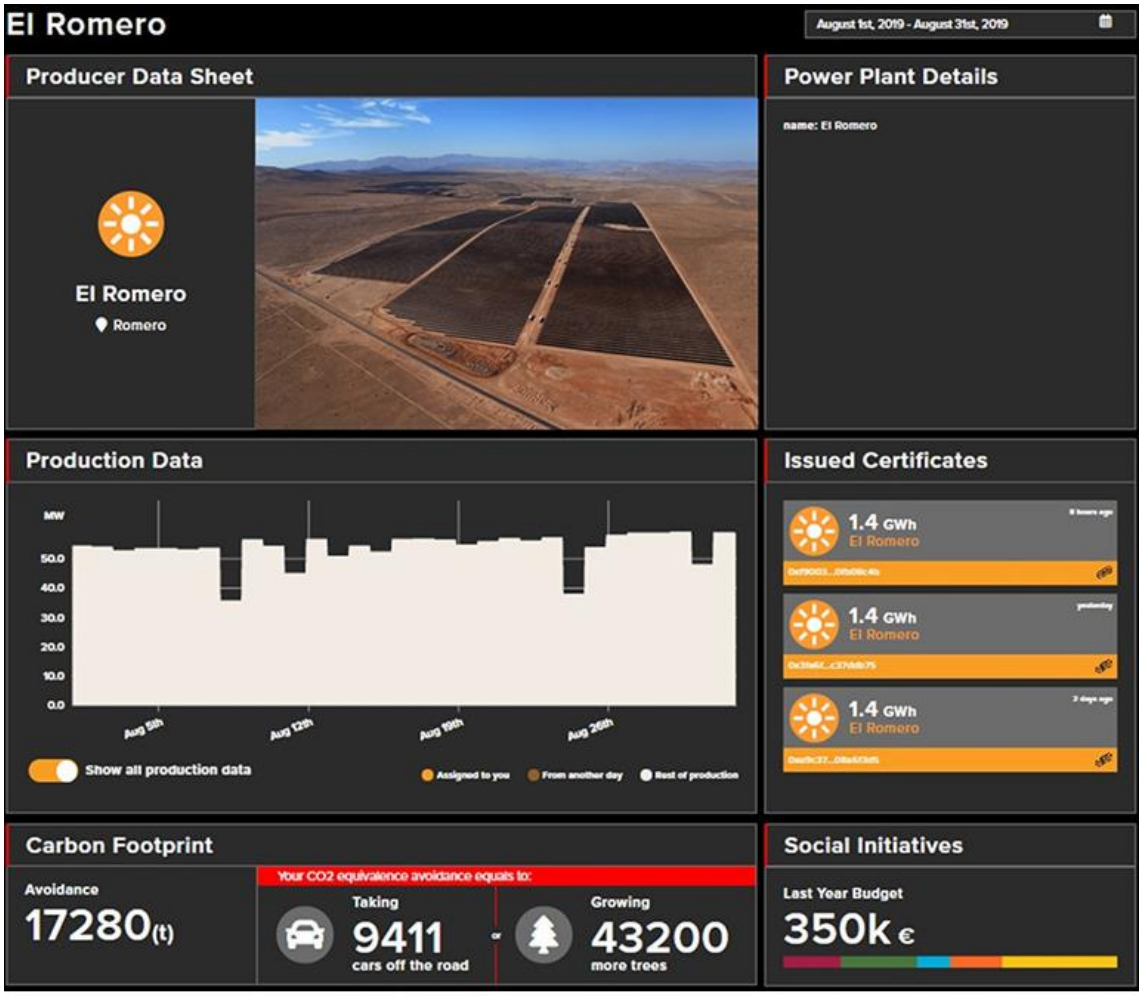
„Greenchain“

Atsinaujinančios energijos atsekamumas garantuojamas „Blockchain“.

„FlexiDAO“ (yra programinė įranga, kuri automatizuoja energijos duomenų apdorojimą ir mainus, pirmą kartą derinant atsekamumą ir skaidrumą, kurį įgalina blokų grandinė, su BDAR suderinamu duomenų privatumu) anksčiau dirbo su „Acciona Energía“, kad sukurtų komercinę blokų grandinės demonstraciją, kuri parodytų atsinaujinančios energijos gamybos iš penkių vėjo ir hidroelektrinių visoje Ispanijoje, tiekiančių energiją keturiems portugalų verslo klientams, atsekamumą.

Technologijai demonstruoti buvo panaudota specialiai energetikos sektoriui sukurta „Energy Web“ grandinės platforma. „Energy Web Chain“ (EW grandinė) yra atvirojo kodo viešoji „Proof-of-Authority“ blokų grandinė, sukurta naudojant „Ethereum“ blokų grandinės technologiją. Tai pagrindinis EW-DOS pasitikėjimo ir atkaklumo sluoksnis. Visi konsensuso mechanizmai turi trūkumų ir privalumų ir yra parenkami atsižvelgiant į blokų grandinės, kurią jie aptarnaus, paskirtį ir naudojimo atvejį. Sutarimas dėl įgaliojimų patvirtinimo. Įgaliojimo patvirtinimo (PoA) konsensuso mechanizmas turi apibrėžtą veikėjų rinkinį, kuris patvirtina operacijas ir skleidžia naujus blokus į grandinę. Užuot konkuruoję ar žaidę dėl galimybės pridėti blokų, jie paeiliui kuria naujus blokus apvaliu būdu. Šie veikėjai vadinami tikrintojais.

„Energy Web“ tikrintojai dalyvauja paleisdami visus blokų grandinės mazgus naudodami „OpenEthereum“ kliento programinę įrangą. Išmaniosiose sutartyse, vadinamose „Validator-Set“ sutartimis yra galimybė pridėti arba pašalinti tikrintojus. Kiekvienas gali paleisti visą blokų grandinės mazgą, tačiau tik adresai, įtraukti į „Validator-Set“ sutartis, gali patvirtinti operacijas ir užplombuoti blokus. „Energy Web Chain“ naudoja tam tikro tipo veiksmų planą, vadinamą „AuRa“. „AuRa Proof-of-Authority“ konsensuso mechanizmą gali naudoti blokų grandinės, kuriose veikia „OpenEthereum“ klientas. „FlexiDao“ generalinis direktorius ir vienas iš įkūrėjų Simone Accornero pridūrė: „Mes parodome, kad atsinaujinančios energijos atsekamumas dabar yra perspektyvus pasiūlymas, sukuriantis tikrą vertę vartotojui. Kartu su „Acciona“ norime būti pionieriais, rodančiais, kad ši „blockchain“ sistema yra komerciškai perspektyvi dideliu mastu. „Greenchain“ padės „Acciona Energía“ ir jos klientams lengvai pasiekti duomenis, tuo pačiu užtikrinant saugumą ir privatumą. “



Šaltinis: Acciona SA.

13 pav. „Greenchain“

„Greenchain“ yra komercinė platforma 13 paveiksle pavyzdys ką mato klientai, kurią sukūrė „ACCIONA“, pagrįsta „blockchain“ technologija. Tai leidžia klientams realiu laiku vizualizuoti 100% atsinaujinančią tiekiamos elektros kilmę visiškai patikimai ir saugiai. Platforma užregistruoja tikslų

momentą, kada sukuriama kiekviena kWh ir ją pagaminusią gamyklą, nurodydama klientui jos suvartojimo lygius bet kuriuo metu. Kiekvienai vartojimo vietai ji taip pat gali priskirti kilmės garantijas arba susijusius žaliuosius atributus. „Blockchain“ technologija reiškia, kad energijos atsekamumas nuo jos generavimo iki vartojimo taško gali būti atliekamas visiškai skaidriai taip pat fiksuojamas jos pagaminimo momentas. Taip užtikrinamas nekeičiamas įrašytų duomenų pobūdis ir neįmanoma atnaujinamų atributų dvigubo įrašo. **Tvarumas ir socialinė atsakomybė** „Greenchain“ suteikia klientui papildomos informacijos apie jo atsinaujinančios energijos vartojimo pranašumus tvarumo požiūriu.

- Kaip matote 13 paveiksle CO2 emisija, kurios išvengiama dėl kliento vartojimo ir energiją tiekiančios gamyklos.
- Reikšmingi atitikmenys (pasodinti medžiai, pašalintos iškastinio kuro transporto priemonės).

„Greenchain“ taip pat teikia informaciją apie bendruomenės projektus, susijusius su atsinaujinančios energijos gamybos jėgaine, susijusius su tvaraus vystymosi tikslais (SDG), nurodydama pradėtų iniciatyvų skaičių ir žmonių, kuriems juos naudos, skaičių.

„ACCIONA Energía“ pasirašė 10 metų elektros energijos pirkimo sutartį (PPA), siekdama tiekti 100 % atsinaujinančią elektros energiją „Sofidel“, vienai iš pasaulio lyderių higieniniam ir buitiniam naudojimui skirto minkštojo popieriaus gamybos rinkoje. Pagal šią sutartį „ACCIONA Energía“ tieks daugiau nei 90 GWh per metus atsinaujinančios elektros energijos iš atsinaujinančios energijos įrenginių Ispanijoje į „Sofidel“ gamyklą Buñuel (Navaroje).

Sutartis apima Ispanijos nacionalinės rinkų ir konkurencijos komisijos (CNMC) akredituotas kilmės garantijas, kurios patvirtina, kad suvartota elektros energija yra 100 % atsinaujinanti, taip pat prieiga prie „ACCIONA Energía“ „GREENCHAIN®“ atsekamumo programos, platformos, paremtos „Blockchain“ technologija, leidžianti sekti atsinaujinančios energijos kilmę realiu laiku. Naudodama šį įrankį, „Sofidel“ žinos, kuri „ACCIONA Energía“ gamykla ir koks atsinaujinantis šaltinis tiekė kiekvieną MW į jos įrenginius.

Ilgalaikė sutartis leis „Sofidel“ garantuoti elektros tiekimą konkurencinga ir stabilia kaina, išvengiant dabartinio rinkos nepastovumo. Be to, šis susitarimas patvirtina popieriaus gamintojo įsipareigojimą siekti tvarumo, kuris daugelį metų dirba įvairiomis kryptimis, siekdamas pagerinti savo procesų energijos vartojimo efektyvumą taip pat sumažinti CO2 emisiją ir plastiko naudojimą pakuotėse. „Sofidel“ išvengs daugiau nei 12 870 tonų CO2 išmetimo per metus, nes savo įrenginiuose Ispanijoje naudos 100 % žaliąją energiją.

„ACCIONA Energia“ paskelbė apie partnerystę su „IKEA“, siekdama aprūpinti elektromobilių (EV) įkrovimo taškus baldų mažmeninės prekybos Ispanijos prekybos centrams. „ACCIONA GREENCHAIN“ blokų grandinė atsektų tiekiamos energijos atsinaujinančią kilmę. Bendradarbiaujant iki 2023 m. pabaigos „ACCIONA“ turėjo įrengti 475 elektromobilių įkrovimo stoteles „IKEA“ prekybos centruose Ispanijoje, o galiausiai jų skaičių planuoja padidinti iki 567. Maždaug 30 % stočių bus

rezervuota „IKEA“ tiekėjams ir automobilių parkui. Šie įkrovimo taškai yra dvikrypčiai, o tai reiškia, kad EV baterijos taip pat gali kaupti elektros energijos perteklių ir tiekti energiją atgal į įkrovimo stotelę arba tinklą (Acciona, 2023).

Apibendrinant galima konstatuoti, „Greenchain“ naudoja blokų grandinės technologiją, kuri užtikrina duomenų saugumą ir nekeičiamumą. Tai padeda išvengti duomenų klastojimo ir sukčiavimo. „Greenchain“ užtikrina pasitikėjimą tarp šalių, nes suteikia galimybę stebėti ir patvirtinti energijos kilmę bei naudojamus išteklius, padeda vartotojams pasirinkti tvarias ir aplinkai draugiškus energijos šaltinius. „Greenchain“ naudojimas energetikos sektoriuje gali padėti efektyviau valdyti energijos tiekimą ir vartojimą bei skatinti tvarų energetikos sektoriaus augimą.

„Store ⁻ chain“

„Acciona STOre Chain“ sistema tvarko duomenis, surinktus iš vėjo ir saulės elektrinių elektros skaitiklių ir suderina pagamintą energiją su atsinaujinančios energijos sertifikatais. Klientas gali prieiti prie duomenų, saugomų blockchain platformoje pagal poreikį.

„Acciona“ tiekia „STOre-Chain“ technologiją dviem savo komunalinio masto saugykloms. Jos yra sujungtos su vėjo jėgainių parku ir saulės jėgainių parku, kurį ji eksploatuoja. Aptariamos saugyklos yra „Acciona Tudela“ saulės elektrinė ir „Barásoain“ vėjo jėgainių parkas Ispanijoje.

Netoli Tudelos esantis PV parkas yra sujungtas su 1 MW/650 kWh talpos sistema. Palyginimui, vėjo parkas turi dvi atskiras baterijas. „Acciona“ teigia, kad vienas 0,7 MW/0,7 MWh skirtas greitam reagavimui, o kitas 1 MW/ 0,39 MWh, skirtas didesniam savarankiškumui. **Skaidrumas realiu laiku** pasak bendrovės, „blockchain“ technologija veikia kaip „virtualus notaras“, pabrėždamas technologijos gebėjimą atlikti šią užduotį realiu laiku ir aukštu skaidrumo lygiu. Pranešama, kad šios funkcijos yra būtinos suinteresuotosioms šalims ir investuotojams, norintiems sukurti žaliosios energijos profilį. „Acciona“ sukūrė „STOre-Chain“, kad galėtų valdyti iš gamyklų gaunamus duomenis ir suderinti juos su atsinaujinančios energijos sertifikatais. Kadangi duomenys saugomi „blockchain“ platformoje, klientai juos gali pasiekti bet kuriuo metu (PV magazine, 2018).

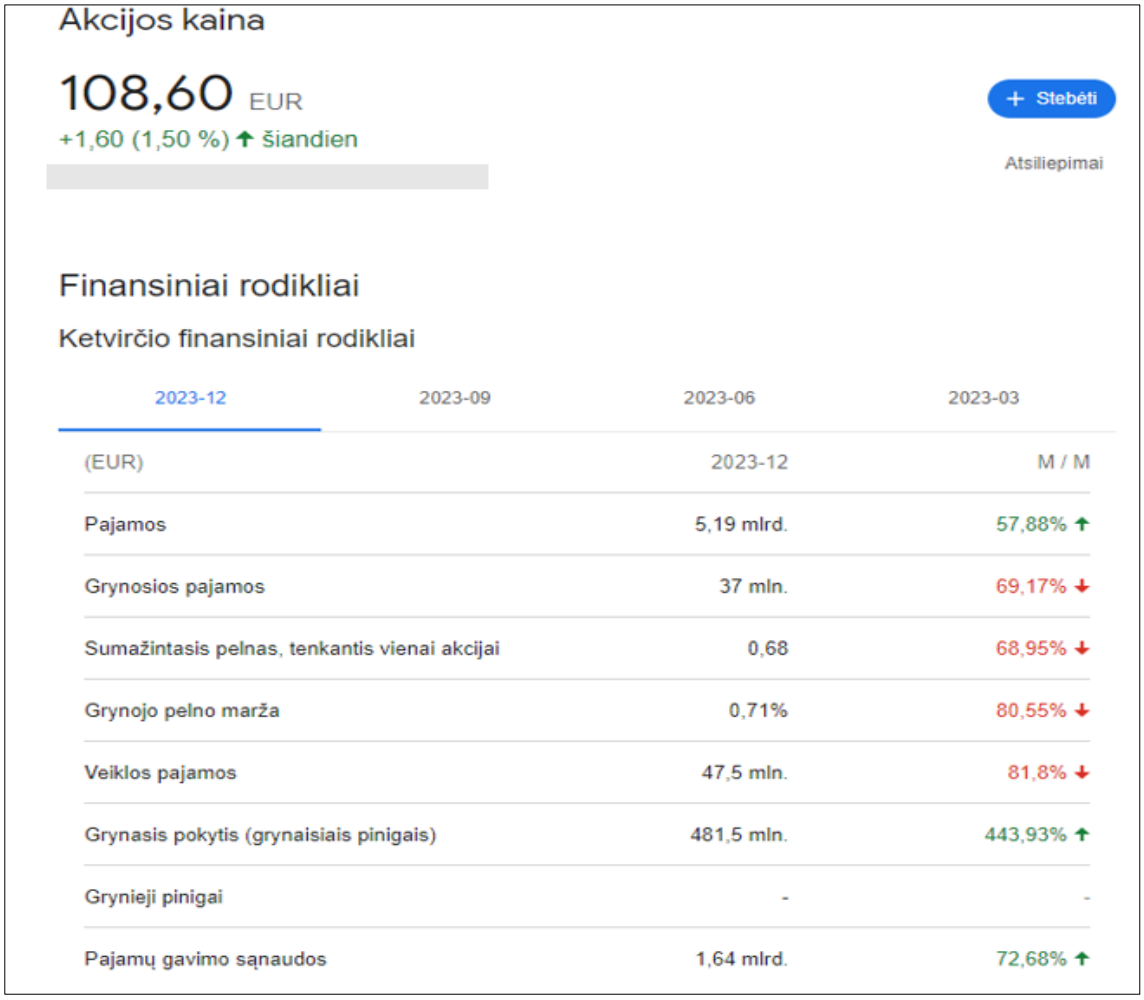
Sistema „STORe ⁻ CHAIN®“ leidžia valdyti įvairių objekto skaitiklių užfiksuotus duomenis, siekiant registruoti sukauptos energijos atsinaujinančią kilmę. Tokie duomenys įrašomi į „blockchain“ platformą, kuri patvirtina ir garantuoja informacijos patikimumą.

Taigi, „STORe-chain“ yra platforma, skirta valdyti ir stebėti tiekimo grandinės procesus. Ši platforma leidžia „Acciona“ įmonei efektyviai valdyti visus tiekimo grandinės žingsnius, nuo gamybos iki pristatymo klientams. „STORe-chain“ suteikia įmonės darbuotojams galimybę stebėti ir kontroliuoti visus tiekimo grandinės veiksmus realiu laiku, taip pagerinant efektyvumą, mažinant laiko ir išteklių sąnaudas bei užtikrinant aukštą kokybę ir saugumą visame tiekimo grandinės procese. Taip pat platforma padeda „Acciona“ įmonei efektyviai bendrauti su tiekimo grandinės partneriais ir užtikrinti sklandų prekių ir paslaugų judėjimą per visą tiekimo grandinę.

„GreenH2chain“

Naudodami „Green H_2 chain®“, „ACCIONA“ klientams suteikia prieiga prie skaitmeninės platformos, kuri leis jiems patikrinti ir vizualizuoti visą žaliojo vandenilio vertės grandinę realiu laiku ir iš bet kurios pasaulio vietos. „ACCIONA“ sukūrė „GreenH2chain®“ – pirmąją pasaulyje platformą, pagrįstą „blockchain“ technologija, kuri garantuoja atsinaujinančią žaliojo vandenilio kilmę . Šis naujas įrankis taip pat leis klientams patikrinti šios rūšies švarios energijos transportavimo ir pristatymo procesą. Naudodami „Green H_2 chain®“, „ACCIONA“ klientams bus suteikta prieiga prie skaitmeninės platformos, kuri leis jiems patikrinti ir vizualizuoti visą žaliojo vandenilio vertės grandinę realiu laiku iš bet kurios pasaulio vietos. Šis technologinis sprendimas leis atsinaujinančio vandenilio vartotojams kiekybiškai įvertinti, registruoti ir stebėti savo energijos tiekimo dekarbonizacijos procesą. Be to, „GreenH2chain ®“ pateikia visą reikiamą informaciją apie patį vandenilio suvartojimą, taip pat duomenis, leidžiančius apskaičiuoti anglies dvideginio (CO2) emisiją, kurios vartotojai išvengia naudodamiesi šia žaliąja energija. Ateityje „Green H_2 chain®“ papildys visas oficialias sistemas, skirtas vandenilio atsinaujinančios kilmės sertifikavimui, kai tik jos bus sukurtos. „ACCIONA“ platforma pasiūlys savo skirtingas vertes šioms schemoms tiek Europos lygiu, tiek kiekvienoje šalyje atskirai. Platforma bus įgyvendinta įgyvendinant projektą *„Power to Green Hydrogen“*, skirtą sukurti žaliąją ekosistemą Maljorkos saloje (Ispanija). „ACCIONA“ taip pat naudos„ Green H_2 chain®“ visuose būsimuose atsinaujinančios vandenilio gamybos projektuose. „ACCIONA“ sukūrė „Green H_2 chain®“ kartu su „FlexiDAO“ – įmone, teikiančia elektros programinės įrangos įrankius skaitmeninės energijos paslaugoms teikti. „FlexiDAO“ yra vienas iš startuolių, dalyvaujančių „ACCIONA“ atvirų inovacijų programoje „I'MNOVATION“ (Acciona, 2021).

14 paveiksle galite pamatyti įmonės finansinius rodiklius surinktus internete.



Akcijos kaina

108,60 EUR

+1,60 (1,50 %) ↑ šiandien

+ Stebėti

Atsiliepimai

Finansiniai rodikliai

Ketvirčio finansiniai rodikliai

2023-12	2023-09	2023-06	2023-03

(EUR)	2023-12	M / M
Pajamos	5,19 mlrd.	57,88% ↑
Grynosios pajamos	37 mln.	69,17% ↓
Sumažintasis pelnas, tenkantis vienai akcijai	0,68	68,95% ↓
Grynojo pelno marža	0,71%	80,55% ↓
Veiklos pajamos	47,5 mln.	81,8% ↓
Grynasis pokytis (grynaisiais pinigais)	481,5 mln.	443,93% ↑
Grynieji pinigai	-	-
Pajamų gavimo sąnaudos	1,64 mlrd.	72,68% ↑

Šaltinis: „Acciona “

14 pav. Finansiniai rodikliai

Projektai

Bendrovė dalyvauja anglies dioksido kreditų projektuose, kuriuose naudojama „blockchain“ technologija. Ji bendradarbiauja su „ClimateTrade“, kad suteiktų sertifikuotus emisijų mažinimo (CER) sertifikatus žaliajai energijai, pagamintai jos gamyklose besivystančiose Pietų Amerikos rinkose. ACCIONA taip pat išplėtė savo santykius su „ClimateTrade“, siekdama savanoriško anglies dioksido kiekio bandymo su Ispanijos vertybinių popierių birža BME.

CER yra Jungtinių Tautų švarios plėtros mechanizmo (CDM) išduotas sertifikatas, skirtas valstybėms narėms, siekiant išvengti vienos tonos anglies dvideginio išmetimo. Šiuo metu CER pardavimas pagal Kioto protokolą trunka apie du mėnesius, o „ClimateTrade“ tai pasiekė per 48 valandas.

Anglies dioksido kreditų rinkos leidžia organizacijoms, įmonėms ir asmenims parduoti arba įsigyti teises į šiltnamio efektą sukeliančių dujų išmetimą. Tai anglies dioksido kompensavimo mechanizmas, tam tikrais atžvilgiais panašus į atsinaujinančios energijos sertifikatus (REC), išskyrus tai, kad REC yra skirti švariai energijai gaminti. „ClimateTrade“ labai palengvins komercinius sandorius tarp gamintojų

ir anglies dioksido teisių pirkėjų, atverdama labai įdomų verslą ir novatorišką ACCIONA perspektyvą pereinant prie dekarbonizuotos ekonomikos, kuri papildo mūsų pagrindinę atsinaujinančios energijos tiekimo veiklą. (Ledger Insights, 2020).

Apibendrinat visa atvejo analizę ACCIONA naudoja blokų grandinę savo energijos valdymo programinei įrangai apsaugoti. Ir patvirtina iškelta hipotezę: Energetikos sektoriaus organizacijos gali pasinaudoti blokų grandinės technologija siekdamos užtikrinti duomenų saugumą ir atsekamumą. „Acciona Energia“ nuolat investuoja į inovacijas ir naujoves, siekdama tobulinti savo veiklą ir pasiūlyti klientams efektyvesnius sprendimus. Blokų grandinės technologija užtikrina aukštą duomenų saugumo lygį, todėl „Acciona Energia“ patikimai saugoja svarbius duomenis apie energijos gamybą ir paskirstymą. Blokų grandinė leidžia „Acciona Energia“ užtikrinti skaidrumą ir atsekamumą savo veikloje, suteikdama klientams ir reguliatoriams galimybę stebėti energijos tiekimą nuo gamybos iki vartojimo. Blokų grandinės technologija gerina „Acciona Energia“ veiklos efektyvumą, optimizuoja procesus, mažinant tarpininkų kiekį ir sumažinant administracines sąnaudas, suteikia galimybę kurti naujus verslo modelius, tokius kaip energijos prekybos platformos ar mikrotinklai, kurie yra pelningi ir inovatyvūs. BC leidžia lengviau bendradarbiauti su tarptautiniais partneriais ir įgyvendinti projektus visame pasaulyje, suteikiant „Acciona Energia“ galimybę plėsti savo veiklą. Sėkminga įmonės veiklą lemia puiki strategija, bendradarbiavimas su kitomis šalimis ir įmonėmis.

4.1.3 „PONTON GmbH“

11 lentelė. „PONTON GmbH“ pagrindinė informacija

Interneto svetainė	http://www.ponton.de
Industrija	Informacinės technologijos ir paslaugos
Įmonės dydis	51-200 darbuotojų
Būstinė	Hamburgas
Tipas	Privati
Įkurta	2001 m
Specialybės	Energija, blokų grandinė, P2P pranešimų siuntimas, B2B integracija ir prekyba prekėmis
Pajamos	$6.7 mln.

Įkurta 2001 metais, šiuo metu dirba 60 darbuotojų. „PONTON GmbH“ yra programinės įrangos įmonė, teikianti standartinius sprendimus B2B (verslas verslui) procesams energetikos pramonėje. „PONTON“ sujungia gilią patirtį energetikos pramonėje su galimybe pritaikyti individualius, novatoriškus sprendimus. Ilgalaikiai santykiai su tarptautiniais klientų konsorciumais ir asociacijomis yra „PONTON“ DNR dalis. Nuo 2000 m. yra pagrindinė XML pagrindu veikiančių pasaulinių B2B tinklų steigėja. Nuo 2004 m. šimtai didmeninių energijos ir prekių prekiautojų, tokių kaip komunalinės paslaugos ir bankai, susibūrę į „EFETnet“ (Energy Federation of Energy traders) konsorciumą, pradėjo naudoti „PONTON“ sukurtą programinę įrangą automatizuoti savo prekybos ir atsiskaitymo procesus, įskaitant sandorių patvirtinimus. 2016 m. įmonė pradėjo naudoti blokų grandinės technologiją prekybai energija, pirmiausia įgyvendindama projektą „Enerchain“, kurio metu pirmą kartą Europoje buvo prekiaujama didmenine energija per „blockchain“. „PONTON“ išplėtė šį metodą tokiais projektais kaip „Gridchain“. 2020 m. vykdydamas bendrą projektą „Šiaurės Vokietijos energijos perėjimas“ (NEW 4.0), savivaldybės energijos tiekėjas „HAMBURG ENERGIE“ kartu su „Ponton GmbH“ ir kitais partneriais sėkmingai išbandė rinka pagrįstą energijos platformą, kuri leidžia greitai, lanksčiai ir saugiai prekiauti regione atsinaujinančių energijos šaltinių. Platforma gali decentralizuoti energijos tiekimą, kad dideli komerciniai elektros vartotojai galėtų prekiauti tiesiogiai su energetikos įmonėmis ir net parduoti perteklinę energiją. „Blockchain“ erdvėje „PONTON“ naudoja savo „WRMHL“ sistemą. „WRMHL“ („Wormhole“) yra įmonėms pritaikyta, mažai delsianti blokų grandinės sistema, skirta pramonės konsorciumams ar bendruomenėms. Be produktų pagrįstų pasiūlymų, įmonė siūlo tokias paslaugas kaip individualių programinės įrangos programų kūrimas, esamų produktų priežiūra, palaikymas ir pritaikymas.

„Enerchain“

„Enerchain“ buvo vienas iš sėkmingiausių Europoje „blockchain“ projektų, parodęs, kaip energijos sandoriai gali būti vykdomi visiškai decentralizuotai – tiek didmeninei prekybai, tiek energijos bendruomenėms. „Enerchain“ koncepcijos įrodymas prasidėjo 2017 m. gegužę kartu su 44 pirmaujančiomis Europos energijos prekybos įmonėmis. Per dvejus metus „PONTON“ padėjo atlikti kelis pramonės mastu vykdomus bandymus, siekdama atlikti prekybos procesą be centrinės platformos operatoriaus ir apsaugoti blokų grandinės infrastruktūrą nuo galimų kibernetinių atakų.

„Enerchain“ pagrindinė „blockchain“ sistema (WRMHL) yra viena greičiausių galimų viso bloko „blockchain“ aplinkų: ji pasiekia trumpesnį nei vienos sekundės blokavimo laiką, o vidutinis galutinio sutarimo laikas yra tik 200 milisekundės. Sistema ypač tinka prekybos procesams, kuriems reikalingas greitas duomenų sinchronizavimas tarp dalyvių. „Enerchain“ misija buvo sumažinti įėjimo kliūtis naujiems rinkos dalyviams, suvienodinti sąlygas sandorių greičiui ir suteikti dalyviams tiesioginę prieigą prie jų pačių sugeneruotų rinkos duomenų.

„Gridchain“

„PONTON“ sukūrė naujovišką bandomąją programinę įrangą, pagrįstą blokų grandinės technologija, kuri imituoja būsimus procesus, skirtus tinklo valdymui realiuoju laiku, vadinamą **Gridchain**. Be to, „Gridchain“ prisideda prie Europos tarp procesinio ryšio standartizacijos kuriant išmaniuosius ateities tinklus:

- Sukūrė integruotą procesą, kuris per kelias sekundes koordinuoja balansavimo galios užklausas tarp perdavimo sistemos operatorių, skirstomųjų tinklų operatorių, agregatorių ir gamybos įrenginių.
- Suteikė galimybę paskirstymo operatoriams sąveikauti su balansavimo užklausų procesu perkrovos situacijose gerokai prieš pristatymo laikotarpį, o ne tik tada, kai generatorius iš tikrųjų padidina generavimo apkrovą.
- Suteikė galimybę informuoti agregatorius apie savo nuopelnų sąrašo koregavimą, atsižvelgiant į trumpalaikius apkrovos signalus.
- Sumažino atsiskaitymo laiką nuo > 1 mėnesio iki vos 15 minučių.

„PONTON“ dalyvauja projekte: „Europos paskirstytų duomenų infrastruktūra energetikai“ jie gavo 376 250,00 € paramos iš Europos sąjungos.

Projekto tikslas: Siekiant pereiti nuo iškastinio kuro prie švaresnės energijos ir įvykdyti Paryžiaus susitarimo įsipareigojimus mažinti šiltnamio efektą sukeliančių dujų išmetimą, ES švarios energijos paketas yra didelis žingsnis energetikos sąjungos strategijos link. Paketu nustatomos teisės prieiti prie energijos duomenų vartotojams ir dalytis jais su pasirinktomis tinkamomis šalimis. Tačiau vienodų procedūrų nebuvimas ES yra iššūkis. Atsižvelgiant į tai, ES finansuojamas EDDIE projektas sukurs decentralizuotą, paskirstytą atvirojo kodo duomenų erdvę, kuri sumažins duomenų integravimo išlaidas ir padidins konkurenciją. Taip pat pagerins energijos duomenimis pagrįstų paslaugų kokybę ir funkcionalumą. Suderintas su Europos sąveikumo kryptimis, projektas leis lengvai pasiekti visus – nuo paslaugų įmonių iki galutinių vartotojų (European Commission, 2023). „PONTON“ veikia daugiau nei 20 metų. Klientai palaikomi daugiau nei 18 metų su „Equias“, daugiau nei 15 metų su ECC ir daugiau nei 10 metų su EDA. Bendras platformos gedimų skaičius per šiuos metus gali būti išmatuotas tik per kelias valandas. Todėl „PONTON“ rimtai žiūri į IT saugumą: jie turi **ISO 27.001** sertifikatą.

Apibendrinant „PONTON“ įmonės, sėkmingą veiklą lemia, parama iš Europos sąjungos, toliau plėsti decentralizaciją. „Enerchain“ leidžia energijos tiekėjams tiesiogiai mainytis energija be tarpininkų, o „Gridchain“ suteikia išsamesnę informaciją apie energijos srautus ir vartojimą.

4.1.4 Rezultatų interpretavimas

Atlikta atvejų analizė atsakė į visus tyrimo klausimus ir įrodė realų blokų grandinės technologijos pritaikymą energetikos sektoriuje.

Išanalizavus „Powerledger“ išsiaškinta, kad „blockchain“ technologiją naudoja šiose srityse: tarpusavio prekybai energija, virtualios elektrinės ir lankstumo paslaugos, elektros energijos pirkimo sutartys, atsinaujinančios energijos sertifikatai. „Blockchain“ padeda patvirtinti duomenis vartotojams, klientai gali pasirinkti, kokio energijos šaltinio nori, pavyzdžiui, vėjo, saulės ar vandens ir atitinkamai pirkti iš tiekimo. Naudojant blokų grandines supaprastintas patikrinimas, kilmė ir sekimas. Įmonės sėkmę lemia prekiavimas įmonės akcijomis ir naujais projektais pritraukia vis daugiau investuotojų. Viešoje erdvėje nėra paskelbta atvejų, dėl kibernetinių atakų, tai galima daryti išvadą, jog įmonė yra gerai apsisaugojusi.

Atlikus įmonės „ACCIONA Energia“ įmonės analizę, pastebėta blokų grandinės technologijos platus pritaikymo spektras net penkiose srityse. BC padeda spręsti įmonėje, tokias problemas kaip duomenų saugumas, transakcijų patikimumas ir tinkamą tiekimo grandinės valdymą. Sėkmingą įmonės veiklą lemia tinkamas blokų grandinės technologijos įdiegimas. Profesionalūs darbuotojai ir bendradarbiavimas su kitomis įmonėmis lemia sėkmę.

Galiausiai išnagrinėjus „Ponton GmbH“ naudoja blokų grandinę technologiją stebėti ir valdyti energijos tiekimo grandinę nuo gamybos iki vartojimo, tai padeda užtikrinti skaidrumą ir efektyvumą.

Remiantis šiuo tyrimu, pavyko pasiekti tyrimo tikslą: ištirti blokų grandinės taikymo ypatumus ir galimybes. Analizuojant praktikoje taikomas blokų grandinių technologijas, prieita išvada, kad blokų grandinė turi perspektyvą.

4.2 Pusiau struktūrizuoto interviu duomenų analizė

Pusiau struktūrizuoti interviu. Šiam metodui būdinga vidinė struktūra, tačiau respondentui leidžiama netrukdomai reikšti savo mintis. Pusiau struktūrizuotas interviu taikomas apklausiant specialistus, nes jie nelinkę kalbėti nežinoma tema. Kaip ir giluminiame interviu, apklausos tyrėjas privalo laikytis taip, kad neturėtų jokios įtakos respondentui (T. Belevičienė ir S. Jonušauskas, 2011).

Struktūrizuotas interviu su kibernetinio saugumo ekspertais ir IT technologijų ekspertais buvo naudingas būdas, gauti išsamią informaciją ir suprasti jų požiūrį bei patirtį energetikos sektoriuje su blokų grandine ir kibernetiniu saugumu. Šis kokybinis tyrimas buvo pasirinktas dėl šių priežasčių: ekspertų požiūrio supratimas, struktūrizuotas interviu leidžia giliau suprasti ekspertų nuomones, patirtį ir požiūrį į kibernetinį saugumą energetikos sektoriuje su blokų grandine. Geresnis sprendimų priėmimas: turint įvairiapusę informaciją iš struktūrizuoto interviu su ekspertais, galima padaryti geriau pagrįstus sprendimus ir rekomendacijas dėl kibernetinio saugumo strategijų energetikos sektoriuje. 1 Priedas klausimai pateikti ekspertams lietuvių ir anglų kalbomis. Atliekant tyrimą, dauguma ekspertų norėjo maksimaliai išlikti anonimiški.

Kibernetinio saugumo ekspertai:

• Ekspertas Nr. 1. Dirba Lietuvoje banke.

1. Pareigos/paskyrimas: *Vyresnysis IT saugumo inžinierius (angl. Senior IT Security Specialist, Detection Engineer)*

2. Darbo patirtis: *15 metų IT darbo patirtis, iš kurių 8 metai kibernetinis saugumas*

3. Išsilavinimas: *Bakalauras Informacinės technologijos inžinerija ir Magistras Elektronikos inžinerija Vilniaus Gedimino technikos universitetas.*

• Ekspertas Nr. 2. Dirbo „Shell“ ir kūrė „Blockchain“. Šiuo metu dirba Vokietijoje.

1. Position/designation *Information Security Analyst*

2. Work experience *20 years in IT, 5 of which in IT security*

3. Education: *Master degree, Physic, (specializatoion: digital telecommunication networks and systems)*

• Ekspertas Nr. 3. Dirba energetikos sektoriuje Lietuvoje.

1. Pareigos/paskyrimas: *Informacijos saugos vadovas, Informacijos saugos įgaliotinis.*

2. Darbo patirtis: *5 metai*

3. Išsilavinimas: *Aukštasis, Vilnius Tech, Informacijos ir informacinių technologijų sauga.*

Ekspertai informatikos srityje:

• Ekspertas Nr. 4. Dirba su kritinėmis IT infrastruktūromis Lietuvoje.

1. Pareigos/paskyrimas*: IT konsultantas/administratorius*

2. Darbo patirtis: *15 metų.*

3. Išsilavinimas: *Aukštasis.*

• Ekspertas Nr. 5. Dirba Vokietijoje.

1. Pareigos/paskyrimas: *System Engineer*

2. Darbo patirtis: *6 year.*

3. Išsilavinimas: *Master's degree in computer science, Philipps University Marburg.*

Pateikti klausimai 12 lentelėje buvo suskirstyti į dvi kategorijas : kibernetinis saugumas ir „Blockchain“. Interviu gauti duomenys buvo suvesti į Excel programą ir klasifikuojami, kad išgauti bendrus pasikartojančius ir aiškius atsakymus.

12 lentelė. Apibendrinti ekspertų atsakymai į tyrimo klausimus

Klausimai	Ekspertų atsakymų į tyrimo klausimus apibendrinimas, dažniausiai pasitaikantys atsakymai
Kibernetinis saugumas	
1. Kokios yra pagrindinės kibernetinio saugumo grėsmės, su kuriomis susiduria organizacijos šiandieninėje skaitmeninėje erdvėje?	1.Duomenų vagystė . 2. Išpirkos reikalaujančios atakos. 3. Duomenų atakos (angl. data breaches) – konfidenciali informacija kopijuoja, perduodama, peržiūrima ar naudojama asmens, kuris neturi leidimo. Šie pažeidimai gali sukelti didelių finansinių nuostolių ar reputacinę žalą įmonėms. 4. Pažangios kibernetinės grupuotės (angl. Advanced persisten Threats (APTs) 5. Paslaugų pasiekiamumo trikdymo atakos (angl. Distributed Denial of Service (DDOS) attacks). 6. Nežinojimas visų savo „assets“; dar pakankamai žema darbuotojų kibernetinio saugumo branda; dažnai prisiimamos neišmatuotos rizikos, nes investuoti į kibernetinį saugumą būna brangu; ydingas mąstymas – „dar nieks nenulaužė arba mes niekam neįdomūs, tai kam kažką daryti“; kibernetinis ir informacijos saugumas nėra prioretizuojamas, suprantamas tik kaip formalumas"
2. Kaip organizacijos gali efektyviai apsaugoti savo duomenis nuo kibernetinių atakų ir pažeidimų? Kaip organizacijos gali užtikrinti, kad jų darbuotojai būtų gerai informuoti ir apmokyti dėl kibernetinių grėsmių bei saugumo priemonių?	1.Saugumo mokymai darbuotojams (sukčiavimo pavojus ir saugaus interneto praktikos svarbą). 2. Tvirta slaptažodžių politika ir kelių veiksnių autentifikacija. 3. Reguliarus programinės į rangos atnaujinimas ir pastebėtų spragų šalinimas. 4. Įsibrovimo aptikimo sistemos ir saugus užkardų (angl. firewall) konfigūravimas. 5. Jautrių duomenų šifravimas. 6. Reguliarios saugumo audito procedūros. 7. Prieigos kontrolė įgyvendinimas. 8. Kenkėjiškos programinės įrangos ir elgesio aptikimo programų naudojimas. 9. Incidentų reagavimo planas. 10. Svarbių duomenų atsarginių kopijų darymas. Parengti aiškiais organizacines priemones – teisės aktai (taisyklės, procesai), identifikuoti savo visą IT/IS ūkį ir techninėmis priemonėmis valdyti atitinkamas rizikas, pvz. informacijos sauga – DLP sprendimas ir t.t. Pirmiausia išsirinkti saugumo standartą kurio vadovausis įmonė. (kaip pvz ISO 27001/27002). Turėti saugumo komandą. Reguliariai naujinti serverius/servisus, tinklo įrangą, kompiuterius. Atlikti saugumo mokymus darbuotojams. Turėti reagavimo planą. Kad darbuotojai būtų informuoti ir apmokyti apie kibernetines grėsmes ir saugumo priemones, organizacijos gali rengti reguliarius mokymus, kuriuose būtų apžvelgiama naujausia kibernetinio saugumo praktika ir grėsmės. Šios sesijos turėtų būti įtraukiančios ir aktualios, naudojant realius pavyzdžius, kad būtų pabrėžta saugumo svarba. Be to, organizacijos gali naudoti informacinius biuletenius, saugos įspėjimus ir viktorinas, kad kibernetinis saugumas būtų darbuotojų dėmesio centre. Taip pat labai svarbu skatinti saugumo kultūrą, kai darbuotojai jaustųsi patogiai pranešdami apie galimas grėsmes ir užduodami klausimus. Reguliarūs saugos politikos ir procedūrų atnaujinimai užtikrina, kad žinios išliks aktualios ir nepamirštų visų darbuotojų.

3. Kokia yra svarbiausia kibernetinio saugumo politika, kurią organizacija turėtų įgyvendinti siekiant užtikrinti duomenų saugumą? Kokius kibernetinio saugumo įrankius ir technologijas vertėtų įtraukti į organizacijos saugumo strategiją?	Pasitikėjimas viena politika negali pakankamai užtikrinti organizacijos pozicijos. Besivystantis grėsmės kraštovaizdis reikalauja daugiasluoksnės gynybos strategijos. Informacijos saugos valdymo sistemų, tokių kaip ISO 27001 arba NIST, pritaikymas yra labai svarbus siekiant visapusiško požiūrio į kibernetinį saugumą. Šios sistemos padeda organizacijoms efektyviai valdyti techninius įrankius, suderinti kibernetinio saugumo pastangas su verslo reikalavimais ir teikti tikslinius mokymus vartotojams ir IT administratoriams. Struktūrizuoto požiūrio, pvz., Informacijos saugumo valdymo sistemos (ISMS), įgyvendinimas leidžia saugumo specialistams nustatyti ir eskaluoti svarbias valdymo rizikas, užtikrinant, kad rizikos mažinimui būtų skirti būtini ištekliai. Be to, kibernetinis saugumas turėtų būti integruotas į organizacijos kultūrą, remiant verslo tikslus ir skatinant saugią aplinką naujose įmonėse. Ši integracija tampa ypač svarbi, nes įmonės plečia savo debesijos paslaugų naudojimą ir atlieka tarpusavyje susijusias operacijas su tiekėjais, partneriais ir išorės kūrėjais. Kurdamos tvirtą saugumo strategiją, organizacijoms labai svarbu įtraukti daugybę kibernetinio saugumo įrankių ir technologijų, skirtų kovoti su įvairiomis šiandienos skaitmeninėmis grėsmėmis. Pagrindiniai, bet svarbūs komponentai, tokie kaip ugniasienės ir antivirusinė programinė įranga, apsaugo nuo neteisėtos prieigos ir kenkėjiškų programų. Įsibrovimų aptikimo ir prevencijos sistemos stebi tinklo pažeidimus ir blokuoja juos prieš jiems įvykstant. Šifravimo įrankiai užtikrina duomenų saugumą, nesvarbu, ar jie saugomi, ar siunčiami internetu. Kelių veiksnių autentifikavimas (MFA) prideda papildomą saugos sluoksnį, nes reikalauja papildomų patvirtinimo metodų, todėl užpuolikams sunkiau gauti neteisėtą prieigą. Virtualūs privatūs tinklai (VPN) yra raktas dirbant nuotoliniu būdu, šifruojant duomenis viešuosiuose tinkluose. Organizacijoms, naudojančioms debesies paslaugas, debesies prieigos saugos tarpininkai (CASB) padeda valdyti ir apsaugoti debesies programas. Saugumo informacijos ir įvykių valdymo (SIEM) sistemos analizuoja saugos įspėjimus realiuoju laiku, padeda greitai nustatyti grėsmes ir į jas reaguoti. Naujos technologijos, tokios kaip dirbtinis intelektas (AI) ir mašininis mokymasis (ML), tampa svarbios numatant ir aptinkant naujas grėsmes. Galinių taškų apsaugos platformos (EPP) apsaugo prie tinklo prijungtus įrenginius nuo kenkėjiškų programų ir kitų atakų. Duomenų praradimo prevencijos (DLP) technologijos sustabdo jautrios informacijos nutekėjimą iš organizacijos. Kartu šios priemonės sudaro visapusišką apsaugą nuo sudėtingų kibernetinio saugumo iššūkių, su kuriais šiandien susiduria organizacijos." EDR/XDR; NDR, SIEM, SOAR, DLP, WAF, anti-DDOS, vulnerability scanner. IDS, IPS, WAF.
4. Kokių priemonių, Jūsų nuomone, reikėtų imtis siekiant pagerinti kibernetinio saugumo esamą padėtį pvz: kad žmonės internete elgtųsi saugiau, mandagiau ir labiau save saugotų ir nedalintų savo asmeninių duomenų?	Daugiau mokymų žmonėms, stipresnio teisinio reguliavimo, interneto saugumo priemonių platesnio naudojimo, geresnės kibernetinio saugumo infrastruktūros ir skatinti žmones pranešti apie netinkamą elgesį. Informacijos sklaidos, teisės aktų reguliavimo.

„Blockchain“	
5. Ar esate susipažinęs su „Blockchain“ technologija ir ar naudojate ją kasdienėje verslo veikloje? Priežastys, kodėl naudojate ar nenaudojate. Kokius BC funkcijos gali būti naudingos Jūsų įmonei?	Visi 5 ekspertai yra susipažinę su blokų grandinę. Tik ekspertas2 daugiau pakomentavo apie šią technologiją. Taip, esu gerai susipažinęs su „blockchain“ technologija ir plačiu jos pritaikymo spektru įvairiuose sektoriuose. Ši technologija, nors ir vis dar tobulinama, yra daug žadanti tokiose srityse kaip tiekimo grandinės valdymas ir situacijose, kai svarbiausia užtikrinti duomenų vientisumą. Šiuo metu, esamose pareigose, mes aktyviai neintegravome blokų grandinės į savo veiklą. Tačiau mano ankstesnėje pozicijoje mes ištyrėme „blockchain“ galimybes konkrečiais naudojimo atvejais. Šis tyrimas pabrėžė technologijos potencialą pakeisti tradicinius procesus, nors mes dar turime ją visiškai įgyvendinti savo dabartinėje verslo praktikoje.
6. Jei naudojate „Blockchain“ kokiomis pagrindinėmis kliūtimis iki šiol susidūrėte? Jei NE – kokie pagrindiniai galimi BC naudojimo trūkumai (veiksniai, neleidžiantys jūsų įmonei įgyvendinti BC)? Jei TAIP – pagal skalę nuo 1 iki 5, kaip įvertintumėte savo patirtį naudojant BC? jei NE – 1–5 skalėje, kaip tikėtina, kad ateityje naudosite „Blockchain“ ir kodėl?	Visi ekspertai atsakė, kad nenaudoja šiuo metu „blockchain“ . Priežastys kodėl: Suderinamumas su esamomis IT sistemomis, nėra atidėliotinų verslo poreikių ar specifinių pavojų, grandinės diegimo ir priežiūros kaina.
7. Kokią ateitis „blockchain“ atsinaujinančios energijos sektoriuje ir kokią įtaką, tai turėtų veiklos meistriškumui, verslo modeliams ir vertės pasiūlymams?	BC atsinaujinančiuose energijos sektoriuje yra dar tik pradiniame panaudojimo lygmenyje. Norint kad ši technologija vystytųsi reikėtų įveikti jau paminėtus verslui kylančius iššūkius (teisinis reguliavimas, suderinamumas su IT sistemomis). Įveikus šiuos iššūkius BC galėtų būti įgyvendinta įkraunant elektrinius automobilius, valdyti pakrovimo stoteles, užtikrinant saugias ir sąžiningas transakcijas tarp elektros tiekėjo ir krovimo stotelės savininko. BC galėtų būti panaudota decentralizuotam energetinio tinklo kūrimui, kai gamintojai ir naudotojai galėtų tiesiogiai vienas su kitu prekiauti. Tinklo valdymui, BC gali būti panaudota balansuoti pasiūlą ir paklausą energetiniame tinkle.
8. Ar galite pateikti apžvalgą, kaip blokų grandinės technologija šiuo metu naudojama energetikos sektoriuje ir galimi jos pritaikymai? Kokie yra pagrindiniai iššūkiai ir kliūtys diegti blokų grandinę energetikos sektoriuje ir kaip jas spręsti?	Tiesioginis (angl. peer-to-peer) prekiavimas ir transakcijų verifikavimas pvz. Power Ledger, Electron platformos. BC įgalina transakcijų decentralizavimą, vartotojus ir gamintojus tiesiogiai prekiauti vieni su kitais. Lo3
	Pagrindiniai iššūkiai diegiant „blockchain“ didelis tam tikrų BC modelių energijos suvartojimas, reguliavimo neapibrėžtumas ir integracijos su esamomis sistemomis sudėtingumas. Galbūt abejotina nauda, noro ir laiko trūkumas. Tinklo delsa ir kaina. Norint įveikti šias kliūtis, reikia priimti efektyvesnius energiją taupančius blokų grandinės protokolus, bendradarbiauti su reguliavimo institucijomis, kad būtų paaiškinta teisinė bazė, ir sukurti sąveikius sprendimus, kurie galėtų sklandžiai integruotis su dabartine energetikos infrastruktūra.
	Saugios komunikacijos. „Blockchain„ gali suteikti saugų komunikacijos kanalą tarp skirtingos infrastruktūros dalių,

9. Kaip „blockchain“ technologija galėtų sustiprinti kibernetinio saugumo priemones energetikos sektoriuje, ypač apsaugant kritinę infrastruktūrą ir jautrius duomenis nuo kibernetinių grėsmių? Kaip vertinate galimą riziką ir pažeidžiamumą, susijusį su blokų grandinės integravimu į energijos sistemas kibernetinio saugumo požiūriu?	kaip antai išmanūs skaitikliai, tinklo operatoriai, energijos gamintojai. Taip pat gali užtikrinti transakcijos nenuginčijamumą, sumanių kontraktų įgalinimą. Užtikrinti decentralizacija. Dėl kritinės infrastruktūros „blockchain“ gali padėti apsaugoti sumanius įrengius, daiktų interneto įrenginius (angl. IoT) užtikrinant identifikacija ir autentifikacija tokių įrenginių kaip sumanūs skaitikliai. Užtikrinti decentralicija, taip sumažinant rizika dėl vieno įrenginio, sistemos taško sutrikimo pavojaus. Autorizacija, priegos kontrolė, duomenų vientisumas.
	Išmaniųjų kontraktų pažeidžiamumai (angl. Smart contracts) – yra rizika, kad programinis kodas gali turėti pažeidžiamumų ir spragų. Norint sumažinti šią riziką turi būti užtikrintas tinkamas testavimas, auditavimas sumanių kontraktų prieš išleidžiant programinę įrangą. Blokų grandinės tinklo dydis – esant mažam blokų grandinės tinklo dydžiui, tinklas yra labiau pažeidžiamas manipuliavimo atakoms, nes reikalinga kontroliuoti pakankamai mažą tinklo mazgų skaičių norint atlikti tokią ataką. Sumažinti tokią riziką turėtų būti sukurtas pakankamai didelis ir įvairus „blockchain“ tinklas.
10. Į kokius reguliavimo aspektus ir atitikties reikalavimus turi atsižvelgti energetikos įmonės, priimdamos blokų grandinę kibernetinio saugumo tikslais?	Duomenų saugumas ir privatumas, įmonės turi atitikti BDAR reguliavimui, taip pat ir „blockchain“ technologijai. Kibernetinio saugumo standartams ir reikalavimams. Energetinio sektoriaus teisinį reguliavimą. Sumanių kontraktų teisinį reguliavimą.
11. Kaip manote, kodėl Lietuvoje neišsilaikė nė vienas startuolis su „blockchain“? Kaip manote, kodėl dauguma startuolių su blockchain neišsilaiko?	Lietuvoje: Teisinis reguliavimas ir jo trūkumai, techniniai iššūkiai, finansavimo šaltiniai, konkurencija kitose šalyse lėmė, kad Lietuvoje neišsilaikė nė vienas startuolis su „blockchain. Per mažas poreikis šios technologijos diegimo, ypatingai valstybiniuose energetikos sektoriuose. Trūksta specialistų, reguliavimas, maža rinka. Apskritai: Per brangu, klientų švietimo ir verslo partnerių dvejonės, Prastas produkto pritaikymas rinkai.
12. Gal žinote, daug geresnių alternatyvių, nei blokų grandinė? Kokios Jos?	Įprastos duomenų bazių sistemos. Amazon QLDB Naudojimo atvejais, kuriems nereikia decentralizacijos ar nekintamumo, tradicinės reliacinės duomenų bazės arba debesų duomenų bazės gali būti efektyvesnės, lengviau valdomos ir pigesnės. Tais atvejais, kai pasitikėjimas nėra problema arba kai pirmenybė teikiama centrinei kontrolei, centralizuotos sistemos gali užtikrinti paprastesnį valdymą ir greitesnį operacijų apdorojimą. Galiausiai, galimas būdas yra blokų grandinės ypatybių derinimas su tradicinėmis ar kitomis naujomis technologijomis, siekiant išnaudoti kiekvieno iš jų stipriąsias puses.

Apibendrinant empirinio tyrimo rezultatus, galima daryti išvadą, kad **blokų grandinė garantuoja** duomenų vientisumą ir skaidrumą. Šis atsakymas buvo vienodas visų ekspertų. Visi dalyvavę interviu ekspertai yra susipažinę su „blockchain“, bet šiuo metu nenaudoja ir buvo skeptiškai nusiteikia, jos atžvilgiu ir tvirtino, kad esamos duomenų bazės yra saugios. Pagrindinės sritis, kuriose naudojamos blokų grandinės ekspertai išskyrė šias:

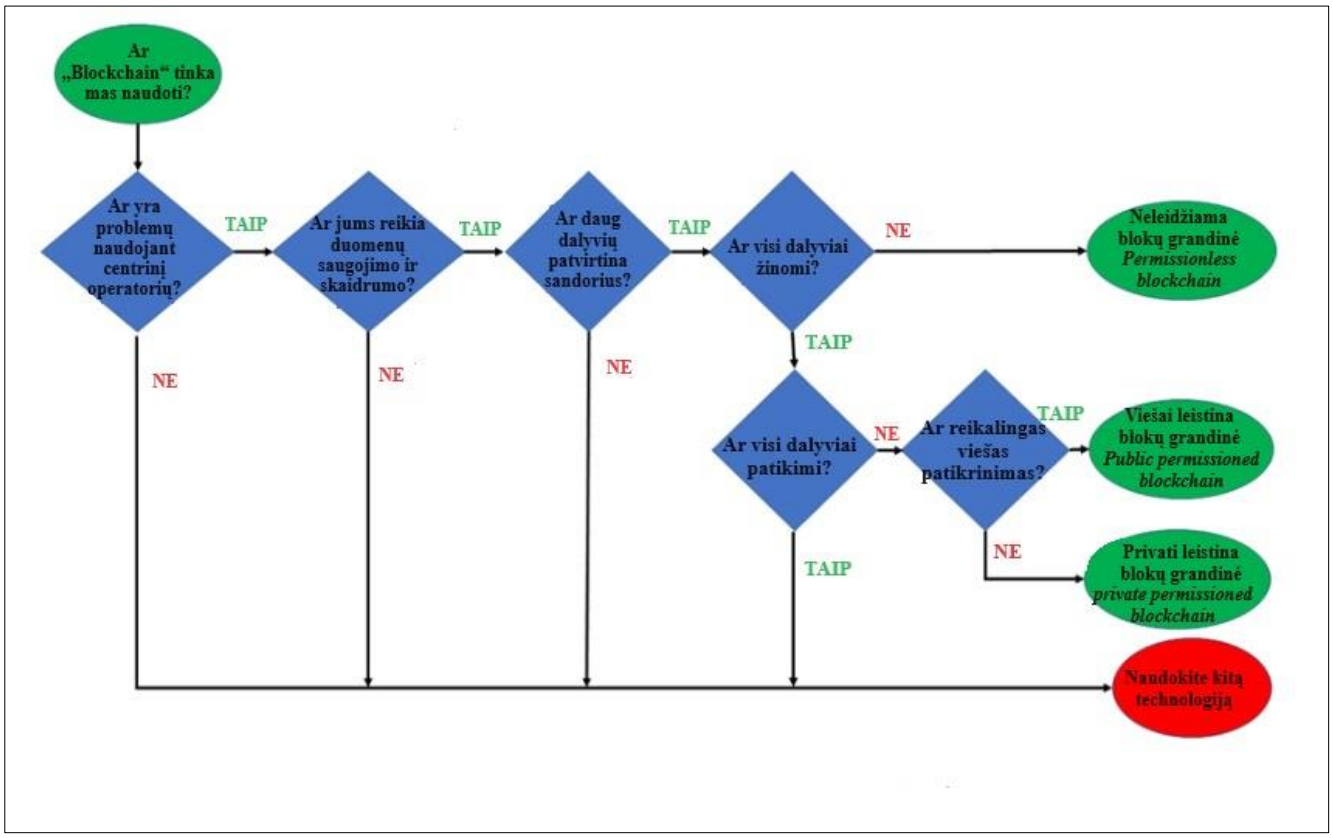
- P2P prekyba;

- Elektromobilumas;
- Išmanieji skaitliukai;
- Tinklo valdyme.

Diegiant BC su kokiais iššūkiais susiduriama, ekspertų vyraujanti nuomonė: teisiniai iššūkiai, integracijos su esamomis sistemomis sudėtingumas, tinklo delsa. Kibernetinio saugumo riziką, ekspertai vertinai taip: esant mažam blokų grandinės tinklo dydžiui, tinklas yra labiau pažeidžiamas manipuliavimo atakoms, nes reikalinga kontroliuoti pakankamai mažą tinklo mazgų skaičių norint atlikti tokią ataką ir būtina testuoti audituoti sumaniuosius kontraktus.

Apklausus ekspertus kaip „blockchain“ galėtų sustiprinti kibernetinį saugumą energetiniame sektoriuje, prieita prie išvados, kad BC gali suteikti saugų komunikacijos kanalą tarp skirtingų infrastruktūros dalių (išmanieji skaitikliai, tinklo operatoriai, energijos gamintojai). Užtikrinti decentralizaciją, taip sumažinant riziką dėl vieno įrenginio, sistemos taško sutrikimo pavojaus.

Remiantis ekspertų nuomonėmis, galima organizacijoms pasiūlyti prieš naudojant blokų grandinės technologiją įsivertinti reikalingumą šios programą, 15 paveiksle pateikti baziniai klausimai, kurie buvo išversti į lietuvių kalbą,



Šaltinis:sudaryta autorės pagal M. Nour, J. P. Chaves-Ávila and Á. Sánchez-Miralles (2022)

15 pav. Preliminarūs „blockchain“ technologijos tinkamumo programai vertinimo kriterijai

Neleidžiamos (Permissionless) blokų grandinės pasiekia sutarimą naudojant decentralizuotą protokolą, taikomą teoriškai neribotam dalyvių ar mazgų rinkiniui. Neleidžiami protokolai nereikalauja, kad mazgai atskleistų savo tapatybę, išskyrus pseudoniminį identifikatorių. Be to, dalyviai bet kuriuo metu gali įsigyti naujų identifikatorių, atsikratyti senų ir valdyti kelis identifikatorius. Taigi neleistinos blokų grandinės negali prisiimti jokio pasitikėjimo savo aplinkoje, nes jų dalyviai lieka anonimiški ir nepasiekiami už blokų grandinės nepriklausančių vykdymo mechanizmų, tokių kaip teismai ar kitos institucijos. Leidžiamos (Permissioned) blokų grandinės, priešingai, reikalauja, kad tikrinimo mazgai, galintys atnaujinti blokų grandinę, turi būti patvirtinti prieš prisiimdami šį vaidmenį, o kai kurios leistinos blokų grandinės taip pat nustato patvirtinimo reikalavimus vartotojo mazgams. Patvirtinimo procese paprastai reikalaujama, kad mazgai užtikrintų visišką skaidrumą dėl savo tapatybės, todėl konsensuso mechanizmai leistinose blokų grandinėse paprastai prisiima bent, tam tikrą pasitikėjimą pagrindine institucine aplinka (Yannis Bakos ir Hanna Halaburda, 2021).

Nelengva įvertinti blokų grandinės technologijos tinkamumą, todėl vykdoma daug projektų ir tyrimų, siekiant ištirti „blockchain“ įvairioms programoms ir įvertinti jo pridėtinę vertę, bei įgyvendinimo iššūkius.

Įmonė „Blue Freedom“ vadovauja energetikos sektoriaus pertvarkai, naudodama pažangiausias „blockchain“ ir decentralizuotos autonominės organizacijos (DAO) technologijas. Jie rekomenduoja energijos tinklo apsauga: „Cyber Kill Chain“ taikymas „Blockchain“.

Štai kaip kibernetinio žudymo grandinė taikoma siekiant sustiprinti blokų grandinės saugumą energetikos sektoriuje:

B	C	D	E	F
CYBER KILL CHAIN				
0x01 Žvalgyba	**0x02 Ginklavimas**	**0x03 PRISTATYMAS**	**0x04 IŠNAUDOJIMAS**	**0x05 DIEGIMAS**
Tradiciniai metodai, tokie kaip prievadų nuskaitymas ir tinklo pirštų atspaudų ėmimas, yra pritaikyti blokų grandinės mazgų ir susijusios infrastruktūros pažeidžiamumui nustatyti. Pažangūs blokų grandinės analizės įrankiai (įrodinėjimo įstaigos (PoS) protokolai) toliau aptinka įtartiną veiklą tinkle, pvz., neįprastus sandorių modelius arba bandymus manipuliuoti sutarimo mechanizmais.	Kai užpuolikai nustato pažeidžiamumą, užpuolikai sukurs kenkėjiškas programas arba išnaudojimus, specialiai sukurtus jiems nukreipti. Reguliarūs programinės įrangos atnaujinimai, pataisų valdymo sistemos, kodų peržiūros (GitFlow) ir reguliarūs saugos auditai, siekiant sumažinti šią riziką.	**„Eclipse“ atakos (izoliuokite mazgą nuo likusio tinklo), „Sybil“ atakos (įgykite tinklo valdymą sukurdami kelias netikras tapatybes) ir „Timejacking“ atakos (manipuliuokite „blockchain“ laiko žymą, kad sutrikdytumėte sutarimą ir sukurtumėte šakes), maršruto parinkimo atakos. (Perimti ir modifikuoti blockchain srautą) veikia kaip Trojos arkliai, atakuojantys grandinės tinklą. Diegiant mazgų diversifikavimą, šifravimą ir raktų valdymą, „ Proof-of-Stake“ (PoS) konsensuso algoritmą ir nuolatinį stebėjimą bei auditą galima veiksmingai blokuoti tokius pristatymo bandymus.**	**Kai kenkėjiška programa įsiskverbia į tinklą, užpuolikai dažnai bando išnaudoti blokų grandinės protokolų ar išmaniųjų sutarčių spragas. Naudojant oficialius tikrinimo metodus ir griežtą kodo peržiūrą (Sauga kaip kodas (SaC)) kūrimo metu žymiai sumažėja eksploatuojamo paviršiaus plotas. Be to, konsensuso mechanizmai, tokie kaip PoS, užtikrina, kad visi tinklo dalyviai susitartų dėl operacijų galiojimo ir blokų grandinės būsenos, o ji realiu laiku aptiks kenkėjiškus veiksmus.**	Pagrindinis užpuolikų tikslas dažnai yra kontroliuoti svarbiausią infrastruktūrą arba pavogti neskelbtinus duomenis. Kriptografija veikia kaip tvirtas vartų sargas, užtikrinantis, kad tik įgalioti subjektai galėtų prieiti ir sąveikauti su blokų grandinės tinklu. Norint patikrinti informaciją neatskleidžiant pagrindinių slaptų duomenų, nulinės žinios įrodymas (ZKP) užtikrina aukštą saugumo ir privatumo lygį.

Šaltinis:sudaryta autorės pagal „Blue Freedom“ 2023

16 pav. Energijos tinklo apsauga: „Cyber Kill Chain“ taikymas „Blockchain“

Kibernetinė žudymo grandinė suteikia vertingą pagrindą norint suprasti ir sumažinti kibernetines grėsmes blokų grandinės tinkluose. Taikydamos daugiasluoksnį metodą, apimantį kiekvieną nužudymo grandinės etapą, energetikos įmonės gali užtikrinti savo blokų grandinės diegimo saugumą ir vientisumą, atverdamos kelią saugesnei ir atsparesnei energetikos ateičiai.

IŠVADOS

1. Išanalizavus blokų grandinės technologijos struktūrą, veikimo principą ir reikšmę šiandieninėje sistemoje, galima teigti, kad blokų grandinės technologija turi perspektyvų ateityje. Tai galėtų būti puiki niša inovacijoms. Blokų grandinės technologijai kol kas būdingas sudėtingumas, todėl jos diegimui reikalingos didelės pastangos ir ištekliai.
2. Ištyrus blokų grandinės technologijos taikymą energetiniame sektoriuje galima teigti, kad blokų grandinėmis pagrįstų technologijų, sprendimų ir paslaugų diegimas pasaulinėje energetikos pramonėje sparčiai auga. Atsižvelgiant į šiame darbe analizuotus verslus, galimybė panaudoti blokų grandinės technologiją, pavyzdžiui, žaliajai energijai, yra perspektyviausia. Blokų grandinės technologija leidžia tiksliai sekti energijos suvartojimą, gamybą ir valdymą. Tai leidžia efektyviau paskirstyti energijos išteklius, sumažinti atliekų kiekį ir sumažinti išlaidas atsinaujinančios energijos operatoriams.
3. Išanalizavus kibernetinį saugumą „blockchain“ energetikos sektoriuje. Pirmiausia pastebėta, kad mažai mokslinių šaltinių susijusia tema. Blokų grandinė didina saugumą – padeda sumažinti atakų ir sukčiavimo riziką. Tiriant blokų grandinės taikymą energetikos sektoriuje Europoje ir visame pasaulyje, ji yra plačiai taikoma visuose sektoriuose, bet nėra populiari dėl techninio sudėtingumo ir teisinio neapibrėžtumo. „Blockchain“ technologija gali pagerinti kibernetinį saugumą energetikos sektoriuje siūlydama decentralizuotą ir apsaugotą nuo klastojimo sistemą, skirtą stebėti ir registruoti operacijas. Tai padidina ypatingos svarbos infrastruktūros ir jautrių duomenų saugumą, todėl kibernetinėms grėsmėms bus sunkiau pažeisti sistemos vientisumą arba pasiekti konfidencialią informaciją
4. Atlikus atvejų analizę, prieita išvada, kad norint sėkmingai veikiančios platformos, reikia pasirinkti tinkamą konsensuso mechanizmą pagal įmonės poreikius, nes nuo tinkamo konsensuso mechanizmo priklauso, kokiu greičiu bus vykdomos operacijos. Atlikus tyrimą pastebėta, kad programos sukūrimas remiantis blokų grandinės technologija reikalauja daug kaštų. Ištyrus ekspertų požiūrius į blokų grandinės technologiją energetikos sektoriuje, galima teigti, kad vyraujanti nuomonė, jog blokų grandinė turi ateitį, bet šiuo metu nėra tam didelio poreikio.
5. Siekiant pagerinti kibernetinį saugumą svarbu suprasti, saugumas yra nuolatinis procesas, o ne fiksuota būsena. Informacinių technologijų specialistai, turi nuolat reaguoti į naujas grėsmes ir kurti strategijas kaip įveikti kylančius iššūkius. Kadangi informacinių technologijų aplinka tampa sudėtingesnė ir atsiranda naujų grėsmių, visada atsiras kliūčių priimti naujas technologijas ir sprendimus. Todėl organizacijos turi laikytis subalansuoto požiūrio, atsižvelgiant į pokyčius ir atidžiai valdyti susijusią riziką, kad išvengtų nepriimtino lygio rizikos. Labai svarbu, kad Europoje būtų laikomasi tokių įstatymų kaip Bendrasis duomenų apsaugos reglamentas (BDAR), kuris įpareigoja apsaugoti asmens duomenis ir privatumą. Nekintama „blockchain“ prigimtis kelia iššūkių laikantis teisės į trynimą („teisė būti pamirštam“) ir teisės atnaujinti. Turi būti laikomasi specialių energetikos sektorių

reglamentuojančių taisyklių, kurios gali skirtis priklausomai nuo regiono. Šios taisyklės gali turėti įtakos energijos sandorių ir duomenų registravimui ir dalijimuisi blokų grandinėje. Jei „blockchain“ naudojama finansinėms operacijoms, pvz., prekybai energijos kreditais, įmonės turi apsvarstyti galimybę laikytis finansinių taisyklių ir kovos su pinigų plovimu (AML) įstatymų.

6. Blokų grandinės technologija gali pagerinti kibernetinį saugumą energetikos sektoriuje siūlydama decentralizuotą ir apsaugotą nuo klastojimo sistemą, skirtą stebėti ir registruoti operacijas. Tai padidina ypatingos svarbos infrastruktūros ir jautrių duomenų saugumą, todėl kibernetinėms grėsmėms bus sunkiau pažeisti sistemos vientisumą arba pasiekti konfidencialią informaciją. Verslo, energetikos sektoriui saugiau ir parankiau rinktis privačios blokų grandinės modelį dėl aiškesnės galimybės įrodyti, jog duomenų valdytojas laikėsi asmens duomenų apsaugos taisyklių.

LITERATŪRA

1. A A Simaremare* , I A Aditya, F N Haryadi and H Indrawan, (2020). *Suitability study of Blockchain application in electric utility company business processes.* IOP Conference Series: Materials Science and Engineering. Indonesia. doi : 10.1088/1757-899X/1098/5/052105.
2. Abou Chacra, S., Sireli, Y. and Cali, U. (2018), "*An overview of the systems of P2P blockchain technology in the energy industry*", Proc. of the ASEM Conference, October 17-20, Coeur D'Alene, ID.
3. ACCIONA to sell carbon credits on ClimateTrade blockchain, 2020. Prieiga per internetą: https://www.ledgerinsights.com/carbon-credit-blockchain-acciona-climatetrade/
4. Akira Summers, (2022). *Basic principles of blockchain.* Prieiga per internetą: https://www-taylorfrancis-com.skaitykla.mruni.eu/chapters/mono/10.1201/9781003187165-2/basic-principles-blockchain-akira-summers?context=ubx&refId=d105c0fb-f34c-4b20-88c7-af336d57e716
5. Alrammal, Muath, Fadi Abu-Amara, Zamhar Ismail, and Muhammad Nadeem. 2023. "Blockchain Technology for Sustainable Management of Electricity and Water Consumption" *Engineering Proceedings* 59, no. 1: 223. https://doi.org/10.3390/engproc2023059223
6. Anak Agung Gde Agung, Rini Handayani, 2022, Blockchain for smart grid, Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 3, Pages 666-675, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2020.01.002.
7. Basden, J. and Cottrell, M. (2017), "*How utilities are using blockchain to modernize the grid*", available at: https://hbr.org/2017/03/how-utilities-are-using-blockchain-to-modernize-the-grid
8. Bela Shrimali, Hiren B. Patel, 2022 Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities, Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 9, Pages 6793-6807, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2021.08.005.
9. Berman DS, Buczak AL, Chavis JS, Corbett CL., 2019 A Survey of Deep Learning Methods for Cyber Security. *Information*.; 10(4):122. https://doi.org/10.3390/info10040122
10. Bryman, A., & Bell, E. (2015). Business research methods (Fourth edition). https://www.academia.edu/35725749/Business_Research_Methods_by_Bryman_A_and_Bell_E_2015_1_
11. Chacra, S.A., Sireli, Y. and Cali, U. (2021), "A review of worldwide blockchain technology initiatives in the energy sector based on go-to-market strategies", *International Journal of Energy Sector Management*, Vol. 15 No. 6, pp. 1050-1065. https://doi-org.skaitykla.mruni.eu/10.1108/IJESM-05-2019-0001

12. D. Hornsteiner, S.Hasenleithner, V. Pesendorfer, 2020, p. 14, Blockchain. Priega per internetą: https://www.cosy.sbg.ac.at/~uhl/PScrypt20/Blockchain_Text.pdf
13. Debatosh Pal Majumder, (2022). *Blockchain.* Department of CSE, Netaji Subhash Engineering College, Kolkata, India. Prieiga per internetą: https://www-taylorfrancis-com.skaitykla.mruni.eu/chapters/edit/10.1201/9781003203957-3/study-consensus-algorithms-blockchain-debatosh-pal-majumder?context=ubx&refId=d451628f-8fb6-4f42-9143-b6357c975288
14. Delmolino, K.; Arnett, M.; Kosba, A.; Miller, A.; Shi, E., 2016 Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados; pp. 79–94. [Google Scholar]
15. Desen Kirli, Benoit Couraud, Valentin Robu, Marcelo Salgado-Bravo, Sonam Norbu, Merlinda Andoni, Ioannis Antonopoulos, Matias Negrete-Pincetic, David Flynn, Aristides Kiprakis,Smart contracts in energy systems: A systematic review of fundamental approaches and implementations, Renewable and Sustainable Energy Reviews, Volume 158, 2022, 112013, SSN 1364-0321, https://doi.org/10.1016/j.rser.2021.112013.
16. Dominique Guegan. Public Blockchain versus Private blockhain. 2017. ⟨halshs-01524440⟩
17. Dr Zoya Pourmirza, 2023. *Cybersecurity in centralised vs decentralised energy systems*. NEWCASTLE UNIVERSITY FEBRUARY 2023. https://www.ncl.ac.uk/media/wwwnclacuk/supergenenergynetwork/files/Cyber%20Security%20in%20Centralised%20vs%20Decentralised%20Energy%20Systems%20(2).pdf
18. Eligijus Sakalauskas, Narimantas Listopadskis, Gediminas Simonas Dosinas, 2008. Kriptografijos teorija. Mokomoji knyga. Kauno technologijos universitetas.
19. Gad, AG, Mosa, DT, Abualigah, L. ir Abohany, AA (2022). Naujos blockchain technologijos ir programų tendencijos: apžvalga ir perspektyvos. *King Saudo universiteto žurnalas - Computer and Information Sciences* , *34* (9), 6719–6742. https://doi-org.skaitykla.mruni.eu/10.1016/j.jksuci.2022.03.007
20. Gans, RB, Ubacht, J. ir Janssen, M. (2022). „Blockchain“ pagrindu sukurtų savarankiškų tapatybių valdymas ir poveikis visuomenei. Politika ir visuomenė , 41 (3), 402–413. https://doi-org.skaitykla.mruni.eu/10.1093/polsoc/puac018
21. Goudz, A., Jasarevic, M. (2020). Einleitung. In: Einsatz der Blockchain-Technologie im Energiesektor. essentials. Springer Gabler, Wiesbaden. https://doi.org/10.1007/978-3-658-31120-9_1
22. Guo Mingxing, Zhang Ke, Wang Su, Xia Jinlei, Wang Xiaohui, Lan Li, Wang Lingling, 2023, Peer-to-peer energy trading and smart contracting platform of community-based virtual power plant

Frontiers in Energy Research , VOLUME=10, URL=https://www.frontiersin.org/articles/10.3389/fenrg.2022.1007694 DOI=10.3389/fenrg.2022.1007694, ISSN=2296-598X.

23. Haque, AB, Naqvi, B., Najmul Islam, AKM ir Hyrynsalmi, S. (2021). Su GDPR suderinamo „blockchain“ pagrindu sukurto COVID vakcinacijos paso link. *Applied Sciences* , *11* (13), 6132. https://doi-org.skaitykla.mruni.eu/10.3390/app11136132
24. Hirsh, Sandra, Alman, Susan Webreck, (2020). *Blockchain.* Chicago : ALA Neal-Schuman.. Prieiga per internetą: https://web-p-ebscohost-com.skaitykla.mruni.eu/ehost/detail/detail?vid=5&sid=5b10ab9a-0eaf-4ca0-a8be-f592475360bf%40redis&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=e000xww&AN=2479358
25. Honari K, Rouhani S, Falak NE, Liu Y, Li Y, Liang H, Dick S, Miller J., 2023 Smart Contract Design in Distributed Energy Systems: A Systematic Review. *Energies*. 16(12):4797. https://doi.org/10.3390/en16124797
26. Hussein, Z., Salama, M.A. & El-Rahman, S.A., (2023). Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms. *Cybersecurity* **6**, https://doi-org.skaitykla.mruni.eu/10.1186/s42400-023-00163-y
27. Yaga, D. , Mell, P. , Roby, N. and Scarfone, K. (2018), Blockchain Technology Overview, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8202 (Accessed December 20, 2023)
28. Yannis Bakos, Hanna Halaburda, 2021. Permissioned vs Permissionless Blockchain Platforms: Tradeoffs in Trust and Performance, NYU Stern School of Business working paper, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3789425
29. Yin, R. K. (2011). Qualitative research from start to finish. Guilford Press. https://eli.johogo.com/Class/Qualitative%20Research.pdf
30. Imran Bashir. (2018). *Mastering Blockchain - Second Edition : Distributed Ledger Technology, Decentralization, and Smart Contracts Explained*. Packt Publishing. https://search-ebscohost-com.skaitykla.mruni.eu/login.aspx?direct=true&db=e000xww&AN=1789486&site=ehost-live
31. JRC Technical Report. 2021 ISBN 978-92-76-40551-1 ISSN 1831-9424 doi:10.2760/416731
32. Juszczyk, Oskar, and Khuram Shahzad. 2022. "Blockchain Technology for Renewable Energy: Principles, Applications and Prospects" *Energies* 15, no. 13: 4603. https://doi.org/10.3390/en15134603
33. Khubrani MM, Alam S., 2023 Blockchain-Based Microgrid for Safe and Reliable Power Generation and Distribution: A Case Study of Saudi Arabia. *Energies (19961073)*.;16(16):5963. doi:10.3390/en16165963

34. Kim, Seong-Kyu, and Jun-Ho Huh. 2018. "A Study on the Improvement of Smart Grid Security Performance and Blockchain Smart Grid Perspective" *Energies* 11, no. 8: 1973. https://doi.org/10.3390/en11081973 Straipsnis: https://www.power-technology.com/news/acciona-blockchain-renewable-generation/
35. Knyga: Alexander Frier.(2024). Blockchain in the Energy Sector. An Advancing Technology to Tackle Global Climate Change? Columbia University Press.
36. Lannquist, A.; Raycraft, R.D., 2020 *Exploring Blockchain Technology for Government Transparency: Blockchain-Based Public Procurement to Reduce Corruption*; World Economic Forum: Davos, Switzerland, 21–24 January; Insight report. [Google Scholar]
37. Li, D., Luo, Z. & Cao, B., (2022) Blockchain pagrindu sukurtos jungtinės mokymosi metodikos išmaniosiose aplinkose. *Cluster Comput* **25**, 2585–2599. https://doi-org.skaitykla.mruni.eu/10.1007/s10586-021-03424-y
38. Liu, M., Yeoh, W., Jiang, F., & Choo, K. K. R. (2022). Blockchain for Cybersecurity: Systematic Literature Review and Classification. *Journal of Computer Information Systems*, *62*(6), 1182–1198. https://doi-org.skaitykla.mruni.eu/10.1080/08874417.2021.1995914
39. Livingston, D., Sivaram, V., Freeman, M., & Fiege, M. (2018). *Applying Blockchain Technology to Electric Power Systems*. Council on Foreign Relations. http://www.jstor.org/stable/resrep21340
40. M. Nour, J. P. Chaves-Ávila and Á. Sánchez-Miralles, 2022. "Review of Blockchain Potential Applications in the Electricity Sector and Challenges for Large Scale Adoption," in IEEE Access, vol. 10, pp. 47384-47418, 2022, doi: 10.1109/ACCESS.2022.3171227.
41. Martin, C. (2018). *How blockchain is threatening to kill the traditional utility*. Bloomberg.Com. Prieiga per internetą: https://www.bloomberg.com/news/articles/2018-04-09/blockchain-latest-death-knell-of-an-old-school-utility-model#xj4y7vzkg
42. Mourtzis, Dimitris, John Angelopoulos, and Nikos Panopoulos. 2023. "Blockchain Integration in the Era of Industrial Metaverse" *Applied Sciences* 13, no. 3: 1353. https://doi.org/10.3390/app13031353
43. Mukherjee, Pratyusa & Pradhan, Chittaranjan. (2021). Blockchain 1.0 to Blockchain 4.0—The Evolutionary Transformation of Blockchain Technology. 10.1007/978-3-030-69395-4_3.
44. Nai Fovino, I., Andreadou, N., Geneiatakis, D., Giuliani, R., Kounelis, I., Lucas, A., Marinopoulos, A., Martin, T., Poursanidis, I., Soupionis, I. and Steri, G. 2021, Blockchain in the Energy Sector, EUR 30782 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-40552-8, doi:10.2760/061600, JRC125221.
45. Niranjanamurthy, M., Nithya, B.N. & Jagannatha, S. (2019). Analysis of Blockchain technology: pros, cons and SWOT. *Cluster Comput* **22** (Suppl 6), 14743–14757 . https://doi.org/10.1007/s10586-018-2387-5

46. Paul J. Taylor, Tooska Dargahi, Ali Dehghantanha, Reza M. Parizi, Kim-Kwang Raymond Choo, 2020, A systematic literature review of blockchain cyber security, Digital Communications and Networks, Volume 6, Issue 2, , Pages 147-156, ISSN 2352-8648, https://doi.org/10.1016/j.dcan.2019.01.005.
47. Paul J. Taylor, Tooska Dargahi, Ali Dehghantanha, Reza M. Parizi, Kim-Kwang Raymond Choo, A systematic literature review of blockchain cyber security, Digital Communications and Networks, Volume 6, Issue 2, 2020, Pages 147-156, ISSN 2352-8648, https://doi.org/10.1016/j.dcan.2019.01.005.
48. Paul, P and Aithal, P. S. and Saavedra, R. and Ghosh, Surajit, Blockchain Technology and Its Types—A Short Review (December 26, 2021). International Journal of Applied Science and Engineering (IJASE), 9(2), 189-200. (2021). ISSN: 2321-0745. , Available at SSRN: https://ssrn.com/abstract=4050933
49. Pohlmann, N. (2022). Blockchain-Technologie. In: Cyber-Sicherheit. Springer Vieweg, Wiesbaden. https://doi.org/10.1007/978-3-658-36243-0_14
50. Powerledger light Paper. Prieiga per internetą : https://assets.website-files.com/612e1d86b8aa434030a7da5c/64f1a32db7bd18d4e09bc6b0_powerledger-lightpaper.pdf
51. Projektas *European Distributed Data Infrastructure for Energy*, prieiga per internetą: https://cordis.europa.eu/project/id/101069510
52. Qiang Wang, Min Su, 2020. Integrating blockchain technology into the energy sector — from theory of blockchain to research and application of energy blockchain, Computer Science Review, Volume 37, 100275, ISSN 1574-0137, https://doi.org/10.1016/j.cosrev.2020.100275.
53. Qiang Wang, Rongrong Li, Lina Zhan, (2021). *Blockchain technology in the energy sector: From basic research to real world applications.* Prieiga per internetą: https://doi.org/10.1016/j.cosrev.2021.100362
54. Ryan, R., & Donohue, M. (2017). Securities on Blockchain. *The Business Lawyer*, *73*(1), 85–108. https://www.jstor.org/stable/26419192
55. Ridoan Karim, Imtiaz Sifat, (2022). *Blockchain technology*. Prieiga per internetą: https://www-taylorfrancis-com.skaitykla.mruni.eu/chapters/edit/10.1201/9781003138082-7/blockchain-technology-energy-industry-ridoan-karim-imtiaz-sifat?context=ubx&refId=f729c545-6913-4963-928e-49b0b9d0265f
56. Robert Sheldon, (2021). *A timeline and history of blockchain technology*. TechTarget. Prieiga per internetą: https://www.techtarget.com/whatis/feature/A-timeline-and-history-of-blockchain-technology.

57. Samreen Mahmood, Mehmood Chadhar and Selena Firmin, 2022.„ Cybersecurity Challenges in Blockchain Technology: A Scoping Review“. Prieiga per internetą: https://doi.org/10.1155/2022/7384000
58. Seyed Mojtaba Hosseini Bamakan, Amirhossein Motavali, Alireza Babaei Bondarti, A survey of blockchain consensus algorithms performance evaluation criteria, Expert Systems with Applications, Volume 154, 2020, 113385, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2020.113385.
59. Shekh S. Uddin, Rahul Joysoyal, Subrata K. Sarker, S.M. Muyeen, Md. Firoj Ali, Md. Mehedi Hasan, Sarafat Hussain Abhi, Md. Robiul Islam, Md. Hafiz Ahamed, Md. Manirul Islam, Sajal K. Das, Md. Faisal R. Badal, Prangon Das, Zinat Tasneem, Next-generation blockchain enabled smart grid: Conceptual framework, key technologies and industry practices review, Energy and AI, Volume 12, 2023, 100228, ISSN 2666-5468, https://doi.org/10.1016/j.egyai.2022.100228.
60. Straipsnis „ACCIONA uses blockchain to secure its energy management software“ (2020) : https://www.acciona.com/updates/news/acciona-uses-blockchain-to-secure-its-energy-management-software/
61. Straipsnis „Blockchain Council proof of History“ (2024) prieiga per internetą: https://www.blockchain-council.org/blockchain/what-is-proof-of-history-and-how-does-it-work/
62. Straipsnis „Blockchain Council blockchain technology“ (2024) prieiga per internetą: https://www.blockchain-council.org/blockchain/what-is-blockchain-technology-and-how-does-it-work/?gad_source=1&gclid=EAIaIQobChMItcH269GjhAMV4K-DBx2APwczEAMYASAAEgJl8vD_BwE
63. Straipsnis „Tectum“ (2023) prieiga per internetą: https://tectum.io/blog/practical-byzantine-fault-tolerance/
64. Straipsnis apie Acciona įmonę (2018) prieiga per internetą: https://www.pv-magazine.com/2018/09/28/acciona-presents-worlds-first-blockchain-renewable-energy-certification-platform/
65. Straipsnis apie įmonę *Phonton* per interneto prieigą: https://www.linkedin.com/company/ponton-consulting/
66. Straipsnis *Blockchain for Cybersecurity and Grid Modernization* : https://www.pnnl.gov/projects/blockchain-cybersecurity-and-grid-modernization
67. Straipsnis Blockchain, Smart Contracts, Smart Metering – Neue Perspektiven für den Peer-to-Peer-Energiehandel?(2021): https://www.kuemmerlein.de/aktuelles/einzelansicht/blockchain-smart-contracts-smart-metering-neue-perspektiven-fuer-den-peer-to-peer-energiehandel

68. Straipsnis ES mokslo centre, Jungtinių tyrimų centras, 2022. *Could blockchain revolutionise the energy market?*. Prieiga per internetą: https://joint-research-centre.ec.europa.eu/jrc-news/could-blockchain-revolutionise-energy-market-2022-03-16_lt
69. Straipsnis „Cyber kill chain“ (2023). Prieiga per internetą: https://www.linkedin.com/pulse/securing-grid-how-cyber-kill-chain-fortifies-energy-blockchain-hgtie?trk=article-ssr-frontend-pulse_more-articles_related-content-card
70. Straipsnis *Powerledger (POWR): An Energy-Efficient Blockchain for a Carbon-Free Future*, (2023) prieiga per internetą*:* https://learn.bybit.com/blockchain/what-is-powerledger-powr/
71. Tatjana Bilevičienė, Steponas Jonušauskas (2011). STATISTINIŲ METODŲ TAIKYMAS RINKOS TYRIMUOSE ,vadovėlis .Vilnius.
72. Wang, J., Wang, Q., Zhou, N., & Chi, Y. (2017). A novel electricity transaction mode of microgrids based on blockchain and continuous double auction. Energies, 10(12), 1971. https://doi .org /10 .3390 /en10121971Yeoh, P.
73. Zeel Dabhi, & Aishwarya. (2023). Blockchain Challenges: Advantages and Algorithms. Journal of Advancement in Software Engineering and Testing, 6(2), 1–13. https://doi.org/10.5281/zenodo.7901941

Urbaitė L. (2024). *Blokų grandinės technologijos energetikos sektoriuje: kibernetinio saugumo iššūkiai ir galimybės* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

ANOTACIJA

Magistro baigiamajame darbe išanalizuoti blokų grandinės raidos teoriniai aspektai, jos taikymas energetiniame sektoriuje ir įvertintas kibernetinis saugumas blokų grandinės technologijoje. Nustatyta kaip plačiai pasaulyje naudojama blokų grandinė. Atvejo studijos metodu pateiktas praktinis blokų grandinės technologijos taikymas įmonėse ir ištirtas ekspertų požiūris į kibernetinį saugumą organizacijose ir blokų grandinėje. Pirmame skyriuje nagrinėjama blokų grandinės raida, veikimas ir klasifikacija, pateikiami mokslininkų atlikti tyrimai, blokų grandinės privalumai ir trūkumai, kibernetinio saugumo apžvalga blokų grandinės technologijoje. Antrame darbo skyriuje yra nagrinėjama blokų grandinė energetikos sektoriuje remiantis įvairių autorių požiūriu, analizuojami diegimo iššūkiai ir kibernetinės atakos prieš blokų grandinę. Trečiame skyriuje pateikiama tyrimo metodologija: tyrimo tikslo pagrindimas, organizavimas, imtis ir tyrimo dizainas. Ketvirtame skyriuje pateikiama atvejų analizės rezultatai, pateikiamas ekspertų požiūris į blokų grandinę ir kibernetinį saugumą, susisteminami ekspertinio tyrimo metu gauti duomenys. Darbo pabaigoje yra pateikiamos išvados bei siūlymai.

Pagrindiniai žodžiai: blokų grandinė, energetikos sektorius, kibernetinis saugumas.

Urbaitė L. (2024). *Blockchain technologies in the energy sector: cybersecurity challenges and opportunities (master thesis).* Vilnius: Mykolas Romeris University

ANNOTATION

In the master thesis analysed the theoretical aspects of blockchain development, its application in the energy sector, and evaluated cybersecurity in blockchain technology. Established as a widely used blockchain. The case study method presents the practical application of blockchain technology in companies, and experts' views on cybersecurity in organizations and blockchain were explored. In the first part of thesis examines the evolution, operation, and classification of blockchain, presents research conducted by scientists, advantages, and disadvantages of blockchain, and an overview of cybersecurity in blockchain technology. The second chapter explores blockchain in the energy sector based on various authors' perspectives, analyses deployment challenges and cyber-attacks against blockchain. The third chapter presents the research methodology: justification of research objectives, organization, data collection, and research design. The fourth chapter presents the results of the cases analysis, expert views on blockchain and cybersecurity, systematizes data obtained during the expert research. The conclusions and recommendations are provided at the end of the thesis.

Key words: blockchain, energy sector, cybersecurity

Urbaitė L. (2024). *Blokų grandinės technologijos energetikos sektoriuje: kibernetinio saugumo iššūkiai ir galimybės* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

SANTRAUKA

Magistro baigiamojo darbo tema aktuali šiuolaikinėms įmonėms, verslininkams, valstybėms ir visiems asmenims, kuriuos domina kibernetinis saugumas ir inovacijos. Darbe analizuojama problematika, susijusi su blokų grandine energetikos sektoriuje. Blokų grandinės technologija yra mažai kam suprantama, dėl to buvo iškelta pagrindinė tyrimo problema – ar blokų grandinės technologijos taikymas energetikos sektoriuje gali užtikrinti saugumą ir efektyvumą? Tyrimo objektas – blokų grandinės technologija energetikos sektoriuje. Šio tyrimo tikslas ištirti blokų grandinės taikymo ypatumus ir galimybes, pranašumus ir trūkumus energetikos sektoriuje. Pateikti kibernetinio saugumo galimybes ir iššūkius taikant blokų grandinę bei pateikti rekomendacijas.

Tyrimo metodika: mokslinės literatūros analizė, atliekant tyrimą taikyta kiekybinė (statistinių duomenų apžvalga ir analizė) bei kokybinė tyrimo (atvejo studijos analizė, ekspertinis tyrimas – pusiau struktūruotas interviu) strategijos. Kokybinio tyrimo instrumentas - klausimynas. Duomenų analizės metodai: duomenų turinio analizės metodas. Atvejų analizė atskleidė, įmonių veiklos principus su blokų grandine. Visos įmonės naudoja skirtingus konsensuso mechanizmus, visuomet bendradarbiauja su kitomis įmonėmis ir kreipiasi pagalbos pas profesionalus. Kaip parodė tyrimas blokų grandinė reikalauja daug investicijų, bet svarbu pabrėžti naudodamos įmonės blokų grandinę, užsitarnauja pasitikėjimą, nes yra garantuojama, kad duomenys yra skaidrūs ir nekeičiami. Ekspertinio tyrimo metu buvo nustatyta, kad pagrindiniai veiksniai, kodėl blokų grandinė nėra plačiai naudojama yra reguliavimo ir įstatyminės bazės neapibrėžtumas. Respondentai pabrėžė, kad kyla problemų suderinimų su esamomis sistemomis, tačiau neatmeta galimybių naudoti blokų grandinės ateityje.

Įvertinus visą tyrimą, galima teigti, kad blokų grandinė yra saugi naudoti, tačiau tai reikalauja didelių investicijų: piniginių ir žinių. Žinoma, atakų rizika taip pat yra, tačiau vertinant šios programos teikiamus privalumus: atsekamumą, efektyvumą, skaidrumą ir duomenų vientisumą, galima teigti, kad blokų grandinė teikia perspektyvų ateityje.

Urbaitė L. (2024). *Blockchain technologies in the energy sector: cybersecurity challenges and opportunities (master thesis).* Vilnius: Mykolas Romeris University

SUMMARY

The topic of the Master's thesis is relevant to modern enterprises, entrepreneurs, governments, and all individuals interested in cybersecurity and innovation. The thesis analyzes issues related to blockchain in the energy sector. The blockchain technology is not well understood by many, hence the main research problem was raised - can the application of blockchain technology ensure security and efficiency in the energy sector? The object of the research is blockchain technology in the energy sector. The aim of this research is to explore the peculiarities and possibilities, advantages and disadvantages of applying blockchain in the energy sector. It aims to present cybersecurity opportunities and challenges when using blockchain and provide recommendations. Research methodology: analysis of scientific literature, quantitative research (review and analysis of statistical data), and qualitative research (analysis of case studies, expert investigation - semi-structured interviews) strategies were applied in the study. The instrument of qualitative research is a questionnaire. Data analysis methods: content analysis method. The analysis of cases revealed the principles of companies' operations with blockchain. All companies use different consensus mechanisms, always collaborate with other companies, and seek help from professionals. As the study showed, blockchain requires significant investments, but it is important to emphasize that by using blockchain in a company, trust is earned because it guarantees that data is transparent and unchangeable. During the expert investigation, it was found that the main reasons why blockchain is not widely used are regulatory and legal uncertainties. Respondents emphasized that there are challenges in integrating with existing systems but do not rule out the possibility of using blockchain in the future. Considering the entire study, it can be stated that blockchain is safe to use, but it requires significant investments: financial and knowledge-wise. Of course, there is also a risk of attacks, however, evaluating the advantages provided by this program: traceability, efficiency, transparency, and data integrity, so the blockchain provides prospects for the future.

PRIEDAI

1 PRIEDAS. Interviu klausimai

Linvida Urbaitė
MYKOLO ROMERIO UNIVERSITETAS, LIETUVA
(Ateities g. 20, LT-08303 Vilnius)

Gerb. Respondente,

Esu magistro studijų studentė, šiuo metu rašau magistrinį darbą tema: **„Blokų grandinės technologijos energetikos sektoriuje: kibernetinio saugumo iššūkiai ir galimybės“.**

Labai norėčiau Jums kaip ekspertui užduoti keletą klausimų apie darbo ypatumus. Magistrinio darbo tyrimui atlikti, bus naudojami nuasmeninti Jūsų pateikti atsakymai, įsipareigoju užtikrinti anonimiškumą. Pateikiu klausimus susipažinimui. Tikiuosi Jūsų bendradarbiavimo.

Užtikrinu, kad apklausos metu gauti duomenys išliks konfidencialūs ir bus panaudoti tik apibendrinta forma baigiamajam magistro projektui parengti.

Labai tikiuosi Jūsų pagalbos ir iš anksto dėkoju už Jūsų nuoširdžius atsakymus!

- Pareigos/paskyrimas:…….
- Darbo patirtis:……..metai
- Išsilavinimas.....

1. Kokios yra pagrindinės kibernetinio saugumo grėsmės, su kuriomis susiduria organizacijos šiandieninėje skaitmeninėje erdvėje?
2. Kaip organizacijos gali efektyviai apsaugoti savo duomenis nuo kibernetinių atakų ir pažeidimų?
3. Kokia yra svarbiausia kibernetinio saugumo politika, kurią organizacija turėtų įgyvendinti siekiant užtikrinti duomenų saugumą?
4. Kokius kibernetinio saugumo įrankius ir technologijas vertėtų įtraukti į organizacijos saugumo strategiją?
5. Kaip organizacijos gali užtikrinti, kad jų darbuotojai būtų gerai informuoti ir apmokyti dėl kibernetinių grėsmių bei saugumo priemonių?
6. Ar esate susipažinęs su „Blockchain“ technologija ir ar naudojate ją kasdienėje verslo veikloje?
7. Jei TAIP, paaiškinkite pagrindinę priežastį, jei NE, paaiškinkite pagrindinę priežastį.

8. Jei TAIP – kokie veiksniai įtikino jus įdiegti BC (Blockchain) savo įmonėje? Jei NE, kokios BC funkcijos, jūsų manymu, gali būti naudingos(arba nenaudingos) jūsų įmonei ateityje?

9. Jei TAIP – kuriuose jūsų įmonės skyriuose naudojate „Blockchain“? Jei NE – kuriuose savo įmonės padaliniuose galėtumėte naudoti BC ateityje (kur tiksliai yra poreikis įmonėje, kuriame skyriuje, verslo srityje ir tt.ir kodėl?

10. Kaip įvertintumėte savo patirtį naudojant BC? jei NE – 1–5 skalėje, kaip tikėtina, kad ateityje naudosite „Blockchain“ ir kodėl?

11. Jei naudojate „Blockchain“ kokiomis pagrindinėmis kliūtimis iki šiol susidūrėte? Jei NE – kokie pagrindiniai galimi BC naudojimo trūkumai (veiksniai, neleidžiantys jūsų įmonei įgyvendinti BC)?

12. Kaip matote BC ateitį atsinaujinančios energijos sektoriuje? Kaip jūs numatote „blockchain“ vaidmenį atsinaujinančios energijos sektoriuje ir kokią įtaką, tai turėtų veiklos meistriškumui, verslo modeliams ir vertės pasiūlymams?

13. Ar galite pateikti apžvalgą, kaip blokų grandinės technologija šiuo metu naudojama energetikos sektoriuje ir galimi jos pritaikymai?

14. Kokie yra pagrindiniai iššūkiai ir kliūtys diegti blokų grandinę energetikos sektoriuje ir kaip jas spręsti?

15. Kaip „blockchain“ technologija galėtų sustiprinti kibernetinio saugumo priemones energetikos sektoriuje, ypač apsaugant kritinę infrastruktūrą ir jautrius duomenis nuo kibernetinių grėsmių?

16. Kaip vertinate galimą riziką ir pažeidžiamumą, susijusį su blokų grandinės integravimu į energijos sistemas kibernetinio saugumo požiūriu?

17. Į kokius reguliavimo aspektus ir atitikties reikalavimus turi atsižvelgti energetikos įmonės, priimdamos blokų grandinę kibernetinio saugumo tikslais?

18. Kaip manote, kodėl Lietuvoje neišsilaikė nė vienas startuolis su „blockchain“?

19. Gal žinote, daug geresnių alternatyvių, nei blokų grandinė? Kokios Jos?

20. Kokių priemonių, Jūsų nuomone, reikėtų imtis siekiant pagerinti kibernetinio saugumo esamą padėtį?

21. Ko trūksta Lietuvoje , kad žmonės internete elgtųsi saugiau, mandagiau ir labiau save saugotų ir nedalintų savo asmeninių duomenų?

Pateikti klausimai pagrinde yra susiję su „Blockchain“ , taigi jei į ne visus klausimus bus atsakyta, bus suprantama, tačiau labai vertinsiu išsakytą savo nuomonę apie kibernetinį saugumą ir pasidalijimą savo patirtimi.